ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

"IMPLEMENTACIÓN DEL MANUAL DE LA METODOLOGÍA ABIERTA DE TESTEO DE SEGURIDAD AL DEPARTAMENTO DE SISTEMAS DEL INTERAMERICAN ACADEMY"

TESIS DE GRADO

Previo a la obtención del Título de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

ING. FRANCISCO BOLAÑOS

GUAYAQUIL – ECUADOR
2013

AGRADECIMIENTO

A Dios.

A mis padres, familiares y amigos por el apoyo incondicional

en mi vida personal y profesional.

Especialmente a mi director de tesis

y al Magíster Lenin Freile

por ser mis mentores en este proyecto.

DEDICATORIA

A Dios.

A mis padres, familiares y amigos.

Alas siguientes personas

por ser quienes han influenciado mi vida:

Piedad Estarellas,

Susana Alonso,

Patricia McTeague,

Sonya Rendón y

Celeste Blacio

TRIBUNAL GRADUACIÓN

PhD. Jorge Olaya
Director de tesis

MBA. Karina Astudillo
Miembro del tribunal

Msig. Albert Espinal
Miembro del tribunal

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

Ing. Francisco Bolaños

RESUMEN

En el presente trabajo de graduación se detalla la implementación del Manual de Metodología Abierta de Testeo de Seguridad a los activos críticos del departamento de sistemas del InterAmerican Academy.

En el capítulo 1 se explica : los antecedentes y el planteamiento del problema, la justificación , los objetivos y el alcance de la solución.

En el capítulo 2 muestra el análisis de metodologías y herramientas para llegar a cabo este proyecto. En esta sección se detalla las características de las metodologías y herramientas para luego realizar las comparaciones respectivas.

En el capítulo 3 se aplica el Manual de Metodología Abierta de Testeo de Seguridad aplicando las fases respectivas de la misma. Por motivos explicados en el marco teórica de la metodología, ciertas fases y módulos no se mostarán ni se implementarán.

En el capítulo 4 se emplean las métricas para Los Valores de Evaluación del Riesgo. También se mostrará el nivel de seguridad actual así como el reporte STAR.

Las conclusiones y recomendaciones sobre la implementación de la metodología se mencionan al final de este trabajo de graduación.

ÍNDICE GENERAL

ABREVIATURAS

IAA: InterAmerican Academy.

MMATS: Metodología Abierta de Testeo de Seguridad.

MMATS STAR: Primer reporte MMTAS.

ISECOM: Instituto de Seguridad de Metodologías Libres.

VER: Valores de Evaluación de Riesgo

MESSI: Marco de Evaluación de Seguridad de Sistemas de Información.

OISSG: Open Information Security System Group.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCION

En la actualidad la seguridad de la información es uno de los temas que está en auge en cuanto a informática se refiere . En el caso particular de InterAmerican Academy debido al nuevo programa que se ha implementado: one to one laptop program, el cual consiste en el uso de portátiles como principal útil escolar. La seguridad de la información juega un rol importante para la institución debido a que se debe garantizar que el contenido de internet que los estudiantes acceden sea el apropiado y controlar el uso de los dispotivos en la red.

Las pruebas de penetración sirven para encontrar falencias de seguridad en una compañía, pero estas no permiten guardar un registro estándar en la seguridad actual. Es por eso que se ha decidido implementar el Manual de la Metodología Abierta de Seguridad para a través de los Valores de Evaluación de Riesgo medir el nivel actual de seguridad de los activos críticos del departamento de sistemas.

La medición del nivel de seguridad servirá para establecer una base comparativa y poder saber si se ha mejorado en el nivel de seguridad. Además se puede aplicar el mismo procedimiento en otros dispositivos de la red como lo son las computadoras de los estudiantes. El nivel de seguridad actual se mide de manera numérica y tiene un soporte matemático.

Es importante recalcar que la última fase de la metodología no se implementará así como ciertos módulos de las otras fases debido a la confidencialidad de la información del centro educativo.

CAPÍTULO 1

1. ANÁLISIS DEL PROBLEMA

1.1. Antecedentes

Este centro cuenta con alumnos de diferentes nacionalidades, y su personal docente tiene certificados de enseñaza internacionales, además de una basta experiencia en la docencia en colegios internacionales alrededor del mundo. Debido a las características mencionadas anteriormente , InterAmerican Academy es una entidad de carácter internacional donde conviven diferentes ideologías basadas en el respeto y la comprensión de las mismas.

Con el objetivo de estar actualizados con los estándares de los colegios internacionales, los directivos han decidido implementar el sistema one to one laptop program que le permitirá al estudiante usar la portátil como principal útil escolar en las asignaturas , haciendo que el aprendizaje sea más entretenido y actual respecto a los cambios tecnológicos. Además esta decisión confirma el liderazgo educativo de IAA ya que es el primer centro docente en el país en impiementar este tipo de proyecto.

1.2. Planteamiento

IAA ha implementado el programa one to one laptop program el 2 de Agosto de 2011 correspondiente al año académico 2011-2012 ,el cual consiste en la utilización de portátiles como principal útil escolar por parte de los estudiantes de la escuela media y secundaria El número total de laptops que forman parte de la red actual de la institución son doscientas, las cuales tienen como sistemas operativos; Windows XP, Windows Vista, Windows 7 y Macintosh.

Este nuevo proyecto presenta un reto en cuanto a la administración y seguridad de la red y las computadoras para el departamento de sistemas ya que en años anteriores sólo se daba mantenimiento y soporte a las 50 máquinas ubicadas en los laboratorios de computación. A esto se suma, la falta de experiencia de los técnicos en el área de seguridad y resolución de problemas.

Dicho departamento ha identificado como su principal prioridad la seguridad de la red interna y externa. Por lo tanto surge la necesidad de contar con los mecanismos apropiados de seguridad en los dispositivos de red que permitan garantizar que el alumnado tenga acceso únicamente a la información plasmada en la guía para estudiantes del uso de laptops y otros dispositivos establecida por dicho departamento.

1.3. Justificación

La implementación del Manual de la Metodología Abierta de Testeo de Seguridad (MMATS) permitirá al personal del departamento de sistemas mejorar la configuración, esquematización y registros de los dispositivos basándose en las plantillas de resultados de dicha metodología. Además, servirá como marco de referencia para medir y mejorar el nivel de seguridad de otros dispositivos de la red . El departamento se alineará a los altos estándares que los departamentos de sistemas en los colegios internacionales tienen, al contar con una metodología que permita tener un buen nivel de organización y control, lo cual ayudará en el proceso de mejora continua para obtener buena calidad en el servicio.

El personal de sistemas aprenderá sobre el tema de seguridad desde la perspectiva teórica, el análisis y la selección de herramientas y la implementación de una metodología profesional. De esta manera se aminorará la curva de aprendizaje y el personal trabajará de una forma eficiente porque le podrá dedicar más tiempo a otras tareas.

La integridad de los alumnos estará protegida ya que al llevar a cabo esta metodología, el personal de sistemas podrá tomar las medidas preventivas o correctivas necesarias. Por otro lado el colegio contará con una buena reputación en seguridad informática internamente como

externamente. Internamente ayudará a que los alumnos o el personal analice el hecho de efectuar un ataque por el miedo de ser descubiertos debido a las medidas de seguridad . Externamente será complicado para agentes ajenos ingresar a la red interna , además de la buena reputación que el colegio tendrá frente a otros colegios en seguridad informática. Demostrando asi que la implementación del proyecto one to one laptop program funciona correctamente, convirtiéndolo en un valor agregado y no en un aspecto negativo a eliminar.

1.4. Objetivos

Objetivo general

Medir el nivel de seguridad del departamento de sistemas del InterAmerican Academy basándose en los valores de la evaluación del riesgo del MMATS.

Objetivos específicos

- Establecer una base comparativa en la medición del nivel de seguridad para poder contrastarla con futuras auditorías de seguridad.
- Realizar el reporte MMATS STAR.
- Crear un marco de referencia para la aplicación de metodologías de análisis de riesgos.
- Proporcionar soluciones a las vulnerabilidades encontradas.

1.5. Alcance de la solución

En base a previas conversaciones con el administrador de red y el encargado del proyecto, se ha identificado como principales activos de información a ser auditados: los servidores de correo, archivos y antivirus, así como el firewall. Así mismo el alcance de las pruebas de penetración abarcan el escaneo de puertos y análisis de vulnerabilidades de los activos antes mencionados. No se mostará la explotación de las vulnerabilidades que se puedan llegar a encontrar en el análisis de vulnerabilidades por petición del personal del departamento de sistemas. Esto está reflejado en el contrato (anexo A).

CAPÍTULO 2

2. ANÁLISIS DE METODOLOGÍAS Y HERRAMIENTAS

2.1 Metodologias de seguridad.

2.1.1 Manual de la Metodologia Abierta de Testeo de Seguridad

El Manual de la Metodología Abierta de Testeo de Seguridad (MMATS) es una metodología que se basa en el método científico para efectuar auditorías de seguridad. Su filosofía es que la seguridad es una ciencia y su objetivo es medir el nivel de seguridad de una compañía. Fue creada por Peter Herzog en el Instituto de Seguridad y Metodologías Libres ISECOM [1] por sus siglas en inglés y es de código abierto.

MMATS versión 3.0 cumple con la legislación de los gobiernos, las regulaciones de la industria, las políticas de negocios y los procesos. Esto se puede ver en su capítulo 12 [2] correspondiente a Compliance. Otro punto fundamental de esta metodología son las reglas del contrato [3] las cuales abarcan: Ventas y Marketing, Valoración/Estimación de entrega, Contados y Negociaciones, Alcance de la definición, Plan de Pruebas, Proceso de pruebas, Presentación de Informe.

A continuación se detallan los componentes de esta inventiva, los cuales organizan y esquematizan el proceso de auditoría en la primera fase:

- Alcance: Abarca procesos, protocolos, recursos, continuidad de recursos es decir, se refiere a lo que se va a auditar.
- El blanco: Abarca los activos de información y los controles. En otras palabras se refiere a lo que se sabe está en el entorno.
- Vector: Es la dirección de la interacción. La auditoría puede ser interna-externa, externa-interna, interna, externa, entre otras.
- Canales: Son los diferentes niveles que se dan en la interacción con un vector. Existen 5 canales: Humano [4], Físico [5], Inalámbrico [6], Telecomunicaciones [7] y Redes de Datos [8].
- Índice: Es la clasificación cuantitativa del blanco.

El creador y los colaboradores de la metodología definen 6 tipos de pruebas [9] las cuales son: a ciegas, doblemente a ciegas, caja gris, doble caja gris, tándem y cambio completo. Los objetivos de dichas pruebas tienen diferentes enfoques los cuales pueden ser: probar la experiencia del auditor (analista), medir el nivel de preparación y

seguridad del blanco o medir la experiencia del analista y el nivel de preparación y seguridad del blanco.

Los Valores de la Evaluación del Riesgo (VER) son una escalada de medición de la superficie de ataque 1 que se calcula por la cantidad de interacciones no controladas con el blanco. Estos se basan en la siguiente ecuación:

VER= Controles – Porosidad - Limitaciones

La porosidad [10] o seguridad operacional se enfoca en todos los puntos interactivos, operaciones, los cuales son categorizados como: Visibilidad, Acceso y Confianza. Los controles [11] proveen seguridad en las operaciones en cuanto al impacto o la reducción de la pérdida que pueda originar la amenaza. Existen 10 controles, los cuales se clasifican en: Clase A (Controles de interacción) y Clase B (Controles de proceso). Mientras que las limitaciones [12] son el estado actual de los límites percibidos y conocidos para canales, las operaciones y controles que se han verificado en la auditoría. Estas son: vulnerabilidad, debilidad, preocupación, exposición y anomalía. La siguiente figura ilustra con mayor detalle la organización de los VER.

[1] La falta específica de separaciones y controles funcionales que existen en un vector.

Categoría		Seguridad Operacional	Limitaciones
Operaciones		Visibilidad	Exposición
		Acceso	Vulnerabilidad
		Confianza	
Controles	Clase A - Interactiva	Autenticación	Debilidades
		Identificación	
		Resistencia	
		Subjugación	
		Continuidad	
	Clase B - Proceso	No repudio	Preocupaciones
		Confidencialidad	
		Privacidad	
		Integridad	
		Alarma	
			Anomalías

Ilustración 1. Clasificación de los VER. Elaborado por Francisco Bolaños.

El análisis de confianza [13] es una nueva característica que incorpora esta versión de la metodología. Este permite cuantificar las razones para confiar, así se puede priorizar los controles a mejorar ya que a menor confianza los controles deben ser mayores y a mayor confianza los controles pueden ser menores. La cuantificación se basa en 10 propiedades, estas son: tamaño, simetría, visibilidad, subyugación, consistencia, integridad, compensaciones, valor, componentes y porosidad. MMATS usa el análisis de confianza y no el análisis de riesgo ya que este es cuantificable y el análisis de riesgo es subjetivo.

El marco de trabajo se descompone en canales, módulos y tareas. Los canales son el enfoque global de la auditoría, mientras que los módulos son sub marcos de trabajo que se deben llevar a cabo para poder culminar la auditoría y las tareas son los aspectos que ha realizar en cada módulo, en otras palabras son las entradas del módulo.

Esta metodología se lleva a cabo en 4 fases [14] conocidas como el proceso de cuatro puntos. La primera se llama Inducción la cual establece los hechos acerca del entorno. La segunda es la Interacción que tiene que ver con la ejecución de las pruebas de penetración en la cual se interactúa y se tiene una respuesta del blanco. Investigación es la tercera fase la cual se basa y recompila la información que genera el entorno y/o el blanco conocida como emanación. Por último la intervención se enfoca en cambiar los recursos de la interacción por otros recursos conocidos por el analista y realizar la respectiva interacción. Cabe recalcar que cada fase tiene módulos que se usan a discreción del auditor. Por lo general la última fase no se aplica en la mayoría de auditorías de seguridad en especial cuando estas se dan por primera vez en una organización. La siguiente figura se puede observar en mayor detalle las 4 fases de la metodología.

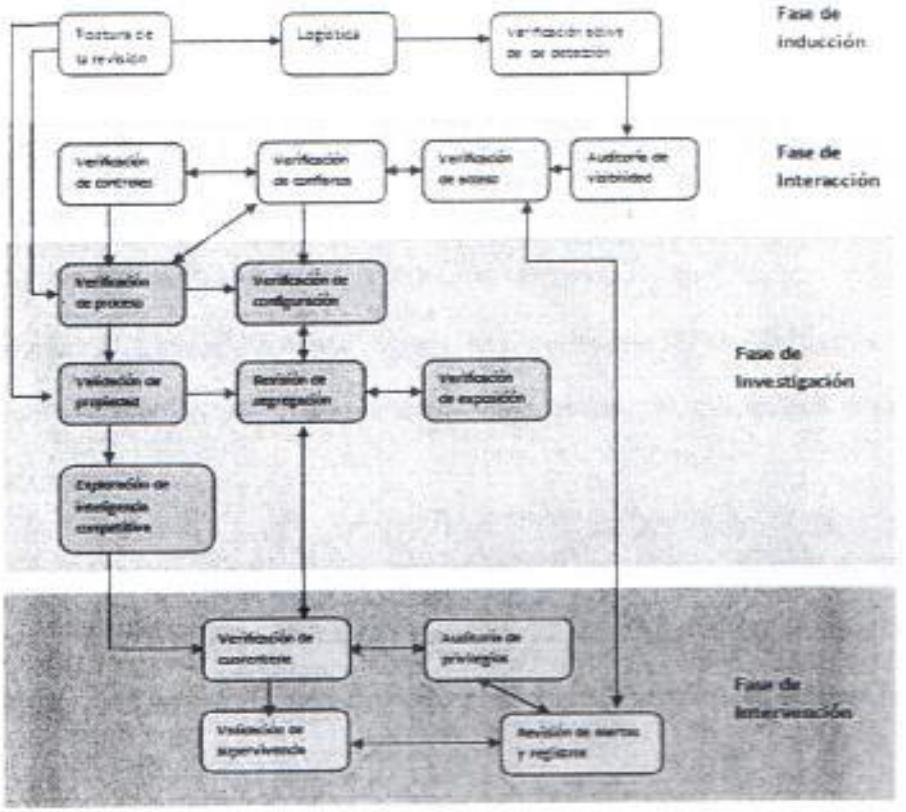

Ilustración 2. Fases de MMATS. Elaborado por Francisco Bolaños.

