ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“DISEÑO Y DESARROLLO DE HACKING ÉTICO APLICADO A LA INFRAESTRUCTURA DE RED, EN UNA EMPRESA DEDICADA A LA FABRICACIÓN DE MUEBLES.”

INFORME DE MATERIA INTEGRADORA.

Previo a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

JORGE ADRIAN BAQUERO DE LA TORRE

KELVIN WILSON VÁSQUEZ BRIONES

GUAYAQUIL – ECUADOR

AÑO: 2017

AGRADECIMIENTOS

Mis más sinceros agradecimientos a todos los docentes que participaron en mi formación profesional a través de mis años de estudio en ESPOL, la exigencia académica crea profesionales preparados para la vida.

Jorge Adrián Baquero De La Torre

Mis más sinceros agradecimientos a mis padres y hermanos, que son y siempre serán el pilar fundamental en mi vida. A mis amigos y compañeros de clases, a mis profesores, por su apoyo y enseñanzas, sin ellos mi vida universitaria no hubiera sido la misma. Finalmente le agradezco a Dios por haberme puesto en el camino correcto.

Kelvin Wilson Vásquez Briones

DEDICATORIA

El presente proyecto lo dedico a mi madre, base fundamental de mi vida; por su amor, compresión, consejos y apoyo en los buenos y malos momentos. A Guissela por ser mi motivación e inspiración con cada palabra de aliento para seguir adelante.

Jorge Adrián Baquero De La Torre

Dedico este trabajo a mis abuelos, por sus enseñanzas y amor constante. A mis padres Jacinto y Brigida, porque sin su esfuerzo no sería la persona que soy hoy en día, porque sin sus locuras mi vida sería aburrida. A mis hermanas Stefanie y Viviana, por apoyarme en todo momento en todas mis decisiones.

Kelvin Wilson Vásquez Briones

TRIBUNAL DE EVALUACIÓN

Ingeniero Robert Andrade

PROFESOR EVALUADOR

Ingeniero Ronald Criollo

PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Jorge Adrián Baquero De La Torre

Kelvin Wilson Vásquez Briones

RESUMEN

El presente proyecto plantea una guía con la que se pudiera desarrollar Hacking Ético a la red de pequeñas y medianas empresas. Tomando como caso de estudio una empresa dedicada a la fabricación de muebles, la cual presenta como problemática el robo de sus diseños los cuales han sido fabricados y puesto en venta por la competencia.

Para ello se toma como referencia las etapas del Hacking Ético, las cuales son: Reconocimiento, Escaneo, Enumeración y Explotación. En cada una de estas etapas se utilizan herramientas de software con el fin de obtener información de vulnerabilidades de red que pudieran ser explotadas por alguna persona o entidad mal intencionada.

En la etapa de reconocimiento se emplea la herramienta web WhoIs y el software Maltego, con la finalidad de recaudar información sensible de la empresa de forma externa a la organización, como: correos electrónicos, números de teléfono, ubicación de la empresa e información de registro del domino.

En las etapas de escaneo y enumeración se enlista los puertos de red, usuarios, grupos y recursos compartidos inseguros a través de las herramientas OpenVas y Hyena.

En la explotación, se efectúa una intrusión a estaciones de trabajo y servidores mediante el programa Armitage, que en conjunto con Metasploit Framework generan payloads para el control remoto equipos, en esta etapa se demuestra que tan expuesta puede llegar a estar la red.

Con los resultados obtenidos se procede a realizar un plan de mitigación usando los servicios tecnológicos ya existentes en la red empresarial para evitar el hurto de datos y fallos de seguridad.

Para el plan de mitigación se implementa con reglas de correo en el servidor Exchange, políticas de firewall en el Enrutador, políticas de grupos y usuarios, políticas de actualización en un servidor WSUS y bloqueo de puertos USB.

ÍNDICE GENERAL

AGRADECIMIENTOS ii
DEDICATORIA iii
TRIBUNAL DE EVALUACIÓN iv
DECLARACIÓN EXPRESA v
RESUMEN vi
ÍNDICE GENERAL viii
ÍNDICE DE TABLAS x
ÍNDICE DE FIGURAS x
CAPÍTULO 1 12
1. GENERALIDADES 12
1.1 Antecedentes. 12
1.2 Planteamiento del problema. 13
1.4 Justificación y Alcance del Proyecto 14
1.5 Objetivos 15
1.5.1 Objetivo General 15
1.5.2 Objetivos Específicos 15
CAPITULO 2 16
2. METODOLOGÍA Y DISEÑO 16
2.1 Situación Actual 16
2.1.1 Usuarios y administradores de red 17
2.1.2 Servicios de red 17
2.1.3 Dispositivos de red 18
2.1.4 Detalle de Equipos Interconectividad 20
2.1.5 Detalle de Servidores 22
2.2 Procedimiento del Hacking 24
2.2.1 Hardware y Software para el Hacking 25
2.3 Manual Etapa de Reconocimiento. 25
2.3.1 Procedimiento a seguir en la Etapa de Reconocimiento. 26

2.4 Manual Etapas de Escaneo y Enumeración. 30
2.4.1 Procedimiento a seguir en la Etapa de Enumeración. 37
2.5 Manual Etapa de Explotación. 39
2.6 Plan de Mitigación. 50
2.6.1 Lista de GPO's a aplicar en el servidor con Active Directory. ... 50
2.6.2 Deshabilitar puertos USB en equipos que no pertenecen al dominio. 51
2.6.3 Implementación WSUS. 52
2.6.4 Establecimiento de reglas para inspeccionar correo. 54
2.6.5 Establecimiento de reglas Firewall. 55
2.7 Plan de Implementación. 57
2.8 Costos de implementación. 59
CAPÍTULO 3 61
3. RESULTADOS 61
3.1 Resultados de la Etapa de Reconocimiento 61
3.1.2 Herramienta Matlego. 62
3.2 Resultados de la Etapa de Escaneo 62
3.3 Resultados de la Etapa de Enumeración 64
3.4 Resultados de la Etapa de Explotación 65
CONCLUSIONES Y RECOMENDACIONES 66
BIBLIOGRAFÍA 68
ANEXOS 72
ANEXO A: Especificaciones técnicas de equipo IPS recomendado. 72
ANEXO B: Políticas y normas de buen uso de equipos de cómputo para pequeñas y medianas empresas. 73

ÍNDICE DE TABLAS

Tabla 2.1 Detalle de los dispositivos de la Matriz. 20

Tabla 2.2 Características de los Servidores de Red. 24

Tabla 2.3 Descripción del equipo de cómputo a utilizar. 25

Tabla 2.4 Políticas aplicadas a Grupos del Active Diretory en Windows 51

Tabla 3.1 Información del dominio 61

Tabla 3.2 Información de contacto de la empresa 62

Tabla 3.3 Datos obtenidos de OpenVAS 63

Tabla 3.4 Datos obtenidos de Hyena 64

ÍNDICE DE FIGURAS

Figura 2.1 Topología de red de la matriz de Meza y Asociados. 16
Figura 2.2 Sucursales interconectadas por VPN PPTP. 18
Figura 2.3 D-Link DSR-100N 20
Figura 2.4 Switch D-Link GS-1024D 21
Figura 2.5 Linksys E900 21
Figura 2.6 TP-Link Archer C3150 22
Figura 2.7 Aplicativos usados por la empresa. 24
Figura 2.8 Información del dominio obtenida con WhoIs. 26
Figura 2.9 Ejecución de Maltego en Kali Linux. 27
Figura 2.10 Selección de reconocimiento Footprint L1. 28
Figura 2.11 mezayasociados.xyz como objetivo del reconocimiento. 28
Figura 2.12 Vista gráfica de los elementos del dominio mezayasociados.xyz. 29
Figura 2.13 Instalación de OpenVAS en Kali Linux. 31
Figura 2.14 Se inicia la aplicación OpenVAS desde la opción openvas initial setup. 31
Figura 2.15 Contraseña de OpenVAS generada para usuario admin. 32

Figura 2.16 Verificación e iniciación del servicio OpenVAS. 32
Figura 2.17 Ingreso de credenciales de acceso al entorno de administración de OpenVAS vía web. 33
Figura 2.18 Configuraciones necesarias para la creación del objetivo. 34
Figura 2.19 Creación de tarea de escaneo en OpenVAS. 35
Figura 2.20 Selección del tipo de escaneo full and fast en la nueva tarea de OpenVAS. 35
Figura 2.21 Se inicia la tarea de escaneo seleccionando la opción Play. 36
Figura 2.22 Reporte generado en OpenVAS. 37
Figura 2.23 Menú para agregar dominio en Hyena. 38
Figura 2.24 Dominio “mezayasociados.local”. 38
Figura 2.25 Información del dominio “mezayasociados.local” obtenida en el proceso de enumeración con Hyena. 39
Figura 2.26 Selección de Matasploit Framework y ejecución del mismo por terminal. 40
Figura 2.27 Iniciando Armitage mediante el terminal y conexión al mismo... 41
Figura 2.28 Selección del tipo de Escaneo a realizar en Armitage. 42
Figura 2.29 Ingreso de objetivo a atacar en Armitage. 42
Figura 2.30 Mensaje de finalización del Escaneo y representacióngráfica del host. 43
Figura 2.31 Proceso para la búsqueda de ataques. 44
Figura 2.32 Menú contextual con posibles ataques a efectuar en Armitage. 45
Figura 2.33 Ventana emergente para el ataque al protocolo SMB. 45
Figura 2.34 Ataque exitoso, host listo para las pruebas de instrucción. 46
Figura 2.35 Ejecución del comando Screenshot en Armitage. 47
Figura 2.36 Captura de pantalla del host cliente 47
Figura 2.37 Comando Getsystem 48
Figura 2.38 Comando Hashdump 48
Figura 2.39 Comando getpid, keyscan_start, keyscan_dump y keyscan_stop en Armitage 48
Figura 2.40 Comando Webcam_snap en Armitage. 49
Figura 2.41 Control del CMD de Windows en Armitage. 49
Figura 2.42 Ventana de GPO para la cración de políticas de WSUS. 53
Figura 2.43 Establecimiento de reglas de correo mediante Exchange Server. 55
Figura 2.44 Interfaz de ingreso de reglas de firewall. 56
Figura 2.45 Configuraciones de regla de firewall. 56
Figura 2.46 Plan de Implementación 58
Figura 2.47 Estado del costo de los recursos de trabajo. 59
Figura 2.48 Distribución de costos por tipo. 60

CAPÍTULO 1

1. GENERALIDADES

1.1 Antecedentes.

En el Ecuador, el 85% de los delitos informáticos suceden por descuido de los usuarios. Según el Centro de Respuesta a Incidentes Informáticos Ecucert [1], esto se debe a que el 58% de ecuatorianos deja olvidados sus dispositivos móviles con información sensible en vehículos o lugares de trabajo, el 60% emplea la misma contraseña para dispositivos personales y laborales, el 35% abre correos electrónicos de remitentes desconocidos, el 59% guarda datos del trabajo en la nube y el 80% instala aplicaciones con la finalidad de saber quiénes visitan su perfil en redes sociales [2].

Esto ubica a Ecuador en la tercera posición en el ranking de países de Latinoamérica que sufren más ataques informáticos y entre los ocho países más vulnerables a escala mundial [3].

Una de las principales amenazas que aprovecha el descuido de los usuarios es el Ransomware. Virus desarrollado por delincuentes informáticos el cual recrea el secuestro. Este cifra y bloquea los sistemas informáticos hasta que se realice una compensación económica para su liberación [4].

Las actividades de los cibercriminales movilizan 20 veces más dinero que el narcotráfico a nivel mundial. [5]

En el ámbito empresarial se conoce que: El mayor activo de una empresa es la información. Elemento que no siempre está protegido, debido al desconocimiento de la seguridad informática por parte de los empresarios; lo que genera falta de conciencia frente al gran impacto económico que puede acarrear la vulneración informática de una organización [6].

1.2 Planteamiento del problema.

Meza y Asociados es una mediana empresa dedicada al diseño y elaboración de mobiliario de oficina. Esta organización posee 4 sucursales en Ecuador en las ciudades de Quito, Cuenca, Puyo y Daule.

Cuenta con un total de 67 empleados y su organigrama estructural se divide en las siguientes áreas: Gerencia, Administración Financiera, Diseño, Producción, Ventas y Sistemas.

Su gestión es centralizada, teniendo la supervisión de las sucursales a cargo de las áreas de Producción Y Ventas.

En la Figura 1.1 se observa el organigrama estructural de la empresa, la cual posee 3 niveles de jerarquía.

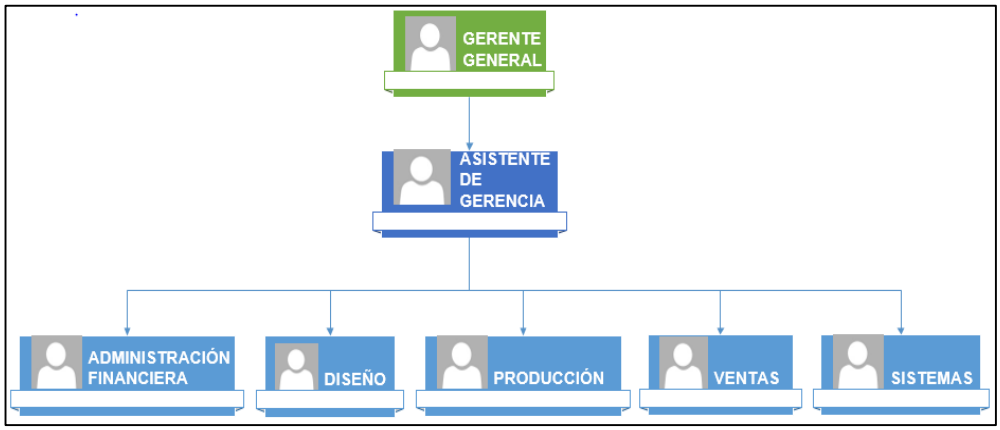


Figura 1.1 Organigrama estructural de Meza y Asociados

Meza y Asociados reporta la sustracción de archivos pertenecientes a modelos de muebles desarrollados por el área de Diseño para el catálogo 2017. Los cuales han sido producidos y puestos en venta por la competencia. Esto generó el incumplimiento de contratos y acuerdos comerciales con sus clientes, causando la pérdida de ingresos.

El robo de información no solo tiene repercusiones económicas, sino también de imagen y reputación.

1.3 Solución Propuesta

Este proyecto propone la elaboración de un manual práctico dirigido a los profesionales de TI que administran la red local de Meza y Asociados. El cual recorre las etapas del proceso de Hacking Ético para determinar el estado de la red de la empresarial de forma interna.

Mediante el uso de herramientas de Hacking se recopila información de vulnerabilidades de red y se realizan pruebas de intrusión. Posteriormente se realiza un plan mitigación para dichas amenazas. Manteniendo una red segura contra posibles ataques informáticos de personas mal intencionadas.

1.4 Justificación y Alcance del Proyecto

Este proyecto permite simplificar una auditoría informática en pasos que cualquier administrador de red sin conocimientos amplios en seguridad informática puede seguir.

Esto resuelve la necesidad de contratar a organizaciones de terceros para la detección de huecos de seguridad, aportando en la reducción de gastos en Meza y Asociados.

El proyecto se desarrolla en la red de área local de la matriz, ya que en ella se contienen todos los servicios utilizados por la organización.

1.5 Objetivos

1.5.1 Objetivo General

Plantear una guía con la que se pueda desarrollar Hacking Ético a la red de Meza y Asociados.

1.5.2 Objetivos Específicos

- Determinar el número de puertos abiertos vulnerables de los servicios de red.
- Determinar la cantidad de estaciones de trabajo que poseen puertos abiertos.
- Elaborar un plan para la realización de pruebas de intrusión y así mostrar las vulnerabilidades actuales y futuras.
- Elaborar un plan de contingencias para la prevención de pérdida de datos.

CAPITULO 2

2. METODOLOGÍA Y DISEÑO

2.1 Situación Actual

Según la información suministrada por el cliente, la red de área local de la matriz no ha sido sujeta a ningún procedimiento de Hacking Ético para la detección en el fallo de seguridades.

Usuarios y estaciones de trabajo no están regidos por políticas de seguridad; y los equipos de conmutación y enrutamiento solo poseen las configuraciones básicas. En la figura 2.1 se muestra el diagrama de red de la matriz donde se observa sus servidores, estaciones de trabajo, equipos de interconectividad y puntos de acceso inalámbrico.

