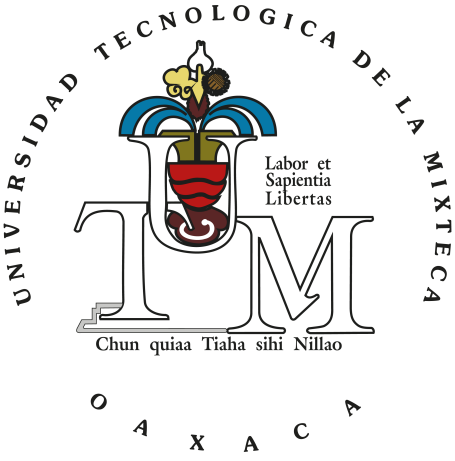


UNIVERSIDAD TECNOLÓGICA DE LA MIXTECA

Detección de Amenazas en una LAN Universitaria utilizando Software Libre

Tesis para obtener el título de:
Ingeniero en Electrónica

Presenta:
Wilfrido López Espinosa

Director de tesis:
M.C. Alejandro E. Ramírez González

H. Cd. de Huajuapan de León, Oaxaca; Junio de 2023

Dedicatoria

A la memoria amorosa y eterna de mi querida madre Leonor, quien, a pesar de su partida física, sigue siendo mi fuente de inspiración y fortaleza.

A mi querido padre Edilberto, cuyo amor, sacrificio y aliento constante han sido la base sólida sobre la que he construido mi camino hacia el conocimiento. Tus palabras de sabiduría y tu inquebrantable fé en mí han sido mi guía constante.

A mi querida tía Elodia, quien ha sido mi pilar de apoyo y ha compartido sus valiosas experiencias conmigo. Su presencia constante y ánimo en cada paso del camino ha sido invaluable.

A mis tías y tíos, quienes han sido un pilar de apoyo incondicional en mi vida. Su constante aliento y sabias palabras me han impulsado alcanzar este logro académico. Con gratitud infinita, les dedico este trabajo, sabiendo que su apoyo incondicional ha sido fundamental para alcanzar mis metas ¡Gracias por ser mi inspiración!

Willy

Agradecimientos

Agradezco al profesor Alejandro Ernesto Ramírez González, por su orientación, paciencia y compromiso con la realización de este trabajo de tesis. Su guía, sabiduría, experiencia y conocimientos fueron fundamentales para dar forma a esta investigación.

Al profesor Heriberto Ildefonso Hernández Martínez, por su valioso asesoramiento, motivación y por compartir su experiencia durante este proceso. Sus comentarios y sugerencias han enriquecido considerablemente mi trabajo.

Al profesor José Antonio Moreno Espinosa, por su tiempo y por sus aportaciones durante el desarrollo de la tesis.

Al profesor Hugo Fermín Ramírez Leyva, por sus valiosas observaciones al trabajo de tesis.

A Eduardo Villanueva Hernández, por su invaluable contribución a este trabajo, mis más sinceras gracias.

A mis amigos y seres queridos, por su comprensión, por estar presentes y por brindarme su respaldo en cada etapa de este camino académico. Sus palabras de aliento y ánimo fueron vitales para superar obstáculos y mantenerme motivado hasta el final.

Willy

Índice General

Índice de Figuras

Índice de Tablas

Capítulo 1

Introducción

El término red de computadoras se refiere a un conjunto de computadoras autónomas interconectadas por distintos medios de transmisión como cable de par trenzado, fibra óptica y/o conexión inalámbrica. En función de su cobertura, las redes pueden ser de área amplia (WAN, *Wide Area Network*), de área metropolitana (MAN, *Metropolitan Area Network*), de área local (LAN, *Local Area Network*) y de área personal (PAN, *Personal Area Network*), entre otras. En la construcción de una red, los siguientes elementos desempeñan un papel fundamental: protocolos de comunicaciones, concentradores (*hub*), conmutadores *(switch)*, enrutadores (*router*), puertas de enlace o pasarelas (*gateway*), cableado y software de gestión de redes [5].

En la actualidad, la Internet[1] es el sistema de ingeniería más grande creado por el hombre, con millones de nodos[2] conectados mediante diferentes enlaces de comunicaciones; con miles de millones de usuarios que se conectan a través de computadoras, tabletas o teléfonos inteligentes; y con una amplia variedad de nuevos dispositivos conectados, tales como consolas de videojuegos, sistemas de vigilancia, relojes y vehículos, entre otros.

Junto con el crecimiento de las redes, se incrementan y ejecutan varios tipos de ataques a través de Internet con diferentes objetivos: robo de información, corrupción y secuestro de máquinas. Estos ataques afectan a la mayoría de los usuarios del sistema [6].

Por esta razón, los especialistas en redes de computadoras necesitan analizar el tráfico con la finalidad de comprender su funcionamiento y prevenir ataques relacionados con la red. Para ello, es importante conocer los tipos de ataques y los problemas relacionados con la red. Hay dos aspectos que hacen que el análisis de paquetes sea importante: en primer lugar, el análisis de paquetes forma parte de las líneas base de cualquier red porque permite conocer su estado por adelantado antes de que surjan problemas; y en segundo lugar, es útil para diagnosticar una red en caso de ataque, y con ello ayudar a los administradores de la red a analizar el tráfico que fluye o los problemas que pueden existir [6]. Este último aspecto es la base para la detección de amenazas en una LAN universitaria.

La detección de amenazas en una LAN permite a los administradores de la red, contestar preguntas relacionadas con la seguridad en redes, por ejemplo ¿Quién es el intruso?, ¿Qué daños ha producido?, ¿Se puede reproducir el ataque y verificar que la solución funcionará? Los ataques de la red pueden identificarse observando el tráfico entrante y saliente.

En este documento se describe la detección de amenazas en una LAN universitaria,

[1] Internet con "I" mayúscula se refiere al sistema global de redes de computadoras interconectadas que se utilizan en el día a día. El uso de la palabra *internet* con "i" minúscula, es una contracción de *interconnection networks* y hace referencia a cualquier grupo de redes conectadas entre sí.

[2] En redes de computadoras cada dispositivo (conmutador, concentrador, puente, *modem*, puerta de enlace, servidor) o punto final de comunicación (computadora) se le conoce como nodo; al punto de conexión de uno o más elementos que convergen.

en donde se identifican, recopilan y analizan paquetes de red utilizando herramientas de software libre.

1.1. Planteamiento del problema

En este trabajo de tesis se propuso realizar una detección de amenazas con el fin de encontrar anomalías en LANs universitarias, utilizando las herramientas de software libre Wireshark y NetworkMiner. Dicho análisis pretende identificar riesgos y vulnerabilidades en los siguientes protocolos de red: ARP, ICMP, TCP, DHCP y TLS. Se consideran estos protocolos porque son las más representativos en una red de computadoras como lo plantean Kaur y Saluja [7].

1.1.1. Limitaciones

Debido a cuestiones administrativas, no se pudo capturar tráfico en distintas ubicaciones y escenarios (departamento de red e institutos) de la Universidad Tecnológica de la Mixteca (UTM). En este trabajo de investigación se utilizan dos muestras para realizar la detección de amenazas en una LAN universitaria. La primera muestra se capturó en el cubículo 14 del Instituto de Electrónica y Mecatrónica (IEM) de la UTM ya que fue el único lugar autorizado por los encargados del departamento de red. La segunda muestra se capturó en el Departamento de Red de una Universidad ubicada en la ciudad de Oaxaca de Juárez.

1.2. Justificación

El presente trabajo expone el uso de los conocimientos académicos adquiridos en la carrera de Ingeniería en Electrónica con el propósito de aportar una solución a un problema de amenazas en una LAN universitaria.

En la UTM no se cuenta con una línea de investigación dedicada a la detección y análisis de amenazas en una red, y dada la importancia de este tema, se considera necesario su estudio para obtener un panorama general de los eventos que suceden en una LAN universitaria.

Esta investigación busca mostrar qué tan vulnerable es una LAN, así mismo, se desea que este documento sirva como referencia para futuros trabajos en esta línea de investigación, y como ayuda a los administradores del departamento de red y profesores de la UTM que les facilite tratar temas de seguridad en redes de computadoras.

1.3. Hipótesis

La recopilación, identificación y análisis de paquetes en una LAN universitaria permitirá encontrar amenazas, riesgos, ataques y vulnerabilidades en los protocolos de red ARP, ICMP, TCP, TLS y DHCP, con la finalidad de proponer mejoras en su infraestructura y funcionamiento.

1.4. Objetivos

1.4.1. Objetivo principal

Detectar amenazas en los protocolos ARP, ICMP, TCP, TLS y DHCP de una LAN universitaria que pudieran afectar su funcionamiento. Dicha detección se puede realizar mediante la recopilación, identificación y análisis utilizando las herramientas de software libre Wireshark y NetworkMiner.

1.4.2. Objetivos específicos

Para cumplir con el objetivo principal, se plantean los siguientes objetivos específicos:

- Capturar paquetes del tráfico de una LAN universitaria utilizando el software Wireshark.
- Identificar las amenazas en los protocolos ARP, ICMP, TCP, TLS y DHCP de una LAN universitaria utilizando el software Wireshark.
- Analizar los paquetes identificados utilizando el software NetworkMiner.
- Recomendar medidas de seguridad para proteger los usuarios de una LAN universitaria.

1.5. Metas

Las metas a cumplir son las siguientes:

- Configuración del software Wireshark para capturar paquetes del tráfico en una LAN universitaria.
- Clasificación de las amenazas encontradas con base a los protocolos ARP, ICMP, TCP, DHCP y TLS.
- Estudio de las amenazas utilizando el software NetworkMiner.
- Planteamiento de recomendaciones para evitar amenazas en una LAN universitaria.

1.6. Metodología

Para la detección de amenazas en una LAN utilizando las herramientas Wireshark y NetworkMiner, se utilizará la metodología planteada por Sammir Datt [8], la cual consiste en:

- Captura: Consiste en la captura de paquetes utilizando la herramienta de software libre Wireshark.
- Identificación: Los paquetes capturados son clasificados con base a los riesgos encontrados utilizando las herramientas de software libre Wireshark y NetworkMiner.
- Análisis: Los paquetes identificados son analizados determinando la causa del riesgo y el tipo de protocolo al que pertenecen.

Se agrega la fase de recomendaciones, la cual consiste en brindar sugerencias para proteger a los huéspedes de una LAN universitaria. Considerando esta modificación, la metodología para este documento se muestra en la Figura 1.1.

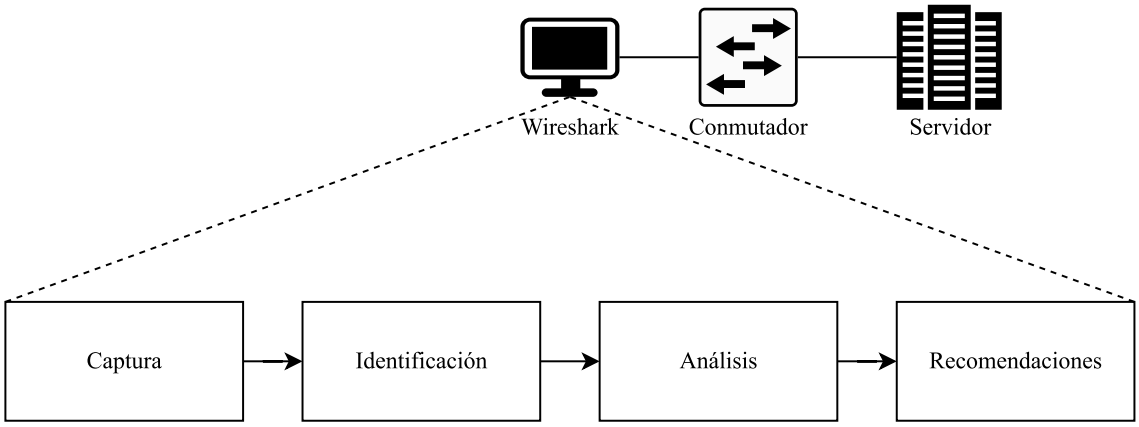


Figura 1.1: Metodología de desarrollo para la detección de amenazas en una LAN.

Capítulo 2

Seguridad en Redes

Una red de computadoras es una conexión entre dos o más nodos que pueden comunicarse entre sí. Para que una red pueda ejecutarse correctamente, deben conjuntarse tres elementos:

1. Hardware. Se encarga de hacer que la comunicación pueda llevarse a cabo. Algunos ejemplos son: computadora, concentrador, conmutador, enrutador (*router*) y tarjeta de red, entre otros.
2. Software. Hace referencia a la implementación de protocolos de comunicación, aplicaciones en servidores, aplicaciones cliente e información.
3. Usuarios. Son aquellos que transmiten o reciben información.

Kurose y Ross explican tres estructuras de red [9]:

- Red periférica (*network edge*): En ella se encuentran los huéspedes, se ejecutan aplicaciones y se utiliza el modelo cliente/servidor; por ejemplo, sitios web o servidores de correos electrónicos.
- Red central (*network core*): En ésta se encuentran nodos (enrutadores y conmutadores) para lograr la conmutación de paquetes y transferirlos a través de la red.
- Red de acceso (*access network*): Hace referencia a la infraestructura que conecta a los usuarios finales.

A su vez, las redes de acceso se clasifican en:

- Red doméstica: Se caracteriza por tener dos tipos de acceso a Internet, la línea de suscriptor digital (DSL, *Digital Subscriber Line*) y el acceso por cable.
- Red empresarial: Se utiliza una LAN para conectar el huésped al enrutador de frontera. Las tecnologías de acceso predominantes de esta red son Wi-Fi y Ethernet.
- Red móvil: Este tipo de red brinda acceso inalámbrico a dispositivos móviles para enviar, compartir y descargar desde mensajes, multimedia y transmisiones en directo, entre otros.

Para que exista una adecuada comunicación en una red de computadoras es importante saber cómo están clasificadas; uno de los criterios más importantes es su cobertura geográfica:

- Red de área local (LAN): Es un conjunto de computadoras conectadas de forma alambrada y ubicadas en un área geográficamente pequeña que permiten compartir información. Se caracterizan por trabajar con velocidades de 10 y 100 Mbps, poseen baja latencia y baja tasa de errores.
- Red de área local inalámbrica (WLAN): Este tipo de redes, comunes en centros educativos, oficinas y hogares. Proporcionan ventajas evidentes en términos de movilidad, facilidad de instalación y configuración.
- Red de área metropolitana (MAN): Es una versión más grande de LAN y está diseñada para extenderse por toda una ciudad. Una MAN puede cubrir de 30 a 100 km conectando múltiples redes situadas en diferentes lugares de una ciudad.
- Red de área amplia (WAN): Cubren una amplia área, como puede ser una ciudad, un estado o un país. Una WAN incorpora conmutadores y enrutadores.

2.1. Protocolo de Red

Un protocolo de red se define como el conjunto de reglas que deben respetarse para intercambiar información entre dos o más dispositivos así como las acciones a realizar al momento de ejecutar la transmisión y/o la recepción de un mensaje. Toda actividad que tenga que ver con Internet y que incluya dos o más dispositivos en diferente ubicación se controlan mediante un protocolo de red.

Se debe enfatizar que las redes de computadoras e Internet hacen uso extensivo de los protocolos de red con el fin de llevar a cabo las diferentes tareas de comunicación. Se utilizan varios protocolos para comunicarse entre dispositivos, de tal forma que cada protocolo de red tiene sus propias características, ventajas y desventajas. La elección de los protocolos afecta significativamente al funcionamiento y rendimiento de la red. A continuación se explican detalladamente los protocolos utilizados en este documento enfocados al análisis de paquetes, empleando el software Wireshark.

2.1.1. Protocolo de Resolución de Direcciones (ARP)

El protocolo de resolución de direcciones (ARP, *Address Resolution Protocol*) se utiliza para determinar qué dirección MAC corresponde a una determinada dirección IP. Los datos viajan a través de diferentes redes, los paquetes utilizan una dirección lógica (dirección IP) junto con el enrutamiento para entregar los datos al destino final. Para esto, la dirección MAC necesita un espacio en la cabecera de la trama (*frame*). El primer dispositivo revisará el caché[1] local y, si no hay una entrada, el dispositivo emite una solicitud ARP (*broadcast*) y esperará una respuesta. De este modo, ARP está compuesto de: a) una solicitud, la cual ocurre cuando un paquete de difusión iniciado por el huésped de origen no conoce la dirección MAC destino; b) una respuesta, la cual ocurre cuando un paquete va dirigido hacia la dirección destino. La cabecera de ARP se muestra en la Figura 2.1.

[1] Es un tipo de memoria intermedia digital que almacena los datos una vez recuperados para accesos posteriores [10].

<table>
<tr><td colspan="2">Tipo de Hardware</td><td>Tipo de Protocolo</td></tr>
<tr><td>Longitud de Hardware</td><td>Longitud de Protocolo</td><td>Operación</td></tr>
<tr><td colspan="3">Dirección de Hardware del Remitente (octeto 0-3)</td></tr>
<tr><td colspan="2">Dirección de Hardware del Remitente (octeto 4-5)</td><td>Remitente IPv4 (octeto 0-1)</td></tr>
<tr><td colspan="2">Remitente IPv4 (octeto 2-3)</td><td>Dirección de Hardware Destino (octeto 0-1)</td></tr>
<tr><td colspan="3">Dirección de Hardware Destino (octeto 2-5)</td></tr>
<tr><td colspan="3">Dirección de Destino IPv4 (octeto 2-5)</td></tr>
</table>

Figura 2.1: Formato de cabecera ARP.

En la Figura 2.2 se observa la solicitud y respuesta ARP, vista con Wireshark, sus elementos son [11]:

- Tipo de hardware: Indica el tipo de conexión para la sesión (*Ethernet, IPsec tunnel, Fiber channel*).
- Tipo de protocolo: Enumera el protocolo de interconexión usado para la sesión.
- Tamaño de hardware: Es el número de bytes en una dirección de hardware.
- Tamaño de protocolo: Indica los bytes en la dirección IP.
- Código de operación: Indica qué operación está ejecutando el emisor.
- Dirección MAC del remitente: Dirección MAC del huésped que envía la solicitud.
- Dirección IP del remitente: Es la dirección de red del emisor.
- Dirección MAC de destino: Es la dirección MAC del destino.
- Dirección IP de destino: Es la dirección de red del destino.

```
Address Resolution Protocol (request)
   Hardware type: Ethernet (1)
   Protocol type: IPv4 (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: request (1)
   Sender MAC address: HP       (3c:d9:2b:77:a1:4e)
   Sender IP address: HP.local (192.16        )
   Target MAC address: 00:00:00_00:00:00 (00:00:00:0
   Target IP address: _gateway (192.168.        )
```

(a) Solicitud ARP.

```
Address Resolution Protocol (reply)
   Hardware type: Ethernet (1)
   Protocol type: IPv4 (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: reply (2)
   Sender MAC address: _gateway (18:     :12:
   Sender IP address: _gateway (192.168.       )
   Target MAC address: HP.local (3c:d9:     :a1:4e)
   Target IP address: HP.local (192.         0)
```

(b) Respuesta ARP.

Figura 2.2: Solicitud y Respuesta ARP vista con Wireshark.

2.1.2. Protocolo de Mensajes de Control de Internet (ICMP)

El protocolo de mensajes de control de Internet (ICMP, *Internet Control Message Protocol*) se utiliza para comprobar errores y actuar como capa de información IP. Este protocolo posee varias funciones, una de las principales es la utilidad *ping*[2], la cual se encarga de enviar solicitudes de eco ICMP a un huésped remoto y obtiene un mensaje de respuesta con ICMP siempre y cuando dicho huésped esté activo. El formato de la cabecera ICMP se muestra en la Figura 2.3.

Figura 2.3: Formato de cabecera ICMP [1].

Este protocolo se utiliza para reportar problemas con el envío de paquetes IP a través de la red. Por ejemplo, puede ser usado para indicar cuando un dispositivo final no está respondiendo, cuando un nodo está sobrecargado o incluso cuando ocurre un error en la cabecera IP [13]. ICMP también se utiliza para verificar la operación correcta de los dispositivos finales y revisar que los enrutadores están enviando correctamente los paquetes a la dirección de destino específica [13].

Los mensajes ICMP se clasifican en dos categorías: a) mensajes de error, para informar de condiciones de error no transitorias; y b) mensajes de consulta, para monitorear la red enviando mensajes de solicitud y respuesta. Por ello, se dice que el protocolo ICMP realiza

[2]Un *ping* (*Packet Internet o Inter-Network Groper*) es un programa básico de Internet que permite a un usuario probar y verificar si una dirección IP de destino existe y puede aceptar peticiones. El acrónimo se inventó para que coincidiera con el término que utilizaban los submarinistas para referirse al sonido de un pulso de sonar devuelto [12].

distintas funciones indicadas en el campo Tipo. Si la función tiene distintas subfunciones, éstas se diferencian entre sí mediante el campo Código. Las funciones que sólo realizan una única tarea tienen un cero en el campo Código. [14].

- Mensajes de error: Informa los problemas que tiene un enrutador o huésped destino cuando procesa un paquete IP. Algunos son: destino inalcanzable (*destination unreachable*), *source quench*[3], tiempo excedido (*time exceded*), problema de parámetros (*parameter problem*) y redirección de mensajes (*redirection messages*).
- Mensajes de consulta: Se producen en pares, ayudan a un huésped o administradores de red a obtener información específica de un enrutador o de otro huésped.

  Por ejemplo, los nodos pueden descubrir a sus vecinos. Además, los huéspedes pueden descubrir y aprender sobre los enrutadores en su red y los enrutadores pueden ayudar a un nodo a redirigir sus mensajes [13].

  Algunos de los mensajes de consulta son: solicitud y respuesta eco *(echo request and reply)*, solicitud y respuesta de marca de tiempo (*timestamp request and reply*), anuncio de enrutador *(ruteador advertisement)* y mensajes de solicitud de enrutamiento (*ruteador solicitation messages*).

Como indica Lisa Bock [16], la cabecera de ICMP en Wireshark debe tener tres características principales, tal como se muestra en la Figura 2.4:

- Tipo (8 bits): Este campo indica la función que realiza ICMP. Por ejemplo, si es una petición de eco el campo debe de ser igual a 8; si es una respuesta de eco su valor es 0.
- Confirmación (16 bits): Tiene un valor numérico, y es utilizado para la detección de errores.

Conociendo lo anterior, el contenido dependerá de lo que ha sido enviado, que en la mayoría de las veces suele ser un error o un mensaje de consulta.

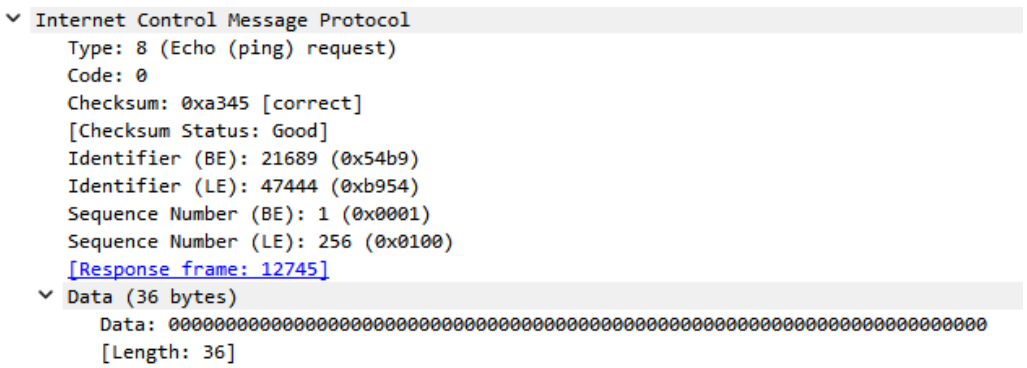


Figura 2.4: Cabecera ICMP vista con Wireshark.

2.1.3. Protocolo de Control de Transmisión (TCP)

El protocolo de control de transmisión (TCP, *Transmition Control Protocol*) es un protocolo de transporte que se apoya en IP. TCP establece una sesión de conexión antes

[3] Se trata de un mensaje nulo, indica a la fuente que el destino se encuentra congestionado, pero no proporciona ninguna información específica sobre esa situación, ni especifica qué quiere exactamente el destino que haga la fuente, aparte de reducir de algún modo su velocidad de transmisión [15].

de transmitir cualquier información; sus principales características son fiabilidad, control de flujo, secuencia, detección y corrección de errores. Cuando finaliza la transmisión de datos, la conexión se cierra. El huésped origen retransmite los datos si no recibe ninguna confirmación en cierto lapso de tiempo; a este proceso se le conoce como tiempo de espera de la conexión. El formato de la cabecera TCP se muestra en la Figura 2.5.

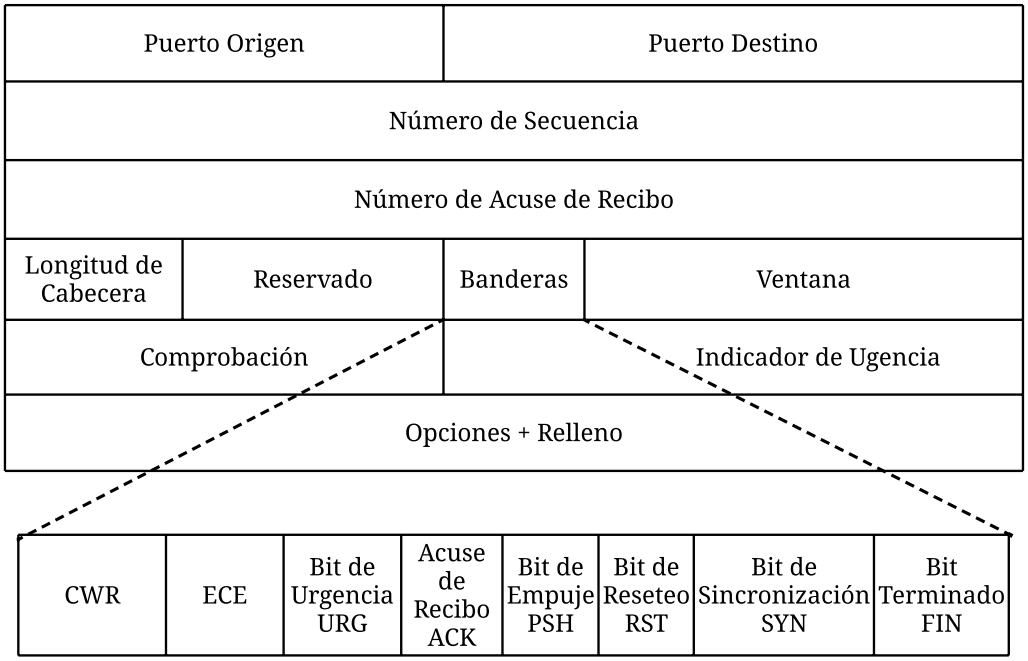


Figura 2.5: Formato de la cabecera TCP.

Las banderas TCP son:

- Sincronización (`SYN`): Solicita una conexión.
- Confirmación (`ACK`): Confirma que un paquete ha sido recibido (acuse de recibo).
- Finalización (`FIN`): Cierra una conexión con normalidad.
- Empuje (`PSH`): Termina inmediatamente una conexión.
- Urgente (`URG`): Procesa un paquete antes que el resto de los paquetes.

Un procedimiento de conexión TCP a tres vías, consiste en establecer una conexión desde el *socket*[4] cliente al *socket* servidor, como se observa en la Figura 2.6.

[4]Los *sockets* son una forma de comunicación entre procesos que se encuentran en diferentes máquinas de una red, proporcionan un punto de comunicación por el cual se puede enviar o recibir información entre procesos [17].

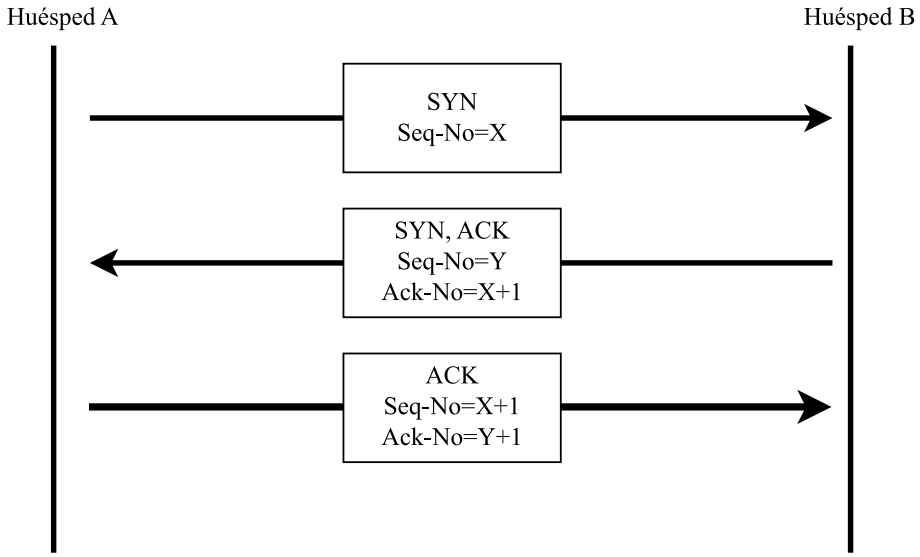


Figura 2.6: Conexión de tres vías en TCP.

Como señala James H. Baxter [18], el contenido y la longitud de la cabecera TCP en Wireshark pueden variar en función de los paquetes que se analicen, sin embargo, en la mayoría de los paquetes se encuentra lo que se observa en la Figura 2.7:

- Puerto origen y puerto destino: Se trata de puertos conocidos y registrados que se utilizan para acceder a servicios de aplicaciones (sitios web, servidores y bases de datos, entre otros).
- Número de Secuencia: Representa el primer byte en cualquier segmento dado. Los números de secuencia se inicializan al principio de las nuevas sesiones como un número aleatorio y se incrementan a medida que se envían bytes de datos.
- Número de Confirmación: Cuando el bit de bandera ACK está activado, este campo contiene el siguiente número de secuencia del remitente, que a su vez, proporciona el acuse de recibo para todos los bytes.
- Banderas: Se utilizan para controlar la configuración de las conexiones, las terminaciones y los mecanismos de control de flujo.
- Tamaño de ventana: Indica el tamaño actual del búfer para almacenar los datos recibidos hasta que puedan ser entregados a la aplicación receptora. Esta información permite al huésped emisor ajustar el flujo de datos en caso de congestión de la red.

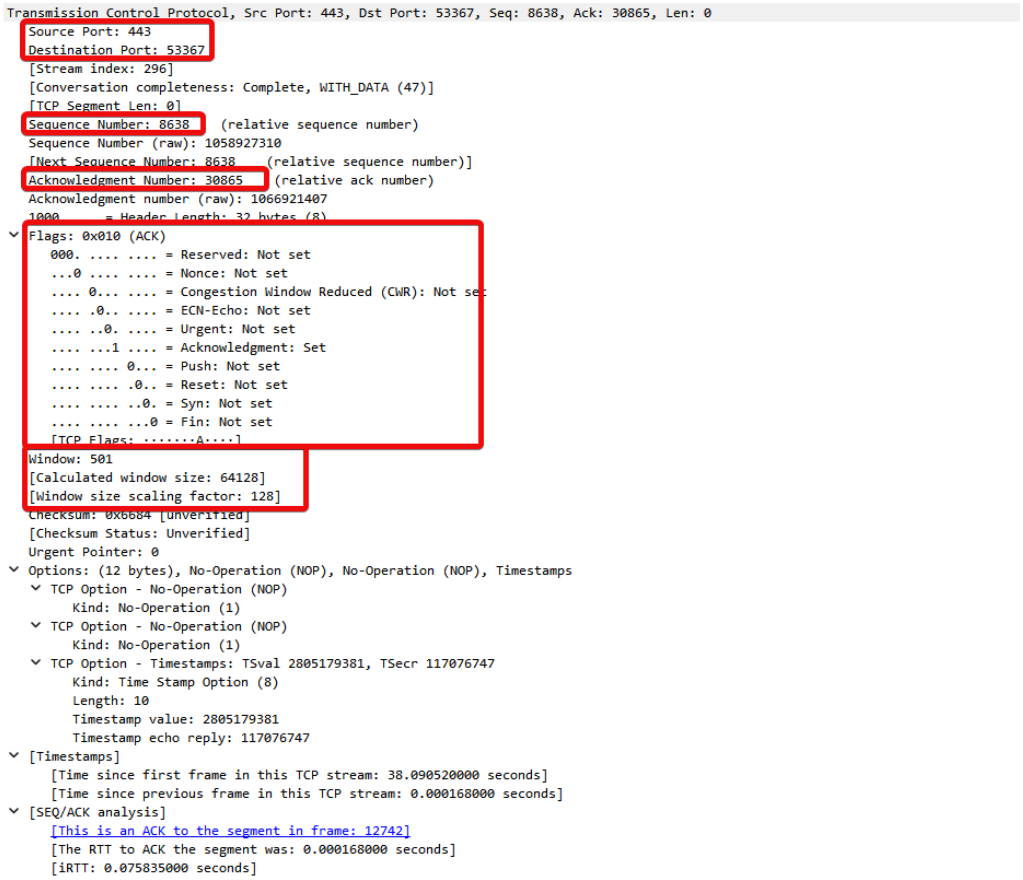


Figura 2.7: Cabecera TCP vista con Wireshark.

Como también se observa en la Figura 2.7, TCP admite una serie de opciones:

- Tamaño Máximo de Segmento: Esta opción permite especificar el número de bytes que pueden seguir a la cabecera TCP.
- Escala de Ventana: El escalado de ventana permite especificar un factor para multiplicar el tamaño de ventana anunciado y conseguir un tamaño de ventana mayor.
- TCP SACK Permitido: Indica que este nodo admite acuses de recibo selectivos, lo que permite a un nodo indicar un acuse de recibo de paquetes de datos en curso y entrantes sin dejar de solicitar un paquete específico que falta.

Finalmente, tal como menciona Lisa Bock [16], en Wireshark no sólo existen las banderas mencionadas en la Figura 2.6, si no que también están otras no tan comunes que se muestran en la Tabla 2.1.

Bandera de Control	Bits	Función
Reserved	3	Es utilizada para conexiones futuras y debería estar a 0.
Nonce	1	Es experimental, se utiliza con ECN.
CWR	1	Indica que el remitente está respondiendo a las indicaciones de cualquier red congestionada para evitar la congestión.
ECE (ECN Echo)	1	Notifica a los puntos finales de cualquier congestión en la red para evitar la pérdida de paquetes.
RST	1	El emisor y el receptor interrumpirán la conexión TCP cuando esta bandera se active. Puede ocurrir por varias razones; muchas veces, se utiliza para cerrar una conexión anormal o maliciosa.

Tabla 2.1: Banderas TCP.

2.1.4. Seguridad en la Capa de Transporte (TLS)

La seguridad en la capa de transporte (TLS, *Transport Layer Security*) se utiliza ampliamente en los servicios de seguridad de Internet. TLS evolucionó del protocolo conocido como capa de puertos seguros (SSL, *Secure Sockets Layer*). TLS es un servicio de propósito general implementado como un conjunto de protocolos que se basan en TCP.

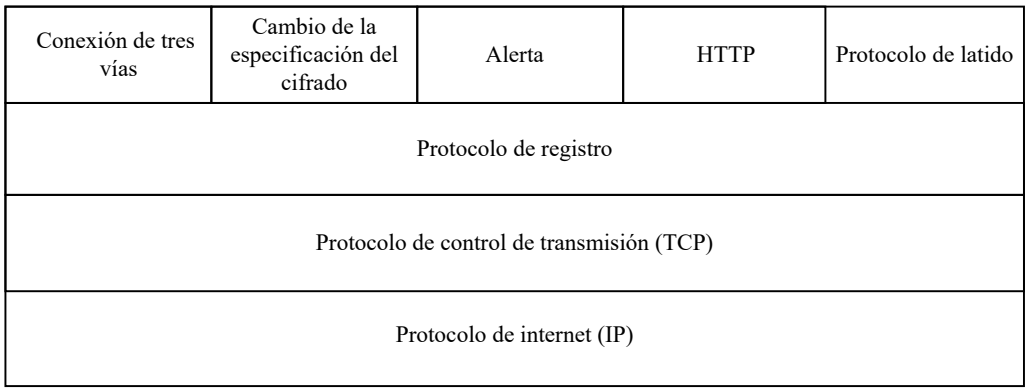


Figura 2.8: Formato de la cabecera TLS.

En la Figura 2.8 se observa la arquitectura del protocolo TLS. HTTP proveé servicios de transferencia para una interacción en la web como cliente-servidor y opera en la capa superior de TLS (véase Anexo A.1).

Los protocolos ubicados en la capa superior de TLS, protocolo *Change Cipher Spec*, conexión de tres vías y protocolo de alerta son utilizados para la administración de intercambios de clave. Existen dos conceptos importantes para TLS:

- Conexión: Es el transporte que ofrece los tipos de servicios adecuados. Todas las conexiones son asociadas con una sesión.
- Sesión: Se trata de la asociación entre un cliente y un servidor. Las sesiones se crean al momento de iniciar la conexión de tres vías y definen el conjunto de parámetros de seguridad criptográficos que pueden ser compartidos entre múltiples conexiones.

HTTPS (HTTP sobre TSL) se refiere a la combinación de HTTP y TSL para implementar una comunicación segura entre un navegador web y un servidor web. HTTPS trabaja con el puerto 443 y, cuando se utiliza, los siguientes elementos son encriptados.

- Documentos solicitados por un URL.

- Contenido de un documento.
- Contenido de la cabecera HTTP.

Es indispensable conocer las versiones de TSL para que se puedan depurar adecuadamente los problemas de conexión. La mayoría de los fallos de conexión ocurren en este proceso. En la Tabla 2.2 se muestran las versiones de TLS, el año de creación y el estado actual.

Versión	Año	Estado
SSL 1.0	N/A	N/A
SSL 2.0	1995	Descontinuado
SSL 3.0	1996	Descontinuado
TLS 1.0	1999	En uso
TLS 1.1	2006	En uso
TLS 1.2	2008	En uso
TLS 1.3	2018	En uso

Tabla 2.2: Versiones de TLS y SSL.

2.1.5. Protocolo de Configuración Dinámica de Huésped (DHCP)

El protocolo de configuración dinámica de huésped (DHCP, *Dynamic Host Configuration Protocol*) es un protocolo cliente-servidor de administración de red utilizado para asignar de forma dinámica una dirección IP a cualquier dispositivo o nodo que se encuentra en una red y se comunica mediante una dirección IP. DHCP administra de forma centralizada estas configuraciones en lugar de asignar manualmente las direcciones IPs a los distintos nodos de la red. Se puede implementar en pequeñas redes locales así como en grandes corporaciones.

DHCP trabaja en la capa de aplicación, está compuesto por un servidor y un cliente. El servidor DHCP (normalmente es un servidor o un enrutador) que se encarga de almacenar direcciones IP e información relacionada con la configuración de la red. Por otro lado, el cliente DHCP (normalmente un dispositivo final) se conecta a una red y se enlaza con el servidor DHCP. Finalmente, el relé DHCP administra las peticiones entre los clientes y servidores DHCP. La Figura 2.9 muestra la conexión entre un cliente y un servidor DHCP.

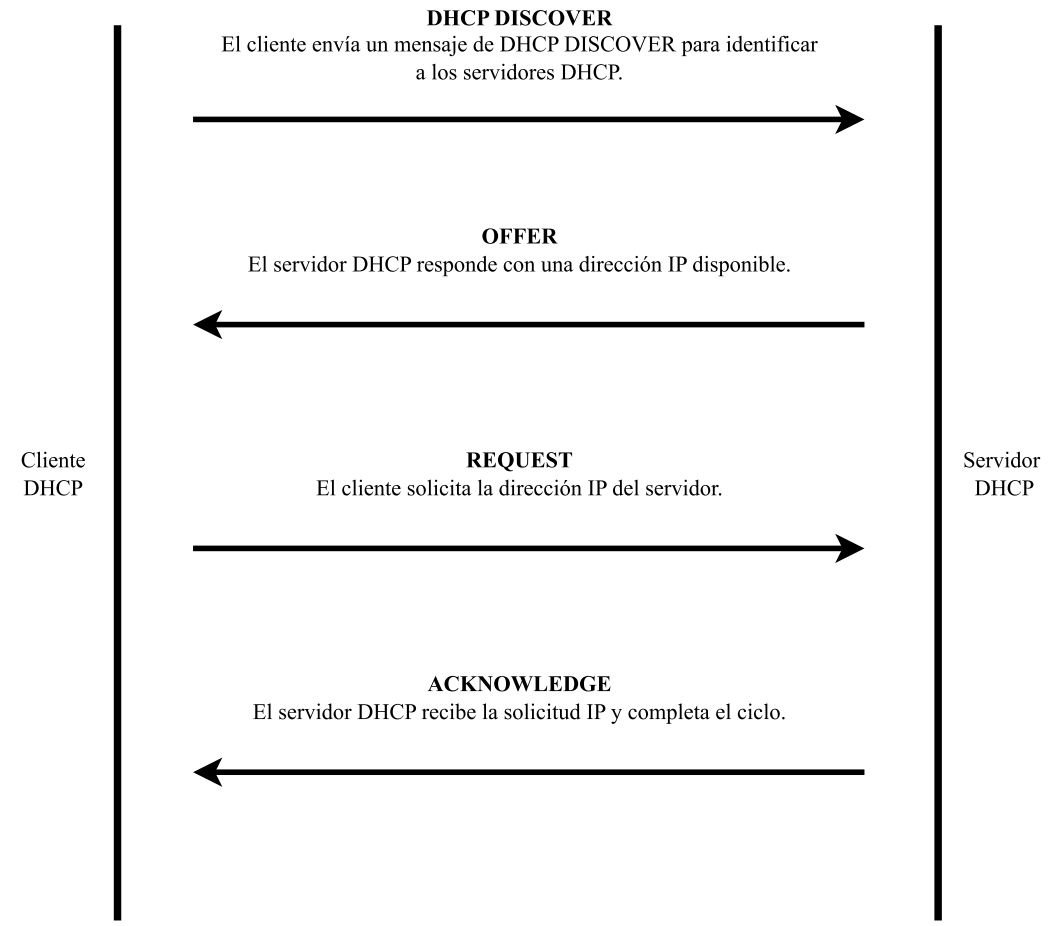


Figura 2.9: Proceso de la conexión DHCP entre un cliente y un servidor.

2.2. Cortafuegos, Servidor Proxy, IDS e IPS

Los cortafuegos son un componente fundamental de una red para la defensa del perímetro. Suele colocarse entre dos redes para actuar como puerta de enlace (véase Figura 2.10). Los principales características de un cortafuegos son [19]:

- Actuar como una puerta a través de la cual debe pasar todo el tráfico (entrante y saliente).
- Permitir unicamente el paso del tráfico autorizado.
- Ser inmune a la penetración o al ataque.

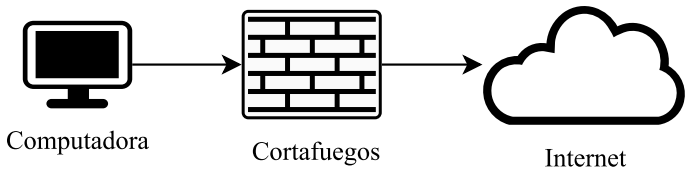


Figura 2.10: Conexión de un cortafuegos en una red.

Los cortafuegos pueden clasificarse de varias maneras; por la capa del modelo OSI en la que operan, por la tecnología que implementan o por el enfoque general que emplean.

Los enfoques empleados por los cortafuegos se pueden separar en dos categorías diferentes, cortafuegos de filtrado y cortafuegos proxy. En este caso, interesan los cortafuegos en función del nivel del modelo OSI, para ello, existen tres tipos básicos de cortafuegos [19]:

- Nivel de Red.
- Nivel de Aplicación (Servidor Proxy).
- Nivel de Circuito[5] (Servidor Proxy).

Un servidor proxy es un componente importante en cualquier red. Actúa como intermediario entre nodos de la red e Internet [8], de modo que no hay contacto directo entre un cliente de una red interna y un servidor en una red que no es de confianza (véase Figura 2.11) [19]. El servidor proxy se ejecuta en el cortafuegos, el proxy sólo es una solución de software para permitir la comunicación entre redes de forma controlada.

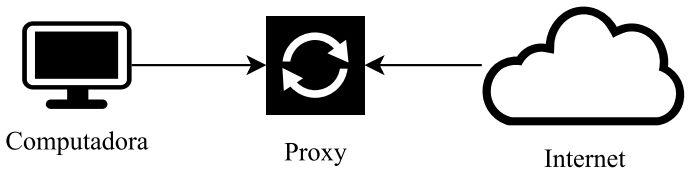


Figura 2.11: Conexión de un servidor proxy en una red.

Un servidor proxy puede utilizarse para lo siguiente [8]:

- Compartir una conexión de red en una LAN.
- Acelerar el acceso a Internet.
- Reducir el ancho de banda.
- Mantener el anonimato.
- Controlar el acceso a Internet.

Existen diferentes tipos de servidores proxy, algunos se especializan en el anonimato con el acceso a Internet, mientras que otros se encargan de almacenar tráfico en caché para optimizar el uso de los recursos de Internet. Los distintos tipos de servidores proxy, se indica a continuación:

- Servidor Proxy de Anonimato.
- Servidor Proxy Transparente.
- Servidor Proxy Distorsionador.
- Servidor Proxy Inverso.

Un sistema de detección de intrusos (IDS, *Intrusion Detection System*) es una tecnología utilizada para detectar vulnerabilidades en las tarjetas de red o computadoras (véase Figura 2.12), esta herramienta puede ser instalada sobre la red, un huésped o en un entorno físico.

[5]Conocido como cortafuegos proxy transparente, no modifica la solicitud o respuesta más allá de lo necesario para la autenticación e identificación de proxy. Un ejemplo es SOCKS (trabaja bajo cliente-servidor) [20].