El informe final debe tener todos los requisitos plasmados en la plantilla reporte STAR [15]. Algo muy importante que se debe poner en este informe son todas las pruebas realizadas, incompletas, no efectuadas y anomalías presentadas. Para que en futuras auditorías la base comparativa tenga el mismo alcance y contexto.

2.1.2 Marco de Evaluación de Seguridad de Sistemas de Información

El Marco de Evaluación de Seguridad de Sistemas de Información (MESSI) es una metodología de código abierto, creada por la agrupación Open Information System Security Group (OISSG) [16] . MESSI está netamente estructurada al análisis de seguridad que abarca varios dominios. Dichos dominios tienen sus correspondientes procesos y pruebas que se deben seguir según la realidad de la empresa a ser auditada.

Esta metodología está organizada en base a los criterios de evaluación. Los criterios de evaluación son tomados de los expertos en el área de seguridad que contribuyeron a la creación de este marco de evaluación de seguridad. Estos son:

- Una descripción de los criterios de evaluación.
- Finalidades y objetivos.
- Los prerrequisitos para la realización de las evaluaciones.
- Los procesos para las evaluaciones.
- Presentación de resultados.
- Contramedidas recomendadas.

- Referencias a documentos externos

MESSI sigue 3 fases para la ejecución de la evaluación de seguridad las cuales son (17):

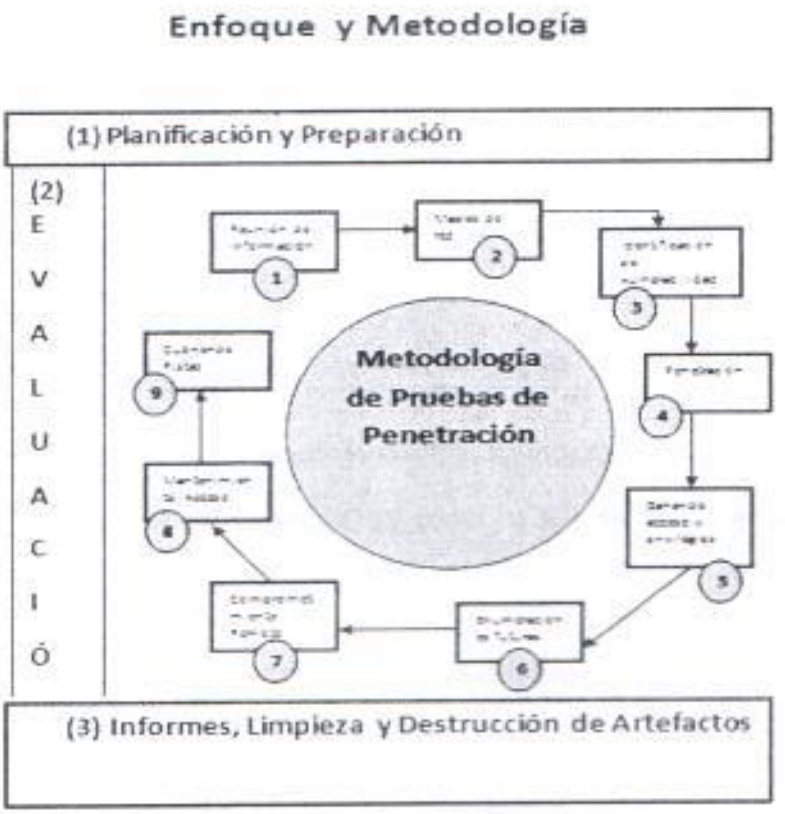

Ilustración 3. Metodología MESSI. Elaborado por Francisco Bolaños.

- Fase I – Planeación y Preparación: Se intercambia información, se planea y se preparan las pruebas. Las actividades que deben

generarse son: La identificación de contactos individuales de ambos lados, citas para confirmar el alcance, el enfoque y la metodología, un acuerdo especifico en el caso de pruebas de elevación de privilegios.

- Fase II – Evaluación: En esta fase se lleva a cabo las pruebas de penetración y se deben seguir el siguiente orden: reunir información, mapeo de la red, identificación de vulnerabilidades, penetración, ganar acceso y elevación de privilegios, futuras enumeraciones, usuarios remotos o sitios comprometidos, manteniendo el acceso y borrar los rastros.

- Fase III – Presentación de informe: Se muestran los resultados de evaluación de seguridad, así como lo que se realizó en el caso de la elevación de privilegios.

Este marco de evaluación de seguridad usa listas de evaluación asociadas a hardening de servicios. Las pruebas de penetración se basan en herramientas y en las buenas prácticas dadas por los expertos de seguridad.

2.1.3 Selección y Justificación de la metodología.

Con el fin de cumplir con los objetivos de esta tesis se decidió usar la metodología MMATS debido a que esta mide el nivel de seguridad (VER), usa el método científico el cual hace que la auditoría de seguridad sea repetida por diferentes autores y tipos de pruebas. Además los resultados de la misma sirven para efectuar un análsis de riesgo basándose en el análisis de confianza, el cual prioriza las vulnerabilidades encontradas. A continuación se muestra un cuadro comparativo entre la metodologías MMATS y MESSI.

CARACTERÍSTICAS	MMATS	MESSI
Centrada en herramientas de hackeo	No	Sí
Lista de revisión para auditorias	No	Sí
Asume conocimiento previo	No	No
Las actualizaciones son frecuentes	Sí	No
Revisión por grupo de expertos	Sí	Sí
Mide el nivel de seguridad	Sí	No
Basada en las buenas prácticas	No	Sí
Basada en algún método de ciencas exactas	Sí	No

Tabla I. Metodología MMATS y MESSI.

Del cuadro comparativo se puede observar el hecho de que MMATS no está sujeta a ninguna tecnología para su ejecución, lo cual la hace una metodología más abierta para que el auditor pueda efectuar la auditoría de seguridad usando las herramientas que él conoce, disminuyendo así la curva de aprendizaje. Por otro lado MMATS no usa listas de revisión ni plantillas de ejecución ya que estas impiden que la metodología pueda ser aplicada a todas las empresas indistintamente de su lógica de negocio. Por último MMATS no se basa en las buenas prácticas ya que estas son dadas por pioneros en seguridad que por lo general son grandes compañías, las cuales promueven sus intereses.

2.2 Herramientas de hackeo ético.

Las herramientas de hackeo ético que se presentarán en esta sección corresponderán únicamente a las definidas en el alcance de esta tesis las cuales abarcan: el escaneo de puertos y análisis de vulnerabilidades.

2.2.1 Marco de trabajo: Backtrack

Es una distribución de linux [18] que se basa en pruebas de penetración con el principal objetivo de que profesionales en la rama de seguridad informática puedan relizar hackeo ético. Esta distribución se ejecuta en

diferentes ambientes ya sea desde un cd, dvd, usb o como uno de los sistemas operativos de arranque del computador. Además posee un módulo de computación forense. Backtrack por ser una distribución linux es de código abierto y sus actualizaciones son inmediatas o se puede personalizar dependiendo de las necesitades del auditor.

2.2.2 Herramientas de escaneo.

Nmap

Es un escáner de puertos creado por Gordon Lyon [19] de código abierto y trabaja en Linux, Windows, Solaris y Mac OS. Está diseñado para escanear un equipo en particular hasta redes complejas. Nmap toma en consideración la latencia, fluctuaciones, congestión de la red, la interferencia de la víctima con el escaneo como parámetros para realizar análisis de puertos. Las principales características son: descubrimiento de equipos, escaneo de puertos, detección de sistemas operativos, servicios , bypass de firewall, entre otros.

SuperScan

Es un escáner de puertos creado por McAfee [20] de código abierto y trabaja en ambiente Windows. SuperScan esta diseñado para detectar puertos abiertos TCP y UDP en un equipo o en una red mediana y determina los servicios que están ejecuntándose en ellos. La última

versión incluye información de Windows tal como: NetBios, cuentas y grupos de usuarios y redes compartidas.

Unicornscan

Es un escáner de puertos creado por Robert E. Lee and Jack C. Louis [21] de código abierto y trabaja en ambiente Linux y Unix. Basicamente se concentra en TCP y en características especificas de UDP. Ciertos Detectores y Preventores de Intrusos pueden interpretar el escaneo de puerto de Unicornscan como un ataque de negación de servicio y lo que hacen es terminar con el análisis de puertos.

PortBunny

Es un escáner de puertos creado por Recurity Labs [22] de código abierto y trabaja en ambiente Linux. Específicamente analiza los puertos TCP y su análisis lo realiza en dos fases: La primera fase trata de encontrar paquetes a los cuales la victima responde y en la segunda fase los paquetes encontrados en la fase anterior son usados para encontrar la velocidad óptima a la cual la victima puede ser escaneada para no ser detectado.

2.2.3 Herramientas de análisis de vulnerabilidades:

Nessus

Es un escáner de vulnerabilidad de red creado por Renaud Deraison [23] de código abierto y trabaja en Linux, Windows, Solaris y Mac OS. Tiene una arquitectura modular la cual consiste servidores centralizados los cuales realizan el escaneo y clientes remotos que pueden interactuar (escanear) con la autorización del servidor. Las caracteristicas de Nesuss son:

- Compatibilidad con todo tipo de computadoras y servidores.
- Detección de huecos de seguridad en dispositivos locales y remotos.
- Detección de actualizaciones o parches faltantes.
- Simula ataques de negación de servicio.
- Auditorias de seguridad.
- Actualización constante de plugins con nuevas vulnerabilidades.
- Reportes personalizados.
- Capacidad para análisis determinístico.
- Análisis de métodos probabilísticos.

Nexpose

Es un escáner de vulnerabilidad de red creado por Reapid7 [24] de código propietario, pero es gratuito para pruebas individuales o comapñías medianas. Trabaja en ambiente Linux y Windows. Nexpose cuenta con las siguientes caracteristicas.

- Capacidad 32 direcciones IP.
- Escaneo personalizado y configuración de reporte y alerta de correo electrónico.
- Escaneo web.
- Herramientas de exploits y de malware.
- Reportes que cumple con las regulaciones del mercado.

Retina

Es un escáner de vulnerabilidad de red creado por ATM Software International [25] de código propietario , trabaja en ambiente Windows. Esta son las principales caracteristicas de Retina:

- Utiliza una motor de búsqueda de inteligencia artificial personalizado (patentado) que simula las tendencias del hacker.

- Se basa en los métodos comunes de ataques del hacker. Estos métodos se actualizan dependiendo de las nuevas vulnerabilidades encontradas por los desarrolladores.
- Posee una base de datos que está ligada nmap.
- Escaneo inteligente.
- Arquitectura abierta ya que permite al administrador crear nuevas vulnerabilidades y reportes.
- Reportes personalizados hay dos tipos de reportes los técnicos y los ejecutivos.

Saint

Es un escaner de vulnerabilidad de red creado por SAINTrl [26] de código propietario , trabaja en ambiente Linux. Esta son las principales características de Saint:

- Escaneo de la red y detección de nuevos dispositivos con sus respectivas vulnerabilidades.
- Actualización de vulnerabilidades es automática.
- Reportes personalizados y administrables.
- Posee un módulo de exploits.

- Prioriza los recursos que deben ser analizados en la red.
- Usa estándares como referencia tales como: PCI, OVAL, CVE, CVSS, BID, IAVA.

2.2.4 Selección y justificación de las herramientas de hackeo ético.

Debido a que no se cuenta con recursos económicos para la ejecución de esta tesis uno de los principales aspectos a ser tomados en cuenta es que las herramientas sean gratuitas. Por lo tanto, como marco de trabajo se usará Backtrack 5 ya que es una plataforma especializada en hackeo ético.

El escáner de puertos seleccionado es Nmap ya ofrece funcionalidades adicionales que los otros escáners en el mercado no ofrecen, tales como: consideración de la latencia, fluctuaciones, congestión de la red, la interferencia de la victima con el escaneo como parámetros para realizar análisis de puertos. Esto es conveniente ya que si se usa otro escaner habria que complementarlo con otros para que el ecaneo de puertos sea preciso y exitoso ya que no son multitarea. Es importante mencionar que Nmap analiza en detalle los puertos TCP y UDP y no así los otros escaners ya que estos se especializan más en uno de ellos que por lo general es TCP.

La herramienta de análisis de vulnerabilidades elegida es Nessus debido a que tiene el mayor número de actualizaciones(plugins) de vulnerabilidades en el mercado. Los resultados que muestra tienen un alto nivel de confiablidad. Cuenta con una excelente interfaz gráfica la cual hace que su uso sea intuitivo. El módulo de exploit efectúa negaciones de servicio efectivos y el análisis de vulnerabilidades puede ser local o remoto abarcando redes complejas.

Cabe recalcar que tanto Nmap como Nessus vienen con Bactrack 5 lo único que hay que hacer es actualizar sus versiones. Además el auditor de la tesis cuenta con conocimientos previos y experiencia con Backtrack y los programas antes mencionados. Esto hace que la curva de aprendizaje sea menor y se optimice el tiempo en la elaboración de esta tesis.

CAPÍTULO 3

3. IMPLEMENTACIÓN DE LA METODOLOGÍA

3.1 Generalidades de la metodología.

Definición de la prueba de seguridad:

- Alcance: puertos abiertos, filtrados y cerrados. Servicios correspondientes a cada blanco, certificados de seguridad, autenticación del servidor de archivos y chequeo de cuentas por defecto.
- El blanco: Firewall, servidores de: correo, biblioteca, voz sobre IP, DHCP, cámaras de seguridad (DVR), contabilidad, administrativo, discos duros.
- Vector: Externa-Interna (Externa al firewall e interna a los otros servidores)
- Canal: Redes de Datos.
- Índice: 11 (son 2 discos duros y 2 DVRs)

El tipo de prueba que se usará es la de caja gris (gray box) debido a que esta prueba evita la etapa de reconocimeinto ya que el administrador de red proveerá información sobre el canal. De esta manera el analista de

seguridad se concentrá en la medición del nivel de seguridad del departamento de sistemas optimizando tiempo y recursos.

Reglas del contrato.

- Ventas y marketing: Las establecidas en este manual [3] .
- Evaluación y entrega estimada: Las establecidas en este manual [3] .
- Contratos y negociaciones: Se encuentran en el Anexo A.
- Definición de alcance: El establecido en la definición de la prueba de seguridad.
- Plan de prueba: Se encuentra en el Anexo B.
- Proceso de prueba: Los establecidos en este manual [3] .
- Presentación de informes: Los establecidos en este manual [3]

Es importante tener en cuenta que por motivos de confidencialidad la parte correspondiente al reconocimiento del canal (Inducción) no se mostrará en este trabajo. Además esta parte fue proporcionada por el administrador de red por lo cual se asume que la información dada es 100% confiable.

Existirán algunos módulos de las fases que no se pueden aplicar ya que no cubren el alcance de la definición de la prueba de seguridad o relvelan información confidencial sobre la empresa. Asimismo no se llevará a cabo la fase de intervención ya que la metodología recomienda que cuando se la aplica por primera vez esta fase no se debe tomar en cuenta. Las pruebas de la ejecución de las herramientas seleccionadas se encuentran en el Anexo C y Anexo D.

3.2 Fase de Inducción.

3.2.1 Postura de la revisión

Política: No aplica.

Legislación y regulaciones: Este trabajo se basa en la Constitución del Ecuador [27] así como la ley de comercio electrónico [28].

Cultura: No aplica.

Edad: No aplica.

Artefactos frágiles: No aplica.

3.2.2 Logística

Marco de trabajo: No aplica.

Calidad de la red: No aplica.

Tiempo: No aplica.

3.2.3Verificación Activa de Detección

Filtrado: No aplica.

Detección activa: No aplica.

3.3 Fase de Interacción.

3.3.1Visibilidad de la interacción.

Topología de la red: No aplica.

Enumeración: No aplica.