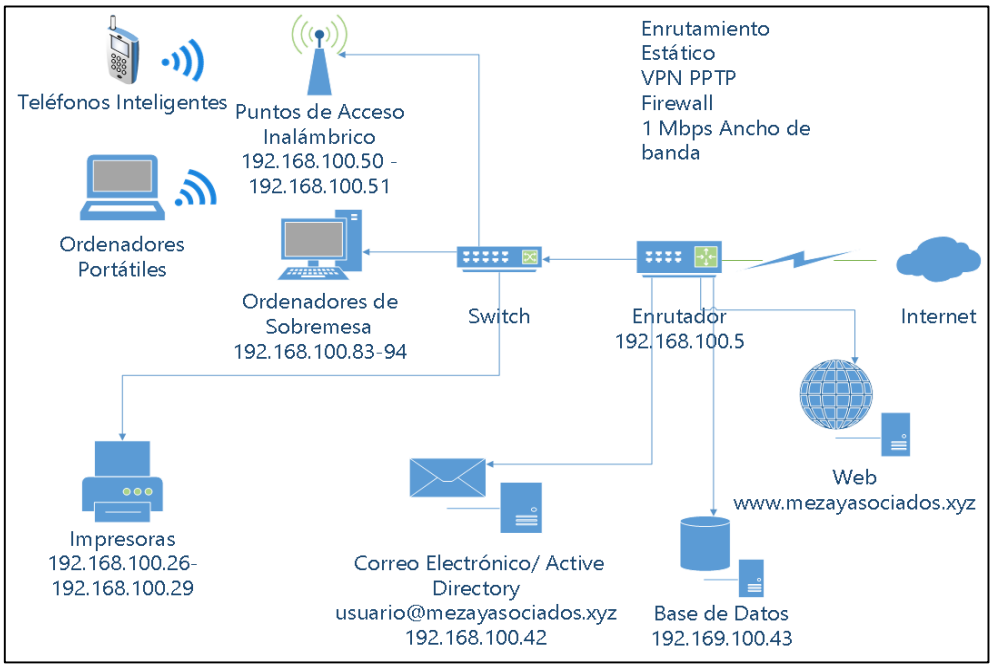


Figura 2.1 Topología de red de la matriz de Meza y Asociados.

2.1.1 Usuarios y administradores de red

El jefe del área de Sistemas de Meza y Asociados, empleado directo que labora a tiempo completo en la compañía; es el encargado del correcto funcionamiento y mantenimiento de todos los equipos de red y cómputo tanto a nivel de hardware como de software. Es especializado en desarrollo de software y con conocimiento básico de redes.

Los usuarios tienen control total de las estaciones de trabajo y no existen restricciones de instalación de programas.

2.1.2 Servicios de red

Los trabajadores de Meza y Asociados cuentan con servicios de correo electrónico empresarial, sitio web, directorio activo y base de datos. Estos servicios se encuentran implementados en servidores dentro de la matriz.

La empresa tiene conexión a internet dedicado con una capacidad de 3 Mbps con los cuales se interconectan la matriz y sus sucursales a través de una Virtual Private Network - VPN utilizando el protocolo Point to Point Tunneling Protocol - PPTP [7], ambas implementaciones fueron realizadas por el ISP.

En la Figura 2.2 se muestra el diagrama de la conexión de la matriz con la demás sucursales.

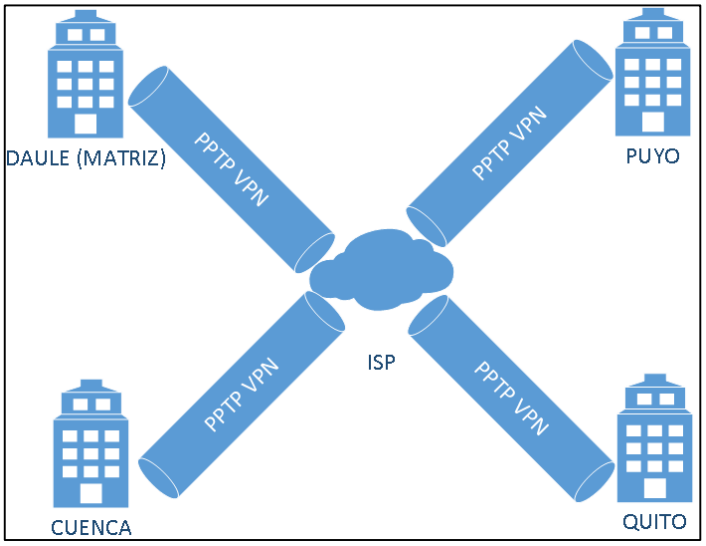


Figura 2.2 Sucursales interconectadas por VPN PPTP.

2.1.3 Dispositivos de red

La matriz cuenta con 17 estaciones de trabajo, las cuales tienen instalados sistemas operativos pertenecientes a la familia Microsoft Windows. Las versiones de los mismos son: XP, 7, 8 y 10.

Se encuentran unidas al dominio local para la administración mediante el directorio activo, el cual se utiliza para el fondo de escritorio institucional en los ordenadores e instalación de programas con formato .exe y .msi.

El hardware mínimo encontrado en las estaciones de trabajo fue de 2 GB de RAM, procesador Intel Core 2 Quad 2.66 Ghz y 500 GB de Disco Duro. Mientras que el hardware máximo encontrado fue de 8 GB de RAM, procesador Intel Core i7 3.4 Ghz y 1 TB de Disco Duro.

En las instalaciones se cuenta con dos puntos de acceso inalámbrico, el primero un Linksys E900 dedicado solo para el área gerencial. Y el

segundo un TP-Link Archer C3150 para el resto de departamentos; en ambos puntos de acceso se conectan ordenadores y celulares tanto de la empresa como personales de los empleados.

Se cuenta con dos impresoras de red, RICOH Aficio MP 2500 y RICOH Aficio MP201SPF habilitadas para todos los departamentos.

Todos estos dispositivos se conectan a través de un Switch D-Link GS-1024D, el cual no tiene VLANs configuradas. Este a su vez se conecta con un Router D-Link DSR-1000N de servicios integrados junto con los servidores de Base de Datos, Web y Correo electrónico. El detalle los dispositivos se presenta en la tabla 2.1 con sus respectivas direcciones IPs.

Marca	**Modelo**	**Descripción**	**Dirección IP Privada**	**Dirección IP Pública**
D-Link	DSR-1000N	Router	192.168.100.5	50.63.202.41
D-Link	DGS-1024D	Switch de 24 puertos	N/A	
RICOH	Aficio MP 2500	Impresora de red	192.168.100.26	
RICOH	Aficio MP201SPF	Impresora de red	192.168.100.29	
N/A	N/A	Servidor de Correo	192.168.100.42	
NA	NA	Servidor de Base de Datos	192.168.100.43	
NA	NA	Servidor Web	N/A	50.63.202.42
TP-Link	Archer C3150	Punto de Acceso Inalámbrico 1	192.168.100.50	

CISCO	E900	Punto de Acceso Inalámbrico 2	192.168.100.51	
N/A	N/A	PC de Escritorio 1 - 12	192.168.100.83 - 192.168.100.94	
N/A	N/A	Laptop 1 - 5	DHCP	

Tabla 2.1 Detalle de los dispositivos de la Matriz.

2.1.4 Detalle de Equipos Interconectividad

El cableado que utiliza la compañía es UTP de categoría 5e, utiliza una topología estrella. A continuación, se mencionan los equipos de interconectividad que posee Meza y Asociados.

Enrutador D-Link DSR-1000N

La figura 2.3 muestra el equipo provee la conexión a internet por medio del ISP, el servicio PPTP y conexión a los servidores. El detalle de las especificaciones técnicas se muestra en la referencia [8].

Figura 2.3 D-Link DSR-100N

Switch D-Link GS-1024D

La figura 2.4 muestra el Switch que permite la interconexión de los equipos finales. Sus características se detallan en la referencia [9].

Figura 2.4 Switch D-Link GS-1024D

Linksys E900

Punto de acceso inalámbrico exclusivo para uso gerencial como se observa en la Figura 2.5. Detalles en referencia [10].

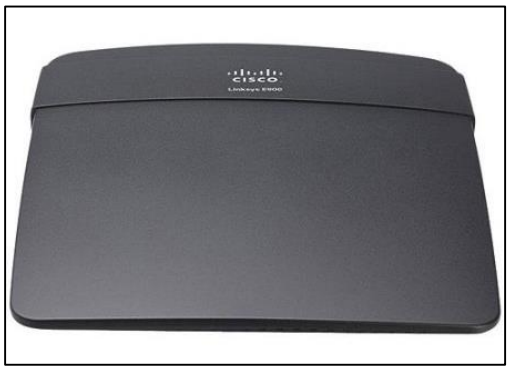


Figura 2.5 Linksys E900

TP-Link Archer C3150

Este equipo, como se ve en la Figura 2.6, es utilizado por todos los empleados de la matriz. Su detalle técnico se presenta en la siguiente referencia [11].

Figura 2.6 TP-Link Archer C3150

2.1.5 Detalle de Servidores

Servidor de Correo

El servidor de correo esta implementado en un ordenador con la dirección 192.680.100.42. Posee el Sistema Operativo Windows Server 2008 R2, ejecutando el aplicativo Microsoft Exchange 2013 [12], administra 57 cuentas de correo con el siguiente formato: usuario@mezayasociados.xyz. Su hardware está conformado por un procesador Intel Xeon E5-2630V4 2.20GHz, 12 GB RAM, 6TB de Disco Duro y 1000 Mbps adaptador de red Gigabit Ethernet.

Servidor de Base de Datos

El servidor de base de datos posee las siguientes características de hardware: Un procesador Intel Xeon E5-2630V4 2.20GHz, 16 GB RAM, 4 TB Disco Duro y 1000 Mbps adaptador de red Gigabit Ethernet. Su sistema operativo es Windows Server 2012 y el motor de base de datos es MySql [13]. La base de datos interactúa con el sistema de

información gerencial Enterprise Resource Planning ERP [14] de la empresa, que es un programa desarrollado en Java que controla información financiera y administrativa de la compañía. Su dirección IP asignada es la 192.168.100.43.

Servidor Web

El servidor Web utiliza la aplicación Apache 2.2 [15] bajo el sistema operativo Windows Server 2008 R2, su dirección IP pública es la 50.63.202.42. En cuanto a su hardware tenemos que el procesador es un Intel Xeon E5 v4 E5-2603V4 de 1.7 Ghz, 4 GM de memoria RAM y un disco duro de 500 GB.

En la Tabla 2.2 se puede visualizar las características de los servidores utilizados por Meza y Asociados; y en la Figura 2.7 se visualiza los logos de las aplicaciones usadas en los servidores.

	IP	**Sistema Operativo**	**Aplicación**	**Hardware**
Correo y Directorio Activo	192.680.100.42	Windows Server 2008 R2	Microsoft Exchange 2013 Active Directory	Intel Xeon E5-2630V4 2.20GHz, 12 GB RAM, 6TB DD, 1000 Mbps.
Base de Datos	192.680.100.43	Windows Server 2012 R2	MySQL	Intel Xeon E5-2630V4

				2.20GHz, 16 GB RAM, 4 TB DD, 1000 Mbps.
Web	50.63.202.42	Windows Server 2008 R2	Apache 2.2	Intel Xeon E5 v4 E5-2603V4 1.7GHz, 4 GB RAM, 500 GB DD, 1000 Mbps.

Tabla 2.1 Características de los Servidores de Red.

Figura 2.7 Aplicativos usados por la empresa.

2.2 Procedimiento del Hacking

En la auditoria se utiliza la modalidad de grey box Hacking [16], en la cual la empresa nos brindará información parcial como las direcciones IP y servicios principales que se tiene. Esta modalidad da paso a dos enfoques de Hacking: el externo y el interno; es decir la empresa vista desde internet y también observada desde el entorno de red local.

2.2.1 Hardware y Software para el Hacking

Se usó un ordenador portátil con las siguientes características de hardware: procesador Intel Core i5-3210M 2.50 GHz TB 3.1GHz, 8 GB de Memoria RAM DDR3, Disco Duro de 750 GB, como se aprecia en la tabla 2.3. En él tendremos dos sistemas operativos en modo de doble booteo. Windows 10 1511 Compilación 10586.753 [17] y Kali Linux 2017.1 [18] para la ejecución de las herramientas de Hacking OpenSocurce [19] y Freeware [20].

Equipo	**Hardware**	**Sistema Operativo**
Portátil Sony VAIO SVE14A27CLS	-Intel Core i5-3210M 2.50 GHz TB 3.1GHz -8 GB de Memoria RAM DDR3 -Disco Duro de 750 GB.	-Windows 10 1511 Compilación 10586.753 -Kali Linux 2017.1

Tabla 2.2 Descripción del equipo de cómputo a utilizar.

2.3 Manual Etapa de Reconocimiento.

Esta primera fase de la auditoría tiene el propósito de obtener la mayor cantidad de información posible de la empresa, misma que sea relevante y nos proporcione de datos sensibles explotables para un posible ataque.

Para una recolección de datos efectiva utilizamos el método de recolección pasivo. Durante esta etapa no contamos con acceso a las instalaciones físicas de la empresa. El propósito es explotar la información de la empresa disponible en internet de forma pública.

2.3.1 Procedimiento a seguir en la Etapa de Reconocimiento.

Reconocimiento con Herramienta WhoIs.

1. Como primer paso en esta etapa se recolecta información general de la organización, esto se logra con la herramienta web WhoIs [21]; para ello se accede mediante cualquier navegador al sitio web https://www.whois.com/whois/ con el objetivo de consultar la información del dominio.

2. Luego en el recuadro de búsqueda se ingresa el nombre de dominio de la empresa, en este caso mezayasociados.xyz.

3. La Figura 2.8 muestra el resultado obtenido bajo la búsqueda del dominio mezayasociados.xyz. Este reporte detalla nombres de los servidores, direcciones IP de dominio, representantes de la empresa, la dirección de la matriz, código postal, fecha de registro de dominio, así como la de expiración de dominio.

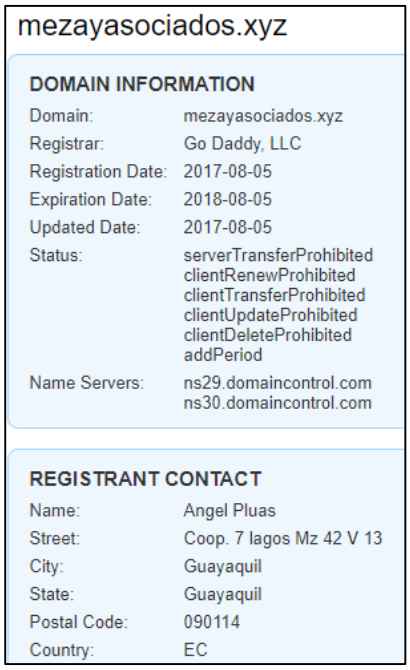


Figura 2.8 Información del dominio obtenida con WhoIs.

Reconocimiento con Maltego.

1. Se usa la herramienta Maltego [22] que se ejecuta bajo el sistema operativo Kali Linux. El objetivo de esta aplicación es recopilar información del dominio, pero de una forma un poco más interactiva ya que la misma cuenta con una interfaz gráfica bastante intuitiva. En la Figura 2.9 se observa el método de ejecución de maltego, para ello nos dirigimos al menú Applications, Information Gathering y luego seleccionamos la opción maltegoce.

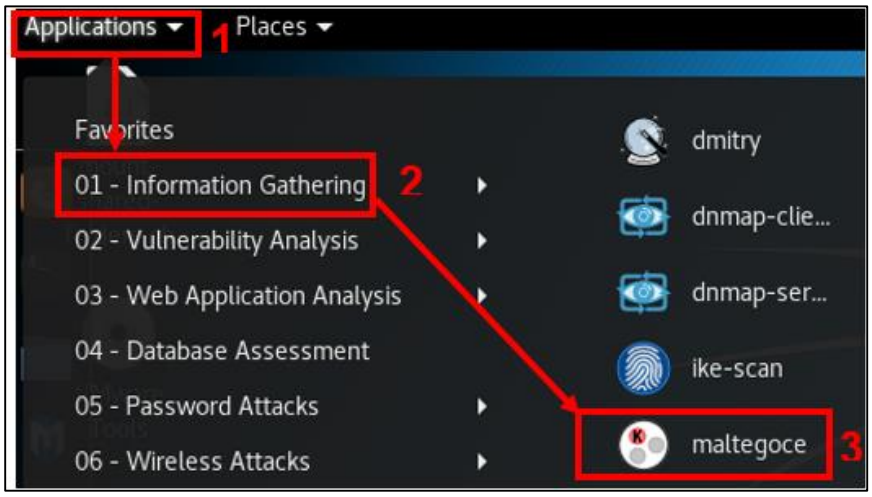


Figura 2.9 Ejecución de Maltego en Kali Linux.

2. Una vez iniciado el programa, se procede a realizar la creación de una cuenta maltego mediante el registro por correo electrónico.