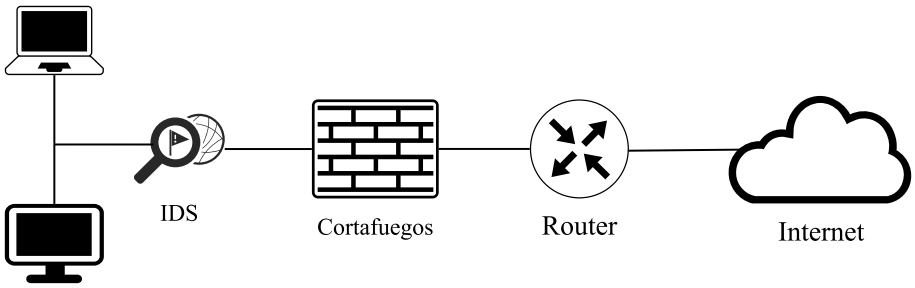


Figura 2.12: Conexión de un IDS.

Mientras que un sistema de prevención de intrusos (IPS, *Intrusion Prevention System*) recopila e identifica el comportamiento de los datos (véase Figura 2.13). Su principal función es permitir o bloquear una actividad. Se utiliza para la red, huéspedes e IDS físicos.

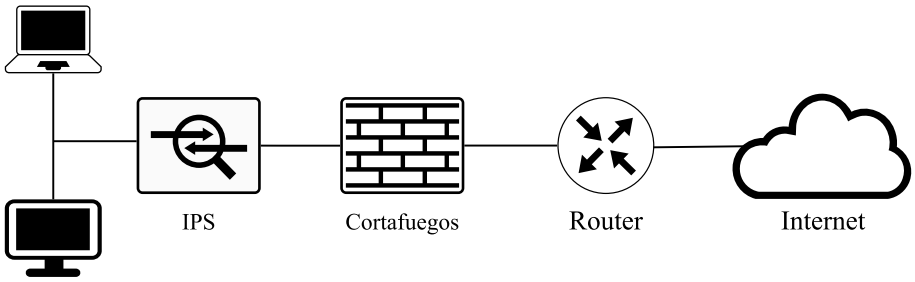


Figura 2.13: Conexión de un IPS.

El objetivo de IDS e IPS es detectar acciones que comprometan la confidencialidad, integridad o disponibilidad de una red.

2.3. Puertos en la Red

Un puerto es un punto virtual en el que se inicia y termina la conexión de una red. Están basados en software y los gestiona el sistema operativo de una computadora. Cada puerto está asociado a un proceso o servicio específico y permite diferenciar fácilmente los distintos tipos de tráfico; por ejemplo los correos electrónicos utilizan un puerto distinto del puerto utilizado por las páginas web [21].

En la Tabla 2.3 se observan los puertos de red más comunes.

Puerto	Protocolo	Descripción
22	TCP	El SSH es uno de los muchos protocolos de túnel que crean conexiones de red seguras.
25	TCP	Se utiliza para el protocolo de transferencia de correo.
53	UDP y TCP	Es utilizado para resolver los nombres de dominio a través de DNS.
80	TCP	Es utilizado por HTTP para los servicios básicos en la Web.
123	UDP	Se utiliza para sincronizar el tiempo en la red por medio del protocolo de tiempo de red (NTP, *Network Time Protocol*).
443	TCP	Versión segura y encriptada de HTTP.
500	UDP	Forma parte del proceso de establecimiento de conexiones seguras IPsec.

Tabla 2.3: Descripción de los puertos comunes en la red.

2.4. Segmentación de la red

La segmentación de la red consiste en dividir una red en varias subredes o segmentos [22]. Una segmentación típica se observa en la Figura 2.14, donde existen dos tipos de segmentación:

- Segmentación física: Consiste en el uso de cortafuegos, cableado, conmutadores entre otros nodos para separar partes de la red. La implementación de ésta resulta ser muy costosa y poco escalable.
- Segmentación virtual: Conocida como segmentación lógica, segmenta el tráfico de red mediante redes virtuales locales (VLAN, *Virtual Local Area Network)*, puede estar protegida por cortafuegos.

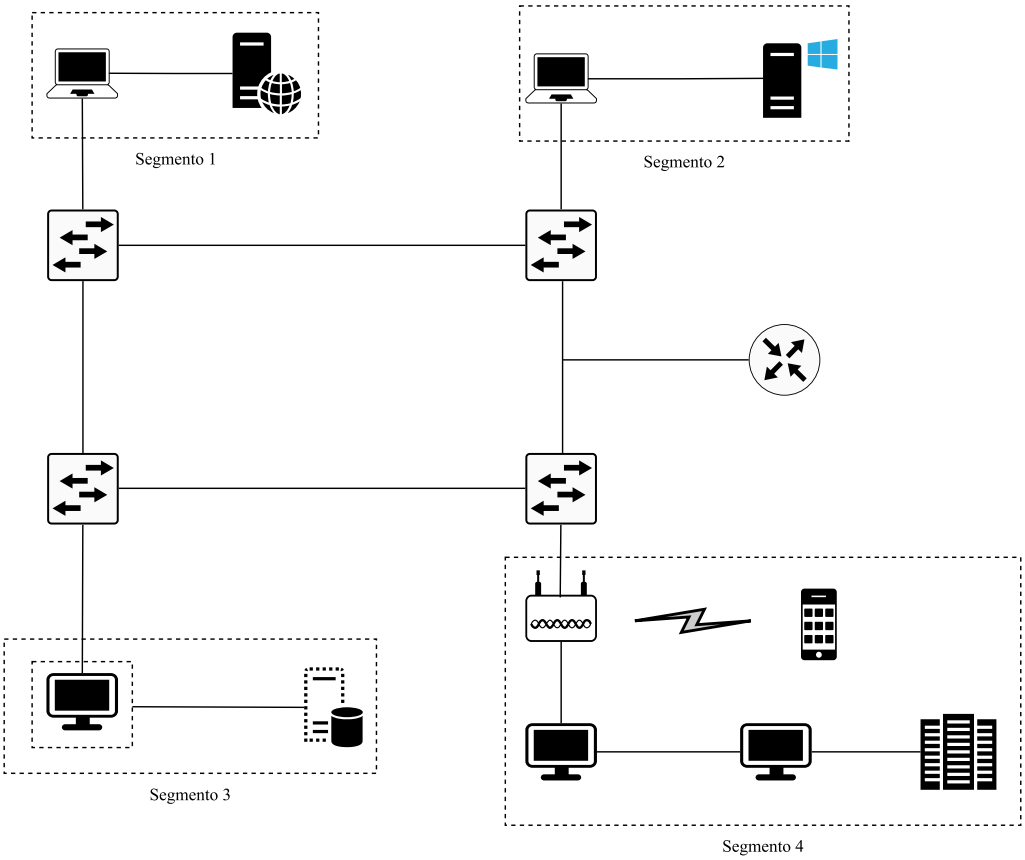


Figura 2.14: Representación de una red segmentada.

2.5. Internet

La Internet es un conjunto de redes interconectadas en las cuales viaja la información. Al acceder a un sistema que tiene conexión a Internet, una computadora puede conectarse a cientos de millones de computadoras que están conectadas a dicha red. Internet se caracteriza por usar la familia de protocolos TCP/IP, sobre los cuales opera HTTP, que se utiliza para acceder a los sitios web que están desarrollados en HTML. Hoy en día, Internet se compone de miles de redes jerárquicas superpuestas, por ello no es posible tener una descripción detallada de la topología exacta de Internet, sin embargo, se puede tener una idea general como muestra la Figura 2.15.

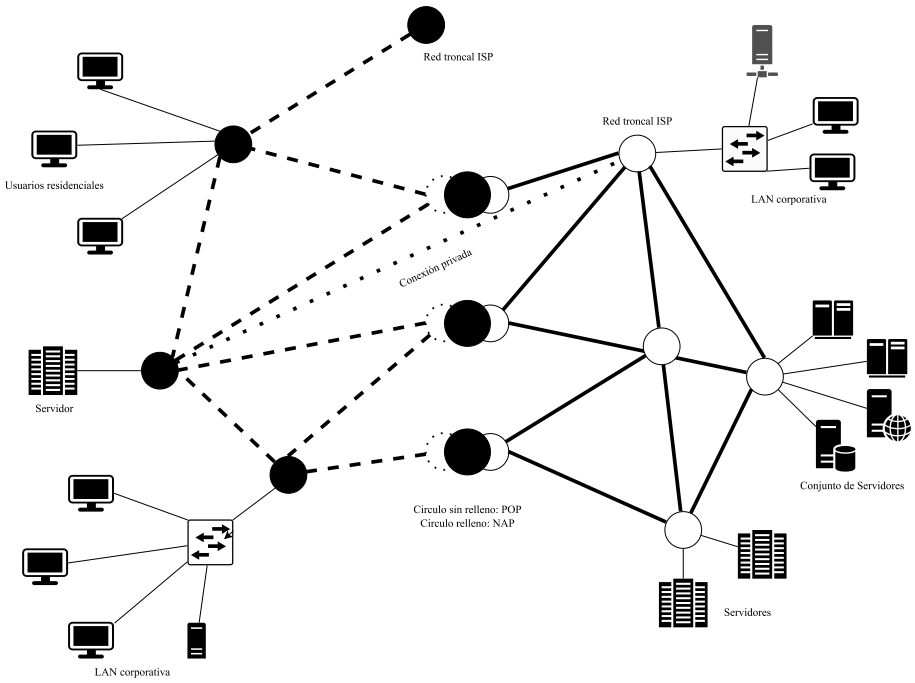


Figura 2.15: Vista simplificada de una parte de Internet [2].

Un elemento clave de Internet es el conjunto de huéspedes (nodos, dispositivos finales) conectados a ella. Huéspedes y LANs se conectan a un proveedor de servicios de internet (ISP, *Internet Service Provider*) a través de un punto de presencia (POP, *Point of Presence*). Un POP es un punto de interconexión en donde se aceptan y autentifican los usuarios. Mientras que un punto de acceso a la red (NAP, *Network Access Point*) es una instalación física que proporciona la infraestructura para mover datos entre las redes conectadas [2].

Para que el servicio de Internet se aproveche al máximo, es necesario conocer el funcionamiento de DNS e ISP, ambos servicios son pieza clave para el funcionamiento y la interacción entre usuarios e Internet.

El sistema de nombres de dominio (DNS) se utiliza para traducir los nombres de dominio de sitios web en direcciones IP. El DNS ayuda a los usuarios solicitantes a encontrar los servidores que buscan. Una zona DNS es una porción distinta del espacio de nombres de dominio en el DNS. Para cada zona, la responsabilidad administrativa se delega en un único grupo de servidores. Existe una variante, *multicast* (mDNS), el cual opera en una red local (redes pequeñas).

El ISP es la empresa que proporciona acceso a la Internet para los usuarios, así mismo, provee servicios como correo electrónico, registro de dominios, alojamiento para páginas web y paquetes de búsqueda.

2.6. Seguridad

El concepto de seguridad de redes se refiere a la protección de información en una organización, ya sea un archivo o un sistema informático. En la Figura 2.16 se muestran, de manera gráfica, los principales elementos que componen la seguridad de redes.

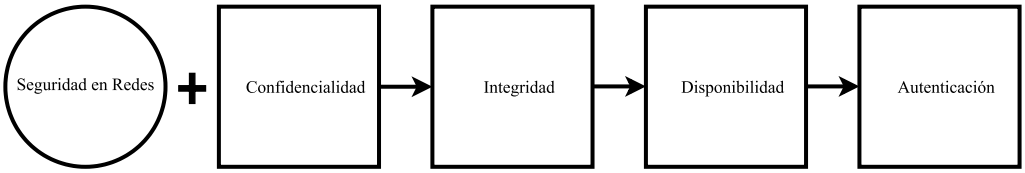


Figura 2.16: Elementos que componen la seguridad en redes de computadoras.

De los elementos de la figura anterior se observa que la seguridad de redes debe tener confidencialidad, garantizando que usuarios ajenos no intercepten, copien o repliquen la información; en segundo lugar, las organizaciones necesitan confiar en la integridad de los datos transportados o almacenados, asegurando que no se produzca una alteración, pérdida o destrucción, ya sea de manera accidental o intencional; otro elemento es la disponibilidad, la cual hace referencia a que las organizaciones puedan recuperar sus datos, perdidos o dañados, y las medidas de seguridad no sirven de nada si las organizaciones no tienen acceso a sus datos vitales que necesitan para operar cuando la requieran; finalmente, la información no es segura sin la autenticación, que determina si el usuario está autorizado para tener acceso a los datos o no.

Toda seguridad es relativa, por lo tanto, puede considerarse desde una red totalmente insegura hasta una altamente segura. Las organizaciones determinan lo que es apropiado de varias maneras, por ejemplo:

- Equilibrando el coste de la seguridad con el valor de los activos que están protegiendo.
- Equilibrando lo probable con lo posible.
- Equilibrando las necesidades del negocio con las necesidades de seguridad.

Con base en lo anterior, existen cuatro escenarios en lo que respecta a la detección de amenazas, cada uno se describe en la Tabla 2.4 [23]:

	Positivo	**Negativo**
Verdadero	**VP:** Identificado correctamente	**VN:** Rechazada correctamente
Falso	**FP:** Identificado incorrectamente	**FN:** Rechazada incorrectamente

Tabla 2.4: Escenarios en la detección de amenazas.

A continuación se explican brevemente:

1. Verdadero positivo (VP): Es cuando la amenaza analizada se clasifica correctamente como una intrusión o como dañina y no se han tomado medidas para mitigarla.
2. Verdadero negativo (VN): Cuando la amenaza se clasifica correctamente como positiva y el sistema de seguridad lo mitiga adecuadamente.
3. Falso positivo (FP): Se produce cuando la amenaza analizada es inocua o limpio en el contexto de la seguridad, sin embargo, el sistema lo clasifica como malicioso o dañino.
4. Falso negativo (FN): Cuando la amenaza analizada es maliciosa, pero se clasifica como inocua.

2.7. Diagrama General de un Sistema de Seguridad

La "triada de la seguridad" (véase Figura 2.17), conformada por prevención, detección y respuesta, constituye la base de la seguridad en una red así como el soporte de todas las políticas y medidas de seguridad que una organización desarrolla y despliega [19].

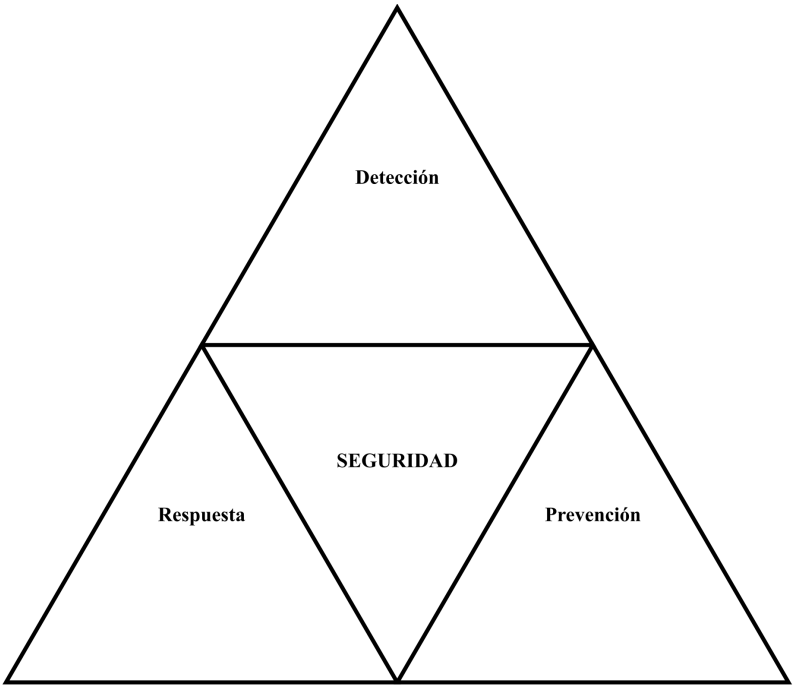


Figura 2.17: La triada de la seguridad.

A continuación se describen los elementos que constituyen dicha trinidad [19]:

- Prevención: Para proporcionar un cierto nivel de seguridad es necesario implementar medidas para prevenir la explotación de vulnerabilidades. Al momento de crear esquemas de seguridad en la red, las organizaciones deben enfatizar las medidas preventivas sobre la detección y la respuesta de posibles amenazas; es más fácil, más eficiente y mucho más rentable prevenir una brecha de seguridad que detectar o responder a una.
- Detección: En caso de que las medidas preventivas fallen, es necesario establecer procedimientos para detectar amenazas o violaciones de la seguridad. Además, es muy importante que los problemas se detecten inmediatamente; cuanto antes se detecte un problema, más fácil será corregirlo.
- Respuesta: Es necesario desarrollar un plan que identifique las respuestas apropiadas para una brecha de seguridad. El plan debe estar por escrito y debe identificar quién es responsable de qué acciones, las diferentes respuestas y los niveles de escalamiento.

2.8. Seguridad en una Red de Computadoras

Cuando se habla de la seguridad de las redes de computadoras se trata de crear un entorno seguro en una red, incluyendo a los usuarios, nodos, recursos y datos que hay en ella, tanto los que están almacenados como los que están en tránsito. Implica diseños

matemáticos más detallados de protocolos criptográficos, de comunicación, de transporte y de intercambio, así como de mejores prácticas. Garantizar la seguridad de un objeto significa protegerlo del acceso no autorizado tanto desde el interior del objeto como desde el exterior. Una red de computadoras tiene objetos tangibles que son recursos de hardware y objetos intangibles que son la información y los datos del sistema, tanto en transición como estáticos en almacenamiento [24].

Los recursos de hardware a proteger son:

- Dispositivos de entrada y punto final como teclado, ratón, pantalla táctil, monitores y computadoras portátiles.
- Dispositivos de red como concentradores, conmutadores, enrutadores, puertas de enlace y puentes.

Los recursos de software a proteger son:

- Sistemas operativos, protocolos del servidor, navegadores, software de aplicación y bases de datos.
- Programas informáticos del cliente, datos financieros, multimedia y otros archivos personales comúnmente almacenados en computadoras personales y empresariales.

2.9. Terminología de Seguridad de la Información

Es importante entender la diferencia entre un riesgo, amenaza, vulnerabilidad o un ataque en el contexto de la seguridad de la red.

Una amenaza es cualquier cosa que pueda interrumpir la operación, el funcionamiento, la integridad o la disponibilidad de una red o sistema. Esto puede tomar cualquier forma y puede ser malévolo o accidental.

Un riesgo es la posibilidad de que un recurso de una organización se pierda, se modifique, sea destruido o que sufra otras consecuencias negativas. El riesgo puede provenir de una sola amenaza o de varias amenazas o de la explotación de una vulnerabilidad [25].

Una vulnerabilidad es una debilidad inherente al diseño, configuración, implementación o gestión de una red o un sistema que lo hace susceptible a una amenaza. Las vulnerabilidades son las que hacen que las redes sean susceptibles a la pérdida de información y al tiempo de inactividad. Cada red y sistema tiene algún tipo de vulnerabilidad.

Un ataque es una técnica específica utilizada para explotar una vulnerabilidad. Existen dos categorías generales de ataques; los pasivos y los activos. Los ataques pasivos son difíciles de detectar, porque no hay actividad manifiesta que pueda ser monitoreada o detectada. Los ataques activos emplean acciones más abiertas en la red o el sistema. Como resultado, pueden ser más fáciles de detectar, pero al mismo tiempo pueden ser mucho más devastadores para una red.

Las redes y los sistemas se enfrentan a muchos tipos de amenazas. Existen virus, suplantadores de identidad, réplicas, cambio de contraseñas, ingeniería social, escaneo de puertos, denegación de servicio y otros ataques basados en protocolos.

2.10. Políticas, Estándares y Reportes

Proteger los recursos de una universidad es responsabilidad de los administradores del departamento de red. Los recursos incluyen información sensible como datos personales de alumnos e información privada de profesores y administrativos, entre otros. Al mismo

tiempo, las medidas de seguridad a menudo restringen las actividades de los usuarios, esto provoca la tentación de hacer caso omiso a las normas de seguridad dictada por los encargados de red. Sin embargo, es responsabilidad de los administradores de red configurar adecuadamente los equipos para cumplir las políticas de seguridad sin afectar, más de lo necesario, la usabilidad o capacidad de los usuarios para realizar sus actividades.

2.10.1. Política de Seguridad

La política de seguridad es un documento que define las metas de las seguridad en organizaciones, en este caso una universidad. Debe identificar los recursos necesarios para que el entorno sea seguro y un plan de respuesta en caso de que los recursos de la red sean comprometidos, también, debe incluir documentación de la configuración del servidor y procedimientos para administrar los cambios de la red. La política de seguridad debe cumplir la normativa legal, que el caso de México, el Instituto Federal de Telecomunicaciones (IFT) es el encargado de estos temas.

Una política de seguridad también debe esbozar un conjunto de normas que se espera que los usuarios sigan. Por ejemplo, puede restringir a los usuarios el uso compartido de documentos en la red, la visita a sitios web que alojen juegos o la instalación de software en computadoras. Cuanto más estricta sea una política de seguridad, más probable será que los usuarios intenten eludirla. Hay que equilibrar la facilidad de uso y los requisitos de productividad de los usuarios con la necesidad de seguridad [26].

2.10.2. Estándares

Los estándares para la administración de la seguridad en redes especifica algunas medidas para que sean implementadas en este caso por una universidad. Otros estándares de administración son descritos por las normas ISO 27001 e ISO 27032.

ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan contra cualquier amenaza, de forma que garantice en todo momento la continuidad de las actividades de una organización [27].

ISO 27032 es una norma internacional que ofrece unas líneas generales de orientación para fortalecer el estado de la seguridad en una organización, utilizando los puntos técnicos y estratégicos más importantes para esa actividad y los que están relacionados con [28]:

- Seguridad en Redes.
- Seguridad en Internet.
- Seguridad de la Información.
- Seguridad de Infraestructuras.

2.10.3. Reportes

Los reportes son documentos necesarios para informar a los encargados de la administración de la red sobre las amenazas existentes. Al desarrollarse explícitamente en un documento, el administrador tendrá el panorama amplio respecto a las áreas de intrusión o vulnerables que presenten amenazas y así solucionar los problemas encontrados con el fin de aumentar la seguridad en la red.

En el Apéndice D se muestra la estructura que debe llevar un reporte de detección de amenazas a una LAN.

2.11. Captura y Análisis del Tráfico de Red

En primer lugar es necesario conocer la definición de los siguientes términos [29]:

- Captura: Tomar datos de lo que se muestra en un momento concreto y almacenarlos.
- Análisis: Consiste en identificar los componentes de un todo, separarlos y examinarlos.

Así pues, los dos términos son la base para la detección de amenazas en una LAN.

2.11.1. Captura del Tráfico de Red

Cuando se habla de estructura de datos a nivel Ethernet, en la literatura se menciona el término "trama" para hacer referencia a la unidad de envío de datos, sin embargo, en seguridad de redes se emplea el término "paquete" como sinónimo de "trama". Según el autor Ric Miesser en su libro Network Forensics [30], cuando se captura tráfico en una LAN se está buscando información en las tramas de Ethernet. Ethernet por defecto tiene una unidad de transmisión máxima (MTU, *Maxim Transmition Unit*) de 1500 bytes, que es el tamaño máximo de los paquetes que puede enviarse usando un protocolo de comunicaciones; si el paquete es mayor a 1500 bytes, éste será fragmentado en paquetes más pequeños.

La captura de paquetes puede realizarse en diferentes sistemas operativos, tales como MS Windows, GNU/Linux o macOS X, sin embargo, este procedimiento necesita determinados privilegios, por ejemplo, la tarjeta de red debe configurarse para operar de un modo especial. Por defecto, las tarjetas de red unicamente responden a los mensajes dirigidos directamente hacia ellas o enviados a una dirección de difusión.

Cuando el direccionamiento MAC determina que el paquete no se relaciona con el huésped, entonces se descarta totalmente; dependiendo de la configuración de la herramienta que se esté utilizando para capturar el tráfico en la red. Existe una manera de deshabilitar este comportamiento y obtener todos los paquetes que están llegando a la interfaz de red. Los controladores de red soportan este comportamiento con una configuración llamada modo promiscuo para tarjetas alambradas y modo monitor para conexiones inalámbricas, en los cuales la tarjeta de red se encarga de aceptar todos los paquetes visibles y los envía a la capa de red permitiendo que sean capturados por el software; en este caso Wireshark.

Sin embargo, en una red Ethernet cableada y conmutada, el huésped ve muy poco o nada de tráfico. Se debe recordar que un conmutador sabe que hay direcciones MAC más allá de cada puerto. Debido a ello el conmutador no reenvía paquetes destinados a otros huéspedes hacia su máquina; si varias máquinas tienen un concentrador entre el usuario y el conmutador más cercano, entonces el modo promiscuo presentaría tráfico de múltiples máquinas. Si es una máquina conectada a un conmutador configurada en modo espejo, entonces el modo promiscuo revelará un poco más de información [31].

Para capturar el tráfico de una red es necesario encontrar un lugar apropiado para conectar el sistema con la herramienta a utilizar. La estructura de una red consta de varios conmutadores, concentradores, servidores y estaciones de trabajo. Lo ideal es ejecutar la herramienta de captura directamente en el servidor para analizar todo el tráfico que se mueve a través del servidor y es distribuido a las terminales finales, sin embargo, podría haber situaciones en las que el acceso físico al servidor no es posible, principalmente por razones de seguridad. A continuación se presentan algunos métodos que pueden servir para solucionar lo anterior.

2.11.1.1. Utilizando un concentrador

Un concentrador permite que todos los dispositivos conectados se comuniquen entre sí. Los concentradores no controlan el tráfico que llega a través de ellos, así pues, cualquier paquete que pasa a través de un puerto se regenera y se difunde por todos los demás puertos. Los concentradores aún están presentes en instalaciones de red antiguas. En la Figura 2.18 se muestra la conexión de un concentrador.

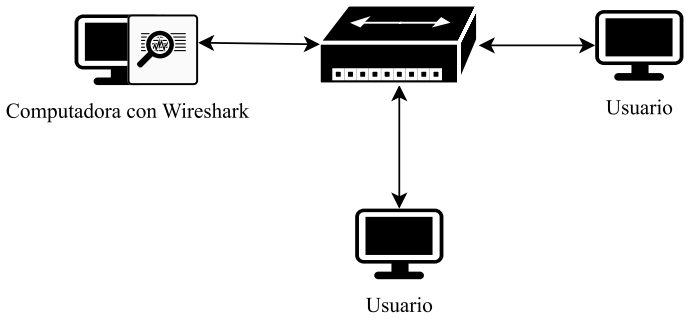


Figura 2.18: Captura del tráfico de red utilizando un concentrador.

2.11.1.2. Utilizando SPAN

Los puertos SPAN (*Switch Port Analizer*) son una característica del conmutador que se utiliza cuando se desea una copia de los paquetes que normalmente no fluyen a través de un puerto. El SPAN se utiliza principalmente para el monitoreo del tráfico de red ya que permite capturar paquetes que normalmente no se ven. Es necesario configurar los puertos de origen, que son los puertos de los cuales se desean obtener los paquetes copiados (denominados puertos espejo) y un puerto destino (denominado puerto monitor). En la Figura 2.19 se observa la configuración de un SPAN.

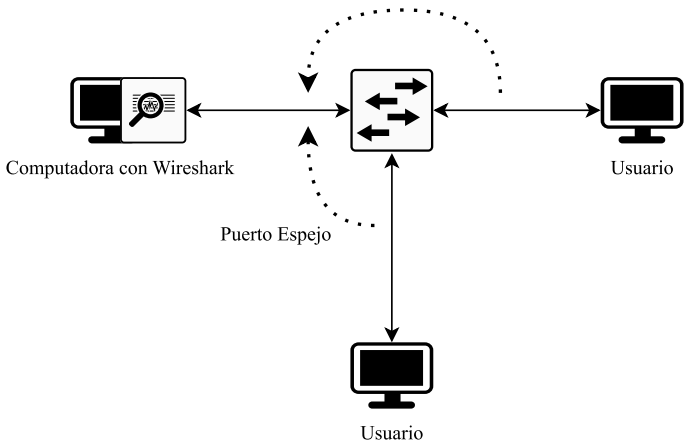


Figura 2.19: Captura del tráfico de red utilizando SPAN.

2.11.2. Análisis del tráfico de red

Algunos autores denominan al análisis de tráfico de red como análisis de paquetes y es una serie de técnicas que los ingenieros y técnicos de redes utilizan para estudiar las propiedades de las redes, incluyendo la conectividad, la capacidad y el rendimiento. El análisis de redes puede utilizarse para estimar la capacidad de una red existente, observar las características de rendimiento o planificar futuras aplicaciones y actualizaciones [32].

Dominar este arte es una habilidad bien afinada y puede lograrse si un administrador de red tiene una sólida comprensión del conjunto de protocolos TCP/IP, está familiarizado con los flujos de paquetes y tiene un excelente dominio de cualquier analizador de paquetes de su elección [33].

El análisis de paquetes puede ayudar a un administrador a:

- Supervisar y proporcionar una estadística detallada de las actividades en la red.
- Distinguir entre el tráfico normal y el inusual.
- Realizar diagnósticos de red.
- Identificar y resolver los problemas de rendimiento de la red, como la utilización excesiva del ancho de banda.
- Realizar una inspección profunda de paquetes.
- Investigar violaciones de la seguridad.

2.12. Analizadores de Red

Los analizadores de red son herramientas utilizadas para capturar datos de la red. Existen varios tipos de programas de detección de paquetes, tanto gratuitos como comerciales. Cada programa está diseñado con objetivos diferentes. Algunos programas populares de análisis de paquetes son:

- tcpdump: Disponible en GNU/Linux y Widows, no posee interfaz gráfica y se basa en diferentes comandos. Se enfoca solamente en capturar una interfaz, guardar los paquetes capturados en archivos con extensión `.pcap` y capturar paquetes fallidos, entre otros.
- Tproxy: Está enfocada para GNU/Linux y macOS X. Es una herramienta que funciona a base de comandos únicamente para conexiones proxy. También inspecciona solicitudes y respuestas HTTP.
- Fiddler: Herramienta gratuita, centrada en rastrear tráfico HTTP/HTTPS. Se pueden manipular sesiones, realizar pruebas de seguridad y pruebas de rendimiento.
- OmniPeek: Herramienta comercial, que permite visualizar el rendimiento de la red mediante diferentes gráficas, funciona como herramienta forense, es decir, utiliza capacidades de bajo nivel y cuadros de mando completos.
- Capsa: Herramienta comercial para analizar protocolos, admite más de 1000 protocolos, así mismo, detecta las amenazas y los ataques que ha sufrido la red. Puede monitorear y leer archivos ya capturados con extensión `.pcap`.
- Nmap: Herramienta gratuita disponible para Windows, macOS y GNU/Linux. Se utiliza para escanear los puertos de una red con el objetivo de obtener información importante sobre la misma para administrar su seguridad. Posee diferentes tipos de escaneo, los más populares son: *ping*, arp, conexión TCP y FIN.
- Snort: Herramienta gratuita de código abierto. Funciona para rastrear y monitorear paquetes en tiempo real. Detecta intrusiones en la red, muestra los paquetes que transitan por la red y almacena los paquetes detectados en el modo *sniffer* para guardarlos en el disco duro.

2.13. Wireshark

Conocido originalmente como Ethereal, Wireshark es un analizador de paquetes de red que presenta los datos de los paquetes capturados con el mayor detalle posible. Se puede considerar un analizador de paquetes de red como un dispositivo de medición para examinar lo que ocurre dentro de un cable de red. En el pasado, estas herramientas eran caras, propietarias o ambas cosas. Sin embargo, con la llegada de Wireshark, eso ha cambiado. Wireshark está disponible de forma gratuita, es de código abierto y es uno de los mejores analizadores de paquetes disponibles en la actualidad para Windows, GNU/Linux y macOS X [34].

Cuando Wireshark captura los datos de la red necesita saber cómo interpretar los paquetes presentes en la red y los ya capturados; a este procedimiento se le conoce como decodificación de protocolos.

Frecuentemente, el número de protocolos que un software de monitoreo puede observar, capturar y analizar determina su potencial, por lo que la mayoría de herramientas que sirven para el estudio del tráfico en la red soportan cientos de protocolos. Wireshark es competitivo en esta área, con soporte actual de más de 750 protocolos y se añaden constantemente nuevos protocolos. Los decodificadores de protocolos, también conocidos como disectores, pueden añadirse directamente al código o incluirse como *plug-ins* [35].

2.13.1. Interfaz gráfica de usuario

La interfaz gráfica de usuario (GUI, *Graphical User Interface*) de Wireshark es configurable y fácil de usar. La Figura 2.20 muestra la pantalla de bienvenida.

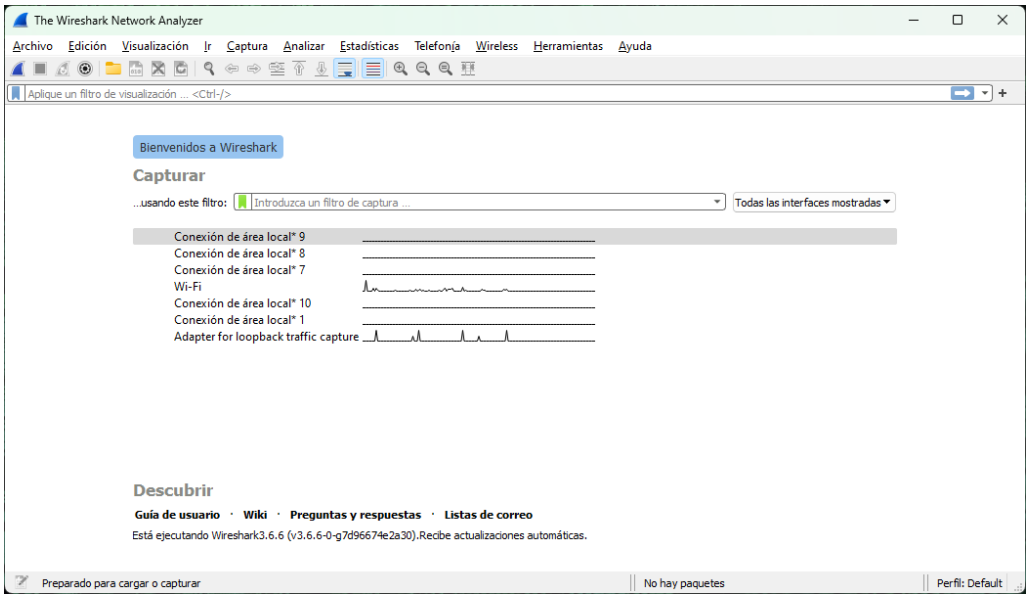


Figura 2.20: Pantalla de bienvenida en Wireshark.

Existen seis secciones principales en la GUI de Wireshark (véase Figura 2.21):

1. Barra de menú: En esta sección se muestran las diferentes herramientas organizadas por su función.
2. Barra principal de herramientas: Aquí se encuentran las herramientas de uso frecuente.

3. Listado de paquetes capturados: En esta sección se muestran todos los paquetes capturados por Wireshark con información general.

4. Información concreta de un paquete: Esta ventana muestra detalles relativos al paquete seleccionado en el panel de la lista de paquetes. Por ejemplo, se pueden ver las direcciones IP de origen y destino y los diferentes protocolos utilizados para la comunicación ordenados en el enfoque inferior-superior (capa de enlace a capa de aplicación). La información relativa a los paquetes aparece en diferentes categorías de protocolos que pueden ampliarse para obtener más detalles del paquete seleccionado [36].

5. Vista de bytes en hexadecimal: Muestra las tramas de cada paquete.

6. Barra de estado: Muestra detalles como el total de paquetes capturados.

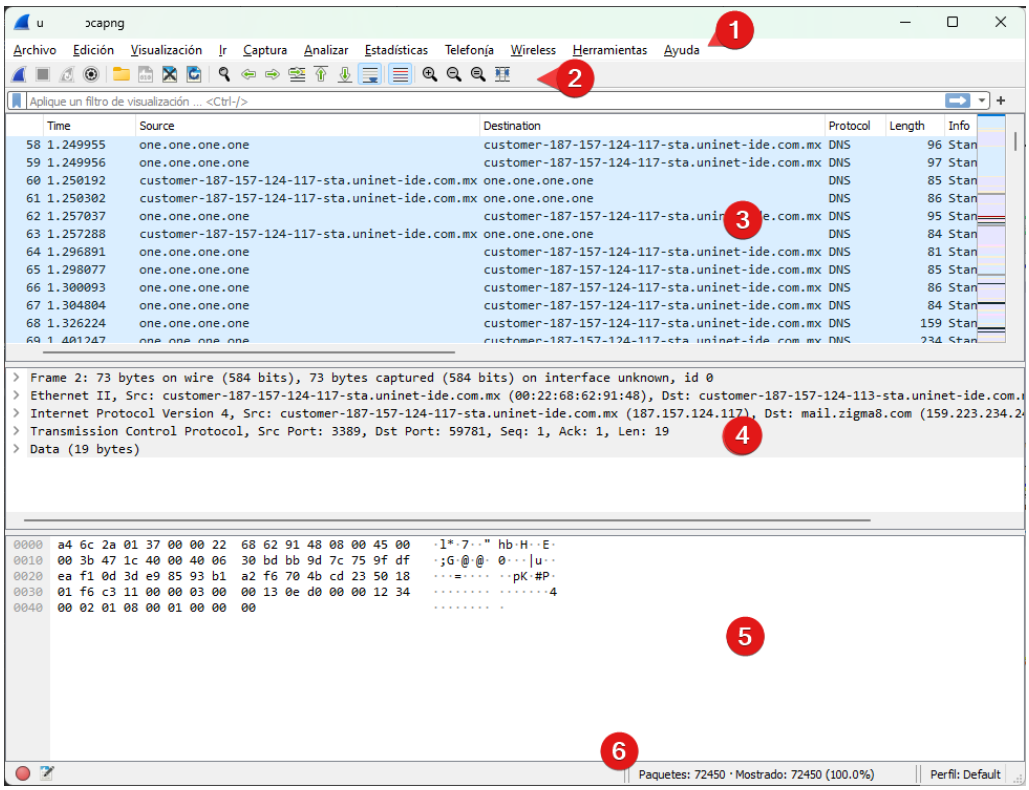


Figura 2.21: Interfaz gráfica de usuario de Wireshark.

Cabe mencionar que a veces no se puede ver ningún paquete en la sección de listado de paquetes capturados. Existen múltiples razones, algunas son:

- No hay tráfico en la red.
- Los paquetes que viajan en la red no están destinados al dispositivo.
- No está habilitado el modo promiscuo o no tiene una opción para activar el modo promiscuo.

2.13.2. Filtros de captura y de visualización

Cuando se capturan paquetes en una red, se pueden capturar todos los paquetes proporcionados por la tarjeta de red de la computadora.

Wireshark proporciona dos tipos de filtros: a) filtros de captura, configurados antes del inicio de la captura y b) filtros de visualización, se pueden utilizar durante la captura o en un archivo ya existente.

Los filtros de captura le permiten a Wireshark analizar únicamente paquetes de interés. Se utilizan antes de iniciar una captura, no se pueden aplicar a un archivo de captura existente y se aplican cuando se sabe exactamente lo que se busca. Estos filtros funcionan de modo que todo el tráfico pasa primero por el filtro de captura y posteriormente es enviado al motor de captura para su procesamiento. La Tabla 2.5 lista los filtros de captura más importantes.

Filtros de captura	Descripción
`ether host <Client's MAC>`	Tráfico cliente y servidor, basado
`and ether host <Server's MAC>`	en sus respectivas direcciones MAC
`port bootpc`	Unicamente trafico DHCP
`ip6`	Solamente tráfico IPv6
`ip proto 1`	Unicamente tráfico ICMP
`udp dst port 162`	Respuestas SNMP

Tabla 2.5: Filtros de captura.

Los paquetes visualizados en la interfaz de Wireshark, ya sea en tiempo real o abriendo un archivo existente, pueden ser demasiados. En estos casos Wireshark proporciona filtros de visualización que le permiten especificar qué paquetes se muestran en la interfaz [35]. Estos filtros de visualización son útiles para el análisis puesto que sólo se centran en paquetes específicos basándose en criterios definidos.

Detección de Huéspedes	
`arp.dst.hw_mac == 00:00:00:00:00:00`	Escaneo ARP
`icmp.type==3 && icmp.code==2`	Escaneo IP
`icmp.type==8 || icmp.type==0`	Barrido de *ping* ICMP
`tcp.dstport==7`	Barrido de *ping* TCP
Detección de exploración de puertos de red	
`tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.window_size<=1024`	Exploración TCP SYN
`tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.window_size>1024`	Exploración de Conexión TCP
`tcp.flags==0`	Exploración TCP Null
`tcp.flags==0x001`	Exploración TCP FIN
`tcp.flags.fin==1 && tcp.flags.push==1 && tcp.flags.urg==1`	Escaneo TCP Xmass
`(tcp.flags&02 && tcp.seq==0) || (tcp.flags&12 && tcp.seq==0) || (tcp.flags.ack && tcp.seq==1 && !tcp.nxtseq > 0 && !tcp.ack >1) || tcp.flags.fin == 1 || tcp. flags.reset ==1`	Detecta e inspecciona sesiones normales configuraciones/desmontajes/reinicios
Detección de ataques a la red	
`arp.duplicate-address-detected || arp.duplicate-address-frame`	Suplantación ARP
`icmp && data.len > 48`	Inundación ICMP
`dtp || vlan.too_many_tags`	VLAN en espera
`tcp.analysis.lost_segment || tcp.analysis.retransmission`	Pérdida y retransmisión de paquetes
`tcp.flags.reset eq 1`	Interrumpe conexiones TCP anormales o maliciosas.
Detección de Fallos en la Conexión TLS	
`tls.record.content_type == 21`	Alertas TLS

Tabla 2.6: Filtros de visualización.

2.13.3. Técnicas esenciales de Wireshark

Wireshark proporciona funciones para analizar paquetes, éstas se encuentran en el menú Estadísticas.

La función Propiedades del archivo de captura se utiliza para mostrar los detalles del archivo, visualizar el tiempo de captura, mostrar detalles de la captura y de visualización, los detalles importantes son: tiempo de captura y duración, características del sistema operativo y de Wireshark, interfaz de captura, cualquier filtro de visualización o de captura utilizado, tamaño promedio de paquetes/seg y promedio de bytes/seg.

Jerarquía de protocolo es una función que proporciona la distribución de los protocolos en el archivo de captura.

La función Conversaciones permite ver la comunicación entre dos entidades o puntos finales, las conversaciones ocurren en diferentes capas tales como la capa de red y transporte.

Un punto final es un lado de la conversación y puede ser Ethernet, IPv4, y otras opciones que son visibles como pestañas en la ventana de Puntos Finales. Esta herramienta muestra columnas que reflejan el país, ciudad, latitud y longitud, sin embargo, es necesario configurar Wireshark con una herramienta extra llamada *Maxmind*.

Por otro lado, Información especializada es una función que arroja un registro de amenazas que detecta automáticamente Wireshark. Cuando se tiene una captura con un número muy elevado de paquetes y no se pretende buscar una situación específica. La idea principal de esta herramienta es mostrar comportamientos inusuales o amenazas en la red. De esta

forma se pueden identificar rápidamente problemas en la red que si se hiciera de forma manual, sobre todo el conjunto de paquetes capturados. Esta función se encuentra en la pestaña Analizar, permite clasificar las conversaciones en Errores, Advertencias, Notas y Conversaciones. Describe de manera general los problemas que se presentan en el archivo con los paquetes capturados, se trata de la herramienta más indispensable en Wireshark para hallar amenazas, ataques y problemas que existan en la red. Con base a esta herramienta se pueden crear filtros para que después se detecten los problemas en tiempo real. Esta opción de Wireshark permite obtener un análisis en términos generales para después realizar un análisis detallado. La información mostrada se debe tratar como una recomendación. Una ausencia de resultados no significa que no existan problemas. La cantidad de entradas mostradas depende del protocolo utilizado. A lo largo de este documento se estará utilizando de manera constante.

En la Tabla 2.7 se muestra las diferentes categorías de Información Especializada

Categoría	**Color**	**Significado**
Error	Rojo	Problema grave, como un paquete mal formado o un nuevo fragmento que se superpone a datos antiguos.
Advertencia	Amarillo	Puede existir alguna amenaza o ataque.
Nota	Cían	Notas generales de interés que, muchas veces, forman parte de una conexión. Las notas también pueden enumerar errores inusuales o un uso no estándar de un protocolo.
Chat	Gris	Especifica el flujo de trabajo típico y el cambio de estado, como una conexión o una actualización de Windows.

Tabla 2.7: Categorías de Información Especializada.

A su vez, la información general es clasificada en los siguientes grupos, [37]:

- Checksum: La suma de comprobación no es válida.
- Secuencia: Secuencias de protocolos sospechosas, por ejemplo duplicación de direcciones IPs o retransmisión de paquetes.
- Protocolo: Violación de las especificaciones del protocolo, por ejemplo, valores del campo inválidos o longitudes ilegales.
- Mal formados: Paquetes mal formados o en el análisis se produjo un error.

2.14. NetworkMiner

NetworkMiner es otra herramienta de software libre para el análisis de paquetes de red. Esta herramienta también puede utilizarse para capturar paquetes, sin embargo, es más útil para el análisis de paquetes. NetworkMiner detecta sistemas operativos, direcciones IPs, nombres de huéspedes y puertos abiertos, entre otros. La extensión de archivos que puede leer es `.pcap` [38]. NetworkMiner posee una pestaña denominada Anomalies, la cual permite mostrar los posibles problemas en determinados paquetes, esta opción acelera el proceso de análisis y búsqueda de amenazas para el estudio de paquetes. Durante el desarrollo de este documento se utilizará de manera constante.

En la Figura 2.22 se observa la interfaz gráfica de usuario de NetworkMiner.