Identificación:

FIREWALL

Controles de puertos

Puerto	Protocolo	Estado	Resultado
80	TCP	Abierto	http (Zimbra http config)
110	TCP	Abierto	pop3 (Zimbra pop3d)
113	TCP	Cerrado	Auth
143	TCP	Abierto	Imap (Zimbra imapd)
443	TCP	Cerrado	https
1723	TCP	Abierto	pptp?
5800	TCP	Abierto	vnc-http?
5900	TCP	Abierto	vnc: VNC (protocol 3.7)
9090	TCP	Abierto	ssl/http thttpd
Tiempo: 563.60 segundos.			

Tabla II. Tabla II. Firewall-Controles de puertos

TCP SYN

IP	Resultado
----------	Se encontraron 12 puertos TCP, tres de los cuales no se encuentran en los **Controles de puertos**. Estos son: 5907/Abierto - vnc : VNC (protocol 3.8) 7025/Abierto - vmsvc-2? 60443/Abierto - ssl/http: thttpd
Tiempo: 485.39 segundos.	

Tabla III. Firewall-TCP SYN

NULL

IP	Resultado
----------	Se encontraron 9 puertos TCP, tres de los cuales no se encuentran en los **Controles de puertos**. Estos son: 60443/Abierto – Servicio desconocido. 5907/ Abierto – vnc: VNC (protocol 3.8) 7025/Abierto - vmsvc-2?
Tiempo: 525.25segundos.	

Tabla IV. Firewall-NULL

FIN

IP	Resultado
----------	Se encontraron 4 puertos TCP, dos de los cuales no se encuentran en los **Controles de puertos**. Estos son: 5907/Abierto - vnc: VNC (protocol 3.8) 60443/Abierto - ssl/http: thttpd
Tiempo: 542.78 segundos.	

Tabla V. Firewall-FIN

XMAS

IP	Resultado
----------	Se encontraron 4 puertos TCP, dos de los cuales no se encuentran en los **Controles de puertos**. Estos son: 7025/Abierto - vmsvc-2? 60443/Abierto - ssl/http: thttpd
Tiempo: 527.02segundos.	

Tabla VI. Firewall-XMAS

UDP

IP	Resultado
----------	No se mostró puerto alguno.
Tiempo: 4111.25 segundos.	

Tabla VII. Firewall-UDP

SERVIDOR DE CORREO

Puerto	Protocolo	Estado	Servicio	Detalle del servicio
25	TCP	Abierto	smtp	Postfix smtpd
53	TCP	Abierto	domain	ISC BIND 9.7.0-P1
80	TCP	Abierto	http	Zimbra http config
110	TCP	Abierto	pop3	Zimbra pop3d
143	TCP	Abierto	imap	Zimbra imapd
389	TCP	Abierto	ldap	OpenLDAP 2.2.X - 2.3.X
443	TCP	Abierto	ssl/http	Thttpd
465	TCP	Abierto	ssl/smtp	Postfix smtpd
587	TCP	Abierto	smtp	Postfix smtpd
993	TCP	Abierto	ssl/imap	Zimbra imapd
995	TCP	Abierto	ssl/pop3	Zimbra pop3d
1723	TCP	Abierto	pptp	MoretonBay (Firmware: 1)
5222	TCP	Abierto	jabber	Zimbra 6 jabberd
5269	TCP	Abierto	jabber	Zimbra 6 jabberd
7025	TCP	Abierto	vmsvc-2?	----------
7777	TCP	Abierto	socks5	(No authentication; connection failed)
9090	TCP	Abierto	http	Thttpd
10000	TCP	Abierto	http	MiniServ 1.580 (Webmin httpd)
60443	TCP	Abierto	ssl/http	thttpd
53	UDP	Abierto	domain ISC	BIND 9.7.0-P1
10000	UDP	Abierto	webmin	(https on TCP port 10000)
Sistema Operativo: Linux 2.4.18 - 2.4.35 (Cisco-Linksys)				

Tabla VIII. Servidor de Correo

SERVIDOR DE BIBLIOTECA

Puerto	Protocolo	Estado	Servicio	Detalle del servicio
81	TCP	Abierto	http	Apache Tomcat/Coyote JSP engine 1.1
5800	TCP	Abierto	Vnc-http	----------
5900	TCP	Abierto	Vnc	----------
5907	TCP	Abierto	Vnc	VNC (protocol 3.6)
Sistema Operativo: Microsoft Windows XP SP3 (VMware)				

Tabla IX. Servidor de biblioteca.

SERVIDOR DE CONTABILIDAD

Puerto	Protocolo	Estado	Servicio	Detalle del servicio
22	TCP	Abierto	Ssh	OpenSSH 5.3p1 Debian 3ubuntu4 (protocol 2.0)
80	TCP	Abierto	http	lighttpd 1.4.26
139	TCP	Abierto	netbios-ssn	Samba smbd 3.X (workgroup: ACIG
443	TCP	Abierto	ssl/http	lighttpd 1.4.26
445	TCP	Abierto	netbios-ssn	Samba smbd 3.X (workgroup: ACIG
123	UDP	Abierto	ntp	NTP v4
137	UDP	Abierto/ Filtrado	netbios-dgm	----------
138	UDP	Abierto	webmin	(https on TCP port 20004)
Sistema Operativo: Linux (VMware)				

Tabla X. Servidor de contabilidad

SERVIDOR DHCP

Puerto	Protocolo	Estado	Servicio	Detalle del servicio
22	TCP	Abierto	Ssh	OpenSSH 4.7p1 Debian 8ubuntu3 (protocol 2.0)
80	TCP	Abierto	http	Apache httpd 2.2.8
443	TCP	Abierto	ssl/http	Apache httpd 2.2.8
67	UDP	Abierto/ Filtrado	Dhcps	----------
120	UDP	Abierto/ Filtrado	cfdptkt	----------
123	UDP	Abierto	ntp	NTP v4 (unsynchronized)
514	UDP	Abierto/ Filtrado	Syslog	----------
1027	UDP	Abierto/ Filtrado	Desconocido	----------
2160	UDP	Abierto/ Filtrado	apc-2160	----------
17205	UDP	Abierto/ Filtrado	Desconocido	----------
18373	UDP	Abierto/ Filtrado	Desconocido	----------
18987	UDP	Abierto/ Filtrado	Desconocido	----------
19120	UDP	Abierto/ Filtrado	Desconocido	----------
19933	UDP	Abierto/ Filtrado	Desconocido	----------
21698	UDP	Abierto/ Filtrado	Desconocido	----------
21702	UDP	Abierto/ Filtrado	Desconocido	----------
22914	UDP	Abierto/ Filtrado	Desconocido	----------
39888	UDP	Abierto/ Filtrado	Desconocido	----------
Sistema Operativo: Linux (VMware)				

Tabla XI. Servidor DHCP

SERVIDOR DVR 1

Puerto	Protocolo	Estado	Servicio	Detalle del servicio
80	TCP	Abierto	http	----------
554	TCP	Abierto	Rtsp	----------
Sistema Operativo: Linux 2.6.12 - 2.6.14 (VMware)				

Tabla XII. Servidor DVR1

SERVIDOR DVR 2

Puerto	Protocolo	Estado	Servicio	Detalle del servicio
80	TCP	Abierto	http	----------
554	TCP	Abierto	Rtsp	----------
Sistema Operativo: Linux 2.6.12 - 2.6.14 (VMware)				

Tabla XIII. Servidor DVR2

SERVIDOR VOZ SOBRE IP

Puerto	Protocolo	Estado	Servicio	Detalle del servicio
22	TCP	Abierto	Ssh	OpenSSH 4.3 (protocol 2.0)
25	TCP	Abierto	Smtp	Postfix smtpd
80	TCP	Abierto	http	Apache httpd 2.2.3 ((CentOS))
110	TCP	Abierto	pop3	Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-12.el5 7.2
111	TCP	Abierto	Rpcbind	----------
143	TCP	Abierto	Imap	Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-12.el5 7.2
443	TCP	Abierto	ssl/http	Apache httpd 2.2.3 ((CentOS))
993	TCP	Abierto	ssl/imap	Cyrus imapd
995	TCP	Abierto	pop3	Cyrus pop3d
3304	TCP	Abierto	Mysql	MySQL (unauthorized)
4445	TCP	Abierto	upnotifyp?	----------
9090	TCP	Abierto	zeus-admin?	----------
Sistema Operativo: Linux 2.6.9 - 2.6.30				

Tabla XIV. Servidor voz sobre IP.

HARD DRIVE 1

Puerto	Protocolo	Estado	Servicio	Detalle del servicio
21	TCP	Abierto	ftp	ProFTPD 1.3.1
80	TCP	Abierto	http	Apache httpd 1.3.41 ((Unix) mod_auth_pam/1.1.1 DAV/1.0.3 mod_ssl/2.8.31 OpenSSL/0.9.8g)
139	TCP	Abierto	netbios-ssn	Samba smbd 3.X (workgroup: ACIG)
443	TCP	Abierto	ssl/http	Apache httpd 1.3.41 ((Unix) mod_auth_pam/1.1.1 DAV/1.0.3 mod_ssl/2.8.31 OpenSSL/0.9.8g)
445	TCP	Abierto	netbios-ssn	Samba smbd 3.X (workgroup: ACIG)
631	TCP	Abierto	ipp	CUPS 1.2
873	TCP	Abierto	Rsync	(protocol version 30)
3260	TCP	Abierto	iscsi?	----------
3289	TCP	Abierto	Daap	mt-daapd DAAP 0.3.1
9000	TCP	Abierto	upnp	TwonkyMedia UPnP (Linux 2.x.x; UPnP 1.0; pvConnect SDK 1.0)
49152	TCP	Abierto	Upnp	Portable SDK for UPnP devices 1.6.9 (kernel 2.6.31.8; UPnP 1.0)
68	UDP	Abierto/ Filtrado	Dhcpc	----------
137	UDP	Abierto	netbios-ns	Microsoft Windows XP netbios-ssn
138	UDP	Abierto/ Filtrado	netbios-dgm	
631	UDP	Abierto/ Filtrado	ipp	
1900	UDP	Abierto/ Filtrado	Upnp	
5353	UDP	Abierto	mdns	DNS-based service discovery
Sistema Operativo: Linux 2.6.19 - 2.6.35 (Iomega)				

Tabla XV. Hard drive 1.

HARD DRIVE 2

Puerto	Protocolo	Estado	Servicio	Detalle del servicio
21	TCP	Abierto	ftp	ProFTPD 1.3.1
80	TCP	Abierto	http	Apache httpd 1.3.41 ((Unix) mod_auth_pam/1.1.1 DAV/1.0.3 mod_ssl/2.8.31 OpenSSL/0.9.8g)
111	TCP	Abierto	Rpcbind	----------
139	TCP	Abierto	netbios-ssn	Samba smbd 3.X (workgroup: ACIG)
443	TCP	Abierto	ssl/http	Apache httpd 1.3.41 ((Unix) mod_auth_pam/1.1.1 DAV/1.0.3 mod_ssl/2.8.31 OpenSSL/0.9.8g)
445	TCP	Abierto	netbios-ssn	Samba smbd 3.X (workgroup: ACIG)
631	TCP	Abierto	Ipp	CUPS 1.2
873	TCP	Abierto	Rsync	(protocol version 30)
2049	TCP	Abierto	Rpcbind	---------- ----
3260	TCP	Abierto	iscsi?	---------- ----
49152	TCP	Abierto	Upnp	Portable SDK for UPnP devices 1.6.9 (kernel 2.6.31.8; UPnP 1.0)
68	UDP	Abierto/ Filtrado	Dhcpc	---------- ----
111	UDP	Abierto	Rpcbind	---------- ----
137	UDP	Abierto	netbios-ns	Microsoft Windows XP netbios-ssn
138	UDP	Abierto/ Filtrado	netbios-dgm	---------- ----
631	UDP	Abierto/ Filtrado	Ipp	---------- ----
1900	UDP	Abierto/ Filtrado	Upnp	---------- ----
2049	UDP	Abierto	rpcbind	2 (rpc #100000)
5353	UDP	Abierto	mdns	DNS-based service discovery
Sistema Operativo: Linux 2.6.19 - 2.6.35 (Iomega)				

Tabla XVI. Tabla XVI. Hard drive 2.

ADMINISTRATIVO

Puerto	Protocolo	Estado	Servicio	Detalle del servicio
5800	TCP	Abierto	vnc-http?	----------
5900	TCP	Abierto	Vnc	VNC (protocol 3.7)
Sistema Operativo: No reconocido				

Tabla XVII. Administrativo.

3.3.2Verificación de acceso.

Red: Los mostrados en el módulo Identificación.

Servicios:

FIREWALL: Web (http,https) , Correo(pop3, imap, zimbra), VCN , No es susceptible a fragmentación de paquetes.

CORREO: Archivo(smtp, OpenLDAP), Web (http,https), Correo(pop3, imap, zimbra), DNS software, MoretonBay (Firmware: 1), MiniServ 1.580

BLIOTECA: Web (Apache Tomcat) , VCN .

CONTABILIDAD: Web (http, https, administrador), ssh (OpenSSH 5.3p1 Debian 3ubuntu4) , NTP.

DHCP: Web (http, https, Apache httpd 2.2.8), ssh (OpenSSH 4.7p1 Debian 8ubuntu3) , NTP, archivos(cfdptkt, apc-2160), dhcps, syslog

DVR1: Web (http), Streamming (stsp)

DVR2: Web (http), Streamming (stsp)

VOZ SOBRE IP: Web (Apache httpd 2.2.3, rpcbind), ssh(OpenSSH 4.3), Archivos(Postfix smtpd, upnotifyp), correo(pop3,imap), Mysql,Zeus.

HARD DRIVE 1: Web (Apache httpd 1.3.41, rpcbind), ssh(OpenSSH 4.3), Archivos(ProFTPD 1.3.1, Samba smbd 3.X, iscsi, netbios), Impresión(CUPS 1.2), Streamming (Daap), Network(upnp), Dhcpc, DNS-based service discovery

HARD DRIVE 2: Web (Apache httpd 1.3.41, rpcbind), ssh(OpenSSH 4.3), Archivos(ProFTPD 1.3.1, Rsync ,Samba smbd 3.X, iscsi, netbios), Impresión(CUPS 1.2), Network(upnp), Dhcpc

ADMINISTRATIVO: VNC.

Autenticación:

Correo: Requiere usuario y contraseña. Después de 5 intentos el servidor de correo se bloquea para ese usuario determinado.

Bilioteca: Requiere usuario y contraseña. Después de 5 intentos el servidor de correo se bloquea para ese usuario determinado.

3.3.3 Verificación de confianza.

Spoofing:

Correo: Exposición en la zona de transferencia del servidor DNS (AXFR). Exposición de la caché en el servidor DNS.

Contabilidad: Desbordamiento remoto del requerimiento de la cabecera lighttpd mod_fastcgi HTTP

DHCP: Apache 2.2 < 2.2.13 APR Desbordamiento de la pila en el módulo apr_palloc (Son 10 fallas de este tipo)

Phishing: No aplica.

Abuso de los recursos: No aplica

3.3.4 Verificación de controles.

No repudio:

Correo: Certificado digital.

Voz sobre IP: Certificado digital.

DHCP: Certificado digital.

Contabilidad: Certificado digital.

Confidencialidad

Correo: Certificado digital.

SSLv2
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
SSLv3
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
TLSv1
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
SSLv2
DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5
SSLv3
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1
TLSv1
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1

SSLv3
ADH-DES-CBC3-SHA Kx=DH Au=None Enc=3DES(168) Mac=SHA1
ADH-RC4-MD5 Kx=DH Au=None Enc=RC4(128) Mac=MD5
TLSv1
ADH-DES-CBC3-SHA Kx=DH Au=None Enc=3DES(168) Mac=SHA1
ADH-AES128-SHA Kx=DH Au=None Enc=AES(128) Mac=SHA1
ADH-AES256-SHA Kx=DH Au=None Enc=AES(256) Mac=SHA1
ADH-CAMELLIA128-SHA Kx=DH Au=None Enc=Camellia(128) Mac=SHA1
ADH-CAMELLIA256-SHA Kx=DH Au=None Enc=Camellia(256) Mac=SHA1
ADH-RC4-MD5 Kx=DH Au=None Enc=RC4(128) Mac=MD5
ADH-SEED-SHA Kx=DH Au=None Enc=SEED(128bh) Mac=SHA1

Voz sobre IP: Certificado digital.

SSLv3
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56) Mac=SHA1
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1
TLSv1
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56) Mac=SHA1
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1

DHCP: Certificado digital.

