



CIB-ESPOL

T
004.6
EGA
C.2

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

**Facultad de Ingeniería en Electricidad y Computación
Licenciatura en Sistemas de Información**

**“Análisis de los Recursos, Servicios de Red, y Diseño de un Esquema
de Seguridades para la Empresa Mafrico S.A.”**

TÓPICO DE GRADUACIÓN

Previa a la obtención del título de:

LICENCIADO EN SISTEMAS DE INFORMACIÓN

Presentado por:



CIB-ESPOL

**Josefina María Egas Alprecht
Christian César Zambrano Intriago
Ángel Edwin Gaona Salinas**



CIB-ESPOL

GUAYAQUIL - ECUADOR

2005

AGRADECIMIENTO

A Dios le doy gracias por todas las bendiciones que ha derramado sobre mi permitiéndome cumplir con otra meta más en mi vida, por darme la fuerza necesaria para poder enfrentar cada obstáculo que se ha presentado en mi camino protegiéndome y cuidándome en cada momento de mi vida.

A mi madre y mis hijos por comprenderme y apoyarme en este difícil camino que es la vida. A mi amigo Harry y compañeros de grupo de proyecto por su invalorable apoyo.

A mis profesores Ing. Albert Espinal, Ing. Néstor Arreaga y Dr. Gustavo Galio por su generoso apoyo, y al personal de la Licenciatura por su paciencia y gentileza demostrada a lo largo de mi carrera.

Infinitas Gracias,

Josefina Egas Alprecht



CIB-ESPOL

AGRADECIMIENTO

Agradezco a Dios que me ha dado fuerzas para terminar el proyecto y por haberme dado la oportunidad de culminar mis estudios en la ESPOL. A mis padres que me apoyaron siempre en el cumplimiento de mis estudios. A todas las personas y amigos bien allegados que de alguna forma aportaron algo para la ejecución de este trabajo.

Gracias,

Christian Zambrano Intriago



CIB-ESPOL

AGRADECIMIENTO

Agradezco a los ingenieros Albert Espinal y Néstor Arreaga, por su guía en el desarrollo de este trabajo, a mis profesores, mis compañeros de grupo, a mis amigos, a la empresa en la cual trabajo Mafrico S.A., sobretodo a Dios y a mis padres.

Ángel Gaona Salinas



CIB-ESPOL

DEDICATORIA

Este trabajo se lo dedico a mi madre y a mis hijos quienes han sido siempre mi inspiración para llevar a cabo todas las metas que me he propuesto en mi vida.

También se lo dedico a mis hermanas que me brindaron su constante apoyo y a quienes siempre he querido que me vean como un buen ejemplo a seguir.

Josefina Egas Alprecht



CIB-ESPOL

DEDICATORIA

A todos los estudiantes de la ESPOL, especialmente para aquellos que necesitan encontrar información acerca de las seguridades en las redes informáticas.

Christian Zambrano Intriago



CIB-ESPOL

DEDICATORIA

Este trabajo lo dedico principalmente a Dios por ser mi guía durante mis años de estudio, a mis padres por su apoyo incondicional y por ser el pilar fundamental para la culminación de mi carrera, a toda mi familia por haber creído en mí y a todos mis amigos. Suerte la mía de haberme rodeado con personas tan maravillosas las cuales me han ayudado a alcanzar esta meta muy valiosa en mi vida, de todo corazón "Gracias".

Ángel Gaona Salinas



CIB-ESPOL

TRIBUNAL DE GRADUACIÓN



MSIG. Mónica Villavicencio.
Coordinadora

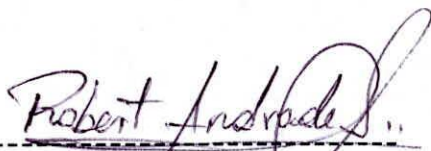


MSIG. Albert Espinal.
Director de Tópico



CIB-ESPOL

MIEMBROS PRINCIPALES



MSIG. Robert Andrade.



MSC. Xavier Ochoa.

DECLARACIÓN EXPRESA

"La responsabilidad por los hechos e ideas expuestas en esta tesis, nos corresponde exclusivamente; y el patrimonio intelectual de la misma, a la **ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**".



Josefina Egas Alprecht



Christian Zambrano Intriago



Ángel Gaona Salinas

RESUMEN

El presente trabajo se lo realizó para la empresa Mafrico S.A., la cual es una empresa líder en el Ecuador en la fabricación y montaje de cámaras para refrigeración, equipos y accesorios. A pesar de ser líder Mafrico es una empresa relativamente pequeña con requisitos de nivel de seguridad informática medios. Actualmente la red tiene algunas vulnerabilidades importantes, como por ejemplo: no existe una cultura de seguridad por parte de los usuarios, en los servidores se ejecutan servicios de red inseguros como: Telnet, FTP anónimo, archivos compartidos, no se encripta el tráfico en la red, ciertos puertos están abiertos y no deberían, no existe un Sistema de Detección de Intrusos en la red y no existe un log que audite el sistema.

Para contrarrestar por lo menos el 60% de las vulnerabilidades, se sugiere hacer cambios importantes en la topología de la red actual. Estos cambios serían: Segmentar la red por medio de la emulación de un router, función que la realizaría un PC que arranca desde un disquete el cual usa el kernel 2.4 de Linux utilizando el software Coyote Linux; se sugiere cerrar puertos innecesarios, desinstalar los servicios que no se usan en la red, instalar y configurar un Sistema de Detección de Intrusos, se configuraría IPTables como Firewall, y restringir el uso a ciertas páginas Web por medio ACLs configuradas en el web-cache del Squid. Además se sugieren en este proyecto políticas de seguridad como complemento, relacionadas al área de Tecnología Informática y se recomienda que todo el personal en general esté en constante capacitación en lo concerniente al uso de los Recursos Informáticos y su Seguridad.



CIB-ESPOL

INDICE GENERAL

	Pág.
INDICE GENERAL	I
INDICE DE TABLAS.....	VII
INDICE DE FIGURAS.....	IX
INTRODUCCIÓN	1
1. CONCEPTOS BASICOS DE SEGURIDAD.....	2
1.1. ¿QUÉ ES SEGURIDAD EN INFORMÁTICA?	2
1.2. ¿CÓMO NACIÓ LA SEGURIDAD INFORMÁTICA?	4
1.3. NIVELES DE HACKERS.....	5
1.4. LA SEGURIDAD EL DÍA DE HOY	6
1.5. ESTANDARIZANDO LA SEGURIDAD	6
1.6. ¿QUÉ QUEREMOS PROTEGER?	7
1.7. ¿DE QUÉ NOS QUEREMOS PROTEGER?	7
1.7.1. PERSONAS	7
1.7.2. AMENAZAS LÓGICAS	8
1.7.3. AMENAZAS EN LAS SEGURIDADES DE LAS REDES	9
1.7.3.1. ARQUITECTURAS INSEGURAS	9
1.7.3.2. REDES BROADCAST.....	9
1.7.3.3. SERVIDORES CENTRALIZADOS	10
1.7.4. AMENAZA A LA SEGURIDAD DE SERVIDORES.....	10
1.7.4.1. SERVICIOS NO USADOS Y PUERTOS ABIERTOS.....	10
1.7.4.2. SERVICIOS NO PARCHADOS	10
1.7.4.3. FALTA DE ATENCIÓN EN LA ADMINISTRACIÓN	11
1.7.4.4. SERVICIOS INHERENTEMENTE INSEGUROS	11
1.7.5. AMENAZAS A LA SEGURIDAD DE LAS ESTACIONES DE TRABAJO. ...	12
1.7.5.1. MALOS PASSWORDS	12
1.7.5.2. APLICACIONES CLIENTE VULNERABLES.....	12
1.7.5.3. BUFFER OVERFLOWS	13
1.7.6. ATAQUES REMOTOS	13
1.7.6.1. ESCANEOS DE PUERTOS	13
1.7.6.2. SPOOFING	14
1.7.6.3. DNS SPOOFING	14
1.7.6.4. ARP SPOOFING	15
1.7.6.5. WEB SPOOFING	15
1.7.6.6. NEGACIONES DE SERVICIO	15
1.7.6.7. INTERCEPTACIÓN	16
1.7.6.8. ATAQUES A APLICACIONES	16
2. SEGURIDAD EN EL ENTORNO DE OPERACIONES.....	18
2.1. INTRODUCCIÓN	18



CIB-ESPOL

2.2. SEGURIDAD FÍSICA DE LOS SISTEMAS	19
2.2.1. PROTECCIÓN DEL HARDWARE	19
2.2.1.1. ACCESO FÍSICO	19
2.2.1.2. DESASTRES NATURALES	20
2.2.1.3. DESASTRES DEL ENTORNO	21
2.2.2. PROTECCIÓN DE LOS DATOS	23
2.2.2.1. INTERCEPCIÓN	23
2.2.2.2. RESPALDOS	24
2.2.2.3. OTROS ELEMENTOS.....	24
2.3. ADMINISTRADORES, USUARIOS Y PERSONAL	25
2.3.1. INTRODUCCIÓN	25
2.3.2. ATAQUES POTENCIALES.....	26
2.3.2.1. INGENIERÍA SOCIAL.....	26
2.3.2.2. SHOULDER SURFING	26
2.3.2.3. MASQUERADING	26
2.3.2.4. ACTOS DELICTIVOS.....	27
2.3.3. ¿QUÉ HACER ANTE ESTOS PROBLEMAS?	27
3. SITUACION ACTUAL DE LA EMPRESA	30
3.1. HISTORIA DE LA EMPRESA	30
3.2. MISIÓN.....	31
3.3. VISIÓN	31
3.4. ORGANIGRAMA DE LA EMPRESA	32
3.5. ESQUEMA ACTUAL DE LA RED DE LA EMPRESA.....	33
3.6. COMPONENTES DE LA RED DE LA EMPRESA	34
3.7. SERVICIOS QUE SE EJECUTAN EN LA RED ACTUALMENTE	35
3.8. ANÁLISIS DE VULNERABILIDADES DE LA EMPRESA.....	35
3.8.1. INTRODUCCION	35
3.8.2. CARACTERÍSTICAS DE GFILANGUARD	36
3.8.3. ANÁLISIS DE VULNERABILIDADES: METODOLOGÍA UTILIZADA.	38
3.8.4. SEGURIDAD LÓGICA.....	40
3.8.4.1. IDENTIFICACIÓN DE USUARIOS	40
3.8.4.2. AUTENTICACIÓN	44
3.8.4.3. PASSWORDS	45
3.8.5. SEGURIDAD EN LA COMUNICACIONES	46
3.8.5.1. CONFIGURACIÓN LÓGICA DE LA RED.....	46
3.8.5.2. E-MAILS	47
3.8.5.3. ANTIVIRUS.....	49
3.8.5.4. FIREWALL	50
3.8.5.5. SERVICIOS	51
3.8.5.6. ATAQUES EN LA RED	53
3.8.6. SEGURIDAD DE LA BASE DE DATOS	54
3.8.7. SEGURIDAD FÍSICA.....	54
3.8.7.1. CONTROL DE ACCESO FÍSICO AL CENTRO DE CÓMPUTO	54
3.8.7.2. CONTROL DE ACCESO A EQUIPOS	55
3.8.7.3. DISPOSITIVOS DE SOPORTE.....	56

3.8.8. ADMINISTRACIÓN DEL CPD	57
3.8.8.1. CAPACITACIÓN	57
3.8.8.2. RESPALDO	58
3.8.8.3. DOCUMENTACIÓN	59
3.8.9. AUDITORÍAS Y REVISIONES	59
3.8.9.1. CHEQUEOS DEL SISTEMA	59
3.8.9.2. AUDITORÍAS DE CONTROL DE ACCESO	62
3.8.9.3. AUDITORÍAS DE REDES	63
3.8.10. PLAN DE CONTINGENCIAS	65
3.8.10.1. ESTRATEGIAS DE RECUPERACIÓN DE DESASTRES	65
3.9. ANÁLISIS DE RIESGOS	66
3.9.1. ACTIVOS Y FACTORES DE RIESGOS	66
3.9.2. CÁLCULO DE NIVELES DE VULNERABILIDAD	67
3.9.3. NIVELES DE VULNERABILIDAD Y RIESGOS.- RESULTADOS.	72
3.9.4. ANÁLISIS DE IMPORTANCIAS	73
3.9.5. VALORES MÁXIMOS, MÍNIMOS Y REALES	75
3.9.6. CONCLUSIÓN GENERAL	76
3.9.6.1. ANALISIS	76
3.9.6.2. INCIDENCIA DEL AREA DE TECNOLOGÍA INFORMÁTICA EN LA EMPRESA	76
3.9.6.3. COSTO PROMEDIO DE FACTORES DE RIESGOS EN LA EMPRESA	77
3.9.6.4. CONCLUSIONES SEGÚN LOS FACTORES DE RIESGOS EN TÉRMINOS MONETARIOS.	78
4. SOLUCIONES DE SEGURIDAD PROPUESTAS	80
4.1. ESQUEMA DE RED PROPUESTO	80
4.2. SERVICIOS EN LOS SERVIDORES	81
4.3. PERMISOS DE CONTENIDO POR GRUPOS	81
4.4. CLASIFICACION DE USUARIOS POR GRUPOS	81
4.5. RUTEO BAJO LINUX	82
4.5.1. TABLA COMPARATIVA DE ROUTER LINUX VS ROUTER CISCO 2620..	82
4.5.2. RAZONES PARA UTILIZAR RUTEO BAJO LINUX	83
4.5.3. REVISION DE COYOTE LINUX	84
4.5.3.1. INTRODUCCIÓN	84
4.5.3.2. REQUERIMIENTOS	85
4.5.3.3. PREPARACIÓN DEL DISCO	86
4.5.3.4. CONFIGURACIÓN	87
4.6. FIREWALL BAJO LINUX	90
4.6.1. TABLA COMPARATIVA DE IPTABLES VS CHECKPOINT FIREWALL-1. .	90
4.6.2. TABLA COMPARATIVA DE IPTABLES VS CISCO PIX 2621	91
4.6.3. RAZONES PARA UTILIZAR IPTABLES	93
4.6.4. REVISION DE IPTABLES.	94
4.6.4.1. ¿QUÉ ES UN FIREWALL?	94
4.6.4.2. ¿QUÉ ES UN FILTRO DE PAQUETES?	97
4.6.4.3. ¿QUÉ ES IPTABLES?	99

4.6.4.4. GENERACIÓN DE POLÍTICAS Y REGLAS DE FILTRADO DE PAQUETES	102
4.6.5. TABLAS COMPARATIVAS DE PROXYS.	109
4.6.5.1. MEDIDA DE PRECIO/RENDIMIENTO.	109
4.6.5.2. TASAS DE REQUERIMIENTO.....	110
4.6.5.3. MEDIDA DEL LATENCIA DEL CACHE	111
4.6.5.4. MEDIDA DE TIEMPO DE RESPUESTA	112
4.6.5.5. MEDIDA DE TIEMPO DE INACTIVIDAD	112
4.6.6. RAZONES PARA UTILIZAR EL SQUID	113
4.6.7. REVISION DE SQUID	114
4.6.7.1. INTRODUCCIÓN	114
4.6.7.2. SOFTWARE REQUERIDO	115
4.6.7.3. INSTALACIÓN DEL SOFTWARE NECESARIO	115
4.6.7.4. ANTES DE CONTINUAR	116
4.6.7.5. CONFIGURACIÓN BÁSICA.....	117
4.6.8. TABLA COMPARATIVA DE SERVIDORES CORREO DE CÓDIGO ABIERTO.	144
4.6.9. RAZONES PARA UTILIZAR QMAIL	146
4.6.10. REVISION DE QMAIL.....	147
4.6.10.1. INTRODUCCIÓN	147
4.6.10.2. ¿POR QUÉ USAR QMAIL?	147
4.6.10.3. REQUISITOS PARA USAR QMAIL.....	148
4.6.10.4. INSTALACIÓN DE QMAIL	148
4.6.11. TABLA COMPARATIVA DE SNORT VS NIDS DE CAJA.....	156
4.6.12. RAZONES PARA UTILIZAR SNORT	157
4.6.13. REVISION DEL SNORT.....	158
4.6.13.1. QUÉ ES SNORT?	158
4.6.13.2. CARACTERÍSTICAS PRINCIPALES DE SNORT	159
4.6.13.3. ¿QUÉ ES ACID?	159
4.6.13.4. CONFIGURACIÓN DEL SNORT.	160
4.7. OTROS CONTROLES DE SEGURIDAD IMPORTANTES EN LINUX...	174
4.7.1. ACTUALIZACIONES DE SEGURIDAD	174
4.7.1.1. USANDO "RED HAT NETWORK"	175
4.7.1.2. USANDO EL "ERRATA WEBSITE" (SITIO WEB DE ACTUALIZACIONES DE ERRORES)	176
4.7.2. SEGURIDAD DE LAS ESTACIONES	179
4.7.2.1. SEGURIDAD DE LA ESTACIÓN DE TRABAJO	179
4.7.2.2. SEGURIDAD DEL CARGADOR DE ARRANQUE Y DEL BIOS	179
4.7.2.3. PASSWORD PARA EL BIOS.....	180
4.7.2.4. SEGURIDAD DEL PASSWORD	186
4.7.2.5. CONTROL ADMINISTRATIVO	194
4.7.2.6. SERVICIOS DE RED DISPONIBLES	205
4.7.2.7. HERRAMIENTAS DE COMUNICACIÓN DE SEGURIDAD MEJORADAS	210
4.7.3. SEGURIDADES DEL SERVIDOR.....	211
4.7.3.1. ASEGURANDO PORTMAP	217
4.7.3.2. ASEGURANDO NIS	219
4.7.3.3. ASEGURANDO NFS.....	223
4.7.3.4. ASEGURANDO FTP.....	224
4.7.3.5. VERIFICANDO QUE PUERTOS ESTÁN ESCUCHANDO	230

4.8. SERVIDOR WINDOWS NT	233
4.8.1. INTRODUCCIÓN	233
4.8.2. CONFIGURACIÓN ADICIONAL A IMPLEMENTAR	233
4.8.2.1. AUDITORÍAS	233
4.8.2.2. PROTEGER ARCHIVOS Y DIRECTORIOS	235
4.8.2.3. PROTEGER EL REGISTRO	237
4.8.2.4. HABILITAR LA AUDITORÍA DEL SISTEMA	247
4.8.2.5. SEGURIDAD DE LOS SERVICIOS	256
4.8.2.6. PROTECCIÓN DE LOS PROTOCOLOS INTERNOS	257
4.8.3. CONSIDERACIONES GENERALES	258
5. POLITICAS DE SEGURIDAD	259
5.1. INTRODUCCIÓN	259
5.2. LINEAMIENTOS PARA LA CREACIÓN DE POLÍTICAS DE SEGURIDAD.	260
5.2.1. POLÍTICAS DE CONFIGURACIÓN	263
5.2.2. POLÍTICAS DE MANTENIMIENTO	263
5.2.3. POLÍTICAS DE REACCIÓN O CONTINGENCIA	263
5.2.4. ESTABLECER LAS REGLAS	264
5.2.5. VELAR POR EL ESTRICTO CUMPLIMIENTO	266
5.3. CÓMO TRATAR LAS INFRACCIONES	267
5.3.1. ANULAR UNA CUENTA	267
5.3.2. RESTRINGIR LAS HORAS DE ACCESO	267
5.3.3. LIMITAR LOS RECURSOS	267
5.3.4. LIMITAR EL ESPACIO EN EL SISTEMA DE ARCHIVOS	268
5.3.5. LIMITAR EL ACCESO A LOS DISPOSITIVOS	268
5.3.6. LIMITAR EL ACCESO A PROGRAMAS	268
5.4. POLÍTICAS DE SEGURIDAD PARA LA EMPRESA	268
5.4.1. SEGURIDAD FÍSICA	268
5.4.1.1. ACCESO FÍSICO	268
5.4.1.2. CONTRA INCENDIOS EN EL DEPARTAMENTO DE SISTEMAS	269
5.4.1.3. SEGURIDAD DE LOS EQUIPOS	270
5.4.1.4. CONFIGURACIÓN DE LOS EQUIPOS	270
5.4.1.5. DE USO INADECUADO	270
5.4.1.6. DE USO ADECUADO	271
5.4.1.7. POLÍTICAS DE RESPALDO	272
5.4.1.8. RECOMENDACIONES	273
5.4.2. SEGURIDAD LÓGICA	273
5.4.2.1. PRIVACIDAD	273
5.4.2.2. CONTRA LA PIRATERÍA DE SOFTWARE	274
5.4.2.3. CONFIDENCIALIDAD Y PRIVACIDAD DE LA EMPRESA	274
5.4.3. MANTENIMIENTO	275
5.4.3.1. DESCARGAS DEL INTERNET	276
5.4.3.2. CONTRA EL SOFTWARE MALICIOSO	276
5.4.3.3. CONFIDENCIALIDAD Y PRIVACIDAD DE LOS EMPLEADOS	277
5.4.3.4. POLÍTICAS DE CUENTAS	278
5.4.3.5. POLÍTICAS DE CONTRASEÑAS	278
5.4.3.6. POLÍTICAS PARA EL USO DE CORREO ELECTRÓNICO	279
5.4.3.7. POLÍTICAS DE SEGURIDAD PARA REDES	284



5.4.3.8. SEGURIDAD EN LOS SERVIDORES	288
5.4.4. PLANES DE CONTINGENCIA	292
5.4.4.1. ESTRATEGIAS DE RECUPERACIÓN DE DESASTRES	292
5.4.5. RECOMENDACIONES DE POLÍTICAS	294
CONCLUSIONES.....	295
RECOMENDACIONES	296
ANEXOS	297
BIBLIOGRAFÍA	315

INDICE DE TABLAS

Pág.

TABLA 3-1. SERVICIOS DE LA RED MAFRICO S.A.	35
TABLA 3-2. VULNERABILIDADES DE USUARIOS.....	44
TABLA 3-3. VULNERABILIDADES DE AUTENTICACIÓN	44
TABLA 3-4. VULNERABILIDADES DE PASSWORDS	45
TABLA 3-5. VULNERABILIDADES DE LA CONFIGURACIÓN LÓGICA DE LA RED ..	47
TABLA 3-6. VULNERABILIDADES DE E-MAILS.....	48
TABLA 3-7. VULNERABILIDADES DEL ANTIVIRUS	50
TABLA 3-8. VULNERABILIDADES DEL FIREWALL.....	51
TABLA 3-9. VULNERABILIDADES DE SERVICIOS EN SERVIDORES.....	53
TABLA 3-10. VULNERABILIDADES DE ATAQUES EN LA RED.....	53
TABLA 3-11. VULNERABILIDADES EN LA BASE DE DATOS.....	54
TABLA 3-12. VULNERABILIDAD DE ACCESO FÍSICO	55
TABLA 3-13. VULNERABILIDADES CONTROL DE ACCESO A EQUIPOS.....	56
TABLA 3-14. VULNERABILIDADES DE DISPOSITIVOS DE SOPORTE.....	57
TABLA 3-15. VULNERABILIDADES POR CAPACITACIÓN.....	58
TABLA 3-16. VULNERABILIDAD EN RESPALDO.	58
TABLA 3-17. VULNERABILIDAD EN DOCUMENTACIÓN	59
TABLA 3-18. VULNERABILIDADES EN CHEQUEOS DE SISTEMA.....	61
TABLA 3-19. VULNERABILIDADES EN AUDITORÍAS DE CONTROL DE ACCESO...	63
TABLA 3-20. VULNERABILIDADES EN AUDITORÍAS DE REDES.....	64
TABLA 3-21. VULNERABILIDADES DE PLANES DE CONTINGENCIA	65
TABLA 3-22. ACTIVOS A PROTEGER	66
TABLA 3-23. CÁLCULO DE NIVELES DE VULNERABILIDAD.....	72
TABLA 3-24. RESULTADOS DE NIVELES DE VULNERABILIDAD.....	73
TABLA 3-25. ANÁLISIS DE IMPORTANCIA	74
TABLA 3-26. VALORES MÁXIMOS, MÍNIMOS Y REALES	75
TABLA 3-27. INTERPRETACIÓN DE RESULTADOS.....	76
TABLA 3-28. INCIDENCIA DEL ÁREA DE TECNOLOGÍA INFORMÁTICA	77
TABLA 3-29. COSTO PROMEDIO DE FACTORES DE RIESGO EN LA EMPRESA....	78
TABLA 4-1. SERVICIOS EN LOS SERVIDORES	81
TABLA 4-2. PERMISOS DE CONTENIDO POR GRUPOS.....	81
TABLA 4-3. CLASIFICACIÓN DE USUARIOS POR GRUPOS	82
TABLA 4-4. COMPARATIVA DE ROUTER.	83
TABLA 4-5. COMPARATIVAS DE FIREWALL.....	91
TABLA 4-6. COMPARATIVA DE FIREWALL	93
TABLA 4-7. TIPOS DE FIREWALLS.	96
TABLA 4-8. REGLAS DE FILTRADO DE PAQUETES.	103
TABLA 4-9. REGLAS DE FILTRADO DE PAQUETES.	105
TABLA 4-10. REGLA DE FILTRADO DE PAQUETES.	105
TABLA 4-11. REGLAS DE FILTRADO DE PAQUETES.	107
TABLA 4-12. COMPARATIVA PROXY MEDIDA DE PRECIO/RENDIMIENTO.....	110
TABLA 4-13. COMPARATIVA PROXY TASA DE REQUERIMIENTO.....	111
TABLA 4-14. COMPARATIVA PROXY LATENCIA DEL CACHE.....	111
TABLA 4-15. COMPARATIVA PROXY TIEMPO DE RESPUESTA.....	112

TABLA 4-16. COMPARATIVAS DE PROXIES TIEMPO INACTIVIDAD	113
TABLA 4-17. COMPARATIVA DE CARACTERÍSTICAS ESPECIFICAS DE SERVIDORES DE CORREO.	145
TABLA 4-18. COMPARATIVA DE CARACTERÍSTICAS GENERALES DE SERVIDORES DE CORREO.	146
TABLA 4-19. COMPARATIVA DE IDS.....	157
TABLA 4-20. ACCESO ROOT MÉTODOS PARA DESHABILITAR LA CUENTA ROOT	198
TABLA 4-21. AUDITORÍA DE WINDOWS NT.....	235
TABLA 4-22. AUDITORÍA DE WINDOWS NT.....	236
TABLA 4-23. AUDITORÍA DE WINDOWS NT.....	236
TABLA 4-24. AUDITORÍA DE WINDOWS NT.....	237
TABLA 4-25. AUDITORÍA DE WINDOWS NT.....	257



CIB-ESPOL

INDICE DE FIGURAS

	Pág.
FIGURA 3-1. ORGANIGRAMA DE MAFRICO S.A.	32
FIGURA 3-2. ESQUEMA ACTUAL DE LA RED MAFRICO S.A.	33
FIGURA 3-3. TOPOLOGÍA ESTRELLA DE LA RED MAFRICO S.A.	34
FIGURA 4-1. ESQUEMA DE RED PROPUESTO.....	80
FIGURA 4-2. ESQUEMA DE SEGURIDAD	85
FIGURA 4-3. INTERFAZ WEB PARA ADMINISTRACIÓN DE COYOTE LINUX.....	87
FIGURA 4-4. CONFIGURACIÓN DE REGLAS DE FIREWALL DE COYOTE LINUX...88	
FIGURA 4-5. CONFIGURACIÓN DE REGLAS DE ACCESO DE COYOTE LINUX.89	
FIGURA 4-6. CONFIGURACIÓN DE REGLAS DE FIREWALL DE COYOTE LINUX..89	
FIGURA 4-7. ARQUITECTURA DE QMAIL	154
FIGURA 4-8. CONFIGURANDO APACHE CON PHP	165
FIGURA 4-9. ESQUEMA DE LA BASE DE DATOS SNORT.....	169
FIGURA 4-10. CONFIGURACIÓN DEL ACID.....	172
FIGURA 4-11. ANÁLISIS DE CONSOLA DE ACID.....	173
FIGURA 4-12. PANEL DE INFORMACIÓN DE PASSWORD	194
FIGURA 4-13. PANEL DE GRUPOS.....	202
FIGURA 4-14. HERRAMIENTA DE CONFIGURACIÓN DE SERVICIOS.....	207



CIB-ESPOL

INTRODUCCIÓN



CIB-ESPOL

El auge del Internet, el avance en las telecomunicaciones y en el hardware de los computadores han sido importantes en los últimos años, lo que ha posibilitado a que un usuario pueda realizar transacciones en forma remota sin desplazarse a ningún sitio. La falta de medidas de seguridad en las redes de las empresas es un problema que está en crecimiento. Cada vez es mayor el número de atacantes, mejores las herramientas que utilizan y cada vez están más organizados.

A lo largo de este trabajo se va a analizar la situación actual de la Empresa objeto de este proyecto, relacionado a los aspectos de seguridad computacional con requisitos de seguridad medios esto es: un Análisis de Vulnerabilidades, Análisis de Riesgos, y proponer soluciones para nuestra empresa estableciendo la importancia de la utilización de herramientas de seguridad como un Firewall y un Sistema de Detección de Intrusos entre otros, utilizando plataformas Linux y Windows y redes de computadoras, sin dejar de lado la importancia que tiene como complemento unas buenas políticas de seguridad.

El objetivo final de este proyecto será marcar unas pautas para conseguir un nivel de seguridad aceptable en los sistemas Linux y Windows conectados a la red de la empresa, entendiendo por "aceptable" un nivel de protección suficiente para que la mayoría de potenciales intrusos interesados en los equipos de nuestra empresa fracasara ante un ataque contra los mismos.

1. CONCEPTOS BASICOS DE SEGURIDAD

1.1. ¿QUÉ ES SEGURIDAD EN INFORMÁTICA?

Podemos entender como seguridad una característica de cualquier sistema informático o no, que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir esa seguridad (según la mayoría de expertos, imposible), se suaviza entonces la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

Es muy difícil de conseguir seguridad en los sistemas operativos o redes de computadores, (según la mayoría de expertos, imposible), entonces se flexibiliza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad.

Dependiendo del entorno en que un sistema Linux o Windows trabaje, a sus responsables les interesaría dar prioridad a un cierto aspecto de la seguridad.

¿Qué implica cada uno de los tres aspectos de los que hablamos?

La confidencialidad nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados; la integridad significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada, y la disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio. Generalmente tienen que existir los tres aspectos descritos para que haya seguridad.

Dependiendo del entorno en que un sistema Linux o Windows trabaje, a sus responsables les interesaría dar prioridad a un cierto aspecto de la seguridad. Por ejemplo, en un sistema militar se antepondría la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad; seguramente, es preferible que alguien borre información confidencial (que se podría recuperar después desde una cinta de respaldo) a que ese mismo atacante pueda leerla, o a que esa información esté disponible en un instante dado para los usuarios autorizados. En cambio, en un servidor NFS de un departamento se premiará la disponibilidad frente a la confidencialidad, importa poco que un atacante lea una unidad, pero que esa misma unidad no sea leída por usuarios autorizados va a suponer una pérdida de tiempo y dinero. En un entorno bancario, la faceta que más ha de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad, es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.



1.2. ¿CÓMO NACIÓ LA SEGURIDAD INFORMÁTICA?

Muchos lectores quizás se recuerdan la película "War Games", protagonizada por Matthew Broderick en la representación de un estudiante de colegio que rompió la seguridad de una supercomputadora del departamento de defensa de los Estados Unidos (DoD) e inadvertidamente causó una amenaza de guerra nuclear.

La popularidad de la película inspiró a muchos individuos y grupos a empezar e implementar algunos de los métodos que el joven protagonista usó para crackear los sistemas restringidos, incluyendo lo que es conocido como war dialing (guerra de marcado), un método de búsqueda de números telefónicos para conexiones de módems analógicos en un código de área definido y una combinación de prefijos telefónicos.

Diez años más tarde, múltiples jurisdicciones fueron perseguidas por el FBI y con la ayuda de profesionales de computadoras a través del país, Kevin Mitnick un infame cracker de computadora fue arrestado y con cargos de 25 cuentas de computadoras y acceso fraudulento a dispositivos que resultaron en alrededor de 80 millones de dólares en pérdidas de propiedad intelectual y código fuente de Nokia, Nec, Sun Microsystem, Novell, Fujitsu y Motorola.

La seguridad de la información ha evolucionado a través de los años debido al incremento de confiabilidad de las redes públicas para descubrir información personal, financiera y otra información restringida. La popularidad del Internet fue uno de los más importantes desarrollos que provocaron un intenso esfuerzo en la seguridad de los datos.

El Internet y sus protocolos antiguos sin embargo fueron desarrollados como un sistema basado en la confianza. Esto es, el protocolo de Internet no fue diseñado para ser seguro por mismo, dejándolo abierto para usuarios potencialmente maliciosos y procesos a través de la red.

Desarrollos modernos han hecho la comunicación de Internet más segura pero todavía existen muchos incidentes que llaman la atención nacional y nos alertan con la verdad de que nada es completamente seguro.



CIB-ESPOL

1.3. NIVELES DE HACKERS

Hay niveles de distinción para describir individuos quienes encuentran y explotan vulnerabilidades en sistemas y redes. Ellos son descritos por el color del sombrero que ellos usan cuando desarrollan sus investigaciones de seguridad, y este color es el que indica sus intenciones.

El hacker sombrero blanco es uno de los cuales prueba las redes y sistemas de un cliente para examinar su rendimiento y determinar cuan vulnerable son para los intrusos, investigadores académicos y consultores de seguridad profesionales son dos ejemplos de hackers de sombrero blanco.

Un hacker sombrero negro es sinónimo de cracker. Ellos frecuentemente confían en programas de crackeo disponibles y vulnerabilidades bien conocidas en sistemas para descubrir información sensitiva para ganar personalidad o para infligir daño en el sistema o red destino.

Los hackers de sombrero gris típicamente suscriben otra forma de hacker ético, lo cual dice que es aceptable vulnerar los sistemas mientras el hacker no roba o rompe la confidencialidad. Algunos argumentarían sin embargo que el acto de vulnerar un sistema no es en si mismo ético.

1.4. LA SEGURIDAD EL DÍA DE HOY

En el nuevo milenio existe alrededor de 400 millones de personas que usan o han usado el Internet a nivel mundial. En cualquier día, existe un estimado de 142 incidentes más importantes de explotación de vulnerabilidades reportadas a CERT (Computer Emergency Response Team). El impacto económico a nivel mundial de los 3 más peligrosos virus de Internet de los últimos dos años fue alrededor resultó en pérdidas de 13.2 billones de dólares y en crecimiento. La seguridad en computadoras hoy en día se ha transformado en un gasto cuantificable y justificable para todos los presupuestos de Tecnología de Información.

1.5. ESTANDARIZANDO LA SEGURIDAD

Las empresas e industrias confían en todas las reglas y regulaciones que son establecidas por estándares creando cuerpos como AMA (American Medical Association) o IEEE (Intitute of Electrical and Electronics Engineers). Muchos consultores de seguridad y vendedores están de acuerdo con el modelo de seguridad estandarizado conocido como CIA o confidencialidad, integridad, y disponibilidad. La descripción de este modelo implica lo siguiente:

- ♦ **Confidencialidad.-** Información sensitiva debe estar disponible solo para un conjunto de individuos autorizados.
- ♦ **Integridad.** – La información no debe ser alterada de forma que quede incompleta o incorrecta. Solo acceden usuarios autorizados.
- ♦ **Disponibilidad.-** La información debe ser accesible para usuarios autorizados a cualquier hora que sea necesaria.



1.6. ¿QUÉ QUEREMOS PROTEGER?

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar.

1.7. ¿DE QUÉ NOS QUEREMOS PROTEGER?

A continuación se presenta una relación de los elementos que potencialmente pueden amenazar a nuestro sistema. No pretende ser exhaustiva, simplemente trata de proporcionar una idea acerca de quién y qué, amenaza a los sistemas y redes de computadoras.

1.7.1. PERSONAS

No podemos engañarnos, la mayoría de ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas como por ejemplo.

- ♦ **Ex-empleados.-** Generalmente se trata de personas descontentas que utilizan información de la empresa para causar algún tipo de daño.
- ♦ **Curiosos.-** Suelen ser empleados que intentan conseguir mayores privilegios para acceder a los sistemas de la empresa.
- ♦ **Crackers.-** Personas que explotan las vulnerabilidades de los sistemas para obtener algún beneficio.
- ♦ **Terroristas.-** Atacan a los sistemas para causar algún tipo de daño.
- ♦ **Intrusos remunerados.-** Son hackers pagados por empresas con el fin de robar información secreta de la competencia.

1.7.2. AMENAZAS LÓGICAS

Bajo la etiqueta de "amenazas lógicas" encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros). Como por ejemplo:

- ♦ **Software mal desarrollado.-** Y que dejan agujeros de seguridad que luego son aprovechados por los hackers.
- ♦ **Herramientas de seguridad.-** Son armas de doble filo ya que son usadas por los administradores de sistemas para control y por hackers para explotar vulnerabilidades.
- ♦ **Bombas lógicas.-** Son programas que se activan para causar daño.
- ♦ **Virus y gusanos.-** Son programas que se esparcen dañando la información.
- ♦ **Caballos de Troya.-** Son programas que realizan funciones ocultas en un PC, estas pueden ser la utilización de información privada para fines no éticos.

- ♦ **Programas conejo.-** Se reproducen hasta que agotan los recursos del sistema produciendo negaciones de servicio.
- ♦ **Técnicas salami.-** Robo automatizado de pequeñas cantidades de dinero.
- ♦ **Applets hostiles.-** Difunden en la red desde un virus hasta robo de información.

1.7.3. AMENAZAS EN LAS SEGURIDADES DE LAS REDES

La mala práctica cuando configuramos los siguientes aspectos de una red puede incrementar el riesgo de un ataque.



CIB-ESPOL

1.7.3.1. ARQUITECTURAS INSEGURAS

Una red mal configurada es el punto de entrada primario para el acceso no autorizado. Dejar una red local abierta basada en confianza es una vulnerabilidad hacia el Internet que es altamente inseguro.

1.7.3.2. REDES BROADCAST

Administradores de sistemas frecuentemente fallan para darse cuenta de la importancia del hardware de red en su esquema de seguridad. Hardware simple como hubs y routers confían en el broadcast o en el principio no-switched; esto es cuando un nodo transmite datos a través de la red hacia un nodo receptor, el hub o router envía un broadcast de los paquetes de datos hasta que el nodo receptor recibe y procesa los datos. Este método es el más vulnerable para el robo de ARP (Address Resolution Protocol) o MAC (Media Access Control) por intrusos de afuera y usuarios no autorizados en redes locales.

1.7.3.3. SERVIDORES CENTRALIZADOS

Otra huella importante de red es el uso de computadoras centralizadas. Esto puede ser conveniente porque es más fácil administrar y ahorrar considerablemente en vez de tener múltiples servidores configurados. Sin embargo un servidor centralizado introduce un solo punto de falla en la red. Si el servidor central está comprometido, este quizás considere a toda la red no usable o peor propensa a la manipulación de datos o robo.

1.7.4. AMENAZA A LA SEGURIDAD DE SERVIDORES

La seguridad de servidores es tan importante como la seguridad de la red porque los servidores frecuentemente tienen un buen compromiso con la información vital de la Empresa. Si un servidor está comprometido, todo su contenido quizás se transforme en disponible para que el cracker lo robe o lo manipule.

1.7.4.1. SERVICIOS NO USADOS Y PUERTOS ABIERTOS

Una ocurrencia común entre los administradores de sistemas es instalar el sistema operativo sin poner atención a que programas actualmente están siendo instalados. Esto puede ser problemático porque los servicios innecesarios podrían ser instalados y configurados con las configuraciones por defecto, y posiblemente levantados por defecto, lo cual en cambio puede causar un tráfico no deseado hacia el servidor o quizás una ruta potencial hacia el sistema para los crackers.

1.7.4.2. SERVICIOS NO PARCHADOS

Desarrolladores y administradores de sistemas frecuentemente encuentran vulnerabilidades explotables y publican la información en sitios webs de

vulnerabilidades y temas relacionados con seguridad tales como la lista de e-mail Bugtraq (<http://www.securityfocus.com>) o el sitio web CERT (Computer Emergency Response Team <http://www.cert.org>) . Es recomendable que los administradores parchen sus sistemas antes de que los hackers hagan uso de estas vulnerabilidades.

1.7.4.3. FALTA DE ATENCIÓN EN LA ADMINISTRACIÓN

De acuerdo a SANS (System Administration Network and Security Institute) la causa principal de la vulnerabilidad en la seguridad de las computadoras es asignar a personas no entrenadas para mantener la seguridad y no proveer un entrenamiento durante ese tiempo para hacer posible su trabajo. Este se aplica tanto para los administradores inexpertos y presumidos, y para desmotivados administradores.



CIB-ESPOL

1.7.4.4. SERVICIOS INHERENTEMENTE INSEGUROS

Hasta las organizaciones que más permanecen alertas pueden caer víctimas de vulnerabilidades si la red de servicios, que ellos han escogido, es inherentemente inseguro. Servicios inseguros son por ejemplo Telnet y FTP los cuales no encriptan la información que envían a la red.

Otro ejemplo de servicios inseguros son el Network File System (NFS) y el Network Information Services (NIS), los cuales fueron desarrollados explícitamente para el uso de una LAN pero son desafortunadamente extendidos a redes WAN (para usuarios remotos). NFS no maneja por defecto ninguna autenticación o mecanismos de seguridad configurados para prevenir que un

cracker alcance un NFS compartido y accese el contenido que hay en él. NIS también tiene información vital que debe ser conocido por cada computadora en una red, incluyendo passwords y permisos de archivos dentro de una base de datos de texto plano ASCII o DBM (derivado de ASCII). Un cracker que obtiene acceso a esta base de datos puede entonces acceder a cada cuenta de usuario en una red incluyendo la cuenta del administrador.

1.7.5. AMENAZAS A LA SEGURIDAD DE LAS ESTACIONES DE TRABAJO.

Las estaciones de trabajo y las PCs del hogar pueden no estar tan propensas a ataques como las redes y los servidores, pero, ya que a menudo contienen información sensitiva tal como información de tarjetas de crédito, ellas, son blanco de crackeadores de sistemas. Las estaciones de trabajo pueden también ser secuestradas sin conocimiento del usuario y usadas por los atacantes como "máquinas esclavas" en ataques coordinados.

1.7.5.1. MALOS PASSWORDS

Los malos passwords son una de las más fáciles maneras por la que un atacante obtiene acceso al sistema.

1.7.5.2. APLICACIONES CLIENTE VULNERABLES

Aunque un administrador puede tener un servidor totalmente seguro y parchado, esto no significa que usuarios remotos estén seguros cuando lo accedan. Por ejemplo, si el servidor ofrece servicios como Telnet o FTP sobre una red pública, un atacante puede capturar el texto plano de nombres de usuarios y passwords

al ganar acceso a la red y luego usar la información de las cuentas de los usuarios para acceder remotamente a sus estaciones de trabajo. Incluso cuando se usan protocolos seguros como SSH (Secure Shell), un usuario remoto puede ser vulnerable a ciertos ataques si ellos no mantienen sus aplicaciones cliente actualizadas.

1.7.5.3. BUFFER OVERFLOWS

Es el snack smashing o desbordamiento de pila, también conocido por buffer overflows. La idea del stack smashing es sencilla: en algunas implementaciones de C es posible corromper la pila de ejecución de un programa escribiendo más allá de los límites de un arreglo (array) y declarado "auto" en una función; esto puede causar que la dirección de retorno de dicha función sea una dirección aleatoria. Esto, unido a permisos de los archivos ejecutables en Linux (principalmente a los bits de Seguid y SetGID), hace que el sistema operativo pueda otorgar acceso root a usuarios sin privilegios.

1.7.6. ATAQUES REMOTOS

1.7.6.1. ESCANEOS DE PUERTOS

Un potencial atacante realizará sin duda un escaneo de puertos (portscan) contra su objetivo, esto le permitirá obtener información de cada máquina como por ejemplo: qué servicios se ofrecen, que sistema operativo usan o ciertas características de la arquitectura de nuestra red. Analizando qué puertos están abiertos en un sistema, es una potencial puerta de entrada a la misma.



CIB-ESPOL

1.7.6.2. SPOOFING

Por spoofing se conoce a la creación de tramas tcp/ip utilizando una dirección IP falseada; un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado.

En el Spoofing entran en juego tres máquinas: un atacante, un atacado, y un sistema suplantado que tiene cierta relación con el atacado; para que el pirata pueda conseguir su objetivo necesita por un lado establecer una comunicación falseada con su objetivo, y por otro evitar que el equipo suplantado interfiera en el ataque.

Hasta ahora hemos hablado del ataque genérico contra un host denominado spoofing o, para ser más exactos, IP Spoofing; existen otros ataques de falseamiento relacionados en mayor o menor medida con este, entre los que destacan el DNS Spoofing, el ARP Spoofing y el Web Spoofing. Para analizar este punto, vamos a comentarlos brevemente a continuación:



CIB-ESPOL

1.7.6.3. DNS SPOOFING

Este tipo de ataque se puede conseguir de diferentes formas, desde modificando las entradas del servidor encargado de resolver una cierta petición para falsear las relaciones dirección-nombre (Servidor DND), hasta comprometiendo un servidor que infecte la caché de otro (lo que se conoce como DNS Poisoning); incluso sin acceso a un servidor DNS real, un atacante puede enviar datos falseados como respuesta a una petición de su víctima sin más que averiguar los números de secuencia correctos.

1.7.6.4. ARP SPOOFING

El ataque denominado ARP Spoofing hace referencia a la construcción de tramas de solicitud y respuesta arp falseadas, de forma que en una red local se puede forzar a una determinada máquina a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo. La idea es sencilla, y los efectos del ataque pueden ser muy negativos: desde negaciones de servicio hasta interceptación de datos, incluyendo algunos Man in the Middle contra ciertos protocolos cifrados.



1.7.6.5. WEB SPOOFING

Este ataque permite a un pirata visualizar y modificar cualquier página web que su víctima solicite a través de un navegador, incluyendo las conexiones seguras vía SSL. Para ello, mediante código malicioso un atacante crea una ventana del navegador correspondiente, de apariencia inofensiva, en la máquina de su víctima; a partir de ahí, enruta todas las páginas dirigidas al equipo atacado (incluyendo las cargadas en nuevas ventanas del navegador) a través de su propia máquina, donde son modificadas para que cualquier evento generado por el cliente sea registrado (esto implica registrar cualquier dato introducido en un formulario, cualquier click en un enlace, etc.).

1.7.6.6. NEGACIONES DE SERVICIO

Las negaciones de servicio (conocidas como DoS, Denial of Service) son ataques dirigidos contra un recurso informático (generalmente una máquina o una red, pero también podría tratarse de una simple impresora o una terminal) con el objetivo de degradar total o parcialmente los servicios prestados por ese recurso

a sus usuarios legítimos; constituyen en muchos casos uno de los ataques más sencillos y contundentes contra todo tipo de servicios, y en entornos donde la disponibilidad es valorada por encima de otros parámetros de la seguridad global puede convertirse en un serio problema, ya que un pirata puede interrumpir constantemente un servicio sin necesidad de grandes conocimientos o recursos, utilizando simplemente sencillos programas y un modem y un PC caseros.

1.7.6.7. INTERCEPTACIÓN

La interceptación lógica de datos más conocida y extendida es el Sniffing. En las redes de difusión, cuando una máquina envía una trama a otra indica en un campo reservado la dirección del host destino; todas las máquinas del dominio de colisión ven esa trama, pero sólo su receptora legítima la captura y elimina de la red. Este es el funcionamiento normal de tcp ip; sin embargo, es necesario insistir en un aspecto: todas las máquinas ven la trama, y si no leen todos sus campos es porque no "quieren". Existe un modo de funcionamiento de las interfaces de red denominado modo promiscuo, en el cual la tarjeta lee todas las tramas que circulan por la red, tanto dirigidas a ella como a otras máquinas; el leerlas no implica el eliminarlas de la red, por lo que el host destino legítimo la recibirá y eliminará sin notar nada extraño.

1.7.6.8. ATAQUES A APLICACIONES

♦ CORREO ELECTRÓNICO

El sendmail, el protocolo smtp y el pop3 causan muchos problemas a los Administradores de la red, ya que son un peligro potencial a tener en cuenta en cualquier entorno informático donde se utilice el correo electrónico: es decir, en

todos. Cualquier servidor smtp proporciona demasiada información a un atacante que simplemente conecte a él. Otro gran problema de smtp es el relay: Si nuestros servidores permiten el relay estamos favoreciendo el spam en la red, el envío de e-mail no deseado con fines casi siempre publicitarios, algo que evidentemente a nadie le hace gracia recibir. Además, el relay causa una negación de servicio, degradando así el servicio ofrecido a nuestros usuarios legítimos. Por si esto fuera poco, ocasionaría que se incluya a nuestra organización en alguna "lista negra" de servidores que facilitan el spam se causa un importante daño a nuestra imagen, e incluso ciertos dominios pueden llegar a negar todo el correo proveniente de nuestros servidores.

♦ ATAQUES VÍA WEB

Los ataques a las páginas web de una organización son casi siempre los más "vistosos" que la misma puede sufrir: en cuestión de minutos piratas de todo el mundo se enteran de cualquier problema en la página web principal de una empresa más o menos grande pueda estar sufriendo, y si se trata de una modificación de la misma incluso existen recopilatorios de páginas "hackeadas". Por supuesto, la noticia de la modificación salta inmediatamente a los medios, que gracias a ella pueden rellenar alguna cabecera sensacionalista sobre "los piratas de la red", y así se consigue que la imagen de la empresa atacada caiga notablemente y la del grupo de piratas suba entre la comunidad "underground" nacional o internacional.

2. SEGURIDAD EN EL ENTORNO DE OPERACIONES.

2.1. INTRODUCCIÓN



CIB-ESPOL

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y medidas contra las amenazas a los recursos y la información confidencial.

Desgraciadamente, la seguridad física es un aspecto olvidado con demasiada frecuencia a la hora de hablar de seguridad informática en general; en muchas organizaciones se suelen tomar medidas para prevenir o detectar accesos no autorizados o negaciones de servicio, pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala de operaciones o al lugar donde se depositan las impresiones del sistema.

Hemos de recordar que cada sitio es diferente, y por tanto también lo son sus necesidades de seguridad; de esta forma, las pautas y recomendaciones de seguridad estarán orientadas a la Empresa objeto de este proyecto, la cuales pueden variar desde el simple sentido común (como es el cerrar con llave la sala de operaciones cuando salimos de ella) hasta medidas que podrían llegar a ser más complejas. En cada Empresa se ha de analizar el valor de lo que se quiere proteger y la probabilidad de las amenazas potenciales, para en función de los resultados obtenidos diseñar un plan de seguridad adecuado.

2.2. SEGURIDAD FÍSICA DE LOS SISTEMAS

2.2.1. PROTECCIÓN DEL HARDWARE

El hardware es frecuentemente el elemento más caro de todo sistema informático, por tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier Empresa.

2.2.1.1. ACCESO FÍSICO

La posibilidad de acceder físicamente por parte de un atacante a una máquina o sistema operativo en general, hace inútiles casi todas las medidas de seguridad que hayamos aplicado sobre ella. Especialmente para el caso de una Empresa donde muchas veces circulan personas que no se saben a donde van o de donde vienen suplantando personalidades como por ejemplo un técnico de computación de tal forma que la persona que accede al equipo puede pararlo o arrancar una versión diferente del sistema operativo sin llamar mucho la atención.

♦ PREVENCIÓN

¿Cómo prevenir un acceso físico no autorizado a un determinado punto?

Hay soluciones para todos los gustos, y también de todos los precios. Una solución concreta, sería el uso de lectores de tarjetas para poder acceder a ciertas dependencias es algo muy a la orden del día y que al menos se lo debería instalar en las áreas donde se maneje información sensible de la empresa.

♦ DETECCIÓN

Cuando la prevención es difícil por cualquier motivo (técnico, económico, humano) es deseable que un potencial ataque sea detectado cuanto antes, para

minimizar así sus efectos. Es importante concienciar a todos de su papel en la política de seguridad del entorno; si por ejemplo un usuario autorizado detecta presencia de alguien de quien sospecha que no tiene autorización para estar en una determinada lugar debe avisar inmediatamente al administrador o al responsable de los equipos, que a su vez puede avisar al servicio de seguridad si es necesario.

2.2.1.2. DESASTRES NATURALES

Un problema que no suele ser tan habitual, pero que en caso de producirse puede acarrear gravísimas consecuencias, es el derivado de los desastres naturales y su falta de prevención. Estos pueden ser:



CIB-ESPOL

♦ TEMBLORES O TERREMOTOS

Los terremotos son el desastre natural menos probable en nuestra ciudad, simplemente por su localización geográfica. Es recomendable y barato utilizar fijaciones para los elementos más críticos, como los CPUs, los monitores, switches o los routers. Para hacer frente a pequeñas vibraciones podemos utilizar plataformas de goma donde situar a los equipos, de forma que la plataforma absorba la mayor parte de los movimientos.

♦ TORMENTAS ELÉCTRICAS

Las tormentas eléctricas son otro evento que en épocas de invierno pueden suceder, generan subidas repentinas de tensión infinitamente superiores a las que pueda generar un problema en la red eléctrica y si sucede un sábado por la noche nadie va a regresar a la Empresa a proteger a los equipos. La caída de un

rayo es algo poco probable en una ciudad donde existen mecanismos destinados justamente a atraer rayos de una forma controlada.

♦ INUNDACIONES Y HUMEDAD

Contra las inundaciones, las medidas más efectivas son las de prevención (frente a las de detección). Medidas de protección menos sofisticadas pueden ser la instalación de un falso suelo por encima del suelo real, o simplemente tener la precaución de situar a los equipos con una cierta elevación respecto al suelo, pero sin llegar a situarlos muy altos por los problemas que ya hemos comentado al hablar de terremotos y vibraciones.

2.2.1.3. DESASTRES DEL ENTORNO

♦ ELECTRICIDAD

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo, etc., a diario amenazan la integridad tanto de nuestro hardware como de los datos que almacena o que circulan por él. Medidas para evitar estos problemas son utilizar tomas de tierra desviando el exceso de corriente hacia el suelo o simplemente hacia cualquier lugar con voltaje nulo. La utilización de estabilizadores de tensión (Reguladores de voltaje) es una solución para las variaciones de voltaje pero un problema que los estabilizadores de tensión o las tomas de tierra no pueden solucionar es justamente el contrario a las subidas de tensión: las bajadas, situaciones en las que la corriente desciende por debajo del voltaje necesario para un correcto

funcionamiento del sistema, pero sin llegar a ser lo suficientemente bajo para que la máquina se apague.

Otro problema, son las idas y venidas rápidas de la corriente; la forma más efectiva de proteger nuestros equipos contra estos problemas de la corriente eléctrica es utilizar un UPS (Servicio de Alimentación Ininterrumpido) conectada al elemento que queremos proteger.

♦ RUIDO ELÉCTRICO

El ruido eléctrico suele ser generado por motores o por maquinaria pesada y se transmite a través del espacio o de líneas eléctricas cercanas a nuestra instalación. Para prevenir los problemas lo más barato es intentar no situar hardware cercano a la maquinaria que puede causar dicho ruido. También es recomendable mantener alejados de los equipos dispositivos emisores de ondas, como teléfonos móviles, transmisores de radio o walkie-talkies; estos elementos puede incluso dañar permanentemente a nuestro hardware si tienen la suficiente potencia de transmisión, o influir directamente en elementos que pueden dañarlo como detectores de incendios o cierto tipo de alarmas.

♦ INCENDIOS Y HUMO

Un método efectivo contra los incendios son los extintores de dióxido de carbono situados en el techo, que se activan automáticamente al detectar humo o calor este es utilizado hoy en día ya que es menos contaminante y perjudicial.



Aparte del fuego y el calor generado, en un incendio existe un tercer elemento perjudicial para los equipos: el humo, un potente abrasivo que ataca especialmente los discos magnéticos y ópticos.

♦ TEMPERATURAS EXTREMAS

Es recomendable que los equipos operen entre 10 y 32 grados Celsius, aunque pequeñas variaciones en este rango tampoco han de incluir en la mayoría de sistemas. Para controlar la temperatura ambiente en el entorno de operaciones nada mejor que un acondicionador de aire, aparato que también influiría positivamente en el rendimiento de los usuarios, las personas también tenemos rangos de temperaturas dentro de los cuales trabajamos más cómodamente.

2.2.2. PROTECCIÓN DE LOS DATOS

La seguridad física también implica una protección a la información de nuestro sistema, tanto a la que está almacenada en él como a la que se transmite entre diferentes equipos. Hay ciertos aspectos a tener en cuenta a la hora de diseñar una política de seguridad física que afectan principalmente, aparte de a los elementos físicos, a los datos de nuestra organización; existen ataques cuyo objetivo no es destruir el medio físico de nuestro sistema, sino simplemente conseguir la información almacenada en dicho medio.

2.2.2.1. INTERCEPCIÓN

La interceptación, es un proceso mediante el cual un agente capta información en claro o cifrada que no le iba dirigida; esta captación puede realizarse de muchas maneras, se lo puede hacer mediante un software pero también mediante un

dispositivo que se engancha directamente al cableado. Contra estos ataques existen diversas soluciones; la más barata a nivel físico es no permitir la existencia de segmentos de red de fácil acceso, lugares idóneos para que un atacante conecte uno de estos aparatos y capture todo nuestro tráfico.

2.2.2.2. RESPALDOS

Resulta recomendable guardar las copias de seguridad en una zona alejada de la sala de cómputo, aunque en este caso descentralicemos la seguridad y tengamos que proteger el lugar donde almacenamos los respaldos igual que protegemos la propia sala o los equipos situados en ella, algo que en ocasiones puede resultar caro. También suele ser común etiquetar las cintas (si fuera el caso) donde hacemos copias de seguridad con abundante información sobre su contenido (sistemas de archivos almacenados, día y hora de la realización, sistema al que corresponde, etc.); esto tiene una parte positiva y una negativa. Por un lado, recuperar un archivo es rápido: sólo tenemos que ir leyendo las etiquetas hasta encontrar la cinta adecuada. Sin embargo, si nos detenemos a pensar, igual que para un administrador es fácil encontrar el respaldo deseado también lo es para un intruso que consiga acceso a las cintas.

2.2.2.3. OTROS ELEMENTOS

En muchas ocasiones los responsables de seguridad de los sistemas tienen muy presente que la información a proteger se encuentra en los equipos, en las copias de seguridad o circulando por la red pero olvidan que esa información también puede encontrarse en lugares menos obvios, como listados de impresora, faxes, teletipos, plotters, facturas telefónicas, manuales que proporcionen información

de los sistemas o la propia documentación de una máquina, todos estos deben estar ubicados en lugares de acceso restringido.

2.3. ADMINISTRADORES, USUARIOS Y PERSONAL

2.3.1. INTRODUCCIÓN

El punto más débil de cualquier sistema informático son las personas relacionadas en mayor o menor medida con él; desde un administrador sin una preparación adecuada o sin la suficiente experiencia, hasta un guardia de seguridad que ni siquiera tiene acceso lógico al sistema, pero que deja acceder a todo el mundo a la sala de cómputo, pasando por supuesto por la gran mayoría de usuarios, que no suelen estar conscientes de que la seguridad también les concierne a ellos. Frente a cada uno de estos grupos (administradores, usuarios y personal externo al sistema) un potencial atacante va a comportarse de una forma determinada para conseguir lograr sus objetivos, y sobre cada uno de ellos ha de aplicarse una política de seguridad diferente, obviamente podemos exigir a un administrador de sistemas unos conocimientos más o menos profundos de temas relacionados con la seguridad informática, pero esos conocimientos han de ser diferentes para el guardia de seguridad (sus conocimientos serían referentes a la seguridad física del entorno), y se convierten en simples nociones básicas si se trata de un usuario medio.