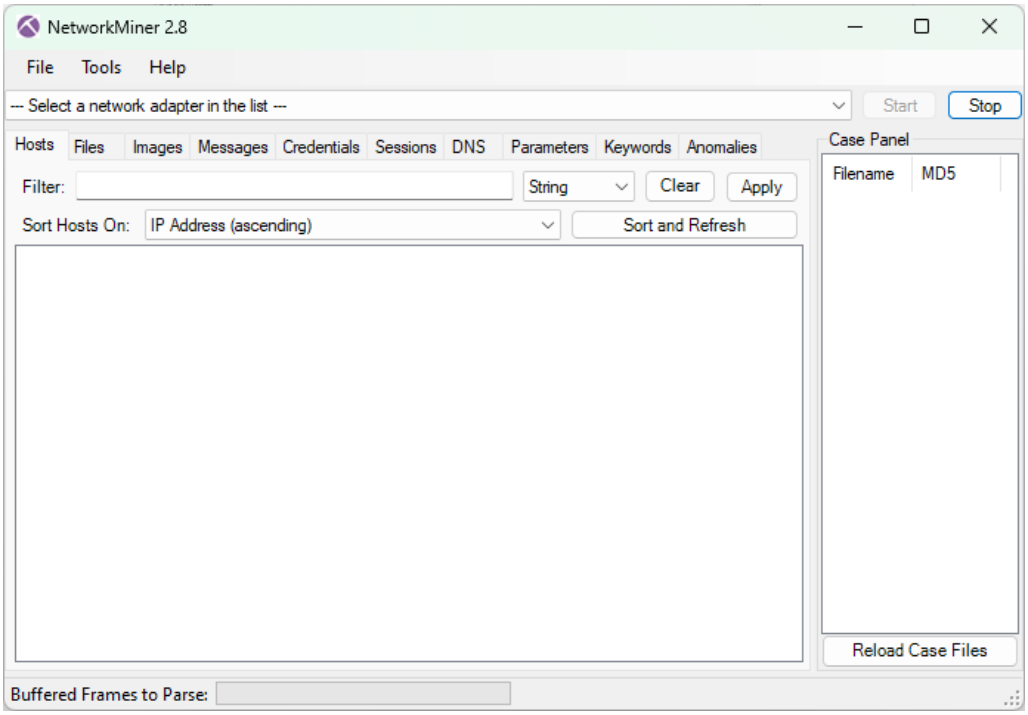


Figura 2.22: Interfaz gráfica de usuario de NetworkMiner.

Capítulo 3

Identificación de Tráfico Sospechoso

En la Figura 3.1 se muestran algunos de los ataques que ocurren en cada capa del modelo de referencia OSI, el cual es ampliamente utilizado para describir la comunicación entre los nodos de una red de computadoras. Estos ataques representan diversas formas en las que los nodos y dispositivos finales pueden ser comprometidos, desde ataques en la capa física hasta ataques en la capa de aplicación. En cada capa del modelo OSI, los ataques se vuelven más sofisticados y aprovechan diferentes vulnerabilidades en los protocolos y servicios utilizados en cada capa. Comprender e identificar estos ataques es fundamental para proteger los nodos y dispositivos finales de posibles amenazas e intrusiones para garantizar la seguridad de la red.

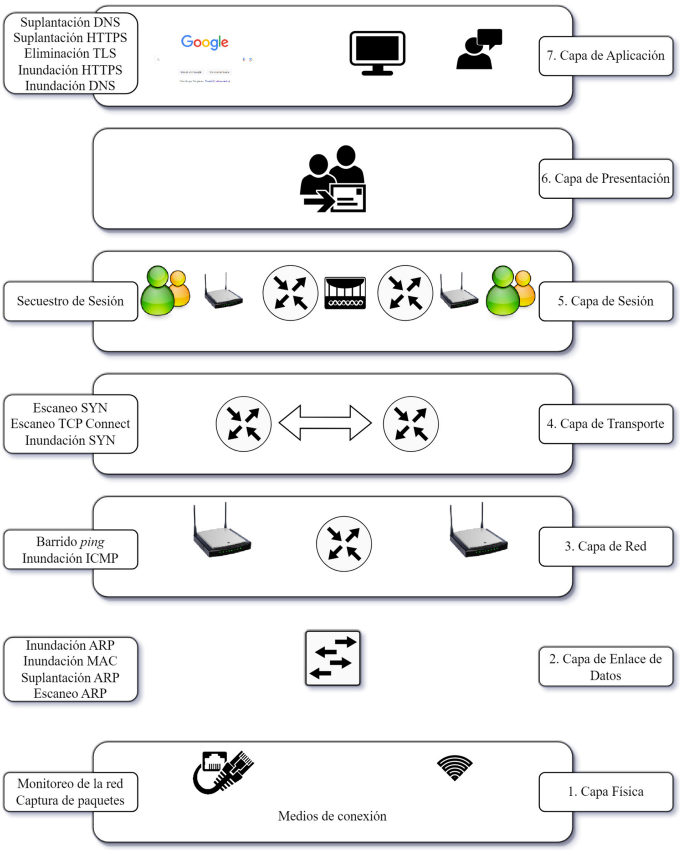


Figura 3.1: Ataques que se producen en las diferentes capas del modelo de referencia OSI.

A continuación se describen las amenazas a la seguridad de una LAN y cómo se puede

utilizar Wireshark para analizarlas. Las amenazas a la seguridad han sido implacablemente inventivas con diferentes tipos de ataques y están en constante evolución [33]. Detectarlas es tan importante como prevenirlas.

Cuando se detectan amenazas en una red es imprescindible conocer los ataques que pueden ser ejecutados; por tal motivo Jessey Bullock y Jeff T. Park clasifican los diferentes ataques que ocurren sobre la red en dos categorías [31]:

- Hombre en el Medio (MitM, *Man in the Middle*).
- Denegación de Servicio (DoS, *Denial of Service*) y Denegación de Servicio Distribuido (DDoS, *Distributed Denial of Service*).

Es necesario saber que un escaneo de puertos es la primera fase de cualquier ataque a una red, dicho con palabras de Jayant Gadge y Anish Anand Patilse [39], se realiza con el fin de localizar, recopilar, identificar y registrar información sobre el objetivo, también plantean los siguientes fases de un ataque para escaneo de puertos (véase Figura 3.2).

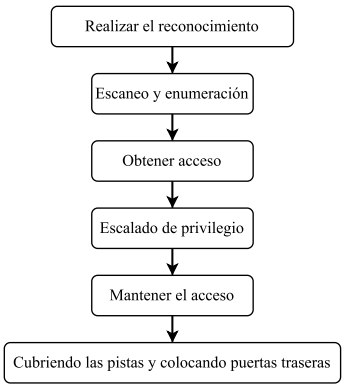


Figura 3.2: Fases de un ataque.

Al realizar el escaneo, el atacante recopila toda la información que está a su alcance, desde la identificación de las máquinas activas, la búsqueda de puertos abiertos, puntos de acceso, datos del sistema operativo hasta el mapeo de la red. Existen dos tipos de escaneo:

- Escaneo de fuerza bruta: Se realiza de forma agresiva y establece una conexión completa con el objetivo e inspecciona si el puerto está abierto. Debido al establecimiento de una conexión completa, es posible detectar su presencia. Así, cuando llega un gran número de paquetes SYN para solicitar una conexión desde una única dirección IP en múltiples puertos de la máquina objetivo, esto indica que se está utilizando un escaneo de fuerza bruta para buscar puertos abiertos.
- Escaneo sigiloso: No establece una conexión completa con el objetivo, envía solamente un paquete con una bandera particular al objetivo; basándose en la respuesta se puede entender si los puertos están abiertos o no.

Los escaneos que pueden realizarse en una red son:

- Escaneo SYN: Consiste en un gran número de paquetes con la bandera SYN llegando al destino. En este escaneo no se completa la conexión de tres vías y corta la conexión después de que la víctima responda con un SYN/ACK. Esto indica que el puerto está abierto. Es un escaneo fácil de identificar si en la captura de paquetes existe un gran número con la bandera SYN.

- Escaneo de Conexión TCP: Se caracteriza por tener un gran número de conexiones establecidas con la víctima en diferentes puertos. Establece una conexión en los puertos indicados que corresponden al puerto abierto. Al establecer la conexión e identificar los puertos abiertos se cierra la conexión. Al tratarse de una conexión completa interfieren las opciones TCP, éstas son: marca de tiempo y acuse de recibo de secuencia. Al momento en que un huésped en particular realice muchas conexiones en diversos puertos durante un lapso de tiempo muy corto se deduce que un escaneo de conexión proviene de esa máquina.
- Escaneo ACK: Llega al destino un gran número de paquetes con la bandera ACK activada. La conexión de tres vías no se completa en este escaneo y después de que la víctima responde con un SYN/ACK se corta la conexión indicando un puerto abierto. Si existe un gran número de paquetes con la bandera ACK proveniente de un único huésped se confirma que existe un escaneo.
- Escaneo FIN: Se trata de un escaneo en el cual un gran número de banderas FIN llegan al destino. El puerto indicará que se encuentra cerrado sí y sólo sí el destino responde con un RST.
- Escaneo Nulo: Se caracteriza porque llega al destino un gran número de paquetes sin bandera. Los paquetes son ignorados por los puertos abiertos mientras que los puertos cerrados responden con RST. Se puede identificar fácilmente si existe un gran número de paquetes con la bandera no establecida en ellos.
- Escaneo XMAS: Las banderas FIN, PSH y URG son activadas en este escaneo. Los paquetes son ignorados por los puertos abiertos, mientras que los cerrados responden con un RST. Este escaneo se identifica fácilmente si hay un gran número de paquetes con las banderas mencionadas provenientes de un único huésped.

3.1. Hombre en el medio (MitM)

El ataque hombre en el medio intercepta o retransmite el tráfico entre dos o más puntos finales (véase Figura 3.3). El atacante, opera entre las dos partes, por lo que es el “hombre en el medio” [31]. El atacante MitM puede interceptar, modificar, cambiar o reemplazar el tráfico de comunicaciones de las víctimas. Además, las víctimas no son conscientes del intruso, por lo que creen que el canal de comunicación está protegido [40].

Figura 3.3: Ataque de hombre en el medio.

Los tipos de ataques MitM se describen en las siguientes secciones.

3.1.1. Suplantación IP

El ataque de suplantación (*Spoofing Attack*) se considera un ataque más complejo, pues el atacante debe ser capaz de formar y enviar paquetes IP sin procesar con cabeceras IP y TCP válidas. Para que un ataque de suplantación tenga éxito, es primordial elegir la

dirección IP a falsificar, posteriormente, el equipo de la víctima no deben responder a los SYN-ACKs que se les envían.

Un atacante podría falsificar una dirección de la víctima que sabe que no responderá a los SYN-ACKs, ya sea porque no existe máquina con esa dirección, o debido a alguna otra propiedad de la dirección o la configuración de la red. Otra opción es falsificar muchas direcciones de origen diferentes, bajo la suposición de que algún porcentaje de las direcciones falsificadas no responderán a los SYN-ACKs. Esta opción se logra ya sea recorriendo una lista de direcciones de origen que se sabe que son deseables para el propósito, o generando direcciones dentro de una subred con propiedades similares. Si una sola dirección de origen es falsificada repetidamente, esta dirección es fácil de detectar y filtrar para el receptor [41].

3.1.2. Suplantación DNS

La suplantación DNS (*DNS spoofing*) también es conocida como *DNS cache poison*. Es uno de los ataques importantes y ampliamente considerados que se producen para el DNS. El servidor de caché local del DNS conserva la información IP de los últimos nombres de dominio consultados, lo que puede reducir el número de consultas a los servidores raíz y mejorar aún más la eficacia del funcionamiento del DNS. El DNS adopta principalmente el protocolo IP del usuario con mecanismos de confianza sencillos, lo que ofrece muchas posibilidades a los atacantes y redirigen a un sitio web malicioso [42]. En la Figura 3.4 se observa el modo de operación de suplantación DNS. Los pasos son:

1. El cliente realiza una solicitud a un sitio web dirigiéndose al servidor DNS para obtener la dirección IP del sitio web.
2. El atacante toma el control del servidor DNS y agrega entradas falsas al servidor DNS.
3. Finalmente, redirigen al cliente a un sitio web falso mediante la entrada falsa en el servidor DNS.

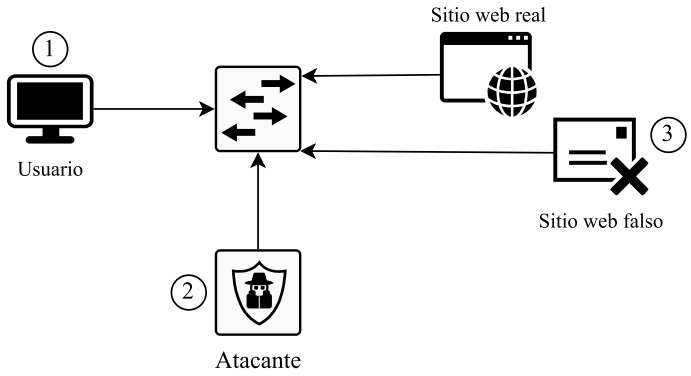


Figura 3.4: Ataque de suplantación DNS.

3.1.3. Suplantación HTTPS

En la suplantación HTTPS el atacante utiliza un dominio que se parece mucho al del sitio web objetivo. Con esta táctica se sustituyen los caracteres del dominio objetivo por otros caracteres no ASCII de aspecto muy similar. Es poco probable que el usuario desprevenido note la diferencia. Para llevar a cabo una suplantación HTTPS, el atacante registra un nombre de dominio similar al del sitio web objetivo, y también registra su certificado

SSL para que parezca legítimo y seguro. A continuación, envía un enlace a su víctima prevista. Como la mayoría de los navegadores admiten la visualización de nombres de huésped con código de barras en su barra de direcciones, cuando la víctima navega hasta la dirección, no se da cuenta de que es una versión falsa del sitio que espera visitar. Su navegador incluso muestra que el certificado del sitio web es legítimo y seguro, lo que dificulta aún más la detección del ataque. A partir de ahí, mientras el usuario cree que está interactuando con un sitio web cifrado legítimo, en realidad ha sido víctima de un ataque de intermediario y está entregando su información a un actor malicioso.

3.1.4. Suplantación ARP

En la suplantación de identidad ARP (*ARP spoofing*), también se conoce como *ARP cache poison*, el atacante suplanta la dirección MAC, por tanto, en lugar de que el tráfico vaya al huésped destino, el tráfico se desvía a la dirección MAC suplantada. No obstante, si el tráfico malicioso es redireccionado, los atacantes pueden interceptar tráfico para obtener información sensible o prepararse para un ataque más avanzado. La Figura 3.5 muestra el patrón común de ataques *ARP spoofing*. Los atacantes utilizan *ARP spoofing* para múltiples propósitos.

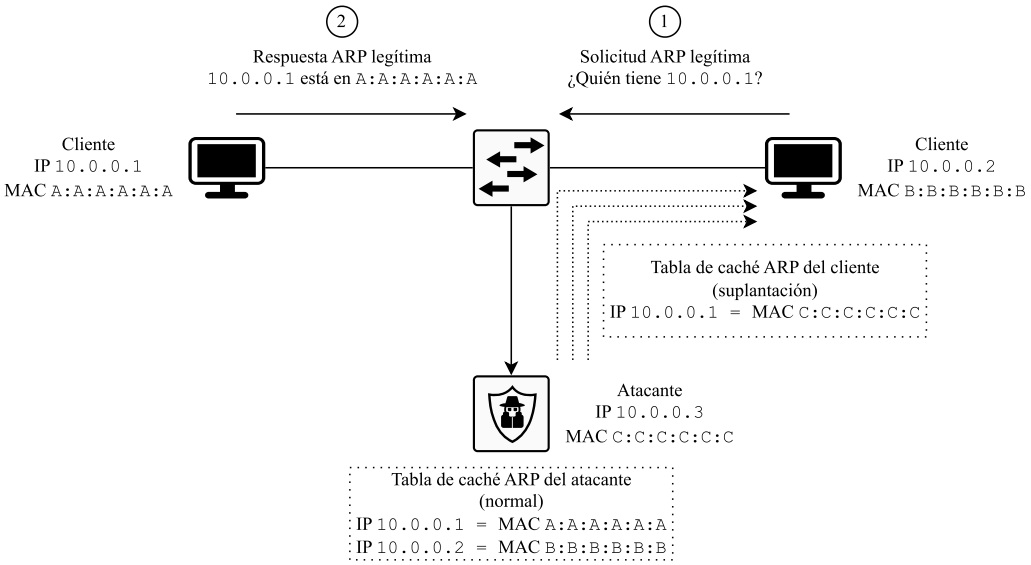


Figura 3.5: Ataque de suplantación de identidad ARP [3].

ARP acepta una respuesta siempre y cuando se emita una solicitud, no tiene métodos de autenticación, ni existe un camino para verificar la legibilidad de lo enviado. El ataque *ARP spoofing* utiliza este comportamiento para "envenenar" a la víctima por manipulación de paquetes ARP. Existen dos técnicas de *spoofing* que utilizan las vulnerabilidades del protocolo ARP, la primer técnica es suplantación del paquete de solicitud ARP y la segunda es suplantación del paquete de respuesta ARP [43], [44], [3].

- La Figura 3.6 ilustra el envenenamiento de la tabla de caché ARP mediante una petición ARP. El atacante envía un paquete de solicitud ARP a la víctima que contiene datos falsos para engañarlo. La víctima cree que el remitente de ese paquete de solicitud ARP es el huésped `10.0.0.1`, por lo que la víctima almacena en caché la información del paquete de solicitud ARP en su propia tabla de caché ARP. Cada vez que el huésped `10.0.0.2` envía datos al huésped `10.0.0.1`, los datos van al dispositivo con la dirección MAC `F:F:F:F:F:F`; en este caso, es la dirección MAC de un dispositivo desconocido [3].

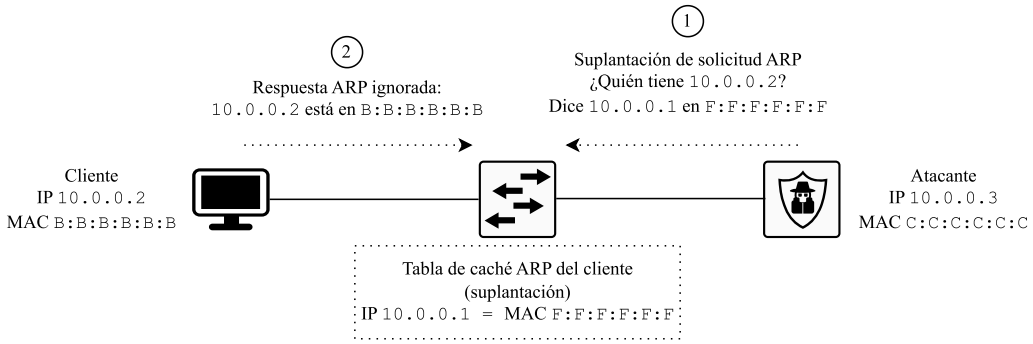


Figura 3.6: Suplantación de identidad de solicitud ARP [3].

- La suplantación de identidad utilizando el paquete de respuesta ARP tiene un efecto similar a la suplantación de identidad utilizando la petición ARP. La única diferencia es el tipo del paquete ARP. Como se ilustra en la Figura 3.7, el atacante envía directamente la respuesta ARP a la víctima aunque ésta nunca la solicite. Sin embargo, a veces este tipo de ataque es fácilmente perceptible por IDS porque resulta inusual que un huésped reciba una respuesta ARP sin antes haber enviado una solicitud ARP [3].

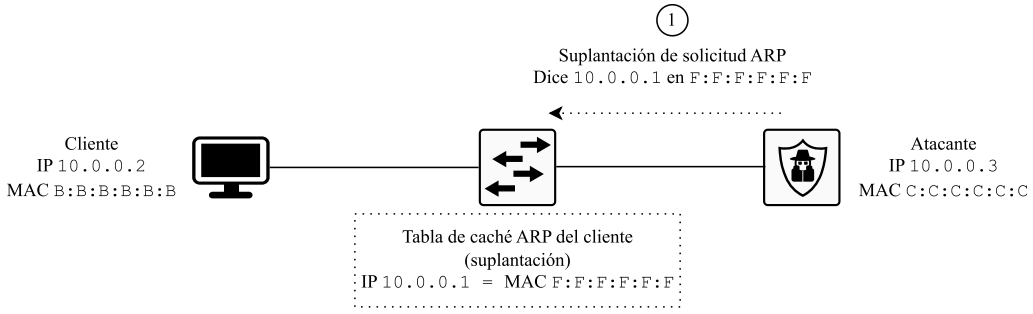


Figura 3.7: Suplantación de identidad de respuesta ARP [3].

3.1.5. Eliminación de TLS

TLS es el estándar de seguridad usado para un sitio web. Todos los mecanismos de seguridad en Internet están basados en TLS. La Figura 3.8 muestra el proceso de eliminación TLS y a continuación se explica el proceso:

1. El usuario visita un sitio web en donde tenga que iniciar sesión (cuentas de banco, paginas escolares, etc).
2. El navegador web añade automáticamente `http://` precediendo a `www.ejemplo.com`, convirtiéndolo así en `http://www.ejemplo.com`.
3. El navegador web solicita al servidor de Ejemplo mediante el método `HTTP GET`.
4. El servidor de Ejemplo recibe la solicitud y la redirige a `https://www.ejemplo.com`.
5. La redirección HTTPS pasa por una red posiblemente no segura, con las siguientes posibilidades [3]:
   - El atacante puede eliminar HTTPS para el usuario.
   - El atacante puede comunicarse con el servidor de Ejemplo a través de HTTPS, y puede hacer todo en nombre del usuario real.

- Generalmente, no se muestra ninguna advertencia desde el navegador web.
- El usuario no tiene conocimiento de este ataque.
- El usuario puede seguir conectándose al servidor de Ejemplo a través de HTTP mediante el atacante, aunque el sitio web haya proporcionado HTTPS.

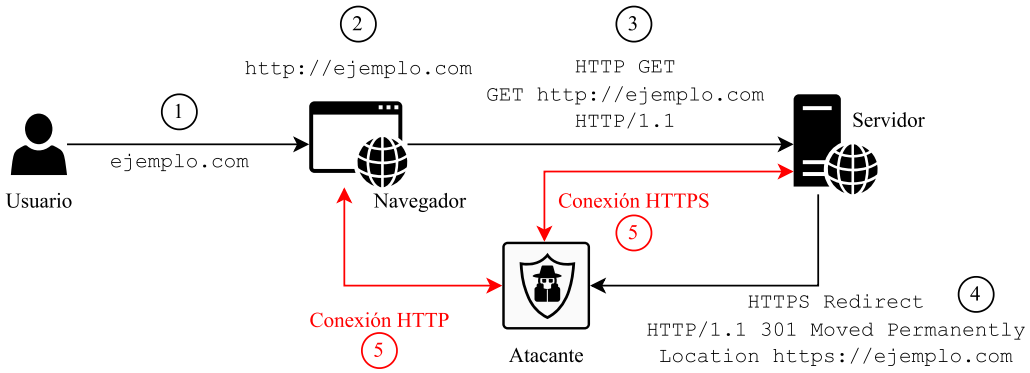


Figura 3.8: Proceso de un ataque de eliminación TLS [4].

3.1.6. Secuestro de Sesión

El secuestro de sesión consiste en la explotación del mecanismo de control de una sesión en un sitio web. La comunicación mediante HTTP utiliza diferentes conexiones TCP, el servidor web necesita un método para reconocer la conexión de todos los usuarios. El método más común depende de un identificador que el servidor web envía para el navegador del cliente y así autenticar satisfactoriamente [45]. En la Figura 3.9 se observa el funcionamiento del secuestro de sesión.

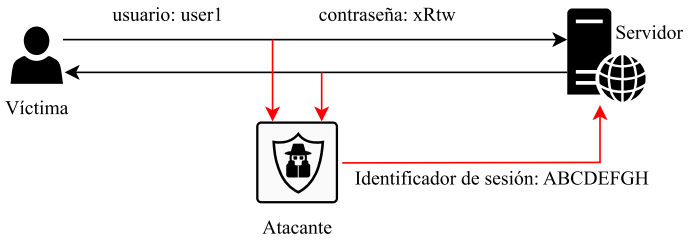


Figura 3.9: Modo de operación del secuestro de sesión.

La gran ventaja del ataque de secuestro de sesión es que no tiene un descanso o cortafuegos de seguridad, únicamente necesita escuchar a la red y tomar cualquier sesión válida. Existen tres tipos de secuestro de sesión y son [46]:

- Secuestro de sesión activa: Es una técnica en la que se ataca una sesión ya activa entre el usuario y el servidor.
- Secuestro de sesión pasiva: El atacante se coloca entre el usuario y el servidor, y envía los paquetes válidos al usuario haciéndose pasar por servidor, recibe los paquetes del usuario y los envía al servidor haciéndose pasar por un usuario válido. El atacante puede ver todos los datos que pasan a través del sistema del atacante e incluso el atacante puede hacer algunos cambios en los paquetes de datos, en donde ni el usuario ni el servidor pueden detectar los cambios en los paquetes de datos [46].
- Secuestro de sesión híbrida: Se divide en dos tipos:

- Ataque de suplantación invisible: Se ataca el sistema objetivo sin ningún cambio en la conexión entre el servidor y el huésped víctima.
- Ataque de suplantación visible: El atacante debe estar en la misma red así como en la misma subred.

3.2. Denegación de Servicio y Denegación de Servicio Distribuido

Los ataques de denegación de servicio (DoS) representan una de las amenazas más importantes para garantizar la fiabilidad y seguridad de los sistemas de información. El objetivo de un ataque de denegación de servicio no es obtener un acceso no autorizado a un sistema, sino evitar que un usuario acceda a dicho recurso; un DoS puede causar problemas tales como consumo de recursos, alteración de los componentes de la red, consumo de ancho de banda y destrucción de archivos y programas [47].

En cuanto al ataque de denegación de servicio distribuido (DDoS), éste intenta hacer que un servicio en línea, un sitio web o una computadora no esté disponible al sobrecargarlo con grandes flujos de tráfico de Internet generados desde múltiples fuentes. Las máquinas explotadas pueden ser computadoras y otros recursos en red, como los dispositivos IoT. Un ataque DDoS ataca muchas computadoras y conexiones a Internet, a menudo distribuidos globalmente en lo que se denomina una red de *bots* [48].

Existen múltiples enfoques para la aplicación de ataques DoS que consideran diferentes propiedades como el tipo de objetivo y el ritmo del ataque.

Los ataques DDoS se clasifican en tres categorías, los cuales se mencionan a continuación [48].

3.2.1. Ataques basados en volumen

El ataque basado en volumen consiste en utilizar una cantidad excesiva de tráfico falso para saturar un huésped. Estos ataques incluyen inundación TCP, inundación ICMP e inundación UDP:

- *Ping* de la muerte: El atacante envía mensajes ICMP excesivamente grandes a un huésped objetivo. Aprovechando la debilidad en la implementación del sistema operativo de la especificación TCP/IP, el atacante puede enviar un paquete ICMP mayor que el máximo de 65535 octetos permitido [49], [14]. Ante este suceso, el huésped puede crear un desbordamiento de búfer y, por tanto, quedar inhabilitado (bloquearse o forzar un reinicio). Algo similar ocurre cuando al huésped destino se le envían múltiples paquetes ICMP fragmentados que requieren que el sistema operativo reestructure los datos a su llegada. Al examinar los paquetes, el sistema operativo descubre que los paquetes no tienen el tamaño que dicen tener, esto origina que la máquina se inhabilite.
- Inundación ARP: La inundación ARP (*ARP flooding*) o tormenta ARP (*ARP storm*) ocurre cuando los conmutadores redirigen los paquetes de difusión directamente a todos los puertos excepto a los puertos de entrada, esto ocasiona problemas como el consumo del ancho de banda, conexión de red lenta, el consumo de CPU y memoria en los huéspedes de la red. Además, puede utilizarse como primera etapa para lanzar más ataques como DoS y DDoS. La Figura 3.10 muestra el escenario del ataque de inundación ARP que se produce en una LAN [50].

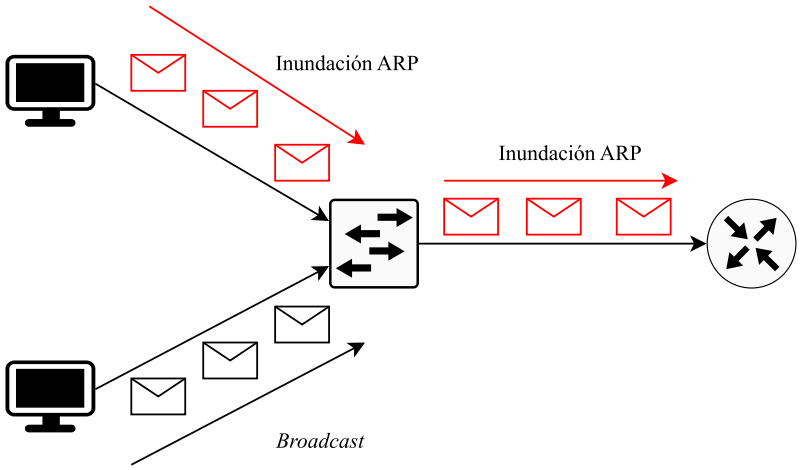


Figura 3.10: Proceso de inundación ARP.

Al tratarse de uno de los ataques más comunes en una red de computadoras, para identificar este tipo de ataques es necesario configurar Wireshark. Así pues, se tiene que dirigir a la pestaña Edición, se elije la opción Preferencias donde aparecerá una ventana y se busca la opción Protocolos, luego se busca la opción ARP/RARP y se habilita la casilla de la opción Detect ARP request storms. Las demás opciones que se observan pertenecen al número de solicitudes ARP que se van a detectar en cierto período de tiempo dado en milisegundos.

- Inundación ICMP: Envía una gran cantidad de mensajes eco (mensajes *ping*) a las direcciones de difusión y a los mensajes *ping* que tienen la dirección de origen falsificada de la víctima (véase la Figura 3.11). Cada huésped responde a las solicitudes enviando una respuesta de eco ICMP. Por lo tanto, para n mensajes de solicitud de eco ICMP enviados a un dominio de difusión, se envían $n \times m$ mensajes de respuesta de eco ICMP fuera del dominio de difusión hacia la computadora víctima, donde m es el número de huéspedes en el dominio de difusión [51].

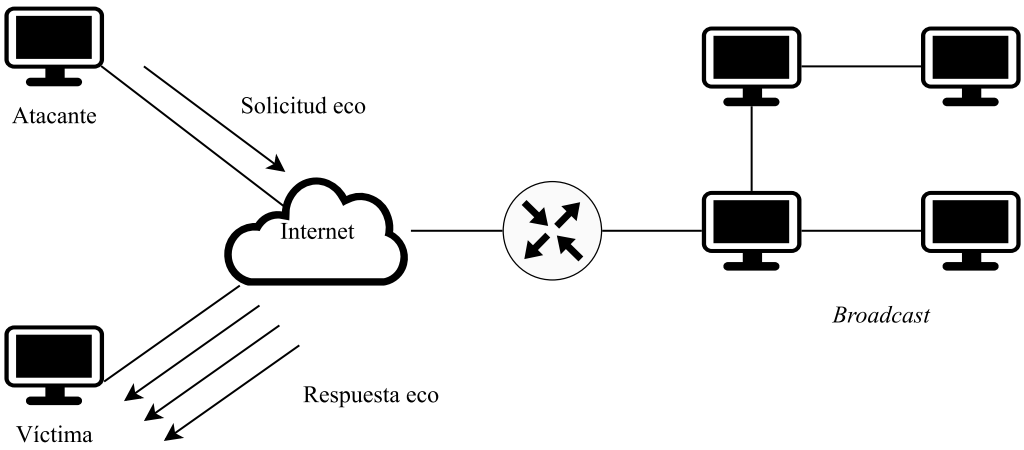


Figura 3.11: Proceso de una inundación ICMP.

- Inundación MAC: La inundación MAC *(MAC Flooding)* ocurre cuando los conmutadores de red son inundados con direcciones MAC falsas para comprometer su seguridad. Un conmutador no difunde paquetes de red a toda la red y mantiene su integridad segregando los datos y haciendo uso de las VLAN (redes de área local virtuales).

El motivo de la inundación MAC es robar datos del sistema de la víctima que se transfieren a una red. Se puede conseguir forzando el contenido de la tabla MAC del conmutador y el comportamiento *unicast*. El resultado es la transferencia de datos sensibles a otras partes de la red y, finalmente, convertir el conmutador en un concentrador y hacer que se inunden cantidades significativas de tramas entrantes en todos los puertos. Por lo tanto, también se denomina ataque de desbordamiento de la tabla de direcciones MAC [52].

3.2.2. Ataques por agotamiento del estado de TCP

Los ataques por agotamieto del estado de TCP, intentan consumir las tablas de estado de conexión que están presentes en muchos componentes de la infraestructura, como equilibradores de carga[1], cortafuegos y los propios servidores de aplicaciones. Incluso los dispositivos de alta capacidad que pueden mantener el estado de millones de conexiones pueden ser derribados por estos ataques [53]. Estos son:

- Inundación SYN: Se hizo conocido en 1996 cuando la revista *2600* y *Phrack* publicaron la descripción del ataque con el código fuente para realizarlo [41], [54]. La base del ataque de inundación SYN parte de la conexión de tres vías utilizada en TCP (véase Figura 2.6). Al recibir el paquete SYN, se responde con el paquete SYN-ACK, en ese momento se genera el bloque de control de transmisión (TCB, *Transmission Control Block*) el cual es una estructura de datos del protocolo de transporte que contiene toda la información sobre una conexión. El estado de TCP SYN-RECEIVED se utiliza para indicar que la conexión está medio abierta, es decir, que la solicitud se encuentra en duda. El TCB se asigna con base a la recepción del paquete SYN antes de que la conexión esté completamente establecida o de que se haya verificado el alcance de retorno del huésped origen. Cuando existen muchas solicitudes, los SYNs entrantes causan las asignación de muchos TCBs originando una saturación en el kernel de la memoria del huésped destino. En la Figura 3.12 se muestra el ataque de inundación SYN.

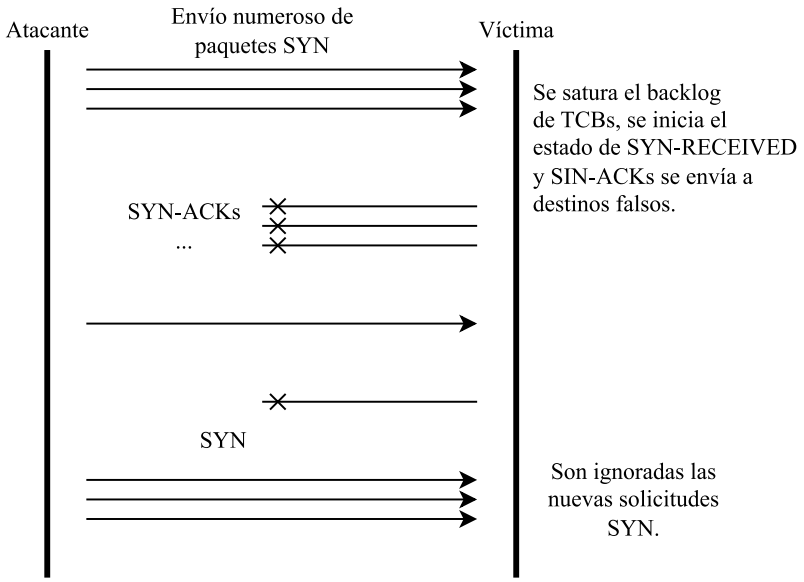


Figura 3.12: Ataque de inundación SYN.

[1]Dispositivo de hardware o software que distribuye las cargas de trabajo entre dos o más servidores, hace que estos dispositivos sean más eficientes, acelerando el rendimiento y reduciendo la latencia.

Algunos sistemas operativos utilizan un parámetro *backlog* con un socket de escucha que establece un límite en el número de TCBs con el fin de evitar el agotamiento de la memoria [41]. Sin espacio en el *backlog* es imposible atender nuevas solicitudes hasta que algunos TCBs sean removidos del estado SYN-RECEIVED. El ataque de inundación SYN tiene diferentes modos de ataque:

- Ataque directo: Cuando el atacante envía segmentos SYN sin falsificar su dirección IP se le conoce como ataque directo. Este modo de ataque es muy fácil de realizar puesto que no requiere de técnicas de suplantación de identidad por debajo del nivel de usuario. Para que sea efectivo, los atacantes deben evitar que su sistema operativo responda a los SYN-ACK, cualquier ACK, RST o *ping* hará que la víctima mueva el TCB fuera de SYN-RECEIVED. Este escenario se puede lograr a través de reglas de cortafuegos que filtren los paquetes salientes hacia la víctima (permitiendo únicamente la salida de SYNs), o que filtren los paquetes entrantes para que cualquier SYN-ACK sea descartado antes de llegar al código de procesamiento TCP local. Cuando se detecta, este tipo de ataque es muy fácil de responder, porque solamente necesita una simple regla de cortafuegos para bloquear los paquetes con la dirección IP de origen del atacante. Este comportamiento de defensa puede automatizarse y tales funciones están disponibles en los cortafuegos reactivos disponibles en el mercado [41].
- Ataque directo distribuido: El atacante se aprovecha de numerosas máquinas en todo Internet, por lo tanto es mucho más difícil de detener. En el caso mostrado en la Figura 3.13, los programas informáticos utilizan ataques directos, pero para aumentar aún más la eficacia, cada *bot* podría utilizar un ataque de suplantación de identidad y múltiples direcciones suplantadas. En la actualidad, los ataques distribuidos son factibles porque existen varios *bots* de miles de máquinas comprometidas que son utilizadas por los delincuentes para los ataques DoS. Como los *bots* se añaden o eliminan constantemente de los ejércitos y pueden cambiar sus direcciones IP o su conectividad, resulta difícil bloquear estos ataques [41].

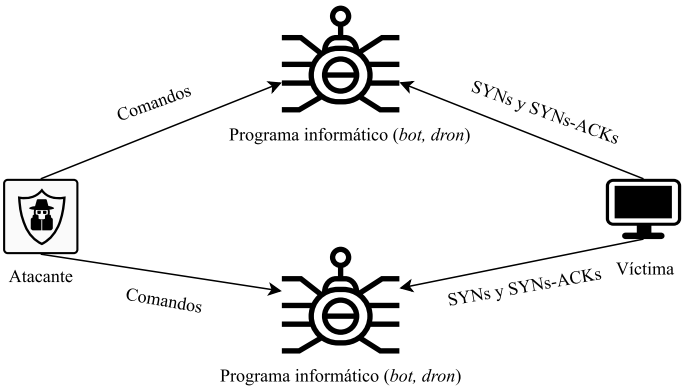


Figura 3.13: Ataque directo distribuido.

3.2.3. Ataques de Capa de Aplicación

Se trata del tipo de ataque más mortífero, ya que puede ser muy eficaz con tan sólo una máquina atacante que genere una baja tasa de tráfico (esto hace que estos ataques sean muy difíciles de detectar y mitigar). Los ataques a la capa de aplicación han llegado a prevalecer en los últimos años y los ataques de inundación de la capa de aplicación han sido algunos de los ataques de denegación de servicio más comunes [53]:

- Inundación HTTP: Consiste en solicitudes HTTP simultáneamente sobre un huésped o servidor. Esta acción provoca el agotamiento de los recursos de la red de la víctima, por ello, no puede responder a las solicitudes reales de los usuarios. Posee dos variantes que son HTTP GET y HTTP POST.
- Inundación DNS: En un ataque de inundación DNS, el agresor intenta sobrecargar un determinado servidor DNS (o servidores) con tráfico aparentemente válido, abrumando los recursos del servidor e impidiendo la capacidad de los servidores para dirigir solicitudes legítimas a los recursos de la zona [55].

Para finalizar este capítulo, se presenta la Tabla 3.1 que proporciona un resumen general de los diferentes ataques que pueden ocurrir en una red de computadoras. Esta tabla permite observar y clasificar los distintos tipos de ataques a los que están expuestas las redes de computadoras, desde ataques de hombre en el medio (MitM) hasta denegación de servicio (DDoS). Mediante el estudio de estos ataques, los administradores de redes pueden comprender mejor el modo de operación por los intrusos y así implementar metodologías efectivas para identificar y prevenir amenazas en las redes de computadoras.

Categoría	Ataques	
Hombre en el Medio (MitM)	Suplantación DNS	
	Suplantación HTTPS	
	Eliminación TLS	
	Secuestro de Sesión	
	Suplantación IP	
	Suplantación ARP	
Denegación de Servicio (DoS, DDoS)	Ataques basados en volumen	*ping* de la muerte
		Inundación ARP
		Inundación ICMP
		Inundación MAC
	Ataque por agotamiento del estado TCP	Inundación SYN
	Ataques de capa de aplicación	Inundación HTTP
		Inundación DNS

Tabla 3.1: Categorías y tipos de ataques analizados en este documento.

Capítulo 4

Detección de Amenazas en la red de la Universidad de Oaxaca de Juárez

Las comunicaciones de una LAN no se limitan a un espacio confinado, necesitan comunicarse con el mundo exterior. Esto hace que la red sea vulnerable a diversas formas de ataque; algunas pueden lanzarse desde fuera de una LAN, mientras que otras pueden llevarse a cabo dentro de la propia red. En esta sección se estudian escenarios de riesgo en una LAN universitaria y se muestra un análisis de las amenazas y los problemas tomando como referencia archivos de paquetes capturados utilizando Wireshark.

La Figura 4.1 proporciona una visión general de las amenazas identificadas en esta tesis mediante el análisis de archivos utilizando Wireshark y NetworkMiner, así mismo, las amenazas identificadas se clasifican con base a los protocolos ARP, ICMP, TCP, DHCP y TLS.

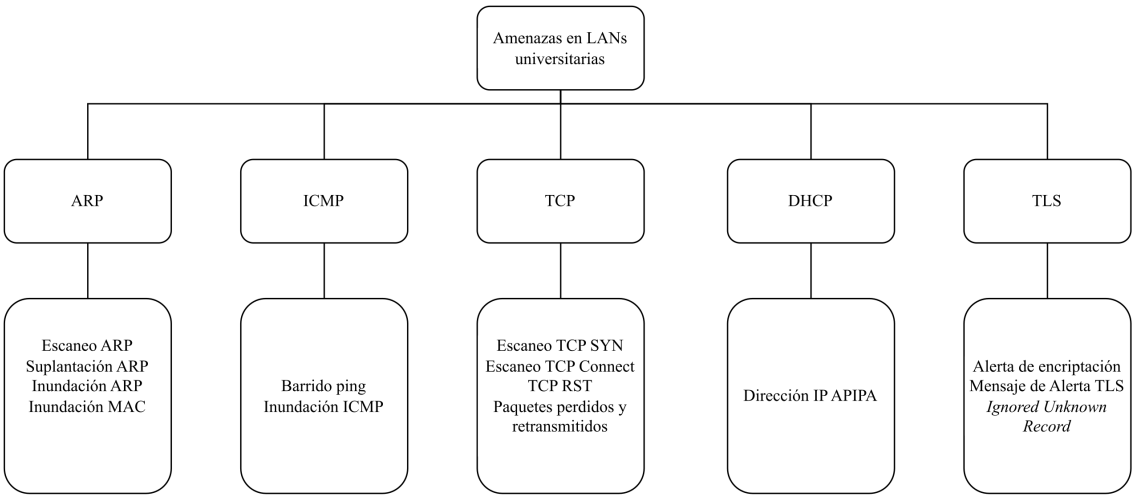


Figura 4.1: Amenazas identificadas en esta investigación.

Es necesario recalcar que las fuentes bibliográficas citadas a lo largo de esta investigación utilizan como ejemplo capturas de Wireshark con parámetros a modo e ideales, sin embargo, las capturas utilizadas en este documento provienen de LANs universitarias con datos reales obtenidos con Wireshark, por tal motivo, algunos datos no serán tan exactos como lo maneja la literatura, es decir, los datos encontrados son aproximaciones que sirvieron para analizar y encontrar aplicaciones reales sobre las amenazas que sufre una LAN universitaria.

En una captura de paquetes se encuentran una gran variedad de protocolos de red que no son conocidos (por no ser protocolos comunes), sin embargo, en esta investigación únicamente se abordan los siguientes protocolos: ARP, ICMP, TCP, DHCP y TLS ya que forman la base para que exista comunicación en una red de computadoras.

Para la detección de amenazas se utilizó un equipo de cómputo con las siguientes características: procesador AMD Ryzen 5 4600H con Radeon Graphics 3.00 GHz, memoria RAM de 16 GB, disco duro de estado sólido de 480 GB y sistema operativo MS Windows 11. Los archivos de captura que tengan extensión `.pcapng` deben convertirse a la extensión `.pcap`, esto para analizar los archivos utilizando la herramienta de NetworkMiner. Wireshark utiliza por defecto la extensión `.pcapng`, sin embargo, el problema con `.pcapng` es la compatibilidad con otras herramientas de análisis de paquetes. La extensión `.pcap` captura paquetes de red de las capas 2 a la 7 del modelo de referencia OSI.

4.1. Escenario de Captura

Con la finalidad de realizar la detección de amenazas en LANs universitarias, se implementó la metodología planteada en la sección 1.6. Se capturaron paquetes de dos universidades; la primera universidad ubicada en la ciudad de Oaxaca de Juárez presenta el escenario mostrado en la Figura 4.2. El segundo análisis corresponde a la UTM y se estudia en el siguiente capítulo.

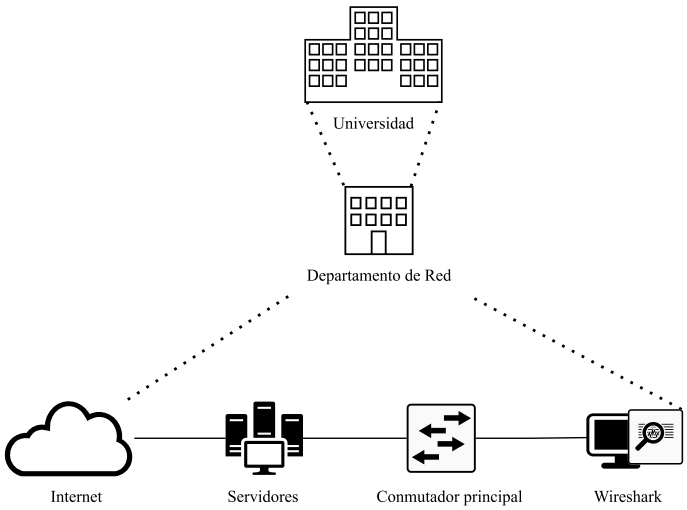


Figura 4.2: Escenario para la captura de paquetes en la Universidad de Oaxaca.