SSLv2
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
SSLv3
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
TLSv1
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
SSLv2
DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5
SSLv3
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1
TLSv1
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1

Contabilidad: Certificado digital.

DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1 TLSv1
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1

Privacidad: No aplica

Integridad: Los mismos controles de confidencialidad.

3.4 Fase de investigación.

3.4.1 Verificación de procesos.

Mantenimiento: No aplica

Desinformación: No aplica

Indemnificación: Los siguientes dispositivos cuentan con garantías ténicas y no técnicas: firewall y el servidor de voz sobre IP.

3.4.2 Verificación de configuración.

Controles de configuración: No aplica

Errores comunes de configuración:

Contabilidad: La firma está deshabilitada en SMB.

Hard drive1: Cuenta FTP por defecto XAMPP, compartimiento de Acceso no privilegiado en Microsoft Windows SMB, FTP Anónimo está habilitado, acceso a la cuenta invitado del usuario local Microsoft Windows SMB, la firma está deshabilitada en SMB.

Hard drive2: Cuenta FTP por defecto XAMPP, compartimiento de Acceso no privilegiado en Microsoft Windows SMB, FTP Anónimo está habilitado, acceso a la cuenta invitado del usuario local Microsoft Windows SMB, usuario compartido montable NFS , compartimiento NFS de lectura, la firma está deshabilitada en SMB.

Mapeo de limitaciones:

CORREO: Puertos abiertos TCP: 7025,7777.

DHCP: Puertos abiertos UDP: 120

VOZ SOBRE IP: Puertos abiertos TCP: 3304(SQL no autorizado), 4445.

HARD DRIVE 1: Puertos abiertos TCP: 3260.

HARD DRIVE 2: Puertos abiertos TCP: 3260.

3.4.3 Validación de propiedad.

Compartir: No aplica

Mercado negro: No aplica

Canales de venta: No aplica

Mapeo de contención de privacidad: No aplica

Revelación: No aplica

Limitaciones: No aplica

3.4.4 Exposición de verificación.

Enumeración de la exposición:

CORREO: Detección del protocolo SSL Versión 2 (v2), certificado SSL auto firmado, conjunto de Cifrado SSL Medio, conjunto de Cifrado SSL Anónimo, el certificado SSL no es confiable, conjunto de Cifrado SSL Débil.

CONTABILIDAD: certificado SSL auto firmado, conjunto de Cifrado SSL Medio, el certificado SSL no es confiable.

BIBLIOTECA : Detección del archivo en Política Web Site Cross-Domain, divulgación de Información en Web Server robots.txt.

DHCP : Los métodos HTTP TRACE / TRACK están permitidos, conjunto de Cifrado SSL Débil, detección del protocolo SSL Versión 2 (v2), certificado SSL auto firmado, conjunto de Cifrado SSL Medio, el certificado SSL no es confiable.

DVR1: XSS genérico en Servidor web.

3.4.5 Revisión de segregación.

DVR2: XSS genérico en Servidor web.

VOZ SOBRE IP: Los métodos HTTP TRACE / TRACK están permitidos, revelación de las cookies en Apache HTTP Server, certificado SSL auto firmado, conjunto de Cifrado SSL Medio, el certificado SSL no es confiable.

HARD DRIVE 1: Detección obsoleta de servidor web, los métodos HTTP TRACE / TRACK están permitidos, revelación de las cookies en Apache HTTP Server, Detección de mDNS, certificado SSL auto firmado, el certificado SSL no es confiable.

HARD DRIVE 2: Detección obsoleta de servidor web, los métodos HTTP TRACE / TRACK están permitidos, revelación de las cookies en Apache HTTP Server, Detección de mDNS, certificado SSL auto firmado, el certificado SSL no es confiable.

ADMINISTRATIVO: Detección de mDNS.

3.4.6 Exploración de inteligencia competitiva.

Red de negocios: No aplica.

Perfil: No aplica.

Ambiente de negocio: No aplica.

Ambiente organizacional: No aplica.

3.4.7 Fase de intervención.

Todos los módulo en esta fase no aplican.

CAPÍTULO 4

4. RESULTADOS OBTENIDOS

4.1 Cálculo de los Valores de Evaluación del Riesgo.

Visibilidad: Es de 11 ya que los blancos son los siguientes: Firewall, servidores de correo, bilioteca, voz sobre IP , DHCP, DVR1,DVR2, contabilidad, administrativo, hard drive1, hard drive 2.

Acceso:

Blanco	Respuesta de puertos o servicios
Firewall	12
Correo	21
Bilioteca	4
Contabilidad	8
DHCP	18
DVR1	2
DVR2	2
Voz sobre IP	12
Hard drive 1	17
Hard drive 2	19
Administrativo	2
Total	**117**

Tabla XVIII. VER - Acceso

Confianza:

Blanco	Respuesta de puertos o servicios
Firewall	10
Correo	21
Biblioteca	4
Contabilidad	7
DHCP	4
DVR1	2
DVR2	2
Voz sobre IP	12
Hard drive 1	13
Hard drive 2	15
Administrativo	2
Total	**92**

Tabla XIX. VER - Confianza

Controles :

	Control Interactivo – Clase A					Control Proceso– Clase B				
Blanco	**Autenticación**	**Indemnización**	**Resistencia**	**Subyugación**	**Continuidad**	**No repudio**	**Confidencialidad**	**Privacidad**	**Integridad**	**Alarmas**
Firewall	0	0	0	0	0	1	0	0	0	0
Correo	1	0	1	1	0	1	1	0	1	0
Biblioteca	1	0	1	1	0	1	1	0	1	0
Contabilidad	1	0	1	1	0	1	1	0	1	0
DHCP	1	0	0	1	0	1	1	0	1	0
DNS1	0	0	0	0	0	0	0	0	0	0
DNS2	0	0	0	0	0	0	0	0	0	0
VoIP	1	0	0	1	0	1	1	0	1	0
Hard drive1	1	0	0	1	0	1	1	0	1	0
Har drive 2	1	0	0	1	0	1	1	0	1	0
Administrativo	0	0	0	0	0	0	0	0	0	0
Sub total	**7**	**2**	**3**	**7**	**0**	**8**	**7**	**0**	**7**	**0**
Total	**19**					**22**				

Tabla XX. VER - Controles

Limitaciones :

Blanco	Vulnerabilidad	Debilidad	Preocupación	Exposición	Anomalía
Firewall	0	0	0	0	0
Correo	2	0	6	2	0
Biblioteca	0	0	0	2	0
Contabilidad	1	1	3	0	0
DHCP	10	0	5	2	0
DVR1	0	0	0	1	0
DVR2	0	0	0	1	0
VoIP	0	0	3	4	0
Hard drive1	0	5	2	4	0
Har drive 2	0	7	2	4	0
Administrativo	0	0		1	0
Sub total	**13**	**13**	**21**	**21**	**0**
Total	**68**				

Tabla XXI. VER - Limitaciones

4.2 Seguridad actual

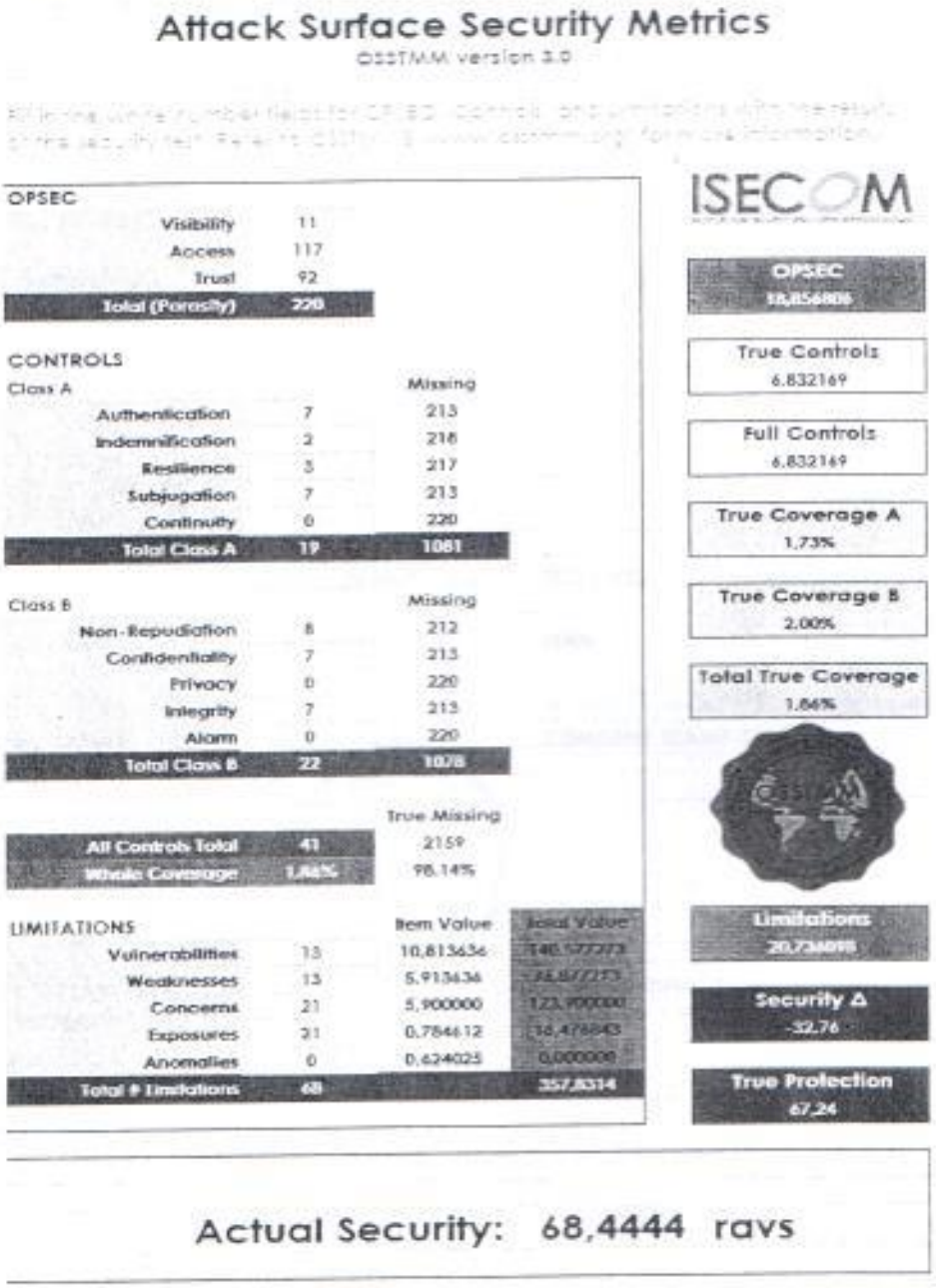

Ilustración 4. Seguridad actual

4.3 Reporte MMATS STAR

OSSTMM Security Test Audit Report

ISECOM

REPORT ID	1	DATE	Julio 30th, 2012
LEAD AUDITOR	Ing. Francisco Bolaños	TEST DATE DURATION	1 month
SCOPE AND INDEX	Puertos abiertos, filtrados y cerrados. Servicios correspondientes a cada blanco, certificados de seguridad, autenticación del servidor de archivos y	VECTORS	Externa-Interna
		TEST TYPES	Caja gris
CHANNELS	Red de datos	TERM	1

SIGNATURE

COMPANY STAMP/SEAL

Open Source Security Testing Methodology Manual — Certified OSSTMM 3.0 Compliant — www.isecom.org

OPST CERTIFICATION NUMBERS	N/A	OPSA CERTIFICATION NUMBERS	N/A

Ilustración 5. Reporte MMAT STAR- Parte 1.

OPERATIONAL SECURITY VALUES	
VISIBILITY	11
ACCESS	117
TRUST	92
POROSITY	220

LIMITATIONS VALUES	VERIFIED
Vulnerability	13
Weakness	13
Concern	21
Exposure	21
Anomaly	0

RAV OPSEC	18,85680618
RAV CONTROLS	6,83216907
RAV LIMITATIONS	17,92642236

CONTROLS VALUES	
AUTHENTICATION	7
INDEMNIFICATION	2
SUBJUGATION	7
CONTINUITY	0
RESILIENCE	3
NON-REPUDIATION	8
CONFIDENTIALITY	7
PRIVACY	0
INTEGRITY	7
ALARM	0

WHOLE COVERAGE	1,96%
TRUE COVERAGE	1,96%

The RAV Score is the Actual Security Value calculated on Operational Security Metrics and Controls

RAV SCORE [redacted]

OVERVIEW
This Open Source Security Testing Methodology Manual provides a methodology for a thorough

RELATED TERMS AND DEFINITIONS
This report may refer to words and terms that may be construed with other intents or meanings.

PURPOSE
The primary purpose of this Audit Report is to provide a standard reporting scheme based on a

PROCESS
This Audit Report must accompany the full security test report document which provides

For this OSSTMM Audit Report to be valid, it must be filled out clearly, properly, and completely.

CERTIFICATION
OSSTMM certification is the assurance of an organization's security according to the thorough

ABOUT ISECOM
ISECOM is an independent, non-profit security research organization and certification authority

Ilustración 6. Reporte MMAT STAR- Parte 2.

1. POSTURE REVIEW

TASK	COMMENTS	COMPLETION STATUS
Identified business objectives and markets.	Dado por el administrador de red.	Hecho
Identified legislation and regulations applicable to	Ninguno	Hecho
Identified business policies.	Dado por el administrador de red.	Hecho
Identified business and industry ethics policies.	Dado por el administrador de red.	Hecho
Identified operation cultures and norms.	Información confidencial	N/A
Identified operation times and flow applicable to the	Información confidencial	N/A
Identified all necessary Channes for this scope.	Información confidencial	N/A
Identified all Vectors for this scope.	Ninguno	Hecho

2. LOGISTICS

TASK	COMMENTS	COMPLETION STATUS
Applied testing safety measures	Información confidencial	N/A
Determined and accounted for test reliabilities.	Información confidencial	N/A
Determined and accounted for downtime in scope.	Información confidencial	N/A
Determined and accounted for test pace according	Información confidencial	N/A

3. ACTIVE DETECTION VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Determined and accounted for interferences.	N/A	N/A
Tested with both interferences active and inactive.	Ninguno	Hecho
Determined restrictions imposed on tests.	Ninguno	Hecho
Verified detection rules and predictability.	Información confidencial	N/A

4. VISIBILITY AUDIT

TASK	COMMENTS	COMPLETION STATUS
Determined targets through all enumeration tasks.	Ciertos puertos UDP no se	Hecho
Determined new targets by researching known	Ciertos puertos UDP no se	Hecho

5. CONTROLS VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Verified controls for Non-Repudiation functioning	Ninguno	Hecho
Verified controls for Confidentiality functioning	Ninguno	Hecho
Verified controls for Privacy functioning according to	Ninguno	Hecho
Verified controls for Integrity functioning according to	Ninguno	Hecho
Verified controls for Alarm functioning according to all	Información confidencial	No hecho
Verified known security limitations of all controls Class B	Ninguno	Hecho
Searched for novel circumvention techniques and	Ninguno	Hecho

Ilustración 7. Reporte MMAT STAR- Parte 3.