CIB-ESPOL

2.3.2. ATAQUES POTENCIALES

2.3.2.1. INGENIERÍA SOCIAL

La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían; aunque a nadie le gusta ser manipulado, en algunos casos no es excesivamente perjudicial (por ejemplo un vendedor puede aplicar ingeniería social para conocer las necesidades de un cliente y ofrecer así mejor sus productos), si las intenciones de quien la pone en práctica no son buenas se convierte quizás el método de ataque más sencillo, menos peligroso para el atacante y por desgracia en uno de los más efectivos. Ese atacante puede aprovechar el desconocimiento de unas mínimas medidas de seguridad por parte de personas relacionadas de una u otra forma con el sistema para poder engañarlas en beneficio propio.



CIB-ESPOL

2.3.2.2. SHOULDER SURFING

Consiste en "espiar" físicamente a los usuarios, para obtener generalmente claves de acceso al sistema. Por ejemplo, una medida que lamentablemente utilizan muchos usuarios para recordar sus contraseñas es apuntarlas en un papel pegado al monitor de su PC o escribirlas en la parte de abajo del teclado; cualquiera que pase por delante del puesto de trabajo, sin problemas puede leer el login, password e incluso el nombre de máquina a la que pertenecen.

2.3.2.3. MASQUERADING

El ataque denominado masquerading o mascarada consiste simplemente en suplantar la identidad de cierto usuario autorizado de un sistema informático o su entorno; esta suplantación puede realizarse electrónicamente, un usuario utiliza

para acceder a una máquina un login y password que no le pertenecen o en persona. La mascarada no es un ataque habitual en entornos normales. El masquerading es más habitual en entornos donde existen controles de acceso físico, y donde un intruso puede “engañar” al dispositivo o persona que realiza el control, por ejemplo con una tarjeta de identificación robada que un lector acepta o con un carné falsificado que un guardia de seguridad da por bueno. Una variante de la mascarada lo constituye el ataque denominado piggybacking, que consiste simplemente en seguir a un usuario autorizado hasta un área restringida y acceder a la misma gracias a la autorización otorgada a dicho usuario. Contra esto se deben aplicar las mismas medidas que contra la mascarada física: controles de acceso estrictos, y convenientemente verificados.



CIB-ESPOL

2.3.2.4. ACTOS DELICTIVOS

Bajo este nombre englobamos actos tipificados claramente como delitos por las leyes de nuestro país como el chantaje, el soborno o la amenaza. Esto no implica que el resto de actividades no sean (o deban ser) delitos, sino simplemente que en la práctica a nadie se le castiga “legalmente” por pasear por una sala de cómputo en busca de claves apuntadas en teclados, pero sí que se le puede castigar por amenazar a un operador para que le permita el acceso al sistema.

2.3.3. ¿QUÉ HACER ANTE ESTOS PROBLEMAS?

La solución a problemas relacionados con el personal es con frecuencia mucho más compleja que la de problemas de seguridad lógica o seguridad de la red, mientras que un administrador puede aprovechar herramientas de seguridad, capacidades del sistema operativo, o cifrado de datos para prevenir ciertos

ataques, es mucho más difícil para él concienciar a los usuarios de unas mínimas medidas de prevención o convencer a un guardia de seguridad de que sólo deje acceder a la sala de cómputo a un número restringido de personas.

Generalmente los usuarios de máquinas Linux o Windows en entornos habituales son personas muy poco formadas en el manejo del sistema operativo, y mucho menos en lo que a seguridad informática se refiere. El responsable de seguridad ha de concienciar a todas estas personas de la necesidad de la seguridad para que el entorno de trabajo funcione como se espera de él; la seguridad informática se ha de ver como una cadena que se rompe si falla uno de sus eslabones, no importa que tengamos un sistema de cifrado resistente a cualquier ataque o una autenticación fuerte de cualquier entidad del sistema si un intruso es capaz de obtener un nombre de usuario con su correspondiente contraseña simplemente llamando por teléfono a una secretaria.

Pero, ¿qué sucede cuando el personal de nuestra propia organización produce ataques (y no accidentes) sobre nuestros sistemas?. En este caso las consecuencias pueden ser gravísimas, y por tanto las medidas de protección y detección han de ser estrictas. Se ha de llevar a cabo un control estricto de las actividades que se realizan en la organización, por ejemplo mediante políticas que han de ser de obligado cumplimiento, así como un control de acceso a todos los recursos de los que disponemos (mediante mecanismos de autenticación de usuarios, alarmas, etc.). Además, las sanciones en caso de incumplimiento de las normas han de ser efectivas y ejemplares: si un usuario viola intencionadamente

nuestra seguridad y no se le sanciona adecuadamente, estamos invitando al resto de usuarios a que hagan lo mismo.



3. SITUACION ACTUAL DE LA EMPRESA

3.1. HISTORIA DE LA EMPRESA

MAFRICO es una Empresa que comenzó hace 36 años, comercializando repuestos y brindando servicio técnico para el área de refrigeración. Posteriormente nos transformamos en fabricantes de última tecnología en Cámaras Frigoríficas y soluciones de aislamiento con poliuretano en general.

En la actualidad estamos incursionando en el mercado de la construcción, logrando una revolución en la solución de sistemas constructivos con aislamiento térmico y acústico, ideales para complejos habitacionales, educativos, comerciales e industriales.

Contamos con el mejor equipo humano y tecnológico para brindarle un servicio garantizado en nuestras instalaciones.

MAFRICO es una Empresa líder del Ecuador en la fabricación y montaje de cámaras para refrigeración, equipos y accesorios. Paneles MAFRICO que están compuestos por planchas de aluzinc en los dos lados y rellenas de poliuretano de alta densidad en diferentes espesores, de acuerdo a los requerimientos del cliente. Somos los representantes y distribuidores exclusivos en el Ecuador de los productos METECNO de Colombia.



CIB-ESPOL

3.2. MISIÓN

Garantizar el más alto nivel de satisfacción de nuestros clientes, entregando productos de alta calidad; promoviendo el desarrollo constante y el bienestar del capital humano de la Empresa; y producir los más altos rendimientos a la inversión de nuestros accionistas.

3.3. VISIÓN

Una Empresa que satisfaga con eficiencia las necesidades del mercado nacional y regional con soluciones integrales, en las áreas de refrigeración, aislamiento térmico, construcción liviana prefabricada, con productos y servicios de primera calidad, contando para ello con un equipo de personas profesionales y comprometidos con este mismo fin.

3.4. ORGANIGRAMA DE LA EMPRESA

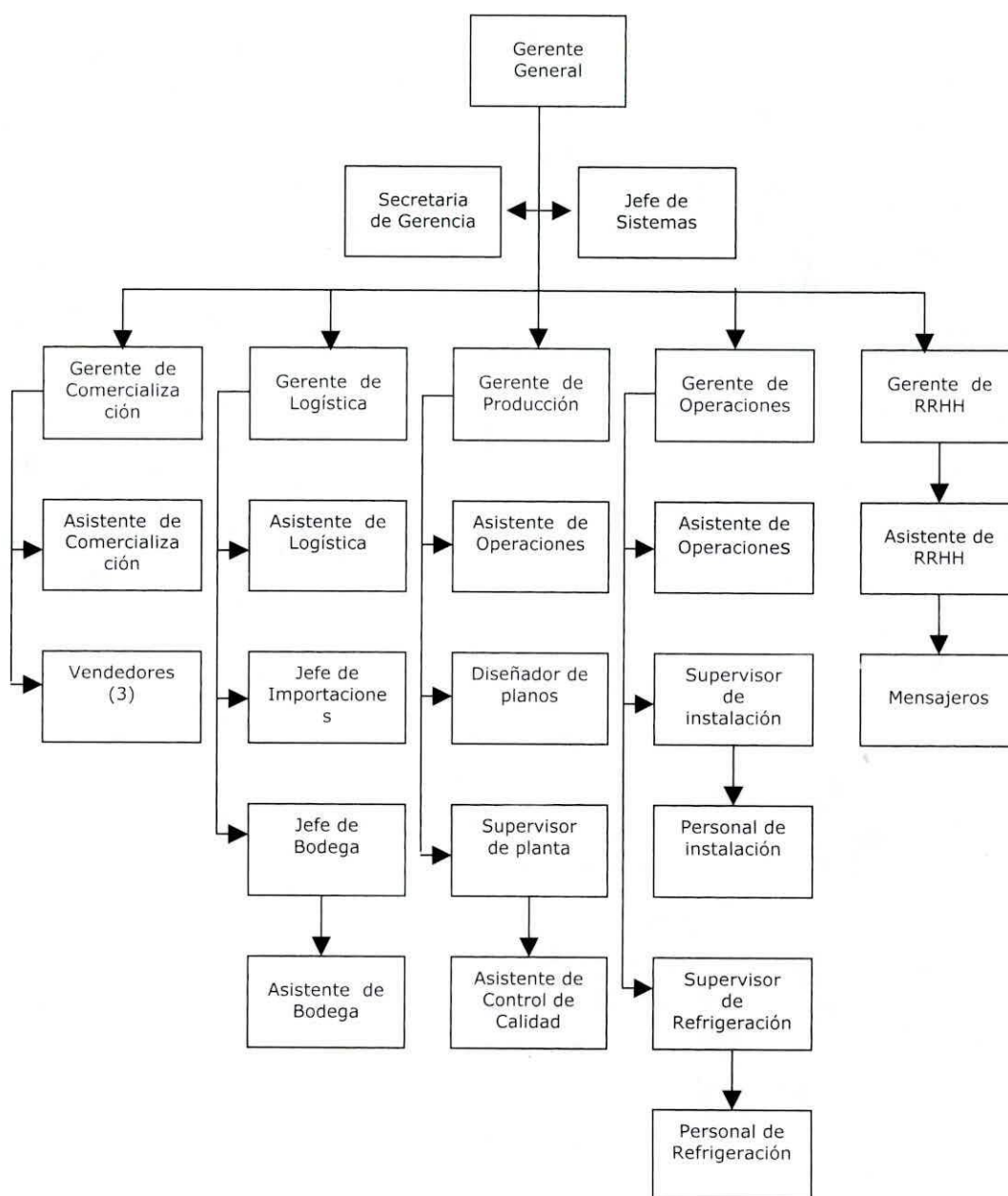


Figura 3-1. Organigrama de MAFRICO S.A.

3.5. ESQUEMA ACTUAL DE LA RED DE LA EMPRESA

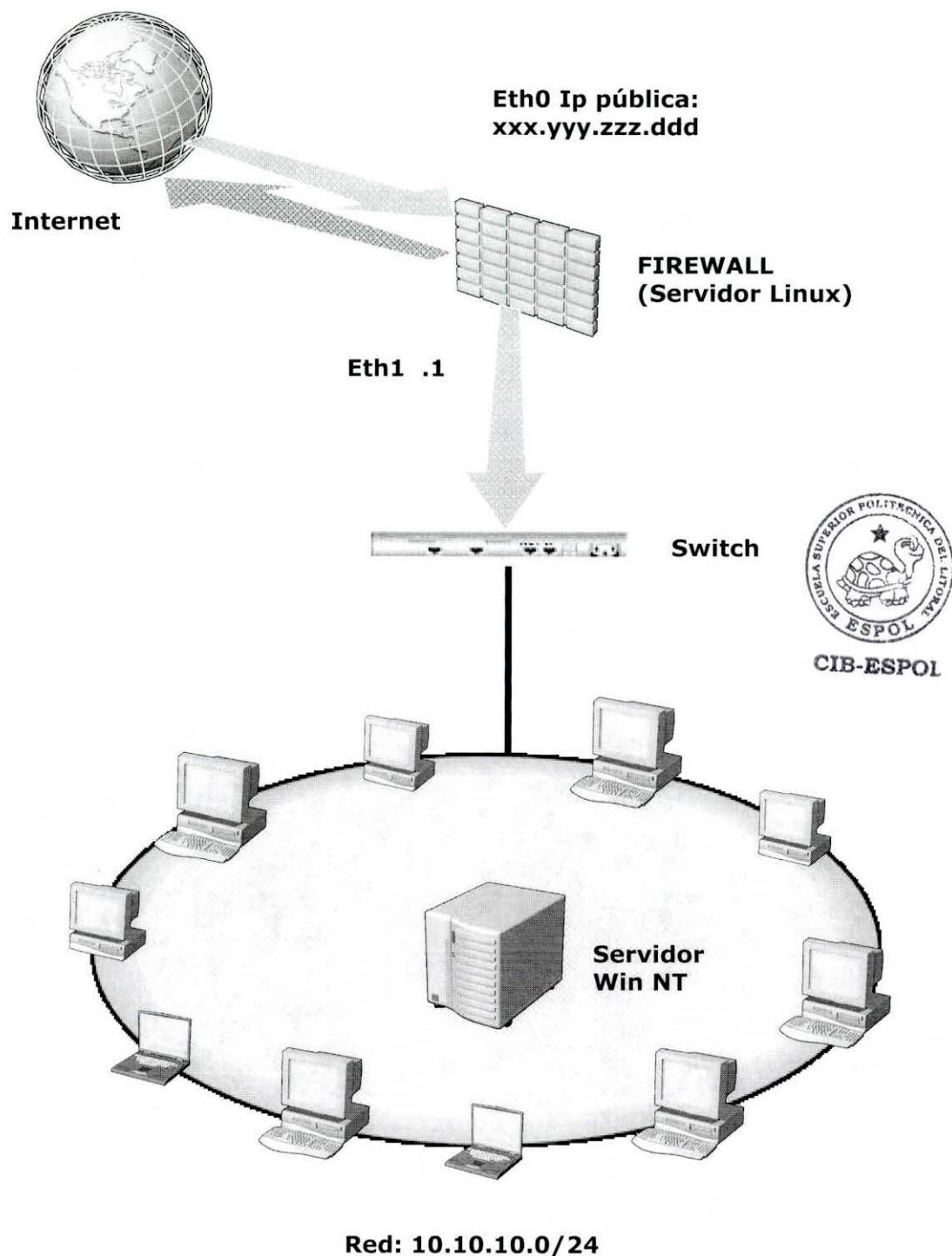


Figura 3-2. Esquema Actual de La Red Mafrico S.A.

3.6. COMPONENTES DE LA RED DE LA EMPRESA

- ♦ Un enlace dedicado de internet con un ancho de banda de 128 Kbps.
- ♦ Un Servidor de Internet con plataforma LINUX (Redhat 9.0) este es el que se conecta con la red WAN y a la vez distribuye el internet dentro de la empresa.
- ♦ Un servidor de archivos con plataforma WINDOWS NT contiene las aplicaciones y las carpetas compartidas.
- ♦ Un Switch DLINK de 24 puertos no administrable, aquí se centraliza todas las conexiones a los dispositivos de la red.
- ♦ Terminales basadas en Windows desde la versión 95 hasta el Xp.

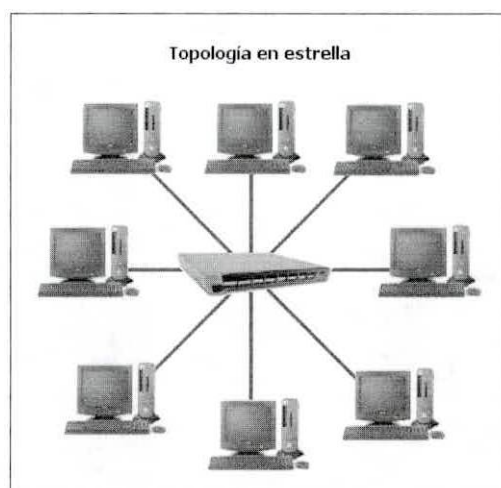


Figura 3-3. Topología Estrella de la Red MAFRICO S.A.

La topología actual de la red es ESTRELLA lo que significa que la red se une en un único punto centralizado en un SWITCH.

3.7. SERVICIOS QUE SE EJECUTAN EN LA RED

ACTUALMENTE

SERVICIOS	DESCRIPCION	PUERTO
POP3	Servicio de correo	109, 110
SMTP	Servicio de correo	25
Auth	Identificación de procesos en la red	
Ftp (anonimo)	Protocolo de transferencia de archivos entre sistemas	21
Http	Navegación en Internet	80
Telnet	Terminal virtual (administración remota)	23
Ssh ver 1	Administración remota con encriptacion	22
X Server	Servidor de ventanas para SSH	6000
Netbios	Compartir Archivos en una LAN	139
Netmetting	Video Conferencia	1503

Tabla 3-1 Servicios de la Red MAFRICO S.A.

3.8. ANÁLISIS DE VULNERABILIDADES DE LA

EMPRESA



3.8.1. INTRODUCCION

En el mercado existen diferentes herramientas para analizar vulnerabilidades en una red. Estas herramientas son muy útiles para los administradores de red preocupados por la seguridad e integridad de su red y la información que por ella transita.

Sin embargo, estas herramientas se convierten en armas de doble filo, pues pueden ser usadas con el objetivo de mejorar la seguridad de la red o pueden ser

usadas por hackers con el objetivo de detectar vulnerabilidades y realizar ataques.

La herramienta que se ha utilizado para nuestro análisis es el GFI LANguard Network Security Scanner 5.0. Esta es una aplicación que permite analizar la red e identificar posibles agujeros de seguridad y también caballos de Troya.

Gracias a su analizador de puertos se puede comprobar si hay alguna aplicación no autorizada ejecutándose en el sistema, examinar puertos de firewall, telnet y proxy, comprobar los accesos al router y ejecutar controles de seguridad.

Además de todo esto, LanGuard Network Security Scanner proporciona información NETBIOS sobre cada Pc: nombre de host, sesión de usuario, datos compartidos, y mucho más. A continuación se procede a mencionar las características principales de la herramienta a utilizar para este análisis.

3.8.2. CARACTERÍSTICAS DE GFILANGUARD

♦ Detecta automáticamente vulnerabilidades de seguridad en su red.

GFI LANguard Network Security Scanner (N.S.S.) chequea su red para todos los métodos potenciales que un hacker podría usar para atacarlo. Analizando el sistema operativo y las aplicaciones que se están ejecutando en su red además, identifica los posibles agujeros de seguridad. En otras palabras, funciona como el abogado del diablo y lo alerta a usted de las debilidades de su red antes de que un hacker las pueda encontrar, permitiéndole que solucione sus problemas antes que un hacker se beneficie de ellos.

♦ **Provee información profunda acerca de todos los componentes su red.**

GFI LANguard N.S.S. escanea su red completa, IP por IP y provee información como niveles de actualización de los parches del sistema, parches de seguridad perdidos, documentos compartidos, puertos abiertos, servicios y aplicaciones activos en una Pc, entradas de registro de claves, passwords débiles, usuarios, grupos y más. Los resultados del escaneo pueden ser fácilmente analizados usando filtros y reportes permitiéndole pro activamente asegurar su red, por ejemplo, apagando puertos innecesarios, cerrando archivos compartidos, instalando paquetes de parches del sistema, y arreglar otros problemas.



♦ **Administración de parches**

GFI LANguard N.S.S. es también una solución completa de administración de parches para el sistema. Después de haber escaneado su red y determinado los parches y servicios de parches que faltan en el sistema operativo y en las aplicaciones, usted puede usar GFI LANguard N.S.S. para hacer uso de estos paquetes de parches en la red.

♦ **Identifica vulnerabilidades de seguridad y recomienda una acción**

Una vez que GFI LANguard N.S.S. ha completado el escaneo en su red, este categoriza las vulnerabilidades de seguridad y recomienda un curso de acción a seguir. En donde sea posible más información o enlaces de red son incluidos referentes a asuntos de seguridad, por ejemplo una identificación de BugTraq, para que usted pueda consultar que tipo de vulnerabilidad se trata.

Otras características de este software son: escaneo rápido de puertos TCP, UDP, servicios y aplicaciones que se están ejecutando para determinar el grado de vulnerabilidad y recomendaciones a efectuar.

3.8.3. ANÁLISIS DE VULNERABILIDADES: METODOLOGÍA UTILIZADA.

- ♦ Escaneo Externo
- ♦ Escaneo interno

El escaneo externo fue dirigido al Servidor Linux el cual es el dispositivo que está conectado directamente al internet a través de su IP pública.

El escaneo interno se lo realizó a cada Servidor esto es Servidor Linux de internet, Servidor Windows NT que es el servidor de archivos y aplicaciones, a la red y sus estaciones de trabajo.

Los tipos de escaneos realizados son los siguientes:

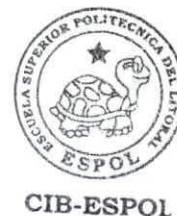
En el escaneo Externo tenemos:

- ♦ Escaneo de puertos tcp abiertos en el servidor Linux.
- ♦ Escaneo de puertos udp abiertos en el servidor Linux.
- ♦ Escaneo de potenciales vulnerabilidades en servidor Linux.

- ♦ Escaneo de potenciales vulnerabilidades en servicios activos en el servidor Linux.

En el escaneo Interno tenemos:

- ♦ Escaneo de puertos tcp abiertos en el servidor Linux.
- ♦ Escaneo de potenciales vulnerabilidades en el servidor Linux.
- ♦ Escaneo de puertos tcp abiertos en el servidor Windows NT.
- ♦ Escaneo de potenciales vulnerabilidades en el servidor Windows NT.
- ♦ Escaneo de estatus de parches de actualizaciones en el servidor Windows NT.
- ♦ Escaneo de servicios activos en el servidor Windows NT.
- ♦ Escaneo de servicios compartidos en el servidor Windows NT.



Para poder obtener esta información se visitó la empresa objeto de este proyecto con el fin de constatar las condiciones de seguridad física y lógica relacionada con el área de tecnología de información.

De acuerdo con los resultados producto de los Escaneos se realizó un análisis el cual se lo clasificó de la siguiente manera:

- ♦ Análisis de Seguridad Lógica
- ♦ Análisis de Seguridad en las comunicaciones
- ♦ Análisis de Seguridad de las aplicaciones
- ♦ Análisis de Seguridad Física
- ♦ Análisis de Administración del CPD (Centro de Procesamiento de Datos)
- ♦ Análisis relacionado a Auditorías y Revisiones

♦ Plan de Contingencias

A continuación se procede a explicar cada uno de estos análisis. Si usted desea ver los resultados de los escaneos internos y externos de la red de la empresa de forma gráfica refiérase al Anexo A.

3.8.4. SEGURIDAD LÓGICA

3.8.4.1. IDENTIFICACIÓN DE USUARIOS

Vulnerabilidad	Efecto	Recomendación
Los usuarios de las aplicaciones y del sistema operativo no tienen asignada una fecha de expiración del password.	El usuario no es obligado, en ningún momento, a modificar su clave de acceso, de manera que se facilita su revelación o robo.	Se debe implementar una política de vigencia de la contraseña actual, para que el usuario se vea obligado a cambiarla cada cierto tiempo.
No hay en la empresa un procedimiento formal para efectuar las bajas de los empleados del sistema.	Es posible que los empleados próximos a desvincularse de la empresa emprendan acciones de vandalismo o sabotaje, por rechazo o insatisfacción con esta decisión, o bien para beneficios personales.	Sería conveniente que el área de recursos humanos de aviso al Administrador de Sistemas con un período de tiempo previo al despido, de esta manera es posible llevar a cabo una política de desvinculación del personal, a través de la cuál se quitan permisos al usuario en forma periódica.
No se lleva a cabo ninguna revisión periódica ni control sobre el buen funcionamiento de las cuentas de los usuarios, ni sobre los permisos que tienen asignados.	Es posible que, por error, negligencia, fraude o algún otro motivo, la cuenta o los permisos de algún usuario sean modificados, permitiendo que usuarios no habilitados	Periódicamente sería conveniente controlar las cuentas de usuarios, viendo que: ♦ Estén activas solo las cuentas necesarias. ♦ No se han creado ni borrado cuentas. ♦ Los datos del usuario son



Vulnerabilidad	Efecto	Recomendación
	accedan a datos que no le están permitidos.	consistentes. ♦ Los permisos que le corresponden son los que tiene asignados. ♦ Los passwords no están expirados y han sido cambiados periódicamente.
No existe en el sistema una lista de control de acceso, esto imposibilita relacionar los usuarios con los datos que les es posible acceder, y qué permisos tienen sobre estos datos (lectura, escritura, modificación, borrado.)	La ausencia de esta relación dificulta la trazabilidad de las acciones, de manera que resulta complicado identificar los permisos de los usuarios con respecto a los datos, archivos y carpetas del sistema, en el caso que sea necesaria una Auditoría o revisión de la actividad particular de un usuario.	Recomendamos la generación de una lista de control de acceso donde se identifiquen a todos los usuarios habilitados en el sistema, los datos a los que pueden acceder y los tipos de permisos que los usuarios poseen sobre los mismos. Esta lista de control de acceso debería almacenarse en el servidor de aplicaciones cifrada, de manera que los permisos de los usuarios no sean revelados a personas no autorizadas, y así evitar la posibilidad de una modificación no autorizada.
No se tiene en cuenta ninguna restricción horaria en el momento de permitir a un usuario el logeo al sistema.	Esta debilidad puede permitir que un usuario no autorizado intente ingresar al sistema en horario no laboral, condición que se ve agravada por el hecho que los servidores no se apagan sino que permanecen prendidos las 24 horas del día.	Debería discriminarse el horario en que puede ser utilizado el sistema informático de la empresa, de manera que: ♦ Las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, de acuerdo al grupo al que pertenezcan (debido a que diferentes grupos pueden tener diferentes horarios). ♦ Durante las vacaciones o licencias las cuentas de usuarios deben desactivarse. ♦ En días feriados las cuentas de usuarios administrativos, a excepción de los del Grupo Ventas, deben permanecer desactivados.
No se tiene en cuenta ninguna	Puede ocurrir que alguna persona no	Se deberá tener en cuenta la localización del PC que se

Vulnerabilidad	Efecto	Recomendación
restricción con respecto al equipo desde donde se logea cada usuario.	autorizada tenga acceso a un equipo que no le corresponde, permitiéndosele ver información para la que no tiene autorización.	intenta logear, para así poder relacionar cada usuario con su propia PC, o con su propio grupo de trabajo, de manera que un usuario de ventas solo podrá logearse en alguna de las PCs del departamento de ventas y un gerente solo pueda logearse en su propia PC.
Aunque el usuario permanezca un largo período de tiempo sin actividad el sistema no ejecuta ninguna acción; Esta situación pudo comprobarse también en los servidores, donde el administrador está logeado en el sistema permanentemente.	Existe la posibilidad de que un usuario autorizado se logee en el sistema y abandone su puesto de trabajo. Si otro usuario no autorizado tiene acceso físico a esta PC, éste último también tendrá acceso a datos que le están prohibidos. Esta situación se ve agravada si los equipos a los que se hace referencia son los servidores de la empresa, debido a que no solo se tiene acceso a datos críticos sino también a opciones de configuración de los sistemas.	Si el sistema permanece ocioso durante cinco minutos, el programa debería encargarse de deslogear al usuario del sistema, borrar la pantalla. Cuando el usuario regrese, se debería solicitar nombre de usuario y contraseña nuevamente. Además, sería conveniente que las PCs utilicen algún protector de pantalla con contraseña. Estas recomendaciones se deben tener presente en la administración de los servidores.  CIB-ESPOL
Los servidores permanecen logeados con el usuario root durante las 24 horas del día. De esta manera la seguridad de los datos de la empresa que residen en el servidor solo dependerá del acceso físico al equipo.	Debido a que no hay controles lógicos, cualquier persona que consiga ingresar al centro de cómputos podría acceder a los datos y a la configuración de los servidores.	El Administrador de Sistemas solo debería utilizar el usuario root del sistema en caso que fuera necesario realizar alguna tarea que así lo requiera. Para las demás actividades debería contar con otro usuario, con menos privilegios y por lo tanto menos riesgoso

Vulnerabilidad	Efecto	Recomendación
No se eliminan los usuarios que vienen por defecto en el sistema operativo de los servidores Windows NT y Linux, como las cuentas Invitado de LINUX y Windows, estas cuentas permanecen en el sistema sin que ningún usuario las utilice. Lo mismo ocurre en las PCs	En el caso que una persona no autorizada conozca la existencia de estas cuentas puede llegar a utilizarlas para tener acceso al sistema operativo del servidor.	Sería conveniente eliminar estos tipos de usuarios, no solo los que trae Linux por defecto sino también los usuarios de Windows NT y Xp. No deben existir en el sistema más usuarios que los necesarios para la empresa.
Los integrantes de los diferentes departamentos comparten sus cuentas (usuarios y passwords) no respetando la confidencialidad de sus perfiles y sus cuentas asignadas por el Administrador del Sistema.	Con este esquema de acceso se imposibilita rastrear las acciones de cada uno de estos usuarios las aplicaciones, así no pueden asignarse responsabilidades individuales ante un posible error.	Sugerimos que no se revelen las contraseñas personales, de tal manera que se puedan diferenciar a los usuarios del sistema.
El mantenimiento técnico especializado externo utiliza una cuenta de administrador para hacer modificaciones en los sistemas operativos de los servidores vía Internet, y una vez finalizado el mantenimiento No se desactiva dicha cuenta.	Esta situación resulta inadmisibles, debido a que existe otra persona, ajena a la organización, que conoce la contraseña del administrador del sistema, de manera que se aumenta el riesgo de intrusión a los sistemas y divulgación o robo de datos. Si esta contraseña es utilizada a través de Internet, el riesgo se hace todavía más	Sugerimos que, para resolver esta situación, se cree una nueva cuenta de usuario para realizar el mantenimiento externo, con los permisos necesarios para dicha tarea. Una vez finalizado el mantenimiento, el administrador del sistema podría modificar la contraseña, de manera de evitar entradas no autorizadas. Esta cuenta, por la peligrosidad que enviste, debería ser chequeada periódicamente por el Administrador del Sistema, comprobando las tareas que

Vulnerabilidad	Efecto	Recomendación
	grande debido a la posibilidad de escuchas o intercepciones en la comunicación, que podrían resultar en el robo del password.	desde allí se realizan.

Tabla 3-2. Vulnerabilidades de Usuarios

3.8.4.2. AUTENTICACIÓN

Vulnerabilidad	Efecto	Recomendación
Los datos de autenticación son almacenados y transmitidos sin ningún cifrado.	Puede ocurrir que alguien acceda al archivo de passwords del sistema de la empresa, y disponga de acceso a todas las cuentas de usuarios existentes, con todos los permisos posibles, y de esta forma no tendría ninguna restricción en el acceso a los menús del sistema. También, alguien podría Interceptar el canal de comunicaciones, consiguiendo las contraseñas y nombres de usuarios en texto plano.	El archivo con los datos de usuarios del sistema debería almacenarse en un formato no legible, es decir encriptado, y almacenado en el servidor de aplicaciones en una carpeta protegida por una contraseña gestionada por el Administrador del Sistema. Además, sería conveniente que los datos de autenticación viajen encriptados a través de la red, durante toda la transmisión. El archivo que almacena los passwords de los usuarios no debería poder modificarse, sino solamente a través de la aplicación de gestión de cuentas.

Tabla 3-3. Vulnerabilidades de Autenticación

3.8.4.3. PASSWORDS

Vulnerabilidad	Efecto	Recomendación
Pudimos ver que el password de un usuario era fácilmente predecible.	Es posible que los demás usuarios lo obtengan y accedan a datos que les están prohibidos.	Deberán considerarse herramientas para controlar que el password no sea fácil de descifrar, como puede ser realizar comparaciones contra una lista de palabras reservadas, por ejemplo el nombre de la empresa, el nombre de cuenta del usuario, números o letras repetitivas, entre otras.
No se controla si el usuario cambia su contraseña ingresando siempre el mismo password, simulando cambiarlo, pero este ingresa nuevamente la clave que ha estado usando siempre.	Las contraseñas que no se modifican por largos periodos de tiempo corren el riesgo de ser descubiertas, debido a que seguramente habrá más oportunidades de descifrarlas.	Deberá controlarse que el usuario ingrese una clave nueva cada vez que la modifique, así como que las últimas 5 claves no se repitan. Esto puede hacerse utilizando una base de datos donde se acumulen las últimas cinco claves que ha empleado cada usuario.
En ambos casos, cuando un usuario se olvida su contraseña o es bloqueado por el sistema, recurre al Administrador del Sistema, el cual lee el password del usuario (en el sistema de gestión de cuentas de usuario), recordándoselo. Pero en ningún momento se lo intima a modificar el password revelado.	El Administrador del Sistema conoce el password del usuario, lo que genera divulgación de información innecesaria. Esto se agrava cuando ocurre el mismo suceso varias veces, de manera que el Administrador del Sistema conocerá el patrón de contraseñas utilizado por el usuario.	Para resolver esto el Administrador del Sistema modificará la fecha de expiración del password, obligando así al usuario a cambiar su contraseña en el momento del logeo. La aplicación, en ningún momento, revelará la contraseña del usuario al Administrador del Sistema.

Tabla 3-4. Vulnerabilidades de Passwords



CIB-ESPOL

3.8.5. SEGURIDAD EN LA COMUNICACIONES

3.8.5.1. CONFIGURACIÓN LÓGICA DE LA RED

Vulnerabilidad	Efecto	Recomendación
No esta segmentada la red por dominios de broadcast, solo existe un switch en toda la red. Las direcciones IP no están subneteadas, actualmente se lleva un esquema de direccionamiento IP estático con una sola dirección de red para toda la empresa.	♦ Posibles ataques DoS exitosos causados por tormenta de broadcast, debido al ingreso de gusanos o troyanos en la red. ♦ LA red no es administrable, debido a que todos pertenecen a la misma red. ♦ NO se puede controlar eficientemente el uso de recursos de red. ♦ Cualquier usuario de cualquier departamento puede acceder directamente a toda la red y a su vez analizar el trafico de toda la red, comprometiendo los datos confidenciales de la empresa. ♦ Se degrada el rendimiento de la red.	Sugerimos, que se haga una segmentación lógica de la red de la siguiente manera: ♦ Haciendo uso de un PC Pentium 1 de 200 MGHZ, 32 MB RAM, floppy disk. ♦ Usando un disco de arranque, que contenga los archivos y configuraciones necesarias para emular un router bajo Linux con Kernel 2.4. ♦ Clasificar las redes según los niveles administrativos: Gerentes, administradores, administración media y Empleados. ♦ Se debe escoger una dirección IP privada y luego subnetearla para cuatro redes y con la cantidad de direcciones de hosts suficientes para cada nivel. Con esto se podrá administrar los accesos y los recursos de la red eficientemente y en caso de que ocurra un ataque DoS este solo afectara a una parte de red, mas no a toda.  CIB-ESPOL
No hay ninguna medida tomada para que un usuario pueda proteger sus datos.	Algún usuario puede acceder a datos de otro usuario que no deberían ser divulgados.	Samba podría utilizarse para el control de perfiles. Con esta aplicación podría gestionarse la protección de las distintas carpetas, incluyendo las de respaldo y de los usuarios, con controles de acceso muy fuertes; esto se logra declarando la aplicación como controladora de

Vulnerabilidad	Efecto	Recomendación
		dominios, para que administre las carpetas, con una funcionalidad similar a la de Linux.
A pesar de que el sistema operativo Windows NT y Linux posee algunos parches, estos no esta parchado en su totalidad. Las PCs tampoco están bien parchadas.	Pueden ingresar al Sistema Troyanos y virus que pueden robar información sensitiva y además pueden cambiar la configuración del sistema reemplazando DLLs. Se pueden ejecutar escripts y código malicioso automáticamente. Ejecución de comandos remotos, ataques de denegación de servicios.	Se debe establecer una política de actualización de los sistemas operativos y servicios de los servidores, cada cierto tiempo y estar al tanto de las nuevas vulnerabilidades.
Fallas e inconsistencia en el registro de Windows NT.	Se pueden sufrir ataques DoS como desbordamiento del buffer, se pueden recibir paquetes ICMP fragmentados los cuales pueden tener ocupado el CPU 100%.	Actualice el sistema operativo lo mas pronto posible. Ejecute un utilitario que repare el registro como el Norton Win Doctor que viene con Norton System Works, este arreglara ciertas inconsistencias en el registro de Windows.

Tabla 3-5. Vulnerabilidades de la Configuración Lógica de la Red



CIB-ESPOL

3.8.5.2. E-MAILS

Vulnerabilidad	Efecto	Recomendación
Al configurar Microsoft Outlook en las PCs no se modifican las opciones de configuración por defecto, es decir que la vista previa y los controles ActiveX y Scripts están	La vista previa de los e-mails y la ejecución de controles ActiveX y Scripts son riesgosas ya que facilitan la infección con virus que se ejecutan automáticamente.	Es conveniente exigir normas respecto a la habilitación y deshabilitación de dichas características y la configuración mínima que debe poseer el Outlook Express en las PCs. Debe deshabilitarse la vista previa de los mensajes y prohibirse la ejecución de controles ActiveX y Scripts.

Vulnerabilidad	Efecto	Recomendación
habilitados.		
No están prohibidos los programas de Chat ni los de compartición de archivos.	Estas aplicaciones encierran incrementan el riesgo de ingreso de virus, troyanos e intrusos al sistema.	Deberían restringirse este tipo de aplicaciones, deshabilitando los servicios que utilizan (como el SOCKS en el caso del MSN).
El servidor de correos permite relay.	Cualquier usuario remoto puede enviar correo desde este servidor de correos, utilizándolo como spammer. Esto puede comprometer a la empresa y su imagen.	Quite el servicio de servidor relay y configúrelo de tal forma que toda la información de autenticación sea guardada y controlada por el servicio.
En Windows NT se usa el servicio de oficina de correos, el cual utiliza una carpeta compartida y no posee ninguna herramienta de administración de los correos.	♦ Se puede producir un ataque DoS, spamm. ♦ Mal uso del recurso y de la red. ♦ Se puede llenar rápidamente el disco duro por motivo de correos muy pesados. ♦ Lentitud del Sistema.	♦ Sugerimos el uso de qmail, ya que este MTA ha sido diseñado con fines de seguridad y deben establecer explícitamente los siguientes parámetros, de tal forma que el usuario no pueda abusar de las bondades del servicio. ♦ Se debe establecer el número de usuarios concurrentes. ♦ Se debe establecer una partición o espacio en disco exclusivamente para el uso del correo. ♦ Se debe establecer un límite de espacio para la bandeja de entrada de cada usuario. ♦ Establecer el número de mensajes que puede enviar y recibir diariamente un usuario. ♦ Establecer el tamaño de cada mensaje.

Tabla 3-6. Vulnerabilidades de E-mails

3.8.5.3. ANTIVIRUS

Vulnerabilidad	Efecto	Recomendación
No existe anti-troyanos instalados en los PCs y en los Servidores.	♦ Si uno o varios troyanos atacan a uno de los PCs o Servidores, estos comprometen la confidencialidad en la empresa. ♦ Se pueden robar información útil acerca de usuario passwords, correos importantes, numero de tarjeta de crédito. ♦ Los hackers se pueden apoderar de todos los servidores y la red completa.	Debido a que actualmente existen en circulación en el Internet mas troyanos que virus, nosotros sugerimos instalar un anti-troyanos, Ej. AVG, en cada una de las PCs y servidores de la red; el cual debe ser actualizado periódicamente
No hay procedimientos formales a seguir en caso de infección de virus.	Al no utilizar un procedimiento como guía, puede ocurrir que el virus no sea eliminado completamente del equipo y se contagie a través de la red interna, además de la posibilidad de pérdida de datos en los equipos infectados.	Debería haber un procedimiento documentado a seguir para el caso que se encuentre un virus en el sistema. Sugerimos las siguientes actividades: ♦ Chequear el disco con el escaneo de virus para determinar si hay un virus, y qué virus es. ♦ Eliminar el virus. ♦ Cerrar los programas, apagar la máquina y arrancar la computadora desde el disco de rescate del antivirus. ♦ Hacer un nuevo chequeo de virus en el disco duro. ♦ Chequear el resto de los dispositivos de datos (disqueteras, disco removibles, etc.), para saber de donde vino el virus. ♦ Tratar de determinar la fuente del virus. La persona que hizo llegar el virus debe ser informada. ♦ Avisar a todos los usuarios del sistema que hayan

Vulnerabilidad	Efecto	Recomendación
		intercambiado datos con la computadora infectada. ♦ Si el virus borró o modificó algún dato, tratar de restaurarlo desde los respaldos y restaurar los programas involucrados. ♦ Hacer un nuevo escaneo del disco, buscando virus en los datos restaurados.

Tabla 3-7. Vulnerabilidades del Antivirus

3.8.5.4. FIREWALL

Vulnerabilidad	Efecto	Recomendación
No esta bien definidas las reglas de firewall en el servidor Linux, y además, no existe instalado un Firewall en el Servidor Windows NT.	♦ Los hackers pueden acceder remotamente al sistema a través de servicios inseguros que no están protegidos con reglas de filtrado. ♦ Los usuarios internos pueden utilizar los servicios a su antojo. ♦ Los usuarios pueden comprometer seriamente la confidencialidad de la empresa. ♦ Si un troyano en ingresado a la red, puede atacar fácilmente a este servidor, produciendo un robo fácil de información. ♦ Se pueden recibir paquetes deformados o fragmentos que pueden producir DoS, y pueden hachear el sistema. ♦ Se pueden producir ataques tipo Spoofing de IP y ARP. ♦ Acceso ilegal a la red.	Teniendo en consideración los puertos que deben estar abiertos, los servicios que se deben estar ejecutando en el Servidor y quienes están autorizados para usarlos, se deben establecer políticas explícitamente bien definidas en función de: ♦ Tipo de protocolo (TCP o UDP). ♦ Numero de puerto. ♦ Por interfaz física de red (tarjeta de red). ♦ Si es entrante o saliente el tráfico. ♦ Aplicar enmascaramiento NAT. ♦ Restringir direcciones privadas entrantes. ♦ Restringir el ingreso de paquetes mal formados y fragmentados.



CIB-ESPOL

Vulnerabilidad	Efecto	Recomendación
No se encuentran restringidos los servicios y protocolos que no son necesarios para el funcionamiento actual del sistema.	Esta situación genera una exposición innecesaria aumentando la probabilidad de ataques o intrusiones de la red.	Sería conveniente restringir más los accesos en el interior de la red. Los siguientes servicios no son necesarios y pueden desactivarse: ♦ Los RSH, RLOGIN y REXECUTE pueden remplazarse con los servicios del SSH, por lo que no deben habilitarse. ♦ No deberían habilitarse el TALK y el FINGER ya que brindan gran cantidad de información a cualquier persona que la solicite. ♦ Los APPLETs y los SCRIPTs no deberían poder ejecutarse en el servidor, aunque sí, en las PCs ya que se dificultaría mucho la navegación si éstos no estuvieran. ♦ El SYSTAT no es necesario salvo cuando se requiere hacer un mantenimiento. Sugerimos que se habilite on demand para esta práctica. El puerto 22 (de SSH) puede restringirse más habilitándolo on demand, y desde alguna PC determinada, la que se usará para el mantenimiento

Tabla 3-8. Vulnerabilidades del Firewall

3.8.5.5. SERVICIOS

Vulnerabilidad	Efecto	Recomendación
El servicio RPC.yasswdd esta activo en el Servidor Linux, este servicio es vulnerable a un ataque remoto por desbordamiento del buffer.	Un usuario malicioso podría explotar esta vulnerabilidad para sobrescribir y ejecutar arbitrariamente código malicioso con privilegios de súper usuario.	Actualizar el sistema operativo con el parche correspondiente y configurarlo de manera segura.

Vulnerabilidad	Efecto	Recomendación
Vieja versión de Open SSH 1.x. en el Servidor Linux.	♦ Con versiones anteriores a la 1, tiene varias vulnerabilidades, las personas pueden ejecutar ciertos comandos. ♦ Acepta conexiones de clientes 1.x, solo debe permitir conexiones de 2 en adelante.	Se recomienda deshabilitar y desinstalar este paquete, cambiarse a la versión Open SSH 2.0 o 3.0.
Telnet se esta ejecutando en el Servidor Linux.	♦ Este servicio no encripta nada, todos los datos (usuarios + passwords) son transferidos en texto plano. ♦ Un usuario remoto puede interceptar los datos con un Sniffer y puede robar los usuarios y passwords.	Se recomienda deshabilitar totalmente este servicio, en su reemplazo se debería usar Open SSH v2.0 o superior, de tal forma que todos los datos de autenticación y los datos viajen encriptados y de manera segura.
Algunos servicios como Pop 3, Telnet y SSH presentan Banners, con información: que sistema operativo se esta ejecutando, la versión del SO y la versión del Kernel o servicio que se esta ejecutando. Esto sucede en ambos servidores Win NT y Linux.	Esta información puede ser de mucha ayuda para el hacker, puesto que con esto el hacker puede encontrar en sitios de internet ciertas vulnerabilidades para el sistema operativo y versión de Kernel en particular, produciendo ataques exitosos y eficaces.	♦ Se recomienda que quite del banner, y los mensajes que muestran las versiones del sistema operativo y las versiones de los servicios. ♦ En el caso de Linux, edite el archivo de configuración del servicio respectivo y cambie los parámetros del banner.
En el Servidor Windows NT y Linux esta habilitado el puerto 21 FTP anónimo	♦ El servicio FTP es un servicio inherentemente inseguro, puesto que los datos, usuario y password son enviados en texto plano. ♦ Un usuario remoto puede interceptar los datos con un Sniffer y	No use FTP anónimo, si necesita usar FTP, manéjelo con usuarios a través de otras aplicaciones como Wu-ftpd o vsftpd, otorgue permisos de solo lectura.



Vulnerabilidad	Efecto	Recomendación
	puede robar los usuarios y passwords. ♦ Su servidor se puede convertir en un repositorio de software robado.	
Todos los servicios presentes en la red están configurados solo para que funcionen y listo, más no de manera segura.	Cualquier hacker puede realizar ataques DoS, debido a que servicios como SMTP, POP3 Y FTP no están correctamente configurados de manera segura.	♦ Se deben usar y proteger los datos de autenticación como usuarios y passwords. ♦ Configurar el número de usuarios concurrentes por servicio. ♦ Numero de conexiones por segundo.

Tabla 3-9. Vulnerabilidades de Servicios en Servidores.

3.8.5.6. ATAQUES EN LA RED

Vulnerabilidad	Efecto	Recomendación
No existe un IDS de red.	♦ El Jefe de Sistema no esta prevenido de los diversos tipos de ataques: DoS, virus, troyanos, Spoofing, sniffing. ♦ Baja rendimiento de la red, debido a la circulación de paquetes innecesarios que no son controlados en la red. ♦ No se controla el buen uso de la red y de los recursos de la empresa.	Se debería usar algún sistema de detección de intrusos, estos deberían ser tolerantes al fallo, y ejecutarse con los mínimos recursos posibles. Ejemplo: Snort.

Tabla 3-10. Vulnerabilidades de Ataques en la Red

3.8.6. SEGURIDAD DE LA BASE DE DATOS

Vulnerabilidad	Efecto	Recomendación
Los datos de la empresa no se clasifican normalmente según su Importancia.	La clasificación de la información de acuerdo a su importancia permite asignar distintos niveles de controles de seguridad según la confidencialidad que sea necesaria, la falta de clasificación en los datos puede provocar la mala asignación de controles de acceso, y así posibilitar la divulgación de información.	Sería conveniente que se clasifique la información en la Empresa, de acuerdo a la importancia de la misma, es decir teniendo en cuenta la confidencialidad y la disponibilidad que debe tener. Se podrían definir tres niveles de información: crítica (la no-disponibilidad de esta información ocasiona un daño en los activos de la empresa), confidencial (en poder de personas no autorizadas compromete los intereses de la empresa) y pública (información de libre circulación). Esta clasificación ser documentada e informada a todo el personal de la organización, y deberá evaluarse y actualizarse periódicamente.
La Base de Datos que se usa es FoxPro la cual no usa la encriptación de datos.	Un hacker, un troyano o un usuario en la empresa podría robar información de la base con herramientas que leen los sectores del disco duro.	Le conviene a la empresa, migrar a una base de datos que maneje los conceptos de encriptación, Ej.: My SQL bajo Linux.

Tabla 3-11. Vulnerabilidades en la Base de Datos



CIB-ESPOL

3.8.7. SEGURIDAD FÍSICA

3.8.7.1. CONTROL DE ACCESO FÍSICO AL CENTRO DE CÓMPUTO

Vulnerabilidad	Efecto	Recomendación
No hay control de acceso físico al centro de cómputos.	Cualquier persona que tenga acceso al área de administración y ante una distracción del personal, puede	Sería conveniente que el área de Sistemas, donde se encuentran los servidores, el switch central y demás equipamiento crítico tenga una medida de seguridad

Vulnerabilidad	Efecto	Recomendación
	ingresar en él, con todo el riesgo que esto implica, debido a la sensibilidad crítica de los datos y activos que allí se Encuentran.	extra, a través de la cuál solo se permita el acceso a los administradores. Esto podría implementarse con una llave, ya que no implica mucho gasto y pueden darse copias solo al personal necesario. Ó, en reemplazo de esta medida, puede agregarse una cámara de video que grabe el interior del centro de cómputos, o modificar la orientación de alguna existente hacia la puerta de ingreso al mismo.

Tabla 3-12. Vulnerabilidad de Acceso Físico



CIB-ESPOL

3.8.7.2. CONTROL DE ACCESO A EQUIPOS

Vulnerabilidad	Efecto	Recomendación
Las máquinas de la empresa disponen de disqueteras y lectoras de CD, aunque solo el 20% de los usuarios no las necesitan. Estos dispositivos están habilitados y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el arranque desde estos dispositivos.	Cualquier usuario puede introducir un disquete o un CD con virus o intentar arrancar desde estos dispositivos, esto implica un gran riesgo a la integridad del equipo y sus datos.	Sería conveniente que las disqueteras y lectoras de discos se deshabilitaran desde el BIOS de cada máquina. Si llega a ser necesario, para realizar alguna tarea de mantenimiento, el administrador de sistemas puede ingresar al BIOS del equipo (utilizando la contraseña que él suministró), habilitar el dispositivo necesario y, una vez utilizado, deshabilitarlo nuevamente.
No hay control de acceso a la configuración del BIOS de las PCs y de los servidores.	Al momento del encendido de la máquina cualquiera podría modificar las opciones de configuración de los equipos.	Sería conveniente que las máquinas tuvieran configurado un password de administrador en el acceso al setup (BIOS), para evitar que se modifiquen las configuraciones base de los equipos, esto podría aplicarse

Vulnerabilidad	Efecto	Recomendación
		tanto a las PCs como a los servidores. Estas contraseñas debería gestionarlas el Administrador del Sistema, en todos los equipos de la red.
No se realizan controles sobre los dispositivos de hardware instalados en las PCs, una vez que se ha completado la instalación de algún equipo, el administrador del sistema no realiza chequeos rutinarios o periódicos.	Cualquier usuario podría sacar, poner o reemplazar algún dispositivo sin que se advierta la modificación.	Sería conveniente que el Administrador del Sistema, o algún encargado de cómputos designado por él, realice chequeos periódicos para comprobar la correcta instalación de los dispositivos de los equipos, su buen funcionamiento y que sus números de series se correspondan con los datos registrados por el Administrador del Sistema al momento de la instalación.
Los servidores del área de Sistemas no se apagan en horarios no laborales, permanecen prendidos las 24 horas del día, aunque durante la noche no se realicen trabajos, permanecen ociosos.	Se acorta el tiempo de vida útil del hardware y se predispone a que se produzcan posibles intrusiones en el momento en que no hay nadie en área de Sistemas para mitigar el ataque.	Debido a que no es necesario que los servidores permanezcan prendidos las 24 horas, podrían apagarse automáticamente a las 12:00, horario en que han cerrado todas las sucursales de la empresa.

Tabla 3-13. Vulnerabilidades Control de Acceso a Equipos

3.8.7.3. DISPOSITIVOS DE SOPORTE

Vulnerabilidad	Efecto	Recomendación
Estaciones de trabajo obsoletas, de las 27 PCs de la empresa, 8 son Pentium I entre 100 y 200 Mghz.	♦ Lentitud, al momento de realizar procesos pesados cada quincena o a fin de mes, debido a que el tiempo de respuesta incrementa.	♦ Sugerimos que compren nuevos equipos, como E] Pentium IV, los cuales vienen con suficiente memoria RAM 256 MB

Vulnerabilidad	Efecto	Recomendación
	♦ No se pueden actualizar los sistemas operativos y las aplicaciones, porque estos requieren mayores demandas de memoria RAM y ciclos de procesador. ♦ Hardware incompatible con sistemas operativos y aplicaciones modernas.	y ciclos de procesador alto 2,4 Ghz o más y suficiente disco duro. ♦ Si la empresa no cuenta actualmente con el dinero necesario para la compra, podría financiarse a un año plazo o ir cambiando poco a poco los equipos

Tabla 3-14. Vulnerabilidades de Dispositivos de Soporte

3.8.8. ADMINISTRACIÓN DEL CPD

3.8.8.1. CAPACITACIÓN

Vulnerabilidad	Efecto	Recomendación
No hay en los empleados de la empresa, plena conciencia con respecto a la importancia de la seguridad informática.	Al no existir una cultura de la seguridad implementada en la empresa, no se asegura el cumplimiento de normas y procedimientos. 	A pesar de que existe una cierta conciencia sobre la seguridad de la información en el sector gerencial de la empresa, el Administrador del Sistema debe hacer hincapié en la concienciación de todos los usuarios, haciéndolos más responsables y partícipes de las medidas de seguridad, ya que son los principales involucrados, tanto los usuarios actuales como los que se incorporen en el futuro. El proceso de concienciación debería ser renovado y transmitido a los usuarios en forma anual para asegurar que todos los usuarios que están afectados tengan acceso a las novedades sobre aspectos de seguridad.

Vulnerabilidad	Efecto	Recomendación
En ningún momento hay consentimiento por parte de los usuarios a que auditen sus actividades en el sistema, ni declaraciones de que conocen las normas de "buen uso" del sistema.	No hay un aval de que el usuario ha comprendido las normas de buen uso del sistema, y que está dispuesto a cumplirlas.	Una vez que el usuario ha sido capacitado en la realización de sus tareas cotidianas y tenga una clara visión del manejo del sistema se le podría comunicar la política de seguridad de la información y los procedimientos establecidos por la empresa, además de un resumen por escrito de las medidas básicas, junto con una copia que debería ser firmada por él y resguardada en el legajo del empleado. Esto implica que está de acuerdo con las normas impuestas, y es conciente de las consecuencias que acarrea el incumplimiento de estas normas.

Tabla 3-15. Vulnerabilidades por Capacitación

3.8.8.2. RESPALDO

Vulnerabilidad	Efecto	Recomendación
No se documentan los cambios que se realizan en la configuración de los servidores, ni la fecha de estas modificaciones.	Se dificulta conocer la configuración exacta y actual de cada servidor, y de esta forma se obstaculiza la tarea del mantenimiento.	Sugerimos que se documente cada uno de estos cambios, para así tener un control y una identificación de los mismos, así se podrá generar un historial de modificaciones y calcular estadísticas de los mismos, y con éstas será posible hacer más eficiente la configuración de los servidores.

Tabla 3-16. Vulnerabilidad en Respaldo.

3.8.8.3. DOCUMENTACIÓN

Vulnerabilidad	Efecto	Recomendación
No hay desarrollados planes de seguridad, procedimientos formales, ni demás manuales o documentos de soporte para la gestión de la seguridad en la red informática.	Al no poseer un buen soporte, la información puede ser incorrecta, inconsistente o desactualizada, lo que genera incertidumbre en el momento de llevar a cabo procedimientos o procesos, lo que dificulta la administración general.	Sugerimos que la documentación posea mas detalles respecto a los siguientes datos: ♦ Plan de contingencia ♦ Política de seguridad ♦ Manual de procedimientos ♦ Manual de usuario (del software y del hardware) ♦ Manual de seguridad para el sistema: detalla las funciones y privilegios de la seguridad. Contiene: configuración, administración y operación del sistema, guías para el buen uso de las características de protección del sistema, etc. ♦ Manual de seguridad para el usuario: asiste a los usuarios del sistema, describe como usar las protecciones, las responsabilidades de la seguridad del sistema.

Tabla 3-17. Vulnerabilidad en Documentación

3.8.9. AUDITORÍAS Y REVISIONES

3.8.9.1. CHEQUEOS DEL SISTEMA



CIB-ESPOL

Vulnerabilidad	Efecto	Recomendación
No cuentan con una aplicación que genere alarmas o avisos cuando ocurre un evento que revista un determinado grado de riesgo.	Para que el Administrador del Sistema tome conocimiento de la ocurrencia de algún incidente problemático, debe leer los registros generados por las aplicaciones,	Aplicación para generar reportes y alarmas, ya que la lectura de los logs es tediosa y poco práctica, sería conveniente generar alarmas o algún otro mecanismo de alerta cuando ocurra algún evento en particular. Usar una aplicación que administre los logs, teniendo en cuenta la severidad de los eventos, e identificando el usuario

Vulnerabilidad	Efecto	Recomendación
	analizarlos y tratar de encontrar problemas en un gran archivo de textos. Esta situación no resulta práctica, y puede ocurrir que la notificación del problema llegue tarde, cuando el error ya está avanzado.	asociado al evento.
No se buscan nuevas herramientas de generación ni gráfico de logs.	Puede perderse efectividad y eficiencia con el uso de herramientas poco prácticas y desactualizadas, que no poseen generación de reportes ni alarmas, para que el Administrador del Sistema esté siempre al tanto de las situaciones riesgosas.	Sería conveniente actualizar continuamente las herramientas que se usan para graficar la información generada en los logs. Debería asignarse la responsabilidad de esta tarea a una persona específica.
No existe una línea de base definida, solo disponen de los datos almacenados en los logs.	No es posible comparar medias o promedios generados en la empresa en situaciones normales con los valores actuales obtenidos de los logs, e identificar actividades inusuales.	Sería conveniente generar líneas de base, en vez de un conjunto de datos históricos, para poder tener información sobre las PCs, los servidores y el sistema en general con detalles sobre, por ejemplo: qué usuario, sector o tarea utiliza más recursos de CPU (para calcular este dato dispongo de los logs generados por el AcuServer), ♦ Qué datos son los que consumen más tráfico de red, memoria o CPU, qué datos se utilizan o se modifican con mas frecuencia, qué archivos tienen mayor índice de crecimiento (en los logs que genera el AcuServer hay información sobre quién accede a cada dato, en que momento accede y en qué

Vulnerabilidad	Efecto	Recomendación
		momento libera los archivos), ♦ Qué aplicaciones son más utilizadas, ♦ Qué aplicaciones consumen más recursos, ♦ Quién utiliza más memoria del servidor, ♦ En qué momento surgen cuellos de botella y en qué recursos, ♦ En qué momento o por cuánto tiempo la memoria o el CPU permanecen usados en un 100% de su capacidad.
Los logs se eliminan sin generar un respaldo de sus datos.	No es posible obtener datos estadísticos para la generación de las líneas de base.	Sería recomendable, antes de eliminar los log, generar un resumen de líneas de base y estos resultados guardarlos en CDs.
En la empresa no se realizan Auditorías programadas, ni rutinas de chequeos de logs.	Resulta difícil verificar el cumplimiento de los requerimientos y procedimientos de seguridad.	Sería conveniente que se programen Auditorías y chequeos aleatorios, para controlar las áreas o funciones críticas con respecto a la seguridad de los datos de la empresa, documentando la ejecución y los resultados de dichas pruebas. Debe tenerse en cuenta la recomendación sobre separación de tareas, ya que la persona que realice dichas revisiones no debería estar comprometida con la tarea a auditar. Además, si el tamaño de la Auditoría lo justifica, sería conveniente que la lleve a cabo un grupo de dos o más personas, para disminuir las tentativas de corrupción.