3. Se escoge el tipo de reconocimiento deseado, en este caso Footprint L1 como se aprecia en la Figura 2.10. El reconocimiento nivel uno implica la detección de dispositivos de red, componentes de infraestructura y locaciones de red de una forma básica y rápida.

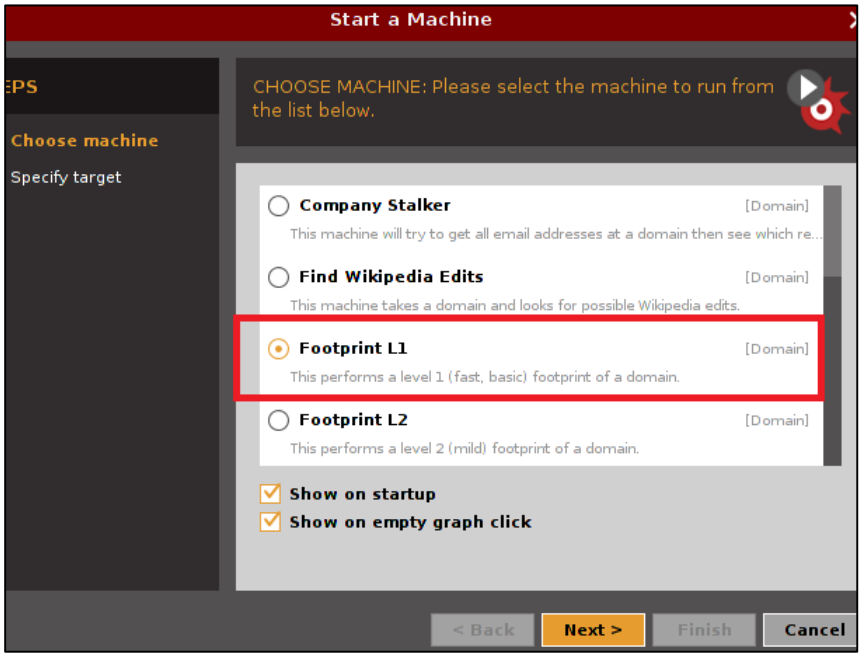


Figura 2.10 Selección de reconocimiento Footprint L1.

4. Se especifica el objetivo del reconocimiento, para esto se agrega el nombre de dominio de la empresa, como se observa en la Figura 2.11.

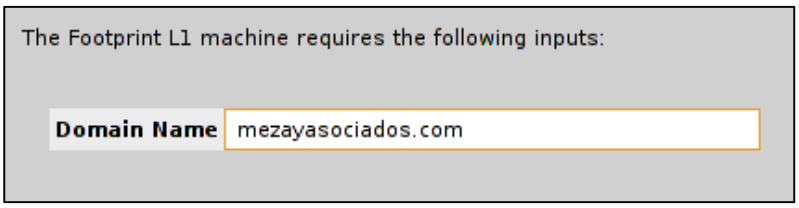


Figura 2.11 mezayasociados.xyz como objetivo del reconocimiento.

5. A continuación, se crea una vista gráfica de los elementos pertenecientes al dominio, ofreciendo información detallada de la infraestructura de red y servidores de la empresa.

Como se visualiza en la Figura 2.13. Los elementos mostrados son el nombre del dominio, servidores DNS [23] asociados, adaptadores de red asociados al servidor de dominio, rango de direcciones IP, número de sistema autónomo al que pertenece el dominio y nombre del ISP.

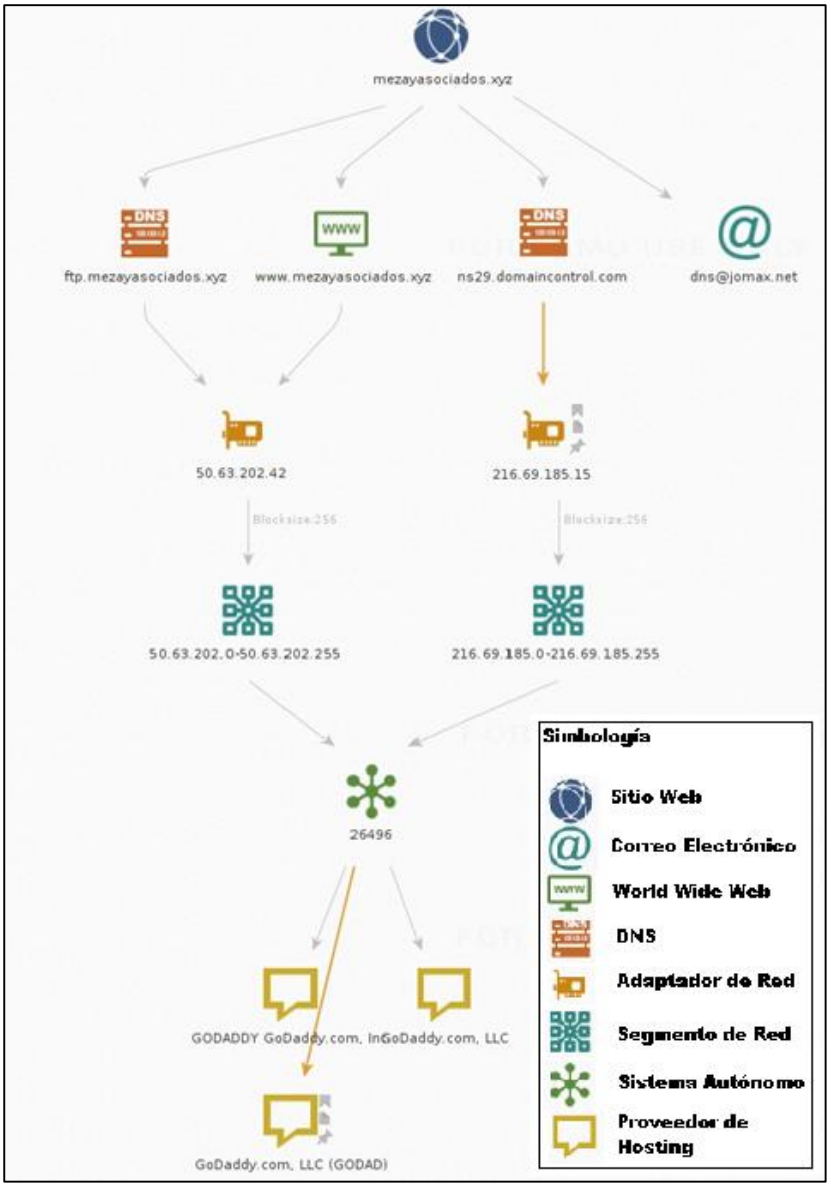


Figura 2.12 Vista gráfica de los elementos del dominio mezayasociados.xyz, generado por la aplicación Maltego.

2.4 Manual Etapas de Escaneo y Enumeración.

En esta fase de la auditoría se empezó a trabajar con la información obtenida en la etapa de reconocimiento e información parcial proporcionada por la empresa como se ha mencionado en párrafos previos.

El objetivo de la fase de escaneo es detectar aquellos puertos abiertos presentes en los equipos que forman parte de la red, en base a esto se puede establecer qué tipos de sistemas operativos existen en la empresa; así como los servicios que se están ejecutando a través de dichos puertos.

El paso posterior al escaneo es la enumeración, cuyo objetivo es realizar un escaneo profundo de las vulnerabilidades en los equipos, para obtener información como: cuentas de usuarios, grupos, recursos, procesos y servicios.

2.4.1 Procedimiento a seguir en la Etapa de Escaneo.

Durante esta etapa, así como en la etapa de enumeración se realiza la auditoría de forma interna, las mismas son etapas previas a la intrusión y permiten determinar qué tipos de Exploits [24] se van a utilizar de acuerdo a las vulnerabilidades encontradas.

Escaneo con OpenVAS.

1. OpenVAS [25] no se encuentra preinstalado en Kali Linux, motivo por el cual es necesario realizar la instalación desde una ventana de terminal, con el comando: **sudo apt-get install openvas**. Como se observa en la Figura 2.13.

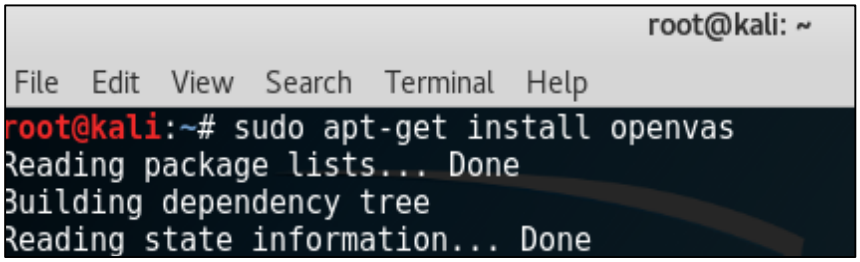


Figura 2.13 Instalación de OpenVAS en Kali Linux.

2. Una vez culminada la instalación se inicia la aplicación desde la opción “openVAS initial setup” ubicada en el menú Applications, Vulnerability Analysis. Como se muestra en la Figura 2.14.

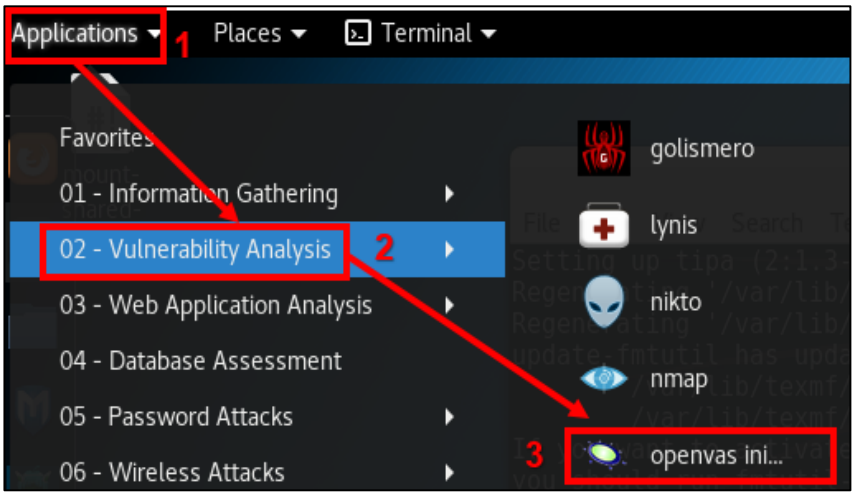


Figura 2.14 Se inicia la aplicación OpenVAS desde la opción openvas initial setup.

3. Luego de iniciar la aplicación se genera una contraseña por defecto para el usuario *admin*, que es el usuario administrador predeterminado. Como se muestra en la Figura 2.15 se ha generado una contraseña de forma aleatoria. Estas credenciales

serán necesarias para acceder al servicio de administración de openVAS desde el navegador web.

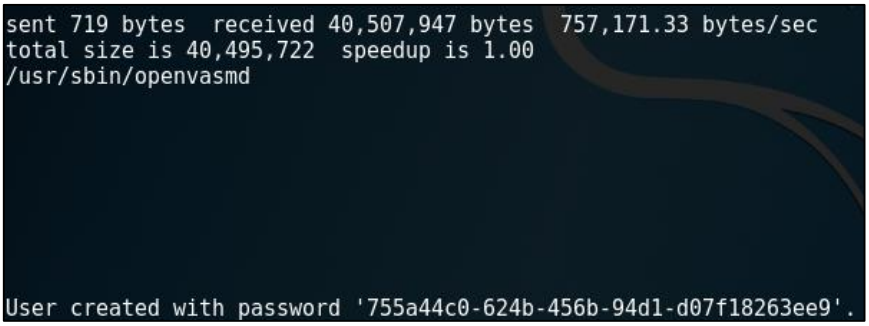


Figura 2.15 Contraseña de OpenVAS generada para usuario admin.

4. Se verifica que los servicios de openVAS estén levantados con el comando; netstat -antp, y se inicia el servicio con el comando: openvas-start. Como se visualiza en la Figura 2.16.

Figura 2.16 Verificación e iniciación del servicio OpenVAS.

5. Desde el navegador web se accede al entorno de administración ingresando a la dirección 127.0.0.1:9392, con el usuario admin y la contraseña asignada en el paso previo. Como se muestra en la Figura 2.17.

Figura 2.17 Ingreso de credenciales de acceso al entorno de administración de OpenVAS vía web.

6. Como paso inicial del análisis en OpenVAS, se crea un objetivo. Esto se logra desde la opción Targets en el menú Configuration seleccionando el símbolo en forma de estrella.

7. Posteriormente se Ingresa el nombre de la tarea y el nombre de dominio de la empresa, en la sección de PortList.

Determinamos que tipos de puertos deseamos escanear de dicho objetivo, en nuestro caso particular deseamos escanear todos los puertos UDP y TCP.

Finalmente damos clic en la opción “Create” para generar el objetivo, en la Figura 2.18 se pueden observar dichas configuraciones.

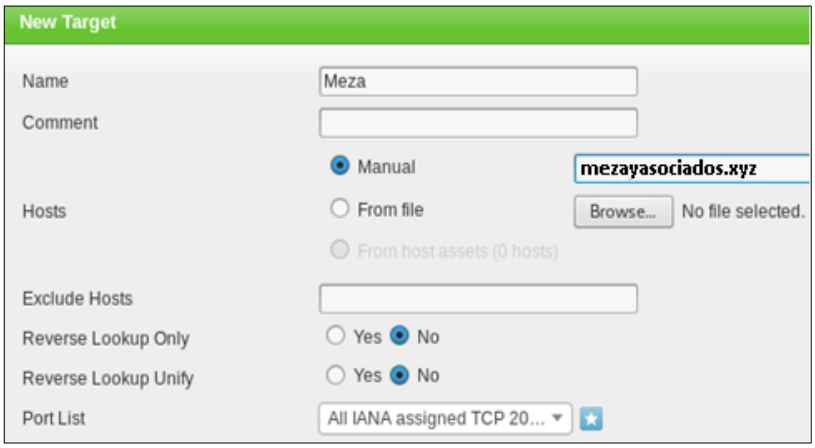


Figura 2.18 Configuraciones necesarias para la creación del objetivo.

8. Luego de crear el objetivo, se procede a crear la tarea de análisis desde la opción Scans, para posteriormente seleccionar la pestaña Tasks; luego se da clic en crear una nueva tarea en el ícono en forma de estrella.

9. La Figura 2.19 muestra la ventana emergente de la creación de una nueva tarea, a la cual se le asigna el objetivo creado en el paso previo.

Se puede asignar alertas, horarios programados y un nivel de severidad para las amenazas que se deseen detectar, en este caso particular se lo configura en un 70%.

Lo que indica que se busca puertos vulnerables que sean explotables.

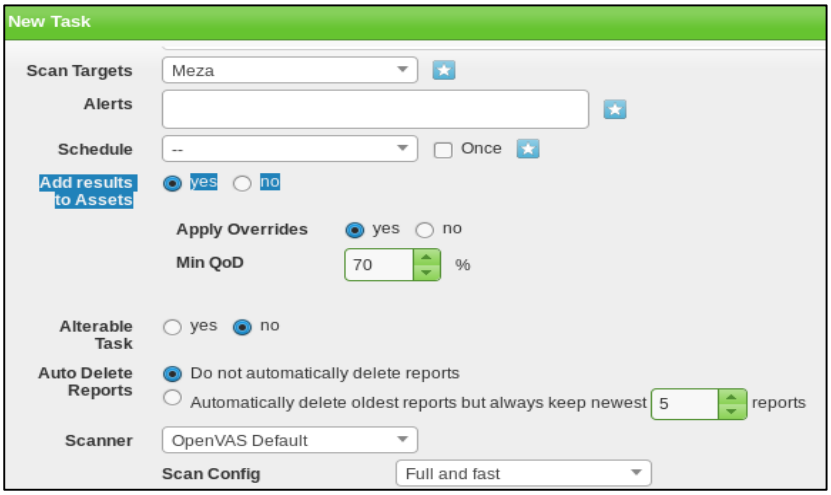


Figura 2.19 Creación de tarea de escaneo en OpenVAS.

10. Dentro de la pantalla New Task, seleccionamos la cantidad de hosts a los que se desea realizar el escaneo, así como el tipo de escaneo en este caso “Full and fast”, que genera un tráfico mínimo en la red empresarial; sin afectar a los demás servicios. Véase Figura 2.20.