6. TRUST VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Determined interactions which rely on other	Ninguno	Hecho
Determined targets with trust relationships to other	Ninguno	No hecho
Determined targets with trust relationships to other	Ninguno	No hecho
Verified known security limitations of discovered trusts	Ninguno	Hecho
Verified known security limitations of discovered trusts	Ninguno	Hecho
Searched for novel circumvention techniques and	Ninguno	No hecho

7. ACCESS VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Verified interactions with access points to all targets in	Ninguno	Hecho
Determined type of interaction for all access points	Ninguno	No hecho
Determined source of interaction defined as a service	Ninguno	Hecho
Verified depth of access	Ninguno	No hecho
Verified known security limitations of discovered	Ninguno	Hecho
Searched for novel circumvention techniques and	Ninguno	No hecho

8. PROCESS VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Determined all processes controlling the action of		Hecho
Verified the interaction operates within the confined		No hecho
Verified the interaction operates within the confined		No hecho
Determined the gap between the operations of		No hecho
Verified known security limitations of discovered		Hecho
Searched for novel circumvention techniques and		No hecho

9. CONFIGURATION/TRAINING VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Verified configuration/training requirements		No hecho
Verified the application of appropriate security		No hecho
Verified the functionality and security limitations		No hecho
Searched for novel circumvention techniques and		No hecho

10. PROPERTY VALIDATION

TASK	COMMENTS	COMPLETION STATUS
Determined the amount and type of unlicensed		No hecho
Verify the amount and type of unlicensed intellectual		No hecho

11. SEGREGATION REVIEW

TASK	COMMENTS	COMPLETION STATUS
Determined the amount and location of private	Dado por el administrador de red	No hecho
Determined the type of private information at	Dado por el administrador de red	No hecho
Verified the relationship between publicly accessible	Dado por el administrador de red	No hecho
Verified the accessibility of public accesses within the	Dado por el administrador de red	No hecho

12. EXPOSURE VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Searched for available targets through publicly	Dado por el administrador de red	No hecho
Searched for available organizational assets at		Hecho
Determined access, visibility, trust, and context		Hecho
Determined a profile of the organization's online		No hecho
Determined a profile of the organization's online		No hecho

13. COMPETITIVE INTELLIGENCE SCOUTING

TASK	COMMENTS	COMPLETION STATUS
Determined the business environment of partners		No hecho
Determined the business environment of partners		No hecho
Determined the organizational environment through		No hecho
Determined the organizational environment through		No hecho

Ilustración 8. Reporte MMAT STAR- Parte 4.

14. QUARANTINE VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Verified quarantine methods for interactions to the		No aplica
Verified quarantine methods for interactions from the		No aplica
Verified length of time of quarantine.		No aplica
Verified quarantine process from receive to release.		No aplica
Verified known security limitations of discovered		No aplica
Searched for novel circumvention techniques and		No aplica

15. PRIVILEGES AUDIT

TASK	COMMENTS	COMPLETION STATUS
Verified the means of legitimately obtaining privileges		No aplica
Verified the use of fraudulent identification to obtain		No aplica
Verified the means of circumventing authentication		No aplica
Verified the means of taking non-public		No aplica
Verified the means hijacking other authentication		No aplica
Verified known security limitations of discovered		No aplica
Searched for novel circumvention techniques and		No aplica
Determined depth of all discovered authentication		No aplica
Determined re-usability of all discovered		No aplica
Verified requirements towards obtaining		No aplica
Verified means towards obtaining authentication		No aplica

16. SURVIVABILITY VALIDATION/SERVICE CONTINUITY

TASK	COMMENTS	COMPLETION STATUS
Determined measures applicable to disrupt or stop		No aplica
Verified continuity processes and safety mechanisms		No aplica
Verified known security limitations of discovered		No aplica
Searched for novel circumvention techniques and		No aplica

17. ALERT AND LOG REVIEW/END SURVEY

TASK	COMMENTS	COMPLETION STATUS
Verified methods for recording and alerting		No aplica
Verified methods for recording and alerting		No aplica
Verified speed of recording and alerting.		No aplica
Verified persistence of recording and alerting.		No aplica
Verified integrity of recording and alerting.		No aplica
Verified distribution process of recording and alerting.		No aplica
Verified known security limitations of discovered		No aplica
Searched for novel circumvention techniques and		No aplica

Ilustración 9.Reporte MMAT STAR- Parte 5.

4.4 Soluciones planteadas

Del análisis de vulnerabilidades realizado se deben parchar los servicios que están desactualizados así como cambiar las cuentas que están por defecto. Además realizar las configuraciones pertinentes para que los servicios no estén expuestos. También se deben analizar los conjuntos de cifrados usados en los certificados digitales para evitar un posible ataque de seguridad, esto dependerá de la lógica del negocio de la empresa. A continuación se detallan las vulnerabilidades encontradas y las soluciones de cada uno de los 11 activos analizados.

SERVIDOR DE CORREO

Vulnerabilidad
1. El certificado SSL no es confiable. 2. Conjunto de Cifrado SSL Débil. 3. Detección del protocolo SSL Versión 2 (v2). 4. Certificado SSL auto firmado. 5. Conjunto de Cifrado SSL Medio. 6. Conjunto de Cifrado SSL Anónimo. 7. Exposición en la zona de transferencia del servidor DNS (AXFR). 8. Exposición de la caché en el servidor DNS.

Tabla XXII. Servidor de correo – Vulnerabilidad

Descripción
1. El certificado no es emitido por una autoridad de certificación pública reconocida. 2. Este es el listado que soporta el servidor de correo: SSLv2 EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export SSLv3 EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export TLSv1 EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export 3. Se está usando cifrado con un protocolo que tiene muchas fallas. El atacante puede efectuar un ataque de hombre en el medio o descifrar las comunicaciones entre el servidor y el cliente. 4. La cadena del certificado SSL (***/-Subject: O=TurnKey Linux/OU=Software appliances***) terminada con un certificado no reconocido. Esto puede ocasionar un ataque de man in the middle. 5. Este es el listado que soporta el servidor de correo. SSLv2 DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5 SSLv3 DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1 TLSv1 DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1 6. Este es el listado que soporta el servidor de correo. SSLv3 ADH-DES-CBC3-SHA Kx=DH Au=None Enc=3DES(168) Mac=SHA1 ADH-RC4-MD5 Kx=DH Au=None Enc=RC4(128) Mac=MD5 TLSv1 ADH-DES-CBC3-SHA Kx=DH Au=None Enc=3DES(168) Mac=SHA1 ADH-AES128-SHA Kx=DH Au=None Enc=AES(128) Mac=SHA1 ADH-AES256-SHA Kx=DH Au=None Enc=AES(256) Mac=SHA1 ADH-CAMELLIA128-SHA Kx=DH Au=None Enc=Camellia(128) Mac=SHA1 ADH-CAMELLIA256-SHA Kx=DH Au=None Enc=Camellia(256) Mac=SHA1 ADH-RC4-MD5 Kx=DH Au=None Enc=RC4(128) Mac=MD5 ADH-SEED-SHA Kx=DH Au=None Enc=SEED(128bh) Mac=SHA1 7. Un atacante puede re direccionar la zona de transferencia y con eso obtenerla topología de la red o engañar a los equipos de la red. 8. El atacante puede acceder a la caché para crear un bosquejo de la topología de la red o comprobar vulnerabilidades de los DNS utilizados.

Tabla XXIII. Servidor de correo – Descripción

Solución
1. Comprar o generar el certificado apropiado. 2. Configurar el Conjunto de Cifrado para evitar niveles débiles de cifrado. 3. Deshabilitar SSL 2.0 y usar SSL 3.0, TLS 1.0, o superior. 4. Comprar o generar el certificado apropiado. 5. Configurar el Conjunto de Cifrado para evitar niveles medios de cifrado 6. Configurar el Conjunto de Cifrado para evitar cifrado anónimo. 7. Limitar la zona de transferencia sólo a los servidores que la necesitan. 8. Contactar al vendedor para instalar el respectivo parche.

Tabla XXIV. Servidor de correo - Solución

SERVIDOR DE BIBLIOTECA

Vulnerabilidad
1. Detección de Archivo en Política Web Site Cross-Domain. 2. Divulgación de Información en Web Server robots.txt.
Descripción
1. El servidor web remoto contiene un archivo de política cross-domain (crossdomain.xml). Políticas inapropiadas en especial no restringidas "*" pueden ocasionar ataques cross-site request forgery and cross-site scripting al servidor web. 2. El servidor web tiene un archivo robots.txt que evita que los robots web accedan a ciertos directorios del sitio. Un atacante puede usar este archivo para aprender y tratar de conectarse a esos directorios protegidos.
Solución
1. Revisar las políticas en el archivo crossdomain.xml. 2. Usar etiquetas ROBOTS META en lugar de entradas al archivo robots.txt y/o restringir el acceso a material sensible en el sitio web.

Tabla XXV. Servidor de biblioteca – Vulnerabilidad,Descripción, Solución.

SERVIDOR DE CONTABILIDAD

Vulnerabilidad
1. Certificado SSL auto firmado. 2. Conjunto de Cifrado SSL Medio. 3. El certificado SSL no es confiable. 4. La firma está deshabilitada en SMB. 5. Desbordamiento remoto del requerimiento de la cabecera lighttpd mod_fastcgi HTTP.
Descripción
1. La cadena del certificado SSL (***/-Subject: O=TurnKey Linux/OU=Software appliances***) terminada con un certificado no reconocido. Esto puede ocasionar un ataque de man in the middle. 2. Este es el listado que soporta el servidor web. DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1 TLSv1 DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1 Un atacante puede realizar un ataque de fuerza bruta debió al tamaño del algoritmo DES 3. El certificado no es emitido por una autoridad de certificación pública reconocida. 4. La firma está deshabilitada en SMB. Esto puede ocasionar un ataque de man in the middle al servidor SMB. 5. Debido a que el módulo (mod_fastcgi). tiene una falla. El atacante puede realizar un ataque del desbordamiento del buffer
Solución
1. Comprar o generar el certificado apropiado. 2. Configurar el Conjunto de Cifrado para evitar niveles medios de cifrado. 3. Comprar o generar el certificado apropiado. 4. Forzar que los mensajes SMB sean firmados esto se puede configurar en Firma del Servidor. 5. Deshabilitar el módulo mod_fastcgi o realizar un upgrade a lighttpd 1.4.18 o una versión mayor

Tabla XXVI. Servidor de contabilidad – Vulnerabilidad,Descripción, Solución.

SERVIDOR DHCP

Vulnerabilidades
1. Múltiple Vulnerabilidades en Apache 2.2 < 2.2.15. 2. Múltiple Vulnerabilidades en Apache 2.2 < 2.2.14. 3. Apache 2.2 < 2.2.13 APR Desbordamiento de la pila en el módulo apr_palloc. 4. Conjunto de Cifrado SSL Débil. 5. Detección del protocolo SSL Versión 2 (v2). 6. Certificado SSL auto firmado. 7. Conjunto de Cifrado SSL Medio. 8. El certificado SSL no es confiable. 9. Los métodos HTTP TRACE / TRACK están permitidos. 10. Múltiple Vulnerabilidades en Apache 2.x < 2.2.12. 11. Múltiple Vulnerabilidades en Apache 2.x < 2.2.22. 12. Negación de servicio en el módulo mod_proxy_ajp de Apache 2.2 < 2.2.21. 13. Múltiple Vulnerabilidades en Apache 2.x < 2.2.17. 14. Múltiple Vulnerabilidades en Apache 2.x < 2.2.16. 15. Negación de servicio en el módulo apr_fnmatch de Apache 2.2 < 2.2.18. 16. Múltiple Vulnerabilidades en Apache 2.x < 2.2.9. (Negación de servicio, XSS)

Tabla XXVII. Servidor DHCP – Vulnerabilidades

Descripción
1. Propenso a múltiples vulnerabilidades tales como: renegociación TLS, ataque back-end, call-backs indefinidos y ataque Slowloris. 2. Propenso a múltiples vulnerabilidades tales como: negación de servicio, bypass de las restricciones en los accesos, 3. Existe una falla en el módulo apr_palloc que puede ocasionar el desbordamiento del buffer. 4. Este es el listado que soporta el servidor web. SSLv2 EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export 5. Se está usando cifrado con un protocolo que tiene muchas fallas. El atacante puede efectuar un ataque de hombre en el medio o descifrar las comunicaciones entre el servidor y el cliente. 6. La cadena del certificado SSL (|-Subject: O=TurnKey Linux/OU=Software appliances) terminada con un certificado no reconocido. Esto puede ocasionar un ataque de man in the middle. 7. Este es el listado que soporta el servidor web. SSLv2 DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5 SSLv3 DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1 TLSv1 DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1 8. El certificado no es emitido por una autoridad de certificación pública reconocida. 9. El servidor web tiene habilitada las opciones HTTP TRACE / TRACK las cuales permiten efectuar una depuración de las conexiones del mismo. 10. Existen múltiples vulnerabilidades que puede ocasionar el desbordamiento del buffer en la pila. 11. Existen múltiples vulnerabilidades que puede ocasionar el desbordamiento del buffer en la pila. 12. Negación de servicio hace que el servidor deje de funcionar. (END ERROR) 13. Existen múltiples vulnerabilidades que puede ocasionar el desbordamiento del buffer en la pila. 14. Existen múltiples vulnerabilidades que puede ocasionar el desbordamiento del buffer en la pila. 15. Negación de servicio hace que el servidor se inhiba. 16. Ataques de negación de servicio y XSS.

Tabla XXVIII. Servidor DHCP – Descripción

Solución
1. Realizar un upgrade a Apache versión 2.2.15 o superior. 2. Realizar un upgrade a Apache versión 2.2.14 o superior. 3. Realizar un upgrade a Apache versión 2.2.13 o superior. 4. Configurar el Conjunto de Cifrado para evitar niveles débiles de cifrado. 5. Deshabilitar SSL 2.0 y usar SSL 3.0, TLS 1.0, o superior. 6. Comprar o generar el certificado apropiado. 7. Configurar el Conjunto de Cifrado para evitar niveles medios de cifrado. 8. Comprar o generar el certificado apropiado. 9. Deshabilitar las opciones HTTP TRACE / TRACK. 10. Realizar un upgrade a Apache versión 2.2.12 o superior. 11. Realizar un upgrade a Apache versión 2.2.22 o superior. 12. Realizar un upgrade a Apache versión 2.2.21 o superior. 13. Realizar un upgrade a Apache versión 2.2.17 o superior. 14. Realizar un upgrade a Apache versión 2.2.16 o superior. 15. Realizar un upgrade a Apache versión 2.2.18 o superior. 16. Realizar un upgrade a Apache versión 2.2.9 o superior.

Tabla XXIX. Servidor DHCP –Solución

SERVIDOR DVR 1

Vulnerabilidades
1. XSS genérico en Servidor web
Descripción
1. El atacante puede ejecutar código malicioso java script en el servidor.
Solución
1. Parchar o realizar un upgrade(Contactarse con el vendedor)

Tabla XXX. Servidor DVR1– Vulnerabilidad,Descripción, Solución.

SERVIDOR DVR 2

Vulnerabilidades
1. XSS genérico en Servidor web
Descripción
1. El atacante puede ejecutar código malicioso java script en el servidor.
Solución
1. Parchar o realizar un upgrade(Contactarse con el vendedor)

Tabla XXXI. Servidor DVR2– Vulnerabilidad,Descripción, Solución.

SERVIDOR VOZ SOBRE IP

Vulnerabilidad
1. Los métodos HTTP TRACE / TRACK están permitidos. 2. Revelación de la cookies en Apache HTTP Server. 3. Certificado SSL auto firmado. 4. Conjunto de Cifrado SSL Medio. 5. El certificado SSL no es confiable.
Descripción
1. El servidor web tiene habilitada las opciones HTTP TRACE / TRACK las cuales permiten efectuar una depuración de las conexiones del mismo. 2. El atacante pueden enviar una cabecera que exceda el límite lo cual puede mostrar información de las cookies. 3. La cadena del certificado SSL (***I-Subject: O=TurnKey Linux/OU=Software appliances***) terminada con un certificado no reconocido. Esto puede ocasionar un ataque de man in the middle. 4. Este es el listado que soporta el servidor web. SSLv3 EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56) Mac=SHA1 DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1 TLSv1 EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56) Mac=SHA1 DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1 5. El certificado no es emitido por una autoridad de certificación pública reconocida.
Solución
1. Deshabilitar las opciones HTTP TRACE / TRACK. 2. Realizar un upgrade a Apache versión 2.2.22 o superior. 3. Comprar o generar el certificado apropiado. 4. Configurar el Conjunto de Cifrado para evitar niveles medios de cifrado. 5. Comprar o generar el certificado apropiado.

Tabla XXXII. Servidor voz sobre IP– Vulnerabilidad,Descripción, Solución.

SERVIDOR HARD DRIVE 1

Vulnerabilidad
1. Detección obsoleta de servidor web. 2. Cuenta FTP por defecto XAMPP. 3. Compartimiento de Acceso no privilegiado en Microsoft Windows SMB. 4. Los métodos HTTP TRACE / TRACK están permitidos. 5. Revelación de la cookies en Apache HTTP Server. 6. Certificado SSL auto firmado. 7. El certificado SSL no es confiable. 8. La firma está deshabilitada en SMB. 9. Acceso a la cuenta invitado del usuario local Microsoft Windows SMB. 10. Detección de mDNS. 11. FTP Anónimo está habilitado.