Tabla 3-18. Vulnerabilidades en Chequeos de Sistema

3.8.9.2. AUDITORÍAS DE CONTROL DE ACCESO

Vulnerabilidad	Efecto	Recomendación
No se generan reportes relativos a las actividades de los usuarios sobre los datos.	Para el administrador del sistema resulta muy complicada la revisión de las actividades de los usuarios basándose en un estudio de los logs, debido a la cantidad de tiempo que implica esta tarea.	Podría utilizarse una herramienta de generación de reportes de manera automática con datos sobre: ♦ Cantidad de usuarios que acceden simultáneamente a la base de datos (cantidad de conexiones activas). ♦ Estadísticas de entrada-salida para cada usuario. ♦ Tiempo y duración de los usuarios en el sistema. ♦ Usuarios que no han ingresado al sistema por un largo período de tiempo. ♦ Ocurrencias de deadlock con la base de datos. ♦ Generación de nuevos objetos de bases de datos. ♦ Modificación de datos. ♦ Número de intentos fallidos de conexiones a bases de datos. Se deberán generar estadísticas o líneas de base de estos datos, a fin de utilizarse para el control de los datos de la base de datos.
No se generan logs cuando un usuario modifica su password.	Deben poder rastrearse todas las actividades del usuario en el sistema.	Sugerimos que se generen logs cuando un usuario modifica su contraseña, agregando datos como la aplicación desde la que se realizó el cambio y en caso que el cambio resulte fallido, el motivo del fallo.
Los logs generados por un login fallido no especifica el motivo del fallo.	No será posible determinar si hubo un error en el sistema, intento de intrusión o el usuario confundió su contraseña, entre otras.	Detallar el motivo del login fallido en el contenido del log.
No se genera un registro cuando	Se imposibilita la generación de estadísticas	Sería conveniente que se generen logs cuando ocurra un

Vulnerabilidad	Efecto	Recomendación
la cuenta de un usuario ha sido bloqueada, ni tampoco un sistema de alerta ante este bloqueo.	al respecto. Al no tener un sistema de alerta que ponga en conocimiento al Administrador del Sistema de esta situación, no le será posible identificar los intentos de intrusión en el momento en que ocurren.	evento de este tipo, y que se avise al Administrador del Sistema por medio de un sistema de alerta. Con este sistema podrían detectarse anticipadamente intentos de intrusión.

Tabla 3-19. Vulnerabilidades en Auditorías de Control de Acceso

3.8.9.3. AUDITORÍAS DE REDES

Vulnerabilidad	Efecto	Recomendación
No poseen un plan de monitorización general de la red.	Puede ocurrir que baje el rendimiento del sistema debido a cuellos de botella en los recursos.	Generar un plan de monitorización, teniendo en cuenta que la monitorización tiene un impacto directo en el rendimiento del sistema. Se podría utilizar, por ejemplo, alguna herramienta para monitorizar el tráfico y rendimiento de red, como un escáner de seguridad integral (Overall Security Scanner).
No se auditan regularmente ni se generan estadísticas sobre los logs referentes al correo electrónico.	Al no tener estas estadísticas no se calculan ni se grafican líneas de base y al no realizar monitoreos periódicos no se puede alertar al Administrador del Sistema sobre anomalías o posibles errores.	El Administrador del Sistema o un encargado del área de Sistemas debería ser responsable de la monitorización de éstos logs, generando reportes diarios o mensuales, con los siguientes datos: ♦ Poco espacio libre de cuotas asignadas al correo. ♦ Disminución en el rendimiento del correo. ♦ Demasiados mensajes entrantes o salientes fuera de lo normal. ♦ Departamento o usuario de la empresa que utiliza más el servicio de e-mail, advertencias ante la aparición de un virus, estadísticas sobre e-mails infectados con virus, períodos de mayor infección, máquinas más afectadas, direcciones fuentes qué mas e-mails infectados

Vulnerabilidad	Efecto	Recomendación
		envían, cantidad de archivos infectados por extensión (Ej. Los archivos de Word se infectan más que los de Excel), entre otras
No se hicieron pruebas de auto-hackeo, escaneos o intentos de intrusión o de escucha en la red informática. Tampoco se hacen pruebas periódicas de puertos o de los servicios que están habilitados.	Al no hacer pruebas o chequeos pueden pasar inadvertidas situaciones que solo serán reveladas utilizando casos prácticos.	Sería conveniente programar chequeos periódicos de la red, incluyendo los siguientes controles: ♦ Los servicios, su configuración y su buen funcionamiento; ♦ Tratar de escuchar o hacer un ataque de intrusión periódicamente, para comprobar que la red sigue siendo inaccesible desde el exterior, realizar pruebas de auto-hackeo: ♦ A los servidores, desde dentro del servidor, ♦ A los servidores, desde la red interna, ♦ A la Intranet desde dentro de ella, ♦ Accesos desde el exterior y/o Internet. Podrían utilizarse herramientas que permiten hacer estas inspecciones en la red en forma automática, para comprobar en qué estado está y determinar si existen vulnerabilidades en algunos sectores de acuerdo a líneas de base ingresadas por el Administrador del Sistema (como COPS, NOCOL, SATAN, SNORK o TRIPWIRE). Además sería posible hacer auto-escaneos para verificar los recursos compartidos, y auto-hackeos para prevenir ataques de intrusión. Sugerimos documentar las pruebas y sus resultados cada vez que se realicen.

Tabla 3-20. Vulnerabilidades en Auditorías de Redes

3.8.10. PLAN DE CONTINGENCIAS

3.8.10.1. ESTRATEGIAS DE RECUPERACIÓN DE DESASTRES

Vulnerabilidad	Efecto	Recomendación
En la empresa no hay planes formales para la administración de incidentes, como Planes de Contingencia, de recuperación de desastres o de reducción de riesgos para el área de Tecnología de Información. Pero se dispone de backups de datos y de un equipo designado a cubrir al servidor de aplicaciones y base de datos en caso de emergencia.	Como no existe un Plan de Contingencias para el área de Tecnología de Información, actualmente las emergencias son administradas por el encargado del departamento de sistemas de acuerdo al criterio de él y las tareas a cumplir en caso de un incidente se las realiza a medida que se presentan y se realizan sin ninguna planificación, lo que en caso de emergencia ocasionaría desorganización y retrasos en la recuperación del sistema o recurso y por periodos de tiempos más prolongados que lo que realmente debería tomar.	Debe conformarse un grupo de desarrollo encargado de concebir, probar e implementar el plan de contingencias para el área de Tecnología de Información. Este debe estar a cargo del administrador del departamento de sistemas, e integrado por los líderes de cada área de la organización.

Tabla 3-21. Vulnerabilidades de Planes de Contingencia

3.9. ANÁLISIS DE RIESGOS

3.9.1. ACTIVOS Y FACTORES DE RIESGOS

Presentamos los distintos activos reconocidos en La Empresa, asignando un valor a la importancia que tienen en la organización, ponderada en una escala del 1 al 10. Esta importancia es un valor subjetivo que refleja el nivel de impacto que puede tener la empresa si un incidente afecta a los activos, sin considerar las medidas de seguridad que existan sobre los mismos.

A continuación se listan los factores de riesgo que pueden afectar a dichos activos, indicando la probabilidad de que estas contingencias ocurran, en una escala del 1 al 3. Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en la organización.

Activos a Proteger	Importancia
Servidores y switch central.	10
Bases de datos.	10
Software de aplicación, programas fuente, sistemas operativos.	9
Respaldo.	9
Datos en tránsito, datos de configuración, datos en medios externos.	8
Administrador de sistemas (Departamento de sistemas).	7
Cableado, antenas, switch, hubs, módems.	6
Red.	6
Usuarios.	5
Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	4
Hardware (teclado, monitor, unidades de discos, medios removibles, etc.).	3
Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	2
Datos de usuarios.	1

Tabla 3-22. Activos a Proteger



CIB-ESPOL

3.9.2. CÁLCULO DE NIVELES DE VULNERABILIDAD

En este cuadro se calculan los niveles de vulnerabilidad (o niveles de riesgo) en los que incurre cada activo. Para esto se tiene en cuenta el nivel de importancia asignado a cada uno y la probabilidad de ocurrencia de estos riesgos. Para realizar dicho cálculo se desarrollaron las siguientes operaciones:

PROBABILIDAD DE OCURRENCIA: Representan la probabilidad de que ocurran los factores de riesgo mencionados, en una escala del 1 al 3. Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en la organización.

PORCENTAJE DE LA PROBABILIDAD DEL RIESGO: Se calcula el porcentaje de probabilidad de que ocurra un determinado factor de riesgo, con respecto a la cantidad de factores de riesgo intervinientes para dicho activo. Esto es debido a que cada activo está afectado por un número diferente de riesgos posibles, de manera que este cálculo sirve para obtener un porcentaje de probabilidades equilibrado por igual para cualquier activo, independientemente de la cantidad de factores de riesgo que lo afecten.

NIVEL DE VULNERABILIDAD: En este momento interviene el nivel de importancia, multiplicando al porcentaje de probabilidad del riesgo. De esta forma se obtiene el nivel de vulnerabilidad de cada activo con respecto a un factor de riesgo. La suma de estos valores es el nivel de vulnerabilidad total que corresponde a cada activo.



Nombre del Activo	Nivel de Importancia.	Factor de Riesgo	Probab. de Ocurrencia	% Prob. Riesgos	Nivel de vulnerabilidad
Servidores y Switch Central	10	Acceso no autorizado	3	30,00	300,00
		Corte de Luz	1	10,00	100,00
		Destrucción de un componente	2	20,00	200,00
		Error de configuración	2	20,00	200,00
		Factores ambientales	1	10,00	100,00
		Límite de vida útil -Máquinas obsoletas	3	30,00	300,00
		Mal mantenimiento	2	20,00	200,00
		Modificación no autorizada de datos	3	30,00	300,00
		Robo	1	10,00	100,00
		Virus	3	30,00	300,00
		Cantidad de factores de riesgo=	10	210,00	2100,00
Bases de datos.	10	Base de datos compleja	2	11,76	117,65
		Copia no autorizada de un medio de datos	2	11,76	117,65
		Errores de software	2	11,76	117,65
		Falla de base de datos	2	11,76	117,65
		Falla en medios externos	1	5,88	58,82
		Falta de espacio de almacenamiento	1	5,88	58,82
		Mala configuración del horario de Respaldos	1	5,88	58,82
		Mala integridad de los datos	2	11,76	117,65
		Pérdida de Respaldos	2	11,76	117,65
		Perdida de confidencialidad en datos privados y de sistema	1	5,88	58,82
		Perdida de datos en tránsito	1	5,88	58,82
		Robo	1	5,88	58,82
		Robo por uso de laptops	1	5,88	58,82
		Sabotaje	2	11,76	117,65
		Spoofing y sniffing	3	17,65	176,47
		Transferencia de datos incorrectos	1	5,88	58,82
		Virus	3	17,65	176,47
		Cantidad de factores de riesgo =	17	164,71	1647,06



CIB-ESPOL

Nombre del Activo	Nivel de Importancia	Factor de Riesgo	Probab. de Ocurrencia	% Prob. Riesgos	Nivel de vulnerabilidad
Datos en tránsito, datos de configuración y datos en medios externos.	8	Copia no autorizada de un medio de datos	3	25,00	200,00
		Falta funciones de encriptación	3	25,00	200,00
		Falla en medios externos	2	16,67	133,33
		Mala integridad de los datos	1	8,33	66,67
		Medios de datos no están disponibles cuando son necesarios	1	8,33	66,67
		Perdida de confidencialidad en datos privados y de sistema	3	25,00	200,00
		Perdida de datos en tránsito	1	8,33	66,67
		Portapapeles, impresoras o directorios compartidos	3	25,00	200,00
		Robo por uso de laptops	1	8,33	66,67
		Sabotaje	2	16,67	133,33
		Spoofing y sniffing	3	25,00	200,00
		Virus	3	25,00	200,00
		Cantidad de factores de riesgo =	12	216,67	1733,33
Administrador de sistemas (Departamento de Sistemas)	7	Administración impropia del sistema de IT (roles y responsabilidades)	2	28,57	200,00
		Almacenamiento de passwords negligente	3	42,86	300,00
		Configuración impropia del Servidor de Correo	2	28,57	200,00
		Errores de configuración y operación	2	28,57	200,00
		Falta de Auditorías en sistema operativo	3	42,86	300,00
		Mal uso de derechos de administrador	1	14,29	100,00
		Falta de evaluación de datos de Auditoría	3	42,86	300,00
		Cantidad de factores de riesgo=	7	228,57	1600,00
Cableado, antenas, switchs, hubs, modem.	6	Ancho de banda insuficiente	2	20,00	120,00
		Conexión de cables inadmisibles	2	20,00	120,00
		Daño de cables inadvertido	1	10,00	60,00
		Factores ambientales	1	10,00	60,00
		Interferencias	1	10,00	60,00
		Límite de vida útil	2	20,00	120,00
		Longitud de los cables de red excedida	1	10,00	60,00
		Mal mantenimiento	2	20,00	120,00
		Reducción de velocidad de transmisión	2	20,00	120,00
		Riesgo por el personal de limpieza o personal externo	2	20,00	120,00
		Cantidad de factores de riesgo =	10	160,00	960,00



Nombre del Activo	Nivel de Importancia	Factor de Riesgo	Probab. de Ocurrencia	% Prob. Riesgos	Nivel de vulnerabilidad
Red.	6	Abuso de puertos para el mantenimiento remoto	2	16,67	100,00
		Ausencia o falta de segmentación	3	25,00	150,00
		Complejidad en el diseño de las redes de sistemas de IT	1	8,33	50,00
		Conexiones todavía activas	2	16,67	100,00
		Configuración inadecuada de componentes de red	2	16,67	100,00
		Denegación de Servicios	3	25,00	150,00
		Errores de configuración y operación	2	16,67	100,00
		Falla en la MAN	1	8,33	50,00
		Falta de autenticación	2	16,67	100,00
		Mal uso de servicios de e-mail	2	16,67	100,00
		Spoofing y sniffing	3	25,00	150,00
		Transporte inseguro de archivos	3	25,00	150,00
		Cantidad de factores de riesgo =	12	216,67	1300,00
Usuarios.	5	Acceso no autorizado a datos	2	12,50	62,50
		Borrado, modificación o revelación desautorizada o inadvertida de información	2	12,50	62,50
		Condiciones de trabajo adversas	1	6,25	31,25
		Destrucción de un componente de hardware	2	12,50	62,50
		Destrucción negligente de datos	2	12,50	62,50
		Documentación deficiente	3	18,75	93,75
		Entrada sin autorización a oficinas	3	18,75	93,75
		Entrenamiento de usuarios inadecuado	3	18,75	93,75
		Falta de Auditorías	3	18,75	93,75
		Falta de cuidado en el manejo de la información (Ej. Password)	3	18,75	93,75
		Ingeniería social - Ingeniería social inversa	3	18,75	93,75
		Mal uso de derechos de administrador (sesiones abiertas)	1	6,25	31,25
		No-cumplimiento con las medidas de seguridad del sistema	3	18,75	93,75
		Pérdida de confidencialidad o integridad de datos como resultado de un error humano en el sistema	2	12,50	62,50
		Desvinculación del personal	1	6,25	31,25
		Uso descontrolado de recursos (DoS)	2	12,50	62,50
		Cantidad de factores de riesgo =	16	225,00	1125,00

Nombre del Activo	Nivel de Importancia.	Factor de Riesgo	Probab. de Ocurrencia	% Pob. Riesgos	Nivel de vulnerabilidad	
Documentación de programas, hardware, sistemas, procedimientos administrativos, locales, manuales, etc.	4	Acceso no autorizado a datos	1	7,69	30,77	
		Borrado, modificación o revelación desautorizada de datos	1	7,69	30,77	
		Browsing de información	1	7,69	30,77	
		Copia no autorizada de un medio de datos	1	7,69	30,77	
		Descripción de archivos inadecuada	1	7,69	30,77	
		Documentación insuficiente o faltante, Funciones no documentadas	2	15,38	61,54	
		Factores ambientales	1	7,69	30,77	
		Mala interpretación	1	7,69	30,77	
		Mantenimiento inadecuado o ausente	2	15,38	61,54	
		Medios de datos no están disponibles cuando son necesarios	1	7,69	30,77	
		Robo	1	7,69	30,77	
		Uso sin autorización	1	7,69	30,77	
		Virus, gusanos y caballos de Troya	1	7,69	30,77	
		Cantidad de Factores de Riesgo =		13	115,38	461,54
		Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	3	Corte de luz o UPS descargado	1	16,67
Destrucción o mal funcionamiento de un componente	2			33,33	100,00	
Factores ambientales	1			16,67	50,00	
Límite de vida útil	2			33,33	100,00	
Mal mantenimiento	1			16,67	50,00	
Robo	1			16,67	50,00	
Cantidad de Factores de Riesgo =				6	133,33	400,00
Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	2	Factores ambientales	1	16,67	33,33	
		Límite de vida útil	1	16,67	33,33	
		Recursos escasos	1	16,67	33,33	
		Uso descontrolado de recursos	1	16,67	33,33	
		Robo	1	16,67	33,33	
		Transporte inseguro de medios de datos	1	16,67	33,33	
		Cantidad de Factores de Riesgo =		6	100,00	200,00



CIB-ESPOL

Nombre del Activo	Nivel de Importancia	Factor de Riesgo	Probabilidad de Ocurrencia	% Pob. Riesgos	Nivel de vulnerabilidad
Datos de usuarios.	1	Falta de espacio de almacenamiento	1	10,00	10,00
		Mala configuración del horario de Respaldos.	1	10,00	10,00
		Medios de datos no están disponibles cuando son necesarios	1	10,00	10,00
		Pérdida de Respaldos	1	10,00	10,00
		Perdida de confidencialidad en datos privados y de sistema	2	20,00	20,00
		Portapapeles, impresoras o directorios compartidos	1	10,00	10,00
		Robo	1	10,00	10,00
		Sabotaje	1	10,00	10,00
		Spoofing y sniffing	3	30,00	30,00
		Virus	3	30,00	30,00
		Cantidad de Factores de Riesgo =	10	150,00	150,00

Tabla 3-23. Cálculo de Niveles de Vulnerabilidad



CIB-ESPOL

3.9.3. NIVELES DE VULNERABILIDAD Y RIESGOS.- RESULTADOS.

En el cuadro se listan los niveles de vulnerabilidad y los porcentajes de riesgo para cada activo obtenidos de la tabla anterior, considerando distintos rangos de valores para la importancia, de 1 a 10, de 1 a 3 y sin tener en cuenta la importancia (es decir con un valor de 1).

N#	Activos	Importancia (1 a 10)	R. %	Import. (1a 3)	R. %
1	Datos de usuarios	150	1,1	150,00	6,8
2	Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	200	1,4	100,00	4,5
3	Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	400	2,9	133,33	6,0
4	Cableado, antenas, Routers, switch, bridge.	960	6,9	160,00	7,2
5	Usuarios.	1125	8,0	225,00	10,1
6	Red.	1300	9,3	216,67	9,8
7	Datos en tránsito, datos de configuración, datos en medios externos.	1733	12,4	216,67	9,8
8	Documentación de programas, hardware, sistemas, procedimientos administrativos, locales, manuales, etc.	462	3,3	115,38	5,2
9	Respaldo.	1108	7,9	123,08	5,5
10	Bases de datos.	1647	11,8	164,71	7,4
11	Software de aplicación, programas fuente, sistemas operativos.	1221	8,7	176,92	8,0
12	Servidores y switch central.	2100	15,0	210,00	9,5
13	Administrador de sistemas (Departamento de sistemas).	1600	11,4	228,57	10,3
		14006,05	100	2220,33	100

Tabla 3-24. Resultados de Niveles de Vulnerabilidad



3.9.4. ANÁLISIS DE IMPORTANCIAS

Aquí vemos un análisis donde se tiene en cuenta el nivel de vulnerabilidad obtenido con una ponderación de la importancia de 1 a 10. Se calculó el porcentaje de los riesgos y el porcentaje de la importancia. Al calcular la diferencia entre estos porcentajes (Dif. de %) se obtiene el porcentaje que muestra cuán sobrevaluados o menospreciados están los activos de acuerdo a sus riesgos. A continuación se calcula el número que representan los porcentajes anteriormente mencionados, de la siguiente manera:

Para aplicar la diferencia de porcentajes a la importancia actual, se multiplican **Imp. x Dif. de %**. Este resultado no está en escala de 1 a 10, por lo que con una regla de tres simple, se centran los valores:

100 % ----- - 10 puntos de importancia

Imp. x Dif. de % ----- ? (= Diferencia de importancia)

A este resultado se le suma (o resta de acuerdo al signo) a la importancia actual, obteniendo la importancia que debería tener cada activo (importancia ideal), de acuerdo al nivel de riesgos encontrado.

Importancia ideal = Importancia actual + Diferencia de importancia

N#	Activos	Σ Riesgo (nivel de vulnerabilidad.)	%	Importancia actual	%	Dif. de %	Dif. De Import.	Import. (ideal)
1	Datos de usuarios.	150	1,07	1	1,25	-0,18	-0,02	0,98
2	Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	200	1,43	2	2,50	-1,07	-0,21	1,79
3	Hardware (teclado, monitor, unidades de discos, medios removibles)	400	2,86	3	3,75	-0,89	-0,27	2,73
4	Cableado, antenas, routers, switch, bridge.	960	6,85	6	7,50	-0,65	-0,39	5,61
5	Usuarios.	1125	8,03	5	6,25	1,78	0,89	5,89
6	Red.	1300	9,28	6	7,50	1,78	1,07	7,07
7	Datos en tránsito, datos de configuración, datos en medios externos.	1733	12,38	8	10,00	2,38	1,90	9,90
8	Documentación de programas, hardware, sistemas, procedimientos	462	3,30	4	5,00	-1,70	-0,68	3,32
9	Respaldo.	1108	7,91	9	11,25	-3,34	-3,01	5,99
10	Bases de datos.	1647	11,76	10	12,50	-0,74	-0,74	9,26
11	Software de aplicación, programas fuente, sistemas operativos.	1221	8,72	9	11,25	-2,53	-2,28	6,72
12	Servidores y switch central.	2100	14,99	10	12,50	2,49	2,49	12,49
13	Administrador de sistemas (Departamento de sistemas).	1600	11,42	7	8,75	2,67	1,87	8,87
		14006	100	80,00	100			80,63

Tabla 3-25. Análisis de Importancia

3.9.5. VALORES MÁXIMOS, MÍNIMOS Y REALES

Se muestran los valores máximos y mínimos de vulnerabilidad que pueden obtener los activos cuando las probabilidades son llevadas a puntos extremos. Estos cálculos se realizan sin tener en cuenta la influencia de la importancia, es decir se representan exclusivamente las debilidades de cada activo, con las medidas de seguridad que actualmente existen en la empresa.

Valores Máximos, Mínimos y Reales= Mínimo Riesgo = 100 (1 x 100), y Máximo Riesgo=300 (3 x 100)							
N#	Activos - Riesgos totales (sin ponderar la importancia)	(333)	%	(111)	%	(123)	%
1	Datos de usuarios.	300	7,69	100	7,69	150,00	6,76
2	Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	300	7,69	100	7,69	100,00	4,50
3	Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	300	7,69	100	7,69	133,33	6,01
4	Cableado, antenas, routers, switch, bridge.	300	7,69	100	7,69	160,00	7,21
5	Usuarios.	300	7,69	100	7,69	225,00	10,13
6	Red.	300	7,69	100	7,69	216,67	9,76
7	Datos en transito, datos de configuración, datos en medios externos.	300	7,69	100	7,69	216,67	9,76
8	Documentación de programas, hardware, sistemas, procedimientos administrativos, manuales, etc.	300	7,69	100	7,69	115,38	5,20
9	Respaldo.	300	7,69	100	7,69	123,08	5,54
10	Bases de datos.	300	7,69	100	7,69	164,71	7,42
11	Software de aplicación, programas fuente, sistemas operativos.	300	7,69	100	7,69	176,92	7,97
12	Servidores y switch central.	300	7,69	100	7,69	210,00	9,46
13	Administrador de sistemas (Departamento de sistemas).	300	7,69	100	7,69	228,57	10,29
		3900	100,00	1300		2220,33	100,00

Tabla 3-26. Valores Máximos, Mínimos y Reales



CIB-ESPOL

3.9.6. CONCLUSIÓN GENERAL

3.9.6.1. ANALISIS

Como conclusión general se puede decir que el porcentaje de riesgos descubiertos en la empresa es del 56,9 % (2220,33 puntos), considerando el nivel máximo de riesgos como el 100% (3900 puntos), y sabiendo que el porcentaje mínimo es de 33.3% (1300 puntos). Por esto podemos concluir que la empresa debería reducir en 23,6 el porcentaje de riesgos descubiertos, para así conseguir el nivel mínimo de riesgos posible y de esta forma llegar a obtener un nivel de seguridad aceptable.

Porcentaje de riesgos descubiertos	56,9
Porcentaje de riesgos mínimos	33,3
Desviación	23,6

Tabla 3-27. Interpretación de Resultados.



CIB-ESPOL

3.9.6.2. INCIDENCIA DEL AREA DE TECNOLOGÍA INFORMÁTICA EN LA EMPRESA

A continuación se muestra la tabla relacionada a los ingresos promedios que la empresa percibe relacionado a la incidencia del área de Tecnología Informática en la empresa, basada en un porcentaje aproximado, para este caso se estimó en 10%.

Mes	Ventas Mensuales (\$)	Incidencia Tecnología Informática a 10%	Peso	Días Laborables	Costo de producción diaria (\$)	Costo de producción por hora (\$)	Costo de producción cada 5 min. (\$)
Enero	200.058	20.005,80	5,36	22	909,35	113,67	9,47
Febrero	246.274	24.627,35	6,60	20	1.231,37	153,92	12,83

Mes	Ventas Mensuales (\$)	Incidencia Tecnología Informática a 10%	Peso	Días Laborables	Costo de producción diaria (\$)	Costo de producción por hora (\$)	Costo de producción cada 5 min. (\$)
Marzo	237.337	23.733,72	6,36	23	1.031,90	128,99	10,75
Abril	241.953	24.195,31	6,48	22	1.099,79	137,47	11,46
Mayo	173.385	17.338,50	4,64	21	825,64	103,21	8,60
Junio	294.160	29.416,00	7,88	22	1.337,09	167,14	13,93
Julio	210.573	21.057,33	5,64	22	957,15	119,64	9,97
Agosto	801.203	80.120,29	21,46	22	3.641,83	455,23	37,94
Septiembre	483.755	48.375,49	12,96	22	2.198,89	274,86	22,91
Octubre	299.837	29.983,71	8,03	21	1.427,80	178,47	14,87
Noviembre	225.000	22.500,00	6,03	19	1.184,21	148,03	12,34
Diciembre	320.000	32.000,00	8,57	21	1.523,81	190,48	15,87
TOTAL	3.733.535	373.353,51	100,00	257	17.368,83	2.171,10	180,93

Tabla 3-28. Incidencia del Área de Tecnología Informática

3.9.6.3. COSTO PROMEDIO DE FACTORES DE RIESGOS EN LA EMPRESA

En la siguiente tabla se muestra los costos promedios de cada factor de riesgo en la empresa, es decir lo que le costaría a la empresa tener inactivo alguno de estos recursos.

N#	Activos	Importancia (1 a 10) %	Promedio de Costo por día (un año) (\$)	Ajustado (\$)	Por hora (\$)	Cada cinco minutos (\$)
1	Datos de usuarios.	1,1	1452,74	15,56	1,94	0,16
2	Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	1,4	1452,74	20,74	2,59	0,22
3	Hardware (teclado, monitor, unidades de discos, medios removibles)	2,9	1452,74	41,49	5,19	0,43
4	Cableado, antenas, routers, switch, bridge.	6,9	1452,74	99,57	12,45	1,04
5	Usuarios.	8,0	1452,74	116,69	14,59	1,22
6	Red.	9,3	1452,74	134,84	16,85	1,40
7	Datos en tránsito, datos de configuración, datos en medios externos.	12,4	1452,74	179,78	22,47	1,87
8	Documentación de programas, hardware, sistemas, procedimientos	3,3	1452,74	47,87	5,98	0,50
9	Respaldo.	7,9	1452,74	114,89	14,36	1,20



N#	Activos	Importancia (1 a 10) %	Promedio de Costo por día (un año) (\$)	Ajustado (\$)	Por hora (\$)	Cada cinco minutos (\$)
10	Bases de datos.	11,8	1452,74	170,84	21,35	1,78
11	Software de aplicación, programas fuente, sistemas operativos.	8,7	1452,74	126,69	15,84	1,32
12	Servidores y switch central.	15,0	1452,74	217,82	27,23	2,27
13	Administrador de sistemas (Departamento de sistemas).	11,4	1452,74	165,96	20,74	1,73
		100,0	18885,59	1452,74	181,59	15,13

Tabla 3-29. Costo promedio de Factores de Riesgo en la Empresa



3.9.6.4. CONCLUSIONES SEGÚN LOS FACTORES DE RIESGOS EN TÉRMINOS MONETARIOS.

En la tabla anterior nos podemos dar cuenta que el departamento de sistemas representa apenas el 10%(\$373.353,51) de las ventas anuales de la empresa. Además, los factores de riesgo más críticos para la empresa son: Servidores, Switch central, Datos en tránsito, datos de configuración, datos en medios externos y Bases de datos, y el de menor riesgo son los datos de usuarios.

En otras palabras a la empresa le costaría \$27,23 tener fuera de servicio los Servidores y Switch central, \$22,47 por perder los Datos en tránsito, datos de configuración, datos en medios externos, y \$ 21,35 por tener fuera de servicio la base de datos, cada uno durante una hora. En el peor de los casos, es decir, que este fuera de servicio absolutamente todo el Departamento de Sistemas le costaría \$181,59 por hora.

Finalmente, la empresa debería establecer un esquema de seguridad, reforzando principalmente y especialmente los factores de riesgos más críticos, ya que el

descuido de estos, provocaría una pérdida de dinero significativa a la empresa por cada hora que estuviera fuera de servicio.



4. SOLUCIONES DE SEGURIDAD PROPUESTAS

4.1. ESQUEMA DE RED PROPUESTO

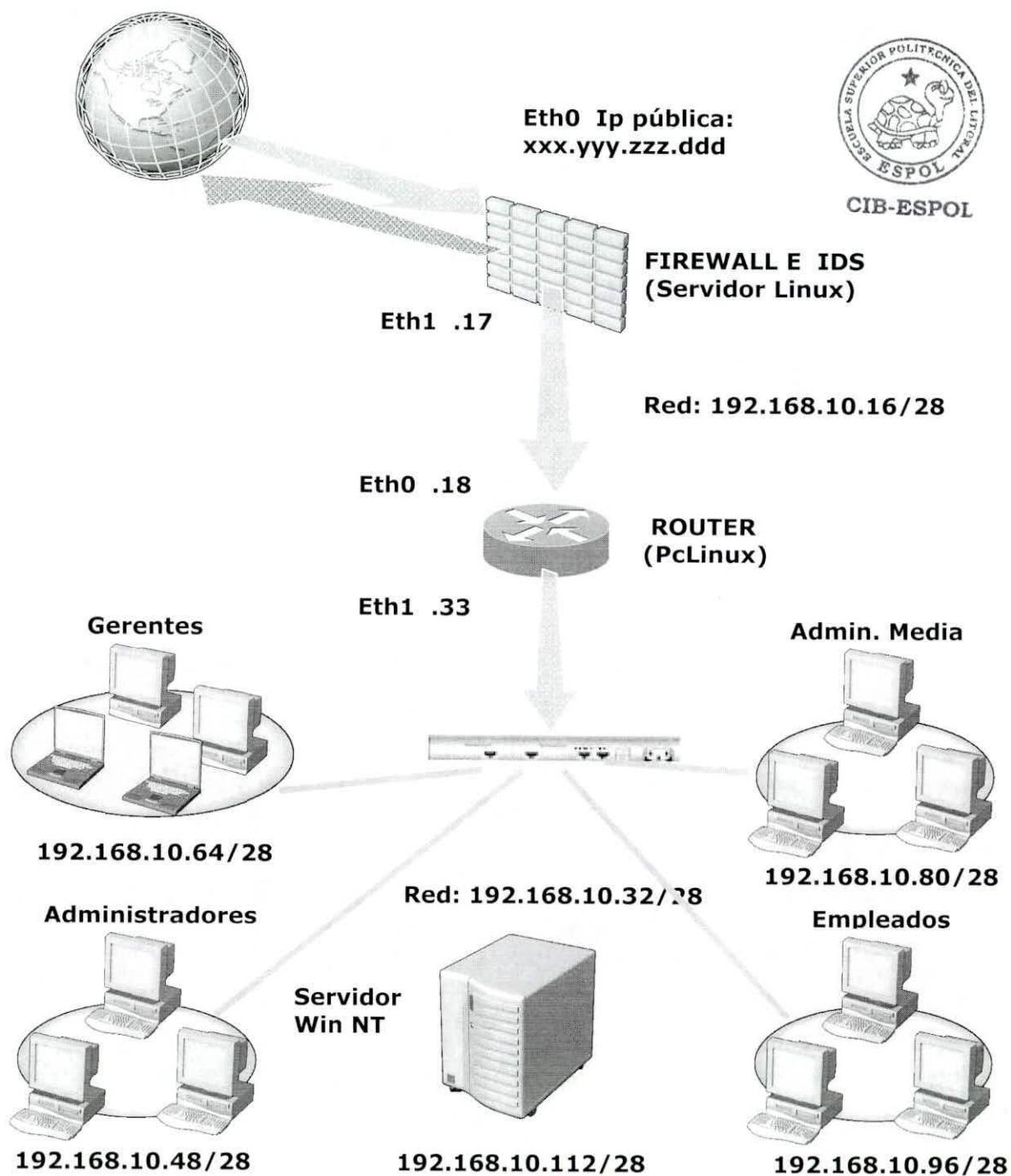


Figura 4-1. Esquema de Red Propuesto

4.2. SERVICIOS EN LOS SERVIDORES.

SERVIDORES	SERVICIOS
Linux	♦ HTTP ♦ IPtables ♦ IDS ♦ Squid (Proxy) ♦ NAT
Windows NT	♦ Base de Datos en FoxPro ♦ Oficina de Correos (Microsoft Outlook)

Tabla 4-1. Servicios en los Servidores

4.3. PERMISOS DE CONTENIDO POR GRUPOS

GRUPO	CONTENIDO
Administradores	Todos los sitios.
Gerentes	Todos los sitios excluidos pornografía, música, videos, juegos.
Admin. Media.	Solo paginas del banco, IESS, SRI.
Empleados	Ningún sitio.

Tabla 4-2. Permisos de Contenido por Grupos

4.4. CLASIFICACION DE USUARIOS POR GRUPOS

GRUPO	RANGO DE DIRECCION	USUARIOS
Administradores	192.168.10.48/28	Gerente General Jefe de Sistemas
Gerentes	192.168.10.64/28	Gerente Financiero Gerente de Logística Gerente de Operaciones Gerente de Importaciones Gerente de RRHH

		Asistente de Importación
Admin. Media.	192.168.10.80/28	Vendedor Contadora Asistente Contable
Empleados	192.168.10.96/28	Asistente de compras Jefe de Bodega Jefe de planta Asistente de cobranzas. Diseñador Arquitectónico Asistente de presupuesto

Tabla 4-3. Clasificación de Usuarios por Grupos



CIB-ESPOL

4.5. RUTEO BAJO LINUX

4.5.1. TABLA COMPARATIVA DE ROUTER LINUX VS ROUTER CISCO 2620.

Características	Router Linux	Cisco 2620
Costo	Pentium I MMX, 200MHz, 1 disquetera 1.44MB, 32MB RAM, monitor no requerido. Menor a \$100.	Procesador Motorola 50MHz, 16MB Flash RAM y 40MB DRAM. Mayor a \$ 3500.
Consumo de Energía Eléctrica	Menor a 30W.	75W.
Numero de Tarjetas Fast Ethernet	Se añaden las necesarias (limitado por el número de ranuras en tarjeta madre).	Solo una disponible.
Modularidad	Puede añadir o quitar paquetes en tiempo de ejecución (usando comando lrpkg).	No es modular.
Compatibilidad de Hardware	Compatible con una amplia variedad de productos disponibles en el mercado.	Generalmente solo productos cisco son usados con routers cisco.
Añadir características adicionales	Puede construir sus propios paquetes conforme a sus	Solo puede usar las características disponibles de la versión del IOS en

Características	Router Linux	Cisco 2620
	necesidades usando Scripts del Shell.	su router específico.
Documentación	Bastante en Internet	Poca en internet. Propiedad de Cisco.
Tecnologías soportadas	Soporta la mayoría, por medio de paquetes adicionales. Además, necesita hardware adicional, el costo de Linux router incrementa, pero sigue siendo mucho menor que el cisco router.	Soporta IPX, Token Ring, VLAN, VPN, Apple Talk y DDR.
Interfaces WAN	Se usan Sangoma WICs, con velocidad sincrónica de 8Mbps. Cuesta alrededor de \$400.	Dos ranuras WIC(una ranura para modulo de red y otra de modo integrado avanzado). Velocidad asincrónica 115.2Kbps y sincrónica de 2048Mbps.

Tabla 4-4. Comparativa de Router.



4.5.2. RAZONES PARA UTILIZAR RUTEO BAJO LINUX

De acuerdo a la tabla comparativa en la que se muestra las posibles soluciones nosotros consideramos que el ruteo lo podemos efectuar utilizando un servidor bajo Linux a través de la herramienta **COYOTE LINUX**, las razones las exponemos a continuación:

- ♦ Debido a que Necesitamos economizar, el Linux router solo nos cuesta \$100 con una PC Pentium I MMX de 200MGHz , lo cual es tres o cuatro veces mas barato que un router comercial con funcionalidades comparables.
- ♦ Debido a que queremos interconectar la empresa de manera segura con internet y además en la LAN hay en total 24 PCs las cuales están repartidas en 4 subredes. No se justifica el costo de un router comercial.

- ♦ Con Coyote Linux se puede arrancar desde un disquete 1.44 MB (no necesita disco duro). Esto hace que su mantenimiento sea barato y sencillo. Es una forma segura contra Hackers.
- ♦ Debido a su rendimiento, estabilidad, bajo costo, alto diseño modular y poco consumo de energía, tomando en cuenta que se trata de una empresa pequeña; el router Linux Es la solución ideal en este caso.

4.5.3. REVISION DE COYOTE LINUX

4.5.3.1. INTRODUCCIÓN

Coyote Linux es una pequeña distribución de Linux diseñada para compartir una conexión a Internet protegiéndola del exterior y que cabe en un disco de 3½ que se crea a partir de un sencillo asistente para Windows o una serie de Shell Scripts en Linux.

Sus características principales con las siguientes:

- ♦ Kernel 2.4.25
- ♦ IPTables
- ♦ Soporte para Ethernet (IP fija o dinámica), PPPoE y PPP DialUp
- ♦ No es necesario Disco Duro ni CD
- ♦ SSH 2.0
- ♦ Soporte QoS

El escenario que queremos conseguir consta de una conexión a Internet, nuestro equipo con Coyote Linux y dentro de la LAN un servidor web y otro de correo:

Esquema

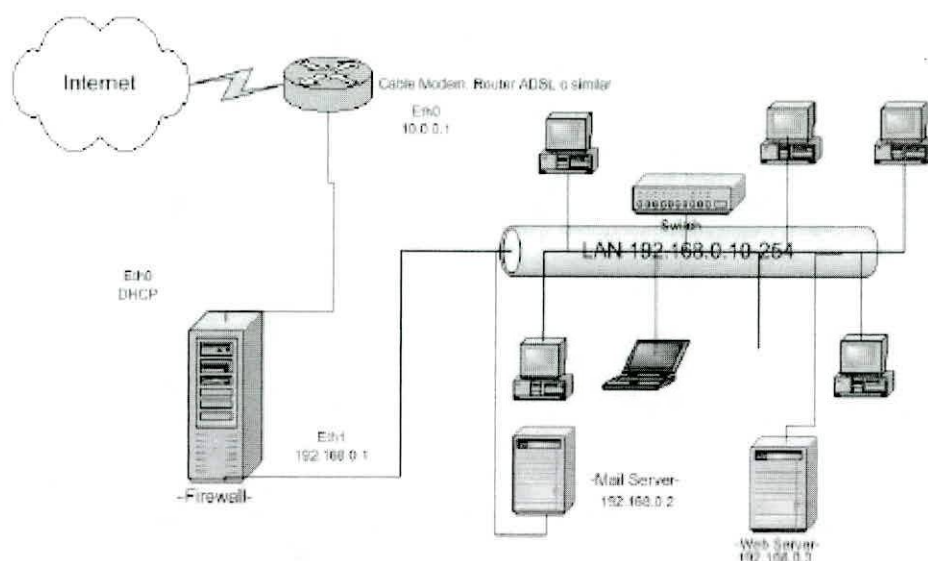


Figura 4-2. Esquema de Seguridad



4.5.3.2. REQUERIMIENTOS

Los requisitos a nivel de Hardware son escasos y los podemos suplir ampliamente con cualquier Pentium con más de 12Mb y una disquetera de 3 ½ es necesario que tenga 2 tarjetas de red a ser posible medianamente conocida (3Com, Intel, Realtek,....)

Para descargar el asistente tenemos que acudir a la siguiente web:

<http://www.coyotelinux.com/downloads/channel.php?ChannelID=5>

4.5.3.3. PREPARACIÓN DEL DISCO

Tras descargar el asistente lo ejecutaremos e ingresamos los siguientes datos a medida que estos nos sean solicitados:

- ♦ Los primeros datos que nos solicita son los referentes a la tarjeta de Red de nuestra LAN:
- ♦ Dirección IP
- ♦ Mascara de subred
- ♦ El siguiente paso es introducir la Password del usuario ROOT:
- ♦ Si disponemos de un servidor SYSLOG para recoger los eventos del Firewall lo Incluiremos.
- ♦ En el siguiente paso se nos solicita el tipo de conexión de la que dispone nuestro Firewall. Por defecto, viene marcado, "DHCP Assigned Address" .
- ♦ Para nuestra red LAN activaremos el servidor DHCP que trae integrado el Firewall en la siguiente pantalla y le pondremos el número máximo de hosts.
- ♦ El paso siguiente es el más delicado ya que tenemos que tener muy claro que tipo de tarjeta de red dispone nuestro equipo. Cuando existan dudas lo mejor es pulsar en el botón Select y luego en la pestaña By Card Name:
- ♦ El último paso es introducir un disquete en blanco y pulsar en el botón Create Disk para que comience el proceso de creación del disco:



CIB-ESPOL

4.5.3.4. CONFIGURACIÓN

Aunque gran parte de la configuración se lleva a cabo con el asistente tenemos que terminar el proceso de configuración creando nuestras reglas en el Firewall para que este sea efectivo.

- ♦ Tras arrancar el equipo y ver que ha reconocido las tarjetas de red la primera prueba que podemos hacer es intentar conectarnos a nuestro Firewall utilizando un PC que esté en la Red Local (LAN) y en el navegador introducir la dirección del Firewall para administrarlo vía Web:



Figura 4-3. Interfaz Web para Administración de Coyote Linux.

- ♦ Lo primero que vamos a cambiar es el puerto de administración por seguridad y algunos datos Administrativos. Para ello tenemos que hacer click en Administrative Configs 8/12.

- ◆ Abrimos los puertos necesarios para navegar en el internet y poder recibir correos desde afuera, abriremos los puertos 80 (http), y 25 (smtp) para que los usuarios puedan navegar en internet y recibir correos.
- ◆ Solo tenemos que introducir el tipo de protocolo (TCP/UDP) el puerto de la máquina interna (80 – http). Este proceso lo tenemos que realizar con todos los puertos que queramos abrir a nuestra red. (21 – 25) Ahora es necesario configurar las reglas para el Firewall en la opción del menú Firewall Configuration: 10/12

Firewall Rules Configuration								
Active	Type	Rule	Protocol	Source	Destination	Port(s)	Comments	Actions
No	Access	Deny	ALL	IP or Host Name 192.168.0.44	Any	ALL	Example - Deny internet access to this IP	[Edit] [Delete]
No	Access	Deny	ALL	IP or Host Name 192.168.0.1013	Any	ALL	Example - Deny internet access to those IP	[Edit] [Delete]
No	Access	Deny	TCP	Any	Any	21	Example - Deny access to FTP sites	[Edit] [Delete]
Yes	Access	Permit	TCP	Any	Any	80	Web Access	[Edit] [Delete]
Yes	Access	Permit	UDP	Any	Any	80	Web Access UDP	[Edit] [Delete]
Yes	Access	Permit	TCP	Any	Any	25	WebMin Access	[Edit] [Delete]
Yes	Access	Permit	TCP	Any	Any	22	SSH Access	[Edit] [Delete]
Yes	Access	Deny	ALL	Any	Any	ALL	Deny All	[Edit] [Delete]

Create a new rule: [Admin | Access | Pre-Configured Services]

Control Actions: [Reload Firewall | Edit Custom Firewall Rules]



Figura 4-4. Configuración de Reglas de Firewall de Coyote Linux.

- ◆ La creación de reglas es muy sencilla de usar y como se puede ver en la anterior imagen todo lo que no se permita explícitamente estará denegado con la última sentencia. En este ejemplo solo se permite el acceso desde cualquier punto al puerto 80, 85, 21 y 22 por lo que el servidor SMTP no podrá funcionar.
- ◆ Vamos a ver como creamos una regla de acceso que permita el tráfico hacia el puerto 25 de nuestro E-mail Server:

Access Rule Configuration	
Active ? Enable/Disable this rule without deleting it	☐ No ☒ Yes
Rule You must choose a rule or custom target	☒ Permit ☐ Deny
Protocol You must choose the protocol or protocol number the service uses	TCP OR
Source Address or Network Computer address or network where the connection is coming from. If you choose IP, Host Name or Mac inform it here else leave this blank.	☐ Not Any
Destination Address or Network Computer address or network where the connection is going to. If you choose IP, Host Name or Mac inform it here else leave this blank.	☐ Not IP or Host Name 192.168.0.2
Starting Port Number The lowest port number of this service.	☐ Not 25
Ending Port Number (Optional) The highest port number of this service.	
Comments (Optional) Any notes about this firewall rule. Suggestion: Machine and service name (e.g. "Web01 HTTP")	Permitir acceso al puerto 25



Figura 4-5. Configuración de Reglas de Acceso de Coyote Linux.

- Tras aceptar nuestra configuración queda de la siguiente forma:

Your firewall rule was ADDED successfully.
You have to Reload Firewall to apply the changes.
Don't forget to save your configuration.

Firewall Rules Configuration								
Active	Type	Rule	Protocol	Source	Destination	Port(s)	Comments	Actions
No	Access Deny		ALL	IP or Host Name 192.168.0.44	Any	ALL	Example - Deny internet access to this IP	[Edit] [Delete]
No	Access Deny		ALL	IP or Host Name 192.168.0.30/23	Any	ALL	Example - Deny internet access to these IP	[Edit] [Delete]
No	Access Deny		TCP	Any	Any	21	Example - Deny access to FTP sites	[Edit] [Delete]
Yes	Access Permit		TCP	Any	Any	80	Web Access	[Edit] [Delete]
Yes	Access Permit		UDP	Any	Any	80	Web Access UDP	[Edit] [Delete]
Yes	Access Permit		TCP	Any	Any	85	WebMin Access	[Edit] [Delete]
Yes	Access Permit		TCP	Any	Any	22	SSH Access	[Edit] [Delete]
Yes	Access Permit		TCP	Any	IP or Host Name 192.168.0.2	25	Permitir acceso al puerto 25	[Edit] [Delete]
Yes	Access Deny		ALL	Any	Any	ALL		[Edit] [Delete]

Figura 4-6. Configuración de Reglas de Firewall de Coyote Linux

- Tras esto solo tenemos que volver a cargar el Firewall y salvar la configuración.

4.6. FIREWALL BAJO LINUX.

4.6.1. TABLA COMPARATIVA DE IPTABLES VS CHECKPOINT

FIREWALL-1.

Características	IPtables	Checkpoint FireWall-1	Ventaja
Filtrado de Paquetes	Graba el estado e inspecciona el contenido en base a: Puerto, dirección IP, red y protocolo.	Inspección statefull y de contenido en base a: Puerto, dirección IP, red y protocolo.	FW-1 es más flexible en configurar las especificaciones de las reglas. IPtables corre Segundo en funcionalidad.
Administración de Políticas	Interfaz de línea de comandos y scripts del shell. Los Constructores de Firewall proveen funcionalidad GUI	GUI fácil de usar. La Administración complicada de las reglas fue hecha por la consola administrable y por el Proveedor-1.	La GUI de FW-1 lo hace superior. Pero el constructor de Firewall le da funcionalidad de arrastrar y soltar a IPtables
Integración de VPN, NAT y protocolos de ruteo.	FreeSWAN provee el cumplimiento de IPsec VPN; IPtables tiene una implementación NAT completa; protocolos de ruteo que Zebra provee.	Provee el cumplimiento de IPsec VPN. FW-1 tiene una implementación NAT completa. Los protocolos de ruteo no los provee Checkpoint.(ipsrd en Nokia)	Añadir y poner en funcionamiento le da a IPtables funcionalidades comparables con FW-1, pero estas no son fáciles de usar.
Rendimiento y Escalabilidad	Capacidad de enlazar a una velocidad mayor a 100Mbps	Capacidad de enlazar a una velocidad mayor a 100 Mbps	Igualdad equitativa, pero IPtables quizás tenga una ventaja en términos de ancho de banda real máximo (throughput) en hardware similar
	No existe un soporte dedicado y disponible,	Actualizaciones, parches y soporte técnico están	A discreción de los usuarios. IPtables tiene flexibilidad



CIB-ESPOL

Características	IPtables	Checkpoint FireWall-1	Ventaja
Mantenimiento y soporte	pero la comunidad open-source provee un soporte amplio. El Código open-source permite a los usuarios aplicar rápidamente arreglos personalizados.	disponibles a través de servicios pagados.	para que lo haga usted mismo, mientras FW-1 tiene un respaldo bien establecido por el vendedor.
Costo	Gratuito.	El Costo de licencias de FW-1 en redes con mas de 100 hosts internos es de \$ 10000	IPtables es definitivamente barato.
Veredicto	La funcionalidad de IPtables y la confiabilidad es excelente, pero requiere más conocimiento para su desarrollo y mantenimiento.	La funcionalidad, soporte y fácil administración son las fortalezas de FW-1.	FW-1 esta a la cabeza, pero IPtables lo esta alcanzando.

Tabla 4-5. Comparativas de Firewall



CIB-ESPOL

4.6.2. TABLA COMPARATIVA DE IPTABLES VS CISCO PIX 2621

Características	IPtables	Cisco PIX 2621	Ventaja
Filtrado de Paquetes	Graba el estado e inspecciona el contenido en base a: Puerto, dirección IP, red y protocolo.	Inspección statefull y de contenido en base a: Puerto, dirección IP, red y protocolo.	El filtrado statefull de red y el dinámico hacen que el Cisco Pix sea mejor en su funcionalidad
Administración	Interfaz de línea de comandos y scripts del shell.	Interfaz de línea de comandos. No pose GUI.	El constructor de Firewall le da funcionalidad de

Características de Políticas	IPtables	Cisco PIX 2621	Ventaja
	Los Constructores de Firewall proveen funcionalidad GUI		arrastrar y soltar a IPtables, esto lo hace ver un poco superior.
Integración de VPN, NAT y protocolos de ruteo.	FreeSWAN provee el cumplimiento de IPsec VPN; IPtables tiene un implementación NAT completa; protocolos de ruteo que Zebra provee.	Provee el cumplimiento de IPsec VPN y soporte propietario CET. Cisco Pix tiene implementación NAT completa; posee algunos protocolos de ruteo dependiendo del modelo.	Cisco Pix le da muchos beneficios a redes heterogéneas porque se integra con muchos protocolos.
Características de protección de Aplicaciones	Filtra Java, Java Scripts, Active X, protection e-mail proxy.	Filtra Java, Java Scripts. Pero no filtra Active X.	IPtables tiene más control sobre este tipo de objetos IPtables, java Scripts y se integra muy bien con el browser.
Rendimiento y Escalabilidad	Capacidad de enlazar a una velocidad mucho mayor Dependiendo del tamaño del paquete y de las reglas.	Capacidad de enlazar a una velocidad en promedio dos veces menor dependiendo del tamaño de los paquetes y las reglas.	IPtables tiene una ventaja en términos de ancho de banda real máximo (throughput), ya que permite establecer enlaces doblemente mas rápidos que los Cisco Pix.
Mantenimiento y soporte	No existe un soporte dedicado y disponible, pero la comunidad open-source provee un soporte amplio. Código open-source permite a los usuarios aplicar	Actualizaciones, parches y soporte técnico están disponibles a través de servicios pagados.	A discreción de los usuarios. IPtables tiene flexibilidad para que lo haga usted mismo, mientras Cisco Pix tiene un respaldo bien establecido por el vendedor.

Características	IPtables	Cisco PIX 2621	Ventaja
	rápida arreglos personalizados.		
Costo	Gratuito.	Cisco Pix 501-50 con licencias para 50 usuarios SOHO. Precio: \$545.00 - \$744.00.	IPtables es definitivamente barato.

Tabla 4-6. Comparativa de Firewall



CIB-ESPOL

4.6.3. RAZONES PARA UTILIZAR IPTABLES

En la tabla comparativa se muestra las posibles soluciones de firewall, nosotros escogimos como Firewall a IPtables por las siguientes razones:

- ♦ La empresa no depende directamente del área del sistemas, razón por la cual, puede prescindir del sistema durante un periodo de tiempo prudencial.
- ♦ Económicamente, no se justifica el gasto en un Firewall de Caja (Cisco Pix) u otro Firewall de software (FireWall-1), ya que la empresa no maneja un volumen de transacciones considerables a través del internet.
- ♦ La empresa es relativamente pequeña.
- ♦ IPtables le da a la empresa un nivel de protección medio.
- ♦ IPtables no se queda atrás, tiene casi las mismas características que los demás firewalls.
- ♦ Es más rápido, en evaluar el tráfico entrante y saliente, permitiendo un mayor ancho de banda que los demás firewalls.
- ♦ Su costo de mantenimiento, es relativamente bajo en comparación con otras soluciones.

- ♦ Es gratuito.
- ♦ Le permite a la empresa aprovechar sus recursos en el momento de la implementación, ya que esta cuenta con un servidor bajo Linux.
- ♦ En el internet existe mucha información de soporte en la comunidad open-source.

4.6.4. REVISION DE IPTABLES.

4.6.4.1. ¿QUÉ ES UN FIREWALL?

Un firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos. El firewall puede ser un dispositivo físico o un software sobre un sistema operativo. En general debemos verlo como una caja con DOS o mas interfaces de red en la que se establecen una reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT.

Esa sería la definición genérica, hoy en día un firewall es un hardware específico con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/..IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red.

Aparte de las diferencias entre firewalls de hardware y software también existen diferencias en la forma en que funciona el firewall que separa una solución de otra.

Método	Descripción	Ventaja	Desventaja
NAT	Network Address Translation (NAT) Ubica sus direcciones IP de subredes internas detrás de una pequeña cola de direcciones IP externas, enmascarando todos los requerimientos hacia un recurso en vez de muchos.	Puede ser configurado transparentemente hacia máquinas en una Lan. Protege muchas máquinas y servicios detrás de una o más direcciones Ip externas simplificando las tareas administrativas. Restringe los accesos de usuarios hacia y desde una Lan y puede ser configurada abriendo y cerrando los puertos en el firewall/gateway NAT.	No puede prevenir actividad maliciosa una vez que los usuarios se conectan hacia un servicio fuera del firewall.
Filtrador de paquetes.	Los firewalls de filtrado de paquetes leen cada paquete que pasa hacia adentro y fuera de una Lan. Puede leer y procesar paquetes a través de la información de la cabecera y filtran los paquetes basándose en un conjunto de reglas programables implementadas por el administrador del firewall. El kernel de Linux tiene construida la funcionalidad de filtrado de paquetes a través del subsistema de kernel Netfilter.	Personalizable a través del utilitario IPTables. No requiere personalización alguna en el lado del cliente, toda la actividad de la red es filtrada a nivel de router y no a nivel de aplicación. Debido a que los paquetes no son transmitidos a través de proxy el rendimiento de la red es más rápido debido a la conexión directa desde el cliente hacia el host remoto.	No puede filtrar paquetes por contenido como un firewall proxy. Procesa los paquetes a nivel de la capa de protocolo pero no puede filtrar los paquetes a nivel de la capa de aplicación. Arquitecturas de red complejas pueden establecer reglas difíciles de filtrado de paquetes, especialmente si el emparejamiento con la mascara IP ó subredes locales y redes de DMZ.



CIB-ESPOL

Método	Descripción	Ventaja	Desventaja
Proxy	Firewalls Proxy filtran todos los requerimientos de ciertos protocolos o tipos desde clientes Lan hacia la máquina Proxy, la cual hace estos requerimientos al internet en medio de un cliente local. Una máquina proxy actúa como memoria entre usuarios remotos maliciosos y las máquinas clientes de la red interna.	Le da control a los administradores sobre que aplicaciones y protocolos fuera de la Lan. Algunos servidores proxy pueden almacenar datos de esta manera los clientes pueden acceder frecuentemente para solicitar datos desde la memoria local en vez de tener que usar la conexión de internet para solicitarlo, lo cual es conveniente para cortar el consumo innecesario de ancho de banda. Los servicios proxy pueden ser registrados y monitoreados cercanamente, permitiendo un estricto control sobre la utilización del recurso en la red.	Los Proxies son frecuentemente aplicaciones específicas (HTTP, Telnet, etc) ó protocolos restringidos (muchos proxies trabajan solo con servicios conectados TCP). Servicios de aplicación no pueden correr detrás de un proxy, de tal forma que sus servidores de aplicación deben usar una forma separada de seguridad de red. Los proxies pueden transformarse en un cuello de botella en la red debido a que todos los requerimientos y transmisiones son pasadas a través de un recurso en vez de hacerlo directamente desde el cliente hacia la conexión del servicio remoto.

Tabla 4-7. Tipos de Firewalls.

4.6.4.2. ¿QUÉ ES UN FILTRO DE PAQUETES?

Un filtro de paquetes es un software que examina la cabecera de los paquetes según van pasando, y decide la suerte del paquete completo. Podría decidir descartarlo (DROP) esto es, como si nunca lo hubiera recibido, ó aceptarlo (ACCEPT) y dejar que pase, o cosas más complicadas.

En Linux, el filtrado de paquetes está programado en el núcleo (como módulo o como componente estático), y hay algunas cosas curiosas que podemos hacer con los paquetes, pero aún sigue ahí el principio general de mirar las cabeceras para decidir la suerte del paquete.



CIB-ESPOL

¿Para qué queremos un Filtro de Paquetes?

♦ Control:

Cuando está usando una máquina Linux para conectar su red interna a otra (por ejemplo, Internet), tiene la oportunidad de permitir ciertos tipos de tráfico, y restringir otros. Por ejemplo, la cabecera de un paquete contiene la dirección de destino del paquete, de manera que puede evitar que salgan los que van a cierto sitio fuera de la red. Otro ejemplo: para los que usan Netscape para acceder a los archivos de Dilbert. Hay anuncios de doubleclick.net en la página, y Netscape malgasta su tiempo bajándoselos alegremente. Se resuelve el problema diciéndole a nuestro filtro de paquetes que no permita que ningún paquete vaya de o hacia las direcciones de doubleclick.net.

♦ Seguridad:

Cuando su máquina Linux es lo único entre el caos de Internet y ordenada red, es bueno saber que puede restringir lo que llega cerrando su puerta. Por ejemplo, podríamos permitir todo lo que salga de la red, pero puede que esté preocupado por el bien conocido «Ping de la Muerte» que puede llegar de gente maliciosa del exterior. En otro ejemplo, podría ser que no quisiera que la gente de fuera pueda hacer telnet a su máquina Linux, incluso aunque todas sus cuentas tengan clave. Quizá quiera (como la mayoría) ser un observador en Internet, y no un servidor. Simplemente, no quiere dejar que nadie se conecte, haciendo que el filtro de paquetes rechace los paquetes entrantes que se usan para establecer conexiones.

♦ Vigilancia:

Algunas veces, una máquina mal configurada de la red local puede decidir votar paquetes al mundo exterior. Es bueno decirle al filtro de paquetes que le avise si ocurre algo anormal; quizá usted pueda hacer algo al respecto, o puede que sencillamente sea curioso por naturaleza.

¿Cómo hago el Filtrado de Paquetes con Linux?

Necesita un núcleo que contenga la infraestructura netfilter. Netfilter es un área de trabajo general dentro del núcleo, a la que pueden conectarse otras cosas (como el módulo de IPtables). Esto significa que necesitará un núcleo 2.3.15 o más nuevo, y responder «Y» a CONFIG_NETFILTER en la configuración del núcleo.