Es necesario analizar diferentes archivos de captura de paquetes debido a que un archivo de paquetes no es suficiente para encontrar amenazas, vulnerabilidades o en su defecto ataques, dependerá mucho de la hora de captura, el tiempo de captura y en algunos casos los filtros de captura que se apliquen al iniciar Wireshark.

4.2. Características de los Paquetes Capturados

Para comenzar con la detección de amenazas, se presenta la Tabla 4.1 con las capturas del escenario mencionado en la Figura 4.2. Cabe señalar que para obtener los datos visualizados en la Tabla 4.1 y 5.1 se debe dirigir a la pestaña Estadísticas, luego Propiedades del archivo de captura y se desplegará información detallada del archivo a analizar.

Archivo	Tamaño	Intervalo de Captura	Paquetes
1	11 GB	2022-08-04 11:00:00 a 2022-08-04 12:00:00	5089353
2	2.2 GB	2022-08-04 12:00:00 a 2022-08-04 12:59:59	1320914
3	908 MB	2022-08-03 18:00:00 a 2022-08-03 18:59:59	1026661
4	98 MB	2022-08-04 05:00:00 a 2022-08-04 05:59:59	424406
5	81 MB	2022-08-04 09:00:00 a 2022-08-04 09:59:59	406592
6	78 MB	2022-08-03 22:59:59 a 2022-08-04 00:00:00	422373
7	73 MB	2022-08-04 05:59:59 a 2022-08-04 06:59:59	399537
8	16 MB	2022-08-04 18:00:00 a 2022-08-04 18:12:30	72450

Tabla 4.1: Características de los paquetes capturados en la Universidad ubicada en Oaxaca de Juárez.

4.3. Análisis

Partiendo de los archivos mostrados en la Tabla 4.1, en la Figura 4.3 se observa el reporte general que ofrece la función Información Especializada de Wireshark, mostrando tres casos que pertenecen a la sección Error, el caso de mayor importancia es TCP, los otros dos protocolos no están al alcance de esta investigación para analizarlos. En la sección de Advertencias el protocolo que predomina es TCP. En la sección Nota se observa que el protocolo predominante es TCP seguido de IPv4, para esta sección se observa que el recuento de paquetes es demasiado, se puede considerar como una falla en el rendimiento de la red, otro protocolo a considerar para iniciar este análisis es ARP/RARP, el cual indica que se detectó una tormenta de paquetes ARP de 5022 paquetes, esto quiere decir que realizaron escaneos a la red.

Gravedad	Resumen	Grupo	Protocolo	Recuento
Error	Invalid Destination Address Mode	Malformed	IEEE 802.15.4	1
Error	Malformed Packet (Exception occurred)	Malformed	ISAKMP	1
Error	New fragment overlaps old data (retransmission?)	Malformed	TCP	85
Warning	ACKed segment that wasn't captured (common at capture...	Sequence	TCP	25
Warning	TCP window specified by the receiver is now completely full	Sequence	TCP	3
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	42576
Warning	TCP Zero Window segment	Sequence	TCP	16
Warning	Ignored Unknown Record	Protocol	TLS	312
Warning	DNS response retransmission. Original response in frame 4...	Protocol	mDNS	3778
Warning	DNS query retransmission. Original request in frame 1770	Protocol	mDNS	3646
Warning	No response seen to ICMP request	Sequence	ICMP	478
Warning	DNS response retransmission. Original response in frame 642	Protocol	DNS	1
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	730
Warning	D-SACK Sequence	Sequence	TCP	1010
Warning	Connection reset (RST)	Sequence	TCP	4395
Note	The acknowledgment number field is nonzero while the A...	Protocol	TCP	13
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	16688
Note	ACK to a TCP keep-alive segment	Sequence	TCP	18
Note	TCP keep-alive segment	Sequence	TCP	18
Note	"Time To Live" != 255 for a packet sent to the Local Networ...	Sequence	IPv4	579
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	322
Note	This session reuses previously negotiated keys (Session res...	Sequence	TLS	64
Note	ARP packet storm detected (30 packets in < 100 ms)	Sequence	ARP/RARP	5022
Note	A new tcp session is started with the same ports as an earli...	Sequence	TCP	2690
Note	This frame undergoes the connection closing	Sequence	TCP	289
Note	This frame initiates the connection closing	Sequence	TCP	412
Note	Duplicate ACK (#1)	Sequence	TCP	414536
Note	This frame is a (suspected) retransmission	Sequence	TCP	43584
Note	"Time To Live" only 1	Sequence	IPv4	435
Note	Didn't find padding of zeros, and an undecoded trailer exis...	Protocol	Ethertype	1819423
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	1
Chat	GET / HTTP/1.1\r\n	Sequence	HTTP	9
Chat	Possible traceroute: hop #2, attempt #3	Sequence	UDP	8
Chat	TCP window update	Sequence	TCP	99
Chat	Connection finish (FIN)	Sequence	TCP	701
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	4473
Chat	Connection establish request (SYN): server port 3389	Sequence	TCP	8595

Figura 4.3: Resumen de la primer captura de paquetes en la Universidad de Oaxaca de Juárez.

Se inició el análisis del archivo utilizando los filtros de visualización para mostrar paquetes SYN sin acuse de recibo y detectar posible escaneo de puertos. Se utilizó el filtro mostrado en la Tabla 2.6 de la sección 2.13.2 y es `tcp.flags.syn == 1 && tcp.flags.ack == 0`. Los paquetes filtrados corresponden a un 0.2 %. Cada paquete SYN muestra que proviene de una dirección IP de origen diferente con un puerto destino 3389 (escritorio remoto de Windows), longitud idéntica 0 y tamaño de ventana 8192. La relación que existe entre el tiempo y los paquetes capturados no presentan señales de

posibles ataques, sin embargo, se observa que la bandera SYN va acompañada de otras banderas que son: ECN y CWR, las cuales están asociadas a la congestión del ancho de banda en la red, por lo tanto, se trata de un caso verdadero positivo (véase Figura 4.4).

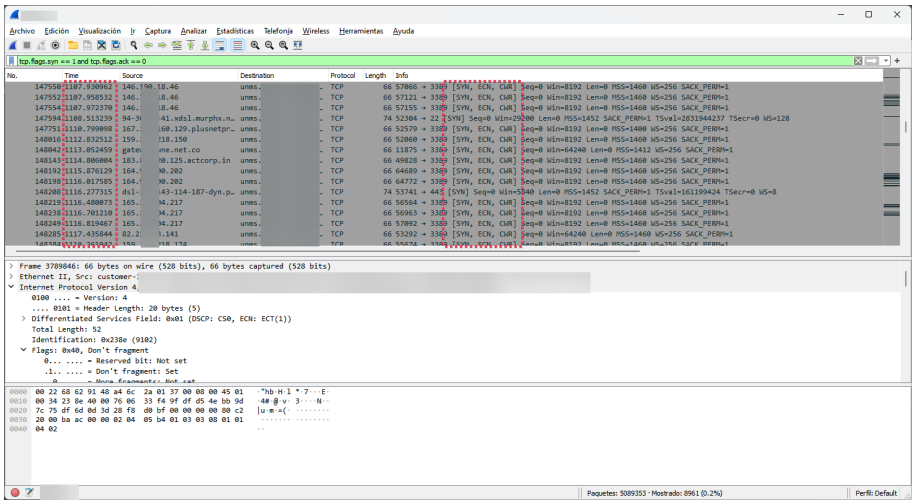


Figura 4.4: Ejemplo de inundación SYN.

Continuando con el escaneo de puertos, se analizó el comportamiento de las banderas SYN/ACKs utilizando el filtro `tcp.flags.syn == 1 && tcp.flags.ack == 1`. Al aplicarlo, se observa que el número de paquetes con SYN/ACKs es demasiado pequeño comparado con el número de paquetes del archivo. La cifra de paquetes capturados SYN/ACKs corresponde a 0.1 %, se observa que el origen parte de un mismo servidor hacia diferentes clientes, el tamaño de la ventana es constante (64240) y la longitud es 0 por lo tanto no representa una amenaza a la red (véase Figura 4.5).

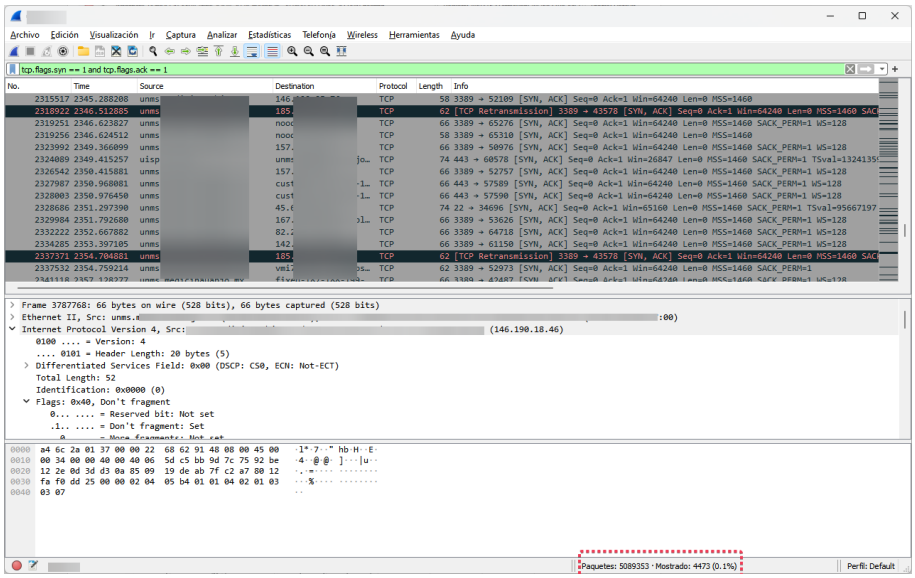


Figura 4.5: Paquetes SYN/ACKs.

En el caso de la Figura 4.6, se observan paquetes que presentan características como barrido de puertos en un periodo demasiado corto. Sin embargo, el número de paquetes filtrados es muy pequeño; corresponde al 0.2 %. De acuerdo a las situaciones para la detección de amenazas esto se clasifica como un caso verdadero positivo, no obstante al ser un número muy pequeño de paquetes es posible que los mecanismos de seguridad

implementados en la red interrumpieron el escaneo.

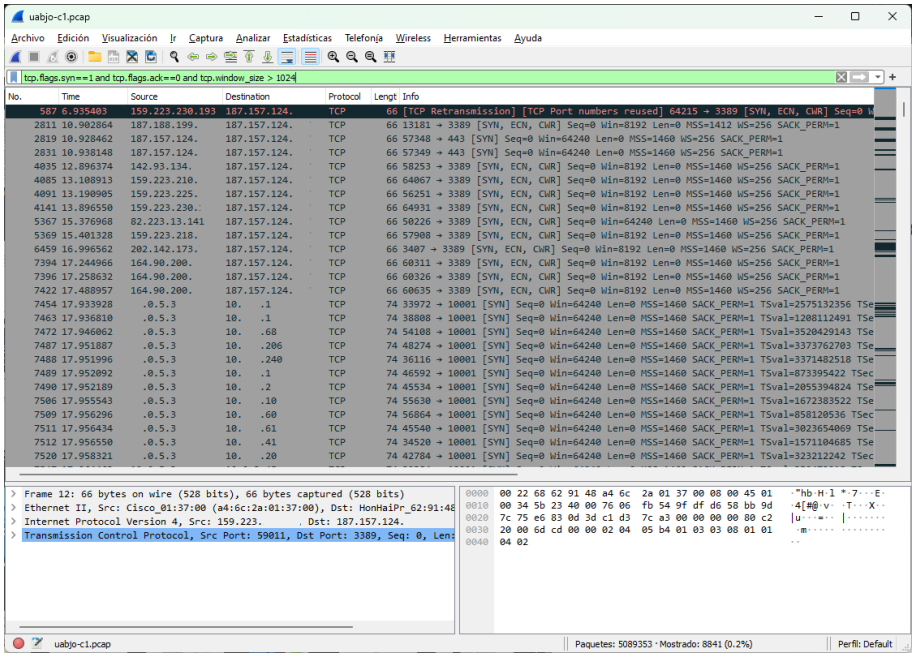


Figura 4.6: Escaneo TCP *Connect* clasificado como verdadero positivo.

La Figura 4.7 muestra paquetes en los cuales diferentes dispositivos realizaron un escaneo a la red preguntando aleatoriamente por direcciones IP (destino), a esta actividad se le conoce como escaneo ARP. Cuando se trata de un posible ataque, el intervalo de tiempo en el que se realizan las peticiones es demasiado corto y las direcciones IP incrementan el valor de su último byte. Con base a la figura en cuestión se observa que algunas peticiones cumplen con las características de escaneo ARP, sin embargo, es necesario recordar que ARP es uno de los protocolo importantes a la hora de iniciar una transmisión de información hacia un destino dentro de una red. Considerando lo anterior este tipo de amenaza es falso positivo aunque Wireshark lo identifica como malicioso.

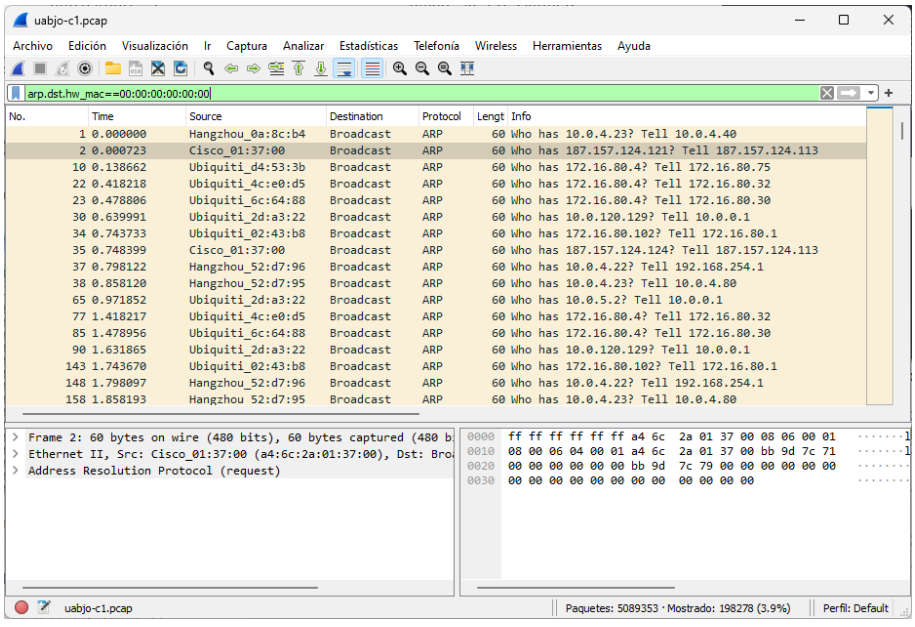


Figura 4.7: Escaneo ARP clasificado como falso positivo.

En la Figura 4.8 se observa sólo un paquete, el cual presentó la característica de mensaje ICMP tipo 3 (destino inalcanzable) código 2 (protocolo inalcanzable), esto indica que se presentó en la red un ataque de escaneo IP. Ante esta situación, es posible que se trate de una amenaza y que el sistema de seguridad de la red interrumpió el escaneo, por lo tanto, se clasifica como un caso verdadero positivo de acuerdo a la tabla de situaciones para la detección de amenazas.

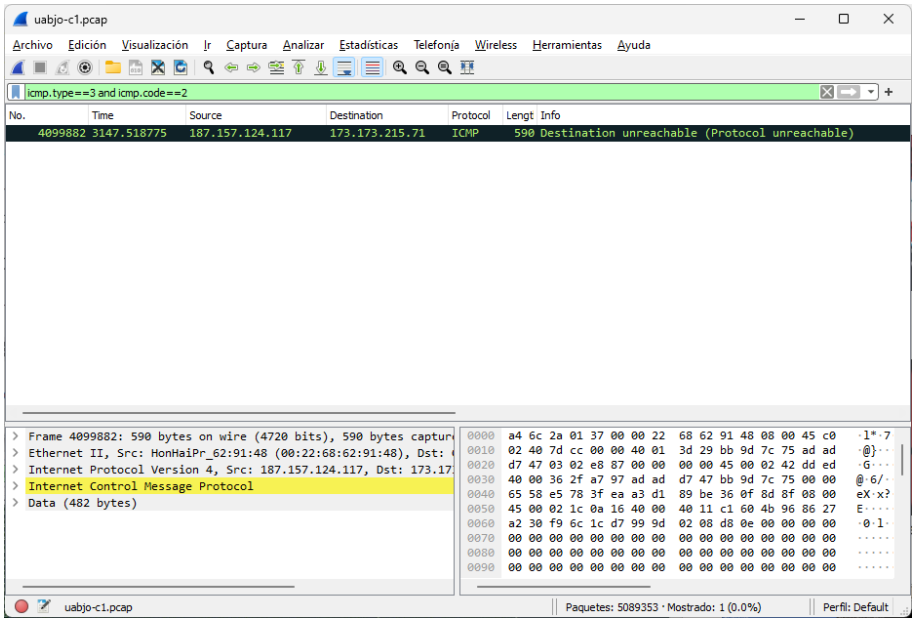


Figura 4.8: Escaneo IP clasificado como verdadero positivo.

La Figura 4.9 muestra paquetes ICMP, cuando se observa demasiado tráfico es probable que se trate de un barrido *ping* siempre y cuando las direcciones IP fuente sean aleatorias, es decir que el último byte se incremente. Sin embargo, al observar la Info de Wireshark algunos paquetes presentan el mensaje (no response found!) mientras que otros paquetes contienen el mensaje (reply in). Con base a este tipo de mensajes únicamente se clasifican como amenazas a la red los paquetes que tengan el mensaje (no response found!). Dicho esto, existen dos situaciones de detección de amenazas para este archivo; verdadero positivo y falso positivo.

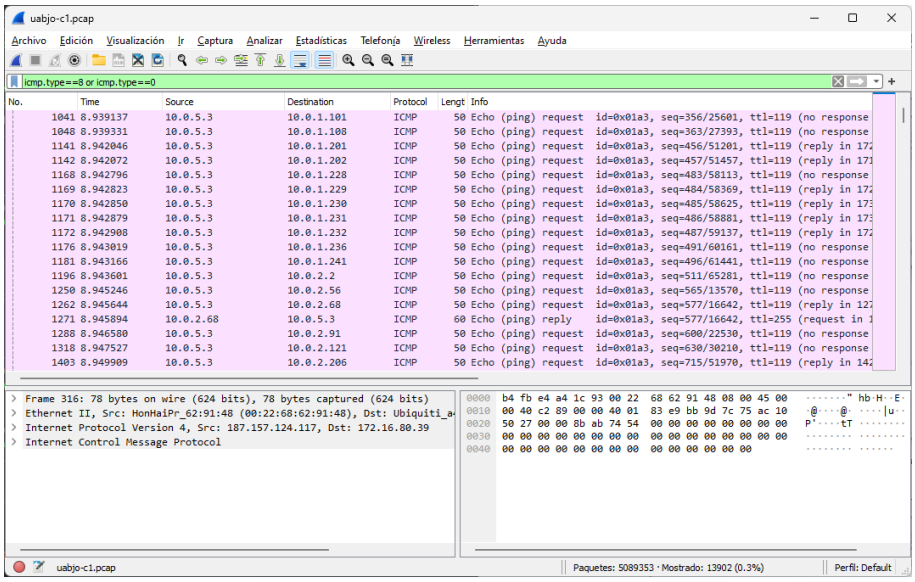


Figura 4.9: Barrido *ping* ICMP clasificado como verdadero positivo y falso positivo.

A fin de encontrar posibles amenazas con una inundación ICMP se tiene que en la Figura 4.10 aparecen paquetes que son demasiado grandes, por tal motivo el filtro indica que los paquetes a mostrar deben ser mayores a 48 bytes. Esta condición implica que detectará cualquier inundación ICMP independientemente del tipo o código. Sin embargo, los paquetes capturados son 206 de 5 089 353, este caso se clasifica como verdadero positivo.

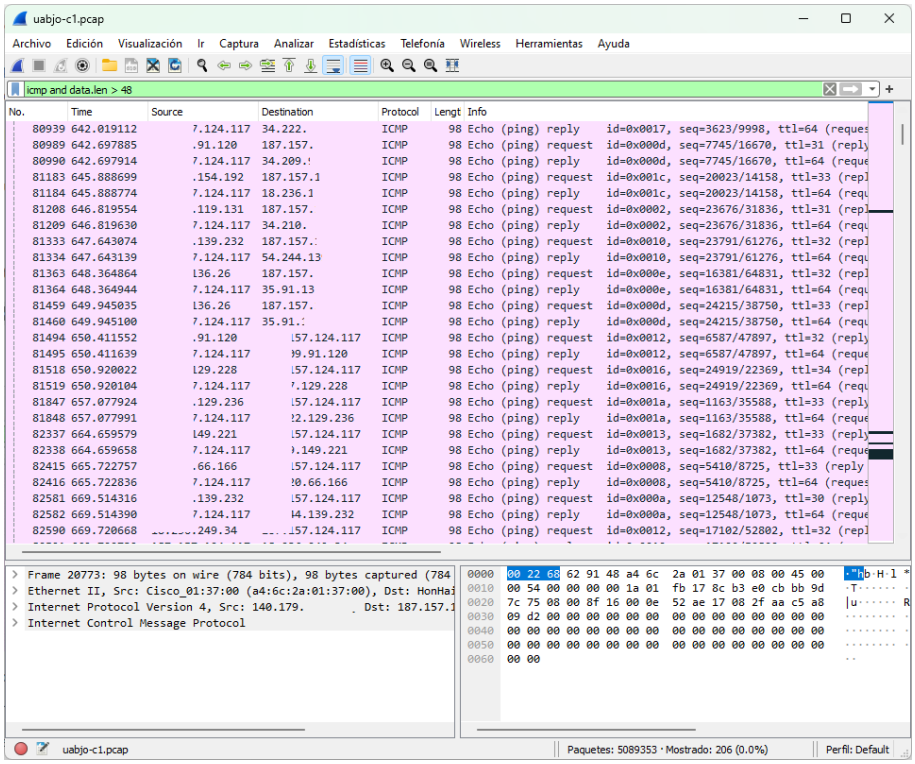


Figura 4.10: Inundación ICMP clasificado como verdadero positivo.

En la Figura 4.11 se presentan paquetes que han sido perdidos y retransmitidos. Esto puede indicar que existe un problema en la administración de la red o probablemente

se trate de un ataque de denegación de servicio. Por el número de paquetes filtrados, la amenaza es clasificada como un caso verdadero positivo.

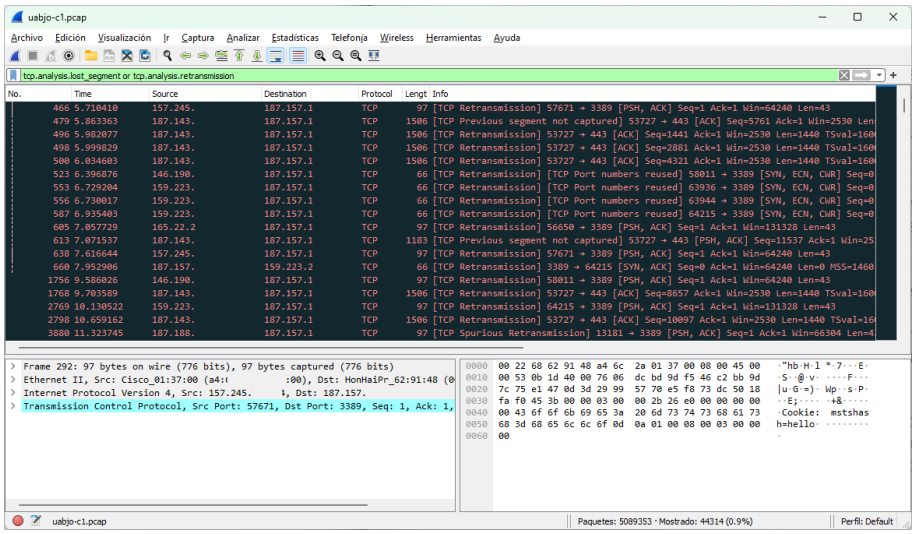


Figura 4.11: Pérdida y retransmisión de paquetes clasificado como verdadero positivo.

Finalmente, la Figura 4.12 muestra los paquetes que presentan la bandera RST. Esta bandera pertenece al protocolo TCP y su función es interrumpir la conexión cuando se presentan conexiones anormales o maliciosas. Por otro lado, el número de paquetes filtrados por esta bandera es de 4 459 que pertenecen al 0.1 %. Con base a este valor, se clasifica como verdadero positivo.

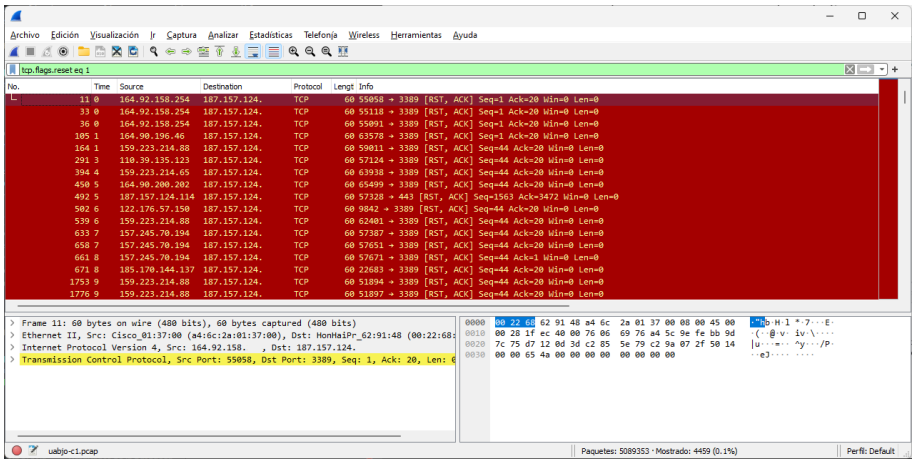


Figura 4.12: Paquetes que presentan la bandera RST activada clasificada como verdadero positivo.

Para iniciar el análisis de paquetes utilizando el software NetworkMiner en la Figura 4.13 se observa que en la sección de huéspedes existen 819, es decir, se capturó la información que intercambiaron 819 huéspedes, mientras que se compartieron 215 archivos. En la sección de DNS se visualizan 15776 conexiones realizadas entre clientes y servidores con diferentes puertos. Finalmente, la sección de anomalías muestra dos posibles ataques de suplantación de ARP.

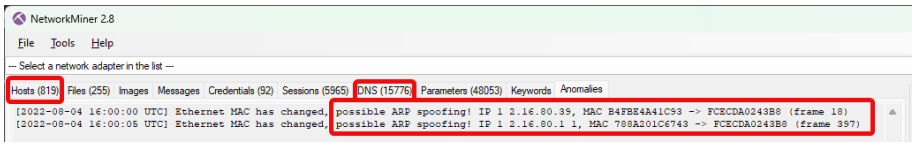


Figura 4.13: Resumen de anomalías desde NetworkMiner.

Para este caso es necesario centrarse en las direcciones IP que se observan en las sección de Anomalies puesto que dan mucho de que hablar en una red de computadoras. Se trata de una posible suplantación ARP, la primera dirección IP que comienza por `172.16.*.*` es una dirección IP privada interna, comúnmente es utilizada para ser la puerta de enlace predeterminada de la mayoría de los enrutadores inalámbricos o *modems* ADSL[1]. Lo anterior indica que existe un problema en los enrutadores, en consecuencia es necesario revisar las interacciones que realizó esa dirección IP. Se comienza por filtrar la dirección MAC que el programa detecta como duplicada, la Figura 4.14 muestra las direcciones IP con la misma dirección MAC.

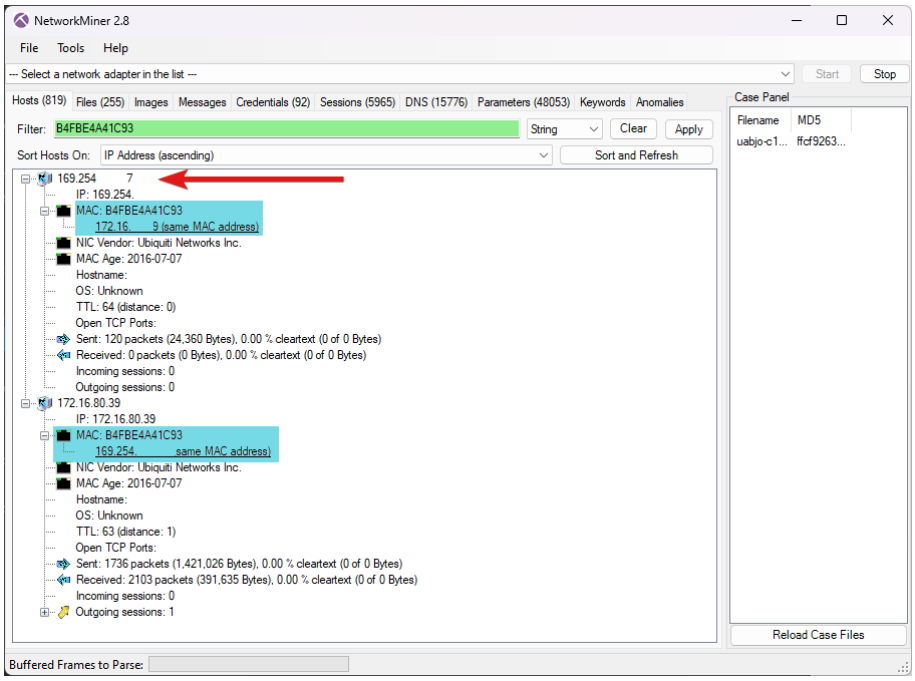


Figura 4.14: Direcciones IP con MAC duplicadas causados por el servidor DHCP.

Sin embargo, en la figura anterior, la flecha indica que la dirección IP tiene los primeros dos bytes en `169.254.*.*`, significa que dicha dirección IP corresponde al direccionamiento privado automático del protocolo de Internet (APIPA, *Automatic Private Internet Protocol Addressing*).Esta dirección IP se asigna cuando los equipos no encuentran su servidor DHCP, sucede porque de alguna forma no encontraron su servidor y se asignaron a la dirección `169.254.*.*` para así comenzar el envío de paquetes. Cuando esos equipos encuentran su servidor se les vuelve a asignar la dirección de `172.16.*.*` y comienzan el envío de paquetes con dicha dirección, sin embargo, al salir de la misma interfaz poseen la misma dirección MAC. Ante esta situación, NetworkMiner lo detectó como posible amenaza pero se considera como un falso positivo. Mientras que la otra dirección IP es probable que exista un tiempo excedido de asignación de direcciones IP.

[1]*Asymmetric Digital Subscriber Line*, línea de abonado digital asimétrica. Es una tecnología que ofrece velocidades de conexión más rápidas que las que podía ofrecer la Internet tradicional a través de líneas telefónicas de marcación. ADSL es la tecnología que impulsa muchas conexiones a Internet en todo el mundo [56].

Es necesario recordar que una dirección IP es asignable durante 24 horas, al exceder este tiempo es posible que exista una asignación a una dirección nueva y por tal motivo contienen la misma dirección MAC. Finalmente, las amenazas detectadas utilizando NetworkMiner se clasifican como falso positivo, esto se debe a que es una amenaza inocua, sin embargo, el software lo clasifica como malicioso o dañino.

Continuando con el análisis del segundo archivo de captura, la Figura 4.15 muestra que en la sección Error se encuentra un grupo que está Mal formado, sin embargo, el protocolo al que pertenece no se encuentra al alcance de esta investigación. Mientras que en la sección de Advertencias se observan doce casos, de las cuales cinco pertenecen al protocolo TCP, uno a ICMP, uno a TLS, uno a ARP. De los protocolos mencionados, es conveniente revisar primero ICMP, debido a que se trata de un protocolo susceptible a ataques, mientras que las advertencias sobre el protocolo TCP ocurren por problemas de transmisión o rastreo de puertos. En segundo lugar, es de vital importancia analizar el protocolo ARP; se trata de una posible suplantación ARP. Para verificar que no se trate de algún ataque es necesario usar los filtros de visualización para la exploración de puertos. La sección Note muestra que existen algunos problemas con TCP, un par con IPv4 y una con TLS, sin embargo, se observa que con Ethertype el recuento de paquetes es demasiado alto, esto genera una posible amenaza para el rendimiento de la red.

Gravedad	Resumen	Grupo	Protocolo	Recuento
Error	Expected: 6 bytes	Malformed	KNX/IP	4
Warning	Duplicate IP address configured (10.0.3.1)	Sequence	ARP/RARP	2
Warning	TCP Zero Window segment	Sequence	TCP	4
Warning	The non-SYN packet does contain a MSS option	Protocol	TCP	7
Warning	No response seen to ICMP request	Sequence	ICMP	463
Warning	DNS query retransmission. Original request in frame 11255	Protocol	mDNS	3527
Warning	Ignored Unknown Record	Protocol	TLS	940
Warning	DNS response retransmission. Original response in frame 1...	Protocol	mDNS	3980
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	565
Warning	ACKed segment that wasn't captured (common at capture...	Sequence	TCP	41
Warning	D-SACK Sequence	Sequence	TCP	604
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	10413
Warning	Connection reset (RST)	Sequence	TCP	5983
Note	The acknowledgment number field is nonzero while the A...	Protocol	TCP	4
Note	ACK to a TCP keep-alive segment	Sequence	TCP	2
Note	TCP keep-alive segment	Sequence	TCP	2
Note	ARP packet storm detected (30 packets in < 100 ms)	Sequence	ARP/RARP	5241
Note	"Time To Live" != 255 for a packet sent to the Local Networ...	Sequence	IPv4	618
Note	This frame undergoes the connection closing	Sequence	TCP	177
Note	This session reuses previously negotiated keys (Session res...	Sequence	TLS	19
Note	A new tcp session is started with the same ports as an earli...	Sequence	TCP	1246
Note	"Time To Live" only 1	Sequence	IPv4	360
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	290
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	3252
Note	This frame is a (suspected) retransmission	Sequence	TCP	8744
Note	This frame initiates the connection closing	Sequence	TCP	309
Note	Duplicate ACK (#1)	Sequence	TCP	83481
Note	Didn't find padding of zeros, and an undecoded trailer exis...	Protocol	Ethertype	346755
Chat	Possible traceroute: hop #6, attempt #3	Sequence	UDP	13
Chat	GET /?q=ultrasurf HTTP/1.1\r\n	Sequence	HTTP	11
Chat	TCP window update	Sequence	TCP	177
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	4833
Chat	Connection establish request (SYN): server port 3389	Sequence	TCP	8019
Chat	Connection finish (FIN)	Sequence	TCP	486

Figura 4.15: Resumen de la segunda captura de paquetes en la Universidad de Oaxaca de Juárez.

El análisis de este archivo se inicia utilizando el filtro `arp.duplicate-address-detected || arp.duplicate-address-frame`, con base al resumen de la Información Especializada, se observa que hay dos paquetes con suplantación ARP de respuesta, es decir, el posible atacante envía directamente una respuesta sin que exista una solicitud, esto se observa en la Figura 4.16 y 4.17. Sin embargo, los paquetes filtrados se caracterizan como una amenaza falsa positiva debido a que la comunicación entre emisor y destino pertenecen a usuarios conocidos dentro de la misma red universitaria.

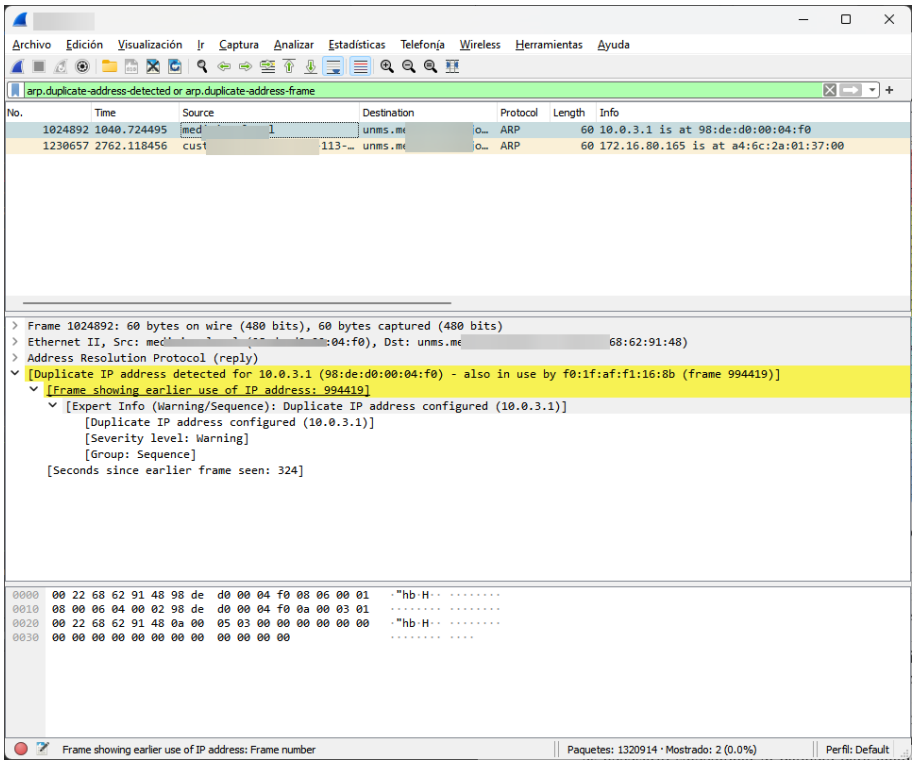


Figura 4.16: Posible ataque MitM mediante suplantación ARP del paquete 1.

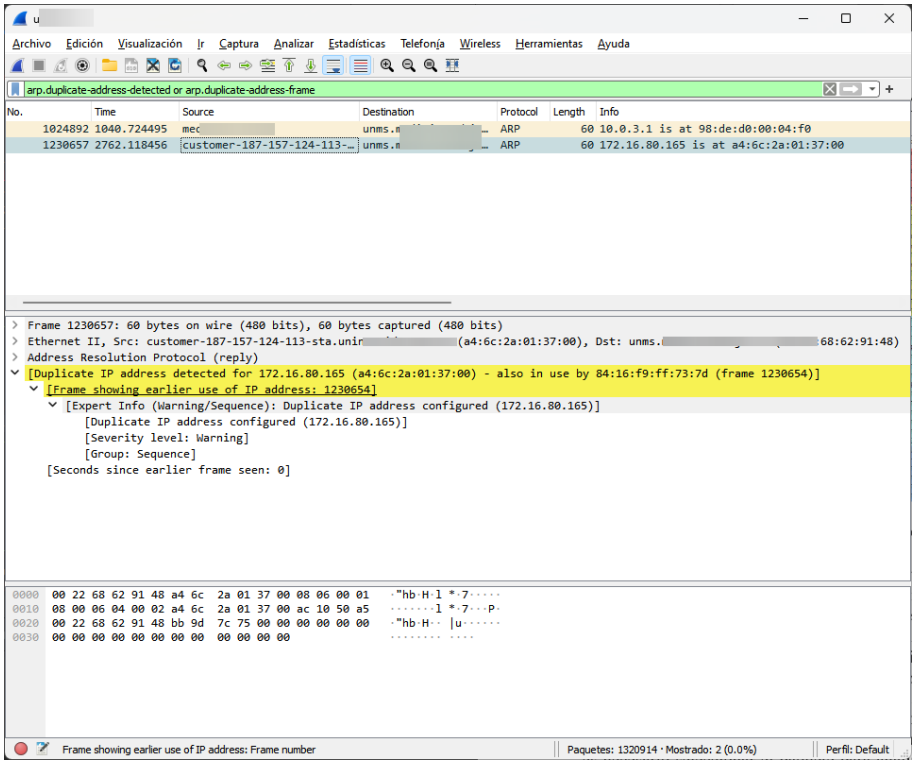


Figura 4.17: Posible ataque MitM mediante suplantación ARP del paquete 2.

Posteriormente, se utilizó el filtro para detectar posibles ataques ICMP. Básicamente consiste en detectar si existe una inundación de ICMP (ataque de denegación de servicio). Un *ping* ICMP estándar típico envía paquetes con 32 bytes de datos (comando *ping* en Windows) o 48 bytes (comando *ping* en Linux). Cuando alguien está haciendo una inun-

dación ICMP, normalmente envía datos mucho más grandes, por lo que el filtro utilizado muestra paquetes ICMP con tamaño de datos de más de 48 bytes. Esto detectará efectivamente cualquier inundación ICMP sin importar el tipo o código ICMP. Se observa en la figura que el número de paquetes filtrados es muy pequeño; llega a 286 paquetes. Muchas veces, esta cifra de paquetes no se puede considerar como ataque a una red, probablemente es una vulnerabilidad que, si no se corrige, puede ser un punto de partida para un ataque a mayor escala como denegación de servicio distribuido (véase Figura 4.18). Esto se clasifica como un caso verdadero negativo debido a que el filtro muestra 286 paquetes, quiere decir que probablemente los mecanismos de seguridad de la red rechazaron adecuadamente la inundación de paquetes ICMP.

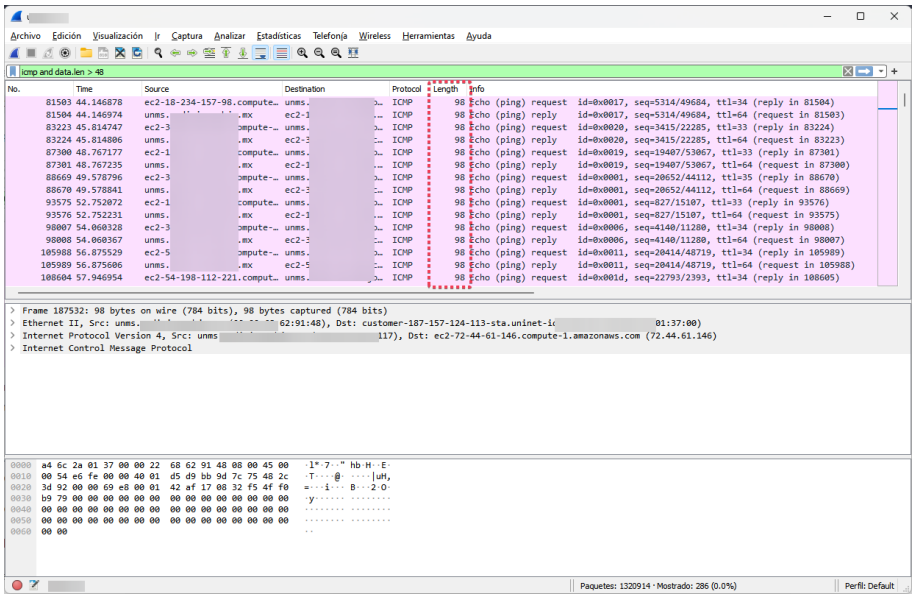


Figura 4.18: Inundación ICMP.

En cuanto al error y la advertencia sobre TLS mostrado en la Figura 4.15, se utilizó el filtro `tls.alert_message` para mostrar las alertas que se deben considerar sobre TLS. En la Figura 4.19 se observa que el paquete contiene la información Encrypted Alert (Alerta Encriptada), esto indica que Wireshark no puede descifrar el paquete. Varía la razón por la que puede aparecer este paquete, sin embargo, si aparece justo antes de un TCP FIN normalmente se toma como un cierre de notificaciones aunque éste no es el caso. La información de Ignored unknown record (Registro desconocido ignorado) significa que el procedimiento de TLS está fallando en algún punto. Por lo tanto, se trata de un caso verdadero positivo.

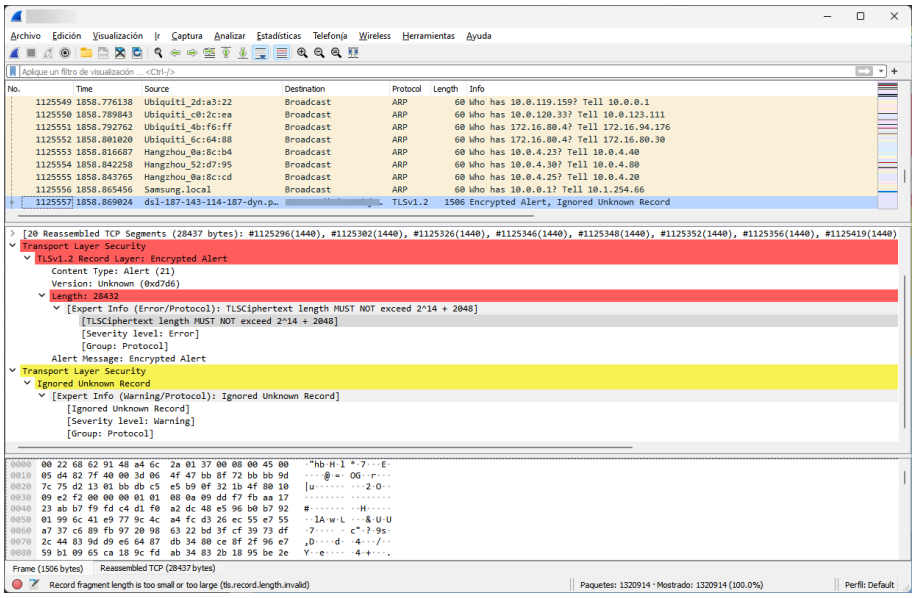


Figura 4.19: Mensaje de alerta TLS.