Tabla XXXIII. Servidor hard drive 1– Vulnerabilidad.

Descripción
1. El servidor web está obsoleto y no soporte técnico del vendedor. 2. El servidor tiene una cuenta (usuario y contraseña) por defecto FTP cuando se instaló XAMPP. Un atacante puede tener acceso al sistema con estos privilegios. 3. Se está compartiendo más de una carpeta sin restricción alguna. 4. El servidor web tiene habilitada las opciones HTTP TRACE / TRACK las cuales permiten efectuar una depuración de las conexiones del mismo. 5. El atacante pueden enviar una cabecera que exceda el límite lo cual puede mostrar información de las cookies. 6. La cadena del certificado SSL (***/-Subject: O=TurnKey Linux/OU=Software appliances***) terminada con un certificado no reconocido. Esto puede ocasionar un ataque de man in the middle. 7. El certificado no es emitido por una autoridad de certificación pública reconocida. 8. La firma está deshabilitada en SMB. Esto puede ocasionar un ataque de man in the middle al servidor SMB. 9. .Hay posibilidades de autenticarse usando el usuario invitado con una contraseña aleatoria. 10. Permite a cualquiera ver el sistema operativo, su version y los servicios que se están ejecutando. 11. Permite a cualquier usuario autenticarse sin la correspondiente contraseña.

Tabla XXXIV. Servidor hard drive 1– Descripción.

Solución
1. Eliminar el servicio si no es necesario caso contrario realice un upgrade del mismo. 2. Cambiar la contraseña FTP. 3. En Windows ir el explorador, dar clic derecho, ir a la pestaña compartir y luego seleccionar permisos. 4. Deshabilitar las opciones HTTP TRACE / TRACK. 5. Realizar un upgrade a Apache versión 2.2.22 o superior. 6. Comprar o generar el certificado apropiado. 7. Comprar o generar el certificado apropiado. 8. Forzar que los mensajes SMB sean firmados esto se puede configurar en la Política de Seguridad Local 9. En política de grupo cambiar la configuración a: 'Acceso a la red: Modelos de compartimentos y seguridad para cuentas locales' de 'Solo invitado –Usuarios locales autenticarse como invitado' a 'Clásica – Usuarios locales auto autenticarse'. 10. Filtrar el tráfico entrante al puerto UDP 5353. 11. Deshabilitar FTP Anónimo si es posible.

Tabla XXXV. Tabla XXXV. Servidor hard drive 1– Solución.

SERVIDOR HARD DRIVE 2

Vulnerabilidad
1. Detección obsoleta de servidor web.
2. Cuenta FTP por defecto XAMPP.
3. Usuario compartido montable NFS
4. Compartimiento de Acceso no privilegiado en Microsoft Windows SMB.
5. Los métodos HTTP TRACE / TRACK están permitidos.
6. Revelación de la cookies en Apache HTTP Server.
7. Certificado SSL auto firmado.
8. El certificado SSL no es confiable.
9. La firma está deshabilitada en SMB.
10. Compartimiento NFS de lectura.
11. Acceso a la cuenta invitado del usuario local Microsoft Windows SMB.
12. Detección de mDNS.
13. FTP Anónimo está habilitado.

Tabla XXXVI. Servidor hard drive 2– Vulnerabilidad.

Descripción
1. El servidor web está obsoleto y no soporte técnico del vendedor. 2. El servidor tiene una cuenta (usuario y contraseña) por defecto FTP cuando se instaló XAMPP. Un atacante puede tener acceso al sistema con estos privilegios. 3. El atacante puede tener privilegios de lectura y escritura en los archivos compartidos. 4. Se está compartiendo más de una carpeta sin restricción alguna. 5. El servidor web tiene habilitada las opciones HTTP TRACE / TRACK las cuales permiten efectuar una depuración de las conexiones del mismo. 6. El atacante pueden enviar una cabecera que exceda el límite lo cual puede mostrar información de las cookies. 7. La cadena del certificado SSL (|-Subject: O=TurnKey Linux/OU=Software appliances) terminada con un certificado no reconocido. Esto puede ocasionar un ataque de man in the middle. 8. El certificado no es emitido por una autoridad de certificación pública reconocida. 9. La firma está deshabilitada en SMB. Esto puede ocasionar un ataque de man in the middle al servidor SMB. 10. El servidor está exportando archivos con permisos de lectura sin realizar el respectivo filtro por IP o nombre del equipo. 11. Hay posibilidades de autenticarse usando el usuario invitado con una contraseña aleatoria. 12. Permite a cualquiera ver el sistema operativo, su version y los servicios que se están ejecutando. 13. Permite a cualquier usuario autenticarse sin la correspondiente contraseña.

Tabla XXXVII. Servidor hard drive 2– Descripción.

Solución
1. Eliminar el servicio si no es necesario caso contrario realice un upgrade del mismo. 2. Cambiar la contraseña FTP. 3. Configurar al servidor para que sólo equipos autorizados puedan tener privilegios en los archivos. 4. En Windows ir el explorador, dar clic derecho, ir a la pestaña compartir y luego seleccionar permisos. 5. Deshabilitar las opciones HTTP TRACE / TRACK. 6. Realizar un upgrade a Apache versión 2.2.22 o superior. 7. Comprar o generar el certificado apropiado. 8. Comprar o generar el certificado apropiado. 9. Forzar que los mensajes SMB sean firmados esto se puede configurar en la Política de Seguridad Local 10. Aplicar las configuraciones apropiadas para compartir un archivo. 11. 12. En política de grupo cambiar la configuración a: 'Acceso a la red: Modelos de compartimentos y seguridad para cuentas locales' de 'Solo invitado –Usuarios locales autenticarse como invitado' a 'Clásica – Usuarios locales auto autenticarse'. 13. Filtrar el tráfico entrante al puerto UDP 5353. 14. Deshabilitar FTP Anónimo si es posible.

Tabla XXXVIII. Servidor hard drive 2– Solución.

SERVIDOR ADMINISTRATIVO

Vulnerabilidad
1. Detección de mDNS
Descripción
1. Permite a cualquiera ver el sistema operativo, su version y los servicios que se están ejecutando.
Solución
1. Filtrar el tráfico entrante al puerto UDP 5353.

Tabla XXXIX. Servidor administrativo– Vulnerabilidad,Descripción,Solución.

4.5 Conclusiones y Recomendaciones

4.5.1 Conclusiones .

1. El VER de la auditoria de seguridad realizada es de 68.44 % lo cual quiere decir que hay un 31.56% de inseguridad en el blanco definido en esta tesis. Este VER permitirá al departamento de sistemas tener una base comparativa en cuanto al nivel de seguridad ya que pueden realizar otras auditorías con el mismo alcance y contrastar los resultados.

2. El reporte MMATS STAR refleja el detalle de la aplicación de esta auditoria en forma general y técnica para que en futuras auditorías de seguridad se puedan comparar las diferentes fases con sus módulos y ver las mejoras en el mismo.

3. Los resultados obtenidos sirven como marco de referencia para la aplicación del análisis de riesgo, ya que sabiendo la porosidad, los controles y las limitaciones, se tendrá un enfoque más claro del activo o servicio que requiere mayor atención.

4. Las soluciones que se dan a las porosidades y limitaciones encontradas deberán ser analizadas por el administrador de red al momento de sus aplicaciones, debido a que podrían ir en contra de la lógica del negocio o bien las vulnerabilidades encontradas podrían tener un nivel de

incidencia mínimo. La mayoría de las soluciones sugeridas deben ser implementadas.

En definitiva se cumplieron todos los objetivos específicos planteados con soluciones reales y prácticas para así medir él nivel de seguridad y mejorarla.

4.5.2 Recomendaciones.

1. Es importante que se cree una política de auditoría de seguridad con un periodicidad de 2 veces en el año escolar. Una al inicio del primer semestre y otra al inicio del 2do semestre. Estas auditorías deberían mantener el mismo alcance para así poder realizar las respectivas comparaciones, caso contrario no servirán. Sería interesante llevar a cabo estas auditorías con diferentes tipos de pruebas para tener perspectivas técnicas.

2. Al contar con un VER inicial se puede aplicar el mismo proceso para obtener el VER de otros activos de la empresa como los son los activos del personal administrativo y más importante los activos de los estudiantes y profesores.

3. Para tener un mejor criterio de selección en cuanto la porosidad o limitación a corregir se deben aplicar los indicadores de confianza. Estos indicadores permite establecer de manera numérica y precisa los pesos que se deben dar a las porsidades y limitaciones encontradas. Si se aplica alguna metodología de análisis de riesgo se deben emplear los indicadores de confianza para que los resultados sean más efectivos.

ANEXO A (CONTRATO)

Guayaquil 3 de Julio de 2012

El siguiente contrato tiene como objetivo efectuar una auditoria de seguridad al departamento de sistemas del InterAmerican Academy, la cual consta de las siguientes partes:

- Alcance: puertos abiertos, filtrados y cerrados. Servicios correspondientes a cada blanco, certificados de seguridad, autenticación del servidor de archivos y chequeo de cuentas por defecto.
- El blanco: Firewall, servidores de: correo, biblioteca, voz sobre IP, DHCP, cámaras de seguridad (DVR), contabilidad, administrativo, discos duros.
- Vector: Externa-Interna (Externa al firewall e interna a los otros servidores)
- Canal: Redes de Datos
- Indice: 11 (son 2 discos duros y 2 DVRs)

Se garantizara la confidencialidad e integridad de la información por lo cual solo se mostrará y se hará el escaneo de puertos y el análisis de vulnerabilidades.

El tipo de prueba que se aplicará es la de caja gris es decir, el administrador de red dará toda la información necesaria para llevar a cabo esta prueba de penetración. Esta auditoria de seguridad se basa en la Constitución del Ecuador así como en la ley de comercio electrónico.

Al final de la prueba de penetración se realizará el reporte MMATS STAR, las soluciones a las porosidades y limitaciones encontradas así como la muestra en detalle del cálculo de los Valores de Evaluación de Riesgo (VER).

A continuación se detallan las firmas de las personas que están de acuerdo con el presente contrato.

Peter Norrenkamp

Executive Director

Francisco Bolaños

Analista de seguridad

ANEXO B (PLAN DE PRUEBAS)

PLAN DE PRUEBAS					
Item	**Tarea**	**Fecha Inicio**	**Fecha Fin**	**Responsable**	**Facilitador**
1	Recolección de información del departamento de sistemas	25/06/2012	29/06/2012	Analista de seguridad	Administrador de red
2	Análisis y selección de las herramientas de hackeo	02/07/2012	06/07/2012	Analista de seguridad	No aplica
3	Escaneo de puertos	09/07/2012	13/07/2012	Analista de seguridad	No aplica
4	Análisis de vulnerabilidades	16/07/2012	20/07/2012	Analista de seguridad	No aplica
5	Aplicación de las fases de la metodología	23/07/2012	27/07/2012	Analista de seguridad	No aplica
6	Cálculo de VER y elaboración del reporte de Seguridad Actual	30/07/2012	30/07/2012	Analista de seguridad	No aplica
7	Elaboración del reporte MAGERIT STAR	30/07/2012	30/07/2012	Analista de seguridad	No aplica
8	Descripción de soluciones planteadas	30/07/2012	30/07/2012	Analista de seguridad	No aplica

ANEXO C (ESCANEO DE PUERTOS)

CONTABILIDAD

```
# Nmap 5.51 scan initiated Wed Jul 18 15:51:39 2012 as: nmap -oN
contabilidad.txt -P 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0026s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (protocol
2.0)
80/tcp  open  http        lighttpd 1.4.26
139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: ACIG)
443/tcp open  ssl/http    lighttpd 1.4.26
445/tcp open  netbios-ssn Samba smbd 3.X (workgroup: ACIG)
MAC Address: 00:0C:29:65:A4:4E (VMware)
No exact OS matches for host (If you know what OS is running on
it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.51%D=7/18%OT=22%CT=1%CU=42856%PV=Y%DS=1%DC=D%G=Y%M=
000C29%TM=50
Network Distance: 1 hop
Service Info: OS: Linux

OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
# Nmap done at Wed Jul 18 15:52:22 2012 -- 1 IP address (1 host
up) scanned in 42.68 seconds
```

```
# Nmap 5.51 scan initiated Tue Jul 24 19:10:45 2012 as: nmap -oN
contabilidadu.txt -sU 0-65535 [redacted]
Nmap scan report for [redacted]
Host is up (0.0015s latency).
Not shown: 996 closed ports
PORT      STATE         SERVICE     VERSION
123/udp   open          ntp         NTP v4
137/udp   open          netbios-ns  Samba nmbd (workgroup: ACIG)
138/udp   open|filtered netbios-dgm
20004/udp open          webmin      (https on TCP port 20004)
MAC Address: 00:0C:29:55:A4:4E (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Service Info: Host: MASTER

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 19:30:09 2012 -- 1 IP address (1 host up)
scanned in 1164.44 seconds
```

DHCP

```
# Nmap 5.51 scan initiated Wed Jul 18 14:24:37 2012 as: nmap -oN
dhcp.txt -P 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 4.7p1 Debian 8ubuntu2 (protocol
2.0)
80/tcp  open  http     Apache httpd 2.2.8
443/tcp open  ssl/http Apache httpd 2.2.8
MAC Address: 00:0C:29:10:CF:1F (VMware)
No exact OS matches for host (If you know what OS is running on
it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.51%D=7/18%OT=22%CT=1%CU=37640%PV=Y%DS=1%DC=D%G=Y%M=
000C29%TM=50

Network Distance: 1 hop
Service Info: OS: Linux

OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
# Nmap done at Wed Jul 18 14:25:14 2012 -- 1 IP address (1 host
up) scanned in 37.77 seconds
```

```
# Nmap 5.61 scan initiated Tue Jul 24 11:30:27 2012 as: nmap -oN
dhcp1.txt -sU 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0018s latency).
Not shown: 985 closed ports
PORT      STATE         SERVICE  VERSION
67/udp    open|filtered dhcps
120/udp   open|filtered cfdptkt
123/udp   open          ntp      NTP v4 (unsynchronized)
514/udp   open|filtered syslog
1027/udp  open|filtered unknown
2160/udp  open|filtered apc-2160
17205/udp open|filtered unknown
18373/udp open|filtered unknown
18987/udp open|filtered unknown
19120/udp open|filtered unknown
19933/udp open|filtered unknown
21699/udp open|filtered unknown
21702/udp open|filtered unknown
22914/udp open|filtered unknown
39999/udp open|filtered unknown
MAC Address: 00:0C:29:10:CF:1F (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 12:06:29 2012 -- 1 IP address (1 host up)
scanned in 2162.05 seconds
```

DVR1

```
# Nmap 5.51 scan initiated Wed Jul 18 14:30:49 2012 as: nmap -oN
dvr1.txt -P 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0018s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
80/tcp  open  http?
554/tcp open  rtsp?
2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
==============
SF-Port80-TCP:V=5.51%I=7%D=7/18%Time=500700EC%P=x86_64-unknown-
linux-gnu%r
MAC Address: 00:0E:53:18:5C:1B (AV Tech)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.12 - 2.6.14 (embedded)
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
# Nmap done at Wed Jul 18 14:32:25 2012 -- 1 IP address (1 host
up) scanned in 96.66 seconds
```

```
# Nmap 5.51 scan initiated Tue Jul 24 13:32:24 2012 as: nmap -oN
dvr1u.txt -sU -P0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0017s latency).
All 65535 scanned ports on 192.168.201.20 are closed
MAC Address: 00:0E:53:18:5F:4B (AV Tech)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 13:50:34 2012 -- 1 IP address (1 host up)
scanned in 1090.72 seconds
```