La herramienta IPtables se comunica con el núcleo y le dice qué paquetes filtrar. A menos que sea programador, o muy curioso, es ésta la manera en que controlará el filtrado de paquetes.

4.6.4.3. ¿QUÉ ES IPTABLES?

IPtables es un sistema de firewall vinculado al kernel de Linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema IPchains, un firewall de IPtables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación (esto es una pequeña mentira, ha tenido alguna vulnerabilidad que permite DoS, pero nunca tendrá tanto peligro como las aplicaciones que escuchan en determinado puerto TCP): IPtables está integrado con el kernel, es parte del sistema operativo.

La herramienta IPtables inserta y elimina reglas de la tabla de filtrado de paquetes del núcleo. Esto significa que cualquier cosa que establezca, se perderá cuando reinicie; vea hacer permanentes las reglas para estar seguro de que serán restauradas la siguiente vez que Linux arranque.

Hacer permanentes las reglas

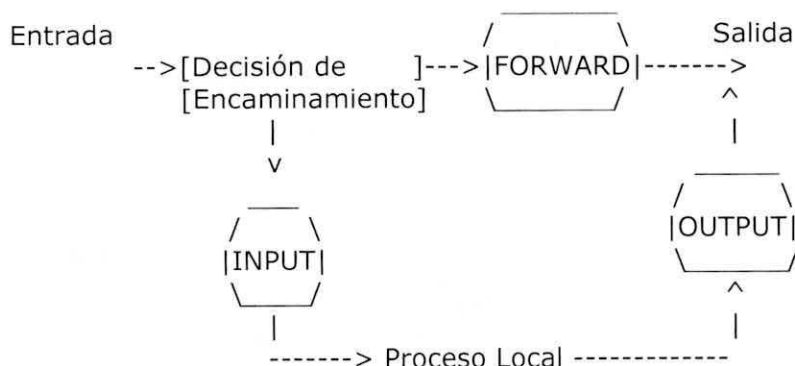
La configuración que su firewall tiene en este momento está almacenada en el núcleo, de manera que se perderá cuando reinicie. En mi lista TODO (Por Hacer) está escribir IPtables-save e IPtables-restore.

Mientras tanto, escriba las órdenes necesarias para configurar sus reglas en un guión (script) de inicio. Asegúrese de que hace algo inteligente en el caso de que alguna de las reglas falle (normalmente «exec /sbin/sulogin»)

¿Cómo pasan los paquetes por los filtros?

El núcleo empieza con tres listas de reglas en la tabla de «filtros»; estas listas se llaman cadenas cortafuegos o sencillamente cadenas. Se llaman INPUT, OUTPUT y FORWARD.

Las cadenas están dispuestas de esta manera:



Estos tres círculos representan las tres cadenas que mencionamos antes. Cuando un paquete alcanza un círculo en el diagrama, se examina esa cadena para decidir la suerte del paquete. Si la cadena dice que hay que descartar (DROP) el paquete, se le muere ahí mismo, pero si la cadena dice que hay aceptarlo (ACCEPT), continúa su camino por el diagrama.

Una cadena es una lista de reglas. Cada regla dice «si el paquete se parece a esto, entonces esto otro es lo que hay que hacer con él». Si la regla no se ajusta

al paquete, entonces se consulta la siguiente regla en la lista. Al final, si no hay más reglas por consultar, el núcleo mira la política de la cadena para decidir qué hacer. En un sistema consciente de la seguridad, esta política suele decirle al núcleo que descarte (DROP) el paquete.

1. Cuando llega un paquete (digamos, por la tarjeta Ethernet) el núcleo mira primero su destino: a esto se le llama «encaminamiento» (routing).
2. Si está destinado a esa misma máquina, el paquete entra en el diagrama hacia la cadena INPUT. Si pasa de aquí, cualquier proceso que esté esperando por el paquete, lo recibirá.
3. En caso contrario, si el núcleo no tiene las capacidades de reenvío activadas, o no sabe hacia dónde reenviar el paquete, se descarta el paquete. Si está activado el reenvío, y el paquete está destinado a otra interfaz de red (si tenemos otra), entonces el paquete pasa directamente a la cadena FORWARD de nuestro diagrama. Si es ACCEPT, entonces saldrá de la máquina.
4. Finalmente, si un programa que se ejecuta en la máquina puede enviar paquetes de red. Estos paquetes pasan por la cadena OUTPUT de forma inmediata: si los acepta (ACCEPT), entonces el paquete continúa hacia afuera, dirigido a la interfaz a la que estuviera destinada.

4.6.4.4. GENERACIÓN DE POLÍTICAS Y REGLAS DE FILTRADO DE PAQUETES

Para comprender los pasos que se indican a continuación es bastante recomendable haber leído algún documento general sobre el funcionamiento de NetFilter, aunque se intentará explicar cada regla con todo el detalle posible. Como introducción, diremos que en NetFilter los paquetes pasan por una serie de tablas, y dentro de las tablas, a su vez por un conjunto de cadenas, en orden. Las tablas predefinidas son filter, nat y mangle, de las cuales las más importantes y usadas son las dos primeras. Dentro de la tabla filter, se usarán las cadenas INPUT y OUTPUT (que filtran el tráfico cuya dirección de origen o de destino es el firewall) y FORWARD (que filtra el tráfico que debe enrutarse de una interfaz a otra). Y dentro de la tabla nat, se usará la cadena POSTROUTING (que es la que permite activar el enmascaramiento).

Dentro de cada cadena se puede definir una serie de reglas, contra las que se comparará cada paquete que pase por esa cadena, y las acciones a tomar en caso de que el paquete se ajuste al definido en la regla. Como parte de la cadena, se define una política, que es la que decide qué se hace con un paquete que ha pasado por dicha cadena, pero no ha coincidido con ninguna regla.

Una vez identificadas las interfaces y clasificados los tipos de tráfico que se permitirán y bloquearán entre ellas mediante las tablas que se han preparado en el apartado anterior, la generación de las reglas para NetFilter es inmediata. A continuación se incluirán los elementos de las tablas anteriores, por partes, junto con las reglas NetFilter que se generarán para ellas.



1. Es necesario comenzar limpiando todas las tablas de las reglas que hubiese anteriormente. Esto se consigue con los siguientes comandos:

```
iptables -t filter -F
iptables -t nat -F
IPTables -t mangle -F
```

2. Segundo se definen las políticas por defecto que se usarán en las cadenas: rechazo (REJECT) en las cadenas INPUT y FORWARD, y aceptar (ACCEPT) en la cadena OUTPUT. Este tipo de política es la más común en los firewalls ("descartar todo lo que no se ajuste a alguna de las reglas explícitas"). Estas políticas se activan con las siguientes reglas:

```
iptables -t filter -P INPUT DROP
iptables -t filter -P FORWARD DROP
iptables -t filter -P OUTPUT ACCEPT
```

3. A continuación, las reglas para el tráfico entre eth0 y ppp0:

Interfaces	Origen	Destino	Permitido	Resto	Descripción
eth0-ppp0	eth0	ppp0	Todo		Permitimos todo el tráfico de salida desde la red privada hacia Internet
	ppp0	eth0	Paquetes de Conexiones Abiertas	Log y Rechazar	Rechazamos todo lo que venga de Internet, salvo los paquetes de vuelta pertenecientes a conexiones establecidas

Tabla 4-8. Reglas de Filtrado de Paquetes.

Esto se consigue mediante las siguientes reglas:

```
IPTables -t filter -A FORWARD -i eth0 -o ppp0 -j ACCEPT
```

```
IPTables -t filter -A FORWARD -i ppp0 -o eth0 -p tcp ! --syn -j ACCEPT
```

Merece especial atención la segunda regla, por la forma en que se especifica la condición "Paquetes de Conexiones Abiertas": esto se traduce en paquetes TCP que no tengan el bit SYN activado (este es el bit que indica una solicitud de conexión). Con esto se permite que los paquetes de vuelta de conexiones iniciadas desde la red en eth0 lleguen a su destino, pero no se permite que se inicien conexiones hacia la red eth0, que es lo que se pretende.

4. Para los paquetes entre eth1 y ppp0, y entre eth0 y eth1, las reglas son idénticas, así que no incluiremos aquí la parte correspondiente de la tabla, simplemente las reglas:

```
IPtables -t filter -A FORWARD -i eth0 -o eth1 -j ACCEPT
```

```
IPtables -t filter -A FORWARD -i eth1 -o eth0 -p tcp ! --syn -j ACCEPT
```

```
IPtables -t filter -A FORWARD -i eth1 -o ppp0 -j ACCEPT
```

```
IPtables -t filter -A FORWARD -i ppp0 -o eth1 -p tcp ! --syn -j ACCEPT
```

5. Para finalizar con la cadena FORWARD, se añadirá la regla necesaria para que cualquier paquete que no haya sido captado por ninguna de las reglas anteriores, sea anotado en el log del sistema, antes de ser rechazado por la política de la cadena:

```
iptables -t filter -A FORWARD -j LOG
```



CIB-ESPOL

6. A continuación, se crearán las reglas necesarias para las cadenas INPUT y OUTPUT, que son las que rigen el tráfico que involucra directamente al firewall. Entre la interfaz eth0 y el nodo:

Interfaz	Origen	Destino	Permitido	Resto	Descripción
eth0	eth0	NODO	Todo		Permitimos todo el tráfico entrante y saliente entre la red privada y el nodo. Suponemos que es una red fiable.
	NODO	eth0	Todo		

Tabla 4-9. Reglas de Filtrado de Paquetes.

La primera regla es muy sencilla; ni siquiera hay que preocuparse de la cadena OUTPUT, ya que la política por defecto en esta cadena es dejar pasar el tráfico. Así que solo hay que añadir la siguiente regla:

IPtables -t filter -A INPUT -i eth0 -j ACCEPT



CIB-ESPOL

7. Entre la interfaz eth1 y el nodo:

Interfaz	Origen	Destino	Permitido	Resto	Notas
eth1	eth1	NODO	DNS(udp), ICMP, DHCP(udp), www(tcp), Paquetes de Conexiones Abiertas	Log y Rechazar	Permitimos tráfico DNS e ICMP ("inofensivo"), WWW (nuestro nodo puede mostrar información de interés), y DHCP (necesario para el funcionamiento de MadridWireless)
	NODO	eth1	Todo		Permitimos todo el tráfico saliente del nodo hacia MadridWireless

Tabla 4-10. Regla de Filtrado de Paquetes.

Las reglas generadas para esta parte son las siguientes:

```

IPTables -t filter -A INPUT -i eth1 -p tcp ! --syn -j ACCEPT
IPTables -t filter -A INPUT -i eth1 -p tcp --dport www --syn -j ACCEPT
IPTables -t filter -A INPUT -i eth1 -p udp --dport domain -j ACCEPT
IPTables -t filter -A INPUT -i eth1 -p udp -s 0.0.0.0 --sport bootpc \
        -d 255.255.255.255 --dport bootps -j ACCEPT
IPTables -t filter -A INPUT -i eth1 -p icmp -j ACCEPT

```

Con la primera de ellas permitimos los paquetes de conexiones TCP ya abiertas. La segunda es la que permite que nuestro nodo ofrezca servicio Web. La tercera es la que permite el tráfico DNS. La cuarta es la más crítica, ya que permite que el nodo reciba paquetes DHCP - paquetes con dirección origen 0.0.0.0 y puerto origen el del cliente BOOTP (bootpc - 68), y con dirección de destino 255.255.255.255 y puerto de destino el del servidor BOOTP (bootps - 67) -. Finalmente, la última de ellas es la que permite que el nodo reciba paquetes ICMP.

De nuevo, no es necesario activar ninguna regla para la cadena OUTPUT, con motivo de la política que está activa en dicha cadena.

8. Y finalmente, para las comunicaciones entre el nodo e Internet:

Interfaz	Origen	Destino	Permitido	Resto	Descripción
ppp0	ppp0	NODO	DNS(udp), ICMP, auth(tcp), Paquetes de Conexiones Abiertas	Log y Rechazar	Permitimos tráfico DNS e ICMP ("inofensivo") y AUTH (algunos servidores FTP se empeñan en saber quien les llama ;-)

Interfaz	Origen	Destino	Permitido	Resto	Descripción
	NODO	ppp0	Todo		Permitimos todo el tráfico saliente del nodo hacia Internet

Tabla 4-11. Reglas de Filtrado de Paquetes.

Las reglas generadas aquí son las siguientes:

```

IPTables -t filter -A INPUT -i ppp0 -p tcp ! --syn -j ACCEPT
IPTables -t filter -A INPUT -i ppp0 -p tcp --dport auth --syn -j ACCEPT
IPTables -t filter -A INPUT -i ppp0 -p udp --sport domain -j ACCEPT
IPTables -t filter -A INPUT -i ppp0 -p icmp -j ACCEPT

```

Con la primera de ellas, al igual que en la tabla anterior, se permiten el tráfico correspondiente a conexiones TCP ya abiertas. La segunda de ellas es la que permite las conexiones AUTH al nodo (este tipo de conexiones son efectuadas a veces por sistemas remotos en respuesta a intentos de conexión, y en caso de no ser permitidas provocan a veces retrasos en las conexiones y ocasionalmente fallos. Para evitarlo, es sencillo abrir este tipo de conexiones, y tener activado un servidor AUTH que no proporcione información al exterior). La tercera permite el tráfico DNS de entrada, es decir, las respuestas a las consultas DNS que haga el nodo. Finalmente, la cuarta permite el tráfico ICMP.

Una vez más no es necesario activar ninguna regla para permitir el tráfico en la cadena OUTPUT, por el motivo descrito antes.



CIB-ESPOL

9. Para finalizar con la cadena INPUT, también se añadirá una regla para anotar en el log cualquier paquete no captado por ninguna de las reglas anteriores, antes de ser rechazado por la política:

```
iptables -t filter -A INPUT -j LOG
```

10. Y como último paso, una vez activados todos los filtros de tráfico necesarios en los pasos anteriores, es necesario activar el enmascaramiento, para que todas las conexiones con destino a Internet y que hayan pasado los filtros anteriores puedan establecerse con normalidad:

```
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

Se incluye a continuación un único listado completo de todas las reglas creadas para la configuración del firewall en el nodo:

```
# limpieza de reglas anteriores
IPTables -t filter -F
iptables -t nat -F
iptables -t mangle -F
```

```
# establecimiento de políticas por defecto
IPTables -t filter -P INPUT DROP
iptables -t filter -P FORWARD DROP
iptables -t filter -P OUTPUT ACCEPT
```

```
# paquetes de entrada al nodo
iptables -t filter -A INPUT -i eth0 -j ACCEPT
iptables -t filter -A INPUT -i eth1 -p tcp --dport www --syn -j ACCEPT
iptables -t filter -A INPUT -i eth1 -p tcp ! --syn -j ACCEPT
iptables -t filter -A INPUT -i eth1 -p udp --dport domain -j ACCEPT
iptables -t filter -A INPUT -i eth1 -p udp -s 0.0.0.0 --sport bootpc \
-d 255.255.255.255 --dport bootps -j ACCEPT
IPTables -t filter -A INPUT -i eth1 -p icmp -j ACCEPT
IPTables -t filter -A INPUT -i ppp0 -p tcp ! --syn -j ACCEPT
```



CIB-ESPOL


```

IPtables -t filter -A INPUT -i ppp0 -p tcp --dport auth --syn -j ACCEPT
IPtables -t filter -A INPUT -i ppp0 -p udp --sport domain -j ACCEPT
IPtables -t filter -A INPUT -i ppp0 -p icmp -j ACCEPT
IPtables -t filter -A INPUT -j LOG

```

filtrado entre redes

```

IPtables -t filter -A FORWARD -i eth0 -o ppp0 -j ACCEPT
IPtables -t filter -A FORWARD -i ppp0 -o eth0 -p tcp ! --syn -j ACCEPT
IPtables -t filter -A FORWARD -i eth0 -o eth1 -j ACCEPT
IPtables -t filter -A FORWARD -i eth1 -o eth0 -p tcp ! --syn -j ACCEPT
IPtables -t filter -A FORWARD -i eth1 -o ppp0 -j ACCEPT
IPtables -t filter -A FORWARD -i ppp0 -o eth1 -p tcp ! --syn -j ACCEPT
iptables -t filter -A FORWARD -j LOG

```

activación del enmascaramiento

```

IPtables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE

```

Estas reglas deberán ser incluidas en alguno de los scripts de inicio del sistema, de forma que sean ejecutadas automáticamente en el arranque del nodo. Un sitio razonable puede ser al final del archivo /etc/rc.d/rc.local, en RedHat. En otras distribuciones hay scripts con funcionalidad similar donde pueden incluirse.

4.6.5. TABLAS COMPARATIVAS DE PROXYS.

4.6.5.1. MEDIDA DE PRECIO/RENDIMIENTO.

El producto con la medida mas alta, tiene el mejor precio / rendimiento.



CIB-ESPOL

Producto	Requerimientos por segundo por \$1,000
iMimic DataReactor 5000	102
IBM 3500M10	72
Dell PowerEdge 130B	67
Quantex Microsystems WebXL-4000	67
Stratacache Flyer 100	63
Compaq TaskSmart 900	60
IBM 5000	54
Microbits Intelli-App Pizza Box	53

Producto	Requerimientos por segundo por \$1,000
IBM 5600	52
Compaq TaskSmart 2500	47
Squid	37
Swell Tsunami CPX-1000	33
Lucent IPWorX WebCache 100	33
InfoLibria DynaCache X1 cluster	32
Lucent IPWorX WebCache 150a	28
InfoLibria DynaCache 30I	25
Network Appliance NetCache	25
Cisco Cache Engine 590	21
Pionex PCA-1000	23
Cisco Cache Engine 7300	18

Tabla 4-12. Comparativa Proxy Medida de Precio/Rendimiento

4.6.5.2. TASAS DE REQUERIMIENTO

Las tasas de petición miden el número de veces que el cache produce una requerimiento vs. las veces que el requerimiento es pasado al web. El producto con tasa más alta, tiene el mejor rendimiento.

Producto	Tasas de requerimientos de documentos
Squid	55.0%
Swell Tsunami CPX-1000	55.0%
Cisco Cache Engine 590	54.8%
Cisco Cache Engine 7300	54.5%
Lucent IPWorX WebCache 150a	54.2%
iMimic DataReactor 5000	53.2%
Pionex PCA-1000	52.9%
Compaq TaskSmart 2500	52.7%
Lucent IPWorX WebCache 100	51.1%
Network Appliance NetCache	50.3%
Microbits Intelli-App Pizza Box	44.4%
IBM 5600	42.1%
IBM 5000	40.8%
Quantex WebXL-4000	40.3%

Producto	Tasas de requerimientos de documentos
Compaq TaskSmart 900	38.7%
IBM 3500M10	37.1%
Dell PowerEdge 130B	36.0%
InfoLibria DynaCache X1 cluster	34.4%
InfoLibria DynaCache 30i	32.3%
Stratacache Flyer 100	32.3%

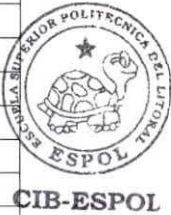
Tabla 4-13. Comparativa Proxy Tasa de Requerimiento

4.6.5.3. MEDIDA DEL LATENCIA DEL CACHE

La latencia del cache muestra el tiempo máximo que un objeto alcanza antes de que sea borrado del cache. El puntaje más alto demuestra un mejor rendimiento porque un recurso que puede almacenar un objeto por mucho tiempo tiene mejores oportunidades de producir un requerimiento.

Producto	Latencia del Cache (Horas)
Swell Tsunami CPX-1000	19.1
Squid	15.6
Cisco Cache Engine 590	11.3
Cisco Cache Engine 7300	8.6
Lucent IPWorX WebCache 150a	8.4
Pionex PCA-1000	7.6
iMimic DataReactor 5000	7.2
Compaq TaskSmart 2500	6.5
Network Appliance NetCache	4.7
Lucent IPWorX WebCache 100	4.3
InfoLibria DynaCache X1 cluster	3.6
InfoLibria DynaCache 30I	3.2
IBM 5000	2.4
Microbits Intelli-App Pizza Box	2.4
IBM 5600	2.3
Quantex WebXL-4000	2.3
Compaq TaskSmart 900	1.7
Dell PowerEdge 130B	1.3
IBM 3500M10	1.3
Stratacache Flyer 100	1.2

Tabla 4-14. Comparativa Proxy Latencia del Cache



4.6.5.4. MEDIDA DE TIEMPO DE RESPUESTA

LA cantidad mas baja tiene el mejor rendimiento.

Producto	Tiempo de Respuesta (Segundos)
iMimic DataReactor 5000	1.35
Squid	1.41
Network Appliance NetCache	1.44
Swell Tsunami CPX-1000	1.44
Compaq TaskSmart 2500	1.45
Cisco Cache Engine 7300	1.48
Cisco Cache Engine 590	1.50
Pionex PCA-1000	1.51
Lucent IPWorX WebCache 150a	1.58
IBM 5600	1.65
Microbits Intelli-App Pizza Box	1.69
Quantex WebXL-4000	1.70
Lucent IPWorX WebCache 100	1.71
Compaq TaskSmart 900	1.72
IBM 5000	1.75
IBM 3500M10	1.78
Dell PowerEdge 130B	1.81
Stratacache Flyer 100	1.89
InfoLibria DynaCache X1 cluster	2.06
InfoLibria DynaCache 30i	3.08



Tabla 4-15. Comparativa Proxy Tiempo de Respuesta

4.6.5.5. MEDIDA DE TIEMPO DE INACTIVIDAD

Mide cuanto tiempo le toma al cache recuperarse de una condición inesperada como la falta de energía. Cuando un cache puede enviar sus primeros errores, los usuarios finales son capaces de acceder al web. LA cantidad mas baja tiene el mejor rendimiento.

Producto	Tiempo de Inactividad (minutos)
InfoLibria DynaCache 30i	0.1
InfoLibria DynaCache X1 cluster	0.7
Network Appliance NetCache	1.2
Microbits Intelli-App Pizza Box	1.6
Lucent IPWorX WebCache 100	1.8
Lucent IPWorX WebCache 150a	1.8
Pionex PCA-1000	2.2
Squid	2.4
Dell PowerEdge 130B	2.5
iMimic DataReactor 5000	2.9
IBM 3500M10	3.0
Stratacache Flyer 100	4.0
Cisco Cache Engine 7300	4.2
Quantex WebXL-4000	4.2
IBM 5600	4.8
IBM 5000	5.1
Cisco Cache Engine 590	6.9
Compaq TaskSmart 900	7.8
Compaq TaskSmart 2500	9.2
Swell Tsunami CPX-1000	n/a



Tabla 4-16. Comparativas de Proxies Tiempo Inactividad

4.6.6. RAZONES PARA UTILIZAR EL SQUID

De acuerdo con análisis comparativo mostrado en las tablas se decidió utilizar como web cache al SQUID por las siguientes razones:

- ♦ Es usado por la mayoría de empresas e ISPs.
- ♦ Esta entre los tres web cache mejores ya que posee los mejores valores en: tiempo de respuesta, una prolongada latencia del cache, alta tasa de requerimiento sin acceder al servidor web remoto.
- ♦ Tiene un aceptable tiempo de inactividad al momento de una contingencia.
- ♦ Para un rendimiento óptimo necesita menos recursos de hardware que los demás.

- ♦ Tiene muchas características adicionales que sirven para optimizar el servicio tal como: Restricciones de acceso por medio ACLs, Proxy inverso para mejorar los tiempos de respuesta, etc.
- ♦ Es gratuito.



4.6.7. REVISION DE SQUID

4.6.7.1. INTRODUCCIÓN

Squid es el software para servidor Proxy más popular y extendido entre los sistemas operativos basados sobre UNIX®. Es muy confiable, robusto y versátil. Al ser software libre, además de estar disponible el código fuente, está libre del pago de costosas licencias por uso o con restricción a un uso con determinado número de usuarios.

Entre otras cosas, Squid puede hacer Proxy y cache con los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, cache transparente, WWCP, aceleración HTTP, cache de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario.

Nota

Squid **no puede funcionar como proxy** para servicios como SMTP, POP3, TELNET, SSH, etc. Si se requiere hacer proxy para cualquier cosa distinta a HTTP, HTTPS, FTP, GOPHER y WAIS se requerirá o bien implementar enmascaramiento de IP a través de un NAT (*Network Address Translation*) o bien hacer uso de un servidor SOCKS como Dante.

4.6.7.2. SOFTWARE REQUERIDO

Para poder llevar la cabo los procedimientos descritos en este manual y documentos relacionados, usted necesitará tener instalado al menos lo siguiente:

- ♦ squid-2.5.STABLE1.
- ♦ httpd-2.0.x (Apache).
- ♦ Todos los parches de seguridad disponibles para la versión de sistema operativo que esté utilizando.

Tómese en consideración que, de ser posible, se debe utilizar siempre las versiones estables más recientes de todo el software que vaya a instalar al realizar los procedimientos descritos en este manual, a fin de contar con los parches de seguridad necesarios. Ninguna versión de Squid anterior a la 2.5.STABLE1 se considera como apropiada debido a fallas de seguridad de gran importancia, y ningún administrador competente utilizaría una versión inferior a la 2.5.STABLE1. Por favor visite el Sitio de Red de su distribución predilecta para estar al tanto de cualquier aviso de actualizaciones de seguridad.

Para Red Hat™ Linux 9 hay paquetería de actualización en los siguientes enlaces: <ftp://updates.redhat.com/9/en/os/i386/>, si posee alguna distribución basada sobre Red Hat™ Linux 9.

4.6.7.3. INSTALACIÓN DEL SOFTWARE NECESARIO

Regularmente Squid no se instala de manera predeterminada a menos que especifique o contrario durante la instalación del sistema operativo, sin embargo



viene incluido en casi todas las distribuciones actuales. El procedimiento de instalación es exactamente el mismo que con cualquier otro software:

```
mount /mnt/cdrom/  
rpm -Uvh /mnt/cdrom/*/RPMS/squid-*.i386.rpm  
eject
```

Si utiliza Fedora™ Core, ejecute lo siguiente y se instalará todo lo necesario junto con sus dependencias:

```
yum install squid httpd
```

IPtables se utilizará para generar las reglas necesarias para el guión de Enmascaramiento de IP. Se instala por defecto en todas las distribuciones actuales que utilicen kernel-2.4.

Es importante tener actualizado el kernel por diversas cuestiones de seguridad. No es recomendable utilizar versiones del kernel anteriores a la 2.4.20. En el manual "Cómo actualizar el Kernel a partir de paquetes RPM®" se describe a detalle lo necesario.

4.6.7.4. ANTES DE CONTINUAR

Tenga en cuenta que este manual ha sido comprobado varias veces y ha funcionado en todos los casos y si algo no funciona solo significa que usted no lo leyó a detalle y no siguió correctamente las indicaciones.

Evite dejar espacios vacíos en lugares indebidos. El siguiente es un ejemplo de como no debe des-comentarse un parámetro.

Mal

Opción incorrectamente descimentada

http_port 3128

El siguiente es un ejemplo de como **si** debe descomentarse un parámetro.

Bien

Opción incorrectamente descimentada

http_port 3128

4.6.7.5. CONFIGURACIÓN BÁSICA

Squid utiliza el fichero de configuración localizado en /etc/squid/squid.conf, y podrá trabajar sobre este utilizando su editor de texto preferido. Existen un gran número de parámetros, de los cuales recomendamos configurar los siguientes:

- ♦ http_port
- ♦ cache_mem
- ♦ ftp_user
- ♦ cache_dir
- ♦ Al menos una Lista de Control de Acceso
- ♦ Al menos una Regla de Control de Acceso
- ♦ httpd_accel_host
- ♦ httpd_accel_port
- ♦ httpd_accel_with_proxy



CIB-ESPOL

PARÁMETRO HTTP_PORT: ¿QUE PUERTO UTILIZAR PARA SQUID?

Squid por defecto utilizará el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto o bien que lo haga en varios puertos a la vez.

En el caso de un Proxy Transparente, regularmente se utilizará el puerto 80 y se valdrá del re-direccionamiento de peticiones de modo tal que no habrá necesidad alguna de modificar la configuración de los navegadores de Red para utilizar el servidor Proxy. bastará con utilizar como puerta de enlace al servidor. Es importante recordar que los servidores HTTP, como Apache, también utilizan dicho puerto, por lo que será necesario reconfigurar el servidor Web para utilizar otro puerto disponible, o bien desinstalar o deshabilitar el servidor Web.

Hoy en día ya no es del todo práctico el utilizar un Proxy Transparente, a menos que se trate de un servicio de Café Internet u oficina pequeña, siendo que uno de los principales problemas con los que lidian los administradores es el mal uso y/o abuso del acceso a Internet por parte del personal. Es por esto que puede resultar más conveniente configurar un servidor Proxy con restricciones por contraseña, lo cual no puede hacerse con un Proxy Transparente, debido a que se requiere un diálogo de nombre de usuario y contraseña.

Regularmente algunos programas utilizados comúnmente por los usuarios suelen traer por defecto el puerto 8080 -servicio de cacheo WWW- para utilizarse al configurar que servidor proxy utilizar. Si queremos aprovechar esto en nuestro favor y ahorrarnos el tener que dar explicaciones innecesarias al usuario,

podemos especificar que Squid escuche peticiones en dicho puerto también. Siendo así localice la sección de definición de http_port, y especifique:

```
#
#       You may specify multiple socket addresses on multiple lines.
#
# Default: http_port 3128
http_port 3128
http_port 8080
```

Si desea incrementar la seguridad, puede vincularse el servicio a una IP que solo se pueda acceder desde la red local. Considerando que el servidor utilizado posee una IP 192.168.1.254, puede hacerse lo siguiente:

```
#
#       You may specify multiple socket addresses on multiple lines.
#
# Default: http_port 3128
http_port 192.168.1.254:3128
http_port 192.168.1.254:8080
```



PARÁMETRO CACHE_MEM

El parámetro cache_mem establece la cantidad ideal de memoria para lo siguiente:

- ♦ Objetos en tránsito.
- ♦ Objetos Hot.
- ♦ Objetos negativamente almacenados en el caché.

Los datos de estos objetos se almacenan en bloques de 4Kb. El parámetro cache_mem especifica un límite máximo en el tamaño total de bloques acomodados, donde los objetos en tránsito tienen mayor prioridad. Sin embargo

los objetos Hot y aquellos negativamente almacenados en el caché podrán utilizar la memoria no utilizada hasta que esta sea requerida. De ser necesario, si un objeto en tránsito es mayor a la cantidad de memoria especificada, Squid excederá lo que sea necesario para satisfacer la petición.

Por defecto se establecen 8 MB. Puede especificarse una cantidad mayor si así se considera necesario, dependiendo esto de los hábitos de los usuarios o necesidades establecidas por el administrador.

Si se posee un servidor con al menos 128 MB de RAM, establezca 16 MB como valor para este parámetro:

cache_mem 16 MB

PARÁMETRO CACHE_DIR: ¿CUÁNTO DESEA ALMACENAR DE INTERNET EN EL DISCO DURO?

Este parámetro se utiliza para establecer que tamaño se desea que tenga el cache en el disco duro para Squid. Para entender esto un poco mejor, responda a esta pregunta: ¿Cuanto desea almacenar de Internet en el disco duro? Por defecto Squid utilizará un cache de 100 MB, de modo tal que encontrará la siguiente línea:

cache_dir ufs /var/spool/squid **100** 16 256

Se puede incrementar el tamaño del cache hasta donde lo desee el administrador. Mientras más grande el cache, más objetos de almacenarán en éste y por lo tanto se utilizará menos el ancho de banda. La siguiente línea establece un cache de 700 MB:

```
cache_dir ufs /var/spool/squid 700 16 256
```

Los números 16 y 256 significan que el directorio del cache contendrá 16 subdirectorios con 256 niveles cada uno. No modifique estos números, no hay necesidad de hacerlo.

Es muy importante considerar que si se especifica un determinado tamaño de cache y este excede al espacio real disponible en el disco duro, Squid se bloqueará inevitablemente. Sea cauteloso con el tamaño de cache especificado.

PARÁMETRO FTP_USER

Al acceder a un servidor FTP de manera anónima, por defecto Squid enviará como contraseña Squid@. Si se desea que el acceso anónimo a los servidores FTP sea más informativo, o bien si se desea acceder a servidores FTP que validan la autenticidad de la dirección de correo especificada como contraseña, puede especificarse la dirección de correo electrónico que uno considere pertinente.

CONTROLES DE ACCESO

Es necesario establecer Listas de Control de Acceso que definan una red o bien ciertas máquinas en particular. A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Squid. Procedamos a entender como definir unas y otras.



LISTAS DE CONTROL DE ACCESO

Regularmente una lista de control de acceso se establece siguiendo la siguiente sintaxis:

```
acl [nombre de la lista] src [lo que compone a la lista]
```

Si uno desea establecer una lista de control de acceso que defina sin mayor trabajo adicional a toda la red local definiendo la IP que corresponde a la red y la máscara de la sub-red.

Por ejemplo, si se tienen una red donde las máquinas tienen direcciones IP 192.168.1.n con máscara de sub-red 255.255.255.0, podemos utilizar lo siguiente:

```
acl miredlocal src 192.168.1.0/255.255.255.0
```

También puede definirse una Lista de Control de Acceso invocando un fichero localizado en cualquier parte del disco duro, y en el cual se en cuenta una lista de direcciones IP. Ejemplo:

```
acl permitidos src "/etc/squid/permitidos"
```

El fichero /etc/squid/permitidos contendría algo como siguiente:

```
192.168.1.1  
192.168.1.2
```

192.168.1.3
 192.168.1.15
 192.168.1.16
 192.168.1.20
 192.168.1.40

Lo anterior estaría definiendo que la Lista de Control de Acceso denominada permitidos estaría compuesta por las direcciones IP incluidas en el fichero /etc/squid/permitidos.

REGLAS DE CONTROL DE ACCESO

Estas definen si se permite o no el acceso a Squid. Se aplican a las Listas de Control de Acceso. Deben colocarse en la sección de reglas de control de acceso definidas por el administrador, es decir, a partir de donde se localiza la siguiente leyenda:

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
```

LA SINTAXIS BÁSICA ES LA SIGUIENTE:

http_access [deny o allow] [lista de control de acceso]



CIB-ESPOL

En el siguiente ejemplo consideramos una regla que establece acceso permitido a Squid a la Lista de Control de Acceso denominada permitidos:

http_access allow permitidos

También pueden definirse reglas valiéndose de la expresión !, la cual significa excepción. Pueden definirse, por ejemplo, dos listas de control de acceso, una denominada lista1 y otra denominada lista2, en la misma regla de control de

acceso, en donde se asigna una expresión a una de estas. La siguiente establece que se permite el acceso a Squid a lo que comprenda lista1 excepto aquello que comprenda lista2:

```
http_access allow lista1 !lista2
```

Este tipo de reglas son útiles cuando se tiene un gran grupo de IP dentro de un rango de red al que se debe permitir acceso, y otro grupo dentro de la misma red al que se debe denegar el acceso.

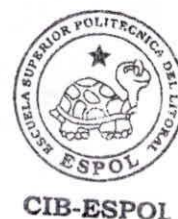
APLICANDO LISTAS Y REGLAS DE CONTROL DE ACCESO

Una vez comprendido el funcionamiento de la Listas y las Regla de Control de Acceso, procederemos a determinar cuales utilizar para nuestra configuración.

Caso 1

Considerando como ejemplo que se dispone de una red 192.168.1.0/255.255.255.0, si se desea definir toda la red local, utilizaremos la siguiente línea en la sección de Listas de Control de Acceso:

```
acl totalared src 192.168.1.0/255.255.255.0
```



CIB-ESPOL

Habiendo hecho lo anterior, la sección de listas de control de acceso debe quedar más o menos del siguiente modo:

LISTAS DE CONTROL DE ACCESO: DEFINICIÓN DE UNA RED LOCAL

COMPLETA

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl todalared src 192.168.1.0/255.255.255.0
```



CIB-ESPOL

A CONTINUACIÓN PROCEDEMOS A APLICAR LA REGLA DE CONTROL DE ACCESO:

```
http_access allow todalared
```

Habiendo hecho lo anterior, la zona de reglas de control de acceso debería quedar más o menos de este modo:

REGLAS DE CONTROL DE ACCESO: ACCESO A UNA LISTA DE CONTROL DE ACCESO

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow todalared
http_access deny all
```

La regla `http_access allow todalared` permite el acceso a Squid a la Lista de Control de Acceso denominada `todalared`, la cual está conformada por `192.168.1.0/255.255.255.0`. Esto significa que cualquier máquina desde `192.168.1.1` hasta `192.168.1.254` podrá acceder a Squid.

Caso 2

Si solo se desea permitir el acceso a Squid a ciertas direcciones IP de la red local, deberemos crear un fichero que contenga dicha lista. Genere el fichero `/etc/squid/lista`, dentro del cual se incluirán solo aquellas direcciones IP que desea confirmen la Lista de Control de acceso. Ejemplo:

```
192.168.1.1
192.168.1.2
192.168.1.3
192.168.1.15
192.168.1.16
192.168.1.20
192.168.1.40
```

DENOMINAREMOS A ESTA LISTA DE CONTROL DE ACCESO COMO REDLOCAL:

```
acl redlocal src "/etc/squid/lista"
```

Habiendo hecho lo anterior, la sección de listas de control de acceso debe quedar más o menos del siguiente modo:

LISTAS DE CONTROL DE ACCESO: DEFINICIÓN DE UNA RED LOCAL COMPLETA

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl redlocal src "/etc/squid/lista"
```

A CONTINUACIÓN PROCEDEMOS A APLICAR LA REGLA DE CONTROL DE ACCESO:

http_access allow redlocal



CIB-ESPOL

Habiendo hecho lo anterior, la zona de reglas de control de acceso debería quedar más o menos de este modo:

REGLAS DE CONTROL DE ACCESO: ACCESO A UNA LISTA DE CONTROL DE ACCESO

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow redlocal
http_access deny all
```

La regla http_access allow redlocal permite el acceso a Squid a la Lista de Control de Acceso denominada redlocal, la cual está conformada por las direcciones IP especificadas en el fichero /etc/squid/lista. esto significa que cualquier máquina no incluida en /etc/squid/lista no tendrá acceso a Squid.

PARÁMETRO CACHE_MGR

Por defecto, si algo ocurre con el Cache, como por ejemplo que muera el procesos, se enviará un mensaje de aviso a la cuenta webmaster del servidor. Puede especificarse una distinta si acaso se considera conveniente.

PARÁMETRO CACHE_PEER: CACHES PADRES Y HERMANOS

El parámetro `cache_peer` se utiliza para especificar otros proxy-cache en una jerarquía como padres o como hermanos. es decir, definir si hay un proxy adelante o en paralelo. La sintaxis básica es la siguiente:

`cache_peer servidor tipo http_port icp_port opciones`



Ejemplo: Si su cache va a estar trabajando detrás de otro servidor cache, es decir un cache padre, y considerando que el cache padre tiene una IP 192.168.1.1, escuchando peticiones HTTP en el puerto 8080 y peticiones ICP en puerto 3130 (puerto utilizado por defecto por Squid) ,especificando que no se almacenen en cache los objetos que ya están presentes en el cache del proxy padre, utilice la siguiente línea:

`cache_peer 192.168.1.1 parent 8080 3130 proxy-only`

Cuando se trabaja en redes muy grandes donde existen varios servidores proxy haciendo cache de contenido de Internet, es una buena idea hacer trabajar todos los cache entre sí. Configurar caches vecinos como sibling (hermanos) tiene como beneficio el que se consultarán estos caches localizados en la red local antes de acceder hacia Internet y consumir ancho de banda para acceder hacia un objeto que ya podría estar presente en otro cache vecino.

Ejemplo: Si su cache va a estar trabajando en paralelo junto con otros caches, es decir caches hermanos, y considerando los caches tienen IP 10.1.0.1, 10.2.0.1 y 10.3.0.1, todos escuchando peticiones HTTP en el puerto 8080 y peticiones ICP

en puerto 3130, especificando que no se almacenen en cache los objetos que ya están presentes en los caches hermanos, utilice las siguientes líneas:

```
cache_peer 10.1.0.1 sibling 8080 3130 proxy-only
cache_peer 10.2.0.1 sibling 8080 3130 proxy-only
cache_peer 10.3.0.1 sibling 8080 3130 proxy-only
```

Pueden hacerse combinaciones que de manera tal que se podrían tener caches padres y hermanos trabajando en conjunto en una red local. Ejemplo:

```
cache_peer 10.0.0.1 parent 8080 3130 proxy-only
cache_peer 10.1.0.1 sibling 8080 3130 proxy-only
cache_peer 10.2.0.1 sibling 8080 3130 proxy-only
cache_peer 10.3.0.1 sibling 8080 3130 proxy-only
```

CACHE CON ACELERACIÓN

Cuando un usuario hace petición hacia un objeto en Internet, este es almacenado en el cache de Squid. Si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificación alguna desde que lo accedió el usuario anterior, Squid mostrará el que ya se encuentra en el cache en lugar de volver a descargarlo desde Internet.

Esta función permite navegar rápidamente cuando los objetos ya están en el cache de Squid y además optimiza enormemente la utilización del ancho de banda.

En la sección HTTPD-ACCELERATOR OPTIONS deben habilitarse los siguientes parámetros:

PROXY ACELERADO: OPCIONES PARA PROXY CONVENCIONAL

```
httpd_accel_host virtual
httpd_accel_port 0
httpd_accel_with_proxy on
```

Si se trata de un Proxy transparente deben utilizarse con las siguientes opciones, considerando que se hará uso del cache de un servidor web (Apache) como auxiliar:

PROXY ACELERADO: OPCIONES PARA PROXY TRANSPARENTE

```
# Debe especificarse la IP de cualquier servidor Web en la red local
# o bien el valor virtual.
httpd_accel_host 192.168.1.254
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```



CIB-ESPOL

NOTA ACERCA DE INTERNET EXPLORER 5.5 Y VERSIONES ANTERIORES

Si va a utilizar Internet Explorer 5.5 y versiones anteriores con un proxy transparente, es importante recuerde que dichas versiones tiene un pésimo soporte con los proxies transparentes imposibilitando por completo la capacidad de refrescar contenido. Lo más conveniente es actualizar hacia Internet Explorer 6.x o definitivamente optar por otras alternativas como Mozilla, que consiste en una suite completa de aplicaciones para Internet, o bien Mozilla Firebird, que consiste en un navegador muy ligero y que cumple con los estándares, de las cuales encontrará versión para Windows. Si se utiliza el parámetro `ie_refresh` con valor `on` puede hacer que se verifique en los servidores de origen para nuevo

contenido para todas las peticiones IMS-REFRESH provenientes de Internet Explorer 5.5 y versiones anteriores.

PROXY ACELERADO: OPCIONES PARA PROXY TRANSPARENTE PARA REDES CON INTERNET EXPLORER 5.5 Y VERSIONES ANTERIORES.

Debe especificarse la IP de cualquier servidor Web en la red local
o bien virtual

```
httpd_accel_host 192.168.1.254
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
ie_refresh on
```

La configuración de Squid como proxy transparente solo requiere complementarse utilizando una regla de *Iptables* que se encargará de redireccionar peticiones haciéndolas pasar por el puerto 8080.



CIB-ESPOL

PROXY ACELERADO: REGLA DE IPTABLES

Considerando que la red local accede a través de eth0 y que Squid
escucha peticiones en puerto 8080, se utiliza la siguiente línea:

```
/sbin/Iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080.
```

Por defecto el parámetro `httpd_accel_with_proxy` viene con el valor off, es importante no olvidar cambiar este valor por on.

Estableciendo el idioma por defecto

Squid incluye traducción a distintos idiomas de las distintas páginas de error e informativas que son desplegadas en un momento dado. Dichas traducciones se pueden encontrar en `/usr/lib/squid/errors/`. Para poder hacer uso de las páginas de error traducidas al español, es necesario cambiar un enlace simbólico

localizado en /etc/squid/errors para que apunte hacia /usr/lib/squid/errors/Spanish en lugar de hacerlo hacia /usr/lib/squid/errors/English.

ELIMINE PRIMERO EL ENLACE SIMBÓLICO ACTUAL:

```
rm -f /etc/squid/errors
```

Coloque un nuevo enlace simbólico apuntando hacia el directorio con los ficheros correspondientes a los errores traducidos al español.

Red Hat™ Linux 9 y Fedora™ Core 1

```
ln -s /usr/share/squid/errors/Spanish /etc/squid/errors
```

INICIANDO, REINICIANDO Y AÑADIENDO EL SERVICIO AL ARRANQUE DEL SISTEMA

Una vez terminada la configuración, ejecute el siguiente comando para iniciar por primera vez Squid:

```
service squid Start
```

Si necesita reiniciar para probar cambios hechos en la configuración, ejecute lo siguiente:

```
service squid restart
```

Si desea que Squid inicie de manera automática la próxima vez que inicie el sistema, ejecute lo siguiente:

```
/sbin/chkconfig squid on
```


LO ANTERIOR HABILITARÁ A SQUID EN LOS NIVELES DE CORRIDA 3, 4 Y 5.

Nota para los novatos: Usted NO tiene porque editar cosa alguna en /etc/rc.d/rc.local o /etc/inittab para que Squid -así como cualquier otro servicio- inicie en el arranque del sistema. Mientras usted sea novato, por favor, olvide que existen esos ficheros y exclame una fuerte amenaza y aléjese de quien le indique que desde ahí debe arrancar servicios.



CIB-ESPOL

DEPURACIÓN DE ERRORES

Cualquier error al inicio de squid solo significa que hubo errores de sintaxis, errores de dedo o bien se están citando incorrectamente las rutas hacia los ficheros de las Listas de Control de Acceso.

Puede realizar diagnóstico de problemas indicándole a Squid que vuelva a leer configuración, lo cual devolverá los errores que existan en /etc/squid/squid.conf.

`service squid reload`

También puede iniciar Squid directamente desde la línea de comando especificando el modo de depuración:

`squid -d 5`

AJUSTES PARA EL FIREWALL Ó GUIÓN DE ENMASCARAMIENTO DE IP

A continuación comentaremos algunos ajustes que pueden añadirse o editarse en el guión de el firewall, como el generado por herramientas como Firestarter, o bien un simple guión de Enmascaramiento de IP.

Sugerimos utilizar Firestarter debido a que permite configurar tanto el enmascaramiento de IP como el firewall y la importancia que tiene la presencia de éste último en un servidor que sirve como puerta de enlace para la red local.

USE IPTABLES EN LUGAR DE IPCHAINS

Desde el kernel 2.4, GNU/Linux utiliza Netfilter, el cual se configura a través de IPtables. La sintaxis cambia con respecto a IPchains, y a fin de permitir a los administradores darse tiempo de adaptarse, distribuciones como Red Hat™ incluyeron soporte para ipchains a manera de aplicación de legado.

Pudiendo utilizarse IPtables no tiene sentido mantener instalado ipchains, que aún es utilizado por defecto en Red Hat™ Linux 7.1 y 7.2. Se recomienda desinstalar ipchains y los paquetes que dependan de este.

Es importante utilizar la más reciente versión de IPtables para la distribución utilizada. **Ninguna versión de IPtables anterior a la 1.2.4 se considera como apropiada** debido a fallas de seguridad de gran importancia, y ningún administrador *competente* utilizaría una versión inferior a la 1.2.4. Por favor visite el Sitio de Red de su distribución predilecta para estar al tanto de cualquier aviso de actualizaciones de seguridad. Ejemplo: para Red Hat™ Linux 7.2, 7.3, 8.0 y 9 hay paquetería de actualización en los siguientes enlaces:

<ftp://updates.redhat.com/7.2/en/os/i386/>, si posee alguna distribución basada sobre Red Hat™ Linux 7.2

<ftp://updates.redhat.com/7.3/en/os/i386/>, si posee alguna distribución basada sobre Red Hat™ Linux 7.3

`ftp://updates.redhat.com/8.0/en/os/i386/`, si posee alguna distribución basada sobre Red Hat™ Linux 8.0

`ftp://updates.redhat.com/9/en/os/i386/`, si posee alguna distribución basada sobre Red Hat™ Linux 9

RE-DIRECCIONAMIENTO DE PETICIONES

En un momento dado se requerirá tener salida transparente hacia Internet para ciertos servicios, pero al mismo tiempo se necesitará re-direccionar peticiones hacia servicio Web, Web SSL, ftp, gopher o WAIS hacia el puerto donde escucha peticiones Squid (8080), de modo que no haya salida alguna hacia alguno de estos protocolos sin que ésta pase antes por Squid.

El re-direccionamiento lo hacemos a través de IPtables. Considerando para este ejemplo que la red local se accede a través de una interfaz eht0, el siguiente esquema ejemplifica un re-direccionamiento:

```
/sbin/IPtables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
```

Lo anterior hace que cualquier petición hacia el puerto 80 (servicio HTTP) hecha desde la red local hacia el exterior, se re-direccionará hacia el puerto 8080 del servidor.



GUIÓN EJEMPLO DE ENMASCARAMIENTO DE IP CON IPTABLES

El guión que mostramos en la tabla a continuación considera que se dispone de dos interfaces: eth0 y eth1. Para nuestro ejemplo la red local se accede por la

interfaz eth0 y la salida hacia Internet se hace por la interfaz eth1. Utilice Firestarter para configurar el enmascaramiento y muro de Firewall siempre que sea posible. Este guión NO es sustituto para un guión de muro de Firewall.

GUIÓN BÁSICO DE ENMASCARAMIENTO DE IP.

```
#!/bin/sh
```

```
# cargamos los módulos del kernel necesarios:
```

```
/sbin/modprobe ip_conntrack
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_conntrack_irc
/sbin/modprobe ipt_REJECT
/sbin/modprobe ipt_REDIRECT
/sbin/modprobe ipt_TOS
/sbin/modprobe ipt_MASQUERADE
/sbin/modprobe ipt_LOG
/sbin/modprobe iptable_mangle
/sbin/modprobe iptable_nat
/sbin/modprobe ip_nat_ftp
/sbin/modprobe ip_nat_irc
```

```
# Habilitamos el reenvío de direcciones IP
if [ -e /proc/sys/net/ipv4/ip_forward ]; then
    echo 0 > /proc/sys/net/ipv4/ip_forward
fi
```

```
# Estableciendo política de reenvío del enmascaramiento
```

```
/sbin/Iptables -t filter -P FORWARD DROP
```

```
# Reenvío de tráfico intento-externo y externo-interno
```

```
/sbin/Iptables -t filter -A FORWARD -d 0/0 -s 192.168.1.0/255.255.255.0 -o eth0
-j ACCEPT
```

```
/sbin/Iptables -t filter -A FORWARD -d 192.168.1.0/255.255.255.0 -j ACCEPT
```

```
# Enmascaramiento de todo el tráfico saliente
```

```
# NOTA: recordemos que la salida hacia Internet es por
```

```
# la interfaz eth0
```


CÓMO CONFIGURAR SQUID: RESTRICCIÓN DE ACCESO A SITIO DE RED

INTRODUCCIÓN

Denegar el acceso a ciertos Sitios de Red permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple, y consiste en denegar el acceso a nombres de dominio o direcciones Web que contengan patrones en común.

Este manual considera que usted ya ha leído previamente, a detalle y en su totalidad el manual "Como configurar Squid: Servidor Proxy" y que ha configurado exitosamente Squid como servidor proxy.

SOFTWARE REQUERIDO

Para poder llevar la cabo los procedimientos descritos en este manual y documentos relacionados, usted necesitará tener instalado al menos squid-2.5STABLE1.



DEFINIENDO PATRONES COMUNES

Lo primero será generar una lista la cual contendrá direcciones Web y palabras usualmente utilizadas en nombres de ciertos dominios. Ejemplos:

www.sitioporno.com

www.otrositioporno.com

sitioindeseable.com

otrositioindeseable.com

napster

sex
 porn
 mp3
 xxx
 adult
 warez
 celebri

Esta lista, la cual deberá ser completada con todas las palabras (muchas de estas son palabras obscenas en distintos idiomas) y direcciones Web que el administrador considere pertinentes, la guardaremos como /etc/squid/sitiosdenegados.



CIB-ESPOL

PARÁMETROS EN /ETC/SQUID/SQUID.CONF

Debemos definir una Lista de Control de Acceso que a su vez defina al fichero /etc/squid/sitiosdenegados. Esta lista la denominaremos como "sitiosdenegados". De modo tal, la línea correspondiente quedaría del siguiente modo:

```
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
```

Habiendo hecho lo anterior, deberemos tener en la sección de Listas de Control de Acceso algo como lo siguiente:

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl redlocal src 192.168.1.0/255.255.255.0
acl password proxy_auth REQUIRED
```

```
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
```

A continuación especificaremos modificaremos una Regla de Control de Acceso existente agregando con un símbolo de ! que se denegará el acceso a la Lista de Control de Acceso denominada sitiosdenegados:

```
http_access allow redlocal !sitiosdenegados
```

La regla anterior permite el acceso a la Lista de Control de Acceso denominada redlocal, pero le niega el acceso a todo lo que coincida con lo especificado en la Lista de Control de Acceso denominada sitiosdenegados.

Ejemplo aplicado a una Regla de Control de Acceso combinando el método de autenticación explicado en el documento Cómo configurar Squid: Acceso por Autenticación:

REGLAS DE CONTROL DE ACCESO: DENEGACIÓN DE SITIOS

```
#
# INSERT YOUR OWN RULE(S) HERE TO allow ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow redlocal password !sitiosdenegados
http_access deny all
```



CIB-ESPOL

PERMITIENDO ACCESO A SITIOS INOCENTES INCIDENTALMENTE BLOQUEADOS

Si por ejemplo el incluir una palabra en particular afecta el acceso a un sitio Web, también puede generarse una lista de dominios o palabras que contengan un patrón pero que consideraremos como apropiados.

Como ejemplo: vamos a suponer que dentro de la Lista de Control de Acceso de sitios denegados está la palabra sex. Esta denegaría el acceso a cualquier nombre de dominio que incluya dicha cadena de caracteres, como extremesex.com. Sin embargo también estaría bloqueando a sitios como sexualidadjoven.cl, el cual no tiene que ver en lo absoluto con pornografía, sino orientación sexual para la juventud. Podemos añadir este nombre de dominio en un ficheros que denominaremos /etc/squid/sitios-inocentes.

Este fichero será definido en una Lista de Control de Acceso del mismo modo en que se hizo anteriormente con el fichero que contiene dominios y palabras denegadas.

```
acl inocentes url_regex "/etc/squid/sitios-inocentes"
```



Para hacer uso de el fichero, solo bastará utilizar la expresión ! en la misma línea utilizada para la Regla de Control de Acceso establecida para denegar el mismo.

```
http_access allow all inocentes
```

La regla anterior especifica que se denegará el acceso a todo lo que comprenda la *Lista de Control de Acceso* denominada *denegados* **excepto** lo que comprenda la *Lista de Control de Acceso* denominada *inocentes*. es decir, se podrá acceder sin dificultad a www.sexualidadjoven.cl manteniendo la restricción para la cadena de caracteres sex.

FINALIZANDO PROCEDIMIENTO

Finalmente, solo bastará reiniciar Squid para que tomen efecto los cambios y podamos hacer pruebas.

service squid restart



CIB-ESPOL

CÓMO CONFIGURAR SQUID: RESTRICCIÓN DE ACCESO A CONTENIDO POR EXTENSIÓN.

INTRODUCCIÓN

Denegar el acceso a ciertos tipos de extensiones de fichero permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple, y consiste en denegar el acceso a ciertos tipos de extensiones que coincidan con lo establecido en una Lista de Control de Acceso.

Este manual considera que usted ya ha leído previamente, a detalle y en su totalidad el manual "Como configurar Squid: Servidor Proxy" y que ha configurado exitosamente Squid como servidor proxy.

SOFTWARE REQUERIDO

Para poder llevar la cabo los procedimientos descritos en este manual y documentos relacionados, usted necesitará tener instalado al menos squid-2.5STABLE1.

DEFINIENDO ELEMENTOS DE LA LISTA DE CONTROL DE ACCESO

Lo primero será generar una lista la cual contendrá direcciones Web y palabras usualmente utilizadas en nombres de ciertos dominios. Ejemplos:

```

\avi$
\mp4$
\mp3$
\mp4$
\mpg$
\mpeg$
\mov$
\ra$
\ram$
\rm$
\rpm$
\vob$
\wma$
\wmv$
\wav$
\doc$
\xls$
\mbd$
\ppt$
\pps$
\ace$
\bat$
\exe$
\lnk$
\pif$
\scr$
\sys$
\zip$
\rar$

```

Esta lista, la cual deberá ser completada con todas las extensiones de fichero que el administrador considere pertinentes, la guardaremos como etc/squid/listaextensiones.

PARÁMETROS EN /ETC/SQUID/SQUID.CONF

Debemos definir una Lista de Control de Acceso que a su vez defina al fichero /etc/squid/listaextensiones. Esta lista la denominaremos como "listaextensiones".

De modo tal, la línea correspondiente quedaría del siguiente modo:

```
acl listaextensiones urlpath_regex "/etc/squid/listaextensiones"
```

Habiendo hecho lo anterior, deberemos tener en la sección de Listas de Control de Acceso algo como lo siguiente:

```
# Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl redlocal src 192.168.1.0/255.255.255.0
acl password proxy_auth REQUIRED
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
acl listaextensiones urlpath_regex "/etc/squid/listaextensiones"
```

A continuación especificaremos modificaremos una Regla de Control de Acceso existente agregando con un símbolo de ! que se denegará el acceso a la Lista de Control de Acceso denominada listaextensiones:

```
http_access allow redlocal !listaextensiones
```

La regla anterior permite el acceso a la Lista de Control de Acceso denominada redlocal, pero le niega el acceso a todo lo que coincida con lo especificado en la Lista de Control de Acceso denominada listaextensiones.

Ejemplo aplicado a una Regla de Control de Acceso combinando el método de autenticación explicado en el documento *Cómo configurar Squid: Acceso por Autenticación* y el de denegación hacia Sitio de Red explicado en el documento *Cómo configurar Squid: Restricción de acceso a Sitio de Red*:

REGLAS DE CONTROL DE ACCESO: DENEGACIÓN DE EXTENSIONES

```
# INSERT YOUR OWN RULE(S) HERE TO allow ACCESS FROM YOUR CLIENTS
http_access allow localhost
http_access allow redlocal password !sitiosdenegados !listaextensiones
http_access deny all
```

FINALIZANDO PROCEDIMIENTO

Finalmente, solo bastará reiniciar Squid para que tomen efecto los cambios y podamos hacer pruebas.

service squid restart



CIB-ESPOL

4.6.8. TABLA COMPARATIVA DE SERVIDORES CORREO DE CÓDIGO ABIERTO.

Características	COURIER-MTA	EXIM	POSTFIX	SENDMAIL	QMAIL
Versión	Courier-0.44.x	Exim Versión 4.2x	Postfix Versión 2.0 Nivel de Parche x	Sendmail 8.12.x	qmail-1.03
Licencia	GPL	GPL	Licencia Publica IBM	?	Especial
Autenticación SMTP	Login/CRAM-MD5	Login/Plain /CRAM-MD5	Sí (usando SASL)	Sí(usando SASL)	parche
SMTP sobre SSL/TLS	Sí	?	?	?	parche
Extensión STARTTLS	Sí	Sí	?	Sí	parche
POP antes SMTP	No	?	Sí	?	Añade y enciende
Soporte para dominios virtuales	Sí	Sí	Sí	Sí	Sí
Backends Soportados	Ldap / MySQL / PostgreSQL	Ldap / MySQL	Ldap / MySQL	Ldap	Parche Ldap / Parche MySQL
Soporte IPv6	Sí	Sí	No (parche)	Sí	parche
Incluye servidor POP.	Sí (soporte SSL, Apop	No	No	No	Sí

Características	COURIER-MTA	EXIM	POSTFIX	SENDMAIL	QMAIL
	No incluido, SASL incluido)				
Incluye servidor IMAP	Sí (SSL incluido)	No	No	No	No
Formato de la Cuenta de correo	Maildir /mbox/Maildir ++	Maildir/mbox/mbox?	Maildir/mbox	mbox	Maildir/mbox
Soporte Quota	Sí	Sí	parche	No	parche / Añade y enciende
Administrador de Listas de correo	courierlm	No	?		ezmlm
Notificación de estado de envío configurable (DSN)	Sí	Sí	No?		No
Utilidades de análisis de Log	No	Sí	Sí	Sí	Sí
Opciones de registro y acceso detallado	No	Sí	Sí	?	Sí
Administración basada en Web	Sí	No	Sí / No	Sí/No	Sí / No

Tabla 4-17. Comparativa de Características Específicas de Servidores de Correo.