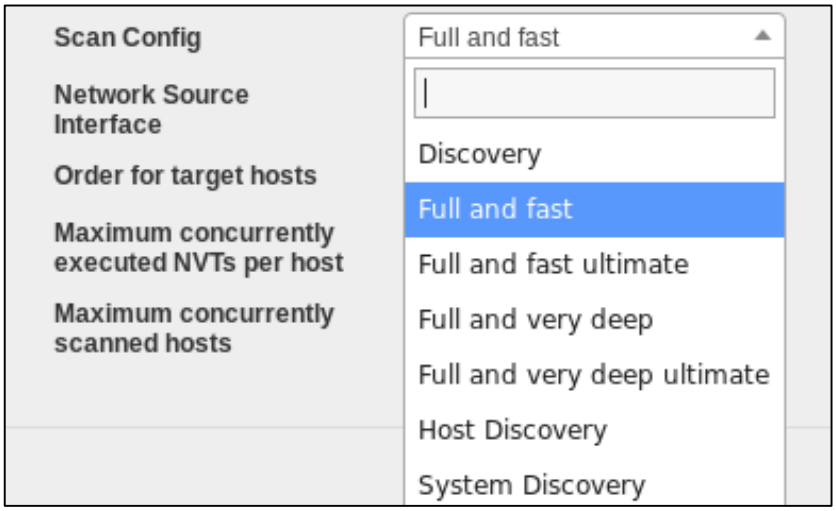


Figura 2.20 Selección del tipo de escaneo full and fast en la nueva tarea de OpenVAS.

11. Luego de crear la tarea, se inicia la misma dando clic en el botón play, como se muestra en la Figura 2.21.

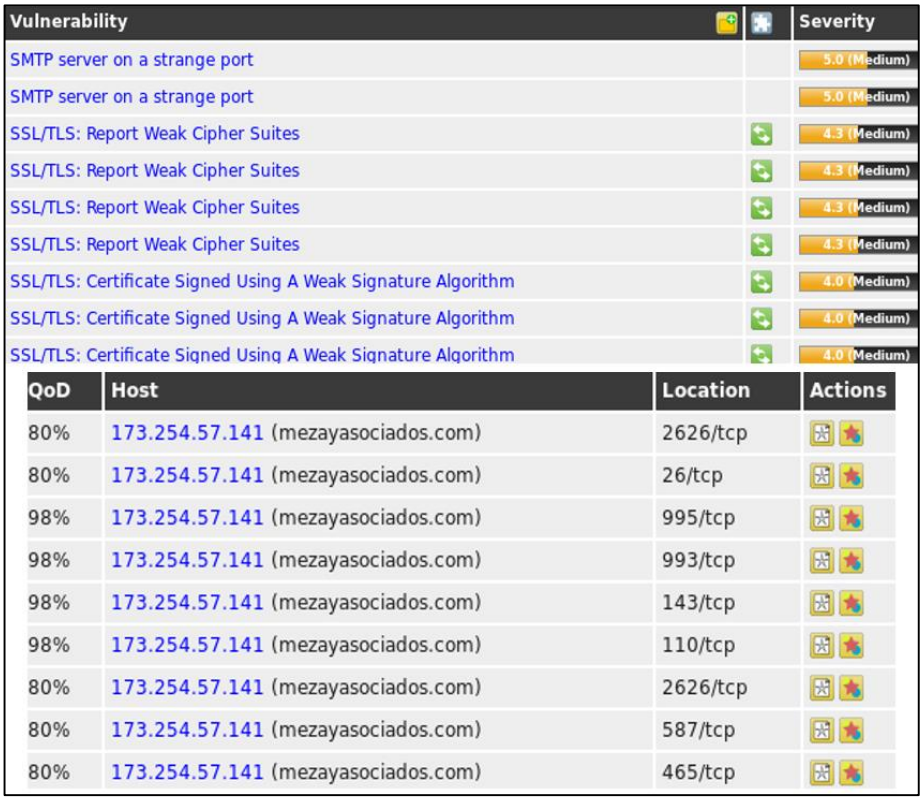
Figura 2.21 Se inicia la tarea de escaneo seleccionando la opción Play.

12. El paso final de este procedimiento es generar el reporte del escaneo realizado, mismo que puede obtenerse desde la opción Scans en la pestaña Reports.

En la Figura 2.22 se observa un reporte generado por OpenVAS en donde se muestran distintas vulnerabilidades, su nivel de severidad, nivel de explotación de dichas vulnerabilidades, el host correspondiente a la vulnerabilidad y el número de puerto.

El nivel de severidad se representa con 3 colores por nivel de severidad. Rojo es crítico, indica que se deben realizar correcciones inmediatas; Naranja indica un nivel de severidad media; y el verde indica que no se ha encontrado ningún hueco o fallo de seguridad.

En la sección de Actions, nos muestra las posibles soluciones que podemos tomar para mitigar fallos de seguridad encontrados en el reporte.



Vulnerability	Severity
SMTP server on a strange port	5.0 (Medium)
SMTP server on a strange port	5.0 (Medium)
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)

QoD	Host	Location	Actions
80%	173.254.57.141 (mezayasociados.com)	2626/tcp	
80%	173.254.57.141 (mezayasociados.com)	26/tcp	
98%	173.254.57.141 (mezayasociados.com)	995/tcp	
98%	173.254.57.141 (mezayasociados.com)	993/tcp	
98%	173.254.57.141 (mezayasociados.com)	143/tcp	
98%	173.254.57.141 (mezayasociados.com)	110/tcp	
80%	173.254.57.141 (mezayasociados.com)	2626/tcp	
80%	173.254.57.141 (mezayasociados.com)	587/tcp	
80%	173.254.57.141 (mezayasociados.com)	465/tcp	

Figura 2.22 Reporte generado en OpenVAS.

2.4.2 Procedimiento a seguir en la Etapa de Enumeración.

En esta etapa, es necesaria la instalación de la herramienta Hyena en un equipo con sistema operativo Windows; mismo que debe estar conectado a la red local y ser parte del dominio. Se puede descargar Hyena de forma gratuita por 30 días desde el sitio web del desarrollador Somarsoft. [40]

Enumeración con Hyena.

1. Como primer paso se debe iniciar la aplicación dando doble clic sobre el acceso directo creado luego de la instalación de Hyena.

2. Luego de iniciado el programa, se agrega el dominio desde la opción Archivo, se selecciona “Agregar dominio”, como se muestra en la Figura 2.23.

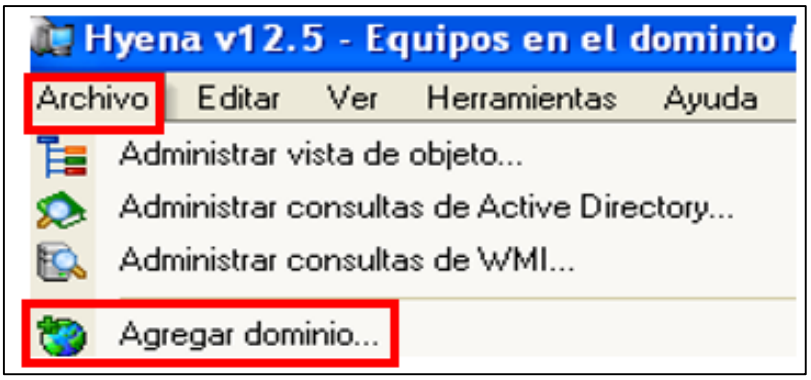


Figura 2.23 Menú para agregar dominio en Hyena.

3. Se da clic en el ícono de la lupa para realizar la búsqueda, y una vez detectado el nombre del dominio de la empresa se lo selecciona y se presiona aceptar.

4. En la Figura 2.24 se observa el nombre de dominio de la empresa Meza y Asociados luego de ser seleccionado en la búsqueda.

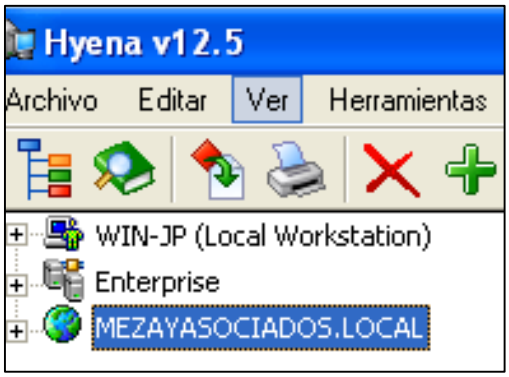


Figura 2.24 Dominio “mezayasociados.local”.

5. Una vez agregado el dominio se verifica el contenido de nombres de usuarios, nombres de equipos, nombres de servidores y grupos. En la Figura 2.25 se observa un menú desplegable el cual contiene información obtenida del directorio activo mezayasociados.local.

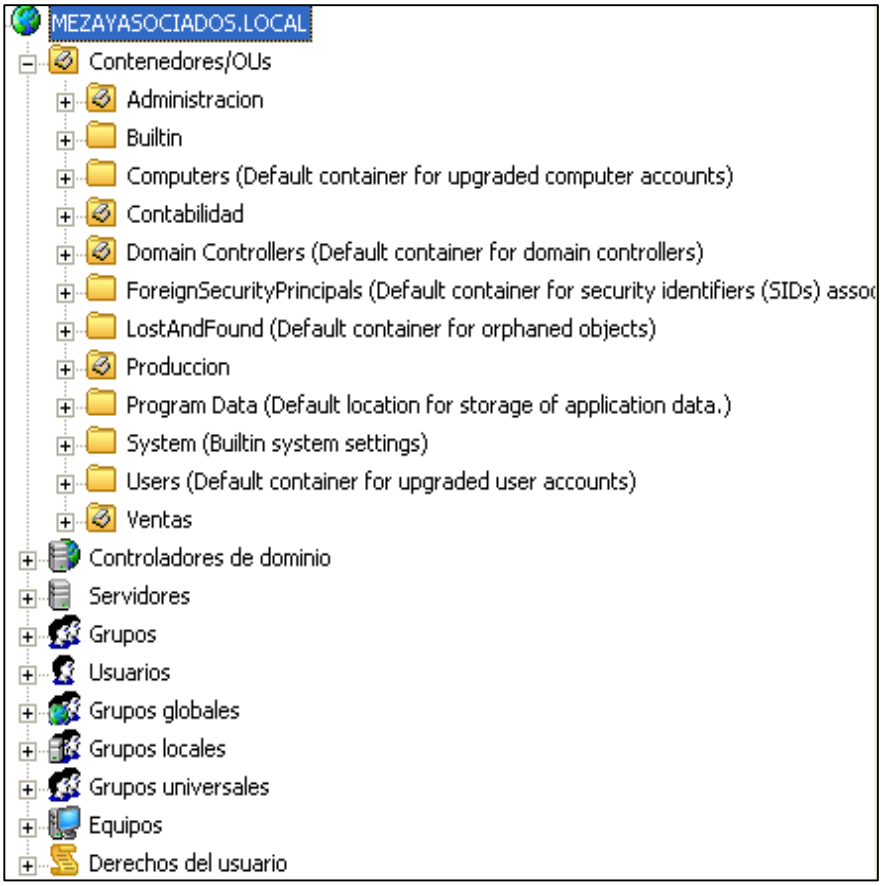


Figura 2.25 Información del dominio “mezayasociados.local” obtenida en el proceso de enumeración con Hyena.

2.5 Manual Etapa de Explotación.

En esta fase se utiliza frameworks de explotación, que son un grupo de herramientas que permiten realizar actividades de reconocimiento, escaneo, análisis de vulnerabilidades y Hacking bajo una interfaz única [26].

Proceso de explotación con Armitage

1. Se Inicia MSF (Metasploit Framework) en Kali Linux. Para ello se seleciona el menú Applications, luego el submenú Exploitation Tools y por último se da clic en Metasploit framework como se muestra en la Figura 2.26, al seleccionar el aplicativo se ejecuta una ventana en el terminal que inicializa el framework.

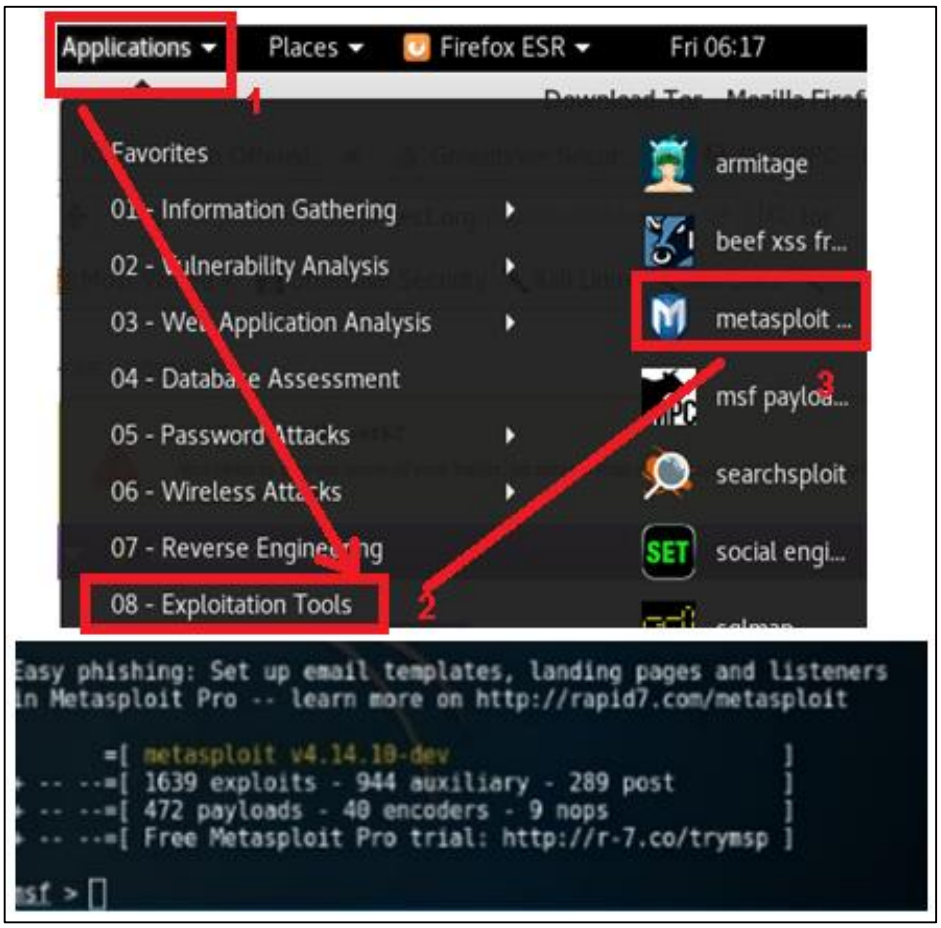


Figura 2.26 Selección de Matasploit Framework y ejecución del mismo por terminal.

2. Para la administración de Metasploit Framework se tienen 3 interfaces que se ajustan al gusto del atacante, estas son: msfconsole, Web (versión de Community) y Armitage. Para el caso práctico se utiliza

Armitage, que es una interfaz gráfica del framework que permite visualizar objetivos, recomiendar exploits para cada objetivo y muestra un conjunto de herramientas para la post-explotación [27].

Para iniciar Armitage tenemos tres formas, la primera es mediante un terminal en modo root (administrador), se ejecuta el comando armitage, como se observa en la figura 2.27. La segunda opción es en el menú Applications, luego al submenú Exploitation Tools para finalizar se da clic izquierdo en Armitage; y la tercera es en el ícono que se encuentra en el panel lateral izquierdo del escritorio.

Posteriormente se visualiza una ventana de conexión con parámetros de Host, puerto, usuario y contraseña predeterminados, le damos clic a Connect para iniciar.

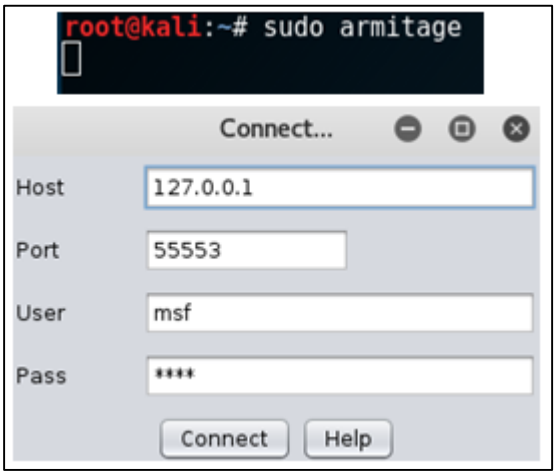


Figura 2.27 Iniciando Armitage mediante el terminal y conexión al mismo.

3. Como se observa en la Figura 2.28, se procede al escaneo y ataque desde Armitage. Se establece el objetivo, en este caso una estación de trabajo de Meza y Asociados. Luego se selecciona el Menú Host y Nmap

Scan, donde se visualiza distintas opciones de escaneo de puertos, se escoge Intensive Scan, el cual realiza un escaneo profundo del host objetivo.