Finalmente, se aplica el filtro `tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.window_size <= 1024` para detectar si existen paquetes TCP SYN o escaneo de puertos (también conocidos como puertos semi-abiertos). Al utilizar este filtro se buscan paquetes que tengan la bandera SYN activada, la bandera ACK desactivada y que el tamaño de la ventana sea menor a 1024 bytes, al ser un tamaño de ventana pequeño se convierte en el parámetro característico utilizado por herramientas de monitoreo como Nmap, si aparecen paquetes con estas características indica que algún intruso está realizando barridos SYN o inundaciones SYN. La Figura 4.20 muestra un pequeño número de paquetes con las características mencionadas, por lo tanto, se clasifica como un caso verdadero negativo.

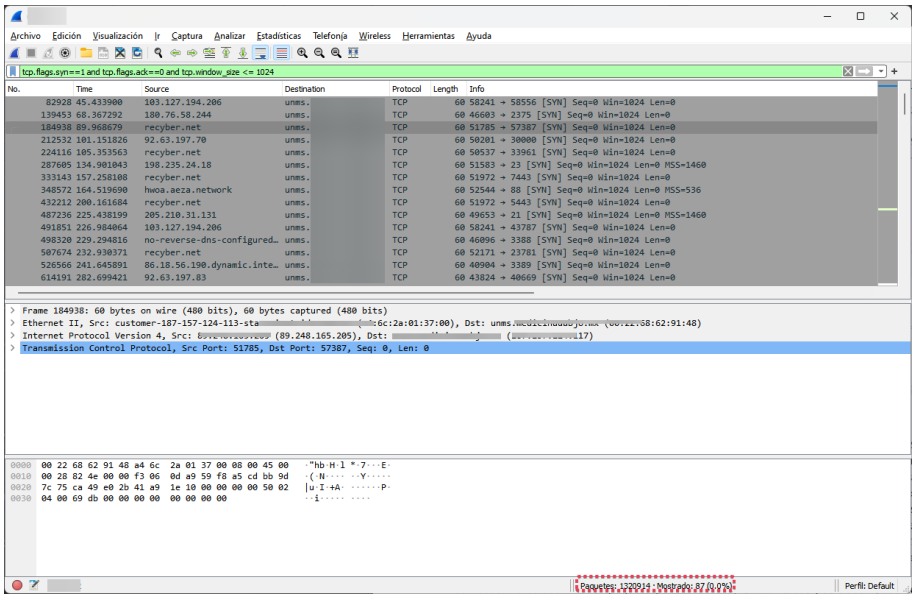


Figura 4.20: Análisis completo de las banderas de TCP.

Para finalizar el análisis de este archivo, se utilizó la herramienta de NetworkMiner, como muestra la Figura 4.21. Se observa que en la captura interactuaron 1137 huéspedes

(servidores y clientes), así mismo se iniciaron 12879 sesiones a diferentes sitios web y las anomalías que presenta son posibles ataques de suplantación ARP.

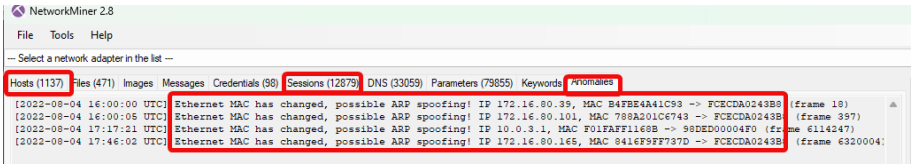


Figura 4.21: Resumen de anomalías desde NetworkMiner.

Por otro lado la Figura 4.21, las dos primeras posibles suplantaciones ARP se presentaron en el archivo de captura número 1, la tercer posible suplantación se observa en la Figura 4.22. La posibilidad de una suplantación ARP es demasiado alta pues son distintas direcciones; una IPv4 y la otra IPv6, este suceso se cataloga como un caso verdadero positivo.

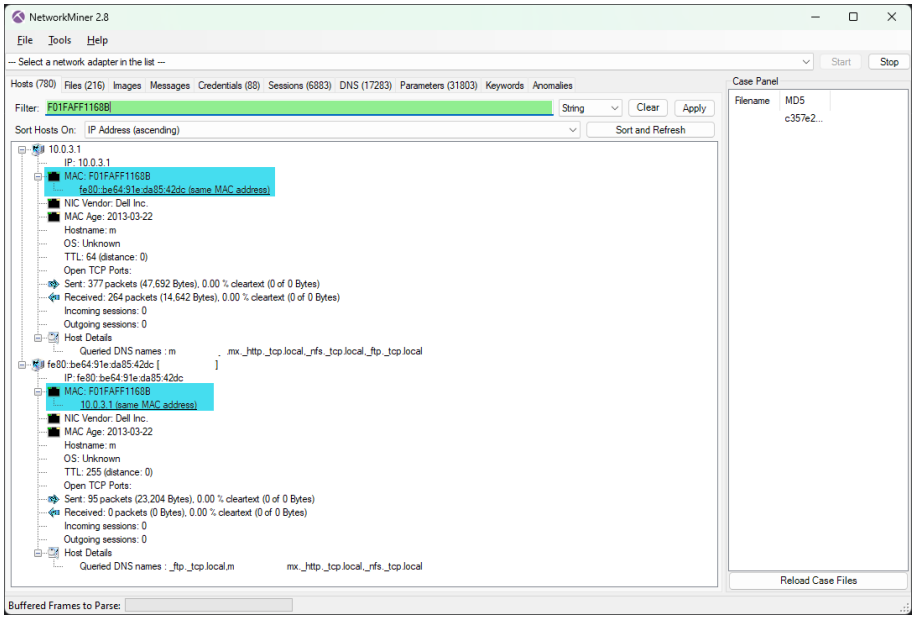


Figura 4.22: Direcciones IP con direcciones MAC duplicadas por un error en el servidor DHCP.

Continuando con la detección de amenazas del tercer archivo de captura, la Figura 4.23 muestra que en la sección Error existen tres casos que se tratan de paquetes mal formados, dos errores pertenecen a protocolos que se encuentran fuera del alcance de esta investigación, el otro error pertenece a TCP. En cuanto a la sección Advertencia, existe una que resulta de vital importancia pues es una probable suplantación ARP, el resumen que se muestra lo indica como Dirección IP duplicada, para visualizar estos paquetes se utiliza el filtro de suplantación ARP mostrado en la Tabla 2.6 de la sección 2.13.2. También se observan advertencias sobre el protocolo TCP, para esto es necesario utilizar los filtros de visualización para descartar algún intento de exploración y acceso a puertos. Finalmente TLS e ICMP resultan protocolos vulnerables ante algún ataque, de este modo es necesario seleccionar el paquete para analizar y evitar falsos positivos. Cabe señalar que el resumen general de Información Especializada muestra muchas veces advertencias en el protocolo TCP que puede estar relacionado con escaneo de puertos o ataques DDoS. Mientras que en la sección Note, el protocolo que predomina es TCP, también se observa un par de IPv4, protocolo Ethertype y ARP/RARP, este último indica que existe inundación de paquetes ARP con treinta paquetes en menos de 100 ms.

Figura 4.23: Resumen de la tercer captura de paquetes en la Universidad de Oaxaca de Juárez.

Para analizar detalladamente este archivo primero se utilizó el filtro de suplantación ARP; `arp.duplicate-address-detected || arp.duplicate-address-frame` (véase Figura 4.24). Se observa que todas las direcciones IP tienen la misma dirección MAC que el remitente y esa dirección MAC también es utilizada por otra dirección IP. Esto se denota como ataque MitM y se clasifica como verdadero positivo.

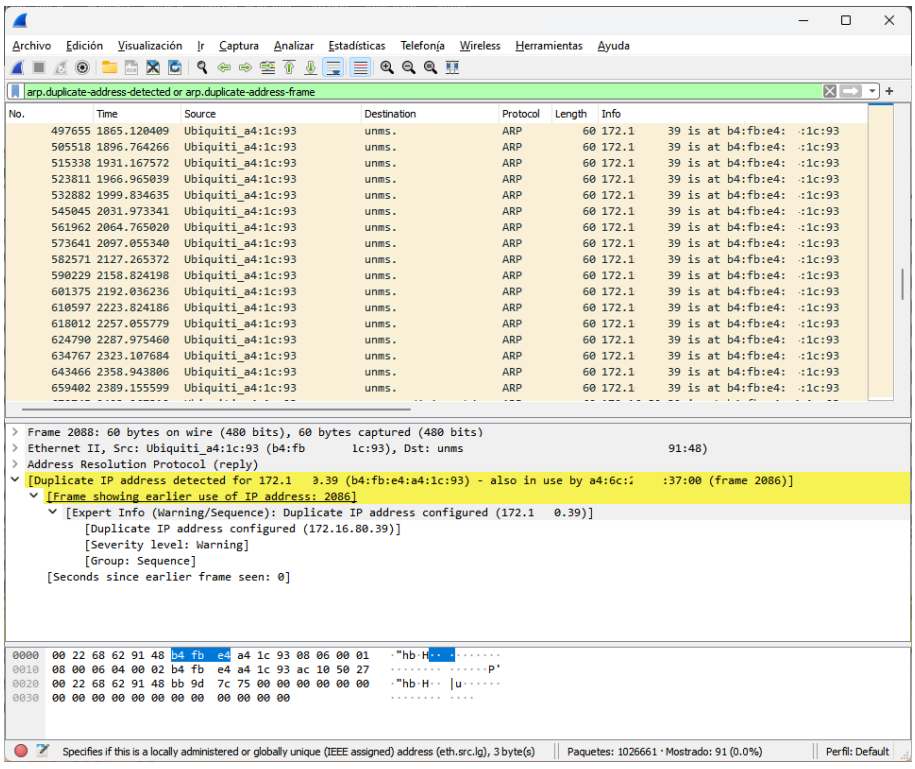


Figura 4.24: Posible ataque MitM mediante suplantación ARP.

Se utiliza el filtro `tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.window_size <= 1024` para detectar si existen TCP SYN o escaneo de puertos (también conocidos como puertos semi-abiertos). Aunque el número de paquetes filtrados en

la Figura 4.25 son muy inferiores a los paquetes capturados, esto se clasifica como verdadero positivo.

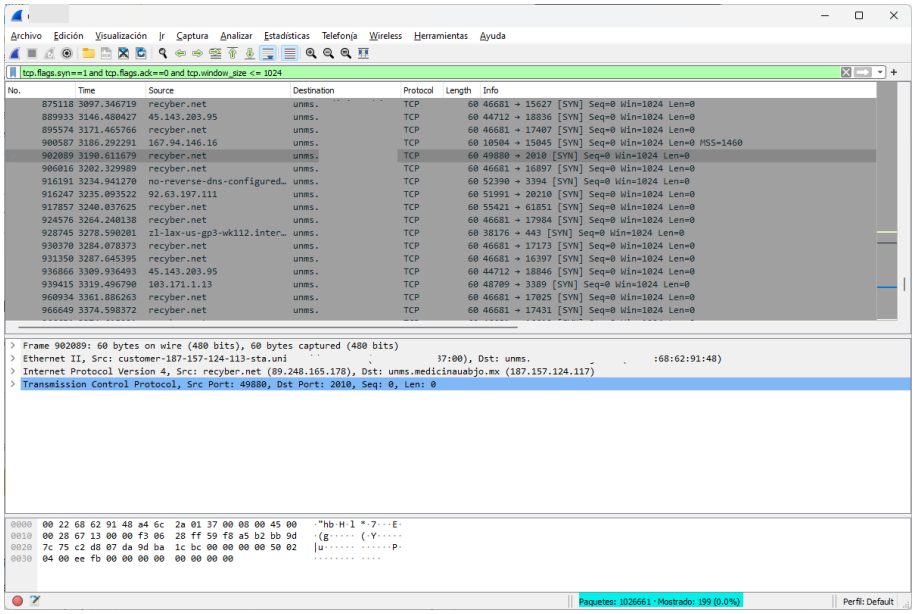


Figura 4.25: Análisis completo de las banderas de TCP.

En la Tabla 2.6 se observa el filtro de escaneo ARP, funciona para identificar las peticiones ARP con la dirección *broadcast* destinadas para descubrir direcciones IP dentro de la red. La Figura 4.26 detalla los paquetes filtrados en donde se lleva a cabo un escaneo ARP clasificado como verdadero positivo.

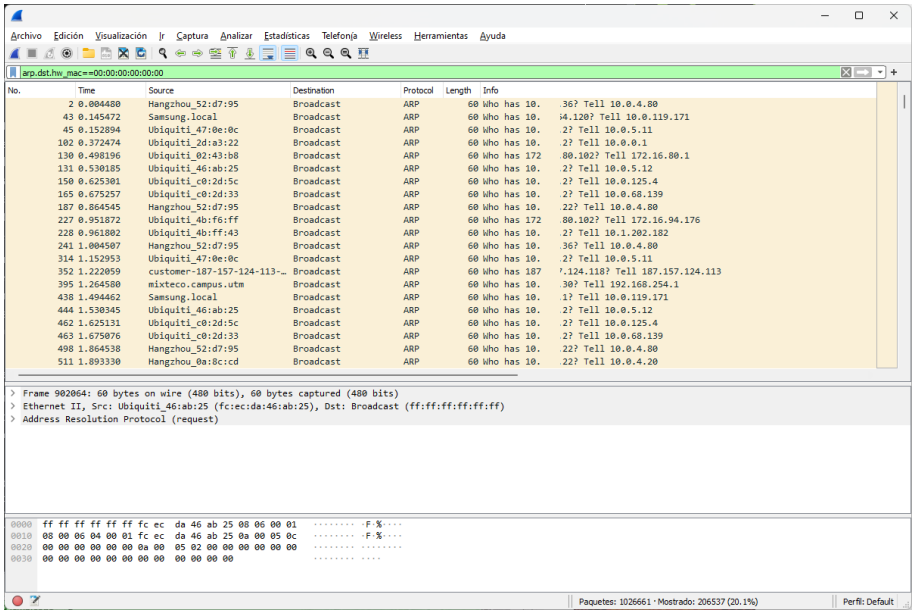


Figura 4.26: Paquetes filtrados a causa de un escaneo ARP.

De la Figura 4.26, el presunto atacante es aquel que pregunta por cierta dirección IP (Tell `10.0.4.80`). Las peticiones ARP que existan en un tiempo demasiado corto preguntando por IP aleatorias, probablemente se deben a que algún intruso está descubriendo direcciones IP activas.

Por otro lado, con base a la información mostrada en la Figura 4.23, es necesario

aplicar el filtro de barrido *ping* ICMP (véase la Figura 4.27). Es necesario la aplicación de este filtro para visualizar peticiones ICMP Echo (tipo 8) o respuestas ICMP Echo (tipo 0). Los paquetes se muestran en un tiempo demasiado corto y apuntan a direcciones IP diferentes, por lo tanto es probable que se trate de un barrido *ping* ICMP y se clasifica como verdadero positivo.

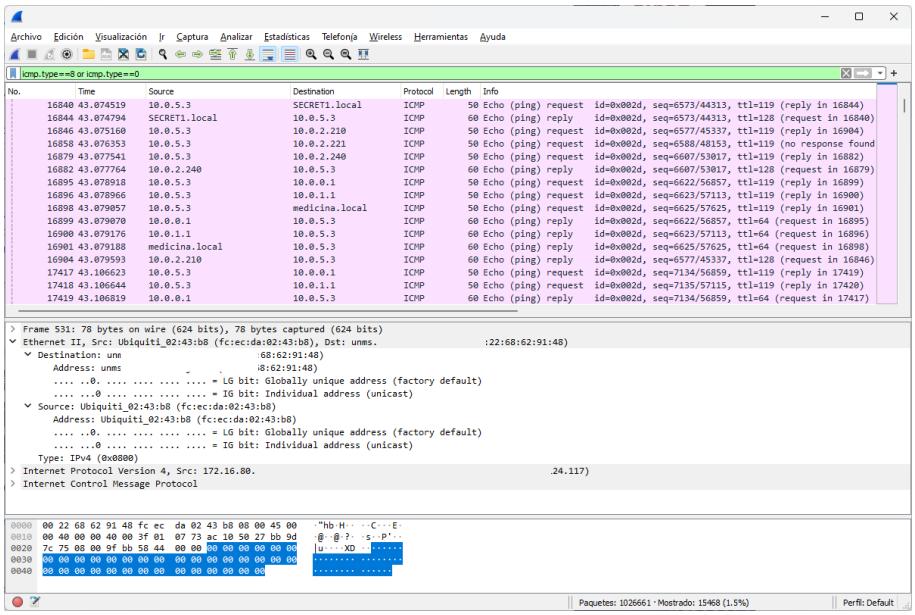


Figura 4.27: Inundación ICMP.

Con respecto a la Figura 4.28, al aplicar el filtro `tls.alert_message.desc`, se observa que el último paquete posee el mensaje Bad Record MAC, indicando que se ha recibido un registro con una MAC incorrecta; se trata de un error fatal y se cataloga como verdadero positivo.

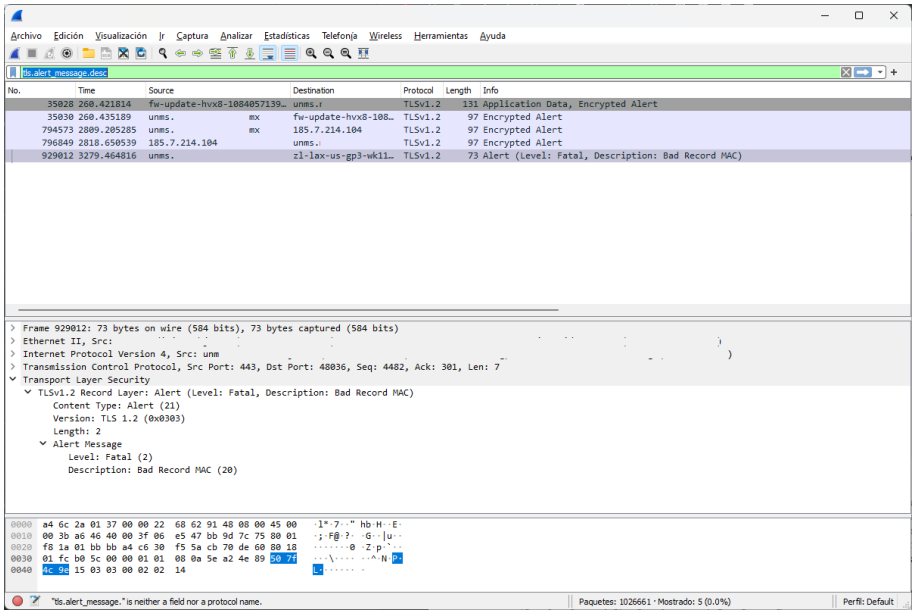


Figura 4.28: Paquetes TLS con mensajes de alerta.

Finalmente, para este archivo de captura se realizó un análisis con la herramienta NetworkMiner. La Figura 4.29 muestra un resumen donde se observa que en la captura in-

teractuaron 567 huéspedes (servidores y clientes), se iniciaron 6512 sesiones a diferentes sitios web y se detectaron 2 posibles suplantaciones ARP.

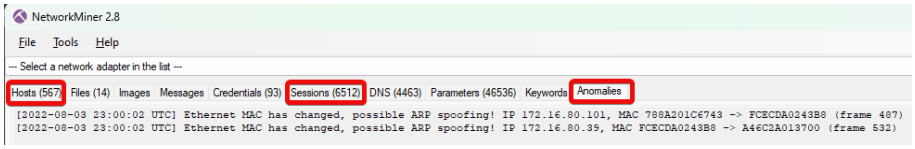


Figura 4.29: Resumen de amenazas desde NetworkMiner.

Al mismo tiempo, se observa que el archivo posee las mismas direcciones IP con posible suplantación ARP que los archivos de captura 1 y 2. Ante esta situación es necesario verificar detalladamente la configuración de la red. Es necesario recordar que la dirección IP `172.16.*.*` de forma predeterminada se especifica como una dirección utilizada para redes locales. Por lo tanto, estas amenazas se clasifican como falsas positivas, puesto que el problema que el NetworkMiner detecta se basa en una configuración incorrecta de la red.

En la Figura 4.30 se observa que existen 2 errores involucrando protocolos que se encuentran fuera del alcance de esta investigación. En cuanto a las advertencias también indica que posiblemente exista una suplantación ARP, el resumen que se muestra lo denota como Dirección IP duplicada. Es necesario utilizar el filtro de visualización para verificar que se trate de un ataque ARP. Otros protocolos de interés para el desarrollo de esta investigación son ICMP, TLS y TCP.

Figura 4.30: Resumen de la cuarta captura de paquetes en la Universidad de Oaxaca de Juárez.

En la Figura 4.31 se destaca que la mitad de los paquetes han sido escaneados y contienen el protocolo ARP, dentro de estos paquetes se encuentra el servidor de la UTM. ¿Existe una razón por la que el servidor de la UTM esté transmitiendo *broadcast* en la red de la Universidad de Oaxaca de Juárez? La respuesta puede ser por una configuración inapropiada en los nodos de la red tanto en la universidad de Oaxaca como en la UTM. Esto no se trata de un ataque. La función de ARP es buscar direcciones IP que sean solicitadas por el origen para compartir información, una vez que la información ha sido transmitida y exista una respuesta los datos de la máquina destino quedan almacenados en el conmutador. Cuando existe mucho tráfico *broadcast* es que la administración de la red no está funcionando adecuadamente y por diferentes razones los datos no han sido

almacenado por el conmutador. Con base a la información encontrada, esta amenaza se clasifica como verdadero positivo.

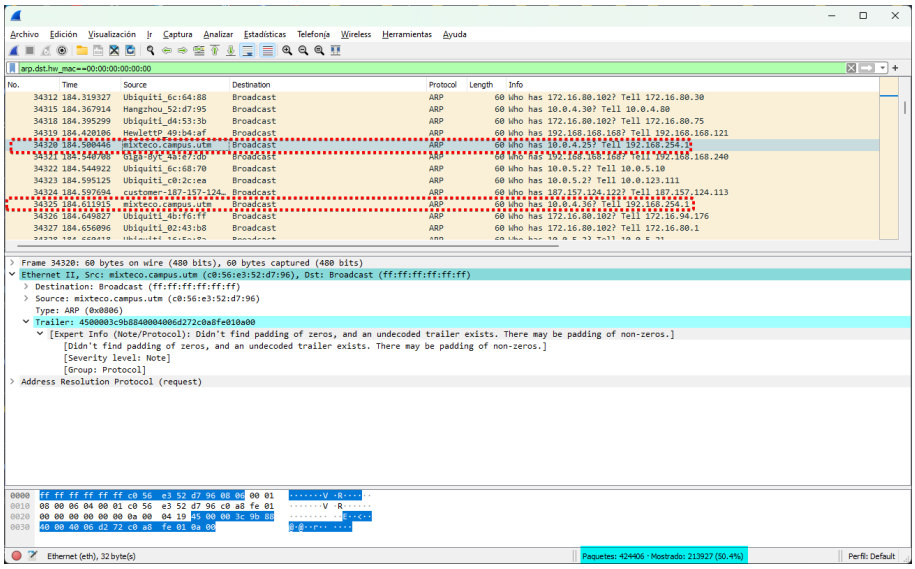


Figura 4.31: Paquetes que presentan características de un escaneo ARP.

En la Figura 4.32 se utilizó el filtro `arp.duplicate-address-detected || arp.duplicate-address-frame`, este filtro se encarga de mostrar los paquetes en donde exista posible suplantación ARP, sin embargo, al aplicar el filtro los paquetes mostrados son solicitudes y respuestas en ARP; estas características no pertenecen a una suplantación ARP. Este problema suele suceder por conflictos en los enrutadores, es decir una imperfección a la hora de implementar los protocolos de enrutamiento (tema fuera del alcance de esta investigación). Este tipo de amenaza se clasifica como falso positivo.

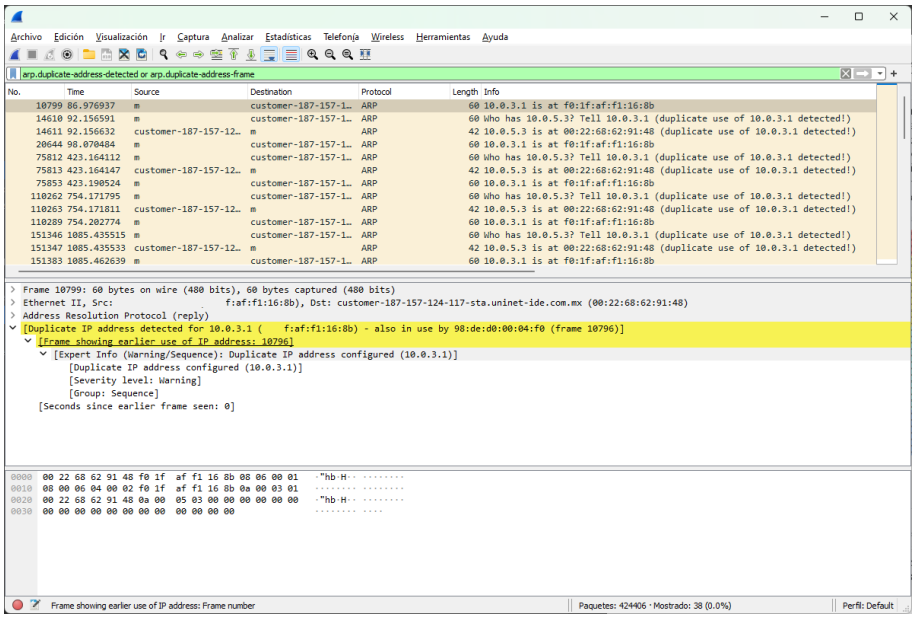


Figura 4.32: Paquetes con posible suplantación ARP.

Continuando con el análisis del archivo, en la Figura 4.33 se muestran los resultados de utilizar el filtro `icmp.type==8 || icmp.type==0` para mostrar algunos paquetes que cumplen con las características del barrido ICMP. Es notable la presencia de otros

paquetes, sin embargo, estos paquetes poseen una respuesta ante una petición y los paquetes enmarcados en la columna Info tienen el mensaje no response found!. Así mismo, las direcciones IP destino tienden a incrementar su último byte. Esta amenaza se clasifica como verdadero positivo.

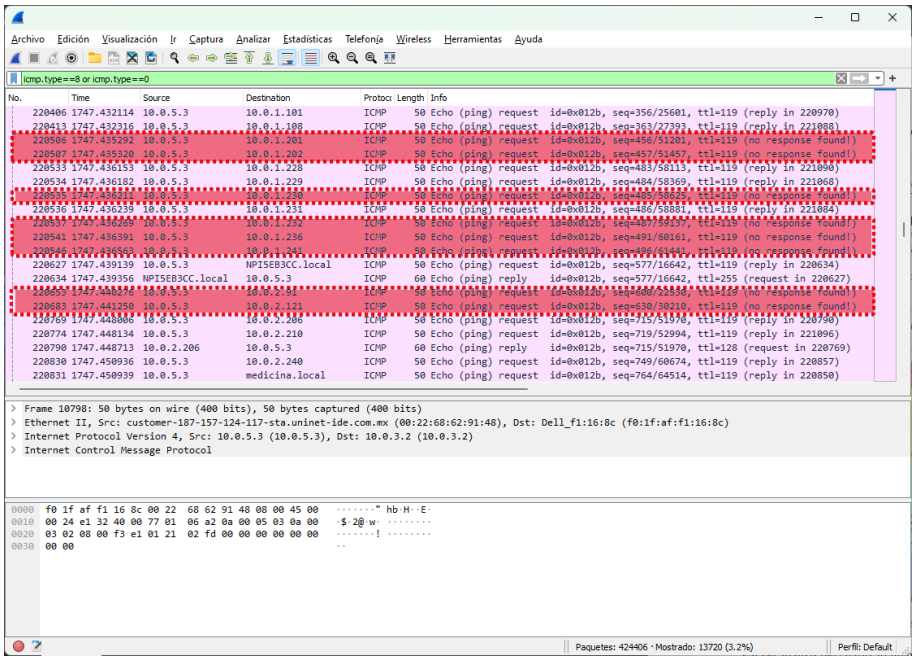


Figura 4.33: Barrido *ping* ICMP.

Ahora, comenzando con el escaneo de puertos mediante TCP, primero se utiliza el filtro `tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.window_size<=1024`, para mostrar los paquetes que tengan la bandera SYN activada, la bandera ACK desactivada y un tamaño de ventana mayor a 1024 bytes. El número de paquetes mostrado en la Figura 4.34 es 105 por lo que la probabilidad de que exista un escaneo es demasiado baja o probablemente los mecanismos de seguridad implementados en la red detectaron la amenaza y la mitigaron. Ante las premisas mencionadas, la clasificación es verdadero positivo.

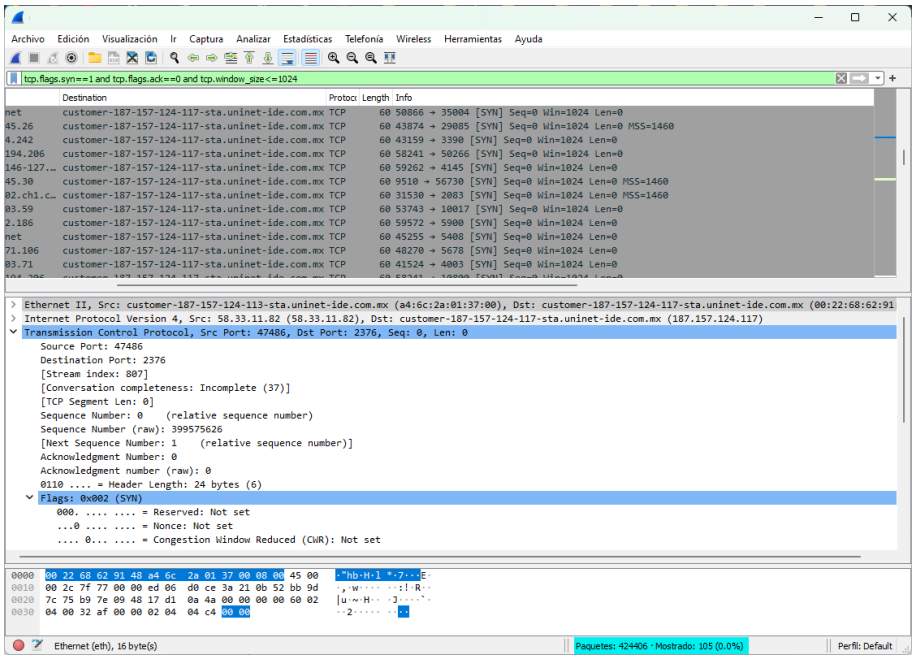


Figura 4.34: Escaneo de banderas SYN a través de TCP.

Posteriormente, con el filtro `tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.window_size > 1024`, la diferencia que presenta con el filtro anterior es el tamaño de la ventana. Se observa que existen paquetes coloreados por la categoría Chat de la Información especializada (véase Figura 4.35).

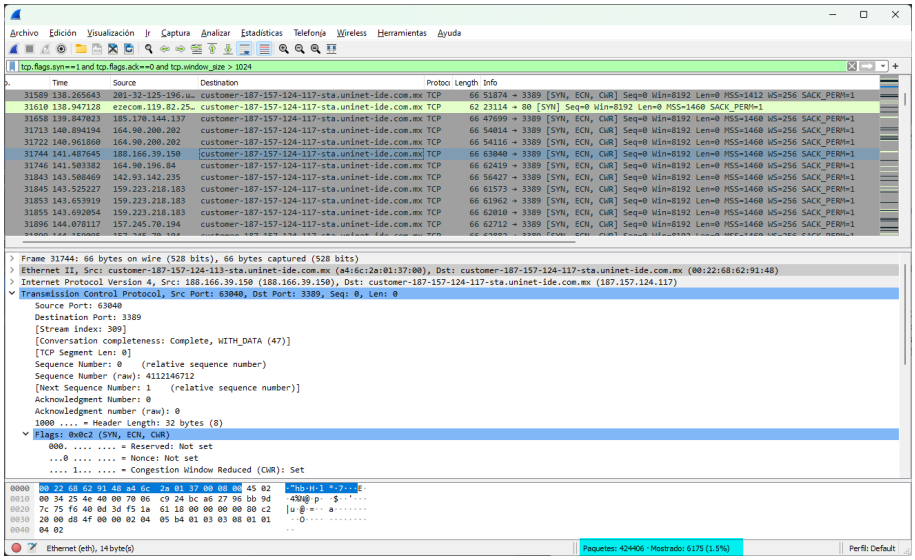


Figura 4.35: Escaneo de banderas SYN con mayor tamaño de ventana.

Cuando alguien está realizando una inundación ICMP, típicamente se envían datos muy grandes. Mediante el filtro `icmp && data.len > 48` se muestran los paquetes ICMP con tamaño de datos de más de 48 bytes. Utilizando este filtro se detecta cualquier inundación ICMP independientemente del tipo o código ICMP (véase Figura 4.36). Estos paquetes se clasifican como verdadero positivo.

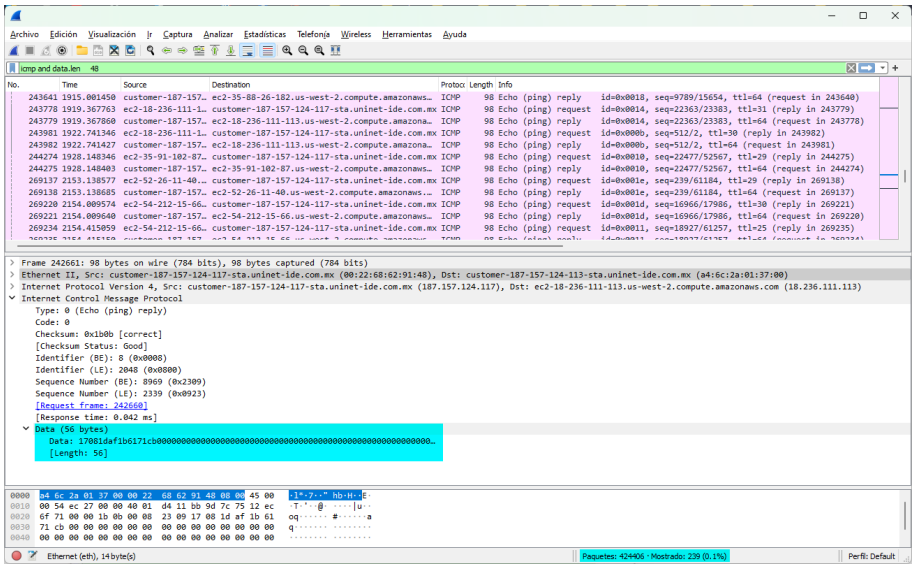


Figura 4.36: Inundación ICMP.

Finalmente, al utilizar el filtro `tcp.analysis.lost_segment || tcp.analysis.retransmission`, se observa que Wireshark presenta los paquetes con un coloreado oscuro, lo que indica Wireshark es que se trata de paquetes TCP erróneos. Así mismo, se observa que un gran número de paquetes son retransmitidos, sto apunta a un problema severo en la red. Es posible que se trate de un ataque DDoS a una escala muy pequeña pues el porcentaje de paquetes filtrados es de 0.5 % (véase Figura 4.37), por tanto entra en la clasificación de verdadero positivo.

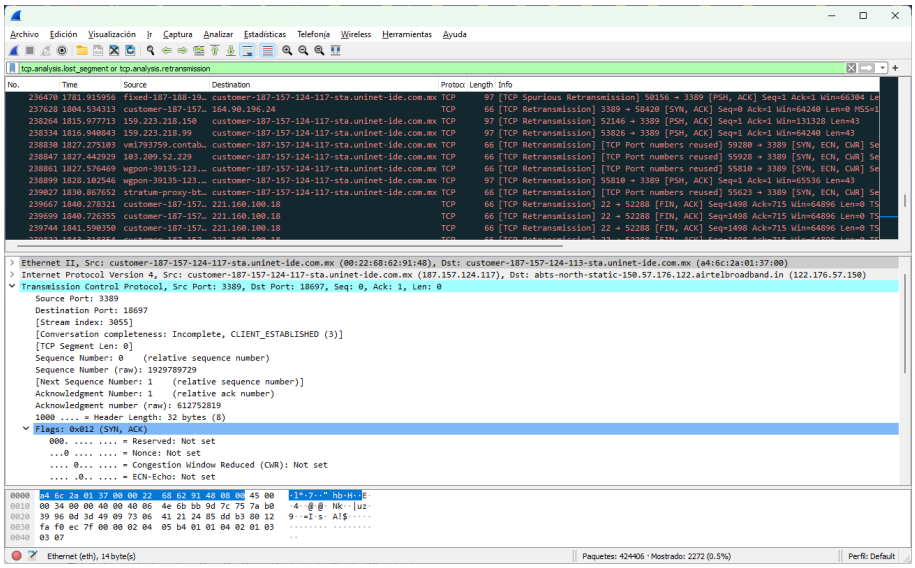


Figura 4.37: Paquetes TCP retransmitidos y perdidos.

Para finalizar el análisis de este archivo, la Figura 4.38 muestra que durante la captura del archivo se realizaron 1579 conexiones entre huéspedes (servidores y clientes), ocurrieron 25239 inicios de sesión y se registraron anomalías de posible suplantación ARP.

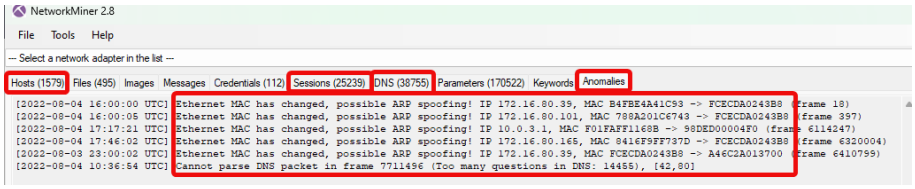


Figura 4.38: Resumen de anomalías desde NetworkMiner.

Al revisar detalladamente las direcciones IP, se observa que las primeras dos posibles suplantaciones son similares a los archivos de captura 1, 2 y 3. Al filtrar la dirección MAC, lo que aparece es un problema con el servidor DHCP (véase Figura 4.39) y se clasifica como una amenaza falso positivo.

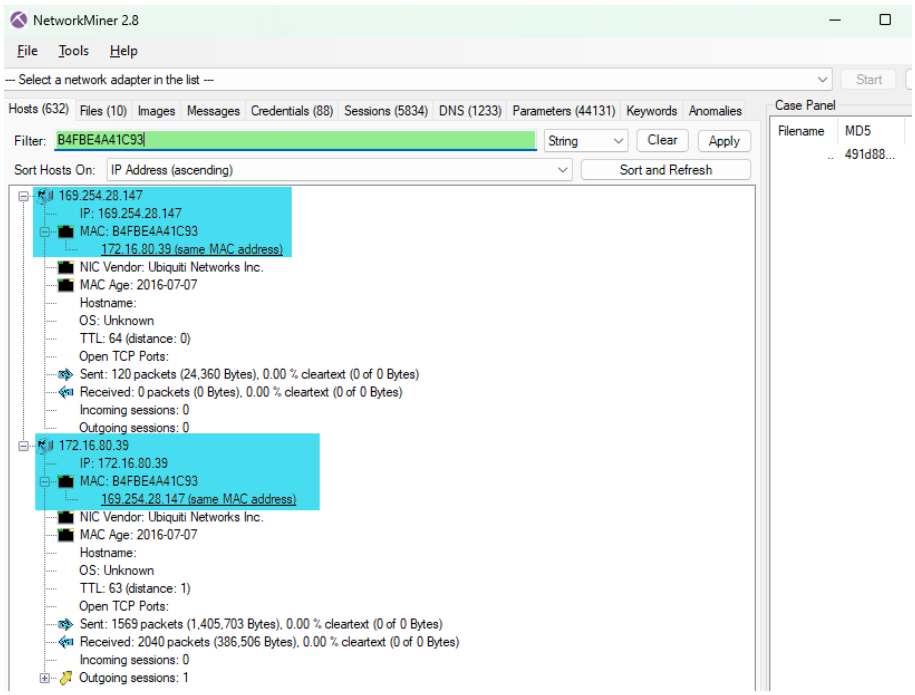


Figura 4.39: Error en el servidor DHCP.

En cuanto a las otras direcciones IP de la Figura 4.38, la probabilidad de que se trate de suplantación ARP es alta convirtiéndose en un caso verdadero positivo.

Para el quinto archivo, la Figura 4.40 muestra ocho errores de los cuales el protocolo de importancia es TLS. En cuanto a las advertencias, existen trece, de las cuales seis tienen que ver con el protocolo TCP. Para descartar posibles ataques DDoS o exploración de puertos de red es necesario utilizar los filtros de visualización.

Gravedad	Resumen	Grupo	Protocolo	Recuento
Error	Malformed Packet (Exception occurred)	Malformed	mDNS	1
Error	Invalid Setting for PAN ID Compression	Malformed	IEEE 802.15.4	1
Error	Frame Version Unknown Cannot Dissect	Malformed	IEEE 802.15.4	1
Error	Malformed Packet (Exception occurred)	Malformed	Manolito	1
Error	Malformed Packet (Exception occurred)	Malformed	HCrt	1
Error	Malformed Packet (Exception occurred)	Malformed	ENIP	2
Error	TLSCiphertext length MUST NOT exceed 2^14 + 2048	Protocol	TLS	2
Error	Malformed Packet (Exception occurred)	Malformed	TZSP	2
Warning	TCP Zero Window segment	Sequence	TCP	1
Warning	DNS response retransmission. Original response in frame 3...	Protocol	DNS	1
Warning	DNS query retransmission. Original request in frame 263210	Protocol	DNS	1
Warning	Unknown type 194	Protocol	Manolito	26
Warning	The non-SYN packet does contain a MSS option	Protocol	TCP	2
Warning	No response seen to ICMP request	Sequence	ICMP	523
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	116
Warning	DNS response retransmission. Original response in frame 1...	Protocol	mDNS	2417
Warning	Ignored Unknown Record	Protocol	TLS	545
Warning	D-SACK Sequence	Sequence	TCP	268
Warning	DNS query retransmission. Original request in frame 79	Protocol	mDNS	2596
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	447
Warning	Connection reset (RST)	Sequence	TCP	5323
Note	ACK to a TCP keep-alive segment	Sequence	TCP	8
Note	TCP keep-alive segment	Sequence	TCP	8
Note	The acknowledgment number field is nonzero while the A...	Protocol	TCP	2
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	10
Note	ARP packet storm detected (30 packets in < 100 ms)	Sequence	ARP/RARP	4855
Note	A new tcp session is started with the same ports as an earli...	Sequence	TCP	328
Note	"Time To Live" != 255 for a packet sent to the Local Networ...	Sequence	IPv4	430
Note	This frame undergoes the connection closing	Sequence	TCP	129
Note	This frame initiates the connection closing	Sequence	TCP	152
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	140
Note	This frame is a (suspected) retransmission	Sequence	TCP	1580
Note	"Time To Live" only 1	Sequence	IPv4	478
Note	Didn't find padding of zeros, and an undecoded trailer exis...	Protocol	Ethertype	5845
Note	Duplicate ACK (#1)	Sequence	TCP	1053
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	1
Chat	HTTP/1.1 400 Bad Request\r\n	Sequence	HTTP	29
Chat	Possible traceroute: hop #7, attempt #1	Sequence	UDP	29
Chat	Connection finish (FIN)	Sequence	TCP	281
Chat	TCP window update	Sequence	TCP	175
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	4900
Chat	Connection establish request (SYN): server port 3389	Sequence	TCP	5982

Figura 4.40: Resumen de la quinta captura de paquetes en la Universidad de Oaxaca de Juárez.

El análisis se inicia con el filtro `arp.dst.hw_mac==00:00:00:00:00:00` para mostrar paquetes con posible escaneo ARP. La Figura 4.41 muestra los resultados, sin embargo, no se trata de un ataque sino de una mala configuración de la red, lo que se deduce por que el origen de los paquetes es el servidor de la universidad. Por lo tanto se trata de un caso falso positivo.

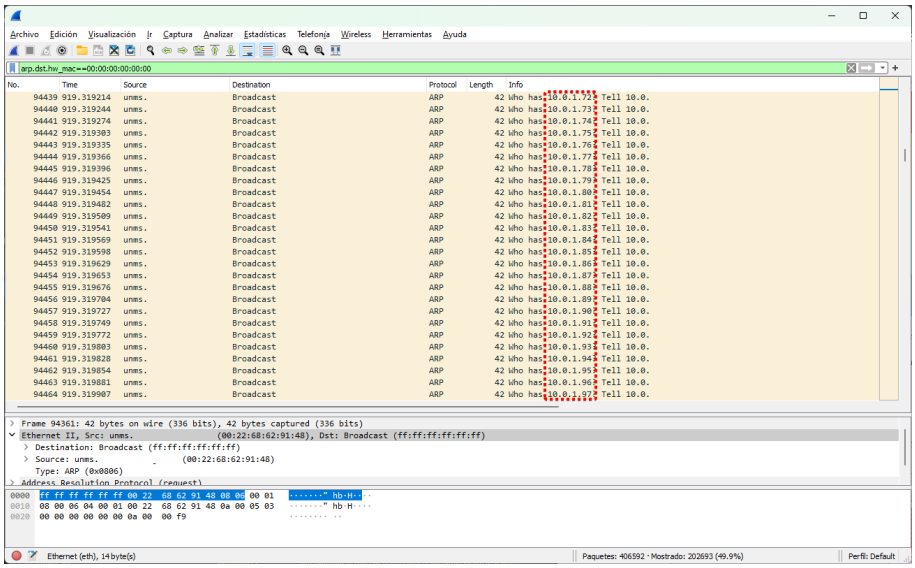


Figura 4.41: Paquetes que presentan un escaneo ARP.

Otro filtro a considerar durante el análisis es el `icmp.type==8 || icmp.type ==0` que muestra los paquetes que presentan un barrido *ping* para saber qué direcciones IP responden, con las posibles respuestas los atacantes pueden obtener algunos datos para efectuar un ataque. La figura 4.42 muestra los paquetes que presentan características del ataque, por lo tanto se clasifica como verdadero positivo.