Características	COURIER-MTA	EXIM	POSTFIX	SENDMAIL	QMAIL
Seguridad	?	Baja-Medio	Alta	Baja	Alta / muy Alta
Instalación	Medio	Medio	Fácil - Medio	Fácil	Medio-difícil
Configuración	Medio	Fácil-Medio	Fácil	difícil	Fácil
Rendimiento	?	Medio	Alta	Baja	Alta
Madurez/Estado	Baja	Baja	Medio	Alta	Medio

Características	COURIER-MTA	EXIM	POSTFIX	SENDMAIL	QMAIL
Documentación	Baja	Alta	Medio-Alta	Alta	Alta (A veces un poco confusas)
Características	Alta	Medio-Alta	Medio	Alta	Baja (Existen muchos parches disponibles para añadir características)

Tabla 4-18. Comparativa de Características Generales de Servidores de Correo.

4.6.9. RAZONES PARA UTILIZAR QMAIL

De acuerdo a la tabla comparativa en la cual se muestran las posibles soluciones a las necesidades de la empresa se decidió Qmail como servidor de Correo por las siguientes razones:

- ♦ Qmail le da a la empresa un nivel de protección muy Alto, ya que sus funcionalidades las maneja por separado, a través de la instalación de parches según las necesidades.
- ♦ Es de fácil configuración.
- ♦ Tiene un rendimiento alto.
- ♦ Existe mucha documentación de soporte en el internet.
- ♦ Usted puede darle más funcionalidades a través de parches o módulos, los cuales están disponibles en el internet.
- ♦ Su costo de mantenimiento, es relativamente bajo en comparación con otras soluciones.
- ♦ Es gratuito.



CIB-ESPOL

- ♦ Le permite a la empresa aprovechar sus recursos en el momento de la implementación, ya que esta cuenta con un servidor bajo Linux.

4.6.10. REVISION DE QMAIL

4.6.10.1. INTRODUCCIÓN

Qmail es un MTA que proporciona el servicio de correo electrónico en sistemas Linux (y Unix.) Está pensado como un reemplazo más seguro para el clásico Sendmail.



4.6.10.2. ¿POR QUÉ USAR QMAIL?

CIB-ESPOL

En pocas palabras: por seguridad y por comodidad. Sendmail y otros MTAs menos utilizados han sido (y de seguro seguirán siendo) una fuente constante de "bugs" y "vulnerabilidades" explotables por los hackers. Según algunos, esto se debe a que toda la complejidad del sistema de correo recae en un solo programa que necesariamente debe ejecutarse con privilegios de administrador. Qmail intenta paliar este problema mediante un esquema modular en el cual diversas etapas del procesamiento del correo electrónico son llevadas a cabo por distintos procesos que mayormente se ejecutan con un usuario no privilegiado.

Asimismo, la modularidad mencionada permite intercalar con facilidad filtros personalizados a criterio del administrador, cosa poco usual en los MTAs sencillos, y compleja en el MTA sendmail. Un caso muy útil correspondería a la instalación de programas antivirus, a fin de filtrar los mensajes maliciosos que pasan por el MTA.

Además, qmail promueve (aunque no obliga) al uso del mailbox en el "home directory" a fin de evitar los riesgos que presenta el tradicional directorio de mailbox común; también promueve el uso de un formato distinto para este archivo, de modo tal que sea invulnerable a los fallos imprevistos que fácilmente corrompen el mailbox tradicional.

4.6.10.3. REQUISITOS PARA USAR QMAIL

Si Ud. descarga qmail del site oficial, probablemente tendrá que compilarlo. Para esto, su sistema deberá disponer del compilador de lenguaje C. Si Ud. no desea hacer esto, los desarrolladores también mantienen paquetes RPM (binarios.)

Es muy recomendable (casi imprescindible) instalar el programa tcpserver. Si por algún motivo no se desea emplear tcpserver, se puede usar una combinación de inetd con los tcp_wrappers tal como recomienda la documentación que acompaña a qmail.

Otros requisitos evidentes corresponden a una conexión de red, y posiblemente la facultad de configurar el nameserver si se está instalando por primera vez un e-mail server para las estaciones de un dominio. Aquí asumiremos que el usuario está familiarizado con la arquitectura de Internet de correo electrónico y con el DNS.



CIB-ESPOL

4.6.10.4. INSTALACIÓN DE QMAIL

Este proceso es algo extenso, pero en general involucra tareas muy sencillas que difícilmente podrían fallar si se realizan con cuidado.

CREAR EL DIRECTORIO DE QMAIL

Lo primero que debemos hacer es crear el directorio de trabajo para qmail. La sugerencia de los creadores es el directorio `/var/qmail` (hay pocos motivos para cambiarlo.) Así que el administrador ejecutará algo como:

```
# mkdir /var/qmail
```

Si se desea emplear otra ubicación, esta se debe registrar en el archivo `conf-qmail`. En lo que sigue, asumiremos la ruta arriba indicada.

USUARIOS PARA QMAIL

Qmail requiere la creación de diversos usuarios para su correcta ejecución. Estos son: `alias`, `qmaild`, `qmaill`, `qmailp`, `qmailq`, `qmailr`, y `qmails`. Si por algún motivo no se puede emplear estos pseudo-usuarios (por ejemplo, si algún usuario real coincide con los mencionados), entonces se deberá especificar los nuevos valores en el archivo `conf-users`. Igualmente se requiere de la creación de dos grupos (especificados en el archivo `conf-groups`.)

Para crear los usuarios y grupos usar:

```
# groupadd nofiles
# useradd -g nofiles -d /var/qmail/alias alias
# useradd -g nofiles -d /var/qmail qmaild
# useradd -g nofiles -d /var/qmail qmaill
# useradd -g nofiles -d /var/qmail qmailp
# groupadd qmail
# useradd -g qmail -d /var/qmail qmailq
# useradd -g qmail -d /var/qmail qmailr
# useradd -g qmail -d /var/qmail qmails
```

COMPILAR Y CONFIGURAR EL DIRECTORIO DE TRABAJO

En este paso se generan los ejecutables de qmail y se prepara el directorio de trabajo de qmail:

```
# make setup check
```

ESPECIFICAR EL NOMBRE DEL HOST

Luego se deberá especificar el nombre de nuestro host (incluyendo el dominio completo) mediante el comando config-fast del siguiente modo:

```
# ./config-fast marquesa.unima.edu.pe
```

ESTABLECER LOS "ALIAS" DEL SISTEMA

En qmail, el correo para los usuarios especiales postmaster, MAILER-DAEMON y root, es redirigido hacia el pseudo-usuario alias. Esto requiere de la existencia de ciertos archivos en el "home directory" del pseudo-usuario alias:

```
# (cd ~alias; touch .qmail-postmaster \
.qmail-mailer-daemon .qmail-root)
# chmod 644 ~alias/.qmail*
```



CIB-ESPOL

ESPECIFICAR EL AGENTE DE PROCESAMIENTO DE CORREO

El correo dirigido a los usuarios locales debe ser almacenado en algún archivo o directorio (el mailbox.) Esto normalmente NO lo realiza el MTA, sino que lo delega a un programa auxiliar. Sendmail normalmente emplea a procmail para este fin. Usaremos procmail. Para esto tan sólo es necesario efectuar el siguiente comando:

```
# cp /var/qmail/boot/proc /var/qmail/rc
```

Sin embargo, procmail en este caso será ejecutado mediante un usuario no privilegiado, por lo que es menester cambiar los permisos del directorio de los mailbox (que se mantendrá en /var/spool/mail.)

```
# chmod 1777 /var/spool/mail
```

Nótese que qmail recomienda cambiar el mailbox; sin embargo, esto requiere algunos pasos adicionales que no veremos aquí. Lea la documentación respectiva (archivo INSTALL.mbox) para más detalles.

ELIMINAR SENDMAIL

Lo primero que debemos hacer es asegurarnos de que sendmail no está en ejecución, por lo que habremos de buscarlo en la tabla de procesos:

```
# ps ax | grep sendmail
698  ?      S          0:00 sendmail: accepting connections
787  pts/0   S          0:00 grep sendmail
```

La primera línea indica que sendmail está en ejecución, por lo que debemos hacer que termine. Para esto usaremos cualquiera de los siguientes comandos (basta con uno) en orden de preferencia:

```
# service sendmail stop
# /etc/rc.d/init.d/sendmail stop

# kill 698
```



CIB-ESPOL

Luego debemos asegurarnos de que sendmail no se vuelva a ejecutar. La manera más sencilla consiste en desinstalarlo mediante:

```
# rpm -e sendmail
```

Probablemente deberá desinstalar otros paquetes (como fetchmail y mutt.) Para forzar la desinstalación de sendmail:

```
# rpm -e --nodeps sendmail
```

El archivo REMOVE.sendmail muestra otras maneras de trabajar sin necesidad de eliminar el paquete sendmail, aunque lo anterior es más recomendable.

INSTALAR EL "REEMPLAZO" DE SENDMAIL

Diversos programas asumen la existencia de sendmail y lo invocan ciegamente. Por esto, qmail proporciona un "reemplazo" básico para sendmail, a fin de mantener operativas a las aplicaciones mencionadas.

```
# ln -s /var/qmail/bin/sendmail /usr/lib/sendmail  
# ln -s /var/qmail/bin/sendmail /usr/sbin/sendmail
```

INSTALACIÓN DE TCPSERVER

Qmail necesita de un mecanismo que lance el demonio qmail-smtpd cada vez que llega un intento de conexión SMTP del exterior del mailserver. Esto se puede hacer de diversas maneras; sin embargo, los creadores recomiendan el uso del programa tcpserver que está disponible como parte del paquete ucspi-tcp de D.J. Bernstein. Es posible configurar inetd para este fin (ver el archivo FAQ) e incluso xinetd como ilustro en esta misma guía en otra sección.

CONFIGURAR EL INICIO AUTOMÁTICO DE QMAIL

Ahora vamos a configurar el sistema para que siempre se ejecute qmail al reiniciarse el computador.

Ud. deberá averiguar el UID y el GID del usuario "qmaild" y del grupo "nofiles" respectivamente:

```
# id qmaild
uid=1003(qmaild) gid=1002(nofiles) groups=1002(nofiles)
```

El número 1003 es el UID del usuario "qmaild", y el número asociado al grupo "nofiles" es 1002. Es seguro que estos valores serán distintos en su sistema.

Ahora, simplemente añada los siguientes comandos:

```
csh -cf '/var/qmail/rc &'
/usr/sbin/tcpserver -u 1003 -g 1002 0 smtp \
/var/qmail/bin/qmail-smtpd &
```

al final del archivo /etc/rc.d/rc.local.



CIB-ESPOL

ALGO SOBRE LA ARQUITECTURA DE QMAIL

Como ya se ha indicado, qmail está compuesto de diversos subprogramas que realizan tareas específicas y que en conjunto constituyen el sistema de correo electrónico. La figura siguiente proporciona una visión esquemática de estos componentes. A continuación se muestra en la siguiente figura el esquema propuesto.

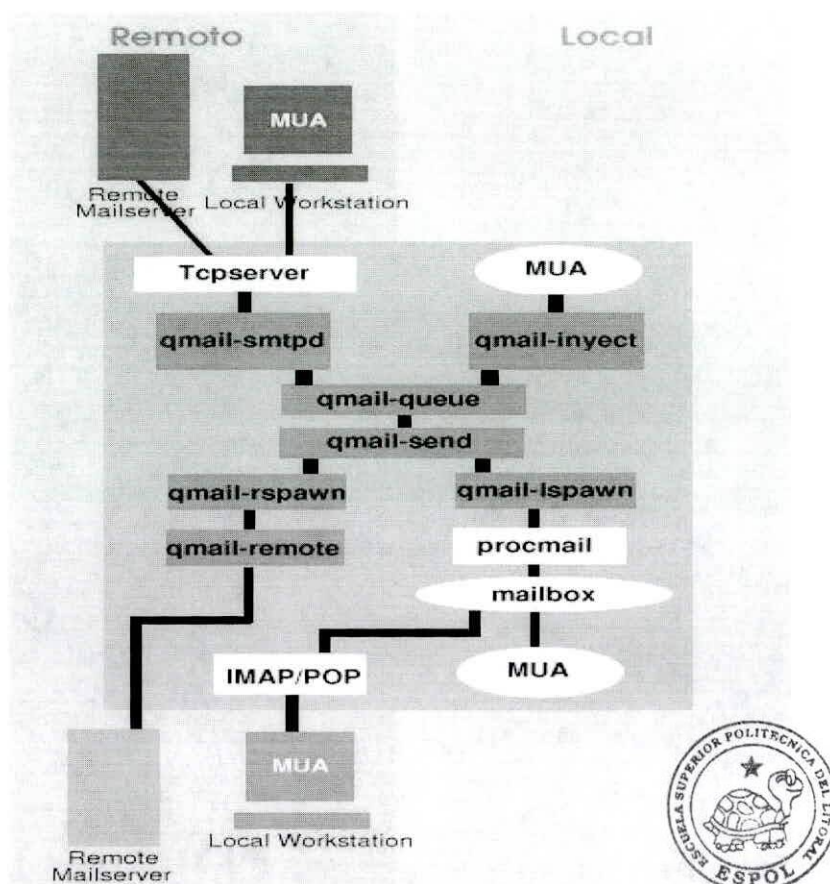


Figura 4-7. Arquitectura de Qmail CIB-ESPOL

Analicemos algunos de los posibles recorridos de un mensaje:

- ♦ **Origen local:** Un usuario Linux operando en el sistema (por ejemplo, con un terminal) remite un mensaje usando un MUA como e-mail. Esto normalmente originará una llamada a qmail-inject el cual llevará el mensaje al programa de encolamiento qmail-queue. Este lo almacenará en la cola de mensajes /var/qmail/queue. Acto seguido, qmail-send intentará remitirlo a su destino (si se puede) mediante los programas qmail-lspawn o qmail-rspawn

- ♦ **Origen remoto exterior:** Un usuario de Internet ha enviado un mensaje hacia nuestra red (hacia un usuario de nuestra organización.) Este mensaje debe provenir de otro servidor de e-mail mediante SMTP. `qmail-smtpd` descubre que el destinatario es de los nuestros, y acepta el mensaje, el cual pasa a la fase de encolamiento.
- ♦ **Origen remoto de la LAN:** Un cliente de nuestra red desea enviar un mensaje. Para esto ha configurado su MUA a fin de remitir hacia el servidor `qmail`. Esta remisión normalmente la efectúa usando SMTP, y por tanto nuevamente `qmail-smtpd` es el encargado de la recepción.
- ♦ **Destino local:** Los mensajes con destino local son guardados en el mailbox por `procmail` (o `qmail-local`) para ser recogidos por los MUAs de los usuarios que trabajan en el servidor. En el caso de que el usuario no esté en el servidor, sino, en una estación de trabajo, entonces su MUA deberá conectarse a un servidor IMAP o POP para obtener los mensajes del mailbox. En cualquier caso, `qmail-lspawn` es el encargado de controlar el agente de delivery local.
- ♦ **Destino remoto:** Los mensajes remotos se remiten con SMTP hacia otros MTA. `qmail-rspawn` es el encargado de los mensajes que se envían remotamente.

No hemos mencionado a `tcpserver` debido a que estrictamente no es parte de `qmail`. Sin embargo, es el encargado de despertar a `qmail-smtpd` de un modo seguro y relativamente inteligente.



4.6.11. TABLA COMPARATIVA DE SNORT VS NIDS DE CAJA

Características	NIDS	Consola de Administración	Detección de ataques	Facilidad de uso	Precio por 100 estaciones de trabajo y 5 servidores	Facilidad de instalación y despliegue	Requerimientos de	de conocimientos (mas estrellas significa menos requeridos).	Detección de intrusos	Comunicación de canal seguro	Facilidad de administración operacional	Frecuencia de actualizaciones del producto.	Compatibilidad SNMP	Capacidad de reporte.	Rendimiento	Adaptación a la infraestructura	Compatibilidad con plataformas Windows	Compatibilidad
Dragon Entera sys (caja)	NIDS	****	****	***	\$6115.89	***	**		***	---	****	****	***	****	***	***	***	***
Cisco Secure IDS (caja)	NIDS	**	***	**	\$7,929.79	**	*		***	---	***	**	***	***	***	***	***	***
Snort (paquete de software)	NIDS	***	***	***	FREE	*	*		****	---	**	***	**	***	****	***	***	***



Características	Snort (paquete de software)	Cisco Secure IDS (caja)	Dragon Entera sys (caja)
con plataformas UNIX			
Respalos y soporte	***	***	****
Registro del monitoreo	***	**	**
Detección de incidentes	***	***	***
Reporte de eventos	***	***	***
Agentes	****	*****	*****
Esta es una carga administrativa. Sin agentes = mas estrellas.			
Resultado	53	61	62

Tabla 4-19. Comparativa de IDS

4.6.12. RAZONES PARA UTILIZAR SNORT

De acuerdo a la tabla comparativa en la que se muestran las posibles soluciones, se ha decidido utilizar como NIDS a Snort por las siguientes razones:

- ♦ Pese a que Snort tiene características un poco inferiores a los NIDS de caja, tomando en cuenta que la empresa es pequeña y necesita un nivel de protección medio y considerando que es una herramienta gratuita. No se justifican los costos exorbitantes de un NIDS de caja el cual cuesta entre \$6000 y \$8000; snort en este caso se convierte en la solución ideal para la empresa ya que le da un nivel de seguridad medio.
- ♦ Tiene un rendimiento muy alto.

- ♦ Tiene un Fuerte soporte para Linux en el internet.
- ♦ Posee Soporte de código abierto Flexible.
- ♦ Hace una Detección de ataque compresiva.
- ♦ Da Soporte a usuarios en listas de correo y a través de interacción por e-mail.
- ♦ Su costo de mantenimiento, es relativamente bajo en comparación con otras soluciones.
- ♦ Le permite a la empresa aprovechar sus recursos en el momento de la implementación, ya que esta cuenta con un servidor bajo Linux.

4.6.13. REVISION DEL SNORT

4.6.13.1. QUÉ ES SNORT?

Snort es lo que se llama un IDS (Sistema de Detección de Intrusos). Su funcionamiento es similar al de un sniffer, poniendo en modo promiscuo la tarjeta de red de la máquina en la que corre. De esta manera, esa tarjeta de red captura todos los paquetes que circulan por un mismo switch, es decir, los capta y lee aun sin ser suyos.

En muchas ocasiones se puede oír hablar de sniffers con intenciones de intrusión en sistemas ajenos, lo cierto es que puede ser un arma de doble filo, y su objetivo principal es el de proteger, no el de atacar.

Un IDS bien configurado y mantenido nos alertará de los intentos de intrusión y ataques varios que nuestra red pueda sufrir, un IDS mal mantenido nos llenará un disco duro de basura y nos colapsará el tráfico de la red.



CIB-ESPOL

Snort es un IDS diseñado para ser comprensivo y preciso en registrar la actividad de red maliciosa exitosamente y notificar a los administradores cuando una vulnerabilidad potencial ocurre. Snort usa la librería estándar libcap y tcpdump como un registro de paquetes final.



CIB-ESPOL

4.6.13.2. CARACTERÍSTICAS PRINCIPALES DE SNORT

- ♦ La característica más apreciada del Snort es su funcionabilidad, es flexible al subsistema de firmas de ataques.
- ♦ Snort tiene una base de datos de ataques constantemente actualizada que puede ser añadida y actualizada a través del internet.
- ♦ Los usuarios pueden crear firmas basándose en un nuevo ataque de red y subiéndolas a la lista de firmas enviadas por e-mail del Snort (ubicadas en <http://www.snort.org/lists.html>), todos los usuarios del Snort pueden beneficiarse de esto.
- ♦ La comunidad ética de compartición ha convertido Snort en uno de los IDSes basados en red más actualizados y robustos disponibles.

Importante

Es importante saber que, según configuremos Snort, este recogerá mayor o menos cantidad de logs. Configurar Snort para que recoja todo tipo de alertas es un suicidio (podemos llegar a captar mas de 100 MB de logs diarios), por tanto debemos descartar muchas de las opciones que vienen por defecto, tratando de minimizar su uso y dedicarlo a aquellos ataques que realmente sean peligrosos para nuestra red.

4.6.13.3. ¿QUÉ ES ACID?

ACID (Analysis Console for Intrusion Databases) es una interfase web desarrollada en lenguaje PHP, que nos muestra los registros guardados por Snort. Snort puede guardarlos en una base de datos o en simples ficheros de

texto (por ejemplo syslog), si queremos usar ACID para visualizar sus efectos, deberemos usar MySQL como almacén para los logs recogidos por Snort.

4.6.13.4. CONFIGURACIÓN DEL SNORT.

REQUERIMIENTOS

La obtención del código fuente de las aplicaciones que se van a configurar se puede llevar a cabo en los websites oficiales, son los siguientes:

Descargue Snort 2.0.2

<http://www.snort.org/dl/snort-2.0.2.tar.gz>



CIB-ESPOL

Descargue MySQL 4.0.15a Source

<http://mysql.secsup.org/Downloads/MySQL-4.0/mysql-4.0.15a.tar.gz>

Descargue Apache 2.0.47

<http://www.apache.org/dist/httpd/httpd-2.0.47.tar.gz>

Descargue PHP 4.3.3

<http://www.php.net/distributions/php-4.3.3.tar.gz>

Descargue ADODB 3.90

<http://phplens.com/lens/dl/adodb390.tgz>

Descargue Acid 0.9.6b23

<http://acidlab.sourceforge.net/acid-0.9.6b23.tar.gz>

Descargue Zlib 1.1.4

<http://flow.dl.sourceforge.net/sourceforge/libpng/zlib-1.1.4.tar.gz>

Descargue JPGraph 1.13

<http://www.aditus.nu/jpgraph/downloads/jpgraph-1.13.tar.gz>

Descargue LibPcap 0.7.2

<http://www.tcpdump.org/release/libpcap-0.7.2.tar.gz>

ANTES DE LA INSTALACIÓN**Importante**

No instale Apache, PHP ó MySQL, esto debe ser instalado desde el código fuente paso a paso que se detallan en las siguientes secciones.

PREPARÁNDONOS PARA LA INSTALACIÓN

Si usted no ha accedido como root, entonces usted necesitará acceder con el comando su hacia el root ("su -" cargará las variables de ambiente desde root).

Asegúrese que usted ha descargado todos los archivos de instalación antes de empezar la instalación. Vaya a su directorio de descarga y comience con el siguiente procedimiento. Este lo guiará en la extracción de los archivos fuentes de las aplicaciones, compilación y luego instalación y configuración para usarlos con el Snort.

(Recuerde que si usted usa SSH para acceder a la consola, usted necesitará usar una cuenta de usuario regular que usted creó cuando instaló Red Hat 9. entonces use el comando "su-" hacia la cuenta root).

INSTALAR ZLIB:

```
tar -xvzf zlib-1.1.4.tar.gz
cd zlib-1.1.4
./configure; make test
make install
cd ..
```

INSTALAR LIBPCAP:

```
tar -xvzf libpcap-0.7.2.tar.gz
cd libpcap-0.7.2
./configure
make
make install
cd ..
```



INSTALAR MYSQL:

Cree el usuario y grupo para MySQL con los siguientes comandos:

```
groupadd mysql
useradd -g mysql
```

En el directorio /root edite el archivo .bash_profile, entonces la línea PATH se lee como sigue:

```
PATH=$PATH:$HOME/bin:/usr/local/mysql/bin
```

Vaya al directorio en donde usted descargó todo, y use los siguientes comandos para instalar y configurar MySQL:

```
install and configure MySQL.
tar -xvzf mysql-4.0.15a.tar.gz
cd mysql-4.0.15a
./configure --prefix=/usr/local/mysql
```

```
make
make install
```

```
scripts/mysql_install_db
```

```
chown -R root /usr/local/mysql
chown -R mysql /usr/local/mysql/var
```

```
chgrp -R mysql /usr/local/mysql
```

```
cp support-files/my-medium.cnf /etc/my.cnf
```

Luego añada las líneas `"/usr/local/mysql/lib/mysql"` y `"/usr/local/lib "` al archivo `/etc/ld.so.conf`

Después que usted añada las líneas, ejecute `"ldconfig -v"`, como root.

CONFIGURE MYSQL PARA QUE ARRANQUE AUTOMÁTICAMENTE

Copie el archivo `"mysql.server"` desde la subcarpeta `support-files` (este está bajo el código para MySQL. Si usted descargó todo en `/root/snortinstall`, entonces la ruta será `/root/snortinstall/mysql-4.0.15a/support-files`) hacia la carpeta `/etc/init.d` y llámelo `mysql` (el comando para copiarla desde el directorio `support-files` es `"cp mysql.server /etc/init.d/mysql"`)

Use los siguiente comandos para crear enlaces simbólicos en las carpetas de inicio del nivel de ejecución 3 y 5. MySQL ahora arrancará automáticamente cuando usted arranque.

```
cd /etc/rc3.d
ln -s ../init.d/mysql S85mysql
ln -s ../init.d/mysql K85mysql
cd /etc/rc5.d
ln -s ../init.d/mysql S85mysql
ln -s ../init.d/mysql K85mysql
cd ../init.d
chmod 755 mysql
```



CIB-ESPOL

INSTALANDO Y CONFIGURANDO APACHE CON PHP

Este procedimiento instalará el servidor Web Apache en "/www". Usted puede, sin embargo, cambiar la ubicación a donde usted desee.

Regrese al directorio de descarga y haga lo siguiente para instalar el Apache y el módulo para PHP.

```
tar -xvzf httpd-2.0.47.tar.gz
cd httpd_2.0.47
./configure --prefix=/www --enable-so
make
make install
```

Tippee "/www/bin/apachectl start"

Revise el sistema para estar seguro de que el servidor web está trabajando (vaya a la IP de este sistema en el web browser, usted probablemente obtendrá un error relacionado con el nombre del host).

Tippe "/www/bin/apachectl stop"

```
cd ..
tar -xvzf php-4.3.3.tar.gz
cd php-4.3.3
```



CIB-ESPOL

```
./configure --prefix=/www/php --with-apxs2=/www/bin/apxs --with-config-
filepath=/
www/php --enable-sockets --with-mysql=/usr/local/mysql --with-zlibdir=/
usr/local --with- gd (one line)
make
make install
```

```
cp php.ini-dist /www/php/php.ini
```

Ahora edite su archivo httpd.conf (este está en /www/conf) y añada:

```
LoadModule php4_module modules/libphp4.so (La nueva versión de PHP añade
esto por usted)
AddType application/x-httpd-php .php (presione ctrl-w y busque AddType)
DirectoryIndex index.php index.html index.html.var (Busque DirectoryIndex)
```


Esto se verá de la siguiente manera cuando usted lo haya hecho:

```
#
# LoadModule foo_module modules/mod_foo.so
LoadModule php4_module modules/libphp4.so

# AddType allows you to tweak mime.types without actually editing it, or $
# make certain files to be certain types.
#
AddType application/x-tar .tgz
AddType image/x-icon .ico
AddType application/x-httpd-php .php

# The index.html.var file (a type-map) is used to deliver content-
# negotiated documents. The MultiViews Option can be used for the
# same purpose, but it is much slower.
#
DirectoryIndex index.php index.html index.html.var
```

Apache 2.0.47 está ahora instalado en el directorio /www. Vaya al directorio /www/bin y ejecute los siguientes comandos:

```
cp apachectl /etc/init.d/httpd
cd /etc/rc3.d
ln -s ../init.d/httpd S85httpd
ln -s ../init.d/httpd K85httpd
cd /etc/rc5.d
ln -s ../init.d/httpd S85httpd
ln -s ../init.d/httpd K85httpd
(Las líneas de arriba añadirán un script de inicio en el sistema para ejecutar los
niveles 3 y 5).
```

Network Query Tool

Host Information	Host Connectivity
☐ Resolve/Reverse Lookup	☐ Check port: 80
☐ Get DNS Records	☐ Ping host
☐ Whois (Web)	☐ Traceroute to host
☐ Whois (IP owner)	☒ Do it all
Enter host or IP Do It	

Figura 4-8. Configurando apache con php

INSTALANDO Y CONFIGURANDO SNORT CON SUS REGLAS

```
groupadd snort
useradd -g snort
mkdir /etc/snort
mkdir /var/log/snort
tar -xvzf snort-2.0.2.tar.gz
cd snort-2.0.2
./configure --with-mysql=/usr/local/mysql
make
make install
```

INSTALANDO LAS REGLAS Y EL ARCHIVO CONF:

(Desde el directorio donde está instalado el Snort)

```
cd rules
cp * /etc/snort
cd ../etc
cp snort.conf /etc/snort
cp *.config /etc/snort
```

MODIFIQUE SU ARCHIVO SNORT.CONF:

El archivo snort.conf está localizado en /etc/snort, haga los siguientes cambios:

var HOME_NET 10.2.2.0/24 (Haga esto cualquiera que sea su red interna)

Cambie la variable rule_path
var RULE_PATH /etc/snort/

Dígale al log de la base de datos (asegúrese que esté en una línea)
new_password es cualquiera que usted quiera siempre y cuando sea el mismo
que usted puso cuando configuró MySQL.

```
output database: log, mysql, user=snort password=new_password
dbname=snort host=localhost
```

CONFIGURE SNORT PARA QUE ARRANQUE AUTOMÁTICAMENTE:

Use el script ubicado en el directorio contrib, S99snort. Cópielo en /etc/init.d y llámelo snort. (cp contrib/S99snort /etc/init.d/snort) Cambie las siguientes líneas:

```
CONFIG=/etc/snort/snort.conf
SNORT_GID=snort
```

Entonces:

Cambie el directorio a /etc/init.d y tipee:

chmod 755 snort (El archivo que usted editó o copió y modificó desde la carpeta contrib)

```
cd /etc/rc3.d
ln -s ../init.d/snort S99snort
ln -s ../init.d/snort K99snort
cd /etc/rc5.d
ln -s ../init.d/snort S99snort
ln -s ../init.d/snort K99snort
```

CONFIGURANDO LA BASE DE DATOS EN MYSQL

Se pondrá una línea con un > en frente de este, de esta manera usted verá lo que la salida debería ser. (Nota: en MySQL, un caracter punto y coma ";" es obligatorio al final de cada línea de entrada) (new_password es cualquier password que usted quiera darle).

```
/usr/local/mysql/bin/mysql
mysql> SET PASSWORD FOR root@localhost=PASSWORD('new_password');
>Query OK, 0 rows affected (0.25 sec)
Version 4 Page 16 of 22 Updated 10/6/2003 9:05 PM
mysql> create database snort;
>Query OK, 1 row affected (0.01 sec)
mysql> grant INSERT,SELECT on root.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('new_password');
>Query OK, 0 rows affected (0.25 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
snort@localhost;
```

```
>Query OK, 0 rows affected (0.02 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
>Query OK, 0 rows affected (0.02 sec)
mysql> exit
>Bye
```

Desde el directorio fuente de Snort 2.0.2 ejecute el siguiente comando: (cuando trabaje con MySQL, si este le pide un password, quiere el que usted definió en la sentencia SQL "SET PASSWORD FOR

```
root@localhost=PASSWORD('new_password');")
```

```
/usr/local/mysql/bin/mysql -u root -p < ./contrib/create_mysql snort
Enter password:
```

Luego instale tablas de bases de datos extras usando el siguiente comando desde el directorio contrib (usted necesitará cambiar de directorio hacia contrib).

```
zcat snortdb-extra.gz | /usr/local/mysql/bin/mysql -p snort
Enter password:
```

Ahora usted necesita revisar y estar seguro de que la base de datos snort fue creada correctamente.

```
/usr/local/mysql/bin/mysql -p
>Enter password:
mysql> SHOW DATABASES;
```

(Usted debe ver lo siguiente)

```
+-----+
| Database
+-----+
| mysql
| snort
| test
+-----+
3 rows in set (0.00 sec)
mysql> use snort
>Database changed
mysql> SHOW TABLES;
+-----+
| Tables_in_snort
+-----+
| data
| detail
```




```

| encoding
| event
| flags
| icmp_hdr
| ip_hdr
| opt
| protocols
| reference
| reference_system
| schema
| sensor
| services
| sig_class
| sig_reference
| signature
| tcp_hdr
| udp_hdr
+-----+

```

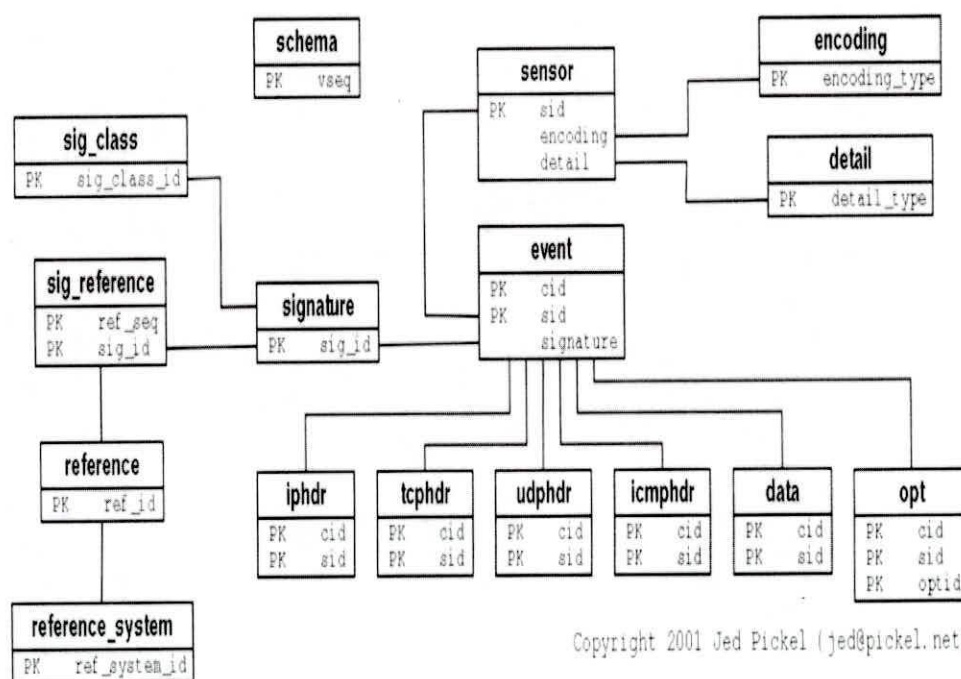
19 rows in set (0.00 sec)>Bye



CIB-ESPOL

La base de datos MySQL debería mostrarse así:

Snort Database ER Diagram (version 1.03): snort 1.8



Copyright 2001 Jed Pickel (jed@pickel.net)

Figura 4-9. Esquema de la Base de Datos Snort

INSTALAR JPGRAPH:

Regrese a su directorio de descargas:

```
cp jpgraph-1.13.tar.gz /www/htdocs
cd /www/htdocs
tar -xvzf jpgraph-1.13.tar.gz
rm -rf jpgraph-1.13.tar.gz
cd jpgraph-1.13
rm -rf README
rm -rf QPL.txt
```

INSTALAR ADODB:

Regrese a su directorio de descargas:

```
cp adodb390.tgz /www/htdocs/
cd /www/htdocs
tar -xvzf adodb390.tgz
rm -rf adodb390.tgz
```

INSTALANDO Y CONFIGURANDO ACID:

Regrese a su directorio de descargas:

```
cp acid-0.9.6b23.tar.gz /www/htdocs
cd /www/htdocs
tar -xvzf acid-0.9.6b23.tar.gz
rm -rf acid-0.9.6b23.tar.gz
```

CONFIGURANDO ACID:

Vaya al directorio /www/htdocs/acid / y edite el archivo acid_conf.php. Este se verá así (por supuesto usted necesitará su password):

```
$DBlib_path = "/www/htdocs/adodb";
/* The type of underlying alert database
*
* MySQL : "mysql"
```

```

* PostgreSQL : "postgres"
* MS SQL Server : "mssql"
*/
$DBtype = "mysql";

/* Alert DB connection parameters
* - $alert_dbname : MySQL database name of Snort alert DB
* - $alert_host : host on which the DB is stored
* - $alert_port : port on which to access the DB
* - $alert_user : login to the database with this user
* - $alert_password : password of the DB user
* This information can be gleaned from the Snort database
* output plugin configuration.
*/
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "snort";
$alert_password = "new_password";

/* Archive DB connection parameters */
$archive_dbname = "snort";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "snort";
$archive_password = "new_password ";

```



CIB-ESPOL

And a little further down

```

$ChartLib_path = "/www/htdocs/jpgraph-1.13/src";

/* File format of charts ('png', 'jpeg', 'gif') */
$chart_file_format = "png";

```

Arranque Apache y vaya a http://yourhost/acid/acid_main.php . Usted obtendrá un mensaje que se verá parecido a esto en su browser:

Analysis Console for Intrusion Databases

The underlying database `snort@localhost` appears to be incomplete/invalid.

The database version is valid, but the ACID DB structure (table: `acid_ag`) is not present. Use the [Setup](#) page to configure and optimize the DB.

Click on the "Setup Page" hyperlink to create the tables that Acid uses, then you will see the following.

ACID

DB Setup

[Home](#)
[Search](#) | [AG Maintenance](#)

[Back]

Operation	Description	Status
ACID tables	Adds tables to extend the Snort DB to support the ACID functionality	Create ACID AG
Search Indexes	(Optional) Adds indexes to the Snort DB to optimize the speed of the queries	DONE

[Loaded in 0 seconds]

ACID v0.9.6b23 (by Roman Danyliw as part of the AirCERT project)

Figura 4-10. Configuración del ACID

Entonces déle click al botón que dice "Create Acid AG"

Ahora cuando usted vaya a `http://yourhost/acid/` usted debería ver la página ACID.

Analysis Console for Intrusion Databases

Added 0 alert(s) to the Alert cache

Queried on : Mon October 06, 2003 15:49:15

Database: snort@localhost (schema version: 100)

Time window: no alerts detected

Sensors: 0

Unique Alerts: 0 (0 categories)

Total Number of Alerts: 0

- Source IP addresses: 0
- Dest. IP addresses: 0
- Unique IP links: 0
- Source Ports: 0
 - TCP (0) UDP (0)
- Dest. Ports: 0
 - TCP (0) UDP (0)

Traffic Profile by Protocol

TCP (0%)

UDP (0%)

ICMP (0%)

Portscan Traffic (0%)

- Search
- Graph Alert data

Figura 4-11. Análisis de Consola de ACID



ASEGURANDO EL DIRECTORIO ACID:

```
mkdir /www/passwords
```

```
/www/bin/htpasswd -c /www/passwords/passwords acid
```

(acid será el nombre de usuario que usted usará para ingresar en este directorio, por medio del password que usted escoja).

Este le pedirá que ingrese el password que usted quiera para este usuario, este es el que usted deberá tipear cuando usted quiera ver su página ACID.

Edite el archivo httpd.conf (/www/conf) e incluya lo siguiente debajo de la sección que empieza con </Directory>

```
<Directory "/www/htdocs/acid">
AuthType Basic
AuthName "SnortIDS"
AuthUserFile /www/passwords/passwords
Require user acid
</Directory>
```

Ahora reinicie el servicio http (/etc/init.d/httpd restart) y la siguiente vez usted verá la página de acid, a usted se le mostrará una ventana que le pedirá su nombre de usuario y password. (Si usted está ejecutando alguna de las características anti-spyware de un software como spybot que busca y destruye usted obtendrá un error cuando intente ver esta página, o cualquiera que requiera

4.7. OTROS CONTROLES DE SEGURIDAD IMPORTANTES EN LINUX.



CIB-ESPOL

4.7.1. ACTUALIZACIONES DE SEGURIDAD

Cuando las vulnerabilidades en el software son descubiertas, el software debe ser actualizado para cerrar los posibles riesgos de seguridad. Si el paquete es parte de una distribución Red Hat Linux que es actualmente es soportado, Red Hat Inc. Está comprometida a enviar paquetes actualizados para arreglar los agujeros de seguridad lo más pronto posible. Si los anuncios de vulnerabilidades de seguridad están acompañados con un parche, el parche es aplicado al paquete de seguridad de Red Hat Linux, probado por el equipo de garantía de seguridad, y publicado como errores actualización. Si el anuncio no incluye un parche, un desarrollador trabajará con el mantenimiento del paquete para arreglar el problema. Luego de que el problema es arreglado, este es probado y publicado como una actualización de errores.

Si Usted está usando un paquete para el cual un reporte de error de seguridad es publicado, es altamente recomendado que Usted actualice sus paquetes de errores de seguridad lo más pronto posible cuando estos sean publicados para minimizar el tiempo que su sistema es vulnerable.

No solo Usted quiere actualizar los últimos paquetes que arreglan cualquier vulnerabilidad, Usted también quiere estar seguro que los últimos paquetes no contienen más vulnerabilidades como un caballo de troya. Un cracker puede fácilmente reconstruir una versión de un paquete (con el mismo número de versión de aquel que supuestamente arregla el problema) pero con diferente vulnerabilidad de seguridad en el paquete y publicarlo en el internet. Si esto ocurre, usando las medidas de seguridad como verificación de archivos contra el RPM original, tal como de Red Hat Inc., y chequear la firma del paquete para asegurarse de que este fue construido por la fuente.

Red Hat ofrece dos maneras de obtener actualizaciones de seguridad:

- 1- Descargar de "Red Hat Network"
- 2- Descargar de "Red Hat Linux errata website"

4.7.1.1. USANDO "RED HAT NETWORK"

"Red Hat Network" le permite automatizar el proceso de actualización. Determina que paquetes RPM son necesarios para su sistema, los descarga desde un repositorio seguro, verifica la firma del RPM para estar seguro de que no han sido

interceptados y luego lo actualiza. La actualización del paquete puede ocurrir inmediatamente o puede ser programada durante cierto periodo de tiempo.

"Red Hat Network" requiere que Usted provea un perfil del sistema para cada máquina que Usted quiera actualizar. El perfil del sistema contiene información de hardware y software acerca del sistema. Esta información es confidencial y no se la da a nadie más. El solo usada para determinar que actualizaciones de errores son aplicables para cada sistema. Sin esto, "Red Hat Network" no podría determinar si su sistema necesita las actualizaciones. Cuando un error de seguridad es publicado, "Red Hat Network" le enviará un e-mail con la descripción del error así como cuales de sus sistemas están afectados. Para aplicar la actualización, Usted puede usar el **Agente de Actualización Red Hat** o programar el paquete a ser actualizado a través del sitio web <http://rhn.redhat.com>.

4.7.1.2. USANDO EL "ERRATA WEBSITE" (SITIO WEB DE ACTUALIZACIONES DE ERRORES)

Cuando los reportes de errores de seguridad son lanzados, estos son publicados en el "Red Hat Errata Website" disponibles <http://www.redhat.com/apps/support/errata/>. De esta página, seleccione el producto y la versión de su sistema, y entonces seleccione seguridad en la cabecera de la página para mostrar solo consejos de seguridad para Red Hat Linux. Si la síntesis de uno de los consejos describe uno de los paquetes usado en sus sistemas, déle un click en la síntesis para más detalles.



CIB-ESPOL

La página de detalles describe las vulnerabilidades de seguridad y algunas instrucciones especiales que deben ser cumplidas en adición a la actualización del paquete para arreglar el agujero de seguridad.

Para descargar los paquetes de seguridad click en el nombre del paquete y guárdelo en el disco duro. Es altamente recomendado que usted cree un nuevo directorio como `/tmp/updates` y descargue todos los paquetes en ese directorio.

Todos los paquetes de Red Hat Linux son firmados con la clave GPG de Red Hat Inc. La utilidad RPM en Red Hat Linux 9 automáticamente trata de verificar la firma GPG de un RPM antes de instalarlo. Si Usted no tiene instalada la clave GPG de Red Hat Inc. Desde un sitio seguro estático como lo es un cd rom de la distribución Red Hat Linux.

Asumiendo que el cd-rom es montado en `/mnt/cdrom`, use el siguiente comando para importarla dentro del repositorio de claves:

```
rpm --import /mnt/cdrom/RPM-GPG-KEY
```

Para mostrar una lista de claves instaladas para la verificación RPM ejecute el comando:

```
rpm -qa gpg-pubkey*
```

Para la clave Red Hat Inc. la salida incluirá:



```
gpg-pubkey-db42a60e-37ea5438
```

Para mostrar detalles acerca de una clave específica use el `rpm -qi` seguido por la salida del comando previo.

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

Es extremadamente importante que usted verifique la firma del archivo RPM antes de instalarlo. Este paso asegura que estos no han sido alterados (como un caballo de troya siendo insertado dentro del paquete) la publicación del paquete desde FORMAL-RHI.

```
rpm -K /tmp/updates/*.rpm
```

Para cada paquete si la verificación de la clave GPG es exitosa, esto deberá retornar `gpg OK` en la salida.

Después de verificar la clave GPG y todos los paquetes asociados con el reporte de errores lo instala como root en un "shell prompt". Por ejemplo:

```
rpm -Uvh /tmp/updates/*.rpm
```

Si el reporte de errores contiene algunas instrucciones especiales recuerde ejecutarlas apropiadamente. Si los paquetes de errores de seguridad están contenidos en un paquete de kernel, asegúrese de reiniciar la máquina para habilitar el nuevo kernel.

4.7.2. SEGURIDAD DE LAS ESTACIONES

La seguridad en un sistema en Linux empieza con la seguridad de la estación de trabajo. Si su estación no está asegurada o el sistema en general de la empresa, la política de seguridad empieza con los PCs. Después de todo una computadora de red es solo tan segura como el nodo más débil.

4.7.2.1. SEGURIDAD DE LA ESTACIÓN DE TRABAJO

Cuando evaluamos la seguridad de una estación de trabajo en Red Hat Linux, considere lo siguiente:

- ♦ **Seguridad del cargador de arranque y de BIOS.-** ¿Puede un usuario no autorizado físicamente acceder a la máquina y arrancar en el modo de un solo usuario o modo de rescate sin un password?
- ♦ **Seguridad de Password.-** ¿Qué tan seguras son los password de las cuentas de usuarios en las máquinas?
- ♦ **Control administrativo.-** ¿Qué servicios están escuchando peticiones en la red y deben estar corriendo totalmente?
- ♦ **Firewall personales.-** ¿Qué tipo de firewall es necesario?
- ♦ **Herramientas de comunicación de seguridad mejoradas -** ¿Qué herramientas deben ser usadas para comunicarse entre estaciones y cuales deben ser evitadas?

4.7.2.2. SEGURIDAD DEL CARGADOR DE ARRANQUE Y DEL BIOS

Protección de password para el Bios y para el cargador de arranque pueden prevenir de usuarios no autorizados quienes tengan acceso físico a su sistema de

bootear de un medio removible u obtener el root a través del modo de un solo usuario. Pero las medidas de seguridad que uno debe tomar protegen contra tales ataques dependiendo de dos cosas de la sensibilidad de la información que la estación de trabajo mantiene y la localización de la máquina.

Por un instante si la máquina es usada en una presentación de negocios y no contiene información sensible, entonces esto no sería crítico prevenir tales ataques. Mientras, si la laptop de un empleado con claves SSH privadas y no protegidas para la red corporativa es dejada sin una atención en la misma presentación de negocios, esto le puede conducir a una importante brecha de seguridad con ramificaciones para toda la compañía.

En otras palabras si la estación de trabajo está ubicada en un lugar donde solo las personas autorizadas o de confianza tienen acceso, entonces la seguridad del BIOS o del Cargador de Arranque quizás no sea necesario.

4.7.2.3. PASSWORD PARA EL BIOS

Las siguientes son dos de las razones principales para proteger el BIOS en una computadora por medio de un password:

1. **Prevenir los cambios de las configuraciones del BIOS.-** Si un intruso tiene acceso al BIOS ellos pueden configurarlo para que arranque desde un disquete o cd-rom. Esto le hace posible entrar al modo de

rescate o al modo de un solo usuario, lo cual les permitiría a ellos instalar programas maliciosos en el sistema o copiar datos sensibles.

2. **Prevenir el booteo del sistema.-** Algunos BIOS le permiten proteger el proceso de arranque con un password. Cuando está activo el intruso es forzado a ingresar el password antes de que el BIOS lance el cargador de arranque.

Por lo que los métodos para configurar el password del BIOS varía entre fabricantes de computadora, consulte el manual de su computadora para las instrucciones.

Si usted olvida el password del BIOS este puede ser frecuentemente inicializado de dos formas: con jumpers en la tarjeta madre o desconectando la batería del CMOS. Por esta razón es una buena practica bloquear el case del computador de ser posible. Sin embargo, consulte el manual de la computadora o de la tarjeta madre antes de efectuar este procedimiento.

PASSWORDS DEL CARGADOR DE ARRANQUE

Las siguientes son las principales razones para proteger el cargador de arranque de Linux por medio de dos pasos:

1. **Prevenir el acceso en modo de un solo usuario.-** Si un intruso puede bootear en modo de un solo usuario, el se convierte en el usuario root.

2. **Prevenir el acceso a la Consola GRUB.-** Si la máquina usa GRUB como su cargador de arranque, un intruso puede usar la interfaz del editor GRUB para cambiar su configuración o recoger información usando el comando `cat`.
3. **Prevenir el acceso de sistemas operativos no seguros.-** Si este es un sistema de doble arranque, un intruso puede seleccionar en tiempo de arranque un sistema operativo como DOS, el cual ignora el control de acceso y el archivo de permisos.

Existen dos cargadores de arranque que se relacionan con Red Hat Linux para la plataforma x86, GRUB y LILO.

PROTEGIENDO GRUB CON UN PASSWORD

Usted puede configurar GRUB añadiendo una directiva de password a su archivo de configuración, para hacer esto, primero decida un password, luego abra una ventana de terminal, accese como root y digite:

`/sbin/grub-md5-crypt`



CIB-ESPOL

Cuando aparezca el cursor digite el password GRUB y presione [ENTER]. Esto retornará una función de hash MD5 del password.

Luego edite el archivo de configuración GRUB `/boot/grub/grub.conf`. Abra el archivo debajo de la línea *time-out* en la sección principal del documento, añada la siguiente línea:

```
password --md5 < password-hash>
```

Reemplace < *password-hash* > con el valor retornado por `/sbin/grub-md5-crypt2`.

La próxima vez que Usted arranque el sistema el menú GRUB no le permitirá acceder a la interfase de comando sin primero presionar la letra [P] seguida por el password GRUB.

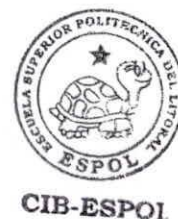
Desafortunadamente, esta solución no previene a un intruso de bootear en un sistema operativo no seguro dentro de un ambiente de booteo doble. Por eso usted necesita editar una parte diferente del archivo `/boot/grub/grub.conf`.

Mire la línea de título del sistema operativo no seguro y añada la línea que dice `lock` directamente debajo de ésta.

Para un sistema DOS, el párrafo debe ser similar a lo siguiente:

```
title DOS
```

```
lock
```



Atención

Usted tiene una línea de password en la sección principal del archivo `/boot/grub/grub.conf` para que trabaje apropiadamente. De otra forma el intruso será capaz de acceder a la interfase del editor GRUB y borrar la línea de bloqueo.

Si Usted desea tener un password diferente para un kernel o sistema operativo particular añada la línea `lock` al párrafo seguido por la línea de password.

Cada párrafo que Usted proteja con un password único debe empezar con líneas similares al siguiente ejemplo:

```
title DOS
lock
password --md5 <password-hash>
```

Finalmente, recuerde que el archivo `/boot/grub/grub.conf` es legible por defecto. Es una buena idea cambiarlo puesto que no afecta a la funcionalidad del GRUB, tipiendo el siguiente comando como root:

```
chmod 600 /boot/grub/grub.conf
```

PROTEGIENDO LILO CON UN PASSWORD

LILO es un cargador de arranque más simple que GRUB y no ofrece una interfaz de comando, Usted no tiene que preocuparse acerca que un intruso tenga acceso al sistema antes de que el kernel sea cargado sin embargo, todavía existe el peligro de que los intrusos arranquen en modo de un solo usuario dentro de un sistema operativo inseguro.

Usted puede configurar LILO para que le pregunte el password antes de arrancar cualquier sistema operativo del kernel o sistema, añadiendo una directiva de password en la sección global de su archivo de configuración. Para hacer esto, abra una ventana de terminal accese como root y edite el archivo `/etc/lilo.conf`. Antes del párrafo *image*, añada la directiva de password similar a esto:

```
password= <password>
```


En la directiva de arriba reemplace la palabra <password> con su password.

Importante

Cada vez que Usted edite el archivo /etc/lilo.conf, Usted debe ejecutar el comando /sbin/lilo -v -v para que los cambios tengan efecto. Si tiene configurado un password cualquiera diferente del root puede leer el archivo, LILO lo instalará, pero le alertará que los permisos de los archivos de configuración son erróneos.

Si usted no quiere un password global usted puede aplicar la directiva de password a cualquier párrafo correspondiente a algún kernel o sistema operativo al cual usted desee restringir el acceso en el archivo /etc/lilo.conf. Para hacer esto añada la directiva de password inmediatamente debajo de la línea *image*. Cuando finalice el comienzo del párrafo protegido por el password se asemejará a lo siguiente:

```
image=/boot/vmlinuz- <version>
password= <password>
```



CIB-ESPOL

En el ejemplo previo, reemplace <version> con la versión de kernel y <password> con el password LILO para ese kernel.

Si Usted quiere permitir arrancar un kernel o sistema operativo sin verificación de password pero no quiere permitir a los usuarios añadir argumentos sin un password, usted puede añadir la directiva *restricted* en la línea debajo de la línea de password dentro del párrafo. Tal párrafo comienza similar a esto:

```
image=/boot/vmlinuz- <version>
password= <password>
restricted
```

Otra vez, reemplace <version> con la versión de kernel y <password> con el password LILO para ese kernel.

Si usted desea la directiva *restricted*, usted debe también tener una línea de password en el párrafo.

Advertencia

El archivo `/etc/lilo.conf` es leíble. Si usted está protegiendo LILO con un password es esencial que Usted solo permita al root leer y editar el archivo desde que todos los password están en texto plano. Para hacer esto tipee el siguiente comando como root:

```
chmod 600 /etc/lilo.conf
```

4.7.2.4. SEGURIDAD DEL PASSWORD

Los password son los métodos primordiales que Red Hat Linux usa para verificar la identidad de los usuarios. Este es el porqué la seguridad de los password es enormemente importante para la seguridad de las estaciones de trabajo y de la red.

Por propósitos de seguridad el programa de instalación configura el sistema para usar el *Message Digest Algorithm* (MD5) y los password ocultos. Es altamente recomendado que usted no altere esta configuración.

Si usted no selecciona password MD5 durante la instalación el viejo formato *data encryption standard* (DES) es usado. Este formato limita los password a 8

caracteres alfanuméricos (no permite puntuación y otros caracteres especiales) y provee un modesto nivel de encriptación de 56-bits.

Si usted no selecciona passwords ocultos todos los password son almacenados como una forma de resumen de una sola vía legible en el archivo `/etc/passwd`, el cual hace el sistema vulnerable para los ataques de crackeo de password fuera de Linux. Si un intruso gana acceso a la máquina como un usuario regular el puede copiar el archivo `/etc/passwd` a su propia máquina y ejecutar un número de programas de crackeo de password contra éste. Si hay un password inseguro en el archivo, es solo cuestión de tiempo antes que el crackeador del password lo descubra.

Los password ocultos eliminan este tipo de ataques almacenando el resumen del password en el archivo de `etc/shadow`, el cual es leíble solo por el usuario root.

Esto fuerza a un intruso potencial a intentar crackear el password remotamente, accedendo dentro del servicio de red en la máquina, como un SSH o FTP. Este tipo de ataques de fuerza bruta es mucho más lento y deja huellas obvias y cientos de intentos de accesos fallidos que son registrados en los archivos del sistema. Si el cracker comienza un ataque en medio de la noche y usted tiene un password débil, el cracker quizás gane acceso antes de que salga a la luz.

Más allá del formato y del almacenamiento es un problema de contenido. La única cosa más importante que un usuario puede hacer para proteger su cuenta contra el ataque del crackeo de password es crear un password fuerte.



CREANDO PASSWORDS FUERTES

Los password son los métodos primordiales que un sistema operativo usa para verificar la identidad de los usuarios. Este es el porqué la seguridad de los password es enormemente importante para la seguridad de las estaciones de trabajo y de la red.

Cuando creamos un password es buena idea seguir las siguientes guías:

No haga lo siguiente:

No use solo palabras o números.- Usted nunca use solo números o palabras en un password.

Algunos ejemplos incluyen lo siguiente:

- 8675309
- Juan
- hackme

No use palabras reconocibles.- palabras como nombres propios o de diccionario o términos de shows de televisión o novelas deben ser evitados aún si es que estos son alfanuméricos.

- ♦ John1
- ♦ DS-9
- ♦ Mentat123

No use palabras en lenguajes extranjeros.- Programas crackeadores de password frecuentemente los chequean contra una lista de palabras encontradas en diccionarios en muchos lenguajes. Confiar en lenguajes extranjeros para asegurar los password es de poco uso.

Algunos ejemplos incluyen lo siguiente:

- ♦ Cheguevara
- ♦ Bienvenido1
- ♦ 1dumbkopf

No use terminología hacker.- Si usted piensa que usted es de la élite porque usa terminología hacker también llamada idioma 1337 (LEET) en su password, píenselo otra vez. Muchas listas de palabras incluyen el lenguaje LEET.

Algunos ejemplos incluyen lo siguiente:

- ♦ H4XOR
- ♦ 1337



No use información personal.- Guía de información personal limpia. Si el intruso sabe quien es usted, él tendrá un tiempo fácil para descifrar su password si este incluye información tal como:

- ♦ Su nombre

- ♦ El nombre de su mascota
- ♦ El nombre de los miembros de la familia
- ♦ Algún cumpleaños
- ♦ Su número de teléfono

No use palabras reconocidas invertidas.- Un buen chequeador de buenos password siempre invierte las palabras comunes, invertir un mal password no lo hace a este más seguro.

Algunos ejemplos incluyen lo siguiente:

- ♦ R0X4H
- ♦ Nauj
- ♦ 9-DS



No escriba su password.- Nunca escriba su password en papel. Es más seguro memorizarlo.

No use el mismo password para todas las máquinas.- Es importante que usted ingrese un password separado para cada máquina. De esta forma si un sistema está comprometido, todas sus máquinas no estarán en riesgo.

Haga lo siguiente:

Cree el password de por lo menos ocho caracteres de longitud.- La longitud del password es la mejor. Si usted está usando password MD5, este debe ser de 15 caracteres de longitud o más. Con password DES, use longitud máxima de 8 caracteres.

Mezcle las letras mayúsculas y minúsculas.- Red Hat Linux es sensible a la tecla bloqueo mayúscula entonces mezclar mayúsculas y minúsculas mejora la fuerza del password.

Mezcle letras y números.- Añadir números a los passwords, especialmente cuando se añade en el medio (no solo en el comienzo o al final), puede mejorar la fuerza del password.

Incluir caracteres de símbolos especiales.- Caracteres especiales como &, \$, >, pueden mejorar enormemente la fuerza del password.

Escoja un password que usted pueda recordar.- El mejor password en el mundo, es mejor si usted no puede recordarlo. Use abreviaciones o nombres de recursos como ayuda en la memorización del password.

Con todas estas reglas parece difícil crear un password que encuentre todos los criterios para un buen password evitando las características de los malos. Afortunadamente, existen algunos pasos sencillos que se pueden tomar para generar un password seguro y que se pueda memorizar.