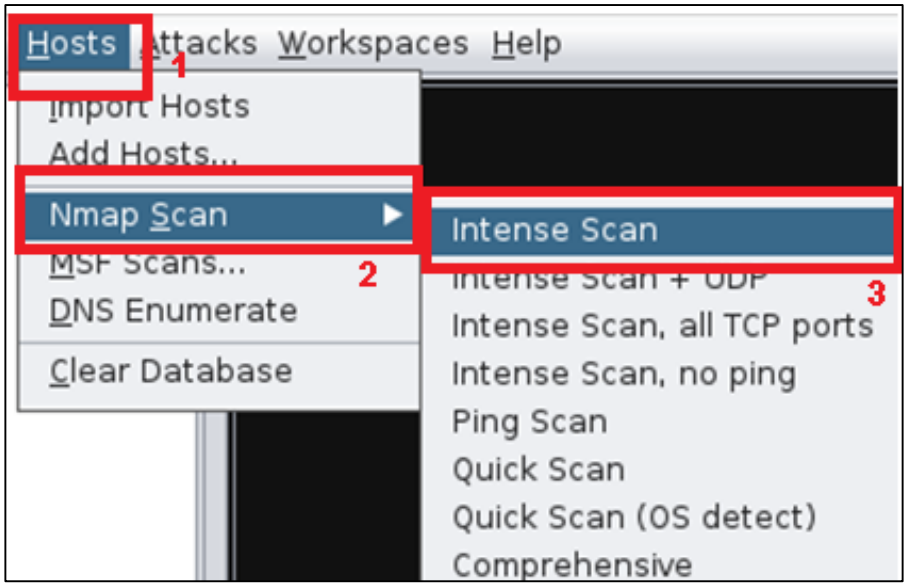


Figura 2.28 Selección del tipo de Escaneo a realizar en Armitage.

4. Aparece una ventana emergente donde se coloca la dirección IP del host objetivo, luego presionamos el botón Ok, como se aprecia en la Figura 2.29. También se puede especificar rangos de direcciones IP para realizar el escaneo a varios objetivos de forma simultánea.

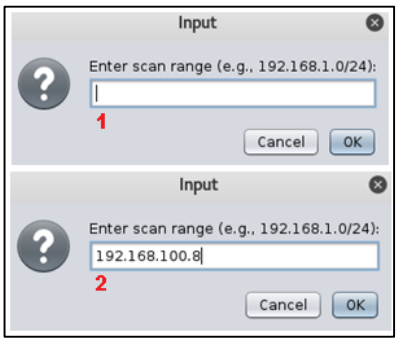


Figura 2.29 Ingreso de objetivo a atacar en Armitage.

5. Metasploit Framework a través de Armitage realiza un escaneo profundo de todos los servicios TCP y UDP; detectando el sistema operativo del host, puertos abiertos, servicios en ejecución y aplicaciones en escucha. La Figura 2.30 muestra el mensaje del escaneo completado, sugiriéndonos el siguiente paso a realizar; que es la búsqueda de ataques. Automáticamente se genera el objeto, a modo de ícono de un monitor con el logo del sistema operativo correspondiente a la estación de trabajo escaneado.

Figura 2.30 Mensaje de finalización del Escaneo y representacióngráfica del host.

6. En la Figura 2.31 se observa la búsqueda de ataques en Armitage. Para ello, se selecciona el ícono host, luego el menú Attacks, Find Attacks. Hecho esto, el Famework relaciona los ataques de su base de datos con el sistema operativo y servicios detectados en el paso anterior. Luego de esto aparece una ventana con el proceso de búsqueda de ataques, el cual finaliza con otra ventana emergente que nos indica que se ha generado una lista de exploits adecuados para el host.

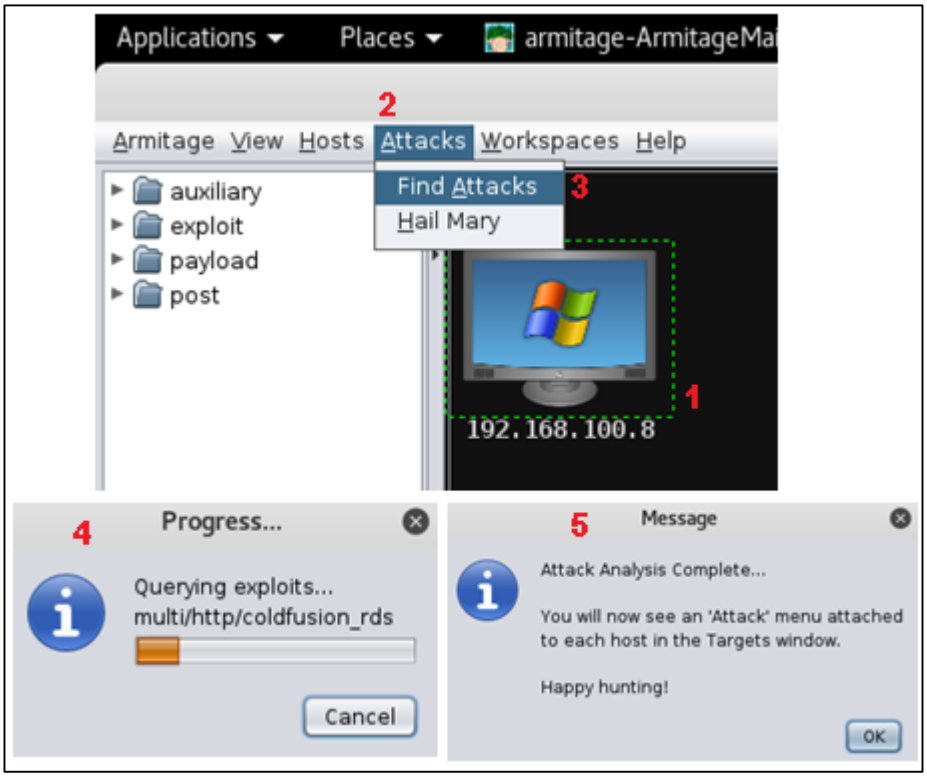


Figura 2.31 Proceso para la búsqueda de ataques.

7. Como se observa en la figura 2.32, se da clic derecho sobre el ícono del host, esto abrirá un menú contextual el cual tendrá la opción llamada Attack, se coloca el cursor sobre la misma y nos mostrará un submenú con todos los posibles ataques que se pueden realizar al host. Se escoge smb, que hace referencia al protocolo SMB, el cual permite el control del host de forma remota. Por último la opción ms08_067_netapi que refiere a una inyección de payload [28] malicioso sobres los protocolos de red de Microsoft Windows.

En la Figura 2.33 se puede observar una ventana emergente, la cual proporciona información del payload para el protocolo SMB [29] y sus configuraciones. Damos clic al botón Launch.

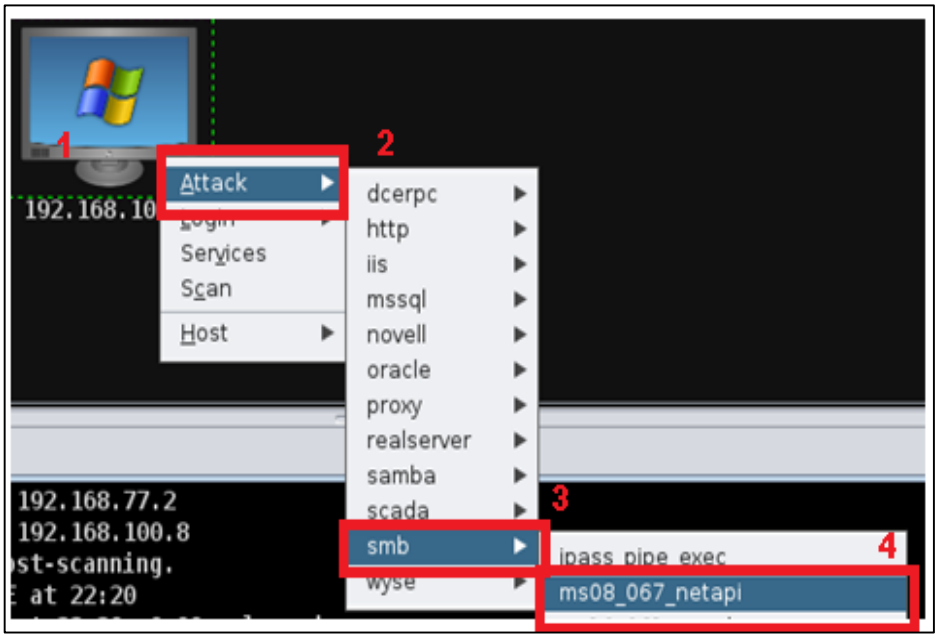


Figura 2.32 Menú contextual con posibles ataques a efectuar en Armitage.

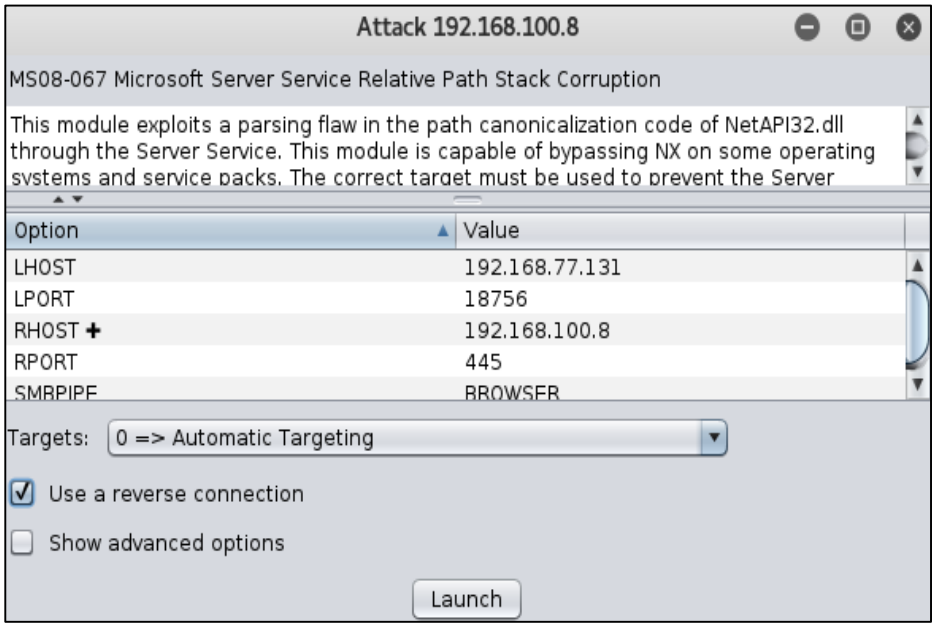


Figura 2.33 Ventana emergente para el ataque al protocolo SMB.

8. Luego de que se ejecuta el paso anterior, se puede apreciar que el exploit se llevó a cabo de forma exitosa; ya que, el ícono del host cambio a una representación color rojo con rayos alrededor. Armitage muestra una tercera viñeta con el nombre de exploit en la sección de la consola. Se puede visualizar el prompt de meterpreter mostrando una sesión abierta con el identificador 1, lo que indica que la inyecciónxn del payload fue exitosa y se ha generado la sesión número uno para las pruebas de intrusión como se muestra en la Figura 2.34.

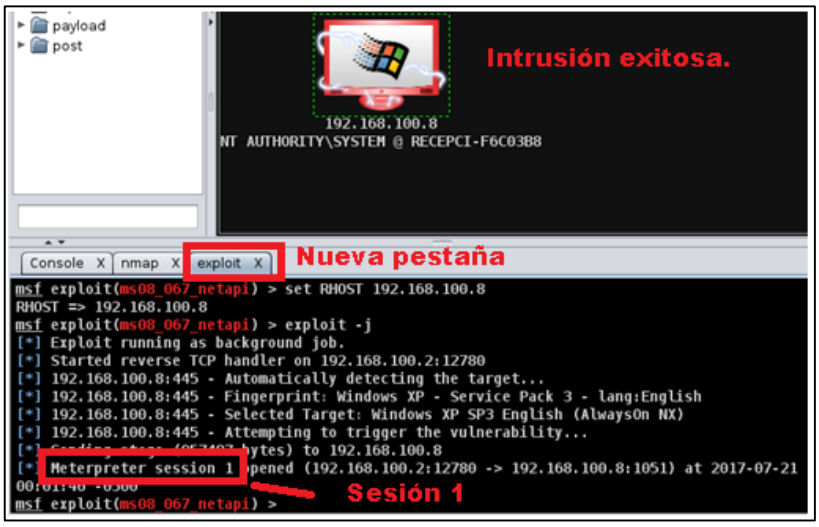


Figura 2.34 Ataque exitoso, host listo para las pruebas de instrucción.

9. A continuación se interactúa con la sesión previamente abierta con la función del meterpreter [30] mediante Shell. Se selecciona el host objeto del ataque, clic derecho en el menú contextual Meterpreter, Interact, Meterpreter Shell. Acto seguido aparece una pestaña llamada con el nombre de: Meterpreter 1, en la cual se ingresa comandos.

10. En la pestaña de Meterpreter se digita comandos para demostrar que la intrusión en el equipo ha sido exitosa. En la Figura 2.35 se utiliza el comando screenshot, el cual muestra una captura de pantalla del host.

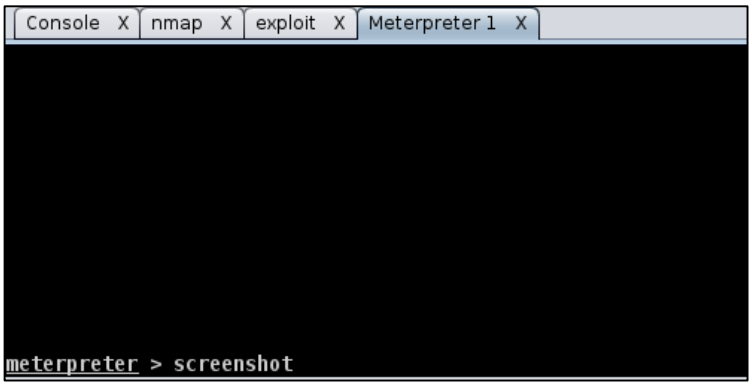


Figura 2.35 Ejecución del comando Screenshot en Armitage.

Como se logra apreciar en la Figura 2.36 el comando screenshot genera una pestaña con la captura de pantalla del host, con las opciones de actualizar y observar cada 10 segundos. Ambas opciones permiten generar capturas de pantalla en tiempo real, la diferencia es que la primera opción es manual y la segunda es automática.

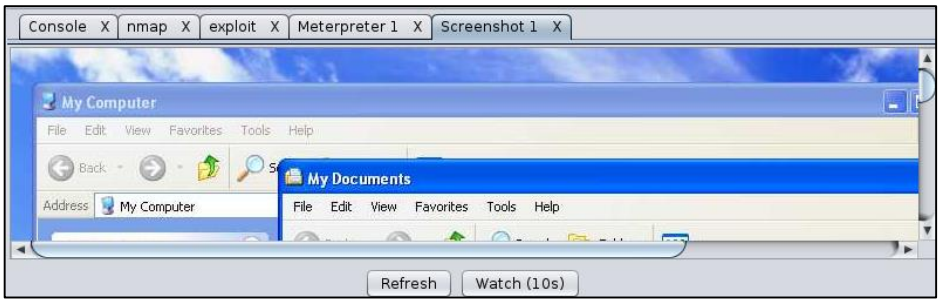


Figura 2.36 Captura de pantalla del host cliente

11. Se consigue privilegios administrativos con el comando getsystem. En Figura 2.37 se observa la introducción del comando getsystem en la consola meterpreter de Armitage.

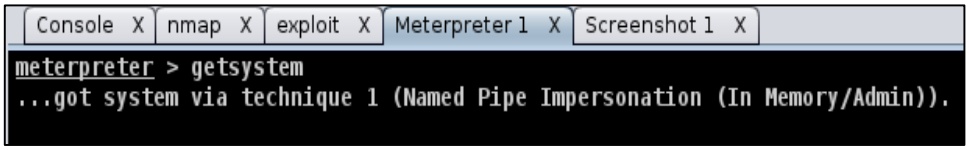


Figura 2.37 Comando Getsystem

12. En la Figura 2.38, se utiliza el comando hashdump para obtener los hashes de las contraseñas de usuario almacenadas en el ordenador además de los nombres de usuario.

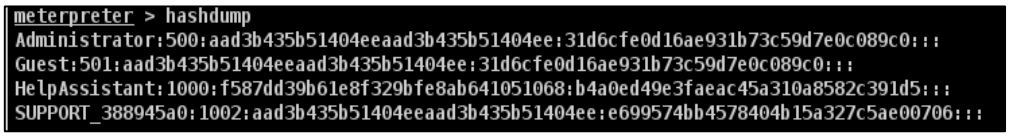


Figura 2.38 Comando Hashdump

13. El comando keyscan_start permite iniciar la captura de teclado, keyscan_dump mostrar los resultados y keyscan_stop detener la captura. Como se muestra en la Figura 2.39, se debe definir la aplicación de la cual se desea obtener información, esto se realiza con el comando getpid se obtienen el número de proceso del aplicativo en ejecución para luego obtener la captura con los comandos antes mencionados.