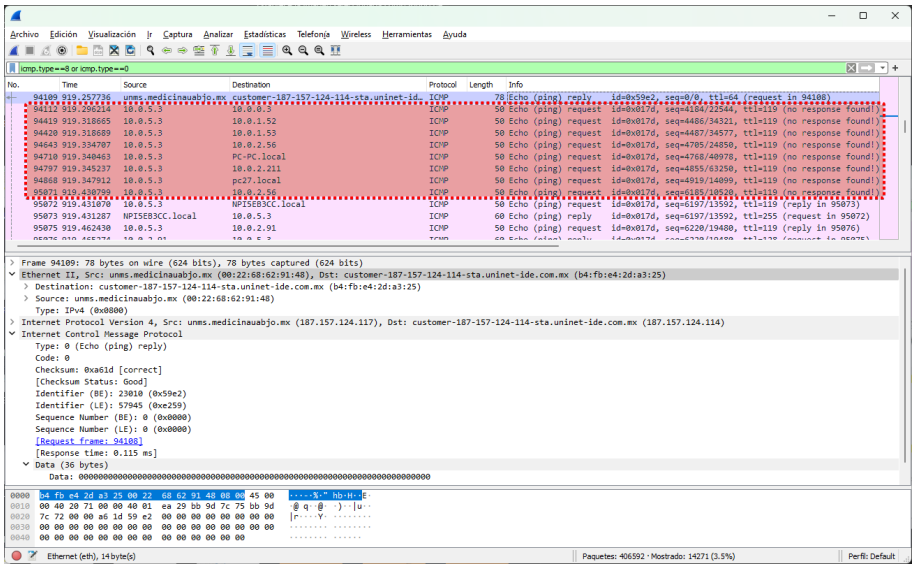


Figura 4.42: Barrido *ping* ICMP.

Al iniciar con el escaneo TCP, primero se comienza por la bandera SYN utilizando el filtro `tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.window_size <=1024`. Los paquetes se muestran en la Figura 4.43. Se puede considerar una amenaza al ser direcciones IP que no se encuentran en la red, sin embargo, apenas llegan a 100 paquetes, posiblemente los mecanismos de seguridad rechazaron las conexiones en su debido tiempo. Ante estas premisas se clasifica como un caso verdadero negativo.

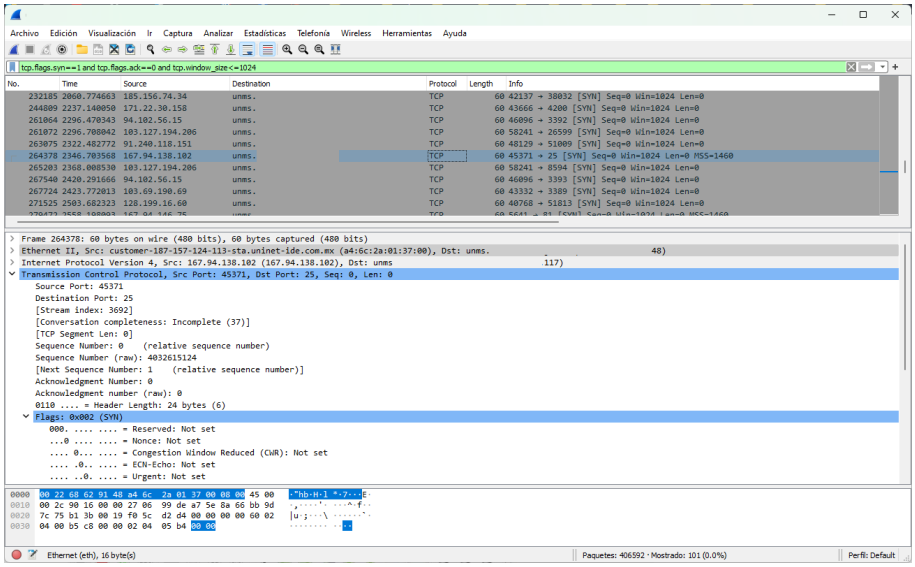


Figura 4.43: Paquetes con banderas SYN en TCP.

Continuando con el escaneo, la Figura 4.44 muestra paquetes relacionados con la conexión TCP, los paquetes filtrados poseen la bandera SYN acompañados de las banderas ECN y CWR que, como se mencionó en párrafos anteriores, dichas banderas indican que el mensaje ha sido entendido por el remitente. Finalmente se observa que la región de información de un paquete capturado está coloreado el protocolo TCP y específicamente en la bandera SYN.

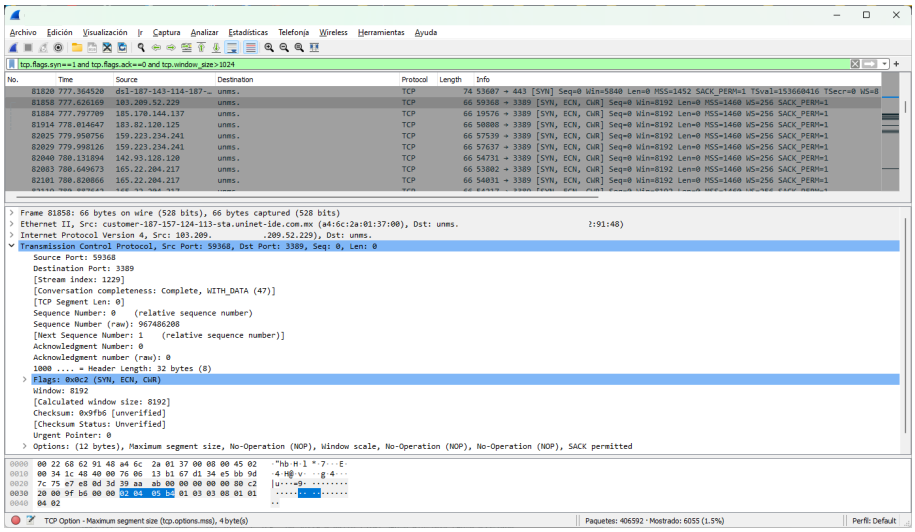


Figura 4.44: Escaneo TCP Connect.

La Figura 4.45 muestra paquetes filtrados que poseen características de una inundación ICMP, en donde todos los paquetes tienen una longitud mayor a 48 bytes (el paquete seleccionado muestra una longitud de 56 bytes). El porcentaje de paquetes capturados equivale a 0.1 %.

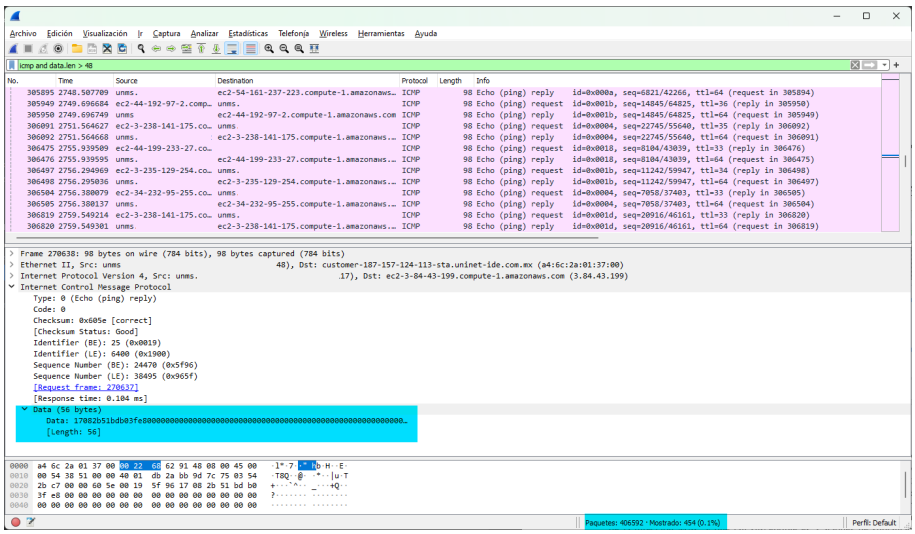


Figura 4.45: Paquetes con inundación ICMP.

Finalmente, la Figura 4.46 muestra paquetes TCP perdidos y retransmitidos, así mismo, dentro de un paquete que está siendo retransmitido se presentan anomalías con TLS, sin embargo, no se trata de alguna anomalía en la red, el mensaje aparece porque el tráfico capturado no se encuentra ensamblado. Para que Wireshark realice el ensamblaje es necesario seguir los siguientes pasos: Edición | Preferencias | Protocolos | TCP activar la casilla Permitir al subdisector reensamblar flujos TCP y Reensamblar segmentos fuera de orden | Aceptar. Siguiendo los pasos anteriores se vuelve a cargar el archivo y desaparecen los mensajes de TLS. Esta amenaza mostrada por Wireshark se clasifica como falso positivo.

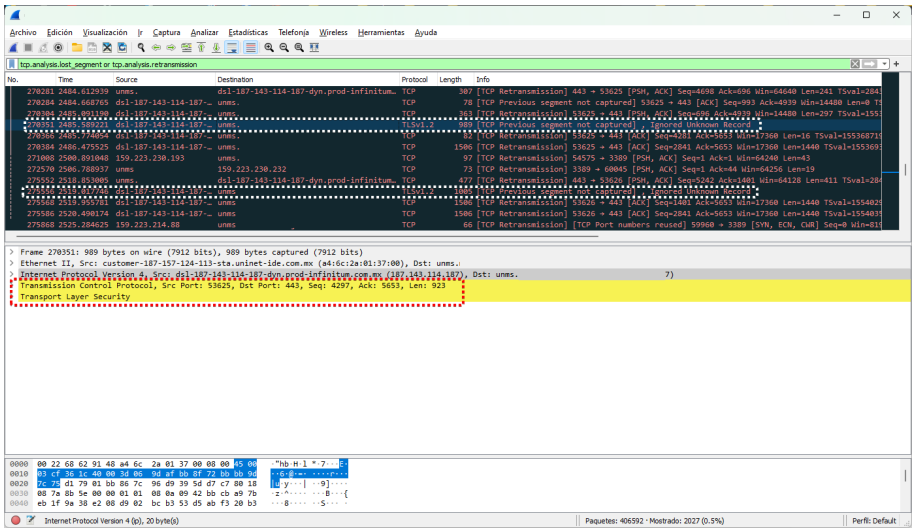


Figura 4.46: Paquetes TCP retransmitidos y perdidos.

En la Figura 4.47 se observa un resumen generado por la herramienta NetworkMiner, durante la conexión se interactuó con 1835 huéspedes, se iniciaron 30937 sesiones y se encontraron 6 posibles ataques de suplantación ARP.

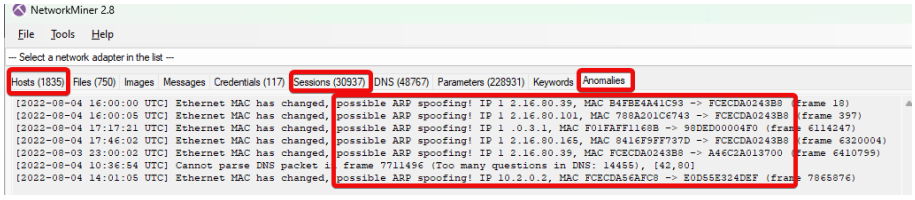


Figura 4.47: Resumen de anomalías desde NetworkMiner.

Las direcciones IP que se observan en la Figura 4.47 no presentan problemas con el servidor DHCP, sin embargo, la probabilidad que sea suplantación ARP es alta, o de lo contrario probablemente se trate de un tiempo excedido en la asignación de direcciones IP. Es necesario recordar que una dirección IP es asignable durante 24 horas, al exceder este tiempo es posible que tenga asignada una dirección nueva y por tal motivo contienen la misma dirección MAC.

Continuando con la detección de amenazas del sexto archivo, la Figura 4.48 muestra que se detectaron tres errores de los cuales el que resulta de interés para esta investigación es TLS. Otra manera de verificar los paquetes con errores es seleccionando el grupo e ir al paquete, sin la necesidad de utilizar un filtro. Dentro de las advertencias que resalta el resumen, existe la que pertenece al protocolo Ethernet. Esta advertencia resulta interesante debido a que alude a la dirección MAC, en secciones anteriores se mencionó la importancia de la dirección MAC y qué tan susceptible es a ataques de suplantación. En segundo lugar se observa la presencia de una posible suplantación de ARP, lo que se puede verificar utilizando el filtro de visualización mostrado en la Tabla 2.6 de la sección 2.13.2.

Finalmente, es necesario verificar los filtros de visualización para descartar posibles ataques DDoS o exploración en los puertos hacia el protocolo TCP. Es importante que se revise el ICMP para evitar ataques.

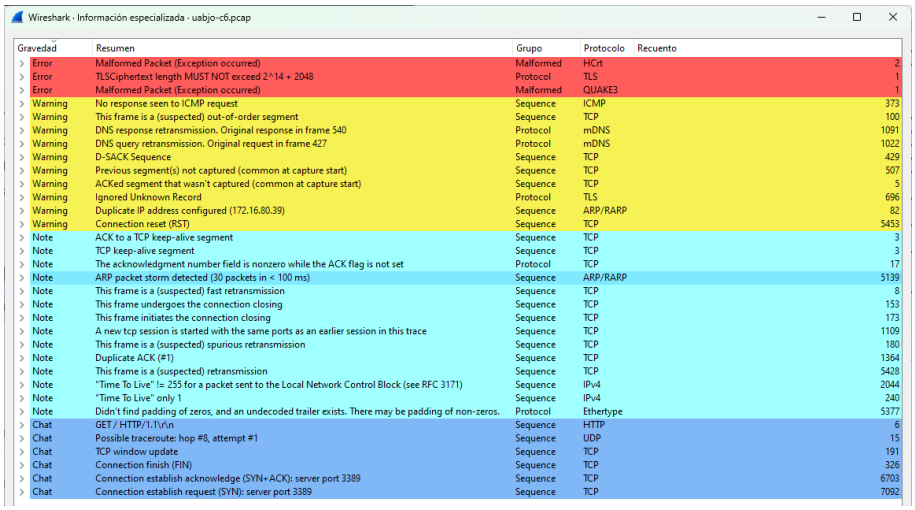


Figura 4.48: Resumen de la sexta captura de paquetes en la Universidad de Oaxaca de Juárez.

Al utilizar el filtro `arp.dst.hw_mac==00:00:00:00:00:00`, se muestran paquetes con el protocolo ARP, la fuente pertenece a direcciones no conocidas así como una del servidor de la UTM. Se observa que las máquinas fuente realizan peticiones ARP hacia el *broadcast*, sin embargo, en la columna Info muestra el mensaje Who has `10.x.x.x` (véase Figura 4.49). Esto significa que el huésped destino intenta descubrir ciertas direcciones IP, afortunadamente la aplicación del filtro en este archivo no se indica como un ataque puesto que no cumple una característica importante la cual es el tiempo; las peticiones se deben realizar en un corto periodo de tiempo. Otro aspecto a considerar es la petición ARP, la dirección IP por la que preguntan debe incrementar sucesivamente; es decir, si el ataque inicia preguntando por `192.168.23.0` el cuarto byte incrementaría de `0,1,2,3,4,5,6,7,8...n` hasta que encuentre una dirección que pueda responder ante esta petición y así concretar el ataque, por lo tanto se trata de una falso positivo.

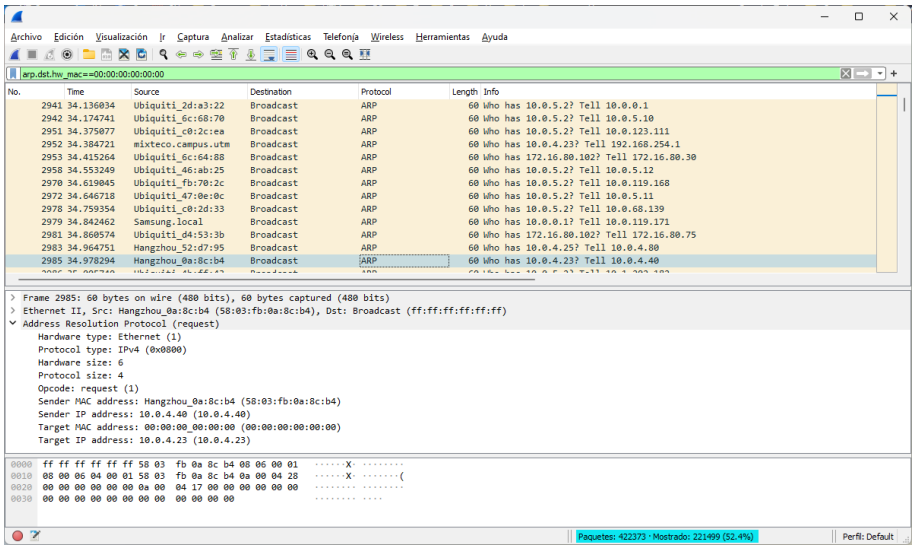


Figura 4.49: Paquetes filtrados que presentan características de escaneo ARP.

Al utilizar el filtro de barrido *ping* ICMP los paquetes que se muestran se observan en la Figura 4.50. Se presentan paquetes de petición y respuesta entre el servidor de la universidad y un cliente, comúnmente se realiza este barrido para descubrir las características de la víctima y así realizar un ataque completo. En este archivo, el porcentaje de

paquetes que se observan es de 3.7 % y se clasifica como caso verdadero positivo.

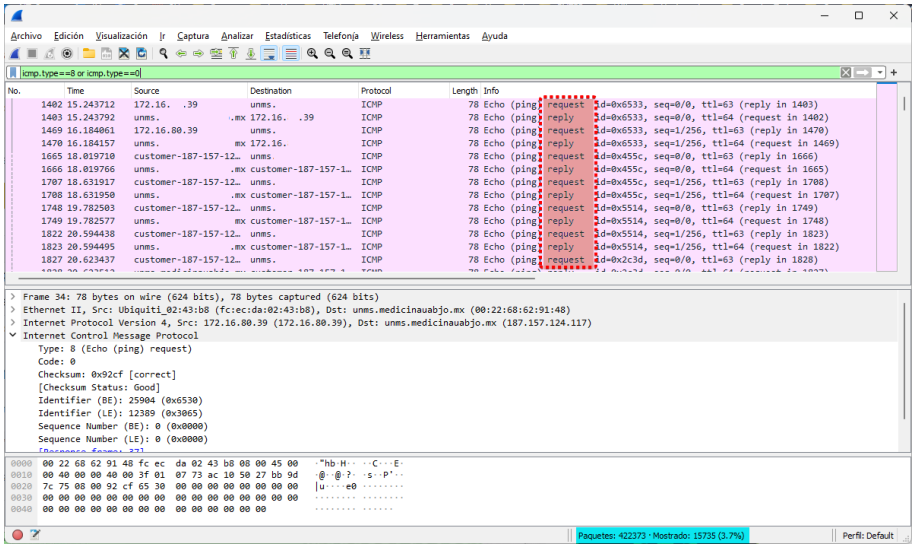


Figura 4.50: Barrido *ping* ICMP.

Continuando con los escaneos, es importante realizar filtrado de paquetes TCP con la bandera SYN activada, la Figura 4.51 muestra paquetes filtrados que conforman el primer paso del inicio de la conexión de tres vías y presentan características como tamaño de ventana muy pequeño (1024 bytes). En este tipo de escaneo, los paquetes que tienen el tamaño de ventana pequeño es el parámetro característico utilizado por herramientas que se encargan de escanear redes. Se trata de un ataque DDoS cuando se capturan paquetes en un corto período de tiempo, sin embargo, los paquetes filtrados son 80 que representan una cantidad mínima comparada con los paquetes capturados.

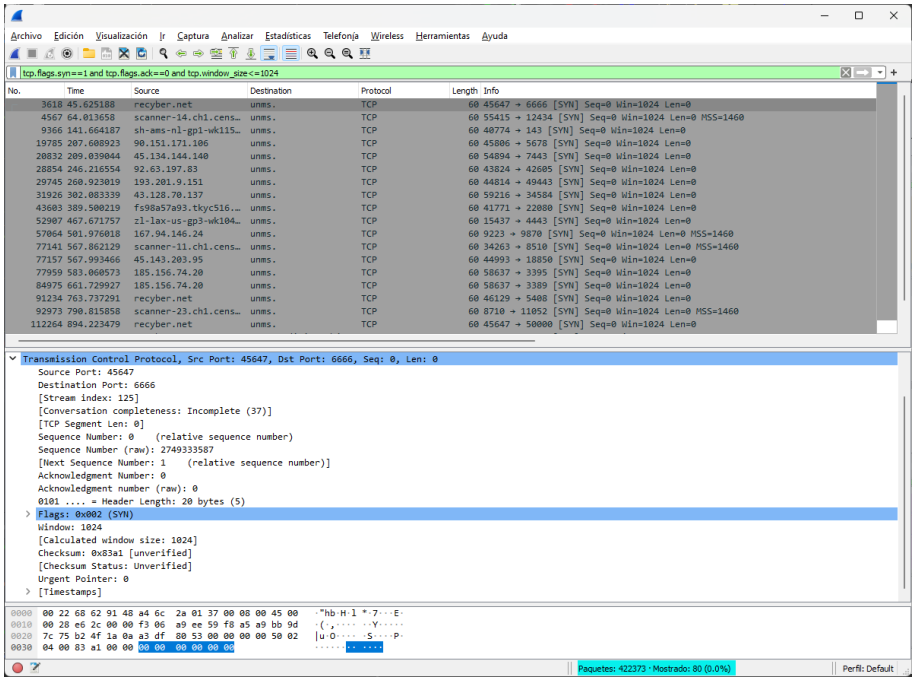


Figura 4.51: Escaneo TCP SYN.

La Figura 4.52 muestra paquetes TCP con la bandera SYN activada pero con un tamaño de ventana mayor a 1024 bytes, es la diferencia respecto al filtro utilizado para la

Figura 4.51. Se trata de un ataque DDoS cuando se capturan paquetes en un corto período de tiempo, sin embargo, los paquetes filtrados son 7129 que equivale al 1.7 % y se clasifica como amenaza verdadero positivo.

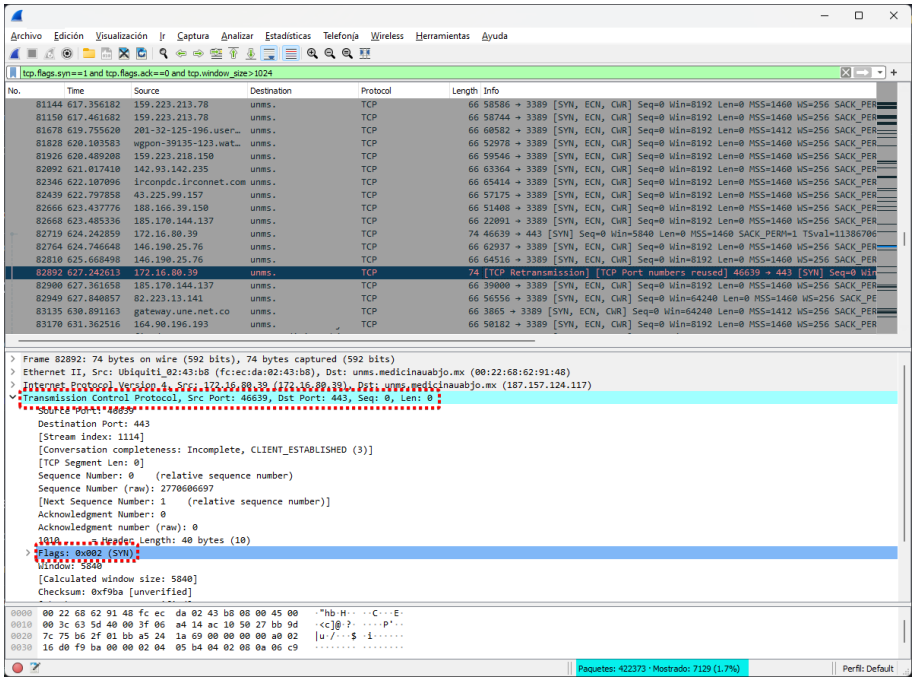


Figura 4.52: Escaneo TCP Connect.

En cuanto a la Figura 4.53, se muestran los paquetes que poseen las siguientes características: los paquetes que tengan una longitud mayor a 48 bytes. En el caso del paquete seleccionado, tiene una longitud de 56 bytes. Sin embargo, el número de paquetes filtrados es menor comparado con los paquetes capturados. Es probable que el número de paquetes sea menor debido a un rechazo correcto por parte de los mecanismos de seguridad implementados en la red, por ello, se clasifica como un caso verdadero negativo.

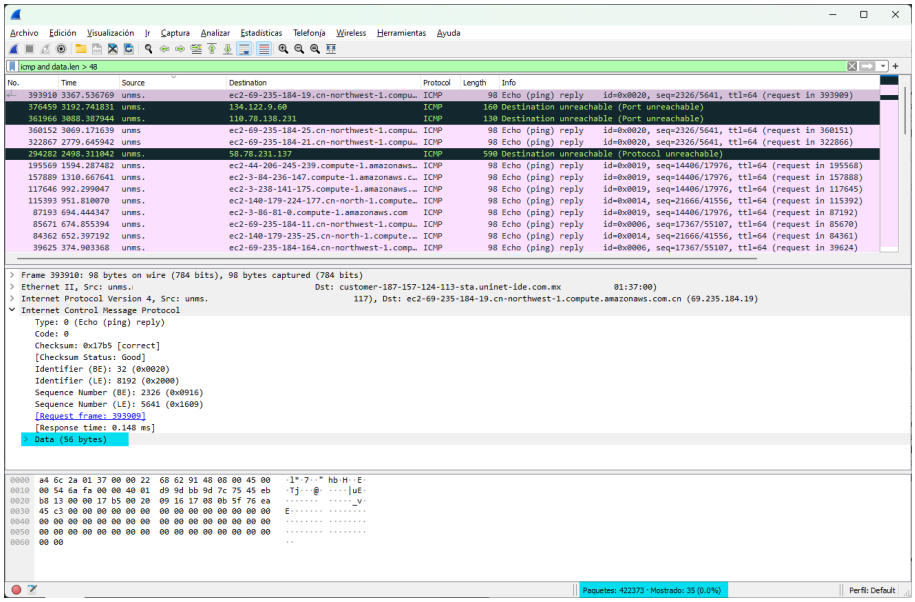


Figura 4.53: Inundación ICMP.

Finalmente, en la Figura 4.54 se observan los paquetes retransmitidos, indican un severo problema en la red, probablemente se trate de un ataque DDoS a menor escala, el porcentaje de paquetes capturados equivale a 1.4 %. Esto se clasifica como un caso verdadero positivo en la cual se observa una probable intrusión.

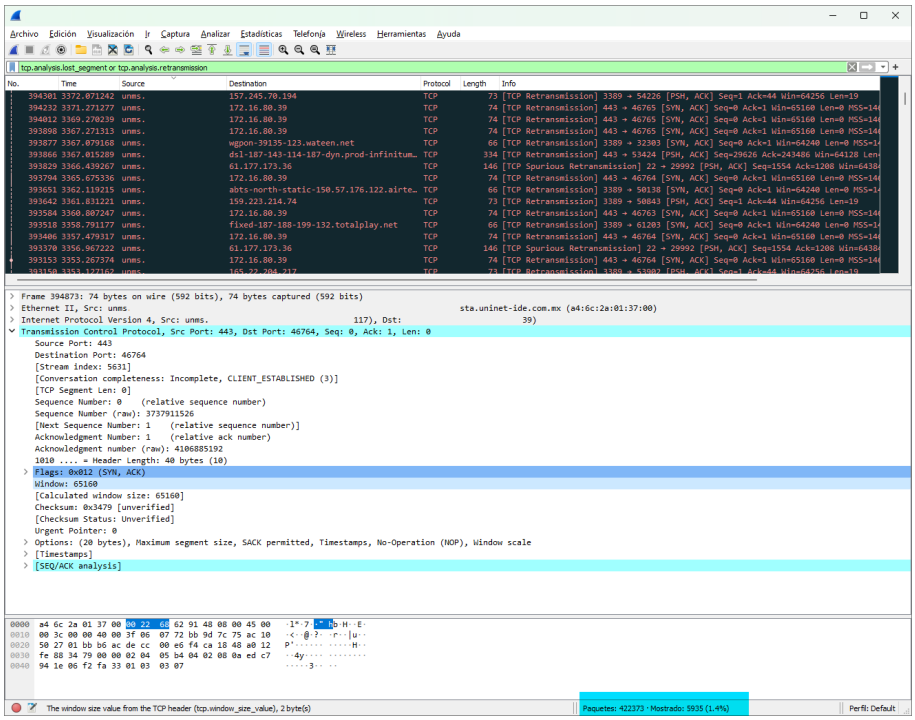


Figura 4.54: Paquetes TCP perdidos y retransmitidos.

La Figura 4.55 muestra un resumen generado por la herramienta NetworkMiner. Se observa una interacción con 567 huéspedes (servidores y clientes), se realizaron 6332 inicios de sesión y en las anomalías se encontraron 2 posibles ataques de suplantación ARP. A simple vista se observa que las amenazas pueden ser clasificadas como verdaderas positivas, sin embargo, es necesario indagar sobre las direcciones MAC que se muestran.

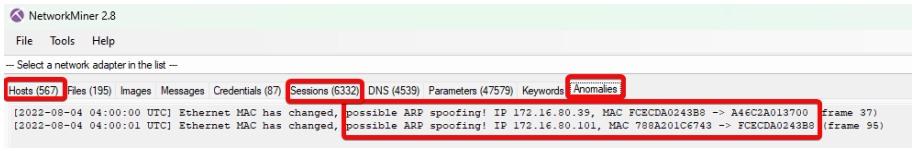


Figura 4.55: Resumen de anomalías desde NetworkMiner.

Se observa que se presentan las mismas direcciones IP que en archivos anteriores así como las mismas direcciones MAC. Sin embargo, al filtrar la dirección MAC `A4:6C:2A:01:37:00` se observan demasiadas direcciones IP (véase Figura 4.56), esta dirección MAC pertenece a la dirección IP `172.16.*.*` que se caracteriza por ser utilizada para redes locales y en algunos casos se configura como dirección IP predeterminada, por ello la relación entre todos los usuarios de la red. Finalmente, esta amenaza se clasifica como falsa positiva.

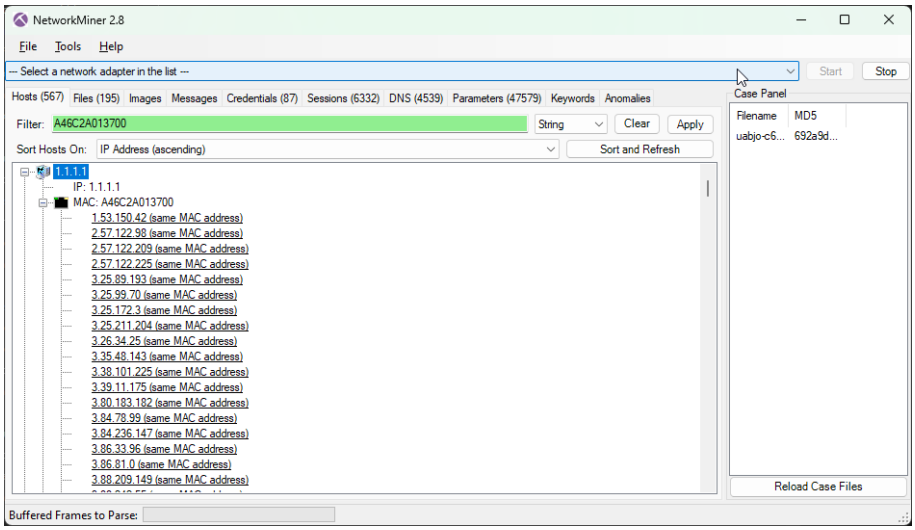
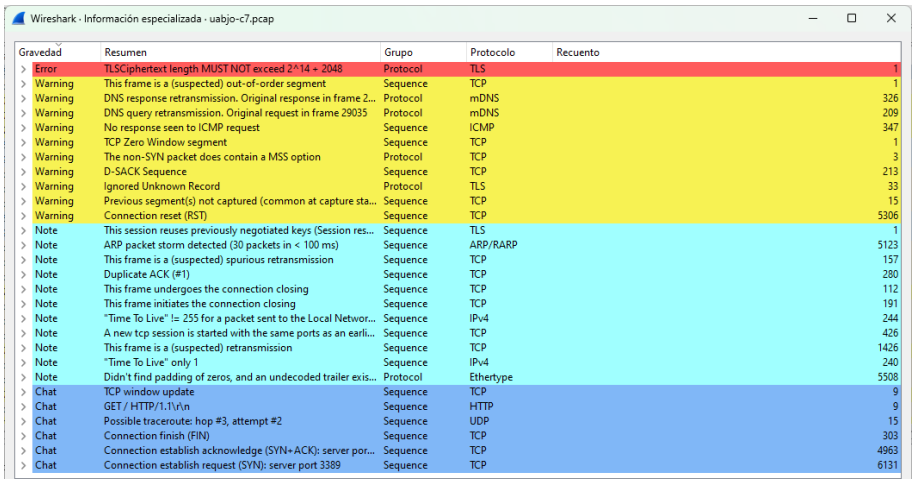


Figura 4.56: Direcciones MAC duplicadas.

En cuanto a la Figura 4.57, se observa que existe un error que pertenece al protocolo TLS. En segundo lugar se encuentran las amenazas, de las cuales 6 pertenecen al protocolo TCP, es necesario revisarlas para evitar que se trate de un ataque DDoS. Se observa que existe una advertencia con ICMP. Finalmente existen algunos detalles con la respuesta de retransmisión utilizando el DNS.



Gravedad	Resumen	Grupo	Protocolo	Recuento
Error	TLSCiphertext length MUST NOT exceed 2^14 + 2048	Protocol	TLS	1
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	1
Warning	DNS response retransmission. Original response in frame 2...	Protocol	mDNS	326
Warning	DNS query retransmission. Original request in frame 29035	Protocol	mDNS	209
Warning	No response seen to ICMP request	Sequence	ICMP	347
Warning	TCP Zero Window segment	Sequence	TCP	1
Warning	The non-SYN packet does contain a MSS option	Protocol	TCP	3
Warning	D-SACK Sequence	Sequence	TCP	213
Warning	Ignored Unknown Record	Protocol	TLS	33
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	15
Warning	Connection reset (RST)	Sequence	TCP	5306
Note	This session reuses previously negotiated keys (Session res...	Sequence	TLS	1
Note	ARP packet storm detected (30 packets in < 100 ms)	Sequence	ARP/RARP	5123
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	157
Note	Duplicate ACK (#1)	Sequence	TCP	280
Note	This frame undergoes the connection closing	Sequence	TCP	112
Note	This frame initiates the connection closing	Sequence	TCP	191
Note	"Time To Live" != 255 for a packet sent to the Local Networ...	Sequence	IPv4	244
Note	A new tcp session is started with the same ports as an earli...	Sequence	TCP	426
Note	This frame is a (suspected) retransmission	Sequence	TCP	1426
Note	"Time To Live" only 1	Sequence	IPv4	240
Note	Didn't find padding of zeros, and an undecoded trailer exis...	Protocol	Ethertype	5508
Chat	TCP window update	Sequence	TCP	9
Chat	GET / HTTP/1.1\r\n	Sequence	HTTP	9
Chat	Possible traceroute: hop #3, attempt #2	Sequence	UDP	15
Chat	Connection finish (FIN)	Sequence	TCP	303
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	4963
Chat	Connection establish request (SYN): server port 3389	Sequence	TCP	6131

Figura 4.57: Resumen de la séptima captura de paquetes en la Universidad de Oaxaca de Juárez.

Para comenzar con el análisis de paquetes para detectar alguna amenaza se implementa el filtro `arp.dst.hw_mac==00:00:00:00:00:00` utilizado para mostrar los paquetes que han sido escaneados mediante el protocolo ARP. En la Figura 4.58 se observan las diferentes solicitudes que hacen las direcciones origen para encontrar determinada dirección IP y compartir información. También, se observa que el número de paquetes que presentan esta característica es de 54.9 %. Es probable que se trate de una amenaza clasificada como falsa positiva, por lo que es necesario utilizar los diferentes filtros de visualización para descartar amenazas.

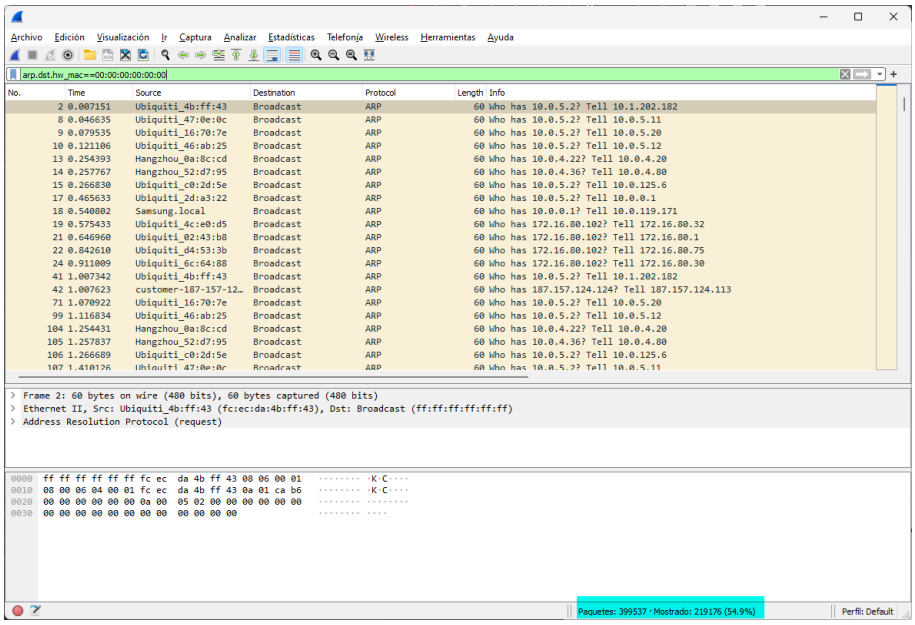


Figura 4.58: Escaneo ARP.

El filtro de `icmp.type==8 || icmp.type==0` muestra los paquetes que presenten características con el barrido *ping* ICMP. En algunos casos, el barrido *ping* ICMP resulta inútil implementarlo cuando la red a la que se desea atacar tiene una excelente configuración de cortafuegos. En la Figura 4.59 se muestra que el número de paquetes que presentan esta característica es de 3.3 %. Se debe recordar que cuando se está recibiendo un incremento inesperado de tráfico ICMP se trata de un ataque. Por lo tanto, este caso se clasifica como un caso verdadero positivo.

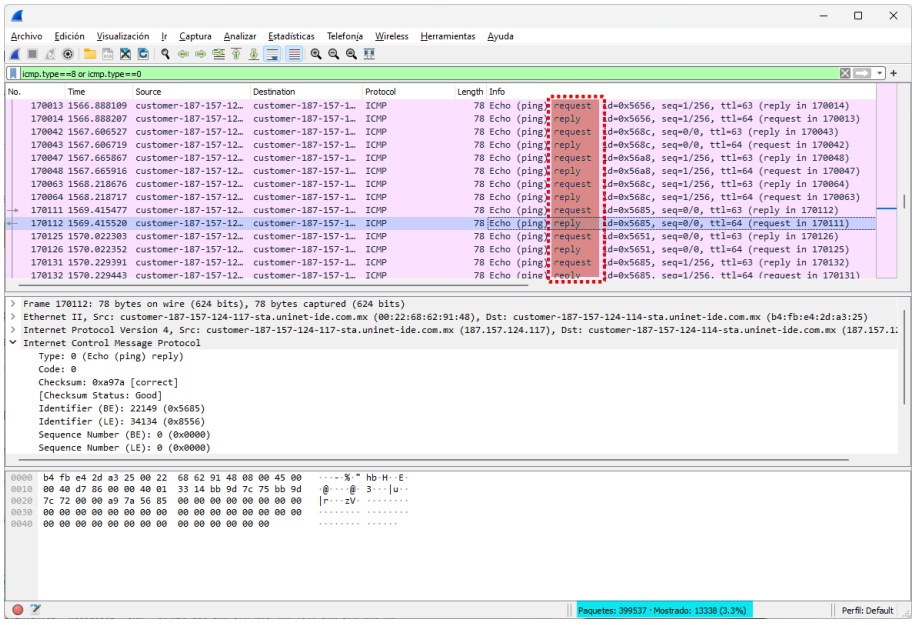


Figura 4.59: Barrido *ping* ICMP.

Es necesario realizar un filtrado de paquetes para detectar posibles escaneos de puertos en la red. El filtro que ayuda a mostrar este tipo de amenazas es `tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.window_size<=1024`, la Figura 4.60 muestra paquetes que presentan estas características. También se observa que el tamaño de

la ventana es 1024 bytes y que diferentes direcciones origen tratan de conectarse con el destino `customer-187-157`. Sin embargo, el número de paquetes capturados es muy bajo. Por tal motivo se descarta de que se trate de una denegación de servicio. Ante esta premisa, se clasifica como un caso verdadero negativo.

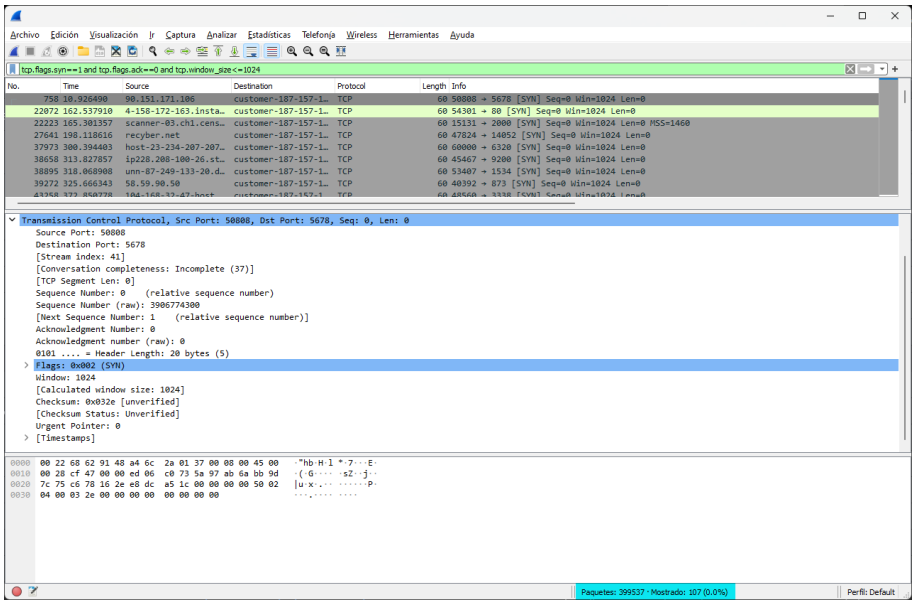


Figura 4.60: Escaneo de puerto TCP SYN.

La Figura 4.61 muestra un filtrado de paquetes en donde se observan aquellos en los que se lleva a cabo una conexión TCP. Se observa también que en la sección Información detallada del paquete uno de los protocolos es TCP, éste se encuentra coloreado de azul, el cual representa algún error inusual de un protocolo; en este caso la bandera SYN de TCP.

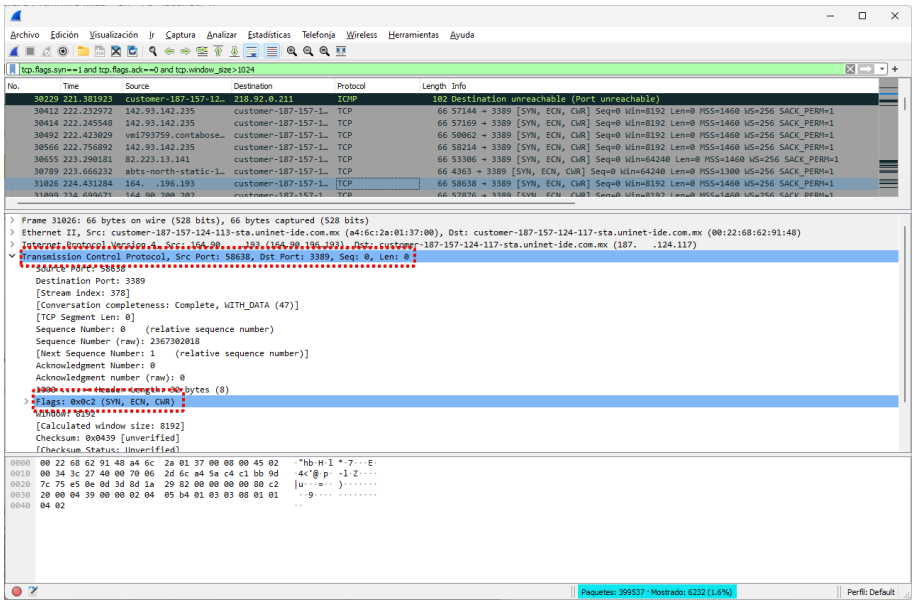


Figura 4.61: Escaneo de puerto TCP Connect.

El escaneo TCP nulo funciona enviando paquetes sin ninguna bandera establecida. Esto podría potencialmente penetrar algunos de los cortafuegos y descubrir puertos abiertos. Con lo antes mencionado, en la Figura 4.62 se observa solamente un paquete que cumple

con las características de escaneo TCP nulo, así mismo presenta un coloreado obscuro indicando un error con el protocolo TCP y se clasifica como un caso verdadero positivo.