CIB-ESPOL

FORZAR PASSWORD FUERTES

Para proteger la red de los intrusos es buena idea para administradores de sistemas verificar que los password usados dentro de una organización sean fuertes. Cuando los usuarios se les dice que creen o cambien los passwords, ellos pueden usar una aplicación bajo la línea de comando *passwd*, el cual es "Pluggable Authentication Manager" (PAM) y además lo chequeará para verificar si el password es fácil de crackear o es muy corto en longitud a través del módulo *pam_cracklib.so* PAM. Desde que PAM es personalizable, es posible añadirle más

chequeos de integridad de password, tal como *pam_passwdqc* o escribir su propio módulo.

Debe ser notado, sin embargo que los chequeos desarrollados en los password en el tiempo de su creación no descubre malos password tan efectivamente como ejecutar un programa de crackeo de passwords contra los passwords de la organización.

Hay muchos programas de crackeo de password que corren bajo Linux, sin embargo ninguno viene con el sistema operativo. Algunos de estos son:

- ♦ John The Ripper, Crack, Slurpie.

Advertencia

Siempre obtenga una autorización de escritura antes de intentar crackear los password en una organización.

CADUCIDAD DE PASSWORD

Caducidad de password es otra técnica utilizada por los administradores de sistemas para defenderse contra los malos password de una organización. Caducidad de password significa que después de una cantidad de tiempo (usualmente 90 días) el usuario es obligado a ingresar un nuevo password. La teoría detrás de esto es que si un usuario es forzado a cambiar su password periódicamente, un password crackeado es solo utilizable para un intruso por una

cantidad de tiempo limitada. La desventaja de esta técnica es que los usuarios están más propensos a escribir sus password.

Hay dos programas principales usados para especificar la caducidad de passwords bajo Red Hat Linux: el comando *chage* o la aplicación gráfica **User Manager** (redhat-config-users).

La opción *-M* del comando *chage* especifica el máximo número de días en que el password es válido. Entonces por un momento si usted quiere que un password de usuario caduque en 90 días tipee el siguiente comando:

```
chage -M 90 <username>
```

Si en el comando de arriba, reemplaza *<username>* con el nombre del usuario. Si usted no quiere que el password caduque, es tradicional usar el valor de 99999 después de la opción *-M* (esto equivale alrededor de 273 años).

Si usted quiere usar la aplicación gráfica **User Manager** para crear las políticas de caducidad de password vaya a **Main Menu button** (en el panel) => **system settings** => **users & groups** o tipee el comando *redhat-config-users* en la ventana de terminal. Click en la tabla **users**, seleccione el usuario de la lista de usuarios y de click en **properties** del botón de menú.

Entonces de click en la tabla **password info** e ingrese el número de días antes de que el password caduque así como se muestra en la siguiente figura:

User Data Account Info Password Info Groups

User last changed password on: Mon Feb 3 2003

☒ Enable password expiration

Days before change allowed: 0

Days before change required: 90

Days warning before change: 0

Days before account inactive: 0

Cancel OK

Figura 4-12. Panel de Información de Password



4.7.2.5. CONTROL ADMINISTRATIVO

Cuando se administra una máquina de casa el usuario tiene que desarrollar algunas tareas como usuario root o adquiriendo privilegios efectivos de root a través del programa *setuid* tal como un comando *sudo* o *su*. Un programa *setuid* es uno que opera con el ID de usuario (UID) del propietario del programa en vez de usar el usuario que opera el programa. Como los programas están identificados con la letra minúscula "s" en la sección de propietario de un listado de formato largo.

Para el administrador de sistemas de una organización sin embargo las opciones deben ser hechas en base a cuanto acceso administrativo los usuarios en una organización deben tener en su máquina. A través del módulo PAM llamado *pam_console.so*, algunas actividades normalmente reservadas para el usuario root tal como reiniciar y montar un medio removible es permitido para el primer

usuario que ingresa a la consola física. Sin embargo, otra tarea importante para la administración de sistemas tal como cambiar las configuraciones de red configurar un mouse nuevo o montar un dispositivo de red son imposibles sin un acceso administrativo. Como resultado los administradores de sistemas deben decidir cuanto acceso administrativo los usuarios deben recibir en su red.

PERMITIENDO ACCESO ROOT

Si los usuarios en una organización son confiables, al grupo computer-savvy, permitirles el acceso root quizás no sea una mala idea. Permitirle acceso root a los usuarios significa menores problemas como añadir un recurso o configurar una interfaz de red pueda ser manejada por un usuario individual, dejando a los administradores de sistemas libres de cumplir con la seguridad de la red y otros temas importantes. Dicho de otra manera, dar acceso root a los usuarios individuales podría provocar los siguientes problemas:

Configuración errónea de la máquina.- Los usuarios con acceso root pueden configurar mal su máquina y requerir una ayuda o peor, abrir un hueco de seguridad sin saberlo.

Ejecutar servicios inseguros.- Los usuarios con acceso root pueden ejecutar servicios inseguros tales como FTP o Telnet, potencialmente poniendo sus nombres de usuarios y password en riesgos así como pasarlos a través de la red en claro.

Enviar archivos adjuntos en e-mails como root.- Aunque es raro, los virus por e-mail que afectan a Linux existen. En el único momento en que ellos son una amenaza es cuando ellos son ejecutados por el usuario root.

DESABILITANDO EL ACCESO ROOT

Si un administrador no está conforme permitiendo a los usuarios ingresar como root por estas u otras razones, el password root debe ser mantenido en secreto y acceder en el modo de ejecución de un solo usuario, debe ser deshabilitado a través de la protección del password del cargador de arranque.

La siguiente tabla muestra formas en que un administrador puede asegurarse más de que los accesos root sean deshabilitados:

Método	Descripción	Efectos	No tiene efectos
Cambiar el shell root	Edite el archivo /etc/passwd y cambie el shell de /bin/bash a /sbin/nologin.	Previene el acceso al shell root y registra los intentos. Los siguientes programas son prevenidos de acceder a la cuenta root: Login Gdm Kdm Xdm Su Ssh Scp Sftp	Programas que no requieren un shell tales como: Clientes FTP, Clientes E-mail y muchos programas <i>setuid</i> . Los siguientes programas no son prevenidos de acceder a la cuenta root: Sudo Clientes FTP Clientes e-mail
Deshabilitando el acceso root a través de un dispositivo de consola (tty).	Un archivo vacío /etc/securetty previene el acceso root en cualquier dispositivo conectado a la computadora.	Previene el acceso de la cuenta root a través de la consola o de la red. Los siguientes programas son prevenidos de acceder a la cuenta root: Login Gdm	Programas que no accesan como root, pero desarrollan tareas administrativas a través de <i>setuid</i> u otros mecanismos. Los siguientes programas no están prevenidos de acceder a la

Método	Descripción	Efectos	No tiene efectos
		Kdm Xdm Otros servicios de red que abren un tty.	cuenta root: Su Sudo Ssh Scp sftp
Deshabilitar acceso root SSH	Edite el archivo /etc/ssh/sshd_config y configure el parámetro PermitRootLogin a "no".	Previene el acceso root a través del conjunto de herramientas OpenSSH. Los siguientes programas son prevenidos de acceder a la cuenta root: Ssh Scp Sftp	Partiendo de que esto solo afecta al conjunto de herramientas OpenSSH, otros programas no son afectados por esta configuración.
Use PAM para limitar el acceso root hacia los servicios.	Edite el archivo para el servicio destino en el directorio /etc/pam.d/. Asegúrese que pam_listfile.so es requerido para autenticación	Previene el acceso root hacia los servicios de red que están pendientes de la aplicación PAM. Los siguientes servicios son prevenidos de acceder a la cuenta root: Clientes FTP Clientes e-mail Login Gdm Kdm Xdm Ssh Scp Sftp Cualquier	Programas y servicios que no están pendientes de la aplicación PAM.  CIB-ESPOL

Método	Descripción	Efectos	No tiene efectos
		servicio pendiente de la aplicación PAM.	

Tabla 4-20. Acceso Root Métodos para Deshabilitar la Cuenta Root

DESABILITANDO EL SHELL DEL ROOT

Para prevenir a los usuarios de ingresar directamente como root el administrador de sistemas puede configurar el shell de la cuenta root hacia `/sbin/nologin` en el archivo `/etc/passwd`. Esto evitará acceder a la cuenta root a través de comandos que requieran un shell, tales como los comandos *su* y *ssh*.

Importante

Los programas que no requieran acceso al shell tales como clientes e-mail o el comando *sudo*, aún pueden acceder a la cuenta root.



CIB-ESPOL

DESABILITANDO EL ACCESO ROOT

Para limitar el acceso a la cuenta root, los administradores pueden deshabilitar el acceso root a la consola editando el archivo `/etc/securetty`. Este archivo enlista todos los recursos del usuario root que están permitidos para acceder. Si el archivo no existe, el usuario root puede ingresar a través de cualquier dispositivo de comunicación en el sistema, sea a través de la consola o a través de una interfaz de red cualquiera. Esto es peligroso porque un usuario puede usar telnet en su máquina como root enviando su password en texto plano a través de la red. Por defecto el archivo de Red Hat Linux `/etc/securetty` puede permitir al usuario root registrarse en la consola física conectada a la máquina. Para evitar

que el root ingrese, borre el contenido de este archivo tipiendo el siguiente comando:

```
echo > /etc/securetty
```

Importante

Un archivo en blanco `/etc/securetty` no evita que el usuario root pueda ingresar remotamente usando el conjunto de herramientas OpenSSH porque la consola no es abierta sino hasta después de la autenticación.

DESABILITANDO EL ACCESO ROOT ATRAVÉS DE SSH

Para evitar el acceso root a través del protocolo SSH, edite el archivo de configuración del demonio SSH: `/etc/ssh/sshd_config`. Cambie la línea que dice:

```
# PermitRootLogin yes
```

Para que se lea como sigue:

```
PermitRootLogin no
```



CIB-ESPOL

DESABILITANDO EL ACCESO ROOT ATRAVÉS DE PAM

PAM a través del módulo `/lib/security/pam_listfile`, permite gran flexibilidad en la denegación de cuentas específicas. Esto le permite al administrador hacer apuntar al módulo hacia una lista de usuarios a quienes no se les permite el acceso. Abajo hay un ejemplo de cómo el módulo es usado por el `vsftpd` servidor ftp en el archivo de configuración PAM `/etc/pam.d/vsftpd` (el carácter `\` al final de la primera línea en el siguiente ejemplo no es necesario si la directiva está en una sola línea):

```
auth required /lib/security/pam_listfile.so item=user \
sense=deny file=/etc/vsftpd.ftputers onerr=succeed
```

Esto le dice a PAM que consulte el archivo `/etc/vsftpd.ftputers` y denegar a cualquier usuario listado en el acceso al servicio. El administrador es libre de poder cambiar el nombre de este archivo y puede mantener una lista separada para cada servicio o usar una lista central para denegar el acceso a múltiples servicios.

Si el administrador quiere denegar el acceso a múltiples servicios, una línea similar puede ser añadida a los servicios de configuración PAM, tal como `/etc/pam.d/imap` para los clientes de e-mail o `/etc/pam.d/ssh` para los clientes ssh.

LIMITANDO EL ACCESO ROOT

En vez de denegar completamente el acceso al usuario root, el administrador quizás desee permitir el acceso solo a los programas a través de *setuid*, tal como *su* o *sudo*.

EL COMANDO "su"

Después de tipiar el comando *su*, el usuario debe ingresar el password del root, y después autenticar, mostrando una ventana de terminal de root. Una vez accedido a través del comando *su*, el usuario es el usuario root y tiene un acceso administrativo absoluto al sistema. Además, una vez que el usuario obtiene el root, es posible en algunos casos usar el comando *su* para cambiar a cualquier otro usuario en el sistema sin que tenga que ingresar el password. Debido a que



este programa es poderoso, los administradores dentro de una organización quizás deseen limitar a quienes tienen acceso al comando.

Una de las formas más simples de hacer esto es añadir usuarios al grupo administrativo especial llamado *Wheel*. Para hacer esto, tipee el siguiente comando como root:

```
usermod -G wheel <username>
```

En el comando previo reemplace <username> con el nombre de usuario que está siendo añadido al grupo *Wheel*.

Para usar el **User Manager** para este propósito, vaya al **Main Menu button** (en el panel) => **system settings** => **users & groups** o tipee el comando `redhat-config-users` en la ventana terminal. Seleccione la tabla `users`, seleccione el usuario de la lista de usuarios y de click en `properties` en el menú de botones (o escoja `file=>properties` en el menú desplegable). Entonces seleccione la tabla `groups` y déle un click en el grupo *Wheel*, como se muestra en la siguiente figura.



CIB-ESPOL

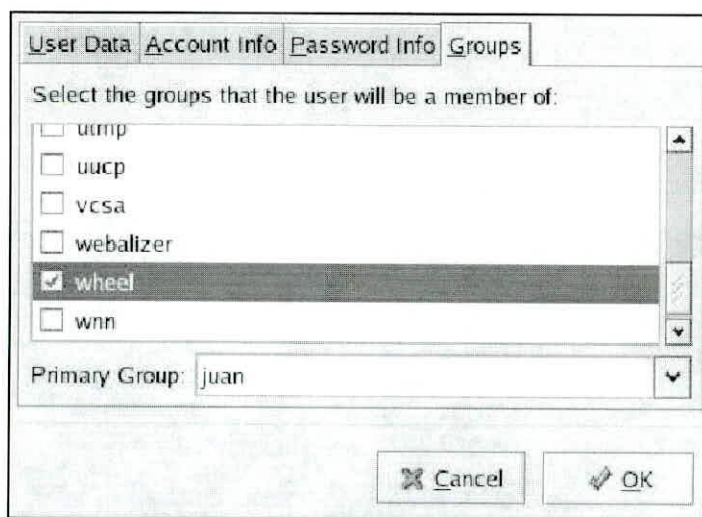


Figura 4-13. Panel de Grupos

Luego abra el archivo de configuración PAM para Su, `/etc/pam.d/su`, en el editor de texto y quite el comentario `[#]` de la siguiente línea:

```
auth required /lib/security/pam_wheel.so use_uid
```

Esto permitirá que solo los miembros del grupo administrativo *Wheel* puedan usar el programa.

Nota

El usuario `root` es parte del grupo *Wheel* por defecto.



CIB-ESPOL

EL COMANDO "sudo"

El comando `sudo` ofrece otro alcance para darle acceso administrativo a los usuarios. Cuando a un usuario confiable le precede un comando administrativo con `sudo` el debe ingresar su password. Entonces, una vez autenticado y

asumiendo que el comando es permitido el comando administrativo es ejecutado como si fuera hecho por el comando root.

El formato básico del comando sudo es como el siguiente:

```
sudo <command>
```

En el ejemplo de arriba <command> sería reemplazado por el comando normalmente reservado para el usuario root tal como *mount*.

Importante

Usuarios del comando sudo deben tener un cuidado extra y salir de la conexión antes de alejarse de sus máquinas por un momento. Porque los otros usuarios sudo pueden usar el comando otra vez sin que se les haya pedido el password por un periodo de 5 minutos. Esta configuración puede ser cambiada por medio del archivo de configuración */etc/sudoers*.

El comando sudo permite un alto grado de flexibilidad. Por el momento, solo los usuarios listados en el archivo de configuración */etc/sudoers* se les permite que usen el comando sudo y el comando es ejecutado en el shell del usuario, no en el shell root. Esto significa que el shell root puede ser completamente deshabilitado tal como se muestra en la sección deshabilitando el shell del root.

El comando sudo también provee una pista comprensiva de Auditoría. Cada autenticación exitosa es ingresada al archivo */bar/log/messages* y el comando emitido a través del nombre del usuario emisor es añadido al archivo */bar/log/secure*.

Otra ventaja del comando `sudo` es que un administrador puede permitir el acceso a diferentes usuarios hacia comandos específicos basándose en sus necesidades.

Los administradores que quieran editar el archivo de configuración `sudo`, `/etc/sudoers`, deben usar el comando *visudo*.

Para otorgarle a alguien privilegios administrativos totales, tipee `visudo` y añádale una línea similar a la siguiente en la sección de especificación de los privilegios de usuario:

```
Juan ALL=(ALL) ALL
```

Este ejemplo sostiene que el usuario Juan, puede usar `sudo` desde cualquier host y ejecutar cualquier comando.

El ejemplo de abajo muestra la granularidad posible cuando configuramos `sudo`:

```
%users localhost=/sbin/shutdown -h now
```

Este ejemplo sostiene que cualquier usuario puede usar el comando `/sbin/shutdown -h now` tan frecuentemente como sea usado en la consola.

La página man para `sudoers` tiene una lista detallada de opciones para este archivo.



CIB-ESPOL

4.7.2.6. SERVICIOS DE RED DISPONIBLES

Mientras los usuarios accedan a los controles administrativos, es un tema importante para los administradores de sistemas dentro de la organización, mantener las tablas de los servicios de red es de vital importancia para cualquiera que instale y maneje un sistema Linux.

Muchos servicios bajo Linux se comportan como servidores de red. Si un servicio de red está corriendo en una máquina, entonces el servidor de aplicación llamado daemon está escuchando las conexiones de uno o más puertos de red. Cada uno de estos servidores deben ser tratados como una vía potencial de ataque.



RIESGOS DE LOS SERVICIOS

Los servicios de red pueden tener muchos riesgos para un sistema Linux. Abajo se muestra una lista de algunos de los principales:

- ♦ **Ataques de desbordamiento de Buffer.**— Los servicios que se conectan a los puertos numerados desde el 0 hasta el 1023 deben ejecutarse como un usuario administrativo. Si la aplicación tiene una vulnerabilidad de desbordamiento del buffer, un intruso puede tener acceso al sistema como un usuario ejecutando el demonio. Debido a que la vulnerabilidad del desbordamiento del buffer existe, los crackers usarán herramientas automatizadas para identificar sistemas con vulnerabilidades, y una vez que ellos hayan ganado acceso ellos usarán herramientas automatizadas para mantener su acceso en el sistema.

- ♦ **Ataques de denegación de servicios (DoS).**– Inundando un servicio con requerimientos, un ataque de denegación de servicios puede llevar a un sistema a colgarse cada vez que intente acceder y obtener una respuesta a cada requerimiento.
- ♦ **Ataques de vulnerabilidad en los scripts.**– Si un servidor está usando scripts para ejecutar acciones del servidor, como un web server normalmente lo hace, un cracker puede montar un ataque impropio escribiendo un script. Este ataque de vulnerabilidad script podría provocar una condición de desbordamiento del buffer o permitir que el intruso modifique archivos en el sistema.

Para limitarnos a estar expuestos a los ataques sobre la red, todos los servicios que no sean usados, deben ser apagados.

IDENTIFICANDO Y CONFIGURANDO LOS SERVICIOS

Para mejorar la seguridad, muchos servicios de red instalados en Red Hat Linux, están apagados por defecto. Existen, sin embargo algunas excepciones notables:

Cupsd.– El servidor de impresión por defecto para Red Hat Linux.

Lpd.– Un servidor de impresión alternativo.

Xinetd.– Un súper servidor que controla las conexiones hacia un host o servidores subordinados tal como: wu-ftpd, telnet, y sgi-fam (el cual es necesario para que el administrador de archivos Nautilus).

Sshd.— El servidor OpenSSH, el cual es un reemplazo seguro para telnet.

Cuando determinamos si debemos o no dejar estos servicios ejecutándose, es mejor usar el sentido común y el sentido de error por precaución. Por ejemplo, si usted no tiene su propia impresora, no deje ejecutando cupsd asumiendo que algún día usted la comprará.

Lo mismo para portmap. Si usted no tiene montado un volumen NFS o usa el NIS (el servicio ypbind) entonces portmap debe ser deshabilitado.

Red Hat Linux viene con tres programas designados para levantar o bajar los servicios. Estos son **"Services Configurations Tool"** (redhat-config-services), ntsysv, y chkconfig.

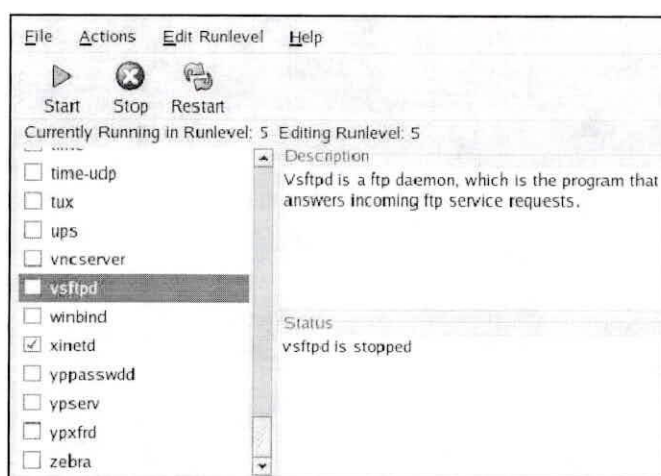


Figura 4-14. Herramienta de Configuración de Servicios

Si usted no está seguro que función tiene un servicio, **"Services Configurations Tool"** tiene una descripción, tal como se muestra en la figura de arriba, la cual podría ser de mucho uso.

No es suficiente chequear para ver cual servicio de red está disponible. Un buen administrador de sistemas debe chequear también que puertos están abiertos y escuchando.

SERVICIOS INSEGUROS

Potencialmente, cualquier servicio de red es inseguro. Por eso es muy importante bajar los servicios que no son usados. Las vulnerabilidades de los servicios son rebeladas y parchadas rutinariamente. De esta manera es importante mantener actualizados los paquetes asociados a cualquier servicio.

Algunos protocolos de red son inherentemente más inseguros que otros. Estos incluyen cualquier servicio que hagan las siguientes cosas:

Pasar los nombres de usuarios y password a través de la red descriptados.- Muchos protocolos viejos tales como Telnet y FTP no encriptan la sesión de autenticación y deben ser evitados en cualquier momento posible.

Pasar datos sensitivos a través de la red descriptados.- Muchos protocolos pasan datos a través de la red descriptados estos protocolos incluyen Telnet, FTP, HTTP y SMTP.

Muchos sistemas de archivos de red, tales como NFS (Network File System) y SMB (Server messages Blocks), también pasan información a través de la red descriptada. Es responsabilidad de los usuarios usar estos protocolos para delimitar que tipos de datos son transmitidos.



Realizar los servicios de vaciado de memoria remotamente, como *netdump* pasa el contenido de la memoria a través de la red descryptado. El vaciado de memoria puede contener passwords, aún peor entradas de bases de datos y otra información sensitiva.

Otros servicios como *finger* y *rwhod* revelan información acerca de los usuarios del sistema. Ejemplos de servicios inherentemente inseguros incluyen lo siguiente:

rlogin

rsh

telnet

vsftpd

wu-ftp



Todos los accesos remotos y los programa shell (rlogin, rsh y telnet) deben ser evitados a favor de ssh.

FTP no es inherentemente peligroso para la seguridad de un sistema como shell remoto, pero los servidores FTP deben ser cuidadosamente configurados y monitorizados para evitar problemas.

Servicios que deben ser cuidadosamente implementados y detrás de un firewall incluyen:

finger
identd
netdump
netdump-server
nfs
portmap
rwhod
sendmail
smb (samba)
yppasswdd
ypserv
ypxfrd

4.7.2.7. HERRAMIENTAS DE COMUNICACIÓN DE SEGURIDAD MEJORADAS

Así como el tamaño y popularidad del internet ha crecido, también ha crecido la interceptación de las comunicaciones. Por años las herramientas han sido desarrolladas para encriptar las comunicaciones cuando son transmitidas a través de la red.

Red Hat Linux viene con dos herramientas básicas que usan algoritmos de alto nivel y basados en criptografías de clave pública para proteger la información cuando esta viaja a través de la red.

OpenSSH.- Una implementación gratuita del protocolo SSH para encriptar la comunicación de Red.

Gnu Privacy Guard (GPG).— Una implementación gratuita de la aplicación de encriptación PGP (Pretty Good Privacy) para encriptar los datos.

OpenSSH es uno de los métodos más seguros para acceder una máquina remota y reemplazar los servicios antiguos y desencryptados como telnet y rsh. OpenSSH incluye un servicio llamado sshd y tres aplicaciones clientes de línea de comando:

- ♦ **Ssh.**— Una consola remota segura de acceso al cliente.
- ♦ **Scp.**— Un comando de copia remota seguro.
- ♦ **Sftp.**— Un cliente seguro seudo-ftp que permite sesiones interactivas de transferencia de archivos.

Es altamente recomendado que cualquier comunicación remota con un sistema Linux sea hecha usando el protocolo ssh.

Importante

A pesar de que sshd es un servicio inherentemente seguro, el servicio debe mantenerse actualizado para prevenir amenazas de seguridad.

GPG es una buena forma de mantener confidenciales los datos privados. Puede ser usado para dos cosas, enviar por e-mail datos sensitivos a través de la red pública y para proteger datos sensitivos en un disco duro.

4.7.3. SEGURIDADES DEL SERVIDOR

Cuando un sistema es usado como servidor en una red pública, este se transforma en un blanco de ataques. Por esta razón configurar el sistema y bajar los servicios es de importancia primordial para el administrador de sistemas.



CIB-ESPOL

Antes de profundizar en temas específicos, usted debe revisar los siguientes temas generales para asegurar la seguridad del servidor:

- ♦ Mantenga todos los servicios actualizados para protegerse contra las últimas vulnerabilidades.
- ♦ Use protocolos seguros cuando sea posible.
- ♦ Sirva un solo tipo de servicio de red por máquina cuando sea posible.
- ♦ Monitoree todos los servidores cuidadosamente por actividades sospechosas.

ASEGURANDO LOS SERVICIOS CON TCP WRAPPERS Y XINETD

TCP Wrappers provee un control de acceso para una variedad de servicios. Muchos de los servicios modernos de red tal como SSH, Telnet y FTP, hace uso de TCP Wrappers, el cual permanece a la guardia entre un requerimiento entrante y el servicio requerido.

Los beneficios ofrecidos por TCP Wrappers son mejorados cuando son usados en conjunto con Xinetd, un súper servicio que provee acceso, registro, redireccionamiento, adicionales y control de la utilización de recurso.

MEJORANDO LA SEGURIDAD CON TCP WRAPERS

TCP Wrappers es capaz de mucho más que denegar el acceso a los servicios. Puede ser usado para enviar anuncios (banners) de conexiones, alarmas de



CIB-ESPOL

ataques de un host particular y mejorar la funcionalidad de registro. Para ver la lista de la funcionalidad de TCP Wrappers y el control de lenguaje, refiérase a la página man *hosts_options* en el sistema Linux.

TCP WRAPPERS Y EL ANUNCIO DE CONEXIÓN

Enviar las conexiones de clientes a un servicio, un anuncio intimidante es una buena forma de ocultar que sistema el servidor está ejecutando mientras se le permite a un atacante potencial saber que el administrador del sistema está vigilando. Para implementar un anuncio TCP Wrappers para un servicio, use la opción *banner*.

Este ejemplo implementa un anuncio para vsftpd. Para empezar usted debe crear un archivo de anuncio. Este puede estar en cualquier directorio del sistema, este debe llevar el mismo nombre del demonio. Este ejemplo nombrará el archivo */etc/banners/vsftpd*.

El contenido del archivo se mostrará así:

```
220-Hello, %c
220-All activity on ftp.example.com is logged.
220-Act up and you will be banned.
```

El toquen *%c* provee una variedad de información al cliente tal como el nombre del usuario y el nombre del host, o el nombre de usuario y la dirección IP para hacer la conexión incluso más intimidante.

Para que este anuncio sea presentado a las conexiones entrantes añada la siguiente línea al archivo */etc/hosts.allow*:

vsftpd : ALL : banners /etc/banners/

TCP WRAPPERS Y LAS ADVERTENCIAS DE ATAQUES

Si un host o una red particular ha sido vista atacando al servidor, TCP Wrappers puede ser usado para advertir los ataques subsecuentes desde un host o una red a través de una directiva spawn.

En este ejemplo asuma que el cracker de la red 206.182.68.0/24 ha sido visto intentando atacar el servidor. Ubicando la siguiente línea en el archivo /etc/hosts.deny, el intento de conexión es denegado y registrado en un archivo especial.

```
ALL : 206.182.68.0 : spawn /bin/ 'date' %c %d >> /var/log/intruder_alert
```

El toquen %d provee el nombre del servicio que el atacante está tratando de acceder.

Para permitir la conexión y registrarla, ubique la directiva spawn en el archivo /etc/hosts.allow.

Importante

Desde que la directiva spawn ejecuta cualquier comando shell, usted puede crear un script especial para que le notifique o ejecute una cadena de comandos en el evento de que un cliente particular intente conectarse al servidor.

TCP WRAPPERS Y EL ACCESO MEJORADO

Si ciertos tipos de conexiones son más preocupantes que otras el nivel de acceso puede ser elevado para ese servicio a través de la opción severity.



En este ejemplo asuma que alguien intenta conectarse al puerto 23 (el puerto Telnet) en un servidor FTP es un cracker. Para denotar esto ubique una bandera *emerg* en el archivo de acceso en vez de la bandera por defecto, *info*, y deniegue la conexión.

Para hacer esto ubique la siguiente línea en el archivo `/etc/hosts.deny`:

```
in.telnetd : ALL : severity emerg
```

Esto usará la facilidad de acceso por defecto *authpriv*, pero elevará la prioridad del valor por defecto de *info* a *emerg*.



MEJORANDO LA SEGURIDAD CON XINETD

CIB-ESPOL

El súper servidor Xinetd es otra herramienta útil para controlar el acceso hacia sus servicios subordinados. Xinetd puede ser usado para configurar un servicio como una trampa y controlar la cantidad de recursos, cualquier servicio Xinetd puede usarse para impedir un ataque de denegación de servicios.

CONFIGURANDO UNA TRAMPA

Una característica importante de Xinetd es su habilidad para añadir host hacia una lista global `no_access`. A los hosts en esta lista se les deniega las conexiones subsecuentes hacia los servicios administrados por Xinetd por una cantidad de tiempo específica o hasta que Xinetd sea reiniciado. Esto es realizado usando el atributo `SENSOR`. Esta técnica es una manera fácil de bloquear los hosts que intentan hacer un análisis de puertos hacia el servidor.

El primer paso para configurar un SENSOR es escoger un servicio que usted no piensa usar. Para este ejemplo Telnet será usado.

Edite el archivo `/etc/xinetd/telnet`, y cambie la línea *flags* para que se vea:

`flags = SENSOR`

Añada la siguiente línea:

`deny_time = 30`

Esto denegará al host que intente conectarse al puerto por 30 minutos. Otro valor aceptable para el atributo `deny_time` es `FOREVER`, el cual mantiene la prohibición en efecto hasta que Xinetd sea reiniciado, y `NEVER`, el cual permite la conexión y la registra.

Finalmente la última línea debería leerse:

`disable = no`

Usar `SENSOR` es una buena forma de detectar y parar las conexiones de un host ilegal, el cual tiene dos inconvenientes:

- Este no trabajará contra un análisis cauteloso.
- Un atacante que sabe que usted está ejecutando `SENSOR` puede montar un ataque de denegación de servicio contra un host particular forzando su dirección IP y conectándose al puerto prohibido.

CONTROLANDO LOS RECURSOS DEL SERVIDOR

Otra característica importante de Xinetd es su habilidad de controlar la cantidad de servicios de recursos bajo su control que puede utilizar.

Esto se hace a través de la siguiente directiva:

- ♦ **cps = <number_of_connections> <wait_period>.-** Dicta las conexiones permitidas hacia un servicio por segundo. Esta directiva acepta solo valores enteros.
- ♦ **instances = <number_of_connections>.-** Dicta el número total de conexiones permitidas hacia el servicio. Esta directiva acepta un valor entero o UNLIMITED.
- ♦ **per_source = <number_of_connections>.-** Dicta las conexiones permitidas hacia un servicio por cada host. Esta directiva acepta un valor entero o UNLIMITED.
- ♦ **rlimit_as = <number[K|M]>.-** Dicta la cantidad de espacio de direcciones de memoria que el servicio puede ocupar en kilobytes o megabytes. Esta directiva acepta un valor entero o UNLIMITED.
- ♦ **rlimit_cpu = <number_of_seconds>.-** Dicta la cantidad de tiempo en segundos que un servicio puede ocupar del CPU. Esta directiva acepta un valor entero o UNLIMITED.

Usando estas directivas puede ayudarnos a prevenir a cualquier servicio Xinetd de sobrecargar al sistema resultando en un ataque de denegación de servicios.

4.7.3.1. ASEGURANDO PORTMAP

El servicio Portmap es un demonio de asignación de puerto dinámico para los servicios RPC tal como NIS y NFS. Este tiene un mecanismo de autenticación débil y tiene la habilidad de asignar un amplio rango de puertos para los servicios que controla. Por estas razones es difícil asegurarlo.



Si usted está ejecutando servicios RPC, usted debe seguir las siguientes reglas básicas.

PROTEGER PORTMAP CON TCWRAPPERS

Es importante usar Tcwrappers para limitar que red o host tienen acceso al servicio Portmap porque este no tiene construido un mecanismo de autenticación. Además, usa solo direcciones ip para limitar el acceso al servicio. Evitar estos nombres de hosts, porque estos pueden ser olvidados falseados a través de envenenamiento DNS y otros métodos.

PROTEGER PORTMAP CON IPTABLES

Para restringir el acceso hacia el servicio Portmap es buena idea añadir reglas IPTables hacia el servidor restringiendo el acceso hacia redes específicas. Abajo hay dos ejemplos de comandos IPTables que permiten conexiones tcp hacia el servicio Portmap (escuchando en puerto 111) de la red (ficticia) 192.168.0/24 y desde el localhost (el cual es necesario para el servicio sgi_fam por medio de Nautilus). Todos los demás paquetes son borrados.

```
iptables -A INPUT -p tcp -s! 192.168.0.0/24 --dport 111 -j DROP
iptables -A INPUT -p tcp -s 127.0.0.1 --dport 111 -j ACCEPT
```

De manera similar limita el tráfico udp usando el siguiente comando:

```
iptables -A INPUT -p udp -s! 192.168.0.0/24 --dport 111 -j DROP
```



CIB-ESPOL

4.7.3.2. ASEGURANDO NIS

NIS permanece para el servicio de información de red (Network Information Services). Es un servicio RPC llamado ypserv el cual es usado en conjunto con Portmap y otros servicios relacionados para distribuir mapas de nombres de usuarios, passwords, y otra información sensitiva hacia cualquier otra computadora que dice estar dentro de su dominio.

Un servidor NIS está compuesto de muchas aplicaciones, estas incluyen lo siguiente:

`/usr/sbin/rpc.yppasswdd`.- También llamado el servicio yppasswdd, este demonio permite a los usuarios cambiar sus passwords NIS.

`/usr/sbin/rpc.ypxfrd`.- También llamado el servicio ypxfrd, este demonio es responsable de la transferencia de mapas NIS a través de la red.

`/usr/sbin/yppush`.- Esta aplicación propaga los cambios de las bases de datos NIS hacia múltiples servidores NIS.

`/usr/sbin/ypserv`.- Este es el demonio del servidor NIS.



NIS es inseguro por los estándares actuales. Este no posee mecanismos de autenticación de hosts y pasa toda su información a través de la red desencryptada incluyendo resúmenes de passwords (hash). Como resultado, cuidado extremo se debe tener para configurar una red que use NIS. Para

complicar más la situación, la configuración por defecto de NIS es inherentemente insegura.

PLANEANDO LA RED CUIDADOSAMENTE

Debido a que NIS pasa información sensible descriptada a través de la red, es importante que el servicio corra a lado de un firewall y una red segura y segmentada. Cada vez que la información NIS es pasada a través de una red insegura corre el riesgo de ser interceptada. Un diseño cuidadoso de la red con estas consideraciones puede ayudar a prevenir vulnerabilidades de seguridad severas.

USE UN PASSWORD COMO NOMBRE DE DOMINIO NIS Y NOMBRE DE HOST.

Cualquier máquina dentro del dominio NIS puede usar un comando para extraer información desde el servidor sin autenticación, tanto como el usuario conozca el nombre del host DNS y el nombre del dominio NIS del servidor NIS.

Por el momento, si alguien se conecta a una computadora laptop dentro de una red o ingresa ilegalmente desde fuera de la red (se roba una dirección ip interna) el siguiente comando rebelará el mapa /etc/passwd:

```
ypcat -d <NIS_domain> -h <DNS_hostname> passwd
```



CIB-ESPOL

Si el atacante es un usuario root ellos pueden obtener el archivo / etc/shadow tipeando el siguiente comando:


```
ypcat -d <NIS_domain> -h <DNS_hostname> shadow
```

Nota

Si se usa kerberos, el archivo /etc/shadow no es guardado dentro del mapa NIS.

Para dificultar el acceso al mapa NIS a un atacante, cree una cadena aleatoria para el nombre del host DNS, tal como o7hfawtgmhgw.domain.com. Similarmente, cree un nombre de dominio en NIS aleatorio que sea diferente. Esto hará mucho más difícil que un atacante pueda acceder al servidor NIS.

EDITE EL ARCHIVO /var/yp/securenets

NIS escuchará a todas las redes si es que el archivo /var/yp/securenets está en blanco o no existe (este es el caso después de una instalación por defecto). Una de las primeras cosas que usted debe hacer es poner una máscara de red y la red dentro del archivo en el cual ypserv solamente responderá hacia los requerimientos desde la red apropiada.

Abajo hay un ejemplo de una entrada del archivo /var/yp/securenets:

```
255.255.255.0      192.168.0.0
```

Advertencia

Nunca levante un servidor NIS por primera vez sin haber creado el archivo /var/yp/securenets.

Esta técnica no provee protección de un ataque de falsificación ip, pero este por lo menos limita en que redes el servidor NIS servirá.

ASIGNANDO PUERTOS ESTÁTICOS Y USANDO REGLAS IPTABLES

Todos los servidores relacionados con NIS se les puede asignar puertos específicos excepto para el demonio `rpc.yppasswdd` – el cual permite a los usuarios cambiar su password de acceso. Asignando los puertos a los otros dos demonios de los servidores NIS, `rpc.ypxfrd` y `ypserv`, le permite crear reglas de firewall para proteger más el demonio del servidor NIS contra intrusos.

Para hacer esto, añade la siguiente línea `/etc/sysconfig/network`:

```
YPSERV_ARGS="-p 834"
```

```
YPXFRD_ARGS="-p 835"
```

La siguiente regla IPtables puede ser considerada para reforzar hacia cual red el servidor escuchará para estos puertos:

```
iptables -A INPUT -p ALL -s! 192.168.0.0/24 --dport 834 -j DROP
```

```
iptables -A INPUT -p ALL -s! 192.168.0.0/24 --dport 835 -j DROP
```



CIB-ESPOL

USE AUTENTICACIÓN KERBEROS

Uno de los más notorios desperfectos inherentes cuando **NIS** es usado para autenticación es que cuando un usuario accesa a una máquina, el resumen del password desde el mapa `/etc/shadow` es enviado a través de la red. Si un intruso tiene acceso al demonio NIS y captura el tráfico de la red, nombres de usuarios y passwords pueden ser tranquilamente recolectados. Con suficiente tiempo un

programa crackeador de password puede descifrar passwords débiles, y un atacante puede ganar acceso hacia una cuenta válida en la red.

Desde que kerberos usa criptografía de clave secreta, resúmenes de passwords no son enviados a través de la red, haciendo el sistema mucho más seguro.

4.7.3.3. ASEGURANDO NFS.

El sistema de archivos de red o NFS es un servicio RPC usado en conjunto con Portmap para proveer un sistema de archivos accesible hacia la red para máquinas clientes.

PLANEAR LA RED CUIDADOSAMENTE

Debido a que NFS pasa toda la información descriptada a través de toda la red es importante que el servicio sea ejecutado a lado de un firewall y de una red segura y segmentada. Cada vez que la información es pasada a través de una red insegura NFS, esta corre riesgo de ser interceptada. Un cuidadoso diseño de la red con estas consideraciones pueden ayudar a prevenir vulnerabilidades de seguridad.

CUIDADO CON LOS ERRORES DE SINTAXIS

El servidor NFS determina que sistema de archivos se debe exportar y a que host se debe exportar estos directorios a través del archivo `/etc/exports`, comparta el directorio `/tmp/nfs/` al host `bob.example.com`, con permisos de lectura y escritura.

```
/tmp/nfs/ bob.example.com(rw)
```

Esta línea en el archivo `/etc/exports`, dicho de otra manera, comparte el mismo directorio hacia el host `bob.example.com` con permisos de solo lectura y lo comparte hacia el mundo con permisos de lectura y escritura debido a que existe un carácter de espacio después del nombre del host.

```
/tmp/nfs/ bob.example.com (rw)
```

Es una buena práctica chequear cualquier configuración NFS compartida usando el comando `showmount` para verificar que está haciendo compartido:

```
showmount -e <hostname>
```



CIB-ESPOL

NO USE LA OPCIÓN `no_root_squash`

Por defecto NFS comparte los cambios de los archivos de la cuenta `root` con el usuario `nfsnobody`. Esto previene la subida de programas con la configuración del `setuid`.

4.7.3.4. ASEGURANDO FTP

El protocolo de transferencia de archivo FTP es un viejo protocolo tcp designado para transferir archivos desde la red. Debido a que todas las transacciones con el servidor, incluyendo autenticación de usuario son descriptadas, es considerado un protocolo inseguro y debe ser cuidadosamente considerado.

Red Hat Linux provee tres servidores FTP.

gssftpd.- Un demonio FTP basado en Xinetd kerberizado el cual no pasa la información de autenticación a través de la red.

Acelerador de contenido Red Hat (tux).- Un espacio de kernel para el servidor web con capacidades FTP.

Vsftpd.- Una implementación orientada a la seguridad e individualidad de un servicio FTP.

Las siguientes guías de seguridad son para configurar los servicios wu-ftp y vsftpd.

Advertencia

Si usted activa ambos servicios wu-ftp y vsftpd, el servicio basado en Xinetd wu-ftp manejará las conexiones FTP.

ANUNCIOS DE SALUDOS FTP (BANNERS GREETING)

Antes de enviar un nombre de usuario y password, a todos los usuarios se les muestra un anuncio de saludo. Por defecto este anuncio incluye información de la versión de mucha ayuda para los crackers que intentan identificar las debilidades en un sistema.

Para cambiar el anuncio de saludo para vsftpd, añada la siguiente directiva al archivo /etc/vsftpd/vsftpd.conf:

ftpd_banner= <insert_greeting_here>



CIB-ESPOL

Reemplace <insert_greeting_here> en la directiva de debajo con el texto de su mensaje de saludo.

Para cambiar el anuncio de saludo para wu-ftp d aña da la siguiente directiva al archivo /etc/ftpusers:

```
greeting text <insert_greeting_here>
```

Reemplace <insert_greeting_here> en la directiva de arriba con el texto de su mensaje de saludo.

Para anuncios de varias líneas es mejor usar un archivo de anuncios. Para simplificar la administración de múltiples anuncios nosotros ubicaremos todos los anuncios en un nuevo directorio llamado /etc/banners/ftp.msg. Abajo hay un ejemplo de cómo el archivo debería verse:

```
#####  
# Hello, all activity on ftp.example.com is logged. #  
#####
```

Para referenciar este archivo de anuncio de saludo para vsftpd, aña da la siguiente directiva al archivo /etc/vsftpd/vsftpd.conf:

```
banner_file=/etc/banners/ftp.msg
```

Para referenciar este archivo de anuncio de saludo para wu-ftp d, aña da la siguiente directiva al archivo /etc/ftpusers:

```
greeting terse  
banner /etc/banners/ftp.msg
```



CIB-ESPOL

ACCESO ANÓNIMO

Para `wu-ftp` y `vsftpd`, la presencia del directorio `/var/ftp/` activa la cuenta anónima.

La manera más fácil de crear este directorio es instalar el paquete `vsftp`. Este paquete configura un árbol de directorio para los usuarios anónimos y configura los permisos, como solo de lectura para los usuarios anónimos.

Precaución

Si habilita el acceso anónimo a un servidor ftp, sea cuidadoso en donde usted almacena los datos sensitivos.

SUBIR ARCHIVOS ANÓNIMAMENTE

Si usted quiere permitir a los usuarios anónimos subir archivos, es recomendado que usted cree un directorio de solo escritura dentro del directorio `/var/ftp/pub/`.

Para hacer esto tipee:

```
mkdir /var/ftp/pub/upload
```

Luego cambie los permisos para que el usuario anónimo no pueda ver que es lo que está dentro del directorio tipeando:

```
chmod 730 /var/ftp/pub/upload
```

Una larga lista de formato del directorio se debe ver así:

```
drwx-wx---  2  root    ftp      4096    Feb 13 20:05 upload
```

Advertencia

Los administradores que permitan a los usuarios anónimos leer y escribir en los directorios frecuentemente encuentran que sus servidores se transforman en un repositorio de software robado.

Adicionalmente, sobre vsftp, añade la siguiente línea al archivo /etc/vsftp/vsftp.conf:

anon_upload_enable=YES

CUENTAS DE USUARIOS

Debido a que FTP pasa los nombres de usuarios y los passwords descriptados a través de la red insegura para autenticación, es buena idea denegar el acceso a los usuarios del sistema hacia el servidor desde sus cuentas de usuarios.

Para deshabilitar cuentas de usuarios en wu-ftpd, añade la siguiente directiva /etc/ftpusers:

deny-uid *



CIB-ESPOL

Para deshabilitar cuentas de usuarios en vsftpd añade la siguiente directiva al archivo /etc/vsftpd/vsftpd.conf:

local_enable=NO

RESTRINGIENDO CUENTAS DE USUARIOS

La manera más fácil de deshabilitar un grupo específico de cuentas, como el usuario root y aquellos que tienen privilegios sudo de acceder a un servidor ftp es usar un archivo de lista PAM. El archivo de configuración PAM para wu-ftpd es /etc/pam.d/ftp. El archivo de configuración PAM para vsftpd es /etc/pam.d/vsftpd.

También es posible desarrollar este test directamente dentro de cada servicio.

Para deshabilitar una cuenta de usuario específica en wu-ftpd, añade el nombre de usuario al archivo /etc/ftpusers:

Para deshabilitar una cuenta de usuario específica en vsftpd, añade el nombre de usuario al archivo /etc/vsftpd.ftpusers:

USAR TCP WRAPPERS PARA CONTROLAR EL ACCESO

Usted puede usar TCP Wrappers para controlar el acceso hacia el demonio FTP.

USE XINETD PARA CONTROLAR LA CARGA

Si usa wu-ftpd, usted puede usar Xinetd para controlar la cantidad de recursos que el servidor FTP consume y también puede limitar los efectos producidos por un ataque de denegación de servicios.



4.7.3.5. VERIFICANDO QUE PUERTOS ESTÁN ESCUCHANDO

Una vez que usted ha configurado el servicio en la red es importante mantener tablas en las cuales los puertos son actualmente escuchados en la interfaces de red del sistema. Cualquier puerto abierto puede ser evidencia de un intruso.

Existen dos acercamientos básicos para listar los puertos que son escuchados en la red. El acercamiento menos confiable es consultar la cola de la red digitando el comando como por ejemplo `netstat -an` ó `lsof -i`. Este método es menos confiable debido a que estos programas no se conectan a la máquina desde la red, en vez de esto chequean para ver que se está ejecutando en el sistema. Por esta razón, estas aplicaciones son frecuentemente blancos de reemplazo para los intrusos. De esta forma los crackers pueden intentar cubrir sus huellas si es que ellos abren un puerto de red no autorizado.

Una manera más confiable de chequear que puertos son escuchados en la red es usar un examinador de puerto como `nmap`.

El siguiente comando de consola determina que puertos son escuchados por la conexiones tcp de una red:

```
nmap -sT -O localhost
```

La salida de este comando se parece a lo siguiente:



CIB-ESPOL

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1596 ports scanned but not shown below are in state: closed)
Port      State Service
22/tcp    open  ssh
```

```

111/tcp      open  sunrpc
515/tcp      open  printer
834/tcp      open  unknown
6000/tcp     open  X11

```

Remote OS guesses: Linux Kernel 2.4.0 or Gentoo 1.2 Linux 2.4.19 rc1-rc7)

Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds

Esta salida muestra que el sistema está ejecutando portmap debido a la presencia del servicio sunrpc. Sin embargo existe también un servicio misterioso en el puerto 834. Para chequear si el puerto está asociado con la lista oficial de servicios conocidos tipee:

```
cat /etc/services | grep 834
```

Este comando no retorna salida. Esto indica que mientras el puerto está en un rango reservado (de 0 hasta 1023) y requiere acceso root para abrirlo, este no está asociado con un servicio conocido.

Luego, usted puede chequear por información acerca del puerto usando netstat o lsof. Para chequear el puerto 834 usando netstat, use el siguiente comando:

```
netstat -anp | grep 834
```

El comando retorna la siguiente salida:



CIB-ESPOL

```
tcp 0 0 0.0.0.0:834 0.0.0.0:* LISTEN 653/ypbind
```

La presencia del puerto abierto en netstat es tranquilizador porque un cracker abriendo clandestinamente en un sistema hackeado probablemente no permitiría ser rebelado a través de este comando. Además, la opción [p] revela el ID del proceso (PID) del servicio que abrió el puerto. En este caso el puerto abierto pertenece a ypbind (NIS) el cual es un servicio RPC manejado en conjunto con el servicio portmap.

El comando lsof revela información similar debido a que es capaz de enlazar un puerto abierto hacia un servicio:

```
lsof -i | grep 834
```

Abajo está una porción relevante de la salida para este comando:

```
ypbind      653    0      7u    IPv4  1319  TCP *:834 (LISTEN)
ypbind      655    0      7u    IPv4  1319  TCP *:834 (LISTEN)
ypbind      656    0      7u    IPv4  1319  TCP *:834 (LISTEN)
ypbind      657    0      7u    IPv4  1319  TCP *:834 (LISTEN)
```

Como usted puede ver, estas herramientas pueden revelar mucha información acerca del estado de los servicios que se están ejecutando en la máquina. Estas herramientas son flexibles y pueden proveer abundante información acerca de los servicios de red y las configuraciones. Usted puede consultar las páginas man para lsof, netstat, nmap y services en el sistema operativo.

4.8. SERVIDOR WINDOWS NT

4.8.1. INTRODUCCIÓN

El sistema operativo Microsoft® Windows NT® proporciona un completo conjunto de características de seguridad. No obstante, la configuración predeterminada de fábrica no es muy elevada, sobre todo en el producto Workstation. Esto es debido a que el sistema operativo se comercializa partiendo de la base de que, por lo general, los clientes no desean estar sometidos a las complicaciones de un sistema muy restrictivo, aunque sea seguro. Esta suposición ha cambiado con el paso del tiempo, debido a que Windows NT ganó en popularidad gracias, en buena parte, a sus características de seguridad. Microsoft investiga una configuración predeterminada más segura para futuras versiones. Mientras tanto, en esta documento acerca del producto se tratan diversas cuestiones de seguridad relacionadas con la configuración de todos los productos del sistema operativo Windows NT versión 4.0 para un entorno informático de mediana seguridad.

4.8.2. CONFIGURACIÓN ADICIONAL A IMPLEMENTAR

4.8.2.1. AUDITORÍAS

Las Auditorías pueden informarle acerca de las acciones que supongan un riesgo para la seguridad, además de identificar las cuentas de usuario desde las que se emprendieron acciones de Auditoría. Tenga en cuenta que la Auditoría sólo indica qué cuentas de usuario fueron utilizadas para los sucesos auditados. Si las contraseñas están protegidas correctamente, esto indicará también qué usuario intentó los sucesos auditados. Sin embargo, si se ha sustraído una contraseña o



CIB-ESPOL

si se realizó alguna acción mientras el usuario mantenía una sesión activa, pero no se encuentra cerca del equipo, es posible que la acción haya sido iniciada por una persona distinta del titular de la cuenta de usuario.

Cuando establezca una directiva de Auditoría, necesitará ponderar el costo (de espacio de disco y ciclos de CPU) de las distintas opciones de Auditoría con respecto a las ventajas de esas opciones. Normalmente, deseará auditar al menos los intentos de inicio de sesión sin éxito, los intentos de acceso a datos confidenciales y los cambios en la configuración de seguridad. Éstas son algunas de las amenazas a la seguridad y el tipo de la Auditoría que puede ayudar a realizar un seguimiento de las mismas:



Amenaza	Acción
Intrusión mediante contraseñas aleatorias	Habilitar la Auditoría de errores para sucesos de inicio y final de sesión.
Intrusión mediante contraseña sustraída	Habilitar la Auditoría de acceso correcto para sucesos de inicio y final de sesión. Las entradas de inicio de sesión no distinguirán entre usuarios reales e impostores. Lo que buscará en este caso será una actividad inusual en las cuentas de usuario, como inicios de sesión a horas poco habituales o en días en los que no cabría esperar actividad.
Uso indebido de privilegios administrativos por parte de usuarios autorizados	Habilite la Auditoría de accesos correctos para evaluar el uso de los derechos de los usuarios, la administración de usuarios y grupos, los cambios de directivas de seguridad, el reinicio, el cierre y los sucesos del sistema. (Nota: Debido al gran número de sucesos que pueden quedar registrados, Windows NT no suele auditar el uso de los derechos de copia de seguridad de archivos y directorios ni el de restauración de archivos y directorios. En el Apéndice B, "Security In a Software Development Environment", se explica cómo habilitar la Auditoría del uso de estos derechos).
Brote de epidemia de virus	Habilite la Auditoría de escritura correcta y fallida en los archivos de programa, tales como los que tienen extensiones .exe y .dll. Habilite la Auditoría de seguimiento correcto o fallido de procesos. Ejecute

Amenaza	Acción
	programas sospechosos y examine en el registro de seguridad los intentos de modificar archivos de programas o de crear procesos inesperados. Tenga en cuenta que todos estos parámetros de configuración generan un gran número de registros de suceso durante el uso normal del sistema. Sólo deberá utilizarlos cuando supervise activamente el registro del sistema.
Acceso inadecuado a los archivos confidenciales	Habilite la Auditoría de sucesos de acceso correcto y fallido a objetos y archivos, y utilice el Administrador de archivos para habilitar la Auditoría de acceso correcto y fallido de lectura y escritura en archivos confidenciales por parte de usuarios o grupos sospechosos.
Acceso inadecuado a impresoras	Habilite la Auditoría de sucesos de acceso correcto y fallido a objetos y archivos, y utilice el Administrador de impresión para habilitar la Auditoría de acceso correcto y fallido a las impresoras por parte de usuarios o grupos sospechosos.

Tabla 4-21. Auditoría de Windows NT

4.8.2.2. PROTEGER ARCHIVOS Y DIRECTORIOS

Entre los archivos y directorios que se deben proteger se encuentran los que componen el propio software del sistema operativo. El conjunto de permisos estándar en los archivos de sistema y en los directorios proporciona un grado de seguridad razonable sin que ello afecte a la facilidad de uso del equipo. Sin embargo, para las instalaciones con un alto nivel de seguridad, tiene la posibilidad de establecer además permisos de directorio para todos los subdirectorios y archivos existentes, tal como se muestra en la siguiente lista, inmediatamente después de que se instale Windows NT. Asegúrese de aplicar permisos a los directorios principales antes de aplicarlos a los subdirectorios.

Aplique primero los siguientes mediante el editor ACL:

Directorio	Permisos
\WINNT y todos los subdirectorios que contiene.	Administradores: Control total CREADOR PROPIETARIO: Control total Todos: Lectura

	SISTEMA: Control total
--	------------------------

Tabla 4-22. Auditoría de Windows NT

Ahora, en el árbol \WINNT, aplique las siguientes excepciones a la configuración de seguridad general:

Directorio	Permisos
\WINNT\REPAIR	Administradores: Control total
\WINNT\SYSTEM32\CONFIG	Administradores: Control total CREADOR PROPIETARIO: Control total Todos: Listado SISTEMA: Control total
\WINNT\SYSTEM32\SPOOL	Administradores: Control total CREADOR PROPIETARIO: Control total Todos: Lectura Usuarios avanzados: Cambio SISTEMA: Control total
\WINNT\COOKIES \WINNT\FORMS \WINNT\HISTORY \WINNT\OCCACHE \WINNT\PROFILES \WINNT\SENDTO \WINNT\Temporary Internet Files	Administradores: Control total CREADOR PROPIETARIO: Control total Todos: Acceso especial a directorios: Lectura, Escritura y Ejecutar, Acceso especial a archivos: Ninguno Sistema: Control total

Tabla 4-23. Auditoría de Windows NT

En el directorio raíz de la partición de sistema de los equipos Pentium e Intel 80486 existen varios archivos críticos del sistema operativo. En las instalaciones de alta seguridad tiene la posibilidad de asignar los siguientes permisos a estos archivos:

Archivo	Permisos de nivel C2
\Boot.ini, \Ntdetect.com, \Ntldr	Administradores: Control total SISTEMA: Control total
\Autoexec.bat, \Config.sys	Todos: Lectura Administradores: Control total SISTEMA: Control total
Directorio \TEMP	Administradores: Control total SISTEMA: Control total CREADOR PROPIETARIO: Control total

**CIB-ESPOL**

	Todos: Acceso especial a directorios: Lectura, Escritura y Ejecutar, Acceso especial a archivos: Ninguno
--	--

Tabla 4-24. Auditoría de Windows NT

Para ver estos archivos en el Administrador de archivos, elija el comando Por tipo de archivo del menú Ver y, a continuación, active la casilla de verificación Mostrar archivos ocultos y de sistema del cuadro de diálogo Por tipo de archivo.

Tenga en cuenta que las protecciones mencionadas en esta sección están por encima de las mencionadas en la sección del nivel de seguridad estándar, entre las que se incluían la exclusividad de las particiones NTFS (excepto la partición de inicio en caso de las máquinas RISC). La partición de inicio FAT para sistemas RISC se puede configurar mediante el comando Partición del sistema segura en el menú Partición de la utilidad Administrador de discos.

También es aconsejable que los administradores examinen manualmente los permisos de varias particiones del sistema y comprueben que están debidamente protegidas para distintos accesos de usuarios en su entorno.



CIB-ESPOL

4.8.2.3. PROTEGER EL REGISTRO

Además de las consideraciones propias de una configuración de seguridad estándar, el administrador de una instalación de alta seguridad tiene la posibilidad de establecer protecciones para varias claves del Registro.

De forma predeterminada, se establecen protecciones para varios componentes del Registro que permitirán que se realice el trabajo mientras se proporciona un dispositivo de seguridad de nivel estándar. Para la seguridad de alto nivel, quizá

desea asignar derechos de acceso a claves de Registro específicas. Esta operación debe realizarse con precaución, ya que los programas que los usuarios necesitan para realizar sus trabajos suelen precisar acceso a diversas claves en nombre del usuario.

Para cada una de las claves enumeradas a continuación, realice el cambio siguiente:

ACCESO PERMITIDO

Valor de consulta del grupo Todos, Enumerar subclaves, Control de notificación y lectura en a clave:

HKEY_LOCAL_MACHINE del cuadro de diálogo Local Machine:
 \Software

Se recomienda este cambio. Bloquee el sistema de modo que no todos los usuarios puedan instalar software. Tenga en cuenta que no se recomienda que se bloquee todo el árbol mediante esta configuración, ya que algunos componentes de software pueden quedar inutilizados.

\Software\Microsoft\RPC (y sus subclaves)

De esta manera se bloquean los servicios RPC.

\Software\Microsoft\Windows NT\ CurrentVersion
 \Software\Microsoft\Windows NT\ CurrentVersion\Profile List
 \Software\Microsoft\Windows NT\ CurrentVersion\AeDebug
 \Software\Microsoft\Windows NT\ CurrentVersion\Compatibility
 \Software\Microsoft\Windows NT\ CurrentVersion\Drivers
 \Software\Microsoft\Windows NT\ CurrentVersion\Embedding
 \Software\Microsoft\Windows NT\ CurrentVersion\Fonts
 \Software\Microsoft\Windows NT\ CurrentVersion\FontSubstitutes
 \Software\Microsoft\Windows NT\ CurrentVersion\Font Drivers
 \Software\Microsoft\Windows NT\ CurrentVersion\Font Mapper
 \Software\Microsoft\Windows NT\ CurrentVersion\Font Cache

\Software\Microsoft\Windows NT\ CurrentVersion\GRE_Initialize
 \Software\Microsoft\Windows NT\ CurrentVersion\MCI
 \Software\Microsoft\Windows NT\ CurrentVersion\MCI Extensions
 \Software\Microsoft\Windows NT\ CurrentVersion\PerfLib

Considere la posibilidad de quitar el acceso de lectura para Todos en esta clave.

Esto permite a los usuarios remotos ver los datos de rendimiento de la máquina.

En vez de eso, podría otorgar acceso de lectura interactiva, que permitirá únicamente el acceso a esta clave a usuarios que inicien sesión de forma interactiva, además de los administradores y el sistema.

\Software\Microsoft\Windows NT\ CurrentVersion\Port (y todas las subclaves)
 \Software\Microsoft\Windows NT\ CurrentVersion\Type1 Installer
 \Software\Microsoft\Windows NT\ CurrentVersion\WOW (y todas las subclaves)
 \Software\Microsoft\Windows NT\ CurrentVersion\Windows3.1MigrationStatus (y todas las subclaves)
 \System\CurrentControlSet\Services\LanmanServer\Shares
 \System\CurrentControlSet\Services\UPS

Tenga en cuenta que, además de configurar la seguridad para esta clave, también es necesario proteger el archivo de comandos (si existe) asociado al servicio SAI, para que permita a los Administradores: Control total, Sistema: Sólo Control total.

En la clave HKEY_CLASSES_ROOT del cuadro de diálogo Local Machine:
 \HKEY_CLASSES_ROOT (y todas sus subclaves)
 En la clave HKEY_USERS del cuadro de diálogo Local Machine:
 \.DEFAULT



El Editor del Registro permite el acceso remoto al Registro de Windows NT. Para restringir el acceso al Registro a través de la red, utilice el Editor del Registro para crear la siguiente clave de Registro:

Sección:	HKEY_LOCAL_MACHINE
Clave:	System\CurrentcontrolSet\Control\SecurePipeServers
Nombre:	\winreg

Los permisos de seguridad establecidos para esta clave definen qué usuarios o grupos se pueden conectarse al sistema para el acceso remoto al Registro. La instalación predeterminada de Windows NT Workstation no define esta clave ni restringe el acceso remoto al Registro. Windows NT Server sólo permite el acceso remoto a la mayor parte del Registro a los administradores. Algunas rutas a las que necesitan tener acceso los usuarios que no son administradores se especifican en la clave:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths.



VER EL REGISTRO DE SUCESOS DE SEGURIDAD

La configuración predeterminada permite a los invitados y a los usuarios que establecen inicios de sesión nulos ver registros de sucesos (registros de sistema y de aplicaciones). El registro de seguridad está protegido del acceso de los invitados de forma predeterminada y puede ser visto por los usuarios que tengan el derecho de "Administrar registros de Auditoría". Los servicios del registro de sucesos utilizan la siguiente clave para restringir el acceso de los invitados a estos registros:

Sección:	HKEY_LOCAL_MACHINE
Clave:	\System\CurrentControlSet\Services\EventLog\[LogName]
Nombre:	RestrictGuestAccess
Tipo:	REG_DWORD
Valor:	1

Configure cada uno de los registros con el valor 1. El cambio tendrá efecto la siguiente vez que se inicie el sistema. Naturalmente, tendrá que cambiar la seguridad en esta clave para desautorizar el acceso a cualquier usuario que no sea administrador o el sistema, ya que, de lo contrario, algún usuario malintencionado podría restablecer estos valores.

EL SERVICIO DE PROGRAMACIÓN (COMANDO AT)

El Servicio de programación (también conocido como comando **AT**) se utiliza para programar tareas que se ejecutarán automáticamente en un momento preestablecido. Dado que la tarea programada se ejecuta en el contexto del Servicio de programación (normalmente, el contexto del sistema operativo), este servicio no se debe utilizar en un entorno con un alto nivel de seguridad.

De forma predeterminada, sólo los administradores pueden enviar comandos **AT**. Para permitir a los operadores que envíen también comandos **AT**, utilice el Editor del Registro para crear o asignar el siguiente valor de clave de Registro:

Sección:	HKEY_LOCAL_MACHINE\SYSTEM
Clave:	\CurrentControlSet\Control\Lsa
Nombre:	Submit Control
Tipo:	REG_DWORD
Valor:	1



CIB-ESPOL

No existe ningún medio para permitir a todos los demás usuarios la posibilidad de enviar comandos AT. Si se protege el Registro tal como se explica anteriormente, se restringe la modificación directa de la clave del Registro mediante el Editor del Registro.

El acceso a la clave de Registro HKEY_LOCAL_MACHINE\System\CurrentControlSet\ Services\Schedule también se debe restringir a los usuarios o grupos (preferentemente, sólo a los administradores) a los que se permite enviar trabajos al servicio programado. Los cambios surtirán efecto la próxima vez que se inicie el equipo. Quizá desee actualizar el disco de reparación de emergencia para reflejar estos cambios.

COMPARTIR ARCHIVOS DE FORMA SEGURA

El servicio nativo de uso compartido de archivos de Windows NT se proporciona mediante los servicios de redirector y servidor basados en SMB. Aunque sólo los administradores pueden crear recursos compartidos, la configuración de seguridad predeterminada del recurso compartido permite a Todos un acceso de control total. Estos permisos controlan el acceso a archivos en sistemas de archivos de bajo nivel, como FAT, que no integran mecanismos de seguridad. Los recursos compartidos en NTFS exigen la seguridad en el directorio subyacente para el que realiza la asignación. Se recomienda que se establezca un sistema de seguridad adecuado a través de NTFS, y no mediante el servicio de uso compartido de archivos.

- ♦ El Service Pack 3 para Windows NT versión 4.0 incluye varias mejoras al protocolo de uso de archivos compartidos basado en SMB. Por ejemplo, permite la autenticación mutua para ataques contra intermediario.
- ♦ También admite la autenticación de mensajes para impedir ataques de mensajes activos.

Estas medidas de seguridad se consiguen mediante la incorporación de la firma de mensajes en paquetes SMB comprobados tanto por el sistema servidor como por el cliente. Existen parámetros de clave de Registro para habilitar firmas SMB en cada extremo.

Para garantizar que el servidor SMB responde a los clientes sólo con la firma de mensajes, configure el siguiente valor de clave:

Sección:	HKEY_LOCAL_MACHINE\SYSTEM
Clave:	System\CurrentControlSet\Services\LanManServer\Parameters
Nombre:	RequireSecuritySignature
Tipo:	REG_DWORD
Valor:	1

Al configurar este valor se garantiza que el servidor se comunique sólo con los clientes que admiten la firma de los mensajes. Tenga en cuenta que esto significa que las instalaciones en las que haya varias versiones de software cliente, las versiones más antiguas no se podrán conectar a servidores en los que se haya configurado este valor de clave.

Asimismo, los clientes más preocupados por la seguridad tienen la posibilidad de establecer comunicación sólo con servidores compatibles con firmas.

Sección:	HKEY_LOCAL_MACHINE\SYSTEM
Clave:	System\CurrentControlSet\Services\Rdr\Parameters
Nombre:	RequireSecuritySignature
Tipo:	REG_DWORD
Valor:	1



CIB-ESPOL

Tenga en cuenta que la configuración de este valor de clave implica que el cliente no pueda conectarse a servidores que no sean compatibles con la firma de mensajes.

Windows NT versión 4.0 Service Pack 3 también incluye otra mejora en el protocolo de uso compartido de archivos SMB, de modo que, de forma predeterminada, no se pueda conectar a servidores SMB, como Samba o Hewlett-Packard (HP) LM/X o LAN Manager para UNIX, con una contraseña no cifrada (de texto normal). Así se impide que se envíen contraseñas de texto sin cifrar a través de la conexión.

Además, es posible que los clientes deseen eliminar los recursos administrativos compartidos (recursos compartidos \$) si no se necesitan en una instalación. Esta operación se puede realizar mediante el comando "net share". Por ejemplo:

C:\> net share admin\$ /d Servicio FTP



CIB-ESPOL

Windows NT también incluye otro servicio estándar de Internet denominado FTP (File Transfer Protocol, Protocolo de transferencia de archivos). Un uso habitual de FTP consiste en permitir acceso público a archivos mediante un inicio de sesión anónimo. Cuando se configura el servidor FTP, el administrador asigna al servidor una cuenta de usuario para inicios de sesión anónimos y un directorio particular predeterminado. La cuenta de usuario anónima predeterminada para FTP es GUEST (invitado). Se debe cambiar esta cuenta por otra cuenta de usuario y es recomendable que tenga una contraseña. Por otra parte, esta cuenta

no debe pertenecer a ningún grupo privilegiado, de modo que el único grupo predeterminado que debe aparecer en el token de seguridad durante el inicio de sesión es Todos. No se debe permitir a esta cuenta el derecho de usuario para "Iniciar sesión localmente" a fin de restringir "ataques internos".

El parámetro del directorio particular debe configurarse con precaución. El servidor FTP exporta particiones de disco enteras. El administrador sólo puede configurar a qué particiones se puede tener acceso a través de FTP, pero no los directorios de esa partición. Por lo tanto, un usuario que tenga acceso desde FTP puede ir a directorios situados por "encima" del directorio particular. Así pues, por lo general se recomienda que, si se tiene que ejecutar el servicio FTP en un sistema, se asigne una partición de disco completa como almacén FTP, y que a esa partición sólo se pueda tener acceso a través de FTP.

OCULTAR EL NOMBRE DEL ÚLTIMO USUARIO

De forma predeterminada, Windows NT coloca el nombre del último usuario que ha iniciado sesión en el equipo en el cuadro de texto Nombre de usuario del cuadro de diálogo **Inicio de sesión**. Esto facilita el inicio de sesión a los usuarios habituales. Para que los nombres de usuario se mantengan en secreto, puede impedir que Windows NT muestre el nombre de usuario del inicio de sesión. Esto es especialmente importante si un equipo al que, por lo general, se puede tener acceso, es utilizado por la cuenta de administrador integrada (con otro nombre).

Para impedir que se muestre un nombre de usuario en el cuadro de diálogo de Inicio de sesión, utilice el Editor del Registro para crear o asignar el siguiente valor de clave de Registro:

Sección:	HKEY_LOCAL_MACHINE\SOFTWARE
Clave:	\Microsoft\Windows NT\Current Version\Winlogon
Nombre:	DontDisplayLastUserName
Tipo:	REG_SZ
Valor:	1



CIB-ESPOL

CONTROLAR EL ACCESO A MEDIOS EXTRAÍBLES

De forma predeterminada, Windows NT permite que cualquier programa tenga acceso a archivos que se encuentran en disquetes y en CD. En un entorno multiusuario de alta seguridad, tiene la posibilidad de permitir que sólo la persona que inicia sesión de forma interactiva tenga acceso a esos dispositivos. Así, el usuario interactivo puede escribir información confidencial en esas unidades, con la confianza de que ningún otro usuario ni programa podrán ver o modificar esos datos.

Cuando trabaje en este modo, los disquetes y los CD del sistema se asignarán a un usuario como parte del proceso de inicio de sesión interactivo. Cuando el usuario cierra la sesión, estos dispositivos se liberan automáticamente para un uso general o para una nueva asignación. Por eso, es importante quitar los datos confidenciales de la unidad de disquete o de CD-ROM antes de cerrar la sesión.

Nota Windows NT permite a los usuarios el acceso a la unidad de cinta, por lo que todos los usuarios pueden leer y escribir el contenido de cualquier cinta que se encuentre en la unidad. Por lo general, esto no representa un problema, ya que nunca hay mas un usuario que mantenga una sesión interactiva en un

momento determinado. Sin embargo, en algunos casos, un programa iniciado por un usuario puede seguir en ejecución después de que el usuario cierre la sesión. Cuando otro usuario inicie sesión y coloque una cinta en la unidad, este programa puede transferir datos confidenciales de la cinta. Si esta posibilidad constituye un motivo de preocupación, reinicie el equipo antes de utilizar la unidad de cinta.

PROTEGER OBJETOS DE SISTEMA BÁSICOS

Para habilitar una protección más eficaz en objetos básicos, agregue el siguiente valor a la clave de Registro
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager:

Nombre:	ProtectionMode
Tipo:	REG_DWORD
Valor:	1

Esta configuración del Registro informa al Administrador de sesiones de Windows NT de que la seguridad de los objetos básicos del sistema debe estar en el nivel C2. Consulte el Apéndice D, Guía de actualización del Kit de recursos de Windows NT, versión 4.0 para conocer los efectos de esta configuración.



CIB-ESPOL

4.8.2.4. HABILITAR LA AUDITORÍA DEL SISTEMA

Si habilita la Auditoría del sistema, obtendrá información acerca de las acciones que planteen riesgos a la seguridad y detectar posibles infracciones de seguridad. Para activar el registro de sucesos de seguridad, siga estos pasos:

1. Inicie la sesión en la estación de trabajo local como administrador.

2. Haga clic en el botón Inicio, seleccione Programas, Herramientas administrativas y, a continuación, haga clic en Administrador de usuarios.
3. En el menú Directivas, haga clic en Auditar.
4. Haga clic en la opción Auditar estos sucesos.

Habilite las opciones que desea utilizar. Dispone de las opciones siguientes:

- ♦ Inicio y cierre de sesión: registra los inicios de sesión de recursos locales y remotos.
- ♦ Acceso a archivos y objetos: acceso a archivos, directorios e impresoras.
- ♦ Nota: los archivos y las carpetas deben residir en una partición NTFS para que se habilite el registro de seguridad. Después de habilitar la Auditoría del acceso a archivos y objetos, utilice el Explorador de Windows NT para seleccionar la Auditoría de archivos y carpetas individuales.
- ♦ Administración de usuarios y grupos: cualquier cuenta de usuario o grupo creada, cambiada o eliminada. Cualquier cuenta de usuario a la que se cambie el nombre, se desactive o se active. Cualquier contraseña establecida o cambiada.
- ♦ Cambios en el plan de seguridad: cualquier cambio en los derechos de usuario o en las directivas de Auditoría.
- ♦ Reinicio, apagado y sistema: registra los apagados y reinicios para la estación de trabajo local.



- ♦ Seguimiento de procesos: realiza un seguimiento de la activación de programas, la duplicación de identificadores, el acceso indirecto a objetos y la salida de procesos.

5. Active la casilla de verificación Correcto para habilitar el registro de las operaciones que se realicen correctamente, y la casilla de verificación Erróneo para habilitar el registro de las operaciones que no se realicen correctamente.
6. Haga clic en Aceptar.

Tenga en cuenta que la Auditoría es una capacidad de "detección", no de "prevención". Le ayudará a descubrir rupturas de seguridad después de que se produzcan, por lo que deberá considerar diversas medidas preventivas.

AUDITAR OBJETOS BÁSICOS

Para habilitar la Auditoría de objetos de sistema básicos, agregue el siguiente valor a la clave de Registro

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa:

Nombre:	AuditBaseObjects
Tipo:	REG_DWORD
Valor:	1



CIB-ESPOL

Tenga en cuenta que la configuración de esta clave no basta para que se inicie la generación de Auditorías. Será necesario que el administrador active la Auditoría para la categoría "Acceso a objetos" mediante el Administrador de usuarios. Esta clave de Registro le indica a la Autoridad de seguridad local que los objetos básicos se deben crear con una lista predeterminada de control de Auditorías del sistema.

AUDITAR PRIVILEGIOS

Algunos privilegios del sistema no se auditan de forma predeterminada aunque esté activada la Auditoría del uso de privilegios. De ese modo se controla el crecimiento de los registros de Auditoría. Los privilegios son los siguientes:

1. Saltarse la comprobación de recorrido (se otorga a todos).
2. Depurar programas (se otorga sólo a administradores)
3. Crear un objeto token (no se otorga a nadie)
4. Reemplazar un token de nivel de proceso (no se otorga a nadie)
5. Generar Auditorías de seguridad (no se otorga a nadie)
6. Copia de seguridad de archivos y directorios (se otorga a administradores y operadores de copia de seguridad)
7. Restaurar archivos y directorios (se otorga a administradores y operadores de copia de seguridad)



CIB-ESPOL

1. Se otorga a todos, de modo que no tiene relevancia por lo que respecta a la Auditoría. 2 no se utiliza en un sistema activo y se puede quitar del grupo de administradores. 3, 4 y 5 no se otorgan a ningún usuario o grupo y son privilegios muy delicados, por lo que no se deben otorgar a nadie. Sin embargo, 6 y 7 se utilizan durante las operaciones normales del sistema y se espera que se usen. Para habilitar la Auditoría de estos privilegios, agregue el siguiente valor a la clave de Registro HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa:

Nombre:	FullPrivilegeAuditing
Tipo:	REG_BINARY
Valor:	1

Tenga en cuenta que estos privilegios no se auditan de forma predeterminada, porque la copia de seguridad y la restauración son operaciones frecuentes y este privilegio se comprueba para cada archivo y directorio del que se realiza una copia de seguridad o que se restaura, lo que puede dar lugar a que el registro de Auditoría se llene con miles de Auditorías en muy poco tiempo. Considere la posibilidad de activar la Auditoría para estos usos de privilegios.

RESTRINGIR EL ACCESO ANÓNIMO AL REGISTRO A TRAVÉS DE RED

Windows NT versión 4.0 Service Pack 3 incluye una mejora de seguridad que restringe los inicios de sesión anónimos (sesión nula) cuando se establecen conexiones a canalizaciones con nombres específicas, incluida la del Registro.

Existe un valor de clave de Registro que define la lista de canalizaciones con nombre "exentas" de esta restricción. El valor de clave es:

Sección:	HKEY_LOCAL_MACHINE\SYSTEM
Clave:	System\CurrentControlSet\Services\LanManServer\Parameters
Nombre:	NullSessionPipes
Tipo:	REG_MULTI_SZ
Valor:	Agregue o quite nombres de la lista, según requiera la configuración.

Windows NT presenta una característica según la cual los usuarios de inicio de sesión anónimo pueden enumerar nombres de usuarios de dominio y nombres de recursos compartidos. Los clientes que desean mejorar la seguridad han solicitado la posibilidad de restringir esta funcionalidad opcionalmente. Windows NT 4.0 Service Pack 3 y una corrección para Windows NT 3.51 proporcionan un mecanismo por el que los administradores restrinjan la posibilidad de los usuarios con inicio de sesión anónimo (también conocidas como conexiones de sesión

NULL) de enumerar nombres de cuentas y de recursos compartidos. El editor ACL de Windows NT necesita que se enumeren los nombres de las cuentas de los controladores de dominio; por ejemplo, para obtener la lista de usuarios y grupos a fin de seleccionar a quién desea otorgar derechos de acceso un usuario. La enumeración de nombres de cuentas también es utilizada por el Explorador de Windows NT para seleccionar los usuarios y grupos a los que se otorgará acceso a un recurso compartido.

El valor de clave de Registro que se debe configurar para habilitar esta característica es:

Sección:	HKEY_LOCAL_MACHINE\SYSTEM
Clave:	System\CurrentControlSet\Control\LSA
Nombre:	RestrictAnonymous
Tipo:	REG_DWORD
Valor:	1.



CIB-ESPOL

EXIGIR CONTRASEÑAS DE ALTO NIVEL PARA USUARIOS

Windows NT 4.0 Service Pack 2 y las versiones posteriores incluyen un archivo DLL de filtro de contraseñas (Passfilt.dll) que le permite exigir requisitos de contraseña de usuario de nivel superior. Passfilt.dll ofrece una mayor seguridad contra la "adivinación de contraseñas" o los "ataques de diccionario" por parte de intrusos.

Passfilt.dll implementa la siguiente directiva de contraseñas:

Las contraseñas deben tener seis (6) caracteres, como mínimo. (La longitud mínima de la contraseña se puede incrementar aún más si se configura un valor superior en la Directiva de contraseña para el dominio.)

Las contraseñas deben contener caracteres de al menos tres (3) de las cuatro (4) clases siguientes:

Descripción	Ejemplos
Mayúsculas	A, B, C... Z
Minúsculas	a, b, c, ... z
Numerales arábigos occidentalizados	0, 1, 2, ... 9
No alfanuméricos ("caracteres especiales"), tales como signos de puntuación	

- ♦ Las contraseñas no pueden contener el nombre de usuario completo ni en parte.



Estos requisitos están codificados en el archivo Passfilt.dll y no pueden ser cambiados por el usuario ni a través del Registro. Si desea aumentar o reducir estos requisitos, puede escribir su propio archivo .dll e implementarlo del mismo modo en que lo hace la versión de Microsoft disponible con Windows NT 4.0 Service Pack 2.

Para utilizar Passfilt.dll, el administrador debe configurar el archivo DLL de filtro de contraseñas en el Registro del sistema en todos los controladores de dominio. Esta operación se puede realizar del modo siguiente:

- ♦ Configure el siguiente valor de clave de Registro:

Sección:	HKEY_LOCAL_MACHINE\SYSTEM
----------	---------------------------

Clave:	System\CurrentControlSet\Control\LSA
Nombre:	Paquetes de notificación
Tipo:	REG_MULTI_SZ
Valor:	Agregue la cadena "PASSFILT" (no quite las existentes).

Al desactivar la compatibilidad con hash en contraseñas de LanManager, Windows NT es compatible con los dos tipos de autenticación de desafío/respuesta siguientes:

- ♦ Desafío/respuesta de LanManager (LM)
- ♦ Desafío/respuesta de Windows NT

Para permitir el acceso a servidores que sólo permiten la autenticación LM, los clientes de Windows NT envían actualmente los dos tipos de autenticación. Microsoft desarrolló una revisión de software que permite configurar los clientes de modo que envíen únicamente la autenticación de Windows NT. De ese modo, se dejan de utilizar los mensajes de desafío/respuesta LM en la red.

Si se aplica esta corrección, se configura la siguiente clave de Registro:

Sección:	HKEY_LOCAL_MACHINE\SYSTEM
Clave:	System\CurrentControlSet\Control\LSA
Nombre:	LMCompatibilityLevel
Tipo:	REG_DWORD
Valor:	0,1,2 (0 como predeterminado)

Configurar el valor como:

- ♦ 0 – Enviar las formas de contraseña Windows NT y LM.



CIB-ESPOL

- ♦ 1 – Enviar las formas de contraseña Windows NT y LM únicamente si el servidor lo solicita.
- ♦ 2 – No enviar nunca la forma de contraseña LM.

Si un cliente de Windows NT selecciona el nivel 2, no se puede conectar a servidores que sólo permitan la autenticación LM, tales como Windows 95 y Windows para Trabajo en Grupo.

El sistema de compatibilidad con la memoria virtual de Windows NT utiliza un archivo de paginación del sistema para intercambiar páginas desde la memoria de distintos procesos al disco cuando no se utilizan. En un sistema en ejecución, este archivo de paginación sólo es abierto por el sistema operativo, por lo que está bien protegido. Sin embargo, para los sistemas configurados de modo que permiten que se inicien otros sistemas operativos, quizá se desee garantizar que se borra el archivo de páginas del sistema cuando se cierra Windows NT. Así se garantiza que la información confidencial de la memoria de procesos que reside en el archivo de paginación no esté disponible para cualquier usuario. Esta operación se puede realizar mediante la configuración de la siguiente clave:

Sección:	HKEY_LOCAL_MACHINE\SYSTEM
Clave:	System\CurrentControlSet\Control\SessionManager\Memory Management
Nombre:	ClearPageFileAtShutdown
Tipo:	REG_DWORD
Valor:	1

Tenga en cuenta que este mecanismo de protección sólo funciona durante un cierre del sistema sin problemas, por lo que es importante que los usuarios que no sean de confianza no tengan la posibilidad de apagar ni reiniciar el sistema



manualmente. Desactivar la copia en caché de las credenciales de inicio de sesión durante un inicio de sesión interactivo.

La configuración predeterminada de Windows NT guarda en caché las últimas credenciales de inicio de sesión de un usuario que inició sesión en un sistema de forma interactiva. Esta característica se proporciona por motivos de disponibilidad del sistema; por ejemplo, debido a que la máquina del usuario está desconectada o a que no está conectado ninguno de los controladores de dominio.

Aunque la caché de credenciales está bien protegida, en los entornos de alta seguridad, los clientes tienen la opción de desactivar esta característica. Esta operación se puede realizar mediante la configuración de la siguiente clave de Registro:

Sección:	HKEY_LOCAL_MACHINE
Clave:	Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Nombre:	CachedLogonsCount
Tipo:	REG_DWORD
Valor:	0



CIB-ESPOL

4.8.2.5. SEGURIDAD DE LOS SERVICIOS

También se pueden configurar las opciones de seguridad TCP/IP para permitir o bloquear la dirección del (los) puerto(s) que se necesiten según los servicios que se quieran ejecutar. Para hacer esto, siga la siguiente secuencia:

Panel de Control -> Red -> Protocolos -> Protocolo TCP/IP -> Propiedades -> Avanzadas.

Marque: Activar seguridad

Pulse el botón Configurar

Seleccione el adaptador correspondiente y marque el numero de puerto/s del servicio/s que quiera permitir.

Los servicios mas importantes junto con sus puertos son los siguientes:

Descripción	Nombre	Puerto
Transferencia de archivos (datos)	ftp-data	20 tcp,udp
Transferencia de archivos (control)	ftp	21 tcp,udp
Telnet	telnet	23 tcp,udp
Servidor de nombres de dominio	domain	53 tcp,udp
WWW HTTP	www	80 tcp,udp

Tabla 4-25. Auditoría de Windows NT

Windows NT tiene internamente servicios propios del Sistema Operativo; apártese pueden instalar otros en cualquier momento que se desee. Se deberían ejecutar tan pocos servicios como sea posible ,para disminuir al máximo la posibilidad de accesos no autorizados por errores de configuración y "bugs" de los servicios . Esto se podrá seleccionar en Servicios del Panel de control, mediante los botones de Iniciar, Detener y Pausa.

4.8.2.6. PROTECCIÓN DE LOS PROTOCOLOS INTERNOS

Cuando se suministra a los usuarios de Internet acceso a los servicios de la red interna, hay que proteger los sistemas internos. Hay dos tipos de servicios de red disponibles en una computadora Windows NT:

- ♦ SMB: (Bloques de mensajes de servidor) de Microsoft que son servicios de archivos y red. Estos servicios están instalados por defecto normalmente.
- ♦ Servicios TCP/IP e Internet como servidores Web y FTP. Se pueden instalar de modo opcional.

Cuando se conecta un sistema Windows a Internet existe el peligro potencial de los protocolos SMB. Si hay carpetas compartidas SMB en la red que conecta a Internet, potencialmente cualquiera de los usuarios de Internet puede acceder a las carpetas o secuestrar sesiones. Además, hay problemas de seguridad intrínsecos a los protocolos. A continuación se describe como desactivar estos servicios apropiadamente, se debe seguir la secuencia:

Panel de Control -> Red -> Enlaces

Seleccionar Todos los servicios en la caja de texto correspondiente a Mostrar enlaces.

Expandir las opciones TCP/IP bajo las cabeceras: NetBIOS, Server y Workstation.

Seleccionar el adaptador a desactivar y pulsar el botón Desactivar.

4.8.3. CONSIDERACIONES GENERALES

- ♦ Procurar no crear un sistema de arranque dual, es decir, que contenga dos o mas particiones de disco cada una de las cuales conteniendo un sistema operativo distinto.
- ♦ Para implementar los mayores niveles de seguridad, intentar dar formato a las particiones Windows NT con el sistema NTFS. Este sistema es más seguro, dado que proporciona permisos extendidos para controlar los accesos a los archivos y oculta datos en el disco cuando alguien intenta arrancar el sistema con otro sistema operativo.



CIB-ESPOL

5. POLITICAS DE SEGURIDAD

5.1. INTRODUCCIÓN

Seguridad, viene del latín "Securitate", que significa "calidad de seguro" y computacional del griego Computare, que significa usar el "cálculo numérico" para medir algo. Las políticas de seguridad computacional son normas materializadas en documentos que escriben la forma correcta y adecuada del uso de los recursos computacionales, las responsabilidades y derechos que administradores y usuarios tienen, además de las medidas (De contingencia para cada inconveniente computacional en caso de catástrofes, donde prima salvaguardar la integridad de las personas y le sigue en jerarquía salvaguardar la integridad de la información antes que cualquier maquinaria y equipo, claro está sin dejar de lado la importancia que el hardware requiere, pero como última prioridad. Las políticas no deben limitarse únicamente al hardware y software, también le concierne el uso adecuado de las instalaciones donde se aplican, es decir, que regulen el acceso del personal, tanto de forma lógica como física. Las políticas de seguridad computacional ayudan a que la educación de cada una de las personas que tienen a cargo la responsabilidad de mantener integridad, confidencialidad, consistencia, disponibilidad, autenticación, control y Auditoría de la información de los demás empleados sea muy importante para la entidad. Desde el funcionario de más bajo cargo de la entidad en cuestión hasta el de más alto, juegan un papel importante en el diseño, desarrollo y aplicación de las políticas de seguridad computacional. Las políticas de seguridad computacional deben dividirse según tres aspectos básicos: Seguridad lógica, física y locativa.

Además se deben tener en cuenta los manuales de funciones y procedimientos de cada cargo, para que se diseñen las políticas de acuerdo al rol que desempeña cada empleado. Es muy importante conocer detalladamente los servicios computacionales para que se desarrollen las políticas por servicios correspondientes.

Las políticas en las Empresas no deben ser vistas como órdenes o leyes autoritarias, sino como mecanismos de control que facilitan la Auditoría de los procedimientos, equipos, funcionarios y sus funciones.

5.2. LINEAMIENTOS PARA LA CREACIÓN DE POLÍTICAS DE SEGURIDAD.



El Administrador de la Red de datos junto con la cúpula administrativa, son quienes deben decidir el nivel de seguridad que desea para su red y computadores. Cuando se decida la política de seguridad a seguir, se deberá buscar el equilibrio entre seguridad, conveniencia y disponibilidad.

Estos son algunos de los interrogantes que deben plantearse cuando se diseñan las políticas de seguridad:

¿Quién debe tener acceso? Si se trata de un negocio, ¿son todos los empleados o solamente algunos?

¿Quién debe tener acceso físico? ¿Los sistemas se encuentran cerrados o de libre de acceso?

¿Cuándo se debe tener acceso? ¿Se permite a los usuarios acceder de 9 AM a 5 PM los días laborales o 24 horas siete días a la semana?

¿De qué clase de acceso se debe disponer? ¿Todos necesitan acceder a Internet o sólo a las impresoras de la red?

¿Qué servicios deben usar? ¿Debe alguno acceder ftp? ¿Qué ocurre con telnet, finger y los demás servicios?

¿Qué clases de programas deben ejecutar? ¿Necesitan acceso a sencillas herramientas de oficina o a sofisticados programas de gráficos y de CAD?

¿Con qué otros computadores de la red deben conectarse? ¿Cuántos servidores deben ver? ¿El servidor Web? ¿Qué pasa con la contabilidad y las nóminas?

¿De cuanto espacio deben disponer los usuarios dentro del sistema de archivos? ¿Necesitan 100 Megas o 10 Gigas?

¿De cuánto espacio del kernel disponen los usuarios? ¿Necesitarán más de 5 megabytes?

¿Qué restricciones se deben implantar al uso de contraseñas? ¿Una longitud mínima? ¿Cambios semanales? ¿Tal vez mensuales?



CIB-ESPOL

¿Qué clase de ataques son posibles? ¿Hay módems o ras en alguno de los sistemas? ¿Hace falta que los usuarios accedan desde el exterior a través del Firewall?

¿Qué ataques son más probables? ¿Se ha despedido recientemente a empleados con conocimiento del sistema? ¿Se han producido recientemente intentos que hayan tenido éxito?

¿De cuánto tiempo se dispone para recuperarse después de un ataque? ¿Es posible permitirse una semana de baja? ¿Un día? ¿Una hora?

¿Cuánto va a costar? Considérese sobre la base hora/trabajador, para volver a la normalidad.

¿Qué valor deben tener los datos protegidos para alguien de afuera? ¿Son secretos corporativos? ¿Información financiera? ¿Lista de clientes?

¿Qué daño pueden causar a la reputación de la Empresa la publicación de la intrusión?

¿Qué perjuicio para las ventas de la entidad supondría la publicación de la intrusión? ¿Se especula con el buen nombre y el historial de seguridad? ¿Qué ocurre si se están facilitando servicios de seguridad y los sistemas se ven comprometidos?

5.2.1. POLÍTICAS DE CONFIGURACIÓN

Hay que decidir la manera de configurar las computadoras para conseguir la calidad conveniente del sistema. El tener sistemas configurados de manera similar ayudará inicialmente y será de utilidad para detectar una configuración que no es igual a las otras.

5.2.2. POLÍTICAS DE MANTENIMIENTO

Debería fijarse un calendario para la Auditoría de los sistemas de seguridad. En él debería fijarse la ejecución del software de Auditoría de la red y el software de Auditoría de la configuración. Generalmente se usa cron, en sistemas Linux/Unix, para ejecutar estos paquetes y los registros de salida son escaneados o enviados por correo electrónico al administrador diariamente.

También debería comprobarse la aparición de parches del fabricante para el software que se ejecuta en el sistema. Para ello son útiles los anuncios de CERT. Véase <http://www.cert.org>. Deben aplicarse esas actualizaciones tan pronto como se tiene conocimiento de ellas para estar prevenidos contra los ataques más recientes.

5.2.3. POLÍTICAS DE REACCIÓN O CONTINGENCIA

Debe prepararse un plan de reacción a las intrusiones predecibles. Identificar los pasos necesarios para recuperarse de una intrusión, incluyendo la conectividad, la recuperación a partir de las copias de seguridad y la prevención de futuras intrusiones. El conocimiento de lo que debe hacerse para minimizar los danos de



un ataque en curso ante hechos consumados evitará confusiones y lo que es más importante, tiempo.

5.2.4. ESTABLECER LAS REGLAS

Además de la política de seguridad, debe existir un conjunto de normas que los usuarios deben seguir cuando usan el sistema. Estas reglas deben señalar lo que se espera de los usuarios y las consecuencias de un mal uso del sistema. Tener unas normas claramente establecidas dará un soporte legal si alguien se convierte en un problema para el sistema. Lo peor que puede ocurrir es que, después de una violación de las reglas, no se pueda demostrar lo que el usuario ha hecho en contra de ellas, porque no está señalado en ningún sitio y peor aún, que lo ocurrido quede impune.

Una buena política de normas deja poco campo a la interpretación. Es muy importante que los usuarios y todos los demás que intenten usar el computador o sus servicios conozcan y entiendan las reglas del sistema.

Algunos puntos a considerar para su inclusión en un conjunto de normas de utilización son:

¿Quién es el propietario del sistema? ¿Generalmente será la Empresa o la entidad que lo paga?

¿Quién debe usar el sistema? ¿Deberían incluirse los términos "-usuarios autorizados" y consistirían en los empleados de la entidad o los estudiantes y facultades de una institución de enseñanza?

Horario de utilización. ¿Podría ser de 9 AM a 5 PM para un banco o entidad financiera y 24 horas, todos los días del año en una Universidad?