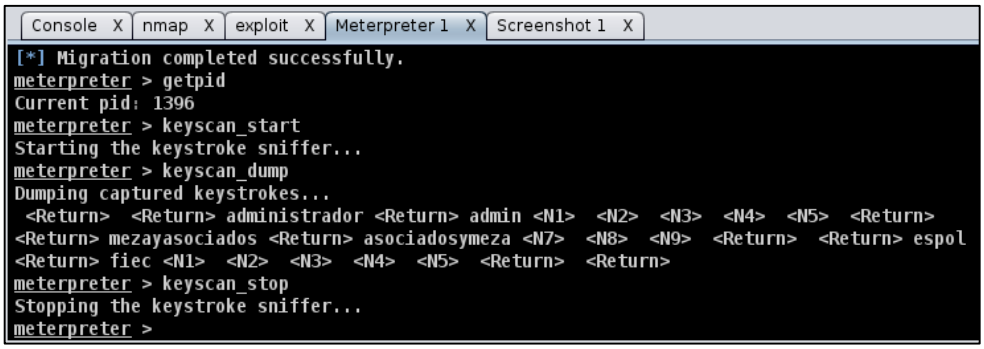


Figura 2.39 Comando getpid, keyscan_start, keyscan_dump y keyscan_stop en Armitage

14. Se realizan fotos desde la cámara web del PC vulnerado utilizando el comando webcam_snap, mediante una ventana emergente llamada Cameras pulsando el botón Take Picture, como muestra en la Figura 2.40.

Figura 2.40 Comando Webcam_snap en Armitage.

15. Se controla el CMD de Windows con el comando Shell. En la Figura 2.41 se muestra el control del CMD remoto mediante los comandos del propio sistema operativo, esto permite cortar, pegar y mover archivos; además de administrar procesos, aplicaciones y recursos del computador.

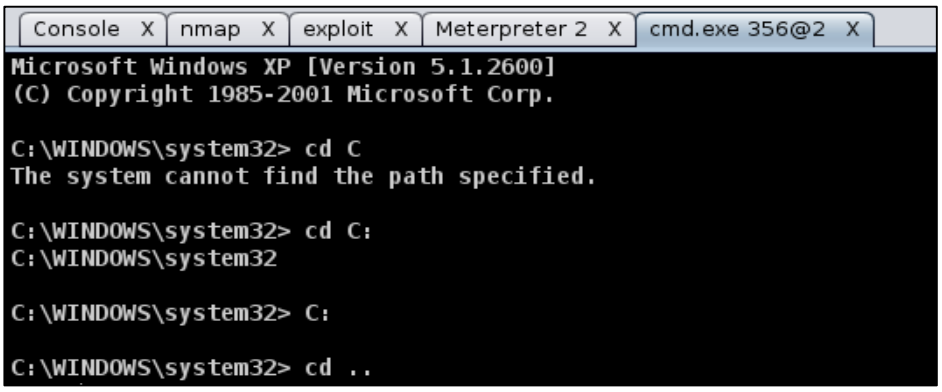


Figura 2.41 Control del CMD de Windows en Armitage.

2.6 Plan de Mitigación.

El principal objetivo de esta etapa es establecer los métodos mediante los cuales podremos mitigar las vulnerabilidades encontradas en las etapas de Hacking Ético dada la infraestructura tecnológica existente en Meza y Asociados.

2.6.1 Lista de GPO's a aplicar en el servidor con Active Directory.

Como se muestra en la Tabla 2.4, se establecen políticas para usuarios, grupos y estaciones de trabajo en el servidor de Directorio Activo [31] Active Directory, distribuidas en 3 tópicos que son: Derechos de usuarios, configuraciones de seguridad en estaciones de trabajo y seguridad de redes. El propósito es estas políticas es limitar el control que posee el usuario común sobre las estaciones de trabajo.

Permisos para usuarios
Restringir el acceso al equipo a través de la red a Administradores y Usuarios autenticados.
Denegar a todos los usuarios el derecho de "actuar como parte del Sistema operativo".
Restringir el inicio de session a los administradores locales.
Denegar a las cuentas de invitado la posibilidad de iniciar sesión para ejecutar servicios localmente o a través de RDP.
Configuraciones de seguridad
Colocar un banner de advertencia de la empresa en el inicio de sesión de los usuarios.
Prohibir a los usuarios la creación y el inicio de sesión con cuentas de Microsoft.
Deshabilitar las cuentas de invitado.
Rquerir Ctrl+Alt+Del para inicios de sesión interactivos.

Configurar tiempo límite de inactividad en la máquina, para proteger las sesiones interactivas inactivas.
Configurar Microsoft Network Client para firmar las comunicaciones de forma digital.
Configurar Microsoft Network Client para firmar las comunicaciones de forma digital si el servidor lo acepta.
Deshabilitar el envío de contraseñas no cifradas a servidores SMB de terceros.
Configurar Microsoft Network Server para firmar las comunicaciones de manera digital.
Configurar Microsoft Network Server para firmar las comunicaciones de manera digital si el cliente está de acuerdo.
Configuraciones de seguridad de red
Permitir que el Sistema local use la identidad del equipo para NTLM.
Deshabilitar la suspension de la sesión del Sistema local NULL.
Configurar Kerberos como tipo de cifrado permitido.
No almacenar valores de hash del administrador de la LAN.
Configurar el nivel de autenticación para el administrador LAN, para permitir únicamente NTLMv2 y rechazar NTLM y LM.
Habilitar el Firewall de Windows en todos los perfiles de usuario (dominio, privado, público).
Configurar el Firewall de Windows en todos los perfiles para bloquear el tráfico entrante de forma predeterminada.

Tabla 2.3 Políticas aplicadas a Grupos del Active Diretory en Windows

2.6.2 Deshabilitar puertos USB en equipos que no pertenecen al dominio.

Se procede a crear dos scripts con extensión .reg, mismos que son usados para habilitar o deshabilitar los puertos USB en las estaciones de trabajo que no requieren la compartición de archivos, como lo son

el área de ventas y diseño. Los equipos que son utilizados para facturación en las sucursales también son incluidos.

Script para habilitar puertos USB.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR]"Start"= dword:
00000003
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR\Enum]"Count"=d
word:00000000"NextInstance"=dword:00000000
```

Script para deshabilitar puertos USB.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR]"Start"= dword:
00000004
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR\Enum]"Count"=d
word:00000000"NextInstance"=dword:00000000
```

2.6.3 Implementación WSUS.

En esta etapa se pone en marcha la instalación de un servidor WSUS [32], de manera que se pueda administrar de forma centralizada las actualizaciones de los equipos.

El objetivo de esta implementación es que los parches de seguridad en los computadores de la empresa se encuentren siempre actualizados, se pueden establecer horarios para las actualizaciones y segmentarlas por grupos, estaciones de trabajo o departamentos.

La figura 2.42 muestra la interfaz de administración de GPO WSUS, donde se procede a configurar las políticas de actualización:

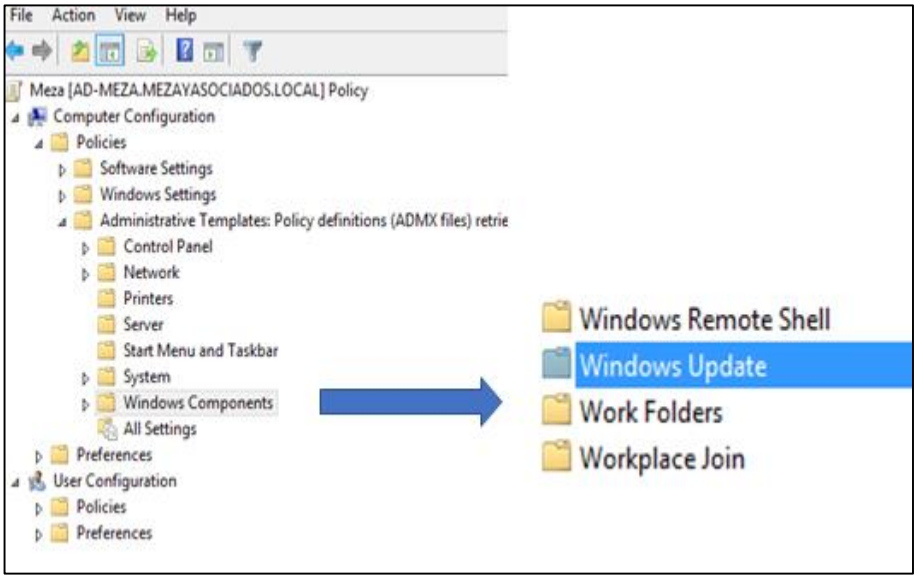


Figura 2.42 Ventana de GPO para la cración de políticas de WSUS.

1. En el Group Policy Management se procede a crear una política de grupo aplicable a los equipos de la empresa.

2. Se da clic derecho en Editar sobre la GPO creada, inmediatamente aparece una ventana con el Group Policy Management Editor.

3. Se navega hasta el menú Computer Configuration → Policies → Administrative Templates →Windows Components →Windows Update.

4. Se selecciona Configure Automatic Updates, y se habilita la directiva marcando la casilla Enabled.

5. Dentro de los parámetros de configuración de la GPO se selecciona el modo en el que se descargan y realizan las actualizaciones, en nuestro caso; Auto Download and Schedule the install.

Así también se escoge los días y la hora en las que se instalarán las actualizaciones en los equipos.

6. Dentro de las configuraciones de Windows update se selecciona la opción Enable client site targeting, se marca Enabled y posterior a esto se ingresa el nombre del grupo de equipos a los que les será habilitada la GPO.

7. En el panel de Windows Update se selecciona la opción Specify intranet Microsoft Update Service Location. Se Marca la opción Enabled y se ingresa el nombre del servidor WSUS en las casillas: Set The Intranet Update Service For Detecting Updates, Set The Intranet Statistics Server.

8. Se aplica la GPO al grupo de equipos del dominio.

2.6.4 Establecimiento de reglas para inspeccionar correo.

Se establecen reglas para evitar la fuga de información mediante el servidor de correo electrónico empresarial Exchange Server, por medio del bloqueo de archivos adjuntos que contengan extensiones de archivos sensibles, como es el caso de: archivos de Excel, Polyboard utilizado para el diseño de muebles y archivos mysql correspondientes a la base de datos. Así también dentro de este ámbito se considera que el límite en tamaño de los archivos adjuntos no supere los 4 MB.

La Figura 2.43 muestra la secuencia de pasos a seguir para la creación de una nueva regla de correo que excluya patrones de texto y extensiones de archivo.

1 Iniciamos Exchange Admin Center → Mail Flow → Rules.

2 More options → Apply this rule if → Any attachment

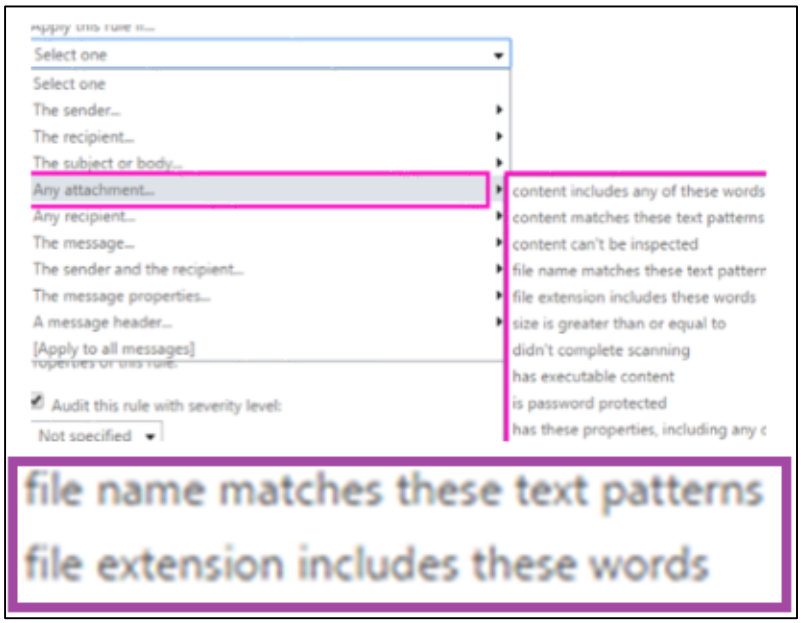
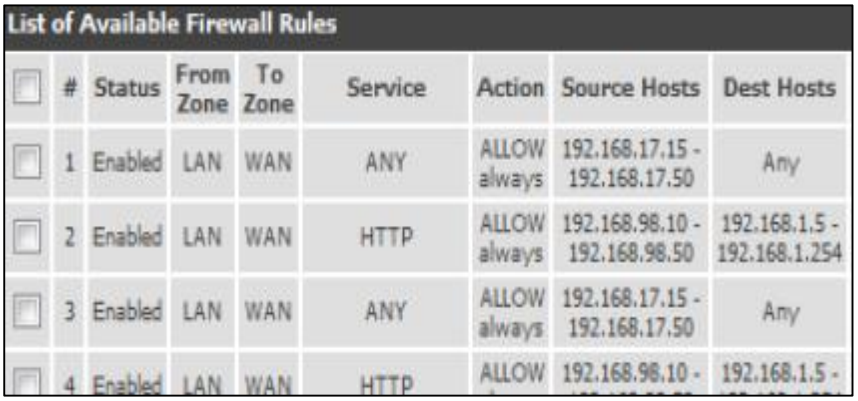


Figura 2.43 Establecimiento de reglas de correo mediante Exchange Server.

2.6.5 Establecimiento de reglas Firewall.

Se establecen reglas de firewall en el Router D-Link DSR-1000N, con el objetivo de evitar tráfico que pueda afectar el desempeño de la red y evitar descargas de archivos que puedan tener software mal intencionado por parte de los usuarios de la empresa. La figura 2.44 y 2.45 nos presenta el ingreso y configuración de una política de Firewall que permite bloquear direcciones IP, URL's y Puertos. Meza y Asociados bloquea toda URL asociada a sitios de correo electrónico, nubes de almacenamiento y sitios P2P.

1 Accedemos al router Advanced → Firewall Settings → Firewall Rules.



List of Available Firewall Rules

	#	Status	From Zone	To Zone	Service	Action	Source Hosts	Dest Hosts
	1	Enabled	LAN	WAN	ANY	ALLOW always	192.168.17.15 - 192.168.17.50	Any
	2	Enabled	LAN	WAN	HTTP	ALLOW always	192.168.98.10 - 192.168.98.50	192.168.1.5 - 192.168.1.254
	3	Enabled	LAN	WAN	ANY	ALLOW always	192.168.17.15 - 192.168.17.50	Any
	4	Enabled	LAN	WAN	HTTP	ALLOW	192.168.98.10 -	192.168.1.5 -

Figura 2.44 Interfaz de ingreso de reglas de firewall.

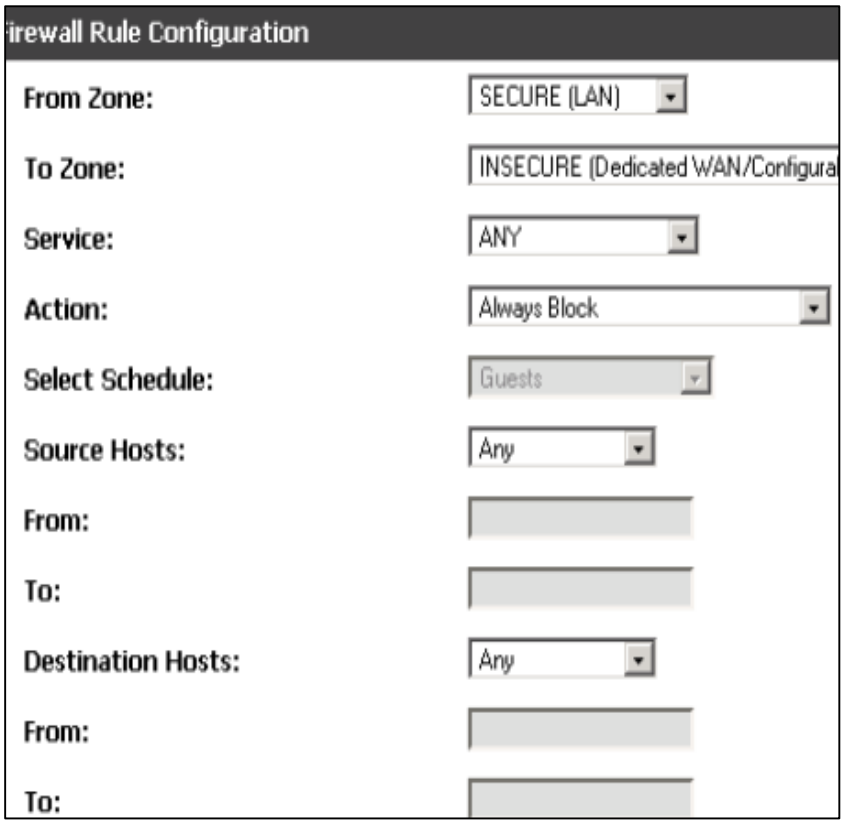


Figura 2.45 Configuraciones de regla de firewall.