DVR2

```
# Nmap 5.51 scan initiated Wed Jul 18 14:31:13 2012 as: nmap -oN
dvr2.txt -P 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
80/tcp  open  http?
554/tcp open  rtsp?
2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
==============
SF-Port80-TCP:V=5.51%I=7%D=7/18%Time=5007010%P=x86_64-unknown-
linux-gnu%r
MAC Address: 00:0E:53:18:5F:4B (AV Tech)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.12 - 2.6.14 (embedded)
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
# Nmap done at Wed Jul 18 14:32:50 2012 -- 1 IP address (1 host
up) scanned in 96.66 seconds


# Nmap 5.51 scan initiated Tue Jul 24 13:54:52 2012 as: nmap -oN
dvr2u.txt -sU 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0050s latency).
All 65535 scanned ports on 192.168.201.19 are closed
MAC Address: 00:0E:53:18:5C:1B (AV Tech)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 14:13:01 2012 -- 1 IP address (1 host up)
scanned in 1089.28 seconds
```

FIREWALL

```
# Nmap 5.51 scan initiated 2012-07-24 20:20 2012 as: nmap -f -oN
fragmented1.txt [redacted]
# Nmap done at 2012-07-24 20:24 2012 2012 -- 1 IP address (0 hosts up)
scanned in 3.33 seconds


# Nmap 5.51 scan initiated 2012-07-24 20:30  2012 as: nmap -mtu 24 -oN
fragmented2.txt [redacted]
# Nmap done at 2012-07-24 20:34 :04 2012 -- 1 IP address (0 hosts up)
scanned in 9.26 seconds

root@root:-# nmap -D [redacted] -oN
fragmented3.txt

Starting Nmap 5.51 ( http://nmap.org ) at 2012-07-24 21:15  EDT
Note: Host seems down. If it is really up, but blocking our ping probes,
try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.22 seconds
```

```
# Nmap 5.51 scan initiated Tue Jul 24 18:07:32 2012 as: nmap -oN
firewall1.txt -p 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.075s latency).
Not shown: 99% filtered ports
PORT     STATE  SERVICE    VERSION
80/tcp   open   http       Zimbra http config
110/tcp  open   pop3       Zimbra pop3d
113/tcp  closed auth
143/tcp  open   imap       Zimbra imapd
443/tcp  closed https
1723/tcp open   pptp?
6500/tcp open   vnc-http?
5900/tcp open   vnc        VNC (protocol 3.7)
8090/tcp open   ssl/http   thttpd
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port5900-TCP:V=5.51%I=7%D=7/24%Time=500F1E87%P=x86_64-unknown-linux-
gnu
SF:%r(GetRequest,76,"HTTP/1\.0\x20404\x20Not\x20found\r\n\r\n<html>
<head><
Device type: general purpose|firewall|broadband router|WAP
Running (JUST GUESSING): Linux 2.6.X|2.4.X (89%), Check Point embedded
(88%), Actiontec embedded (87%)
Aggressive OS guesses: Linux 2.6.31 (88%), Check Point ZoneAlarm Z100G
firewall (89%), Actiontec GT701 DSL modem (87%), Check Point UTM-1 Edge
X firewall (87%), DD-WRT v23 (Linux 2.6.24) (87%), Linux 2.6.23 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: mail.interamerican.edu.ec

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 18:16:55 2012 -- 1 IP address (1 host up)
scanned in 563.60 seconds
```

```
# Nmap 5.51 scan initiated Tue Jul 24 18:18:11 2012 as: nmap -oN
firewallFIN.txt -P 0-65535 -sF -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.049s latency).
Not shown: 996 open|filtered ports
PORT      STATE SERVICE    VERSION
5800/tcp  open  vnc-http?
5900/tcp  open  vnc        VNC (protocol 3.7)
5907/tcp  open  vnc        VNC (protocol 3.8)
60443/tcp open  ssl/http   thttpd
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port5800-TCP:V=5.51%I=7%D=7/24%Time=500F1FE5%P=x86_64-unknown-linux-
gnu
SF:%r(GetRequest,76,"HTTP/1\.0\x20404\x20Not\x20found\r\n\r\n<html>
<head><
SF:title>File\x20Not\x20Found</title></head>\n<body><h1>File\x20Not
\x20Fou
SF:nd</h1></body></html>\n");
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results
incomplete
No OS matches for host

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 18:24:14 2012 -- 1 IP address (1 host up)
scanned in 542.78 seconds
```

```
# Nmap 5.51 scan initiated Tue Jul 24 18:13:20 2012 as: nmap -oN
firewallNull.txt -P 0-65535 -sN -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.065s latency).
Not shown: 991 open|filtered ports
PORT      STATE SERVICE     VERSION
80/tcp    open  http        Zimbra http config
143/tcp   open  imap        Zimbra imapd
1723/tcp  open  pptp?
5800/tcp  open  vnc-http?
5900/tcp  open  vnc         VNC (protocol 3.7)
5907/tcp  open  vnc         VNC (protocol 3.8)
7025/tcp  open  vmsvc-2?
9090/tcp  open  zeus-admin?
60443/tcp open  unknown
2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
==============
SF-Port5800-TCP:V=5.51%I=7%D=7/24%Time=500F1F76%P=x86_64-unknown-linux-
gnu
SF:%r(GetRequest,76,"HTTP/1\.0\x20404\x20Not\x20found\r\n\r\n<html>
<head><
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Device type: firewall|WAP|storage-misc|general purpose|VoIP adapter
Running: Fortinet embedded, Linux 2.4.X, Netgear RAIDiator 4.X, Sun
OpenSolaris, Vonage embedded
OS details: Fortinet FortiGate-50B or 310B firewall, Fortinet
FortiGate-60B or -100A firewall, DD-WRT v23 (Linux 2.4.36), Tomato 1.27
(Linux 2.4.20), Netgear ReadyNAS Duo NAS device (RAIDiator 4.1.4), Sun
OpenSolaris 2009.06, Vonage V-Portal VoIP gateway
Service Info: Host: mail.interamerican.edu.ec

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 18:22:04 2012 -- 1 IP address (1 host up)
scanned in 525.25 seconds
```

```
# Nmap 5.51 scan initiated Tue Jul 24 15:28:01 2012 as: nmap -oN
firewalle5.txt -P 0-65535 -sS -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.067s latency).
Not shown: 989 filtered ports
PORT      STATE  SERVICE    VERSION
80/tcp    open   http       Zimbra http config
110/tcp   open   pop3       Zimbra pop3d
113/tcp   closed auth
143/tcp   open   imap       Zimbra imapd
443/tcp   closed https
1723/tcp  open   pptp?
5800/tcp  open   vnc-http?
5900/tcp  open   vnc        VNC (protocol 3.7)
5907/tcp  open   vnc        VNC (protocol 3.8)
7025/tcp  open   vmsvc-2?
60443/tcp open   ssl/http   thttpd
2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
==============
SF-Port5800-TCP:V=5.51%I=7%D=7/24%Time=500F22CA%P=x86_64-unknown-linux-
gnu
Device type: firewall|broadband router|WAP|general purpose
Running (JUST GUESSING): Check Point embedded (89%), Actiontec embedded
(89%), Linux 2.4.X|2.6.X (89%), NetworksAOK embedded (85%)
Aggressive OS guesses: Check Point ZoneAlarm 2100G firewall (89%),
Actiontec GT701 DSL modem (89%), Check Point UTM-1 Edge X firewall
(89%), DD-WRT v23 (Linux 2.4.34) (89%), Linux 2.6.23 (89%), Linux
2.6.31 (85%), NetworksAOK network monitoring applicance (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: mail.interamerican.edu.ec

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 15:36:06 2012 -- 1 IP address (1 host up)
scanned in 485.39 seconds
```

```
# Nmap 5.51 scan initiated Tue Jul 24 18:29:00 2012 as: nmap -sN
firewallUDP.txt  -sU 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up.
All 65535 scanned ports on 200.93.199.170 are closed|filtered
Too many fingerprints match this host to give specific OS details

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 19:37:51 2012 -- 1 IP address (1 host up)
scanned in 4111.25 seconds


# Nmap 5.51 scan initiated Tue Jul 24 18:18:05 2012 as: nmap -sN
firewallXmas.txt -P 0-65535 -sX -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.048s latency).
Not shown: 996 open|filtered ports
PORT      STATE SERVICE  VERSION
1723/tcp  open  pptp?
7025/tcp  open  vmsvc-2?
9090/tcp  open  ssl/http thttpd
60443/tcp open  ssl/http thttpd
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port7025-TCP:V=5.51%I=7%D=7/24%Time=500F20A5%P=x86_64-unknown-linux-
gnu
Running (JUST GUESSING): AVM embedded (91%), Linksys embedded (89%),
Linux 2.4.X|2.6.X (89%), MontaVista Linux 2.4.X (89%), Motorola
embedded (85%), NetworksACX embedded (88%), Accrp embedded (87%), D-
Link embedded (87%)
Aggressive OS guesses: AVM FRITZ!Box FON WLAN 7170 WAP (91%), Linksys
WRV200 wireless broadband router (89%), Linux 2.4.21 (embedded) (89%),
Linux 2.6.29 (Gentoo) (89%), MontaVista embedded Linux 2.4.17 (89%),
Linux 2.6.18 (88%), Motorola AP-51xx WAP (88%), NetworksACX network
monitoring appliance (88%), Accrp W4000 or W4220 wireless ADSL modem
(MontaVista embedded Linux 2.4.17) (87%), D-Link DNS-323 NAS device or
Linksys WRT300N wireless broadband router (87%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 18:26:52 2012 -- 1 IP address (1 host up)
scanned in 527.02 seconds
```

Hard drive 1

```
# Nmap 5.51 scan initiated Tue Jul 24 12:30:22 2012 as: nmap -oN
hdiu.txt -sU -sV 0-65535 -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0014s latency).
Not shown: 994 closed ports
PORT     STATE         SERVICE      VERSION
68/udp   open|filtered dhcpc
137/udp  open          netbios-ns   Microsoft Windows XP netbios-ssn
138/udp  open|filtered netbios-dgm
631/udp  open|filtered ipp
1900/udp open|filtered upnp
5353/udp open          mdns         DNS-based service discovery
MAC Address: 00:D0:B8:16:1E:D9 (Iomega)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Service Info: Host: MULTIMEDIA; OS: Windows

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 12:49:38 2012 -- 1 IP address (1 host up)
scanned in 1155.57 seconds
```

Hard drive 2

```
# Nmap 5.51 scan initiated Wed Jul 18 14:25:39 2012 as: nmap -oN
hd1.txt -P 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0026s latency).
Not shown: 969 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
80/tcp    open  http         Apache httpd 1.3.41 ((Unix)
mod_auth_pam/1.1.1 DAV/1.0.3 mod_ssl/2.8.31 OpenSSL/0.9.8g)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: ACIG)
443/tcp   open  ssl/http     Apache httpd 1.3.41 ((Unix)
mod_auth_pam/1.1.1 DAV/1.0.3 mod_ssl/2.8.31 OpenSSL/0.9.8g)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: ACIG)
631/tcp   open  ipp          CUPS 1.2
873/tcp   open  rsync        (protocol version 30)
3260/tcp  open  iscsi?
3689/tcp  open  daap         mt-daapd DAAP 0.9.1
9000/tcp  open  upnp         TwonkyMedia UPnP (Linux 2.x.x; UPnP
1.0; pvConnect SDK 1.0)
49152/tcp open  upnp         Portable SDK for UPnP devices 1.6.9
(Kernel 2.6.31.8; UPnP 1.0)
MAC Address: D0:D0:B8:16:1E:D9 (Iomega)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.19 - 2.6.31
Network Distance: 1 hop
Service Info: OSs: Unix, Linux

OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
# Nmap done at Wed Jul 18 14:27:12 2012 -- 1 IP address (1 host
up) scanned in 103.51 seconds
```

```
# Nmap 5.51 scan initiated Wed Jul 18 14:25:33 2012 as: nmap -oN
hd2.txt -P 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0021s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         ProFTPD 1.3.1
80/tcp    open  http        Apache httpd 1.3.41 ((Unix)
mod_auth_pam/1.1.1 DAV/1.0.3 mod_ssl/2.8.31 OpenSSL/0.9.8g)
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: ACIG)
443/tcp   open  ssl/http    Apache httpd 1.3.41 ((Unix)
mod_auth_pam/1.1.1 DAV/1.0.3 mod_ssl/2.8.31 OpenSSL/0.9.8g)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: ACIG)
631/tcp   open  ipp         CUPS 1.2
873/tcp   open  rsync       (protocol version 30)
2049/tcp  open  rpcbind
3260/tcp  open  iscsi?
49152/tcp open  upnp        Portable SDK for UPnP devices 1.6.9
(kernel 2.6.31.6; UPnP 1.0)
MAC Address: 00:D0:B8:26:1C:93 (Iomega)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.19 - 2.6.33
Network Distance: 1 hop
Service Info: OSs: Unix, Linux

OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
# Nmap done at Wed Jul 18 14:27:37 2012 -- 1 IP address (1 host
up) scanned in 124.05 seconds
```

```
# Nmap 5.51 scan initiated Tue Jul 24 12:50:42 2012 as: nmap -sN
nd2u.txt -sU 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0012s latency).
Not shown: 992 closed ports
PORT     STATE         SERVICE      VERSION
68/udp   open|filtered dhcpc
111/udp  open          rpcbind
137/udp  open          netbios-ns   Microsoft Windows XP netbios-ssn
138/udp  open|filtered netbios-dgm
631/udp  open|filtered ipp
1900/udp open|filtered upnp
2049/udp open          rpcbind      0 (rpc #100000)
5353/udp open          mdns         DNS-based service discovery
MAC Address: 00:D0:B8:16:1C:93 (Iomega)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Service Info: Host: IX2-C; OS: Windows

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 13:09:54 2012 -- 1 IP address (1 host up)
scanned in 1152.70 seconds
```

Administrativo

```
# Nmap 5.51 scan initiated Wed Jul 18 14:33:13 2012 as: nmap -oN
jc.txt -P 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0015s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE   VERSION
5800/tcp open  vnc-http?
5900/tcp open  vnc       VNC (protocol 3.7)
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port5800-TCP:V=5.51%I=7%D=7/18%Time=5007017C%P=x86_64-unknown-
linux-gnu
SF:%r(GetRequest,76,"HTTP/1\.0\x20404\x20Not\x20found\r\n\r\n
<html><head><

Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
# Nmap done at Wed Jul 18 14:35:06 2012 -- 1 IP address (1 host
up) scanned in 113.71 seconds
```

```
# Nmap 5.61 scan initiated Wed Jul 18 14:16:16 2012 as: nmap -sV
elastix.txt -p 0-65535 -sT -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0021s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE      VERSION
22/tcp   open  ssh          OpenSSH 4.3 (protocol 2.0)
25/tcp   open  smtp         Postfix smtpd
80/tcp   open  http         Apache httpd 2.2.3 ((CentOS))
110/tcp  open  pop3         Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-
12.el5_7.2
111/tcp  open  rpcbind
143/tcp  open  imap         Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-
12.el5_7.2
443/tcp  open  ssl/http     Apache httpd 2.2.3 ((CentOS))
993/tcp  open  ssl/imap     Cyrus imapd
995/tcp  open  pop3         Cyrus pop3d
3306/tcp open  mysql        MySQL (unauthorized)
4445/tcp open  upnotifyp?
5038/tcp open  zeus-admin?
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port9090-TCP:V=5.61%I=7%D=7/18%Time=5006FD83%P=x86_64-unknown-
linux-gnu
SF:%r(GetRequest,14D,"HTTP/1\.1\x20200\x20OK\r\nExpires:\x20Thu,
\x2001\x20
MAC Address: 38:60:77:2E:83:FB (Unknown)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop
Service Info: Hosts:  interamerican.edu.ec, example.com
OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
# Nmap done at Wed Jul 18 14:18:32 2012 -- 1 IP address (1 host
up) scanned in 136.31 seconds
```