Servicios que deben usarse. Serán los servicios que el usuario debe utilizar y no son necesariamente todos los programas instalados.

Servicios estrictamente prohibidos. Que incluiría el almacenamiento de archivos no autorizados, como pornografía, software pirata o el tráfico con ellos.

Software prohibido en el sistema. Además de lo anterior, puede ser software legal pero no aprobado por el servicio de soporte técnico del equipo computacional.

Sanciones por uso indebido. Debe ser la revocación del acceso o sanciones penales.

Contacto para preguntas o información de uso indebido. Normalmente debe ser alguien en los servicios de seguridad computacional o en el soporte técnico del equipo computacional.

Dónde debe obtenerse más información. Pueden ser archivos almacenados o incluso enviados por Internet.

Debe colocarse el conjunto de normas de utilización donde todos los usuarios deban verlo o en su defecto difundirlo a través de los mismos servicios de la entidad, como son ftp, correo electrónico o Web.

5.2.5. VELAR POR EL ESTRICTO CUMPLIMIENTO

La forma menos conflictiva de aplicar el cumplimiento estricto de las políticas de seguridad es que, siempre que sea posible, sea el propio sistema el que informe automáticamente esto ayudara a evitar la confrontación directa con los usuarios que violen las políticas Si es el sistema el que les dice que están cometiendo una infracción, la cosa resulta más impersonal y no lo verán como algo represivo o un ataque personal. Las contraseñas los horarios de inicio, los permisos de acceso a dispositivos y la limitación del uso de recursos deben ser controlados y su cumplimiento implantado por el sistema según lo tratado anteriormente en este documento. Además, ello ayudará a reducir la carga de trabajo como Administrador de una Red de Datos.

Debe ejercerse una estrecha vigilancia sobre el sistema y los usuarios. No hay que permitir que queden impunes las violaciones de las políticas de utilización. Hay que reaccionar con prontitud y de acuerdo con las medidas que se establecieron en los términos de la política de utilizaron. No hay que aplicar a nadie excepciones que no este dispuesto a aplicar a los demás. Hay que controlar diariamente los registros del sistema en busca de violaciones El conocimiento de la forma que los usuarios utilizan el sistema es una parte importante de la administración de sistemas computacionales seguros.



CIB-ESPOL

5.3. CÓMO TRATAR LAS INFRACCIONES

Hay que tratar con cautela a quienes violen la política de seguridad. Cuando la infracción ha sido leve y no llega a constituir una amenaza (el usuario ha sobrepasado largamente los límites de utilización del disco, por ejemplo), el envío de advertencias documentadas suele ser un buen primer paso. Se puede limitar el acceso del usuario a los recursos. Si el usuario reincide, se puede aumentar la penalización anulando su cuenta durante un tiempo prudente, por ejemplo.

5.3.1. ANULAR UNA CUENTA

Anular una cuenta es una forma de llamar rápidamente la atención del usuario. Le obligará a ponerse en contacto con el administrador de la red de datos para que se la restablezca y se podrá aprovechar la ocasión para comentarle las infracciones cometidas.

5.3.2. RESTRINGIR LAS HORAS DE ACCESO

Se puede limitar las horas a las que un usuario debe conectarse al sistema. Puede que desee limitar las horas de acceso de un usuario a aquellas en las que el administrador del sistema computacional pueda vigilar directamente su actividad.

5.3.3. LIMITAR LOS RECURSOS

Cuando un usuario escribe o ejecuta frecuentemente programas que ocupan recursos del sistema tales como tiempo de CPLJ, memoria o espacio en la tabla

de procesos, pueden cambiarse ciertos parámetros con el fin de mantenerles por debajo de ciertos umbrales.

5.3.4. LIMITAR EL ESPACIO EN EL SISTEMA DE ARCHIVOS

Si se nota que algún usuario está ocupando espacio en disco, puede considerarse la posibilidad de instalar cuotas para fijar un límite máximo que cada usuario tiene derecho a utilizar.

5.3.5. LIMITAR EL ACCESO A LOS DISPOSITIVOS

Si un usuario abusa de los dispositivos, como, por ejemplo, quemar demasiados CDs o ejecutar sonidos con volumen molesto para otros usuarios que están trabajando, es posible configurar el sistema para restringir el acceso a estos dispositivos mientras el usuario está conectado a una consola.



5.3.6. LIMITAR EL ACCESO A PROGRAMAS

Cuando un usuario abusa de sus privilegios, ejecutando programas que no debe, o a horas indebidas, se pueden usar grupos para limitarle el acceso.

CIB-ESPOL

5.4. POLÍTICAS DE SEGURIDAD PARA LA EMPRESA.

5.4.1. SEGURIDAD FÍSICA

5.4.1.1. ACCESO FÍSICO

- ♦ El servicio de vigilancia (guardias) será el encargado de controlar el acceso de todas las personas a la Empresa. Este servicio estará encargado de colocar

los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.

- ♦ A cualquier personal ajeno a la planta se le solicitara completar un formulario de datos personales, los motivos de la visita, hora de ingreso y de regreso.
- ♦ Para controlar el ingreso y egreso de vehículos, el personal de vigilancia debe asentar en una plantilla los datos personales de los ocupantes del vehículo, la marca y patente del mismo, y la hora de ingreso y egreso de la Empresa.

5.4.1.2. CONTRA INCENDIOS EN EL DEPARTAMENTO DE SISTEMAS

- ♦ El área en la que se encuentran las computadoras debe estar en un local que no sea combustible e inflamable.
- ♦ El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- ♦ Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- ♦ Debe construirse un falso piso instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
- ♦ Deben emplearse muebles incombustibles y cestos metálicos para papeles. Deben evitarse materiales plásticos e inflamables.
- ♦ El piso y el techo en el centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

5.4.1.3. SEGURIDAD DE LOS EQUIPOS

- ♦ La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- ♦ Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- ♦ Deben instalarse extintores manuales (portátil) y/o automáticos (rociadores).

5.4.1.4. CONFIGURACIÓN DE LOS EQUIPOS

- ♦ Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Sistemas.

5.4.1.5. DE USO INADECUADO

- ♦ No se permite fumar, comer o beber mientras se está usando un PC.
- ♦ No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente al Jefe de Sistemas.
- ♦ No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Empresa se requiere una autorización escrita dirigida al Gerente de Sistemas.
- ♦ No deben usarse disquetes u otros medios de almacenamiento en cualquier computadora de la Empresa a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

- ♦ Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado por el Jefe de Sistemas. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Empresa.

5.4.1.6. DE USO ADECUADO

- ♦ Para obtener un rendimiento de operabilidad óptima en los usuarios es indispensable que los centros de cómputo estén bien iluminados.
- ♦ Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
- ♦ Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS).
- ♦ Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
- ♦ Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.
- ♦ Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.
- ♦ La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente al Jefe de Sistemas.



5.4.1.7. POLÍTICAS DE RESPALDO

- ♦ Sin importar el tipo de información que se va a respaldar, esta debe ser almacenada en CDs.
- ♦ Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los gerentes de los distintos departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).
- ♦ Semanalmente, es decir, por lo menos una vez por semana, debe hacerse el respaldo de los datos guardados y las copias de respaldo deben guardarse en un lugar seguro y bajo llave dentro del Departamento de Sistemas de la Empresa, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de Empresa deben guardarse en otra sede, lejos del edificio en una de sus sucursales.
- ♦ No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.
- ♦ Para ayudar a restaurar los programas originales no dañados o infectados el Jefe de Sistemas debe hacer copias de todo software nuevo antes de su uso, y debe guardarse tales copias en un lugar seguro en dispositivos como CDs.
- ♦ En el momento en que la información respaldada deje de ser útil a la organización, dicha información deberá ser borrada o destruida totalmente antes de deshacerse del medio.



5.4.1.8. RECOMENDACIONES

- ♦ El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.
- ♦ Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger alrededor del incendio que podría originarse en las áreas adyacentes.
- ♦ Usar pantallas o anteojos antirreflejos con protección para el monitor, para evitar trastornos visuales en los operadores.

5.4.2. SEGURIDAD LÓGICA

Los equipos de la Empresa sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

5.4.2.1. PRIVACIDAD

- ♦ Los usuarios deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.
- ♦ Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

5.4.2.2. CONTRA LA PIRATERÍA DE SOFTWARE

- ♦ A menos que se indique lo contrario, los usuarios deben asumir que todo el software la Empresa está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.
- ♦ Los usuarios no deben copiar a un medio removible (como un disquete), el software o los datos residentes en las computadoras de la Empresa, sin la aprobación previa de la gerencia.

5.4.2.3. CONFIDENCIALIDAD Y PRIVACIDAD DE LA EMPRESA

- ♦ No pueden extraerse datos fuera de la sede de la Empresa sin la aprobación previa de la gerencia. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.
- ♦ Siempre que sea posible, deba eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por Empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión del Jefe de Sistemas.
- ♦ El personal que utiliza un computador portátil que contenga información confidencial de la Empresa, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información debe estar cifrada.
- ♦ La información de la Empresa clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando



herramientas de encriptación robustas y que hayan sido aprobadas por el Jefe de Informática.

- ♦ El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas como Gerentes o Jefes Departamentales y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

5.4.3. MANTENIMIENTO

- ♦ El jefe de Sistemas es el responsable de proteger con contraseña el acceso al BIOS de cada una de las PCs y de los Servidores.
- ♦ El jefe de Sistemas es el responsable de actualizar periódicamente, cada seis meses (o cuando un parche de alguna vulnerabilidad este disponible y haya sido publicado de manera oficial en el Internet) los Sistemas Operativos de Los PCs y los servidores de la Empresa.
- ♦ Debe instalarse y activarse una herramienta antivirus (AVG), la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe Sistemas y poner la PC en cuarentena hasta que el problema sea resuelto.
- ♦ El antivirus de los PCs debe ser actualizado por el usuario, por lo menos una vez al mes.
- ♦ El antivirus debe ser instalado en cada una de las PCs y en los Servidores Bajo Windows NT y bajo Linux Red Hat 9.
- ♦ Borre constantemente los cookies, archivos temporales e historial, en la opción Herramientas, Opciones de Internet, de su navegador.
- ♦ Configurar el sistema para que muestre las extensiones de todos los archivos.

5.4.3.1. DESCARGAS DEL INTERNET

- ♦ Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la Empresa.
- ♦ No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Sistemas.
- ♦ Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el Departamento de Sistemas.

5.4.3.2. CONTRA EL SOFTWARE MALICIOSO

- ♦ Está terminantemente prohibido ejecutar programas que intenten adivinar las contraseñas alojadas en las tablas de usuarios de máquinas locales o remotas.
- ♦ Está estrictamente prohibido hacer uso de herramientas propias de delincuentes informáticos, tales como programas que rastrean vulnerabilidades en sistemas de cómputo propio o ajeno.
- ♦ Está estrictamente prohibido hacer uso de programas que explotan alguna vulnerabilidad de un sistema para proporcionar privilegios no otorgados explícitamente por el Jefe de Sistemas.



CIB-ESPOL

- ♦ Tomar precauciones con los contenidos de applets de Java, JavaScripts y Controles ActiveX, durante la navegación, así como los Certificados de Seguridad. Es recomendable configurar el navegador desactivando la ejecución automática de estos contenidos.
- ♦ De ninguna manera se debe ejecutar ningún archivo con doble extensión.

5.4.3.3. CONFIDENCIALIDAD Y PRIVACIDAD DE LOS EMPLEADOS

- ♦ Los empleados y funcionarios de la Empresa no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La Empresa se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.
- ♦ Es política de la Empresa no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o Auditoría. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.
- ♦ De manera consistente con prácticas generalmente aceptadas, la Empresa procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica (PABX) contienen detalles sobre el número llamado, la duración de la llamada, y la hora en que se efectuó la llamada.

5.4.3.4. POLÍTICAS DE CUENTAS

- ♦ Las cuentas deben ser otorgadas exclusivamente a usuarios legítimos.
- ♦ Una cuenta deberá estar conformada por un nombre de usuario y su respectiva contraseña.
- ♦ El nombre de usuario de una cuenta deberá estar conformado por la primera letra de su nombre y su apellido paterno.

5.4.3.5. POLÍTICAS DE CONTRASEÑAS

- ♦ La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el usuario. Todas las contraseñas deberán contar con al menos ocho caracteres.
- ♦ Todas las contraseñas elegidas por los usuarios deben ser difíciles de adivinar. No deben ser utilizadas palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.
- ♦ Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar.
- ♦ Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores.
- ♦ Está prohibido acceder al sistema con una cuenta diferente de la propia, aun con la autorización del dueño de dicha cuenta.
- ♦ Al momento de ingresar al sistema, cada usuario deberá ser notificado de la fecha, hora y dirección desde la que se conectó al sistema por última vez, lo cual permitirá detectar fácilmente el uso no autorizado del sistema.



5.4.3.6. POLÍTICAS PARA EL USO DE CORREO ELECTRÓNICO

NORMAS PARA EL USO DE LAS CUENTAS DE CORREO ELECTRÓNICO

- ♦ El único software cliente que debe ser usado y bien configurado por el Jefe de Sistemas es el Microsoft Outlook.
- ♦ Los empleados únicamente pueden enviar correo internamente a otros empleados.
- ♦ Los usuarios autorizados podrán enviar correo fuera de la Empresa a otros agentes de Correo de uso publico (ejemplo: Hotmail, Yahoo) u otras Empresas.
- ♦ El contenido de los mensajes no debe ser NUNCA insultante, injurioso, ofensivo u obsceno. Explícitamente son considerados ofensivos los de carácter sexista o racista. Será considerado como FALTA GRAVE el incumplimiento de esta norma.
- ♦ Queda prohibido enviar mensajes a un grupo, o a un usuario que no los quiera recibir.
- ♦ Queda prohibido el uso de seudónimos u otros sistemas de ocultamiento de identidad. Debe quedar claro al receptor de los mensajes el nombre de quien los envía.
- ♦ No deben usarse sistemas de transferencia de archivos mediante correo, por ejemplo ftpmail, debido al peligro de saturación del sistema que esto provoca.
- ♦ Cuando en una respuesta se incluye el mensaje original, se debe eliminar toda la información accesorio, que no esté relacionada con el contenido de la respuesta (cabeceras, apartados irrelevantes del mensaje, firmas, despedidas, etc.).

- ♦ El usuario se hace responsable de mantener espacio disponible en su cuenta para permitir la correcta recepción de mensajes. Se aconseja leer diariamente su correo.
- ♦ Cualquier queja, referente al usuario, recibida de los administradores de correo de redes externas será considerada una FALTA MUY GRAVE.
- ♦ No se permite enviar repetidamente, de manera sistemática, un mismo mensaje a una o varias listas (alias).
- ♦ Se prohíbe expresamente el envío de mensajes publicitarios a las listas (alias), a menos que esté previamente autorizado por el Jefe de Sistemas y el Gerente General.
- ♦ Está estrictamente prohibido usar la cuenta de correo electrónico proporcionada por la organización para propósitos ajenos a sus actividades laborales.
- ♦ No se permite el uso de la cuenta de correo electrónico para subscribirse a listas electrónicas de discusión de interés personal. El usuario deberá limitarse a estar suscrito a las listas indicadas y aprobadas por la Empresa.

RECOMENDACIONES PARA EL USO DE LAS CUENTAS DE CORREO ELECTRÓNICO.

- ♦ No reenviar correspondencia privada sin permiso del autor. No leer el correo de otra persona sin su permiso.
- ♦ Si se recibe un mensaje por accidente, devolverlo al remitente o realizar un "forward" a la persona a la que iba dirigido.



- ♦ No enviar información falsa y no pretender ser alguien que no se es, para conseguir las ventajas de ese alguien.
- ♦ Dañar un sistema implica dañar a mucha gente.
- ♦ Los usuarios que eligen claves obvias (conocido como agujeros), están aumentando la probabilidad de estropear no solo sus propios correos sino los de los demás también.
- ♦ A todos los efectos, emplear un "agujero" de seguridad para provocar daños en un sistema de forma voluntaria es equivalente a forzar ese sistema con cualquier método para realizar los mismos daños.
- ♦ En términos absolutos, quien conociendo la existencia de un "agujero" de seguridad, no hace lo posible para que se corrija, es cuando menos "cómplice involuntario" o incluso co-responsable de los daños que puedan ser infringidos por un tercero a través de ese "agujero".
- ♦ Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento, es decir, por lo menos una vez por semana hasta un periodo máximo de un mes. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.



RECOMENDACIONES SOBRE LA UTILIZACIÓN DE LAS LISTAS DE INTERÉS

- ♦ Las listas, al ser un medio de amplia difusión (los mensajes son recibidos por TODOS los subscriptores), deben ser utilizadas con prudencia. Los mensajes a las listas no deben enviarse antes de haber preparado el tema a tratar. En el caso de una pregunta, deben

agotarse primero otros medios de consulta disponibles (bibliotecas, tutorías, libros, manuales, etc.).

- ♦ El envío masivo de mensajes a una lista provoca irremediablemente su inoperatividad. Cuando una lista recibe más de 30 mensajes diarios los usuarios tienden a abandonarla, al verse incapaces de atender la avalancha. Por tanto, se restringe el número de mensajes a 15 por usuario, lista y día.
- ♦ Cualquier duda o problema relacionado con el servicio de correo y listas de distribución en este servidor pueden ser comentados con el Jefe de Sistemas.
- ♦ Es muy importante asegurarse de pertenecer a la lista adecuada.

UTILIZACIÓN CORRECTA DE LAS CUENTAS DE CORREO ELECTRÓNICO

- ♦ Las cuentas son personales e intransferibles. Se considera falta MUY GRAVE el uso de cuentas ajenas, así como la sesión de la cuenta propia a terceros.
- ♦ El propietario de la cuenta es el ÚNICO responsable de la privacidad de su clave. Cualquier acción efectuada desde ésta será atribuida a dicho propietario.
- ♦ Al momento de la creación de una Cuenta de correo electrónico se asigna como espacio disponible para la recepción de correo electrónico 3 MB para todos los usuarios de la Empresa.



CIB-ESPOL

ATAQUE Y PROTECCIÓN A LAS CUENTAS DE CORREO

ELECTRÓNICO

- ♦ Uno de los posibles ataques a la cuenta de un usuario es de conocimiento de su clave de acceso a través de medios no autorizados como son: verla digitar, leerla de un papel donde esté escrita, oírla decir, etc. La medida de precaución adecuada a este caso es cambiar la clave periódicamente o cuando la privacidad de ésta haya estado en peligro. El cambio de clave se realiza por medio del administrador de la red o por el mismo usuario.
- ♦ Otro posible ataque a una cuenta puede producirse al abandonar una terminal o PC sin haber cerrado la sesión abierta. Al finalizar la sesión de trabajo se debe salir siempre de la cuenta. Se debe cerrar Microsoft Outlook después de revisar su correo o antes de abandonar su PC.
- ♦ No contestar los mensajes SPAM, ya que al hacerlo se re-confirmará su dirección IP, ni prestar atención a los mensajes con falsos contenidos (Hoaxes), tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc.

SANCIONES POR FALTAS SOBRE EL USO DE LAS CUENTAS DE CORREO ELECTRÓNICO

Las posibles sanciones a aplicar, dependiendo de la gravedad de la falta cometida, son las siguientes:

- ♦ Inhabilitación temporal o definitiva de la cuenta de correo.
- ♦ Suspensión indefinida de la cuenta.



- ♦ La administración de la red de datos o el comité encargado de estudiar las faltas, tendrá la potestad de aplicar estas sanciones.

5.4.3.7. POLÍTICAS DE SEGURIDAD PARA REDES

ALCANCE

Esta política se aplica a todos los empleados, contratistas, consultores y personal temporal de la Empresa.

ASPECTOS GENERALES

Es política de la Empresa prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras Empresas o personas y que le haya sido confiada.

MODIFICACIONES

Todos los cambios en la central telefónica (PABX) y en los servidores y equipos de red de la Empresa, incluyendo la instalación de el nuevo software, el cambio de direcciones IP, la re-configuración de routers y switches, deben ser documentados y debidamente aprobados por el Gerente General de La Empresa, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

CUENTAS DE LOS USUARIOS

- ♦ Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
- ♦ La solicitud de una nueva cuenta o el cambio de privilegios deben ser hechos por escrito y debe ser debidamente aprobada en conjunto por el Jefe de Sistemas y el Gerente General.
- ♦ No debe concederse una cuenta a personas que no sean empleados de la Empresa a menos que estén debidamente autorizados en conjunto por el Jefe de Sistemas y el Gerente General, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.
- ♦ Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo debe otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas en este caso al Jefe de Sistemas y el Gerente General.
- ♦ No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que en conjunto el Jefe de Sistemas y el Gerente General determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto).
- ♦ Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que Jefe de Sistemas quien es el administrador del sistema Linux no deben entrar inicialmente como "root", sino primero empleando su propio ID y luego mediante "set userid" para



obtener el acceso como "root". En cualquier caso debe registrarse en la bitácora todos los cambios de ID.

- ♦ Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.
- ♦ Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Jefe de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.
- ♦ Cuando un empleado es despedido o renuncia a la Empresa, debe desactivarse su cuenta antes de que deje el cargo.

CONTRASEÑAS Y EL CONTROL DE ACCESO

- ♦ Las carpetas compartidas, dentro de una Red, deben tener una Clave de Acceso, la misma que deberá ser cambiada periódicamente, por lo menos una vez al mes.
- ♦ El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
- ♦ Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.



CIB-ESPOL

- ♦ Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.
- ♦ La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
- ♦ Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.
- ♦ Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.
- ♦ Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.
- ♦ Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Empresa, pudiendo ser causal de despido.
- ♦ Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se

sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

5.4.3.8. SEGURIDAD EN LOS SERVIDORES

UBICACIÓN

- ♦ Los servidores de red y los equipos de comunicación (PABX, routers, switches etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras.

ACCESO Y RESPONSABILIDAD

- ♦ El jefe de Sistemas es el único responsable del uso, configuraciones, mantenimiento, respaldo, acceso y funcionamiento de todos los Servidores de la Empresa.
- ♦ El Jefe de Sistemas es la única persona autorizada para realizar cambios, respaldos, configurar y acceder de manera remota al sistema.
- ♦ El jefe de Sistemas es el responsable de proteger con contraseña el acceso al BIOS y de los Servidores.
- ♦ Cualquier Empresa y/o personal externo contratado por la Empresa, que requiera modificar, configurar, acceder remotamente en cualquiera de los servidores, debe tener un permiso previo del Jefe de Sistemas y el Gerente General.
- ♦ Cualquier trabajo que vaya a realizar una Empresa y/o personal externo contratado por la Empresa, debe ser supervisado y realizado en presencia del Jefe de Sistemas.



CIB-ESPOL

- ♦ El Jefe de Sistemas debe crear una cuenta de usuario temporal con los privilegios necesarios, para Empresa y/o personal externo contratado para acceder a cualquiera de los Servidores. Y su vigencia debe expirar inmediatamente después de realizar el trabajo.
- ♦ Se prohíbe el uso de cuentas anónimas o de invitado dentro de los servidores, el administrador entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que Jefe de Sistemas quien es el administrador del sistema Linux no deben entrar inicialmente como "root", sino primero empleando su propio ID y luego mediante "set userid" para obtener el acceso como "root". En cualquier caso debe registrarse en la bitácora todos los cambios de ID.

MANTENIMIENTO

- ♦ Los Servidores Principales: El Servidor con Linux Red Hat 9, El PC con Linux Red Hat 9(funciones de ruteo), Servidor con Windows NT. Todos estos deben estar ubicados dentro del departamento de Sistemas bajo supervisión y Auditoría del Jefe de Sistemas. Por ningún motivo deben ser movidos sin autorización conjunta del Jefe de Sistemas y El Gerente General.
- ♦ El jefe de Sistemas es el responsable de parchar periódicamente, cada seis meses (o cuando un parche de alguna vulnerabilidad este disponible y haya sido publicado de manera oficial en el Internet) los Sistemas Operativos y los Servicios instalados en los Servidores de la Empresa.
- ♦ Debe instalarse y activarse una herramienta antivirus (AVG) en todos los Servidores Linux y Windows NT, la cual debe mantenerse actualizada.
- ♦ El antivirus de los Servidores debe ser actualizado por el Jefe de Sistemas, por lo menos una vez al mes.

AUDITORÍA

- ♦ Los archivos de bitácora (logs) y los registros de Auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente por lo menos una vez por semana y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de Auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas como el Jefe de Sistemas y el Gerente General.
- ♦ Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

SERVIDOR LINUX

- ♦ Va a existir un Servidor bajo Linux ejecutando los siguientes Servicios, con sus políticas y configuraciones bien definidas: IPTables, IDS Snort, Sendmail, Squid, SSH.

SERVIDOR WINDOWS NT

- ♦ Debe tener instalado y configurado un Firewall (Zone Alarm).
- ♦ Este aloja las aplicaciones y base de datos bajo FoxPro de la Empresa.



CIB-ESPOL

POLÍTICAS DE RESPALDO EN LOS SERVIDORES

- ♦ Sin importar el tipo de información que se va a respaldar, esta debe ser almacenada en CDs.
- ♦ Semanalmente, es decir, por lo menos una vez por semana, debe hacerse el respaldo de los datos guardados y de los servidores.
- ♦ Las copias de respaldo deben guardarse en un lugar seguro y bajo llave dentro del Departamento de Sistemas de la Empresa, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de Empresa deben guardarse en otra sede, lejos del edificio en una de sus sucursales.
- ♦ En los servidores Linux, el Jefe de Sistemas, deberá hacer un respaldo total del disco.
- ♦ No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.
- ♦ Para ayudar a restaurar los programas originales no dañados o infectados el Jefe de Sistemas debe hacer copias de todo software nuevo antes de su uso, y debe guardarse tales copias en un lugar seguro en dispositivos como CDs.
- ♦ En el momento en que la información respaldada deje de ser útil a la organización, dicha información deberá ser borrada o destruida totalmente antes de deshacerse del medio.

5.4.4. PLANES DE CONTINGENCIA

5.4.4.1. ESTRATEGIAS DE RECUPERACIÓN DE DESASTRES

- ♦ Debe conformarse un grupo de desarrollo encargado de concebir, probar e implementar el plan de contingencias para el área de Tecnología de Información. Este debe estar a cargo del administrador del departamento de sistemas, e integrado por los líderes de cada área de la organización.
- ♦ Debe asignarse un orden de importancia a los sistemas de información y a los equipos de la red informática, de acuerdo al análisis de riesgo y al impacto que representaría para la empresa su ausencia.
- ♦ Deberán definirse las funciones o servicios críticos de la empresa, junto con los recursos mínimos necesarios para su funcionamiento, asignándoles una prioridad en el plan de contingencia.
- ♦ Deberán identificarse las contingencias que podrían ocurrir para cada nivel de servicio crítico definido.
- ♦ Deberá conformarse un plan de emergencias, determinando los procedimientos a llevar a cabo para cada contingencia identificada, considerando los distintos escenarios posibles. Cada procedimiento deberá estar claramente definido, y tener asignado un responsable para su ejecución.
- ♦ Para el desarrollo del plan de contingencias deben contemplarse las siguientes pautas:
 - ♦ Deberá estar documentado y testeado antes de su puesta en práctica.



CIB-ESPOL

- ♦ Deberá basarse en un análisis de riesgo, determinando que acciones merecen estar incluidas.
- ♦ Deberá abarcar la totalidad del área de Tecnología Información.
- ♦ Deberá mantenerse actualizado de acuerdo a nuevos puestos de trabajos y funciones.
- ♦ Deberá ser probado con cierta periodicidad.
- ♦ Deberá contener la siguiente información:
 - ♦ Objetivo del plan,
 - ♦ Tiempo de duración,
 - ♦ Recursos necesarios,
 - ♦ Evento a partir del cual se pondrá en marcha el plan.
- ♦ Debe documentarse la realización de las siguientes actividades después de un incidente:
 - ♦ Determinar la causa del daño,
 - ♦ Evaluar la magnitud del daño que se ha producido,
 - ♦ Qué sistemas se han afectado,
 - ♦ Qué modificaciones de emergencia se han realizado,
 - ♦ Qué equipos han quedado no operativos,
 - ♦ Cuales se pueden recuperar y en cuanto tiempo.
 - ♦ Costos involucrados



Cada una estas actividades deberán ser reportadas por los líderes de cada área a un miembro de la Gerencia.

- ♦ Deberá asignarse el papel de coordinador a un empleado, que se encargará de las operaciones necesarias para que el sistema funcione correctamente

después de la emergencia. Éste deberá determinar las acciones a seguir basándose en el plan de emergencias.

- ♦ Deberá retroalimentarse el plan luego de una contingencia, ajustando las directivas en consecuencia.
- ♦ Deben establecerse planes de prueba periódicos que incluyan simulacros de siniestros para evaluar la eficacia y eficiencia del plan.

5.4.5. RECOMENDACIONES DE POLÍTICAS

CAPACITACIÓN

- ♦ El personal en general de la Empresa, debe ser capacitado constantemente en temas de seguridad. Como por ejemplo: manejo de extinguidores, Planes de contingencia, uso de un Firewall, Manejo de utilitarios y aplicaciones informáticas, Vulnerabilidades y Precauciones al navegar en el Internet, virus, gusanos, troyanos, Ingeniería Social.
- ♦ El Jefe de Sistemas debe estar en capacitación constante en temas de seguridad de redes y servidores. Como por ejemplo: Administración y manejo de Servicios de los Servidores en Linux y Windows, Manejo y administración de respaldos de seguridad, Vulnerabilidades, Nuevas formas de ataque y riesgos, Planes de Contingencia, Administración y configuración de la Red.

CONCLUSIONES

La seguridad de las redes de comunicaciones, y concretamente el Internet, evoluciona a pasos agigantados cada minuto que transcurre. Nuevas vulnerabilidades y utilidades, tanto para explotarlas como para combatirlas, son distribuidas públicamente en la red. La información disponible al respecto es inmanejable, por lo que el diseño de un sistema de seguridad debe basarse en la fortaleza de las tecnologías empleadas, y no en la ocultación de las mismas.

La seguridad de la empresa MAFRICO S.A., no debe basarse en una sola técnica de protección, sino que debe ser reforzada por varias metodologías que permitan monitorear y gestionar cada uno de los aspectos de la red. LA gerencia junto con el Administrador de la red, tendrán que revisar periódicamente los procedimientos y políticas actuales y actualizarlas de ser necesario, de tal forma que estas se ajusten conforme avanzan las vulnerabilidades del sistema informático. Además hay que concienciar y capacitar a los usuarios en lo que concierne a seguridad informática.

Finalmente, con nuestro trabajo por lo menos hemos asegurado el 60% en los tres pilares fundamentales de la seguridad como son la integridad de la información, la privacidad y la confidencialidad.



CIB-ESPOL

RECOMENDACIONES



CIB-ESPOL

Después de haber realizado este proyecto y haber presentado soluciones para los problemas actuales de la red MAFRICO S.A., es necesario que la empresa haga un énfasis en los siguientes aspectos:

- ♦ Constante capacitación del personal que utiliza la red, según sus funciones.
- ♦ Restringir el acceso al departamento de Sistemas ya que actualmente cualquier persona tiene libre acceso.
- ♦ La Gerencia debe asignar un mayor presupuesto destinado a reforzar la seguridad y optimización de la red ya que es necesario el reemplazo de varios equipos obsoletos que bajan el rendimiento de la misma, como también la adquisición de nuevo software que facilite y permita una Auditoría efectiva y constante de toda la red.
- ♦ La empresa debe incorporar dentro de sus políticas sanciones o reprensiones para los usuarios que den un mal uso de los recursos informáticos.
- ♦ Se debe establecer un plan de contingencia completo y bien estructurado en todas las áreas importantes, de tal modo que se disminuyan los riesgos en caso de que las condiciones normales cambien totalmente en cierto momento.

Lo descrito anteriormente es fundamental para complementar nuestra propuesta de seguridad requerida para la red MAFRICO S.A.

ANEXOS



CIB-ESPOL

ANEXO A

"ESCANEEO EXTERNO"

PUERTOS TCP ABIERTOS EN EL SERVIDOR LINUX

The screenshot displays a network scanning application interface. At the top, the 'Scan Target' is set to '200.93.233.42' and the 'Profile' is 'Default'. The 'Scan Results' pane on the right lists the following open ports and services:

- 21 [FTP => File Transfer Protocol]
 - 220 [vsFTPd 1.1.3]
- 22 [SSH => Remote Login Protocol]
 - SSH-1.99-OpenSSH_3.5p1
- 23 [Telnet => Remote Login Protocol]
- 25 [SMTP => Simple Mail transfer Protocol]
 - 220 AVG ESMTP Proxy Server Beta - 7.0.279/7.0.280 [264.10.3]
- 110 [Pop3 => Post Office Protocol 3]
- 8080 [Http-Proxy]
 - HTTP/1.0 400 Bad Request
 - Server: squid/2.5.STABLE1
 - Mime-Version: 1.0
 - Date: Sun, 07 Nov 2004 06:18:54 GMT
 - Content-Type: text/html
 - Content-Length: 1207
 - Expires: Sun, 07 Nov 2004 06:18:54 GMT
 - X-Squid-Error: ERR_INVALID_REQ 0
 - X-Cache: MISS from maffico
 - Proxy-Connection: close

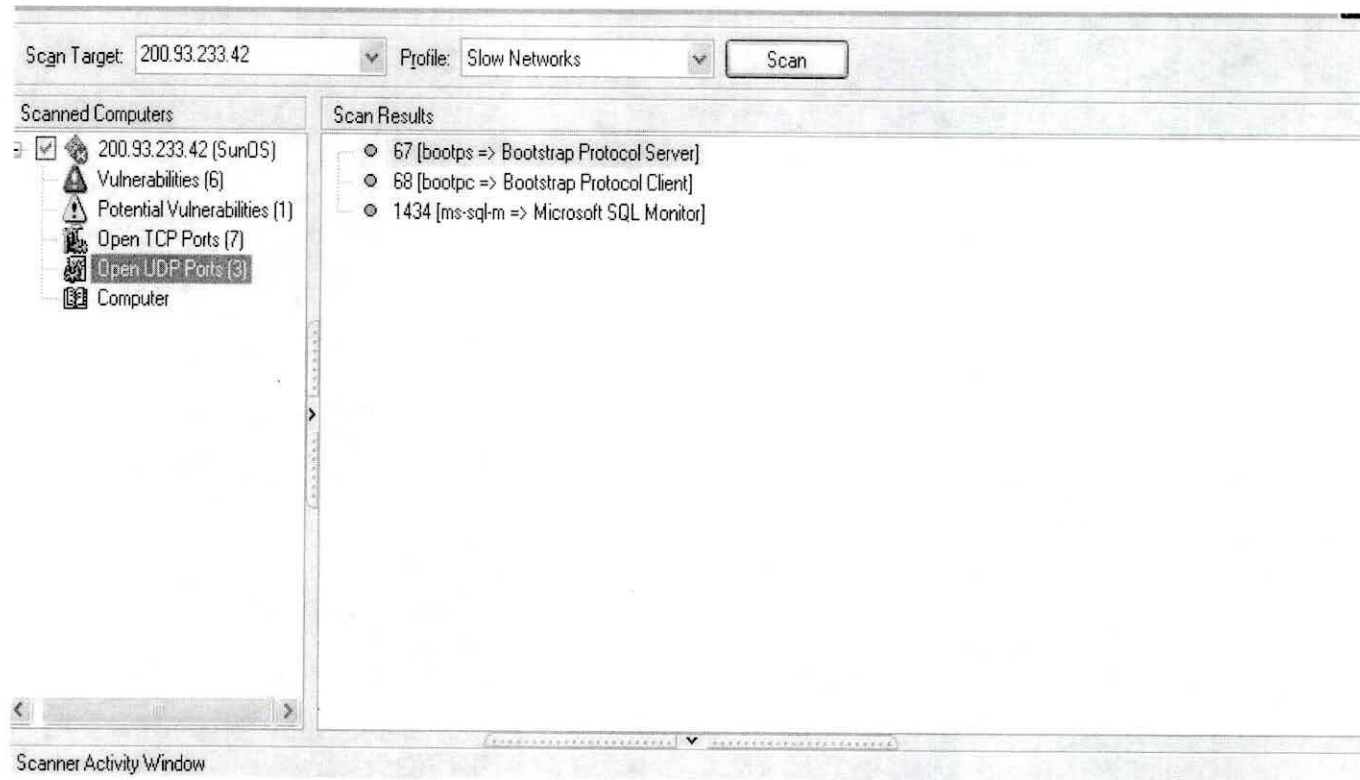
Three Telnet session windows are overlaid on the main interface:

- Telnet 200.93.233.42**: Shows the SSH banner 'SSH-1.99-OpenSSH_3.5p1'.
- Telnet 200.93.233.42**: Shows the Red Hat Linux banner 'Red Hat Linux release 9 <Shrike> Kernel 2.4.20-8 on an i686' followed by a 'login:' prompt and the message 'Se ha perdido la conexión con el host.'.
- Telnet 200.93.233.42**: Shows the banner '220 AVG ESMTP Proxy Server Beta - 7.0.279/7.0.280 [264.10.3]'.

A file explorer window titled 'ftp://200.93.233.42/ - Micros...' is also visible, showing a directory listing with a folder named 'pub'.



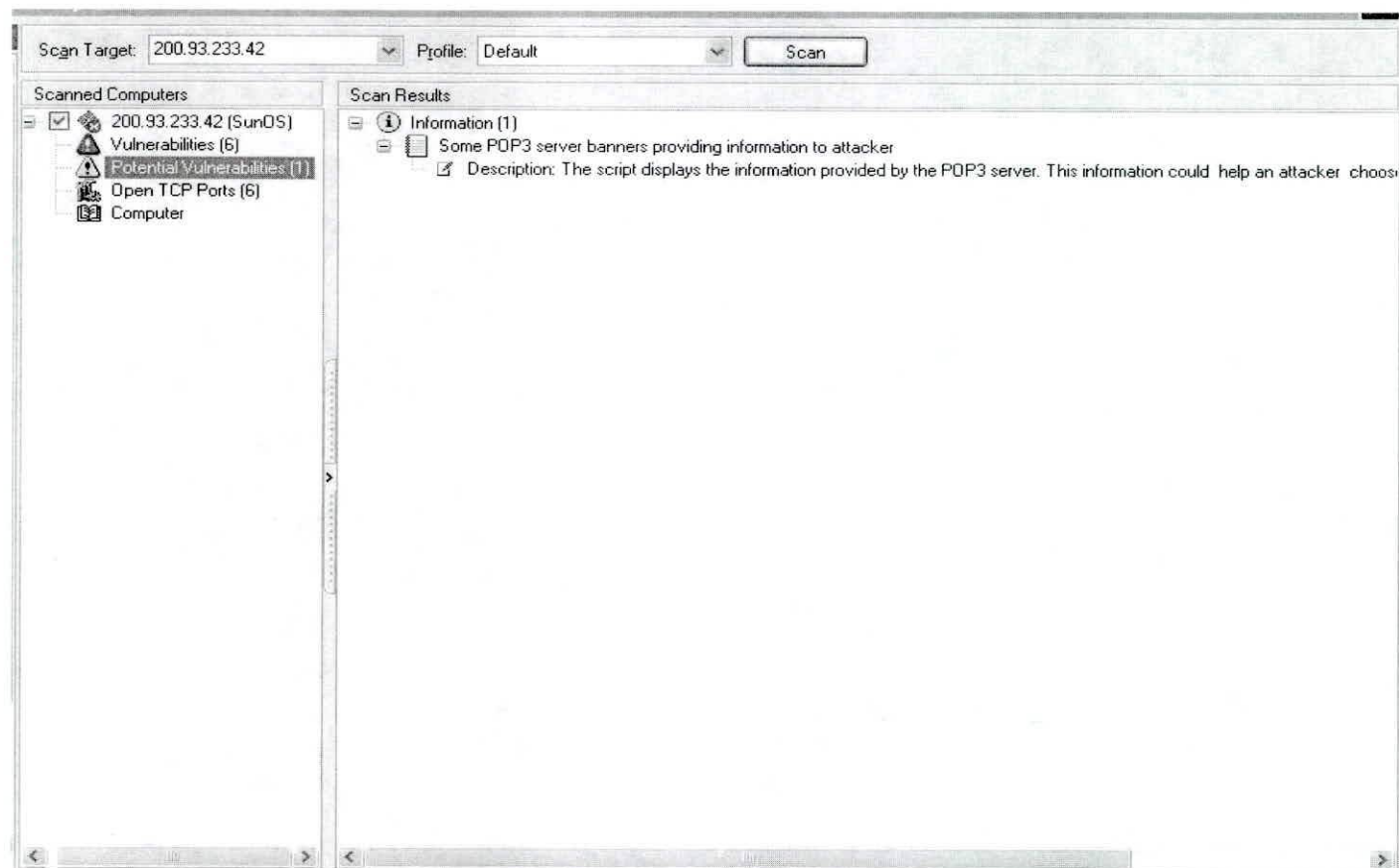
PUERTOS UDP ABIERTOS EN EL SERVIDOR LINUX



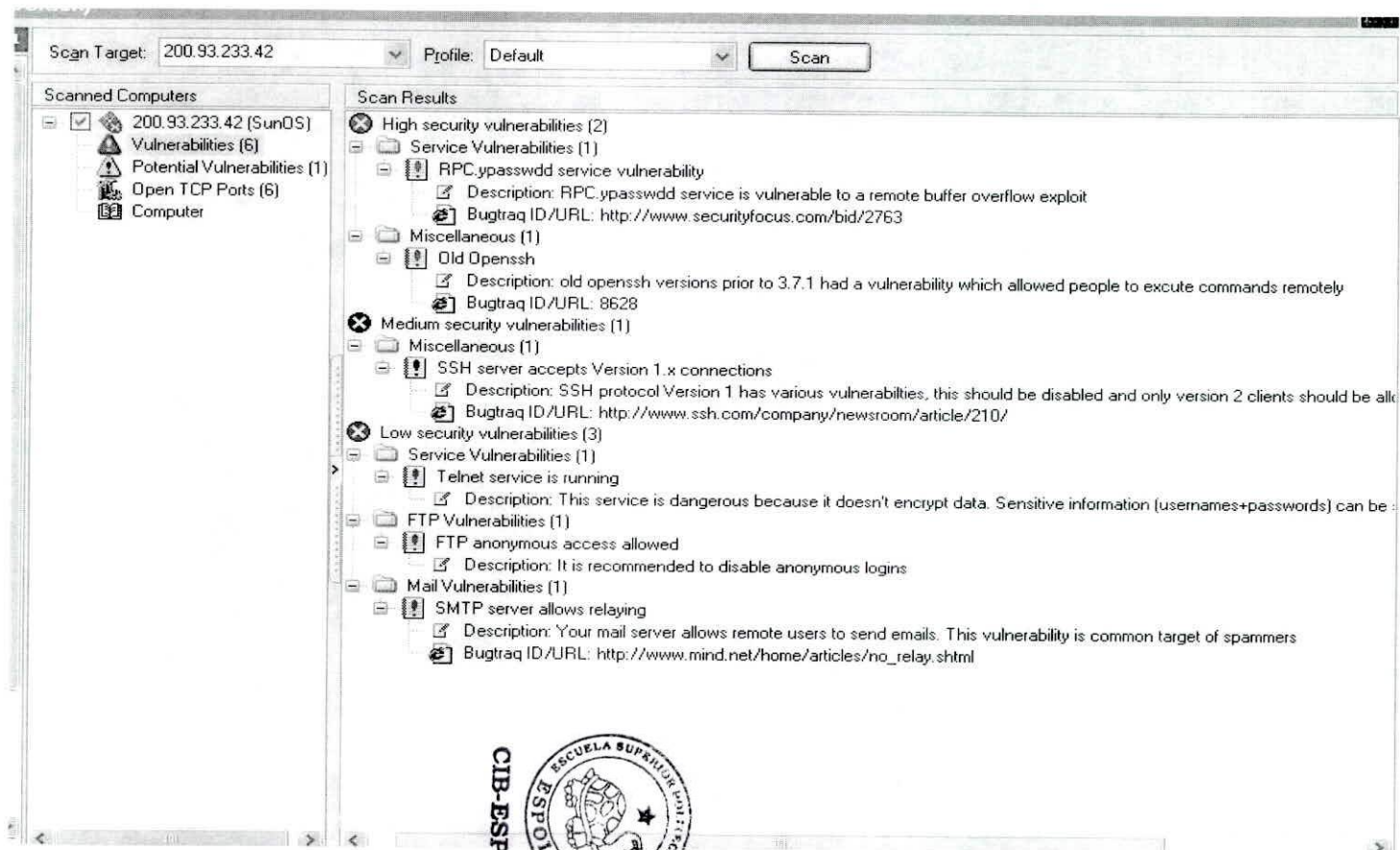
CIB-ESPOL



POTENCIALES VULNERABILIDADES EN EL SERVIDOR LINUX



VULNERABILIDADES EN EL SERVIDOR LINUX



CIB-ESPOL



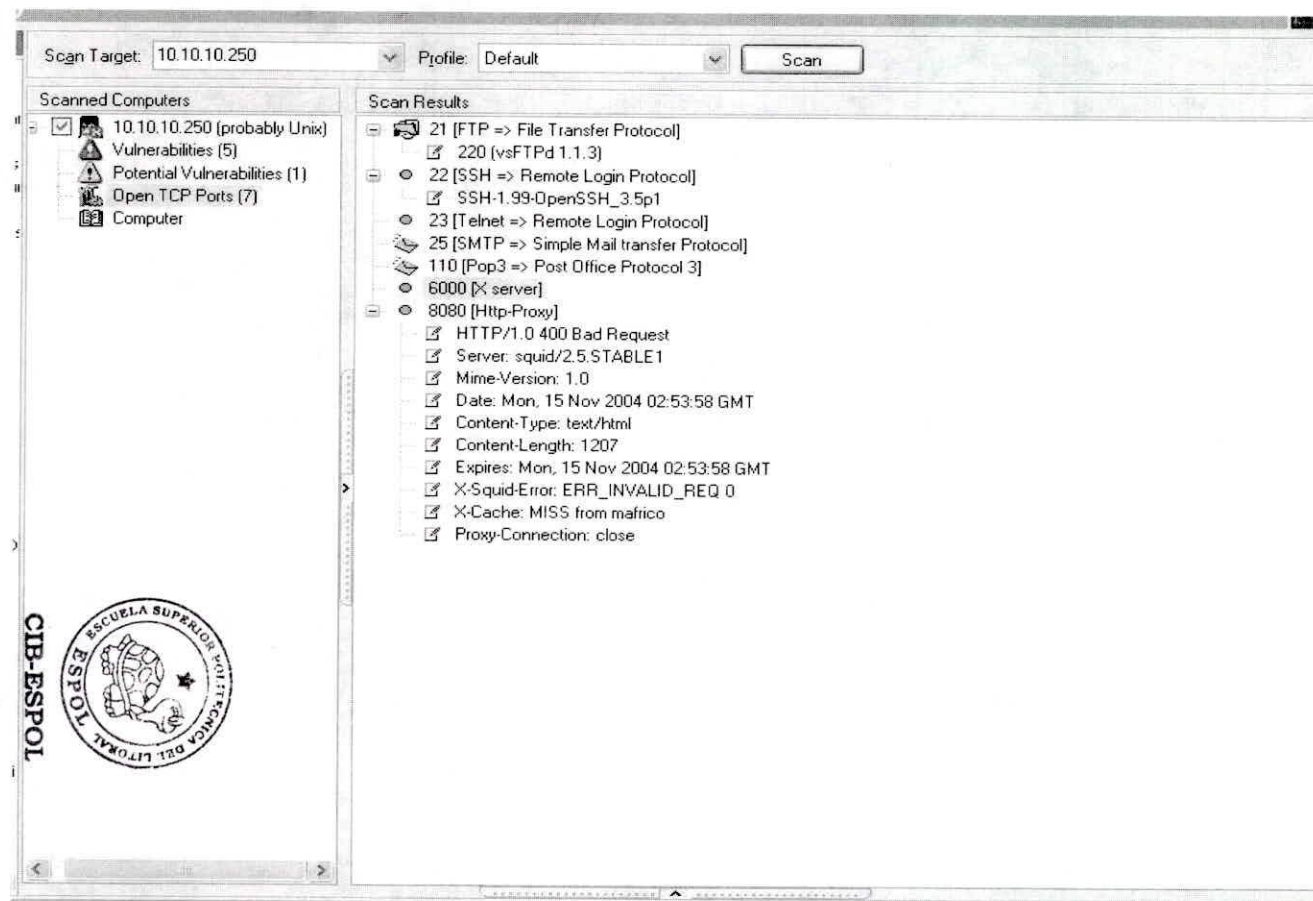
ANEXO B

"ESCANEEO INTERNO"

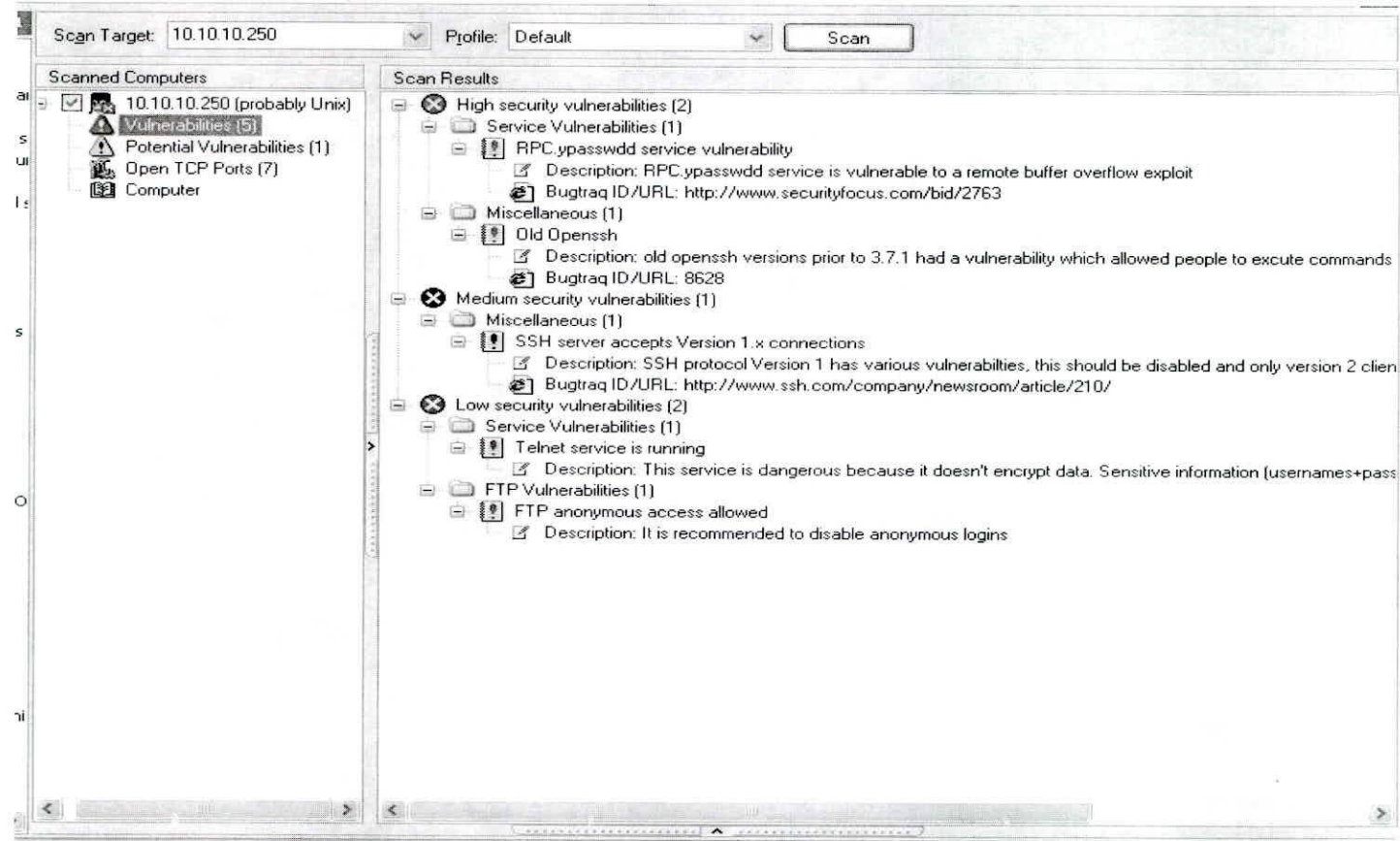


CIB-ESPOL

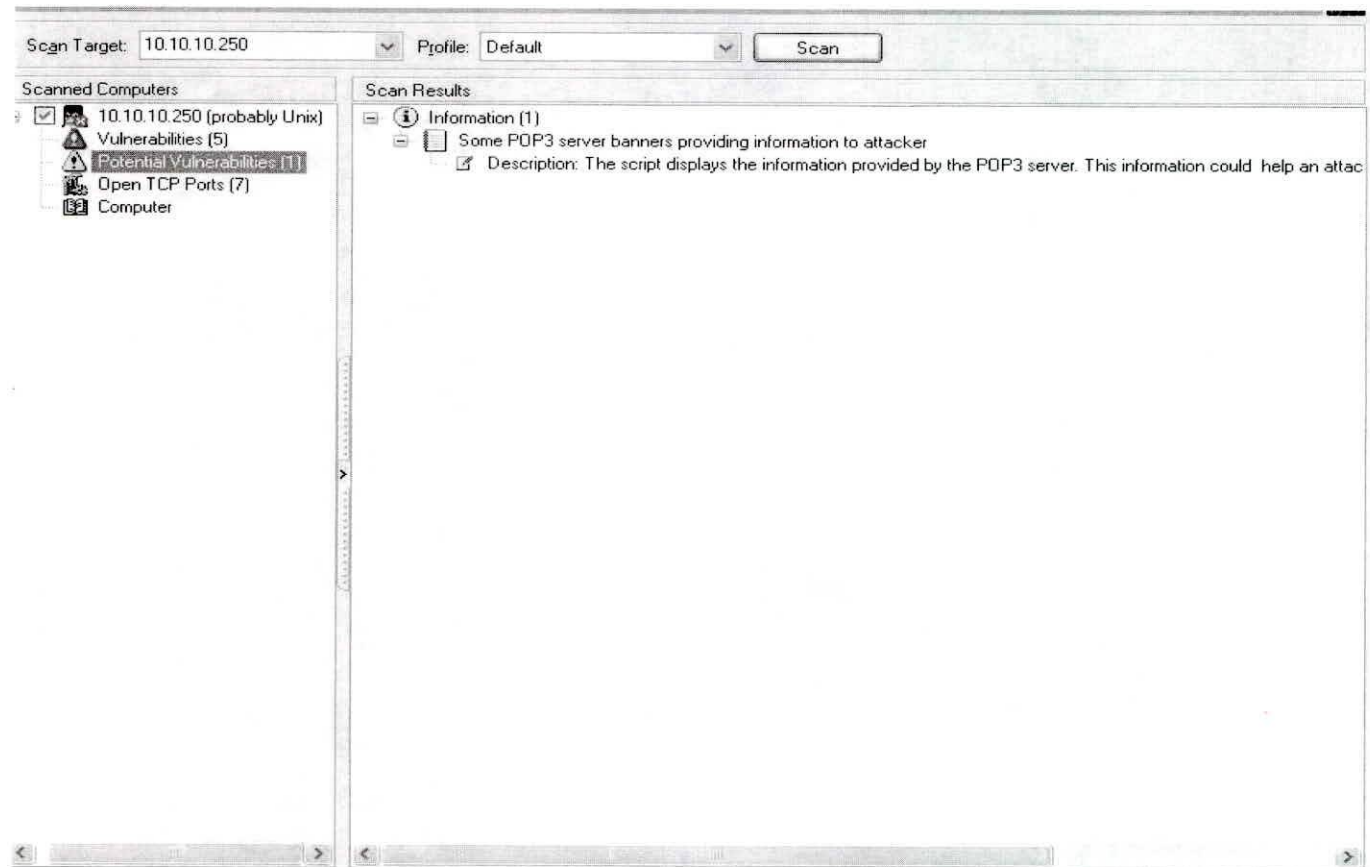
PUERTOS TCP ABIERTOS EN LA RED INTERNA (Lan)



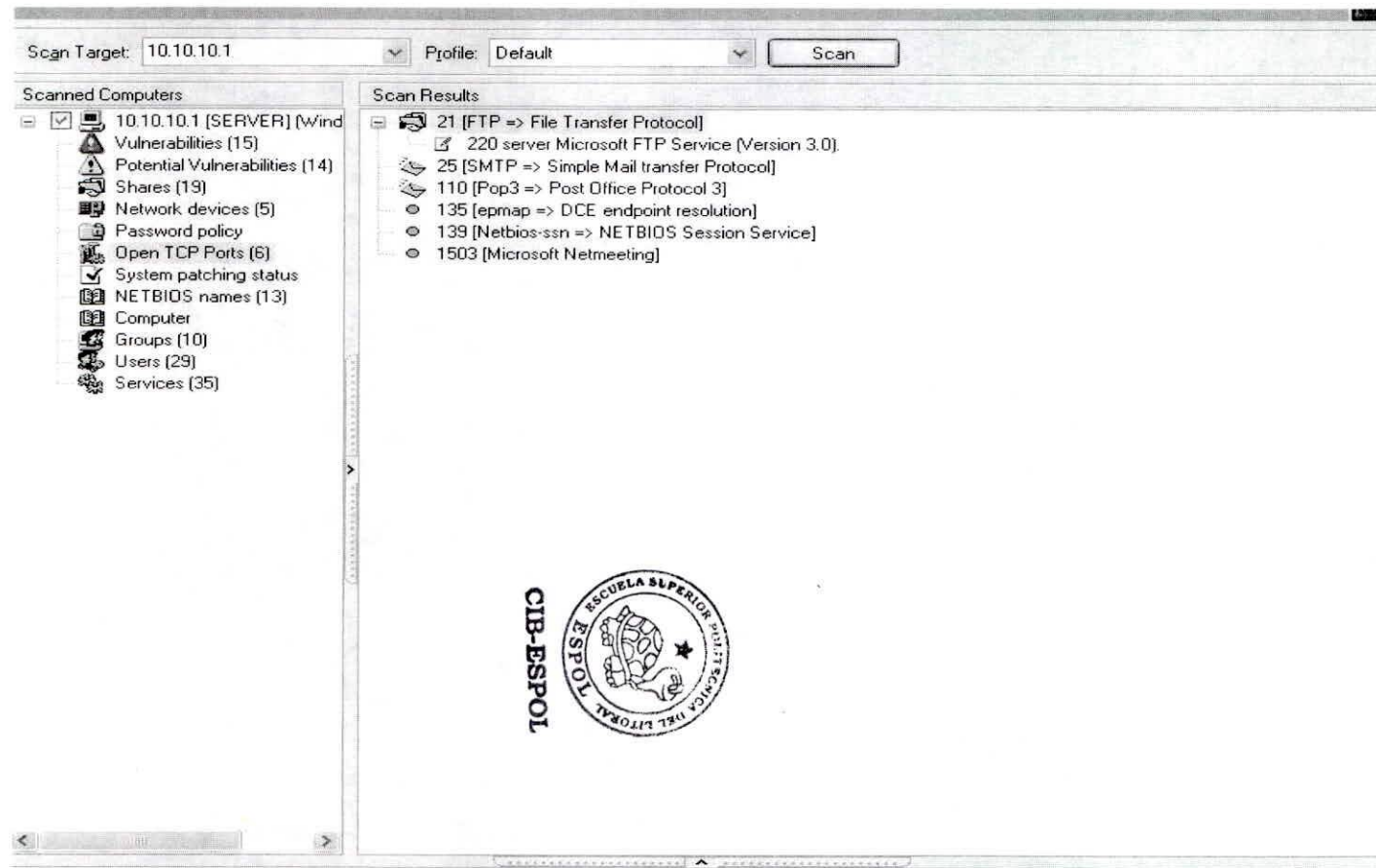
VULNERABILIDADES EN LA RED INTERNA (Lan)



POTENCIALES VULNERABILIDADES EN LA RED INTERNA (Lan)



PUERTOS TCP ABIERTOS EN EL SERVIDOR WINDOWS NT



POTENCIALES VULNERABILIDADES EN EL SERVIDOR WINDOWS NT

Scan Target: 10.10.10.1 Profile: Default Scan

Scanned Computers

- 10.10.10.1 [SERVER] (wind)
- Vulnerabilities (15)
- Potential Vulnerabilities (14)
- Shares (19)
- Network devices (5)
- Password policy
- Open TCP Ports (6)
- System patching status
- NETBIOS names (13)
- Computer
- Groups (10)
- Users (29)
- Services (35)

Scan Results

- Non-detectable patches (10)
- Windows NT Server 4.0 Service Pack 6a
 - MS04-024 (839645)
 - Title: Vulnerability in Windows Shell Could Allow Remote Code Execution (839645)
 - Reason: Cannot determine if this patch is installed or not.
 - Date posted: 2004/07/13
 - Date revised: 2004/07/13
 - URL: NA
 - MS04-022 (841873)
 - Title: Vulnerability in Task Scheduler Could Allow Code Execution (841873)
 - Reason: Cannot determine if this patch is installed or not.
 - Date posted: 2004/07/13
 - Date revised: 2004/07/13
 - URL: <http://download.microsoft.com/download/5/0/0/5004c98d-cacc-42d5-980c-b5c9efb7a627/IE-KBE>
 - MS03-030 (819696)
 - Title: Unchecked Buffer in DirectX Could Enable System Compromise (819696)
 - Reason: Cannot determine if this patch is installed or not.
 - Date posted: 2003/07/23
 - Date revised: 2003/07/23
 - URL: <http://www.microsoft.com/technet/security/bulletin/MS03-030.mspx>
 - MS03-019 (817772)
 - Title: Flaw in ISAPI extension for Windows Media Services could cause denial of service (817772)
 - Reason: Cannot determine if this patch is installed or not.
 - Date posted: 2003/05/28
 - Date revised: 2003/05/28
 - URL: <http://download.microsoft.com/download/7/3/c/73c35094-45f4-469d-9609-2c7288abeec3/window>
 - MS03-008 (814078)
 - Title: Flaw in Windows Script Engine could allow code execution (814078)
 - Reason: Cannot determine if this patch is installed or not.
 - Date posted: 2003/03/19
 - Date revised: 2003/03/19
 - URL: <http://download.microsoft.com/download/5/c/f/5cfd55d8-74b2-4338-868b-129ec01b5bd4/js56mei>
 - MS02-053 (324096)

CIB-ESPOL



POTENCIALES VULNERABILIDADES EN EL SERVIDOR WINDOWS NT

The screenshot displays a security scanning application window. At the top, the 'Scan Target' is set to '10.10.10.1' and the 'Profile' is 'Default'. A 'Scan' button is visible. The left pane, titled 'Scanned Computers', shows a tree view with the following items: 10.10.10.1 [SERVER] (Windows), Vulnerabilities (15), Potential Vulnerabilities (14), Shares (19), Network devices (5), Password policy, Open TCP Ports (6), System patching status, NETBIOS names (13), Computer, Groups (10), Users (29), and Services (35). The right pane, titled 'Scan Results', shows a list of vulnerabilities and information. The vulnerabilities listed are: MS01-022 (296441) with title 'WebDAV Service Provider Can Allow Scripts to Levy Requests as User', MS99-041 (242294) with title 'RASMAN Security Descriptor Vulnerability', MS99-036 (155197) with title 'Windows NT 4.0 Does Not Delete Unattended Installation File', and MS98-001 (169556) with title 'Disabling Creation of Local Groups on a Domain by Non-Administrative Users'. Each vulnerability entry includes details such as the reason, date posted, date revised, and a URL. Below the vulnerabilities, there is an 'Information (4)' section listing four users: User Apagado, User charlie, User FINANCIERO2\$, and User SERVER\$, each with a description recommending removal if not used.

Scan Target: 10.10.10.1 Profile: Default Scan

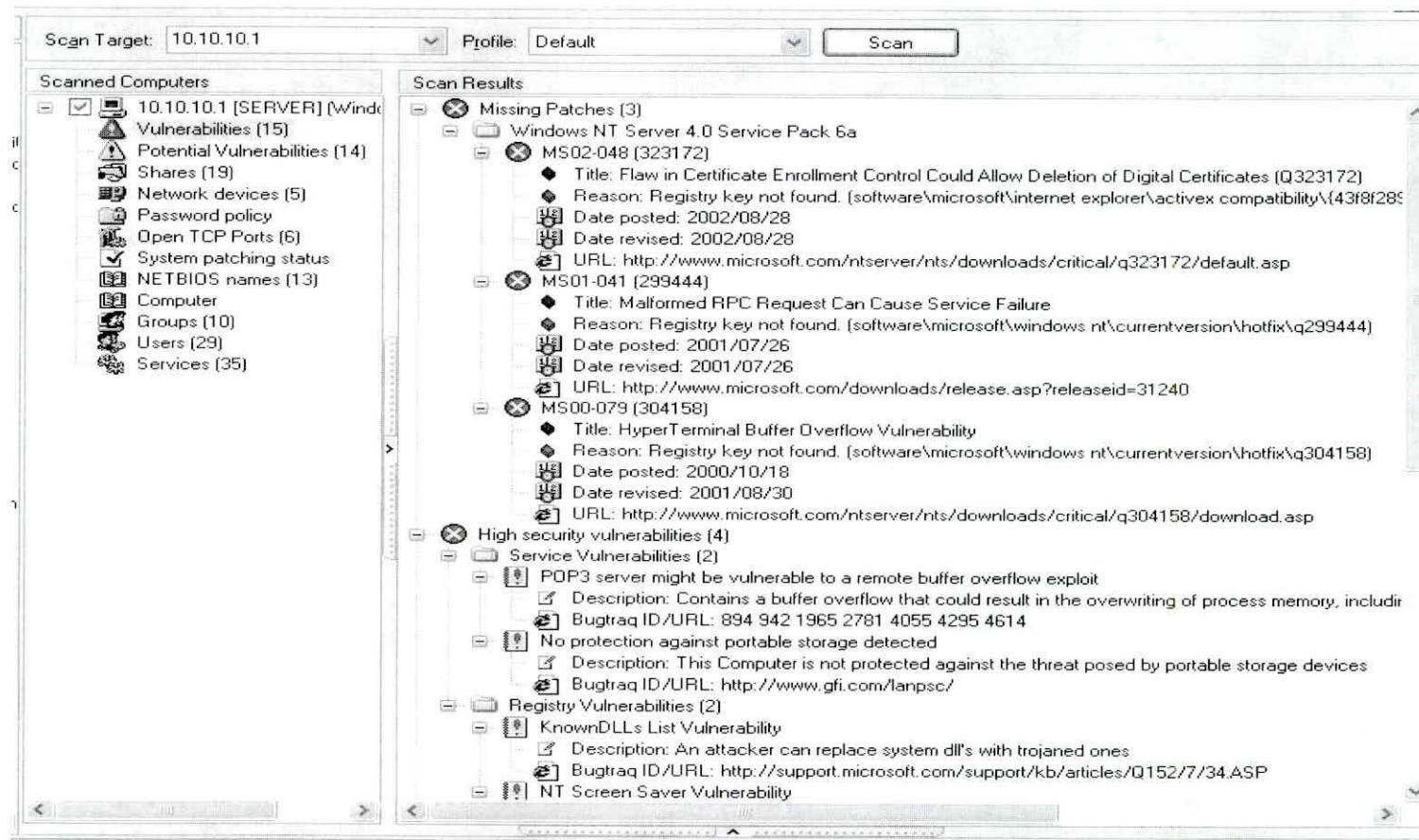
Scanned Computers

- 10.10.10.1 [SERVER] (Wind
- Vulnerabilities (15)
- Potential Vulnerabilities (14)
- Shares (19)
- Network devices (5)
- Password policy
- Open TCP Ports (6)
- System patching status
- NETBIOS names (13)
- Computer
- Groups (10)
- Users (29)
- Services (35)

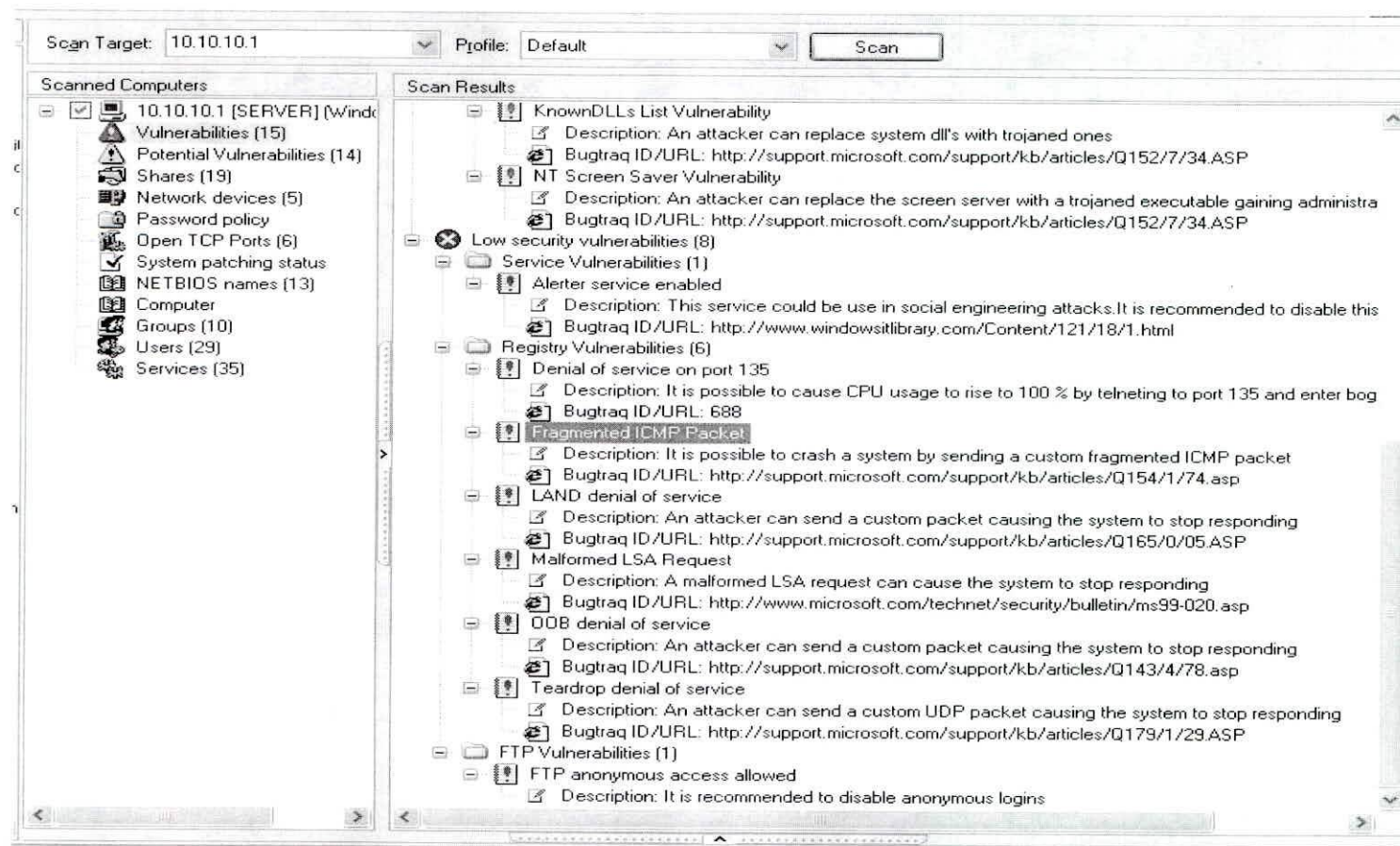
Scan Results

- MS01-022 (296441)
 - Title: WebDAV Service Provider Can Allow Scripts to Levy Requests as User
 - Reason: Cannot determine if this patch is installed or not.
 - Date posted: 2001/04/18
 - Date revised: 2001/04/18
 - URL: <http://download.microsoft.com/download/win2000platform/update/1.5/win98me/en-us/rbupdate.e>
- MS99-041 (242294)
 - Title: RASMAN Security Descriptor Vulnerability
 - Reason: Cannot determine if this patch is installed or not.
 - Date posted: 1999/09/30
 - Date revised: 1999/09/30
 - URL: <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postsp6/security/rasman->
- MS99-036 (155197)
 - Title: Windows NT 4.0 Does Not Delete Unattended Installation File
 - Reason: Cannot determine if this patch is installed or not.
 - Date posted: 1999/09/10
 - Date revised: 1999/09/10
 - URL: <http://www.microsoft.com/technet/security/bulletin/ms99-036.asp>
- MS98-001 (169556)
 - Title: Disabling Creation of Local Groups on a Domain by Non-Administrative Users
 - Reason: Cannot determine if this patch is installed or not.
 - Date posted: 1998/06/01
 - Date revised: 1999/03/24
 - URL: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/nt40/i386/creatals_x86.exe
- Information (4)
 - User Apagado never logged on
 - Description: It is recommended to remove this account if not used
 - User charlie never logged on
 - Description: It is recommended to remove this account if not used
 - User FINANCIERO2\$ never logged on
 - Description: It is recommended to remove this account if not used
 - User SERVER\$ never logged on
 - Description: It is recommended to remove this account if not used

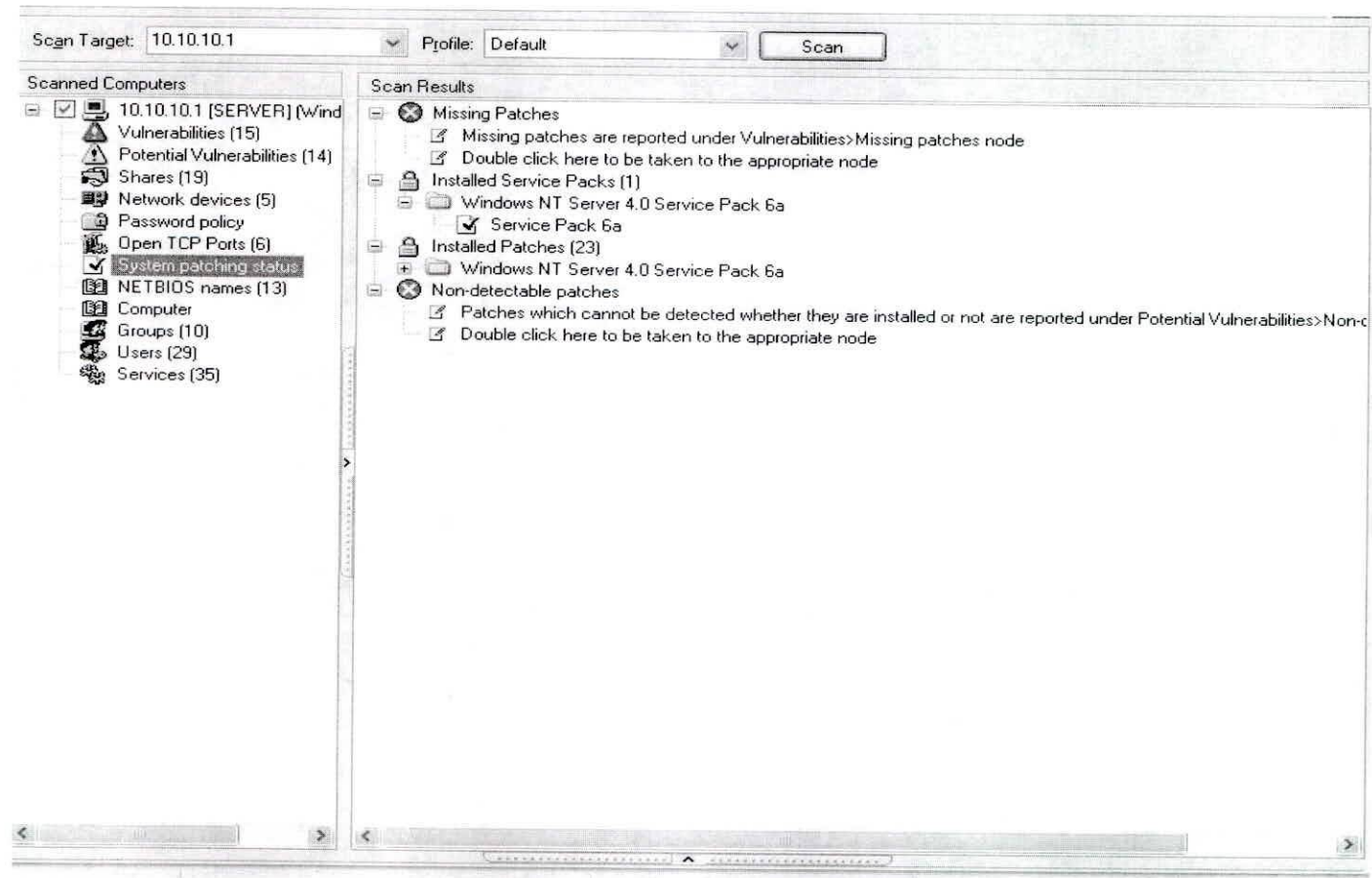
VULNERABILIDADES EN EL SERVIDOR WINDOWS NT



VULNERABILIDADES EN EL SERVIDOR WINDOWS NT



ESTATUS DE PARCHES DE ACTUALIZACIONES EN EL SERVIDOR WINDOWS NT



SERVICIOS ACTIVOS EN EL SERVIDOR WINDOWS NT

Scan Target: 10.10.10.1 Profile: Default Scan

Scanned Computers

- 10.10.10.1 [SERVER] (Windows NT)
- Vulnerabilities (15)
- Potential Vulnerabilities (14)
- Shares (19)
- Network devices (5)
- Password policy
- Open TCP Ports (6)
- System patching status
- NETBIOS names (13)
- Computer
- Groups (10)
- Users (29)
- Services (35)**

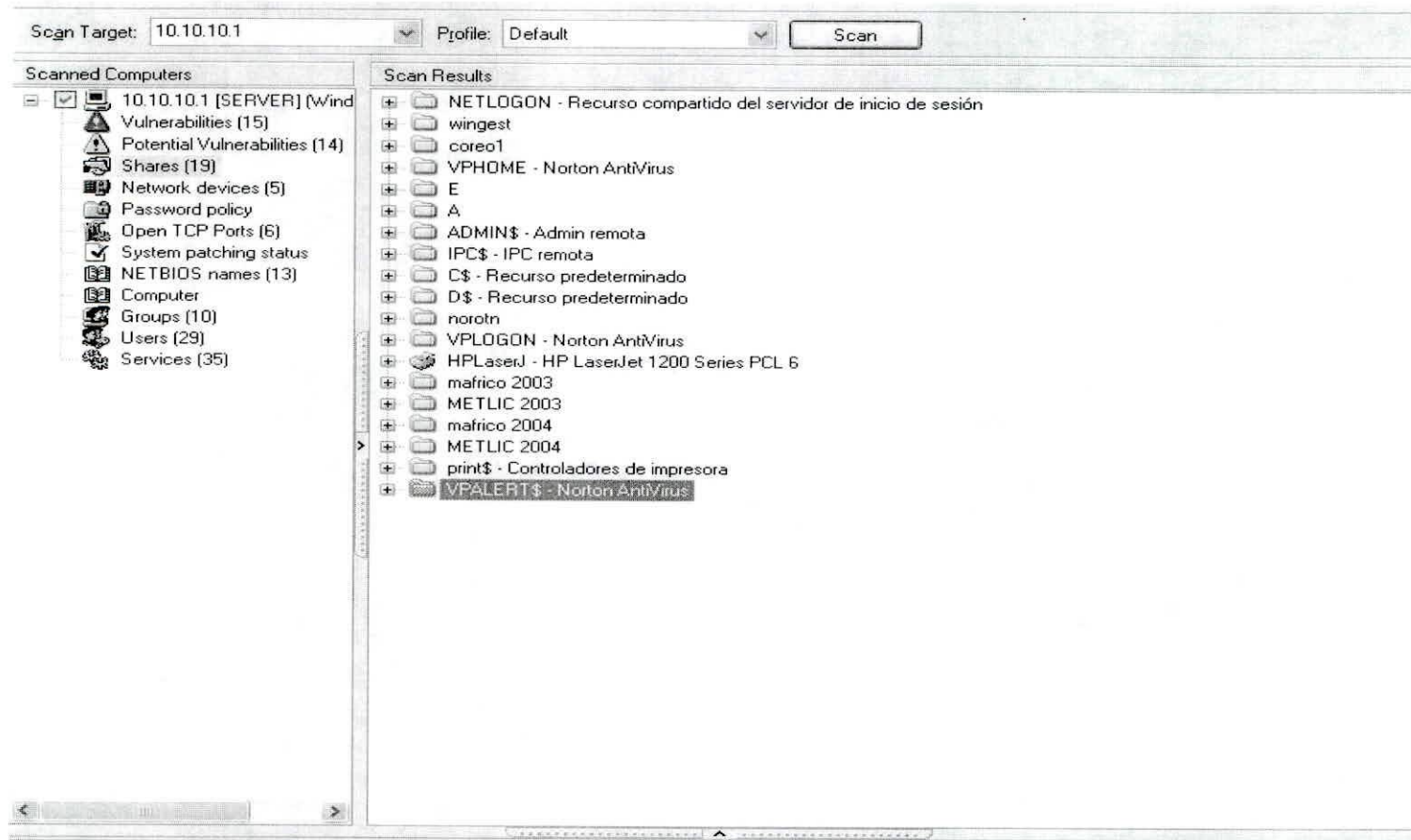
Scan Results

Service	Display Name	Status	StartUp Type
Alerter	Alerta	Running	Automatic
Browser	Examinador de equipos	Running	Automatic
ClipSrv	Servidor del portapapeles	Stopped	Manual
DefWatch	DefWatch	Running	Automatic
DHCP	Cliente DHCP	Stopped	Disabled
EventLog	EventLog	Running	Automatic
EventSystem	COM+ Event System	Stopped	Manual
GOPHERSVC	Servicio de publicación Gopher	Running	Automatic
Intel Alert Handler	Intel Alert Handler	Running	Automatic
Intel Alert Originator	Intel Alert Originator	Running	Automatic
Intel File Transfer	Intel File Transfer	Running	Automatic
Intel PDS	Intel PDS	Running	Automatic
LanmanServer	Servidor	Running	Automatic
LanmanWorkstation	Estación de trabajo	Running	Automatic
LicenseService	Servicio de registro de licencias	Running	Automatic
LmHosts	Ayuda de NetBIOS de TCP/IP	Running	Automatic
Messenger	Mensajería	Running	Automatic
MSFTPSVC	Servicio de publicación FTP	Running	Automatic
MSIServer	Windows Installer	Stopped	Manual
NetDDE	DDE de red	Stopped	Manual
NetDDEdsdm	DSDM de DDE de red	Stopped	Manual
Netlogon	Inicio de sesión	Running	Automatic
Norton AntiVirus S...	Norton AntiVirus Server	Running	Automatic
NtLmSsp	Proveedor de seguridad NT LM	Running	Manual
PlugPlay	Plug and Play	Running	Automatic
ProtectedStorage	Protected Storage	Running	Automatic
Replicator	Duplicador de directorios	Stopped	Manual
RPCLOCATOR	Localizador de llamada a procedimientos remotos (RPC)	Running	Automatic
RpcSs	Servicio de RPC (llamada a proc. remoto)	Running	Automatic
Schedule	Task Scheduler	Running	Automatic

CIB-ESPOL



SERVICIOS COMPARTIDOS EN EL SERVIDOR WINDOWS NT



BIBLIOGRAFÍA

a) Tesis

M. Dolores Cerini Y Pablo Ignacio Prá "Plan De Seguridad Informática" (Tesis, Facultad De Ingeniería En Sistemas, Universidad De Córdoba, 2002).

b) Tesis

Antonio Villalón Huerta, "Seguridad En Unix Y Redes" (Tesis, Universidad Politécnica de Valencia, Versión 2.1, 2002)

c) Tesis

Cristian F. Borghello, "Seguridad Informática: Sus implicancias e implementación" (Tesis, Universidad Tecnológica Nacional de Argentina, 2001).

d) Libro

Red Hat, Inc., Red Hat Linux 9: Red Hat Linux Security Guide, (2002).

e) Artículo de internet

Kaleem Anwar Muhammad Amir Ahmad Saeed Muhammad Imran, "The Linux Router", Revista Linux Journal, Jueves 01 agosto, 2002.
<http://www.linuxjournal.com>

f) Artículo de internet

Ricky M. Magalhaes. "Host-Based IDS vs Network-Based IDS, Part 2 - Comparative Analysis", Windows Security, Jul 23, 2004.
http://www.windowsecurity.com/articles/Hids_vs_Nids_Part2.html.

g) Reporte Técnico

Alex Rousskov, Duane Wessels, The Third Cache-Off, (The Measurement Factory, Inc., October 11, 2000) <http://www.measurement-factory.com/results/>

Internet:

<http://www.snort.org>

<http://www.squid-cache.org>

<http://www.hackemate.com.ar/tools/>

<http://www.netfilter.org>

<http://www.yolinux.com>

<http://www.linuxparatodos.com>

<http://infosecuritymag.techtarget.com>

<http://cacheoff.ircache.net/>

<http://www.segu-info.com.ar/>



CIB-ESPOL

<http://www.qmail.org>

<http://www.linuxrouter.org>

<http://www.redhat.com>

<http://www.nwfusion.com/reviews/2000/0410tables.html#price>

<http://www.geocities.com/mailsoftware42/>



CIB-ESPOL