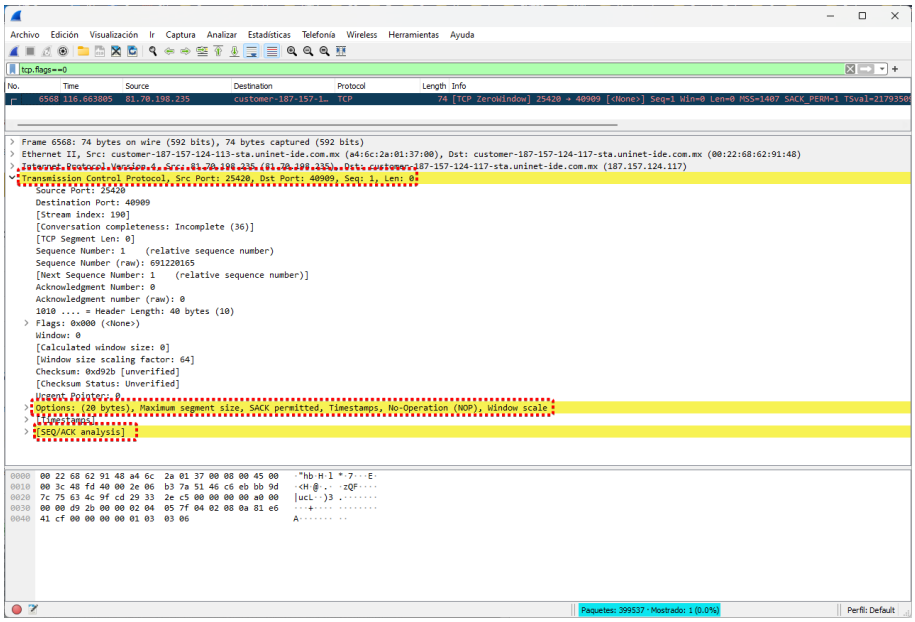


Figura 4.62: Escaneo de puerto TCP Nulo.

Para concluir el análisis de este archivo, la Figura 4.63 muestra un resumen de anomalías generado por la herramienta NetworkMiner, se observa que interactuaron 616 huéspedes, se realizaron 5778 inicios de sesión y se detectaron 2 posibles ataques de suplantación ARP.

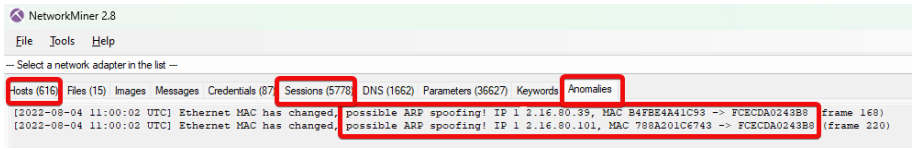


Figura 4.63: Resumen de anomalías desde NetworkMiner.

En la Figura 4.63 se observa que este archivo presenta las mismas direcciones IP que se han visualizado en los archivos de captura 1, 2, 3, 4, 5 y 6. En la Figura 4.64 se observa que la dirección IP con los bytes en `169.254.*.*`, corresponde a APIPA y se asigna cuando los equipos no encuentran su servidor DHCP y se asignaron a la dirección `169.254.*.*` para así comenzar el envío de paquetes. A la hora de que estas direcciones encontraron su servidor se les volvió a asignar la dirección de `172.16.*.*` y comenzó el envío de paquetes con dicha dirección, sin embargo, al salir de la misma interfaz poseen la misma dirección MAC. Conviene subrayar que existe una diferencia respecto a las capturas mencionadas a lo largo de esta sección, se trata del envío y recepción de paquetes. Por ello, esta situación se clasifica como una amenaza falsa positiva.

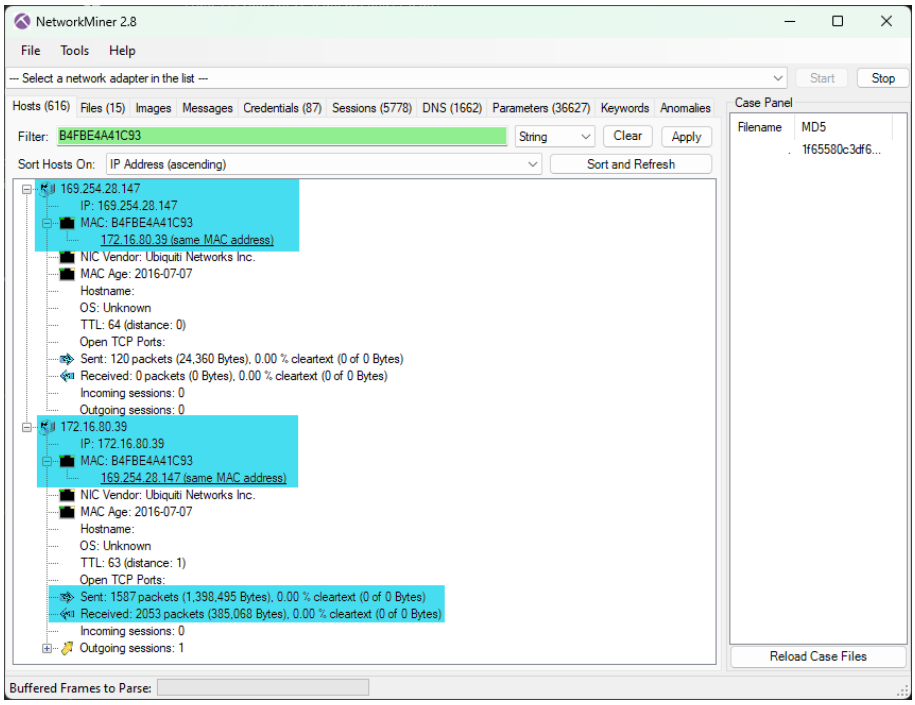


Figura 4.64: Dirección MAC duplicada.

Para finalizar el análisis de los archivos de la Tabla 4.1, la Figura 4.65 muestra un error que tiene que ver con el protocolo Ethernet. Es necesario verificar los paquetes en cuestión de tal manera que se pueda encontrar la falla en la red y así evitar este tipo de anomalías. En cuanto a la sección Advertencias, el protocolo TCP predomina y es considerado como una amenaza ya que existe la posibilidad de que sea un ataque DDoS o una exploración a los puertos TCP. Por otro lado, en la sección Note se observa un mensaje expresando que se detectó una tormenta de paquetes ARP en menos de 100 ms, es decir, se trata de un posible ataque DDoS.

Gravedad	Resumen	Grupo	Protocolo	Recuento
Error	Malformed Packet (Exception occurred)	Malformed	Ethernet	22
Warning	The non-SYN packet does contain a MSS option	Protocol	TCP	1
Warning	No response seen to ICMP request	Sequence	ICMP	64
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	42
Warning	DNS response retransmission. Original response in frame 5...	Protocol	mDNS	46
Warning	Ignored Unknown Record	Protocol	TLS	164
Warning	DNS query retransmission. Original request in frame 1005	Protocol	mDNS	126
Warning	D-SACK Sequence	Sequence	TCP	68
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	101
Warning	Connection reset (RST)	Sequence	TCP	1080
Note	ARP packet storm detected (30 packets in < 100 ms)	Sequence	ARP/RARP	924
Note	"Time To Live" != 255 for a packet sent to the Local Networ...	Sequence	IPv4	2
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	4
Note	A new tcp session is started with the same ports as an earli...	Sequence	TCP	43
Note	This frame undergoes the connection closing	Sequence	TCP	24
Note	This frame initiates the connection closing	Sequence	TCP	52
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	43
Note	Duplicate ACK (#1)	Sequence	TCP	220
Note	This frame is a (suspected) retransmission	Sequence	TCP	328
Note	"Time To Live" only 1	Sequence	IPv4	50
Note	Didn't find padding of zeros, and an undecoded trailer exis...	Protocol	Ethertype	1151
Chat	TCP window update	Sequence	TCP	70
Chat	Connection finish (FIN)	Sequence	TCP	76
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	986
Chat	Connection establish request (SYN): server port 50136	Sequence	TCP	1200

Figura 4.65: Resumen de la octava captura de paquetes en la Universidad de Oaxaca de Juárez.

Para descartar cualquier posible ataque de suplantación ARP es necesario utilizar el filtro de suplantación ARP (véase Figura 4.66), sin embargo, el archivo se encuentra limpio.

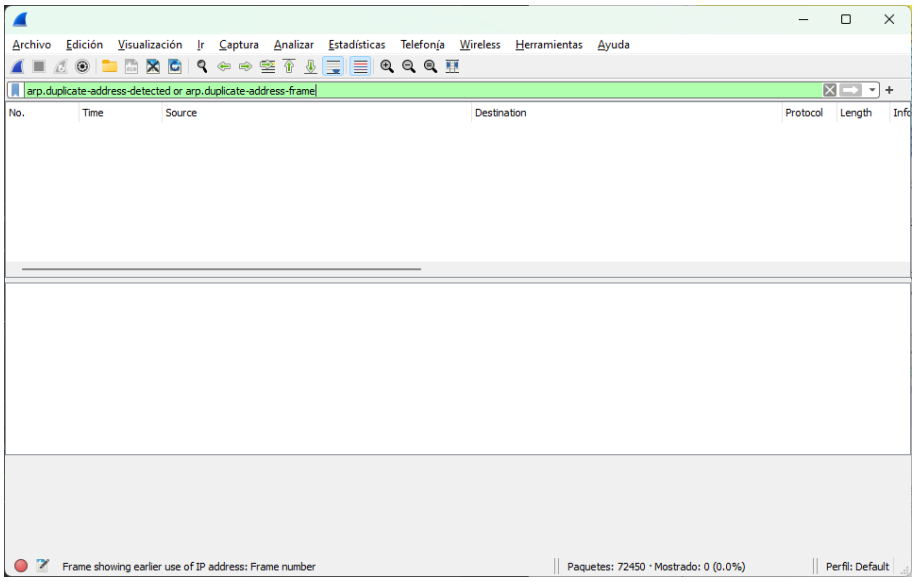


Figura 4.66: Existencia nula de suplantación ARP.

Posterior a esto, se verifica que no exista alguna inundación ICMP. Se utiliza el filtro `icmp && data.len > 48` y los resultados se observan en la Figura 4.67. El número de paquetes filtrados resulta mínimo comparado con los capturados, por ello esto se clasifica como una amenaza falsa positiva.

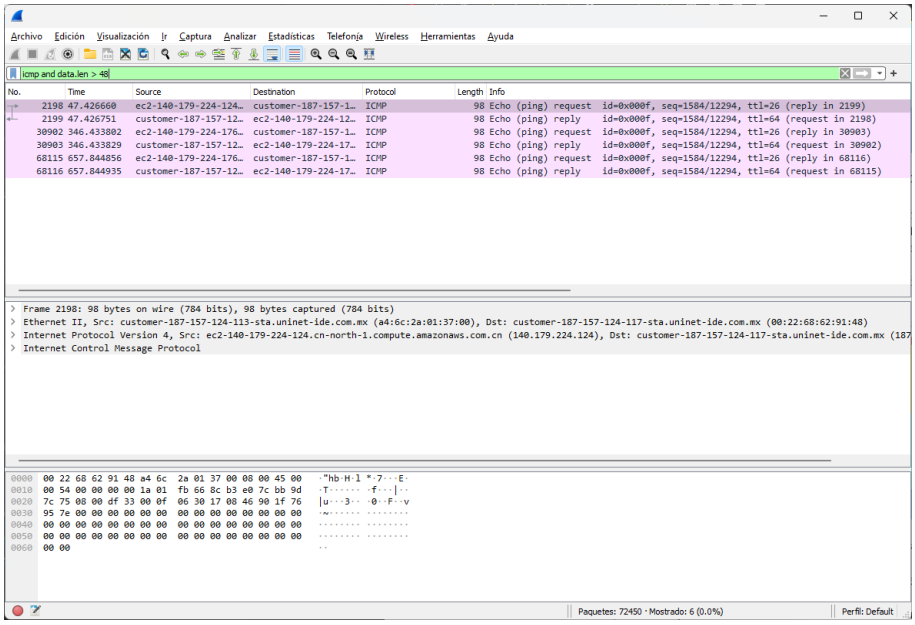


Figura 4.67: Inundación ICMP.

Es necesario realizar una revisión de los puertos que son susceptibles a escaneos. En la Figura 4.68 se observan los paquetes SYN TCP. El número de paquetes filtrados es mínimo, representa el 0.1 %. Esto quiere decir que los puertos de la red no han sido escaneados en su totalidad.

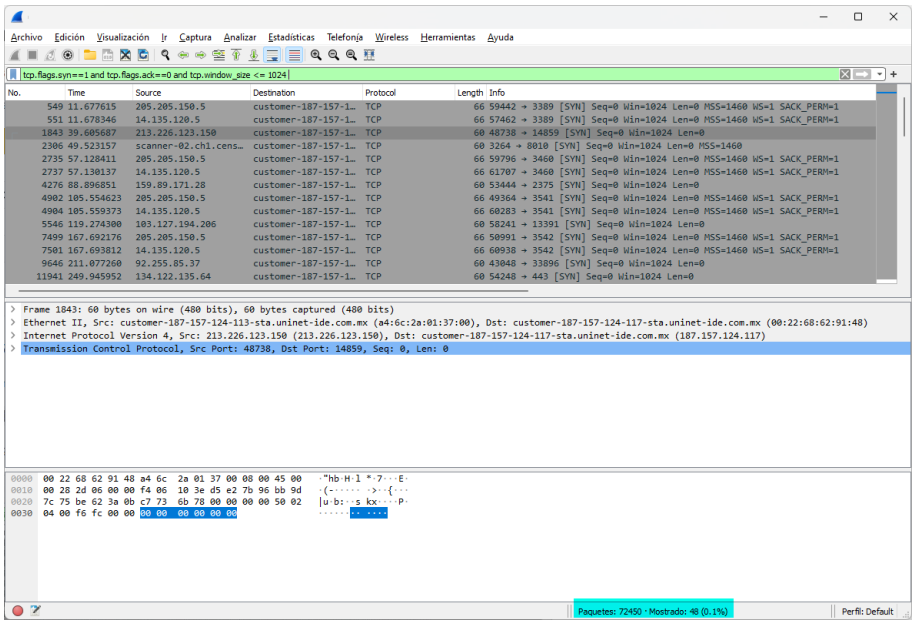


Figura 4.68: Escaneo TCP SYN.

Para detectar escaneos de TCP Connect se utiliza el filtro `tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.window_size > 1024`, los paquetes filtrados se observan en la Figura 4.69. Nótese que los paquetes filtrados representan el 1.7 %, en este caso las direcciones IP intentan conectarse a un servidor de la universidad sin embargo, la información que ofrece Wireshark es de SYN, ECN y CWR, es decir que no se logra una conexión completa entre la fuente y el destino, por lo que, indica que existe un problema de congestión en la red.

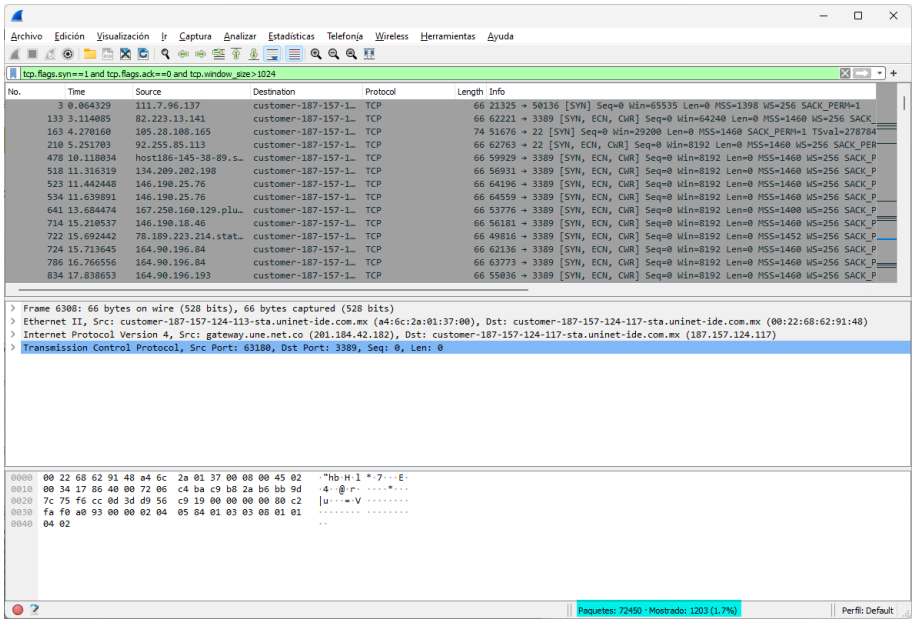


Figura 4.69: Escaneo TCP Connect.

Finalmente, el filtro `icmp.type==3 && icmp.code==3` muestra los puertos escaneados UDP. Sí los paquetes filtrados ICMP tienen el tipo 3 (destino inalcanzable) con código 3 (puerto inalcanzable) resulta un buen indicador del escaneo de puertos UDP, esto quiere decir que los mensajes ICMP en particular indican que el puerto UDP remoto

está cerrado. No obstante, sí existe un alto número de estos paquetes en la red en un corto periodo de tiempo, la probabilidad de que alguien esté realizando escaneos de puertos UDP es demasiado alta (véase Figura 4.70). Sin embargo, no se cumplen completamente las características para que se pueda catalogar como paquete, por ello se clasifica como amenaza falsa positiva.

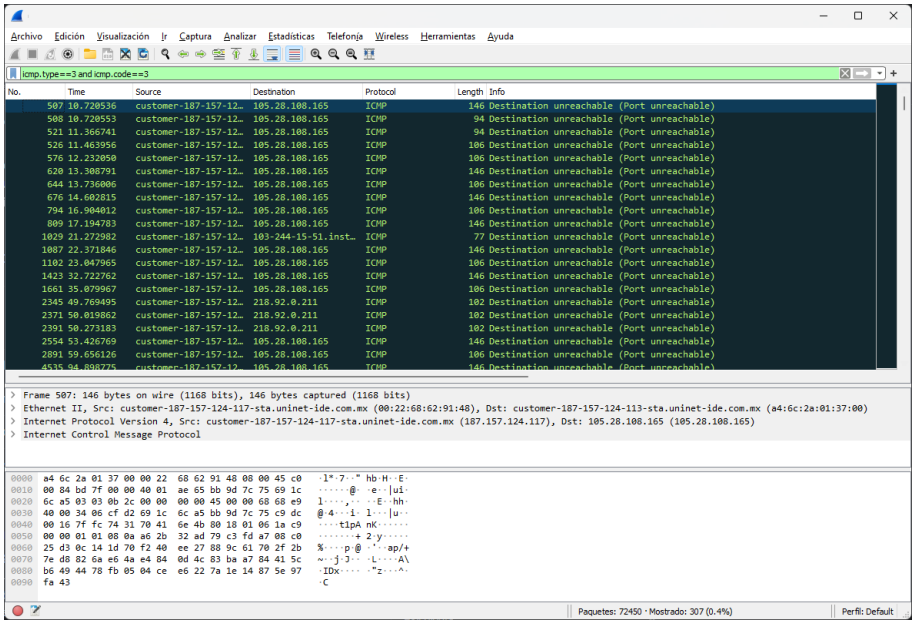


Figura 4.70: Escaneo de puertos ICMP.

La Figura 4.71 muestra los paquetes que en su mayoría de veces han sido transmitidos y muy pocas veces perdidos, el recuento de paquetes representa un 0.6 %, el error que presenta es que, el destino pertenece a un huésped educativo y el destino de la misma manera, es hacia el DNS de servicios educativos pertenecientes a la universidad.

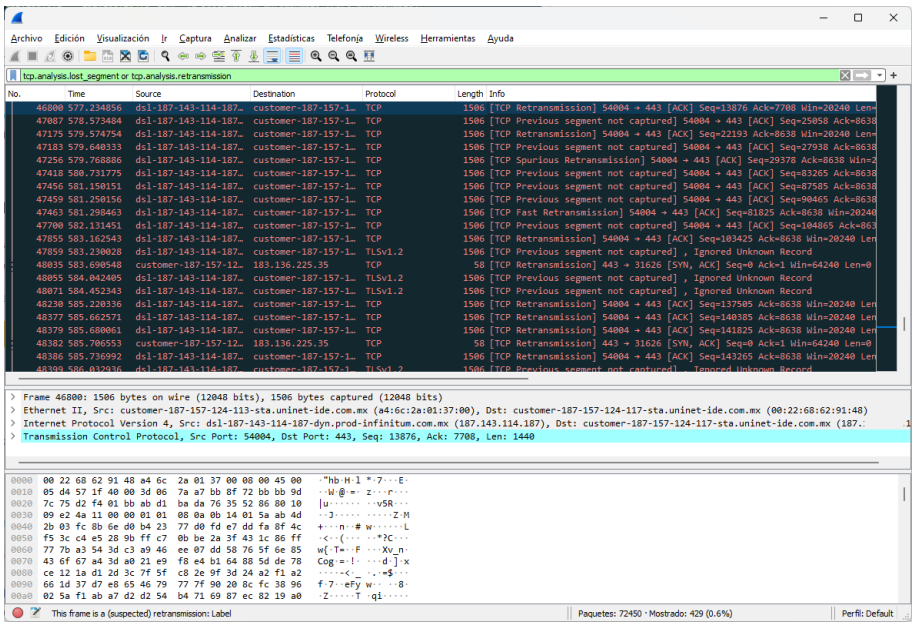


Figura 4.71: Paquetes TCP retransmitidos y perdidos.

Para finalizar el análisis, la Figura 4.72 se observa un resumen generado por la herra-

mienta NetworkMiner, en donde interactuaron 290 huéspedes, se realizaron 1187 inicios de sesión y se detectaron dos posibles ataques de suplantación ARP.

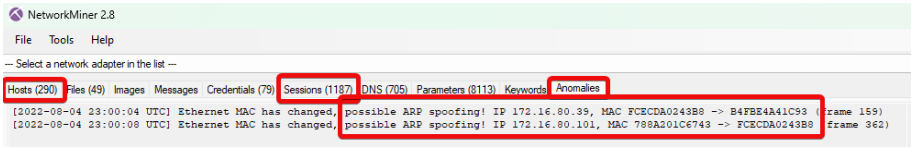


Figura 4.72: Resumen de anomalías desde NetworkMiner.

En la Figura 4.73 se observan las direcciones IP que tienen asociada la siguiente dirección IP `169.254.*.*` llamada APIPA, esto ocurre debido a una inadecuada configuración del servidor DHCP. Como se ha mencionado anteriormente, a los dispositivos que no logran acceder al servidor DHCP se les asigna la dirección IP APIPA y cuando se activa el servidor se les asigna su dirección final. Como la dirección MAC es la misma, NetworkMiner lo detecta como suplantación ARP. Por ello esto se clasifica como falso positivo.

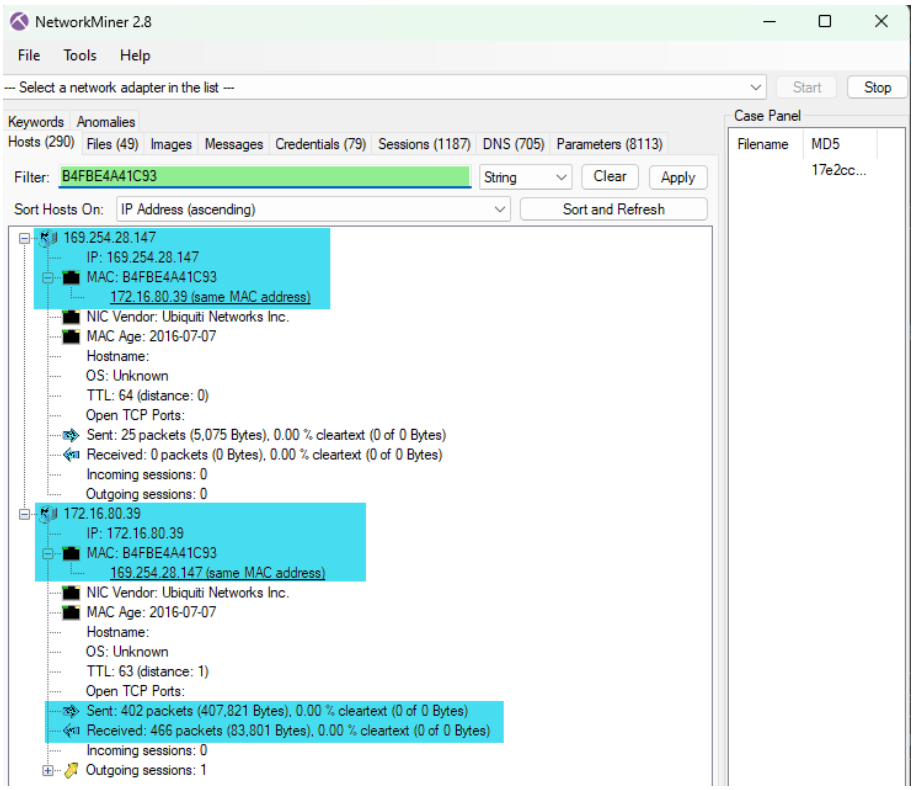


Figura 4.73: Direcciones IP con direcciones MAC duplicadas a causa de un error en el servidor DHCP.

Capítulo 5

Detección de Amenazas en la red de la UTM

En este capítulo se detallan las amenazas en la red LAN universitaria de la UTM y se presenta un análisis de las amenazas y problemas detectados mediante el estudio de archivos de los paquetes capturados.

La Figura 4.1 del Capítulo 4 ofrece una visión general de las amenazas identificadas en esta investigación a través del análisis de archivos con Wireshark y NetworkMiner. Además, se clasifican las amenazas identificadas en función de los protocolos ARP, ICMP, TCP, DHCP y TLS.

5.1. Escenario de Captura

El escenario de captura de la red en la UTM se muestra en la Figura 5.1, en donde se observa que en el departamento de red se encuentra el servidor y de ahí sale una línea dirigida hacia un conmutador ubicado en el IEM, y es en el cubículo 14 donde se ejecutó Wireshark.

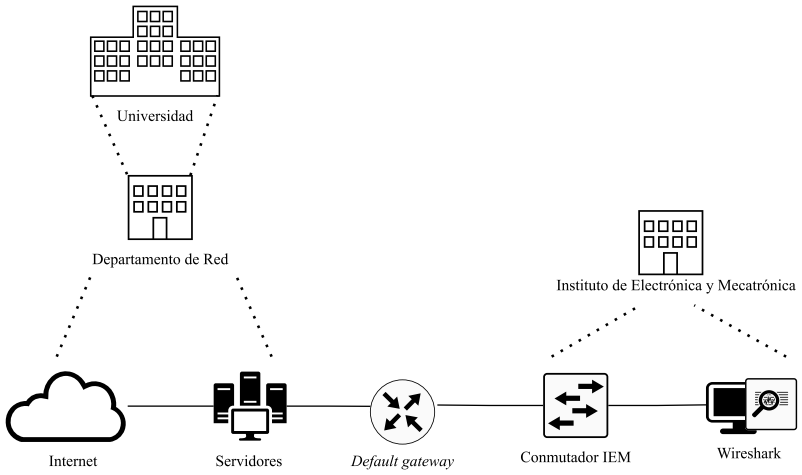


Figura 5.1: Escenario para la captura de paquetes en la UTM.

5.2. Características de los Paquetes Capturados

En la Tabla 5.1 se presentan los archivos capturados en la UTM desde el cubículo 14 del IEM. Para realizar la captura de los archivos se utilizó un equipo de cómputo con las siguientes características: memoria RAM de 6 GB, procesador Intel® Core™ i5-2400 CPU 3.10 GHz × 4 y disco duro de estado solido de 480 GB con sistema operativo GNU/Linux y distribución Ubuntu 22.04.2 LTS.

Archivo	Tamaño	Intervalo de Captura	Paquetes
1	722 MB	2022-06-03 09:58:10 a 2022-06-03 17:11:00	1375305
2	1.1 GB	2022-06-13 08:27:57 a 2022-06-15 13:03:43	4283777
3	413 MB	2022-08-12 18:57:32 a 2022-08-15 09:02:18	1851116
4	1.2 GB	2022-08-31 15:38:38 a 2022-08-31 15:57:14	12333033
5	587 MB	2022-08-31 16:02:54 a 2022-09-02 18:40:37	3279864
6	204 MB	2022-09-08 11:58:28 a 2022-09-09 08:37:14	300796
7	1.1 GB	2022-11-14 08:26:12 a 2022-11-15 18:54:24	1353703
8	212 MB	2022-12-05 16:31:31 a 2022-12-09 18:43:57	594694

Tabla 5.1: Características de los paquetes capturados en la UTM.

Como se explicó en la sección 2.13.3 la función Información Especializada muestra de manera general el estado de la red con base a los paquetes capturados, de esta manera se inicia con el análisis de los paquetes para detectar las amenazas existentes mediante filtros o diferentes funciones de Wireshark.

5.3. Análisis

En la Figura 5.2 se observa que en la sección Error existen tres casos, dos de ellos pertenecen a protocolos que no están al alcance de esta investigación. En cuanto al grupo Advertencia, existen dos protocolos de suma importancia para analizarlos debido a que son susceptibles a ataques, uno de estos es una posible suplantación ARP y el otro pertenece a TCP en el cual posiblemente se trate de escaneo de puertos.

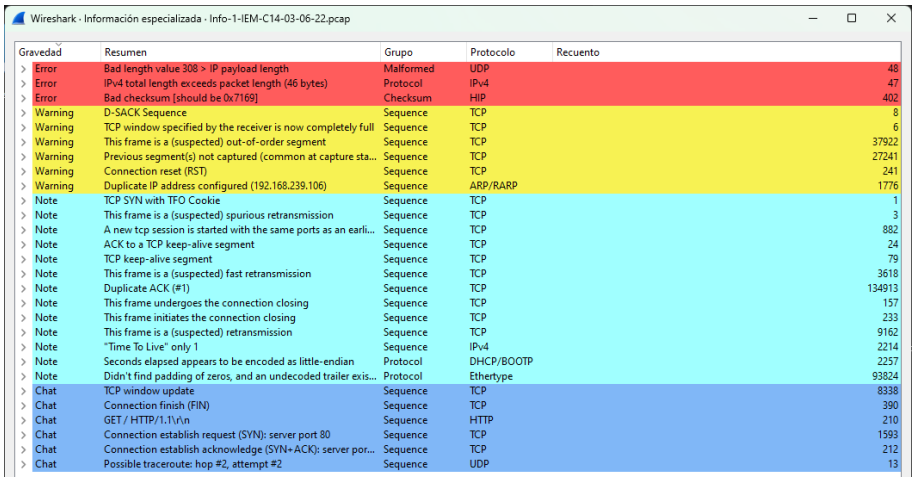


Figura 5.2: Resumen de la primer captura de paquetes en la UTM.

Para el análisis de este archivo primero se comienza por la detección de suplantación ARP, para esto se utiliza el filtro de la Tabla 2.6. La Figura 5.3 muestra los paquetes en

los cuales Wireshark ha detectado que existe un posible ataque de suplantación ARP, por tal motivo se clasifica como amenaza verdadera positiva.

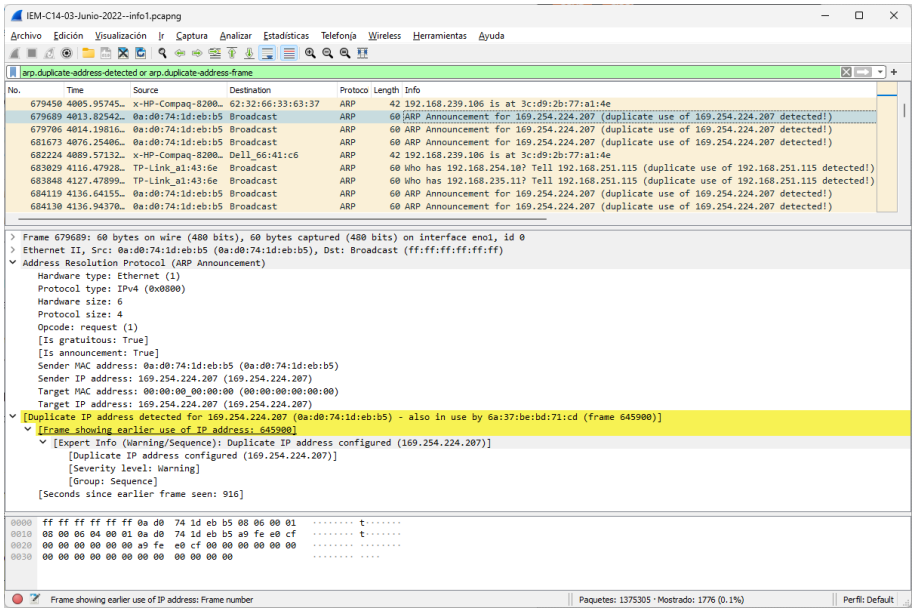


Figura 5.3: Filtrado de paquetes utilizando el filtro de suplantación ARP.

Continuando el análisis, la Figura 5.4 muestra los paquetes al utilizar el filtro de barrido *ping* ICMP, observando que el número de paquetes capturados son 7. Este caso puede clasificarse como amenaza verdadera negativa.

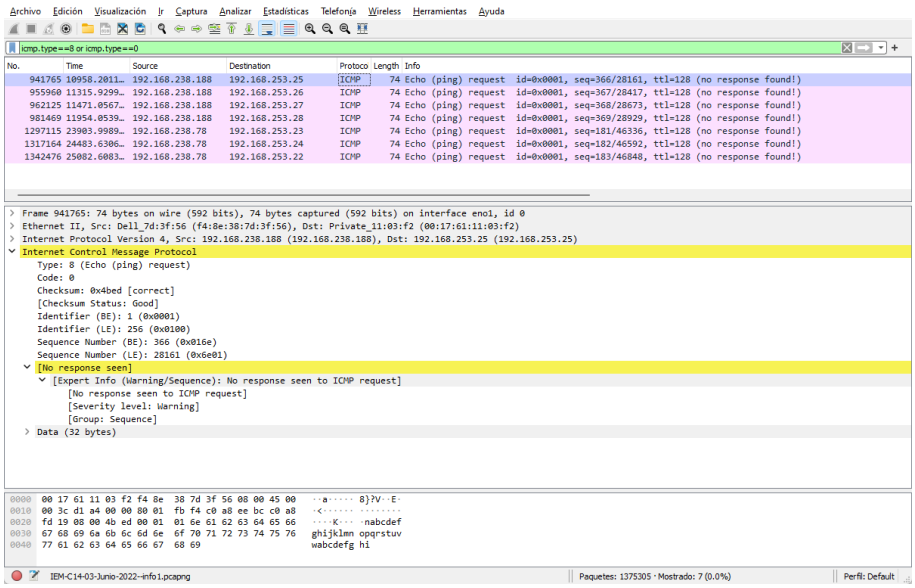


Figura 5.4: Barrido *ping* ICMP.

En la Figura 5.5 se observan paquetes retransmitidos y perdidos, esto se logra utilizando el filtro `tcp.analysis.lost_segment || tcp.analysis.retransmission`. Los paquetes filtrados indican que existe un problema grave en la red, posiblemente causado por un ataque de denegación de servicio o por escaneo de puertos. Este caso se clasifica como amenaza verdadera positiva.

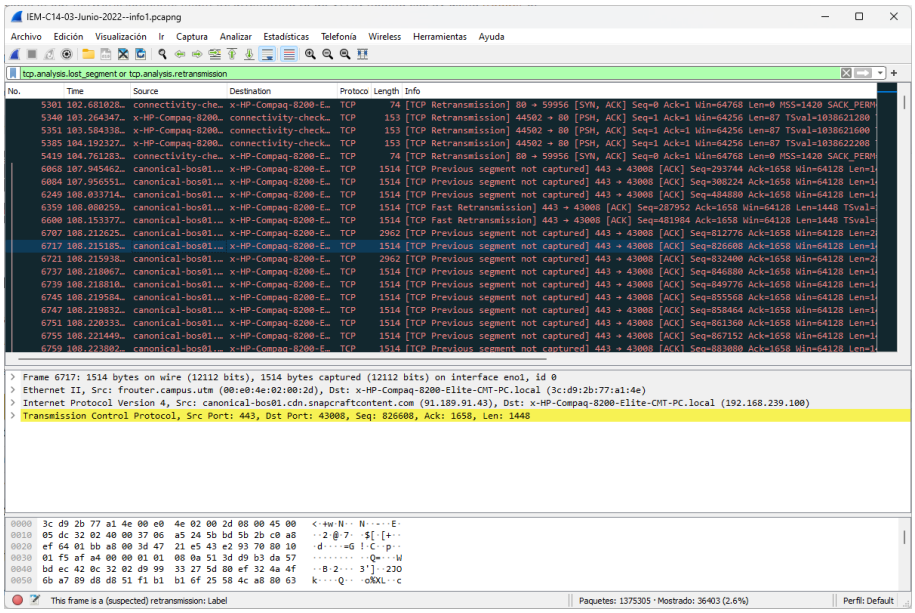


Figura 5.5: Retransmisión de paquetes.

En la Figura 5.6 se observan paquetes en donde un atacante envía un gran número de peticiones ARP a través del *broadcast* (`ff:ff:ff:ff:ff:ff`) con destino a la dirección MAC `00:00:00:00:00:00` para descubrir direcciones IP disponibles de atacar en la red local. Se observa que el número de paquetes filtrados equivale a 43.6 % por lo tanto, este caso se considera como una amenaza verdadera positiva.

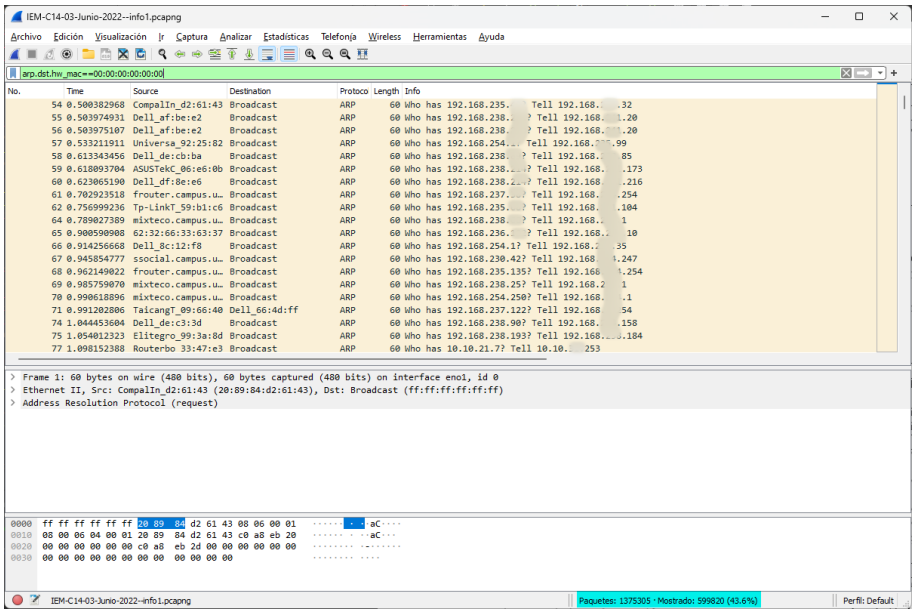


Figura 5.6: Paquetes que presentan características de un escaneo ARP.

Continuando el análisis con la herramienta NetworkMiner, al dirigirse a la pestaña Anomalies se muestra un resumen de las posibles amenazas que tiene el archivo en cuestión. La Figura 5.7 muestra el resumen de amenazas. Se observan diferentes tipos de amenazas, dentro de las más importantes se encuentran la suplantación ARP y en DHCP.

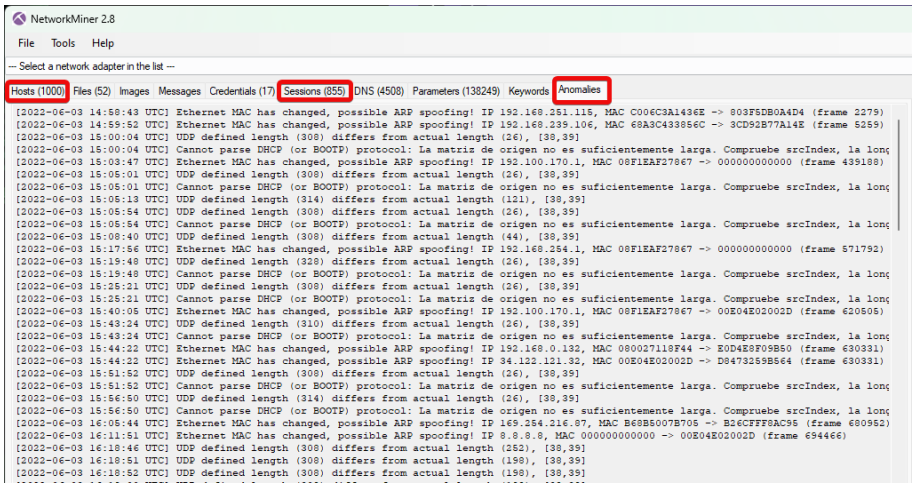


Figura 5.7: Resumen de anomalías desde NetworkMiner.

En la Figura 5.8 se observa que al filtrar una de las direcciones MAC aparecen cuatro direcciones IP que presuntamente tienen la misma dirección MAC. Se observa que una dirección IP tiene los primeros dos bytes en `169.254`, esto significa que dicha dirección IP corresponde al direccionamiento privado automático. Como se ha mencionado, esto sucede porque de alguna forma las direcciones IP no encontraron su servidor y se asignaron a la dirección `169.254.*.*` para así comenzar el envío de paquetes. A la hora de que estas direcciones encontraron su servidor se les asigna la dirección `192.168.*.*` y se restableció el envío de paquetes con dicha dirección, sin embargo, al salir de la misma interfaz (dirección IP `164.254.*.*`) poseen la misma dirección MAC. Por ello NetworkMiner lo detecta como posible suplantación ARP. Ante este suceso, esta amenaza se clasifica como falsa positiva.

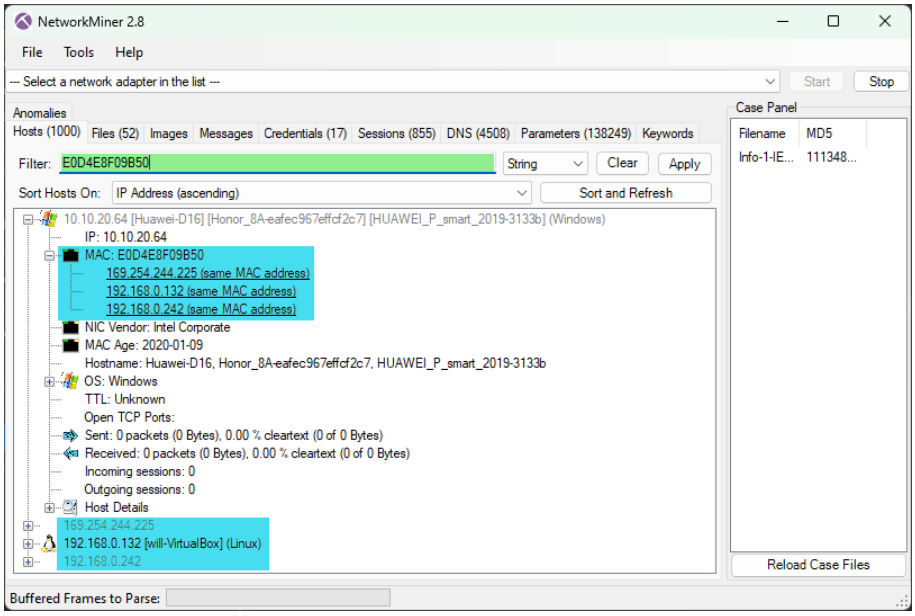


Figura 5.8: Error en la configuración del servidor DHCP.

Se debe agregar que las otras posibles suplantaciones ARP se deben al tiempo excedido de asignación de dirección IP. Recuerde que una dirección IP es asignable durante 24 horas, al exceder este tiempo es posible que tenga asignada una dirección nueva y por tal motivo contienen la misma dirección MAC. Sin embargo, no se descarta la probabilidad

de que se trate de una suplantación ARP.

En cuanto a la Figura 5.9 se observan cuatro problemas en la sección Error en donde los más interesantes pertenecen a DHCP e IPv4. En la sección Advertencia existen nueve casos, de los cuales seis pertenecen a TCP, uno a ICMP y uno a ARP/RARP, el protocolo restante no se encuentra al alcance de esta investigación para su análisis. Mientras que en la sección Nota existen diez casos pertenecientes a TCP, uno de IPv4, Ethertype, DHCP, Ethernet y ARP/RARP, en este último es probable que se trate de una amenaza verdadera positiva debido a que en Resumen menciona una inundación de treinta paquetes ARP en menos de 100 ms. Finalmente, en la sección Chat los casos pertenecen a TCP.

Gravedad	Resumen	Grupo	Protocolo	Recuento
Error	Malformed Packet (Exception occurred)	Malformed	F5 Ethernet trailer	306
Error	Malformed Packet (Exception occurred)	Malformed	DHCP/BOOTP	135
Error	Bad length value 308 > IP payload length	Malformed	UDP	141
Error	IPv4 total length exceeds packet length (60 bytes)	Protocol	IPv4	141
Error	Bad checksum [should be 0xfdc6]	Checksum	HIP	1987
Warning	TCP window specified by the receiver is now completely full	Sequence	TCP	8
Warning	ACKed segment that wasn't captured (common at capture...	Sequence	TCP	114
Warning	Invalid capability length	Protocol	WSP	796
Warning	Duplicate IP address configured (169.254.121.4)	Sequence	ARP/RARP	30908
Warning	No response seen to ICMP request	Sequence	ICMP	15
Warning	D-SACK Sequence	Sequence	TCP	110
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	42555
Warning	Connection reset (RST)	Sequence	TCP	2952
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	30362
Note	ACK to a TCP keep-alive segment	Sequence	TCP	752
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	27
Note	TCP keep-alive segment	Sequence	TCP	999
Note	TCP SYN with TFO Cookie	Sequence	TCP	19
Note	A new tcp session is started with the same ports as an earli...	Sequence	TCP	5960
Note	ARP packet storm detected (30 packets in < 100 ms)	Sequence	ARP/RARP	10755
Note	Didn't find padding of zeros, and an undecoded trailer exis...	Protocol	Ethernet	2687
Note	Seconds elapsed appears to be encoded as little-endian	Protocol	DHCP/BOOTP	5720
Note	"Time To Live" only 1	Sequence	IPv4	14357
Note	Didn't find padding of zeros, and an undecoded trailer exis...	Protocol	Ethertype	481289
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	3403
Note	This frame is a (suspected) retransmission	Sequence	TCP	13515
Note	Duplicate ACK (#1)	Sequence	TCP	154107
Note	This frame undergoes the connection closing	Sequence	TCP	991
Note	This frame initiates the connection closing	Sequence	TCP	1370
Chat	Possible traceroute: hop #5, attempt #2	Sequence	UDP	51
Chat	GET /ubuntu/dists/focal-security/InRelease HTTP/1.1\r\n	Sequence	HTTP	1600
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	1112
Chat	Connection establish request (SYN): server port 443	Sequence	TCP	10084
Chat	TCP window update	Sequence	TCP	12251
Chat	Connection finish (FIN)	Sequence	TCP	2361

Figura 5.9: Resumen de la segunda captura de paquetes en la UTM.