2.7 Plan de Implementación.

La implementación de este proyecto tuvo una duración de 70 días. De los cuales 5 días tomó la etapa de reconocimiento, 10 días la etapa de escaneo y enumeración, 5 días para las pruebas de intrusión en la etapa de explotación, 20 días para el desarrollo del plan de mitigación y 30 días la definición de políticas, así como la implementación de las mismas. Como se detalla en la Figura 2.46.

DIAGRAMA DE GANTT

	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos
1	**"DISEÑO Y DESARROLLO DE HACKING ETICO APLICADO A LA INFRAESTRUCTURA DE RED DE UNA EMPRESA DEDICADA A LA FABRICACION DE MUEBLES"**	**70 días**	**lun 15/5/17**	**vie 18/8/17**	**Jorge Baquero;Kelvin Vásquez;Laptop[1]**
2	**Reconocimiento**	**5 días**	**lun 15/5/17**	**vie 19/5/17**	
3	Búsqueda de dominio en base de datos pública Whois	2 días	lun 15/5/17	mar 16/5/17	Kelvin Vásquez;Laptop[1]
4	Determinar topología de red de la empresa con Maltego	3 días	mié 17/5/17	vie 19/5/17	Kelvin Vásquez;Laptop[1]
5	Recopilación de datos obtenidos	0 días	vie 19/5/17	vie 19/5/17	Kelvin Vásquez;Laptop[0]
6	Elaboración de informe	0 días	vie 19/5/17	vie 19/5/17	Kelvin Vásquez;Laptop[0]
7	**Escaneo y Enumeración**	**10 días**	**lun 22/5/17**	**vie 2/6/17**	
8	Procedimiento de escaneo con OpenVAS	5 días	lun 22/5/17	vie 26/5/17	Jorge Baquero;Laptop[1]
9	Enumeración con Hyena	5 días	lun 29/5/17	vie 2/6/17	Jorge Baquero;Laptop[1]
10	Recopilación de datos obtenidos	0 días	vie 2/6/17	vie 2/6/17	Jorge Baquero;Laptop[0]
11	Elaboración de informe	0 días	vie 2/6/17	vie 2/6/17	Jorge Baquero;Laptop[0]
12	**Explotación**	**5 días**	**lun 5/6/17**	**vie 9/6/17**	
13	**Explotación de equipo con Armitage**	**4 días**	**lun 5/6/17**	**jue 8/6/17**	
14	Escaneo	2 días	lun 5/6/17	mar 6/6/17	Kelvin Vásquez;Laptop[1]
15	Selección de ataques	1 día	mié 7/6/17	mié 7/6/17	Jorge Baquero;Laptop[1]
16	Procesos de ataques	1 día	jue 8/6/17	jue 8/6/17	Jorge Baquero;Laptop[1]
17	Recopilación de datos obtenidos	0 días	vie 9/6/17	vie 9/6/17	Jorge Baquero;Kelvin Vásquez;Laptop[0]
18	Elaboración de informe	0 días	vie 9/6/17	vie 9/6/17	Jorge Baquero;Kelvin Vásquez;Laptop[0]
19	**Plan de mitigación**	**20 días**	**lun 12/6/17**	**vie 7/7/17**	
20	Establecimiento de GPO's	5 días	lun 12/6/17	vie 16/6/17	Kelvin Vásquez;Laptop[1]
21	Configuración de scripts para bloqueo de puertos USB	4 días	lun 19/6/17	jue 22/6/17	Kelvin Vásquez;Laptop[1]
22	Instalación de servidor WSUS	2 días	vie 23/6/17	lun 26/6/17	Kelvin Vásquez;Laptop[1]
23	Configuración de reglas de correo	3 días	mar 27/6/17	jue 29/6/17	Jorge Baquero;Laptop[1]
24	Configuración de reglas de firewall	3 días	vie 30/6/17	mar 4/7/17	Jorge Baquero;Laptop[1]
25	Verificar configuración de registros en equipos salientes	3 días	mié 5/7/17	vie 7/7/17	Kelvin Vásquez;Laptop[1]
26	**Definición de políticas e implementación**	**30 días**	**lun 10/7/17**	**vie 18/8/17**	
27	Evaluar los procedimientos	5 días	lun 10/7/17	vie 14/7/17	Jorge Baquero;Kelvin Vásquez;Laptop[1]
28	Determinar los posibles riesgos	3 días	lun 17/7/17	mié 19/7/17	Jorge Baquero;Kelvin Vásquez;Laptop[1]
29	Elaborar el documento	5 días	jue 20/7/17	mié 26/7/17	Jorge Baquero;Kelvin Vásquez;Laptop[1]
30	Revisión del documento por la gerencia	5 días	jue 27/7/17	mié 2/8/17	
31	Aprobación del documento	1 día	jue 3/8/17	jue 3/8/17	
32	Capacitar a los empleados de la empresa	10 días	vie 4/8/17	jue 17/8/17	Jorge Baquero;Kelvin Vásquez;Laptop[1]

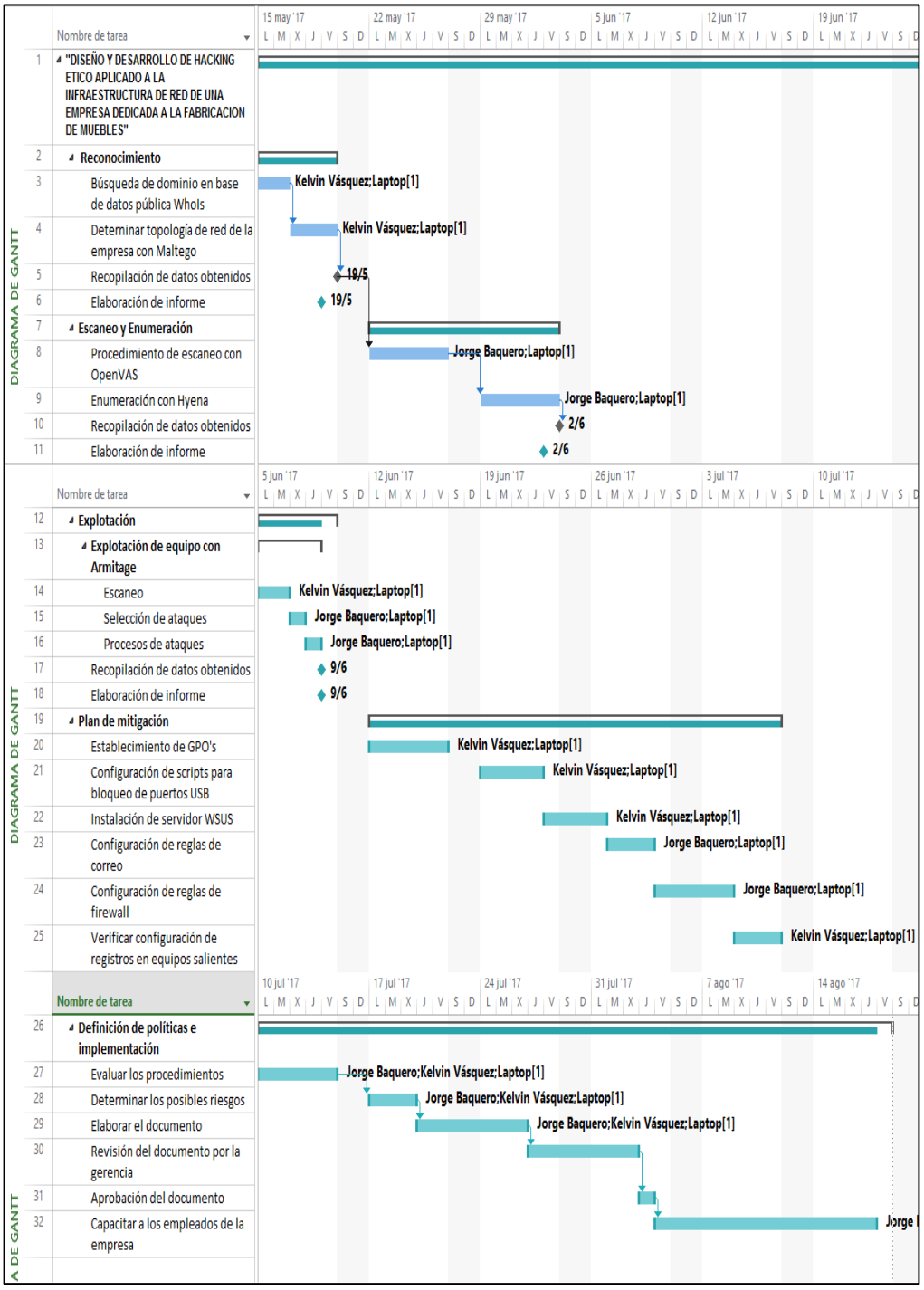


Figura 2.46 Plan de Implementación

2.8 Costos de implementación.

Para llevar a cabo la implementación del proyecto, se contemplan las horas de trabajo asignadas a cada recurso, entendiéndose que un recurso con horas laborales asignadas corresponde a un activo humano.

En las Figuras 2.47 y 2.48 se presenta una visión general de los costos del uso de los recursos (Jorge Baquero, Kelvin Vásquez), en la implementación del proyecto con una duración de 70 días, laborando 8 horas diarias, 5 días a la semana. Siendo el costo de cada recurso $7.50/hora, representando esto un costo total de $ 13,500.

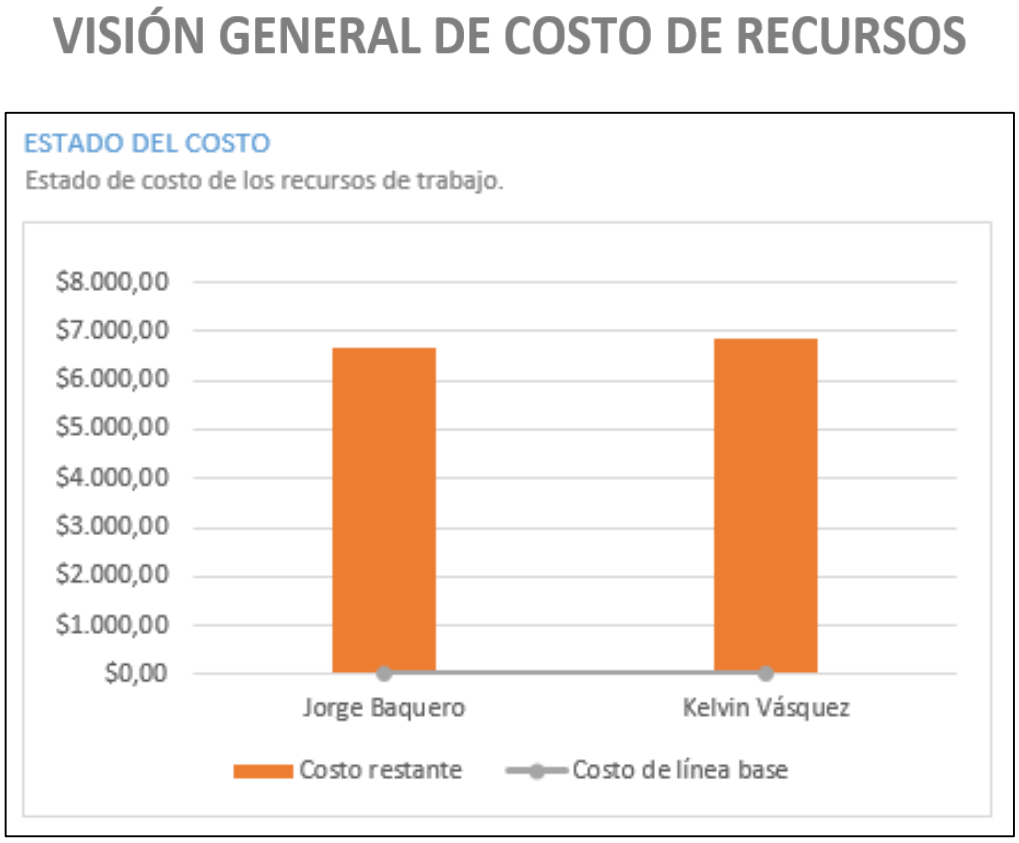


Figura 2.47 Estado del costo de los recursos de trabajo.

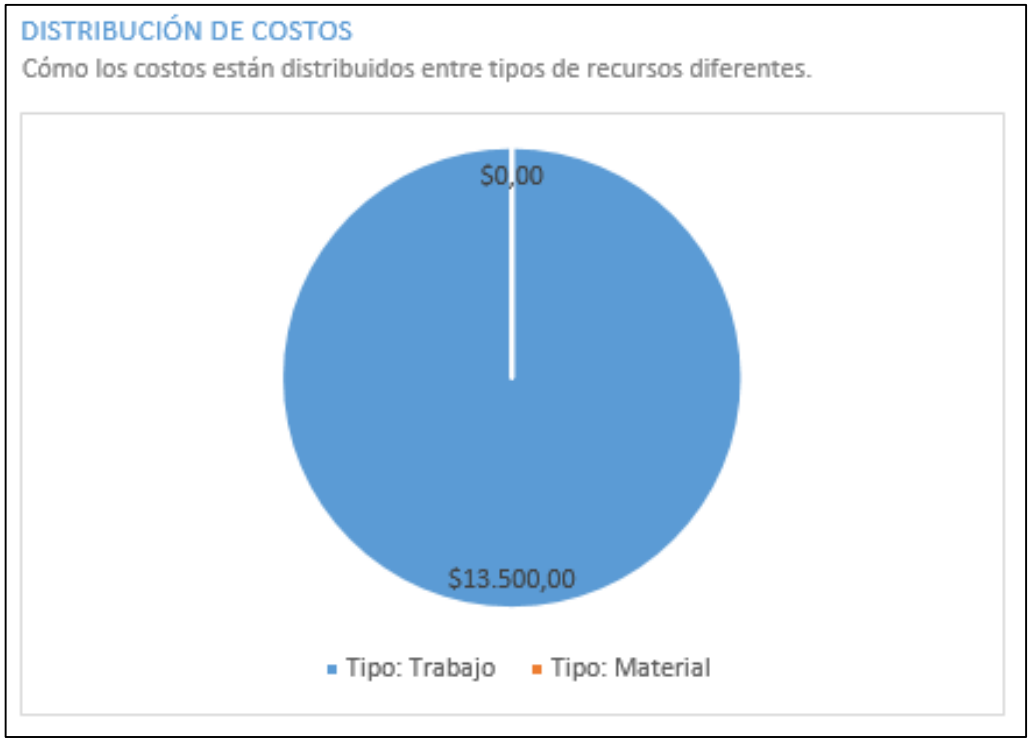


Figura 2.48 Distribución de costos por tipo.

CAPÍTULO 3

3. RESULTADOS

En este capítulo se procede a mostrar de forma detallada los resultados obtenidos en la auditoría realizada, para luego emitir las respectivas conclusiones y recomendaciones.

3.1 Resultados de la Etapa de Reconocimiento

3.1.1 Información obtenida del aplicativo WhoIs

La tabla 3.1 muestra la información relevante obtenida con la herramienta web WhoIs. Dónde encontramos en nombre de dominio, fecha de registro y expiración del mismo; y los DNS asociados a ese dominio. La tabla 3.2 muestra los datos de contacto, en este caso el del gerente general, teléfono, correo electrónico, nombre y dirección de la empresa. Datos con los que se podría realizar un ataque de ingeniería social [33].

Información del dominio

Dominio	mezayasociados.xyz
Fecha registro	2012-02-22
Fecha de expiración	2018-10-22
Nombre de los servidores	ns1.mezayasociados.xyz ns2.mezayasociados.xyz dns3.mezayasociados.xyz dns4.mezayascoiados.xyz

Tabla 3.1 Información del dominio

Nombres	Lissette Meza
Teléfono	+00.593986981991
Correo Electrónico	lmezavega@mezayasociados.xyz
Nombre de la Empresa	Meza Y Asociados
Dirección de la Empresa	Metropolis Dos Mz. 1289 S. 24

Tabla 3.2 Información de contacto de la empresa

3.1.2 Herramienta Matlego.

El sitio web está alojado en un solo servidor con un adaptador de red único, con la IP pública 50.63.202.42 perteneciente al bloque de IPs 50.63.202.0-50.63.202.255. Este servidor tiene salida a internet mediante el ISP local TELCONET S.A., su número de sistema autónomo es el 26496 y su puerta de enlace predeterminada es la 192.168.100.5.