CORREO

```
Nmap scan report for [redacted]
Host is up (0.0015s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE  VERSION
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC BIND 9.7.0-P1
80/tcp    open  http     Zimbra http config
110/tcp   open  pop3     Zimbra pop3d
143/tcp   open  imap     Zimbra imapd
389/tcp   open  ldap     OpenLDAP 2.2.X - 2.3.X
465/tcp   open  ssl/smtp Postfix smtpd
587/tcp   open  smtp     Postfix smtpd
993/tcp   open  ssl/imap Zimbra imapd
995/tcp   open  ssl/pop3 Zimbra pop3d
5222/tcp  open  jabber   Zimbra 6 jabberd
5269/tcp  open  jabber   Zimbra 6 jabberd
7025/tcp  open  vmsvc-2?
7777/tcp  open  socks5   (No authentication; connection failed)
10000/tcp open  http     MiniServ 1.550 (Webmin httpd)
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port7025-TCP:V=5.51%I=7%D=7/18%Time=5006F3A2%P=x86_64-unknown-
linux-gnu
SF:%r(NULL,38,"220\x20mail\.interamerican\.edu\.ec\x20Zimbra
\x20LMTP\x20se
|
Network Distance: 1 hop
Service Info: Host:  mail.interamerican.edu.ec

OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
# Nmap done at Wed Jul 18 14:06:25 2012 -- 1 IP address (1 host
up) scanned in 146.29 seconds
```

```
# Nmap 5.51 scan initiated Tue Jul 24 12:08:34 2012 as: nmap -sN
zimbrau.txt -sU 0-65535 -sV -O [redacted]
Nmap scan report for [redacted]
Host is up (0.0013s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
53/udp    open  domain  ISC BIND 9.7.0-P1
10000/udp open  webmin  (https on TCP port 10000)
MAC Address: E4:11:5B:A9:C6:6C (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
# Nmap done at Tue Jul 24 12:26:33 2012 -- 1 IP address (1 host up)
scanned in 1079.70 seconds
```

ANEXO D (ANÁLISIS DE VULNERABILIDADES)

Contabilidad

PLUGIN ID	# OF ISSUES	PLUGIN NAME	SEVERITY
57582	1	SSL Self-Signed Certificate	Medium Severity problem(s) found
42873	1	SSL Medium Strength Cipher Suites Supported	Medium Severity problem(s) found
51192	1	SSL Certificate Cannot Be Trusted	Medium Severity problem(s) found
57608	1	SMB Signing Disabled	Medium Severity problem(s) found
26057	1	lighttpd mod_fastcgi HTTP Request Header Remote Overflow	Medium Severity problem(s) found
22964	4	Service Detection	Low Severity problem(s) found
11011	2	Microsoft Windows SMB Service Detection	Low Severity problem(s) found
24260	2	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found
10107	2	HTTP Server Type and Version	Low Severity problem(s) found
10150	1	Windows NetBIOS / SMB Remote Host Information Disclosure	Low Severity problem(s) found
20094	1	VMware Virtual Machine Detection	Low Severity problem(s) found
10287	1	Traceroute Information	Low Severity problem(s) found
25220	1	TCP/IP Timestamps Supported	Low Severity problem(s) found
51891	1	SSL Session Resume Supported	Low Severity problem(s) found
21643	1	SSL Cipher Suites Supported	Low Severity problem(s) found
10863	1	SSL Certificate Information	Low Severity problem(s) found
56984	1	SSL / TLS Versions Supported	Low Severity problem(s) found
42981	1	SSL / TLS Renegotiation DoS	Low Severity problem(s) found
35297	1	SSH Server Type and Version Information	Low Severity problem(s) found
10881	1	SSH Protocol Versions Supported	Low Severity problem(s) found

DHCP

PLUGIN ID	# OF ISSUES	PLUGIN NAME	SEVERITY
45004	2	Apache 2.2 < 2.2.15 Multiple Vulnerabilities	High Severity problem(s) found
42052	2	Apache 2.2 < 2.2.14 Multiple Vulnerabilities	High Severity problem(s) found
57603	2	Apache 2.2 < 2.2.17 APR apr_palloc Heap Overflow	High Severity problem(s) found
26928	2	SSL Weak Cipher Suites Supported	[illegible]
20007	2	SSL Version 2 (v2) Protocol Detection	[illegible]
57582	2	SSL Self-Signed Certificate	[illegible]
42873	2	SSL Medium Strength Cipher Suites Supported	[illegible]
51192	2	SSL Certificate Cannot Be Trusted	[illegible]
11213	2	HTTP TRACE / TRACK Methods Allowed	[illegible]
40467	2	Apache 2.x < 2.2.12 Multiple Vulnerabilities	[illegible]
42791	2	Apache 2.2 < 2.2.22 Multiple Vulnerabilities	[illegible]
56216	2	Apache 2.2 < 2.2.21 mod_proxy_ajp DoS	[illegible]
53896	2	Apache 2.2 < 2.2.18 APR apr_fnmatch DoS	[illegible]
50070	2	Apache 2.2 < 2.2.17 Multiple Vulnerabilities	[illegible]
48205	2	Apache 2.2 < 2.2.16 Multiple Vulnerabilities	[illegible]
33477	2	Apache < 2.2.9 Multiple Vulnerabilities (DoS, XSS)	[illegible]
22964	6	Service Detection	Info Severity problem(s) found
10107	2	HTTP Server Type and Version	Info Severity problem(s) found
21643	2	SSL Cipher Suites Supported	Info Severity problem(s) found

DVR 1

PLUGIN ID	# OF ISSUES	PLUGIN NAME	SEVERITY
10815	2	Web Server Generic XSS	Low Severity problem(s) found
22964	2	Service Detection	Low Severity problem(s) found
24260	2	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found
10107	2	HTTP Server Type and Version	Low Severity problem(s) found
10287	1	Traceroute Information	Low Severity problem(s) found
25220	1	TCP/IP Timestamps Supported	Low Severity problem(s) found
10762	1	RTSP Server Type / Version Detection	Low Severity problem(s) found
11936	1	OS Identification	Low Severity problem(s) found
19506	1	Nessus Scan Information	Low Severity problem(s) found
10114	1	ICMP Timestamp Request Remote Date Disclosure	Low Severity problem(s) found
35716	1	Ethernet Card Manufacturer Detection	Low Severity problem(s) found
54615	1	Device Type	Low Severity problem(s) found
45590	1	Common Platform Enumeration (CPE)	Low Severity problem(s) found

DVR 2

PLUGIN ID	# OF ISSUES	PLUGIN NAME	SEVERITY
10815	2	Web Server Generic XSS	Low Severity problem(s) found
22964	2	Service Detection	Low Severity problem(s) found
24260	2	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found
10107	2	HTTP Server Type and Version	Low Severity problem(s) found
10287	1	Traceroute Information	Low Severity problem(s) found
25220	1	TCP/IP Timestamps Supported	Low Severity problem(s) found
10762	1	RTSP Server Type / Version Detection	Low Severity problem(s) found
11936	1	OS Identification	Low Severity problem(s) found
19506	1	Nessus Scan Information	Low Severity problem(s) found
10114	1	ICMP Timestamp Request Remote Date Disclosure	Low Severity problem(s) found
35716	1	Ethernet Card Manufacturer Detection	Low Severity problem(s) found
54615	1	Device Type	Low Severity problem(s) found
45590	1	Common Platform Enumeration (CPE)	Low Severity problem(s) found

Hard drive 1

PLUGIN ID	# OF ISSUES	PLUGIN NAME	SEVERITY
34460	2	Obsolete Web Server Detection	High Severity problem(s) found
38832	1	XAMPP Default FTP Account	High Severity problem(s) found
42411	1	Microsoft Windows SMB Shares Unprivileged Access	High Severity problem(s) found
11213	2	HTTP TRACE / TRACK Methods Allowed	Medium Severity problem(s) found
57792	2	Apache HTTP Server httpOnly Cookie Information Disclosure	Medium Severity problem(s) found
57582	1	SSL Self-Signed Certificate	Medium Severity problem(s) found
51192	1	SSL Certificate Cannot Be Trusted	Medium Severity problem(s) found
57608	1	SMB Signing Disabled	Medium Severity problem(s) found
26919	1	Microsoft Windows SMB Guest Account Local User Access	Medium Severity problem(s) found
12218	1	mDNS Detection	Medium Severity problem(s) found
10079	1	Anonymous FTP Enabled	Low Severity problem(s) found
22964	8	Service Detection	Low Severity problem(s) found
10107	5	HTTP Server Type and Version	Low Severity problem(s) found
24260	3	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found
11424	2	WebDAV Detection	Low Severity problem(s) found
57323	2	OpenSSL Version Detection	Low Severity problem(s) found
11011	2	Microsoft Windows SMB Service Detection	Low Severity problem(s) found
10150	1	Windows NetBIOS / SMB Remote Host Information Disclosure	Low Severity problem(s) found
10287	1	Traceroute Information	Low Severity problem(s) found
25220	1	TCP/IP Timestamps Supported	Low Severity problem(s) found

Hard drive 2

PLUGIN ID	# OF ISSUES	PLUGIN NAME	SEVERITY
34460	2	Obsolete Web Server Detection	High Severity problem(s) found
10437	1	XAMPP Default FTP Account	High Severity problem(s) found
10394	1	NFS Share User Mountable	High Severity problem(s) found
42411	1	Microsoft Windows SMB Shares Unprivileged Access	High Severity problem(s) found
11213	2	HTTP TRACE / TRACK Methods Allowed	[illegible]
57792	2	Apache HTTP Server httpOnly Cookie Information Disclosure	[illegible]
51192	1	SSL Self-Signed Certificate	[illegible]
51192	1	SSL Certificate Cannot Be Trusted	[illegible]
57608	1	SMB Signing Disabled	[illegible]
42256	1	NFS Shares World Readable	[illegible]
11356	1	NFS Exported Share Information Disclosure	[illegible]
26919	1	Microsoft Windows SMB Guest Account Local User Access	[illegible]
12218	1	mDNS Detection	[illegible]
10079	1	Anonymous FTP Enabled	Low Severity problem(s) found
11111	10	RPC Services Enumeration	Low Severity problem(s) found
22964	8	Service Detection	Low Severity problem(s) found
10107	1	HTTP Server Type and Version	Low Severity problem(s) found
11424	1	WebDAV Detection	

Administrativo

PLUGIN ID	# OF ISSUES	PLUGIN NAME	SEVERITY
12218	1	mDNS Detection	[illegible]
22964	3	Service Detection	Low Severity problem(s) found
24260	2	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found
10287	1	Traceroute Information	Low Severity problem(s) found
25220	1	TCP/IP Timestamps Supported	Low Severity problem(s) found
11936	1	OS Identification	Low Severity problem(s) found
19506	1	Nessus Scan Information	[illegible]
10114	1	ICMP Timestamp Request Remote Date Disclosure	Low Severity problem(s) found
35716	1	Ethernet Card Manufacturer Detection	Low Severity problem(s) found
54615	1	Device Type	Low Severity problem(s) found
45590	1	Common Platform Enumeration (CPE)	[illegible]

Voz sobre IP

PLUGIN ID	# OF ISSUES	PLUGIN NAME	SEVERITY
11213	2	HTTP TRACE / TRACK Methods Allowed	
57792	2	Apache HTTP Server httpOnly Cookie Information Disclosure	
57582	1	SSL Self-Signed Certificate	
42873	1	SSL Medium Strength Cipher Suites Supported	
51192	1	SSL Certificate Cannot Be Trusted	
22964	8	Service Detection	Low Severity problem(s) found
11111	4	RPC Services Enumeration	Low Severity problem(s) found
24260	3	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found
11414	2	IMAP Service Banner Retrieval	Low Severity problem(s) found
10107	2	HTTP Server Type and Version	Low Severity problem(s) found
26024	2	Backported Security Patch Detection (WWW)	Low Severity problem(s) found
10302	1	Web Server robots.txt Information Disclosure	Low Severity problem(s) found
10386	1	Web Server No 404 Error Code Check	Low Severity problem(s) found
11154	1	Unknown Service Detection: Banner Retrieval	Low Severity problem(s) found
10287	1	Traceroute Information	Low Severity problem(s) found
19619	1	TFTP Daemon Detection	Low Severity problem(s) found
25220	1	TCP/IP Timestamps Supported	Low Severity problem(s) found
21643	1	SSL Session Resume Supported	Low Severity problem(s) found

Correo

PLUGIN ID	# OF ISSUES	PLUGIN NAME	SEVERITY
51192	11	SSL Certificate Cannot Be Trusted	
26928	2	SSL Weak Cipher Suites Supported	
20007	1	SSL Version 2 (v2) Protocol Detection	
57582	7	SSL Self-Signed Certificate	
42873	3	SSL Medium Strength Cipher Suites Supported	
31705	2	SSL Anonymous Cipher Suites Supported	
15901	1	DNS Server Zone Transfer Information Disclosure (AXFR)	
12217	1	DNS Server Cache Snooping Remote Information Disclosure	
22964	15	Service Detection	Low Severity problem(s) found
10863	11	SSL Certificate Information	Low Severity problem(s) found
56984	11	SSL / TLS Versions Supported	Low Severity problem(s) found
83738	6	SSL Server Accepts Weak Diffie-Hellman Keys	Low Severity problem(s) found
21643	8	SSL Cipher Suites Supported	Low Severity problem(s) found
57041	8	SSL Perfect Forward Secrecy Cipher Suites Supported	Low Severity problem(s) found
62491	6	SSL / TLS Renegotiation DoS	Low Severity problem(s) found
35372	4	XMPP Server Detection	Low Severity problem(s) found
10263	2	SMTP Server Detection	Low Severity problem(s) found
54580	3	SMTP Authentication Methods	Low Severity problem(s) found
64049	2	OpenSSL Detection	Low Severity problem(s) found
42088	2	SMTP Service STARTTLS Command Support	Low Severity problem(s) found
10185	2	POP Server Detection	Low Severity problem(s) found
22823	2	Network Camera Web Server Detection	Low Severity problem(s) found

BIBLIOGRAFIA

1. **ISECOM.** [En linea] [Citado el: 4 de Mayo de 2012.] http://www.isecom.org/

2. **Pete Herzog.** "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 185-190.

3. **Pete Herzog.** "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 38-40.

4. **Pete Herzog.** "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 105-119.

5. **Pete Herzog.** "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 120-137.

6. **Pete Herzog.** "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 138-150.

7. **Pete Herzog.** "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 151-166.

8. **Pete Herzog**, "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 167-184.

9. **Pete Herzog**, "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 37.

10. **Pete Herzog**, "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 23.

11. **Pete Herzog**, "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 24-25.

12. **Pete Herzog**, "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 28.

13. **Pete Herzog**, "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 87-94.

14. **Pete Herzog**, "Open-Source Security Testing Methodology Manual 3.1", Abril 2012, Pag 99-103.

15. **ISECOM**. [En linea] [Citado el: 8 de Mayo de 2012.] http://www.isecom.org/mirror/STAR.3.pdf

16. **Open Information System Security**. [En linea] [Citado el: 5 de Mayo de 2012.] http://www.i/oissg.org/

17. **Balwant Rathore, Mark Brunner.** "Information System Security Assesment Framework Draft 0.2.1", Abril 2012, Pag 128.

18. **BACKTRACK.** [En linea] [Citado el: 2 de Abril de 2012.] http://www.backtrack-linux.org/

19. **NMAP.** [En linea] [Citado el: 10 de Abril de 2012.] http://www.nmap.org/

20. **MCAFEE.** [En linea] [Citado el: 5 de Abril de 2012.] http://www.mcafee.com/us/downloads/free-tools/superscan.aspx

21. **UNICORNSCAN.** [En linea] [Citado el: 10 de Abril de 2012.] http://www.unicornscan.org/

22. **PORTBUNNY.** [En linea] [Citado el: 8 de Abril de 2012.] http://portbunny.recurity.com

23. **NESSUS.** [En linea] [Citado el: 12 de Abril de 2012.] http://www.tenable.com/products/nessus

24. **NEXPOSE.** [En linea] [Citado el: 3 de Abril de 2012.] http://www.rapid7.com/products/nexpose-community-edition.jsp

25. **RETINA.** [En linea] [Citado el: 8 de Abril de 2012.] http://amtsoft.com/retina/

26. **SAINT.** [En linea] [Citado el: 6 de Abril de 2012.] http://www.saintcorporation.com/

27. **Constitución del Ecuador.** [En linea] [Citado el: 21 de Abril de 2012.] http://www.montecristivive.ec/portal/index.php?option=com_docman&Itemid=61

28. **Ley de Comercio Electrónico.** [En linea] [Citado el: 6 de Abril de 2012.] http://www.conatel.gob.ec/site_conatel/index.php?view=article&catid=48%3Anormas-del-sector&id=98%3Aley-de-comercio-electronico-firmas-electronicas-y-mensajes-de-datos&tmpl=component&print=1&page=&option=com_content&Itemid=103