3.2 Resultados de la Etapa de Escaneo

3.2.1 Herramienta OpenVas

Se muestra información de puertos de todas las estaciones de trabajo y servidores; su función y vulnerabilidad, como se observa en la tabla 3.3. Para mayor detalle de los equipos auditados ver el siguiente enlace: https://goo.gl/GAmMYY

Host	Dirección IP	Puertos Abiertos	Función	Vulnerabilidad
PC 1	192.168.100.83	TCP 80 21 515 53 UDP 53	 HTTP FTP PRINTER DOMAIN DOMAIN	DNS en ejecución, aceptando cualquier petición. Servicio de impresión en ejecución, puede sufrir

				sobrecarga en buffer de memoria. Colgar equipo mediante el envío de paquetes TCP mal formados y opciones inválidas.

Host	Dirección IP	Puertos Abiertos	Función	Vulnerabilidad
PC 2	192.168.100.84	TCP 1723 20000 1875 10000 3306 143 110 82 81 80 25 22 443	 PPTP DNP WESTELL NDMP MYSQL IMAP POP3 XFER HOSTS2-NS HTTP SMTP SSH HTTPS	Colgar equipo mediante el envío de paquetes TCP mal formados y opciones inválidas.

Tabla 3.3 Datos obtenidos de OpenVAS

En el servidor SQL se detectó el protocolo de escritorio remoto activo y el protocolo de archivos compartidos e impresoras SMB.

El servidor de correo posee los siguientes puertos abiertos: FTP, IRC, SMB. Además del puerto TCP 3306 MYSQL.

En el servidor web se detectó una versión de Apache obsoleta, la 2.2. En la cual se puede realizar un ataque de DoS mediante el puerto Debug HTTP, tiene activo los puertos 22,80,111 y 443 TCP; debido a la falta de instalación de los parches de seguridad, se detectan como vulnerables.

3.3 Resultados de la Etapa de Enumeración

3.3.1 Herramienta Hyena

Se obtuvo información como: el nombre de equipo de 4 computadoras y 2 servidores. Aadicionalmente a esto, los usuarios de cada computador. Como se detalla en la tabla 3.4.

Nombre de Host	Nombre de Equipo	Dirección IP	Usuarios
PC de Escritorio 10	Ventas_03	192.168.100.92	jestrada, invitado, Administrador
PC de Escritorio 9	Ventas_04	192.168.100.91	lcastro, Adminstrador
Laptop 3	Gerente	192.168.100.152	Gerencia
Laptop 2	Finaciero_02	192.168.100.127	Departamento_gerencia, invitado, Administrador
Servidor de Base de Datos	BD	192.680.100.43	Administrador
Servidor de Correo	CORREO	192.680.100.42	Administrador

Tabla 3.4 Datos obtenidos de Hyena

3.4 Resultados de la Etapa de Explotación

3.4.1 Herramienta Armitage

El uso de la herramienta Armitage obtuvo los siguietes resultados:
En el servidor de base de datos, se vulneró la seguridad mediante el protocolo SMB, este fallo de seguridad se debe a la falta de actualización en el sistema operativo Windows Server 2008 R2. Debido a esto, se pudo obtener información de captura de pantallas, acceso a la consola de Símbolos del Sistema, captura de la entrada del teclado, elevar privilegios a una cuenta administrativa y revelada de hashes de contraseñas.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

La realización de una auditoría informática es un procedimiento vital para generar conciencia y desarrollar una cultura en seguridad informática en empresarios, trabajadores y profesionales de TI.

El llevar a cabo procesos de Hacking ético de forma periódica, ayuda a las empresas a cuidar su información ante posibles pérdidas.

Establecer reglas de filtrado de tráfico a nivel de firewall previenen la fuga de información y tráfico de servicios innecesarios en la red.

Realizar una auditoría informática lleva un tiempo prudencial, donde se deben revisar de forma minuciosa las herramientas a utilizar, que las mismas sean confiables y efectivas.

Al no existir políticas de seguridad dirigidas a los usuarios, se crea un estado de incertidumbre con respecto a que se puede o no hacer en la organización. Una política que integre sanciones por faltas debe ser un correctivo efectivo para la mitigación de ataques.

Ninguna prueba de Hacking afecto de la alguna manera a los sistemas informáticos de la empresa.

Recomendaciones

Se recomienda realizar el pago a la NIC, de manera que la misma mantenga oculta la información del dominio de la empresa.

Adquisición de equipo IPS para la prevención de intrusos en la red local. Véase el Anexo A para obtener información detalla del equipo sugerido.

Establecer políticas de uso de equipos de cómputo, en las que se incluyan privilegios de usuario. Ver Anexo B.

Actualizar de forma periódica los componentes de la red, para no generar un tráfico inusual que afecte el desempeño de la organización, se debe establecer horarios de actualización para las estaciones de trabajo en horas de almuerzo, y los servidores en horas no laborales.

Se debe llevar una bitácora de puertos, servicios y sitios web utilizados en la red local. Con el fin de tener un control eficiente del tráfico entrante y saliente, a través de un servidor proxy que lo limite y evite fugas de información.

Realizar un plan de recuperación de datos ante desastres, no solo ante la amenaza de cibercriminales, sino también de fenómenos naturales.

Migrar el sitio web de la empresa a un hosting, con el objetivo de mejorar costos ya que los requerimientos de la empresa no ameritan el uso de un servidor web exclusivo.

Se recomienda apagar las estaciones de trabajo y puntos de acceso inalámbrico cuando se termine la jornada laboral. Esto asegura que no se realicen pruebas de intrusión por persona malintencionadas.

Mantenerse al tanto de las nuevas amenazas informáticas que se generan, a través de sitios web que ofrezcan información actualizada acerca de seguridad informática permite incorporar nuevas técnicas a futuras auditorias y prevenir ataques informáticos.

BIBLIOGRAFÍA

[1] Ecucert, «Ecucert,» [En línea]. Available: https://www.ecucert.gob.ec/.

[2] R. Justicia, «El Telégrafo,» 16 Agosto 2016. [En línea]. Available: http://www.eltelegrafo.com.ec/noticias/judicial/13/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario.

[3] F. Medina, «El Comercio,» 29 Octubre 2016. [En línea]. Available: http://www.elcomercio.com/actualidad/hackers-rusia-ecuador-ciberataques-seguridad.html.

[4] S. Pham, «CNN,» 15 Mayo 2017. [En línea]. Available: http://cnnespanol.cnn.com/2017/05/15/que-es-un-virus-ransomware-y-como-actua/.

[5] Ejecutivo TI, «Ejecutivo TI,» 1 2017 Marzo. [En línea]. Available: http://www.ejecutivoti.com/portal/revista03-17/.

[6] AMCHAM GUAYAQUIL, «AMCHAM GUAYAQUIL,» 12 Agosto 2015. [En línea]. Available: http://amchamgye.org.ec/seguridad-informatica-y-hacking-etico-una-mirada-preventiva-al-mayor-activo-de-la-empresa-la-informacion/.

[7] Cisco.com, «Cisco.com,» 29781, 1 Febrero 2007. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/ip/point-to-point-tunneling-protocol-pptp/29781-pptp-ios.html#intro.

[8] Dlink, 2012. [En línea]. Available: http://www.dlink.com/es/es/-/media/business_products/dsr/dsr-1000n/datasheet/dsr_series_datasheet_en_eu.pdf.

[9] Dlink, «Dlink,» 2013. [En línea]. Available: http://www.dlink.com/es/es/-/media/business_products/dgs/dgs-1024d/datasheet/dgs_1016d_1024d_h1_datasheet_en_eu.pdf.

[10] E900, «Lnksys,» [En línea]. Available: https://www.linksys.com/co/p/P-E900/#product-features.

[11] A. C3150, «Archer C3150,» [En línea]. Available: http://www.tp-link.es/products/details/cat-9_Archer-C3150.html#specifications.

[12] M. Rouse, «searchdatacenter.techtarget.com,» Noviembre 2012. [En línea]. Available: http://searchdatacenter.techtarget.com/es/definicion/Microsoft-Exchange-Server-2013.

[13] M. Rouse, «searchdatacenter.techtarget.com,» Enero 2015. [En línea]. Available: http://searchdatacenter.techtarget.com/es/definicion/MySQL.

[14] oracle.com, «oracle.com,» 2016. [En línea]. Available: https://www.oracle.com/applications/erp/what-is-erp.html.

[15] E. F. Cases, «ibrugor.com,» 11 Junio 2014. [En línea]. Available: http://www.ibrugor.com/blog/apache-http-server-que-es-como-funciona-y-para-que-sirve/.

[16] D. M. Hafele, «sans.org,» 23 Febrero 2004. [En línea]. Available: https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-gray-1390.

[17] E. Marin, «hipertextual.com,» 30 Septiembre 2014. [En línea]. Available: https://hipertextual.com/2014/09/windows-10-caracteristicas.

[18] R. Andrés, «computerhoy.com,» 03 Abril 2016. [En línea]. Available: http://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671.

[19] gpsos.es, «gpsos.es,» [En línea]. Available: https://www.gpsos.es/soluciones-open-source/definicion-de-open-source/.

[20] Iiemd.com, «Iiemd.com,» [En línea]. Available: https://iiemd.com/freeware/que-es-freeware.

[21] one.com, «one.com,» [En línea]. Available: https://www.one.com/es/support/faq/que-es-whois.

[22] S. Esteban, «backtrackacademy.com,» 2016. [En línea]. Available: https://backtrackacademy.com/articulo/maltego-herramienta-para-recopilar-informacion.

[23] Cisco.com, «Cisco.com,» 26 Octubre 2005. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/ip/domain-name-system-dns/12683-dns-descript.html.

[24] J. Albors, «welivesecurity.com,» 9 Octubre 2014. [En línea]. Available: https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/.

[25] L. Á. Huerta, «openwebinars.net,» 30 Mayo 2014. [En línea]. Available: https://openwebinars.net/blog/openvas-en-linux-explorando-nuestros-sistemas/.

[26] Elixircorp.com, «Elixircorp.com,» [En línea]. Available: http://elixircorp.com/blog/hacking_frameworks_explotacion/.

[27] Kali.org, «Kali.org,» [En línea]. Available: https://tools.kali.org/exploitation-tools/armitage.

[28] Offensive-security.com, «Offensive-security.com,» [En línea]. Available: https://www.offensive-security.com/metasploit-unleashed/payloads/.

[29] S. Singh, «Symantec,» 4 Enero 2012. [En línea]. Available: https://www.symantec.com/connect/articles/microsoft-server-service-relative-path-stack-corruption-exploitation-and-prevention-part-i.

[30] Ofensive-security.com, «Ofensive-security.com,» 2017. [En línea]. Available: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/.

[31] Microsoft.com, «Microsoft.com,» 2013. [En línea]. Available: https://support.microsoft.com/es-es/help/196464.

[32] Microsoft.com, «Microsoft.com,» 2012. [En línea]. Available: https://msdn.microsoft.com/es-es/library/hh852340(v=ws.11).aspx.

[33] Enter.co, «Enter.co,» 27 Julio 2016. [En línea]. Available: http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/.

[34] Economía Digital, «Economía Digital,» 13 Mayo 2017. [En línea]. Available: http://www.economiadigital.es/tecnologia-y-tendencias/ciberataques-empresas_406275_102.html.

[35] Ejecutivo TI, «Ejecutivo TI,» 31 Mayo 2017. [En línea]. Available: http://www.ejecutivoti.com/portal/noticia_detalle.php?idnoticia=506.

[36] TSOFT, «TSOFT,» 27 mAYO 2014. [En línea]. Available: http://www.tsoftlatam.com/noticias/asegurando-aplicaciones-web/.

[37] M. Rodríguez, «BBC Mundo,» 27 Octubre 2011 . [En línea]. Available: http://www.bbc.com/mundo/noticias/2011/10/111027_entre_al_mundo_hacker_etico_mr.shtml.

[38] K. Astudillo, «Blog Elixircorp,» [En línea]. Available: http://elixircorp.com/blog/internet-lento-wifi-hackeada/.

[39] A. M. Cañavate, «Hipertext.net,» 2003. [En línea]. Available: https://www.upf.edu/hipertextnet/numero-1/sistem_infor.html.

[40] La Hora, «La Hora,» 22 Agosto 2011. [En línea]. Available: https://lahora.com.ec/noticia/1101192492/e28098ecuador-es-un-blanco-fc3a1cil-para-ataque-de-hackerse28099.

[41] K. A. B., HACKING ÉTICO 101, Guayaquil, 2013.

[42] Gestión, «Gestión,» 30 Septiembre 2016. [En línea]. Available: http://gestion.pe/tecnologia/hay-mas-temor-empresas-ataques-ciberneticos-internos-que-externos-2171344.

[43] E. Medina, «Muyseguridad.net,» 24 Mayo 2016. [En línea]. Available: http://muyseguridad.net/2016/05/24/roban-12-millones-dolares-hackear-banco-ecuador/.

[44] Sofecom, «Sofecom,» [En línea]. Available: http://sofecom.com/peor-enemigo-de-la-seguridad-informatica/.

ANEXOS

ANEXO A: Especificaciones técnicas de equipo IPS recomendado.

Características	HPE S10 20 Mb/s IPS (JC184A)
Puertos	4 puertos RJ-45 con auto detección de velocidades 10/100/1000 MB, Half o Full Dúplex
Dimensiones	18.75 x 27 x 5.13 cm (Altura 2U)
Peso	2.49 kg (5.49 lb)
Latencia	< 600 µs
Rendimiento IPS/IDS	20 Mb/s
Rendimiento de red	20 Mb/s
Contexto de seguridad	250,000
Conexiones por segundo	3600+
Sesiones concurrentes	1,000,000
Voltaje	100 - 240 V ac
Corriente	1.8 A
Frecuencia	50/60 Hz

ANEXO B: Políticas y normas de buen uso de equipos de cómputo para pequeñas y medianas empresas.

A continuación, se presentan algunas normas o buenas prácticas con las cuales se pretende fomentar el buen uso de los equipos de cómputo que forman parte de los activos en pequeñas y medianas empresas.

1. Conexión y administración de red.

1.1 El departamento de TI, se encarga de la administración de red de la empresa, contemplando dentro de su alcance la red cableada e inalámbrica.

1.2 Los equipos conectados a la red cableada, se deben configurar con una ip estática y un nombre único en el dominio. Dicha información se debe registrar en una bitácora, junto con los nombres de los responsables.

1.3 El acceso a la red inalámbrica, debe restringirse únicamente a los servidores de la empresa y a los visitantes, siempre que soliciten el debido acceso al administrador de redes del departamento de TI.

1.4 Lo enlaces de red entre las sucursales, son administrados por el ISP y a su vez monitoreados por el administrador de red, quien en caso de fallas eventuales será el encargado de reportar el problema al proveedor.

1.5 En los casos en los que los usuarios necesiten conectarse a la red interna de la empresa desde una red externa, deben conectarse a través de la VPN de la empresa ingresando su respectivo usuario y contraseña (provisto por TI).

1.6 La comunicación entre los equipos conectados a la red debe ser cifrada.

2. En lo referente a software.

2.1 El departamento de TI, es el único ente autorizado a realizar instalaciones de software en los equipos de cómputo. Si un usuario se ve en la necesidad de usar un software especial para llevar a cabo sus labores, debe informar al departamento de TI mismo que hará las gestiones pertinentes para proceder con dicha instalación.

2.2 Únicamente el administrador de red está autorizado a llevar a cabo procesos de monitoreo de red. Mismos que deben realizarse el segundo fin de semana cada mes en horarios en los que no se vean afectadas las actividades de los colaboradores.

2.3 Los equipos conectados a la red, deben contar con las actualizaciones de sus sistemas operativos al día. Para solventar esta necesidad la empresa debe contar con un servidor WSUS, mismo que administrará dichas actualizaciones y las instalará cada 15 días siguiendo la prioridad de; críticas o importantes.

2.4 Todos los equipos de cómputo deben tener instalado un software antivirus actualizado.

2.5 Los equipos deben ser configurados con un bloqueo luego de un tiempo prudencial de inactividad. Así también aquellos eventos como intentos de autenticación fallidos deben ser registrados en las bitácoras respectivas.

3 Responsabilidades de los usuarios.

3.1 El acceso a los equipos de la empresa, se realizará con las respectivas credenciales (usuario y contraseña) provistos por el departamento de TI. Dichas credenciales deben ser únicas por usuario, así como intransferibles.

3.2 De existir usuarios que requieran hacer uso de certificados electrónicos, una vez asignados serán de responsabilidad exclusiva del colaborador. En casos de pérdidas, dichos eventos deben ser reportados al departamento de TI.

3.3 La protección física de los equipos de cómputo asignados, serán responsabilidad del usuario. De presentarse daños físicos, la reparación de los mismos irá por cuenta del colaborador responsable.

3.4 Los usuarios deben colaborar con el administrador de red, siempre que este se lo solicite; entendiéndose que se les puede solicitar asistencia con el acceso a sus equipos, o de ser el caso aportando información en investigaciones.