Con respecto al análisis de este archivo, es necesario la aplicación de los filtros para encontrar diferentes anomalías en la red. En primer lugar se aplicó el filtro de escaneo ARP, la Figura 5.10 muestra los paquetes filtrados, en la mayoría de estos se visualiza que el origen de paquetes es de los conmutadores y enrutadores de la red para comenzar una difusión y lograr una conexión adecuada. Por lo tanto, este caso se clasifica como amenaza falsa positiva.

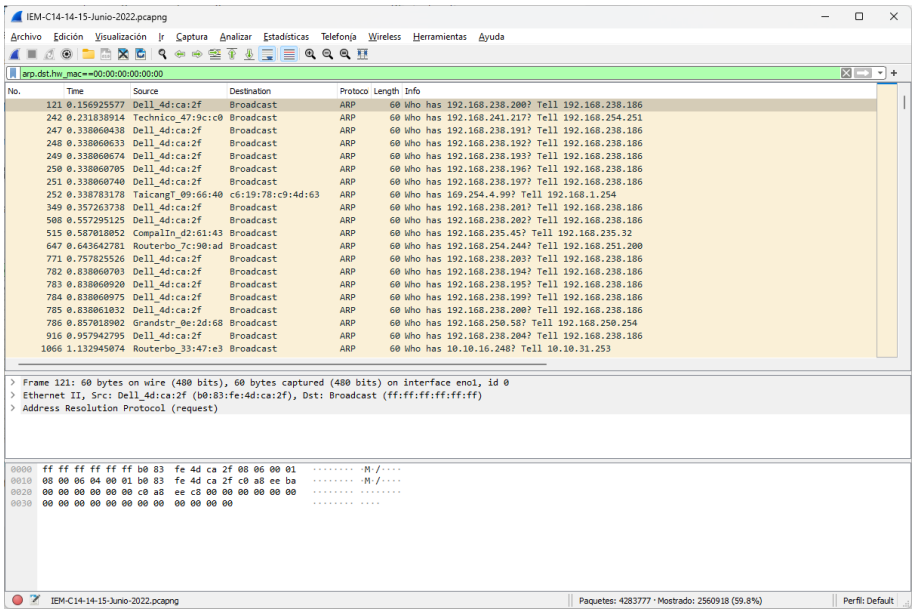


Figura 5.10: Paquetes que presentan un posible escaneo ARP.

En la Figura 5.11 se observa un bajo número de paquetes intentando un escaneo ICMP, los detalles que éste presenta es la variación del último byte de la dirección IP destino. Nótese que, en la información detallada de los paquetes, el paquete ICMP se encuentra coloreado indicando una amenaza.

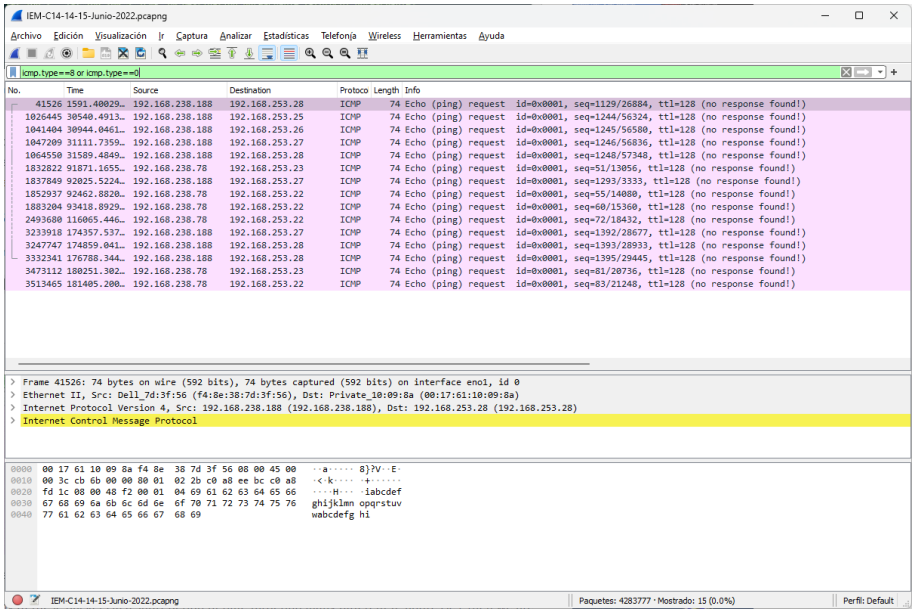


Figura 5.11: Detección de barrido *ping* ICMP.

Así mismo, en la Figura 5.12 se observa que existe un paquete al utilizar el filtro de barrido *ping* TCP, este tipo de *ping* hacia TCP comúnmente utiliza el puerto 7 (eco). Este puerto se caracteriza por trabajar en conjunto con ICMP, sin embargo, resulta ser un puerto anticuado. En este caso, el puerto realiza un eco de lo que se le envía y se utiliza en diferentes ataques, por ello, se clasifica como un caso verdadero positivo.

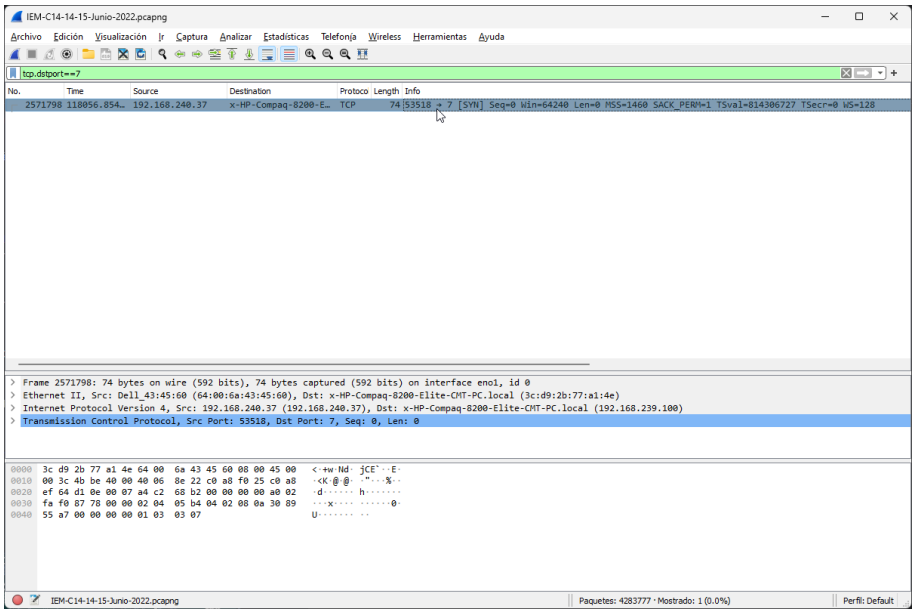


Figura 5.12: Detección de barrido *ping* TCP.

Por otro lado, la Figura 5.13 muestra paquetes en los cuales se lleva a cabo una suplantación ARP perteneciente a la categoría de MitM. Para este caso se observa que las direcciones origen son visualizadas desde la dirección MAC, esto es un blanco para concretar un ataque. Se observa que en la columna Info aparece ARP *Announcement*, que se caracteriza por actualizar la asignación de otros huéspedes siempre y cuando se cambie la dirección MAC o IP del origen. Por ello, este caso se clasifica como verdadero positivo.

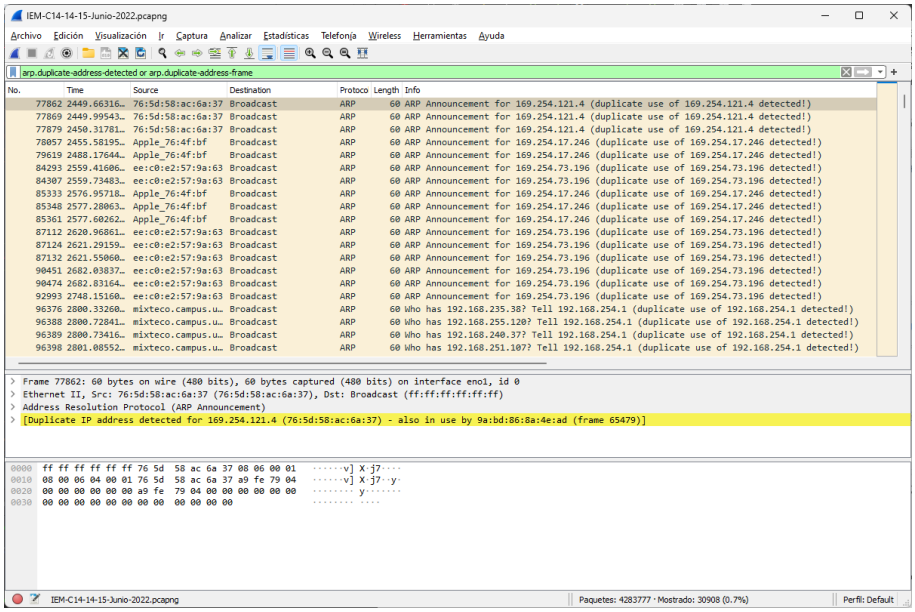


Figura 5.13: Detección de suplantación ARP.

Por otro lado, en la Figura 5.14 se observan paquetes filtrados con características de un escaneo ICMP. Se observa que el número de paquetes filtrados representa una cantidad mínima comparada con los paquetes capturados. La Info de cada paquete muestra el mensaje Port unreachable, esto quiere decir que se trata de una posible amenaza de inundación ICMP, por ello se clasifica como verdadera positiva. El hecho de que existan pocos paquetes indica que la inundación ICMP fue interrumpida por algún mecanismo de seguridad

en la red.

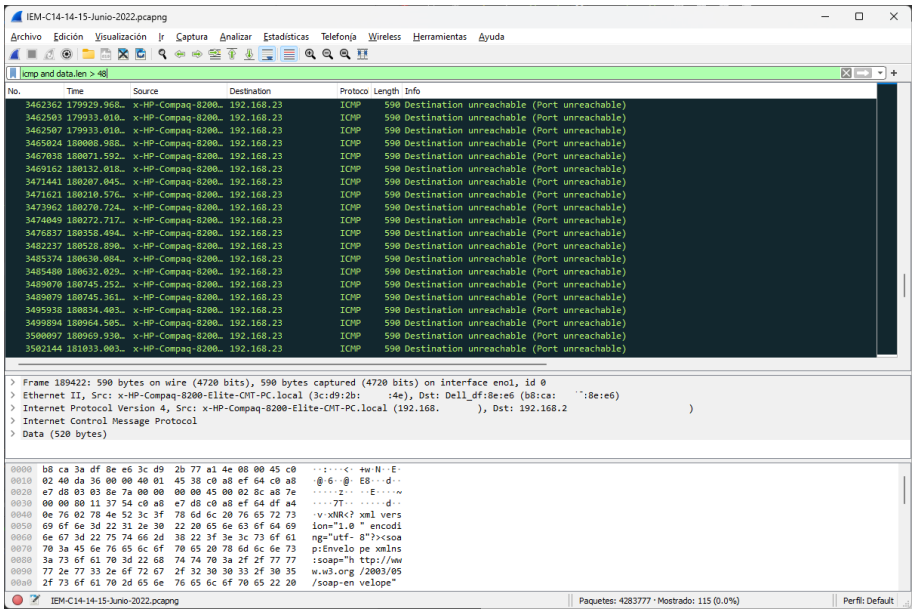


Figura 5.14: Inundación ICMP.

Continuando con el análisis, en la Figura 5.15 se utilizó el filtro `tcp.analysis.lost_segment`, el cual indica que existe un hueco en los números de secuencia[1] en la captura, esto indica que existe un paquete perdido o una llegada de paquete fuera de orden, por ello, esta amenaza se clasifica como falso positivo.

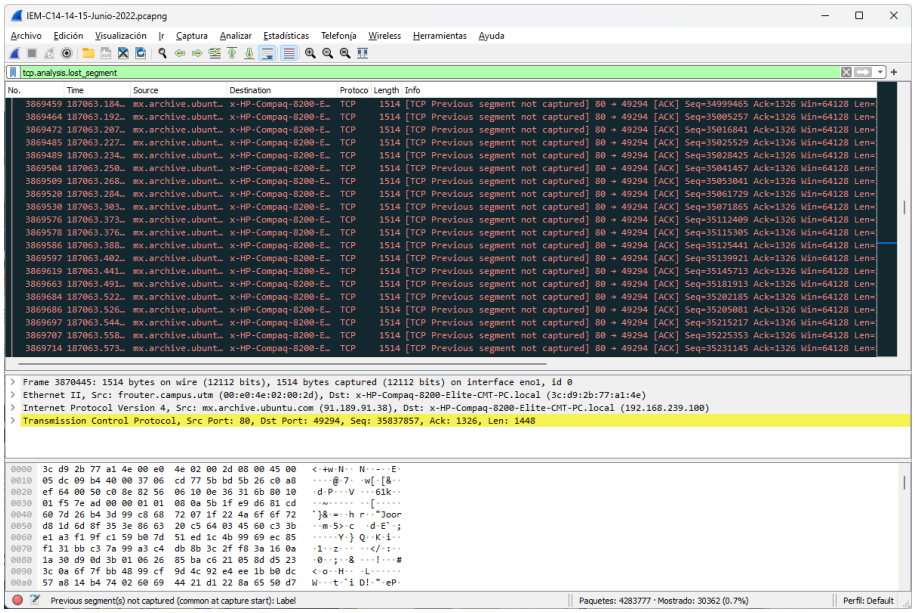


Figura 5.15: Pérdida de paquetes TCP.

Mientras que en la Figura 5.16 se empleó el filtro `tcp.analysis.retransmission`, observando los paquetes retransmitidos. Unas pocas retransmisiones están bien (para este archivo representa un 0.3 %), un exceso de retransmisiones implica problemas graves en la red. El que existan paquetes retransmitidos significa que el usuario presenta un rendimiento lento. Por ello, este caso se clasifica como falso positivo.

[1] Identifica el byte del flujo de datos enviado por el origen al destino. Representa el primer byte del segmento.

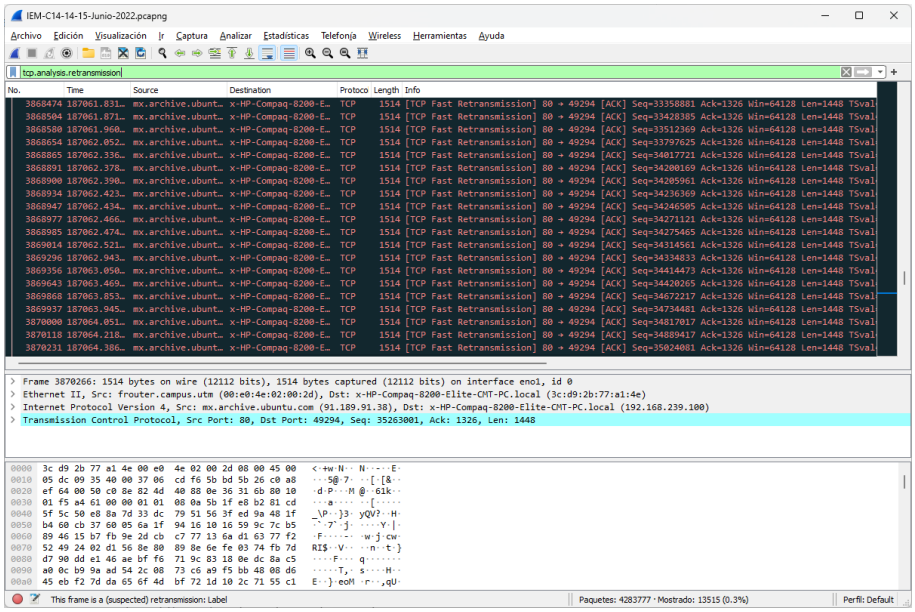


Figura 5.16: Retransmisión TCP.

En resumen, con respecto a las Figuras 5.15 y 5.16 el problema que se presenta es debido a la conexión de un usuario con la página de actualización del sistema operativo (Ubuntu, `mx.archive.ubuntu.com`). Ante este falso positivo, es necesario que los equipos que se mantienen conectados a la red sean configurados de tal manera que las actualizaciones en segundo plano sean desactivadas o programadas en ciertos horarios para prevenir saturación en la red.

El problema mencionado ocurre por la congestión de la red en la que los paquetes se pierden (ya sea porque un segmento TCP se pierde en su camino hacia el destino, o porque el ACK asociado se pierde en el camino de vuelta al remitente). La tasa de retransmisión del tráfico desde y hacia Internet no debe superar el 2 %.

Analizando el archivo con NetworkMiner, en la pestaña Anomalies se muestra un resumen de las posibles amenazas que tiene el archivo en cuestión. La Figura 5.17 presenta las posibles amenazas que se encontraron en el archivo de captura.

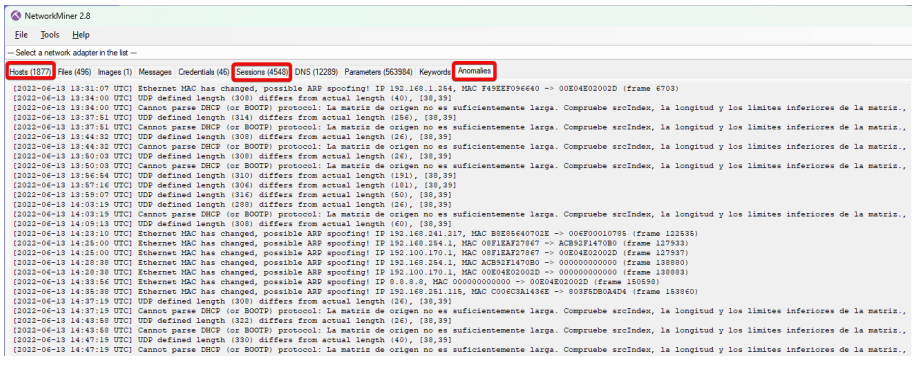


Figura 5.17: Resumen de anomalías desde NetworkMiner.

Para analizar el archivo de captura, se filtró una dirección MAC de las posibles suplantaciones ARP y se encontró que todas las direcciones de IPv4 e IPv6 están enlazadas. Este comportamiento no es normal, por lo tanto, se trata de un problema de configuración incorrecta. Ante esta premisa, este caso se clasifica como verdadero positivo.

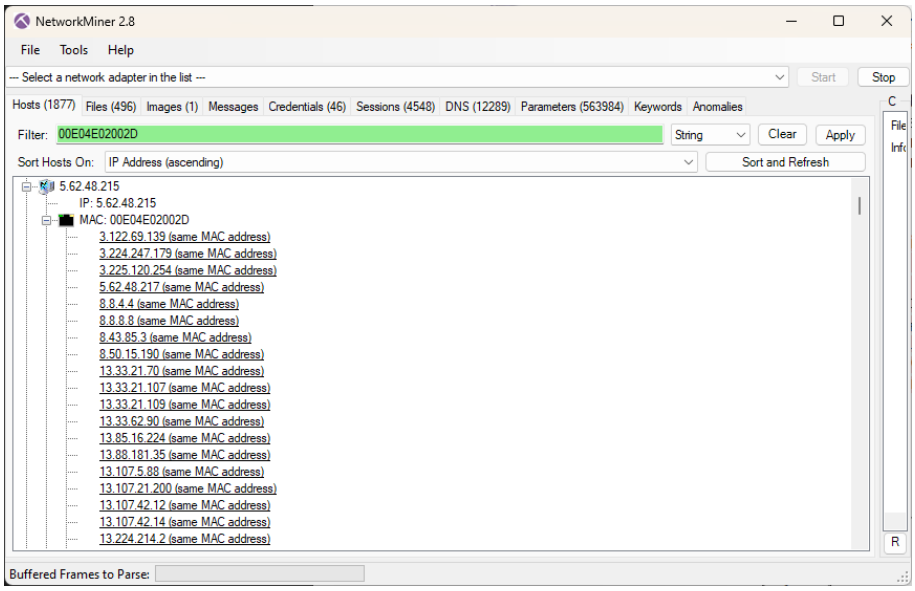


Figura 5.18: Direcciones MAC duplicadas.

Así mismo, se detectaron errores en el servidor DHCP provocando que diferentes dispositivos en la red no tengan una dirección IP válida (véase Figura 5.19). Se les asignó una dirección APIPA, que, mencionado anteriormente, es una dirección IP autogenerada que se asigna a los dispositivos cuando no pueden obtener una dirección IP válida desde un servidor DHCP. Esta situación puede causar problemas de conectividad y debe ser corregida para garantizar un funcionamiento adecuado de la red. En la flecha de color rojo se dimensiona la cantidad de direcciones APIPA que se generaron por esta situación.

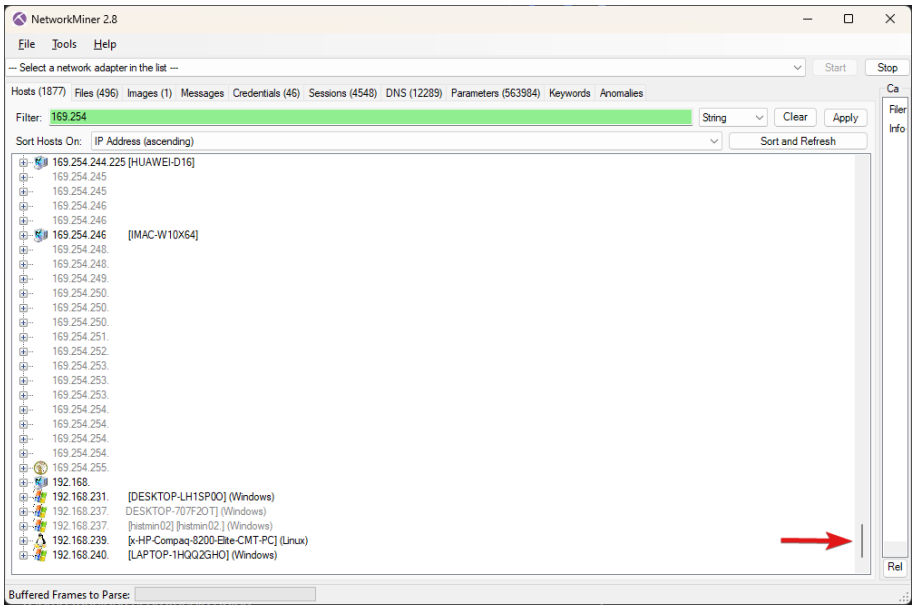


Figura 5.19: Error de configuración del servidor DHCP.

Por último, se filtró la dirección de *broadcast* observándose que en este caso también están incluidas algunas direcciones APIPA (véase Figura 5.20).

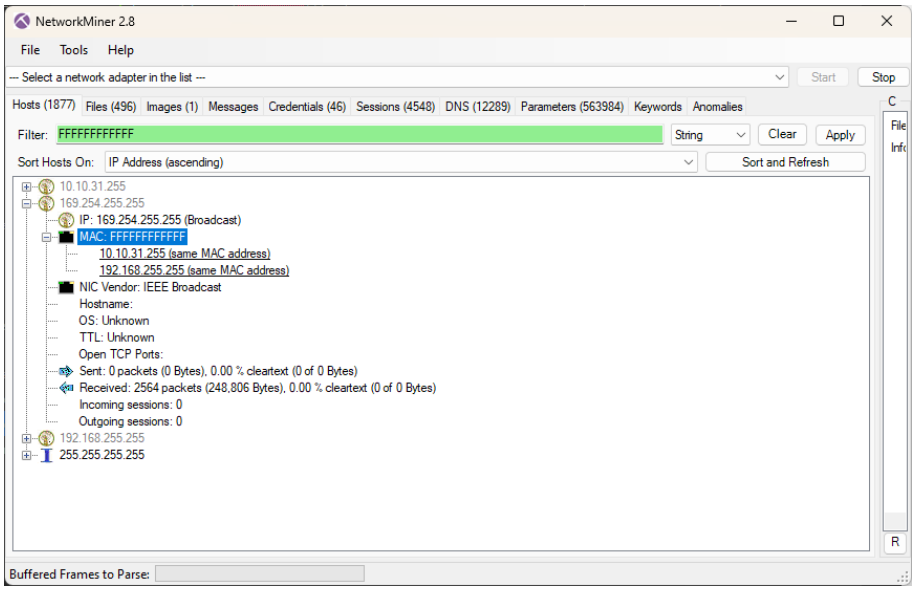


Figura 5.20: Error en la configuración del servidor DHCP.

Continuando con el análisis de los archivos, la Figura 5.21 muestra que la sección Error tiene un caso, sin embargo, pertenece a un protocolo que se encuentra fuera del alcance de esta investigación. En la sección Advertencias, la mayoría tienen que ver con el protocolo TCP, es necesario analizarlas para descartar un posible ataque DDoS o exploración de puertos, así mismo, se observa un caso que tiene que ver con el protocolo ARP, específicamente sobre una dirección IP duplicada. Por otro lado, en la sección Nota, existen diferentes casos, entre ellos TCP, DHCP y ARP/RARP; este último muestra un mensaje indicando que existe una inundación de paquetes ARP. Finalmente en la sección Chat se observan casos entre HTTP y TCP, probablemente exista una exploración de puertos.

Gravedad	Resumen	Grupo	Protocolo	Recuento
Error	Bad checksum [should be 0x9559]	Checksum	HIP	990
Warning	ACKed segment that wasn't captured (common at capture...	Sequence	TCP	74
Warning	TCP window specified by the receiver is now completely full	Sequence	TCP	1
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	3244
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	2145
Warning	Duplicate IP address configured (192.168.254.1)	Sequence	ARP/RARP	719
Warning	DNS query retransmission. Original request in frame 598	Protocol	mDNS	1
Warning	Connection reset (RST)	Sequence	TCP	70
Note	A new tcp session is started with the same ports as an earli...	Sequence	TCP	464
Note	ACK to a TCP keep-alive segment	Sequence	TCP	6
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	414
Note	Duplicate ACK (#1)	Sequence	TCP	12069
Note	This frame undergoes the connection closing	Sequence	TCP	773
Note	ARP packet storm detected (30 packets in < 100 ms)	Sequence	ARP/RARP	2256
Note	Seconds elapsed appears to be encoded as little-endian	Protocol	DHCP/BOOTP	820
Note	Didn't find padding of zeros, and an undecoded trailer exis...	Protocol	Ethernet	80
Note	This frame is a (suspected) retransmission	Sequence	TCP	1666
Note	This frame initiates the connection closing	Sequence	TCP	842
Note	"Time To Live" only 1	Sequence	IPv4	1366
Note	TCP keep-alive segment	Sequence	TCP	15
Note	Didn't find padding of zeros, and an undecoded trailer exis...	Protocol	Ethertype	237414
Chat	Possible traceroute: hop #8, attempt #2	Sequence	UDP	19
Chat	TCP window update	Sequence	TCP	990
Chat	GET / HTTP/1.1\r\n	Sequence	HTTP	1665
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	801
Chat	Connection finish (FIN)	Sequence	TCP	1615
Chat	Connection establish request (SYN): server port 80	Sequence	TCP	1378

Figura 5.21: Resumen de la tercer captura de paquetes en la UTM.

A continuación, en la Figura 5.22 se observan los paquetes filtrados mediante suplantación ARP. Muestra que la dirección fuente se trata del servidor de la UTM que trata de enviar información hacia una dirección IP de la LAN. Este ejemplo no se trata de un ataque como tal, se trata de un error en la red. La solución ante este problema es utilizar protocolos de enrutamiento así como la segmentación física y lógica. Estas recomendaciones permitirán que la red sea más eficiente y evite que el tráfico no deseado llegue a otros dispositivos de la LAN. Este caso se clasifica como falso positivo.

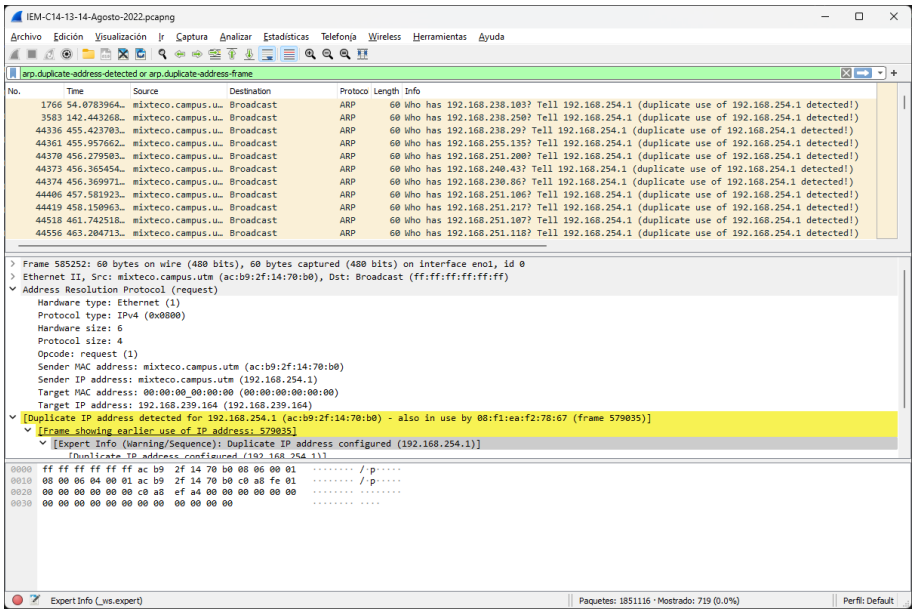


Figura 5.22: Posible suplantación ARP.

En la Figura 5.23 se observan los paquetes al utilizar el filtro de escaneo ARP, el cual se encarga de mostrar paquetes en donde la dirección IP destino pregunta por direcciones IP aleatorias en un corto periodo de tiempo. También se observa el porcentaje de paquetes capturados que equivale a 58.2 % y el tiempo en el que se generaron esos paquetes fue muy corto, por lo tanto, se clasifica como verdadero positivo.

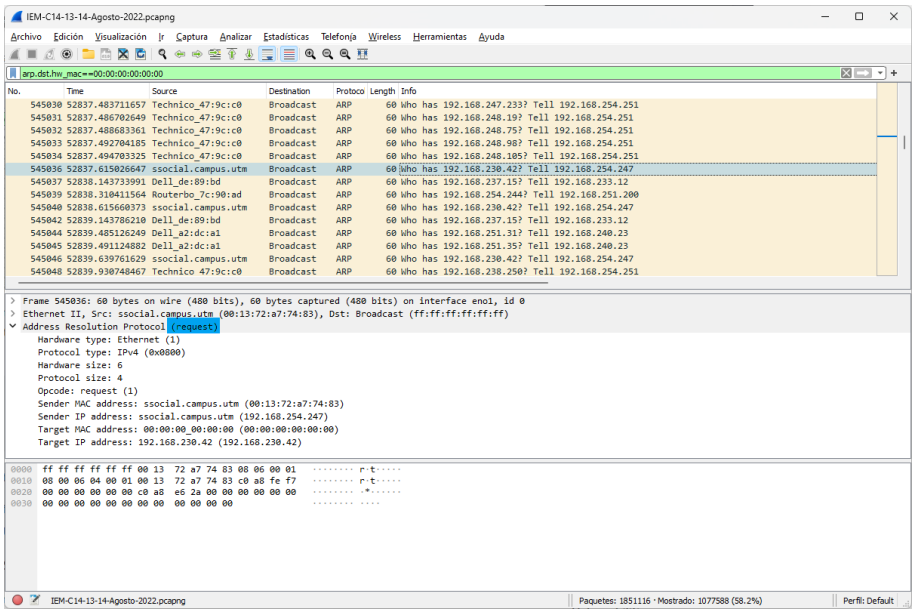


Figura 5.23: Detección de un escaneo ARP.

Por otro lado, el barrido *ping* ICMP de la Figura 5.24 muestra dos paquetes, resultado de una solicitud de direcciones IP desconocidas. Por tal motivo, se clasifica como un verdadero positivo.

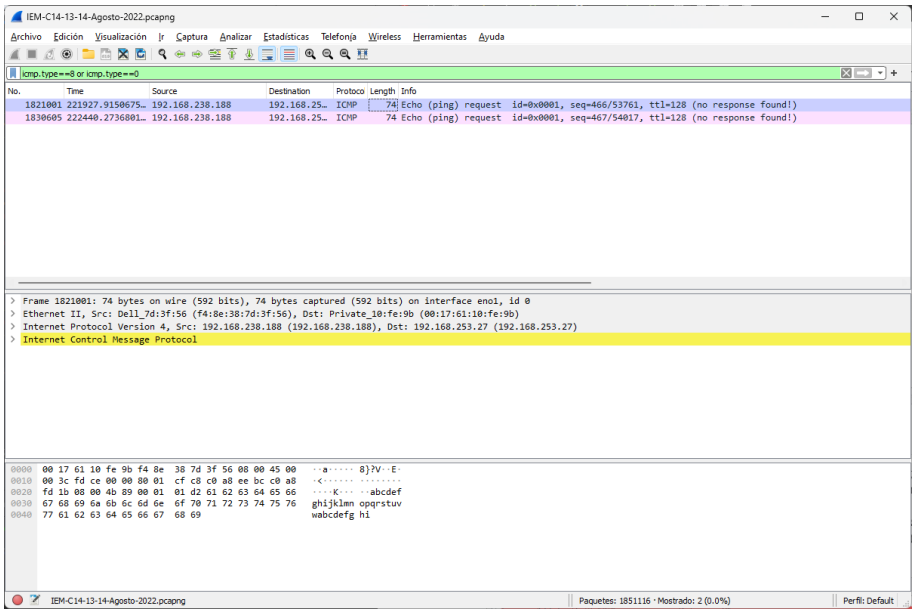


Figura 5.24: Barrido *ping* ICMP.

Analizando el archivo con la herramienta NetworkMiner, la Figura 5.25 muestra que existen 525 huéspedes involucrados, se iniciaron 1008 sesiones a distintos sitios web, en la pestaña Anomalies se muestra un resumen de las posibles amenazas que tiene el archivo en cuestión, relacionadas con la suplantación ARP. Para entender éstas suplantaciones es necesario filtrar las direcciones MAC.

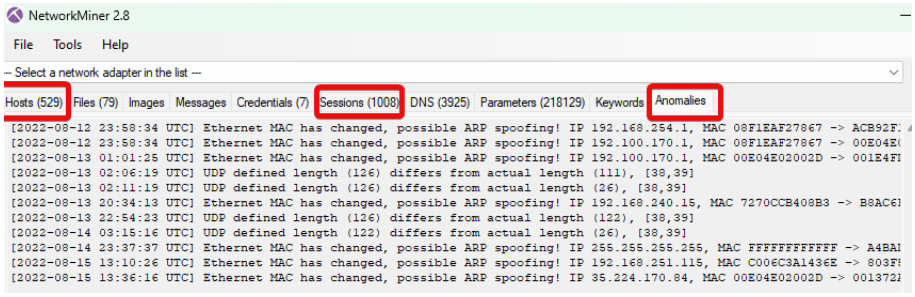


Figura 5.25: Resumen de anomalías desde NetworkMiner.

Al filtrar las direcciones MAC en cuestión, se observa que se trata de un posible ataque de suplantación ARP debido a un cambio en las direcciones MAC en un tiempo mínimo (véase la Figura 5.26).

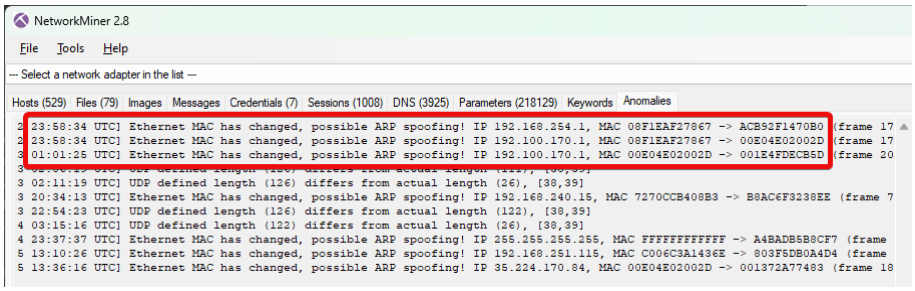


Figura 5.26: Ataque de suplantación ARP.

Continuando con el cuarto archivo de captura, con la opción Información Especializada

arroja el resumen general mostrado en la Figura 5.27. De los protocolos que interesa analizar posee TCP, ICMP, TLS y DHCP.

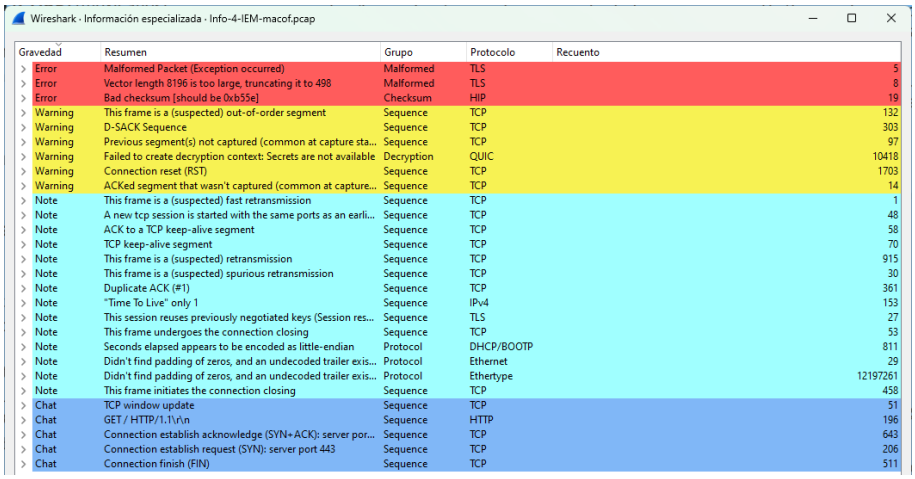


Figura 5.27: Resumen de la cuarta captura de paquetes en la UTM.

Para iniciar el análisis de este archivo, primero se inicia con el filtro de un escaneo ARP. La Figura 5.28 muestra los paquetes que presentan las características para catalogarse como suplantaciones ARP, sin embargo, al estar interactuando con diferentes dispositivos de la red, se sabe que son conmutadores por la firma DELL y una característica de la suplantación ARP es que las peticiones de los paquetes se deben realizar en un periodo de tiempo muy corto, no obstante para este caso no se cumple, por lo tanto, se clasifica como falso positivo.

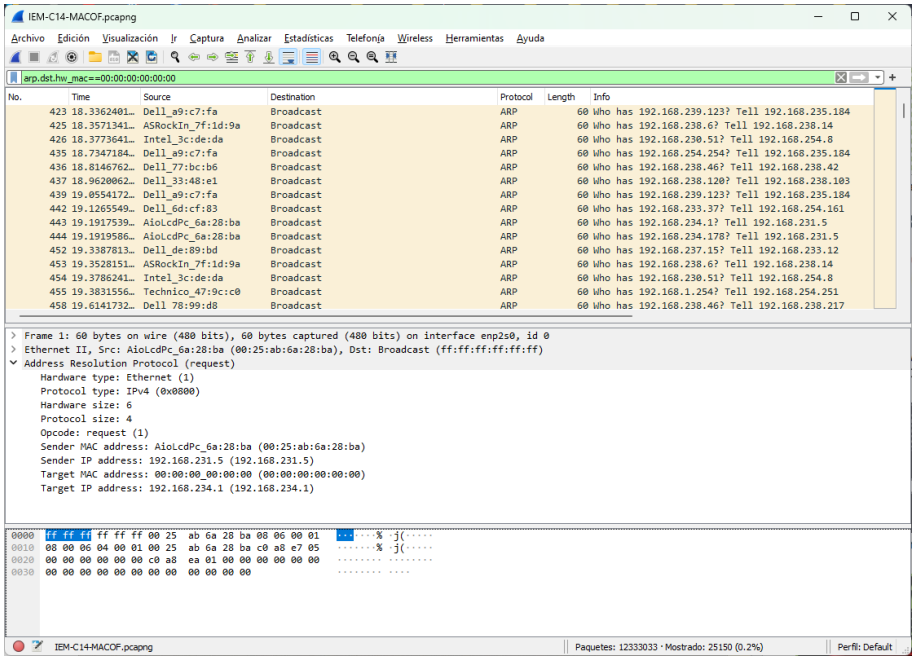


Figura 5.28: Escaneo ARP.

Continuando con el análisis, para realizar un escaneo ICMP se utilizó el filtro `icmp.type==8 || icmp.type == 0`; la Figura 5.29 muestra los paquetes filtrados que posiblemente fueron utilizados para realizar escaneo de puertos hacia una red (destino). Esto se debe a que el filtro busca paquetes ICMP con un tipo de mensaje igual a 8 (solicitud

de eco) o igual a 0 (respuesta de eco). Estos mensajes se utilizan en la herramienta *ping*, que es una forma común de determinar si un huésped está activo en una red. Por ello, si se capturan muchos de estos paquetes con estos tipos de mensajes es probable que se trate de un escaneo ICMP, sin embargo, en este archivo de captura apenas se filtraron 150 paquetes.

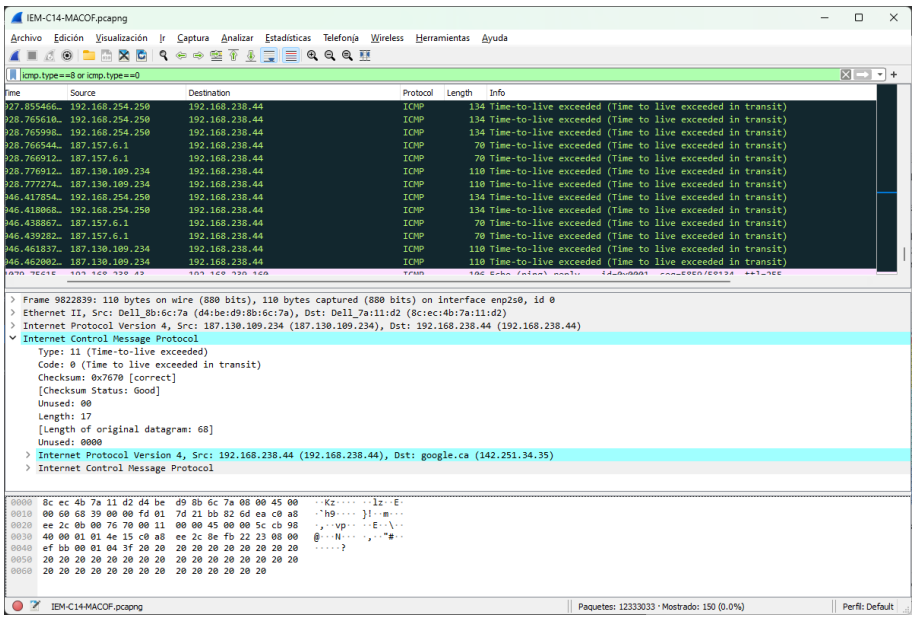


Figura 5.29: Escaneo de puertos ICMP.

Posteriormente, se utilizó el filtro `tcp.flags.syn == 1 and tcp.flags.ack == 0 and tcp.window_size>1024` para mostrar los paquetes que presentan características de escaneo de puertos tipo TCP Connect (véase Figura 5.30). Se observa que el número de paquetes filtrados es mucho menor comparado con los capturados. No obstante, Wireshark emitió una alerta en la sección Chat específicamente sobre el protocolo TCP y en particular con la bandera SYN. Este caso se clasifica como verdadero positivo, es posible que algún mecanismo de seguridad haya interrumpido los escaneos.

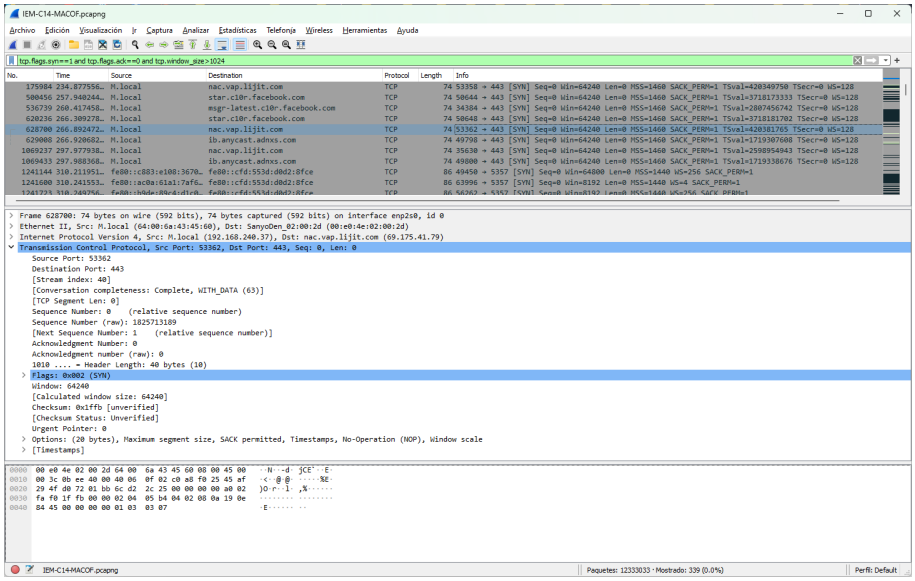


Figura 5.30: Escaneo TCP Connect.

Se utilizó el filtro `arp.duplicate-address-detected || arp.duplicate-address-frame` para la detección de suplantaciones ARP, este filtro buscó los paquetes que presentaran una dirección ARP duplicada en la red (véase Figura 5.31). Los paquetes filtrados indican que alguien intentó realizar una ataque o que existe un error de configuración en algún dispositivo de la red. Ante esta premisa, este caso se clasifica como verdadero positivo.

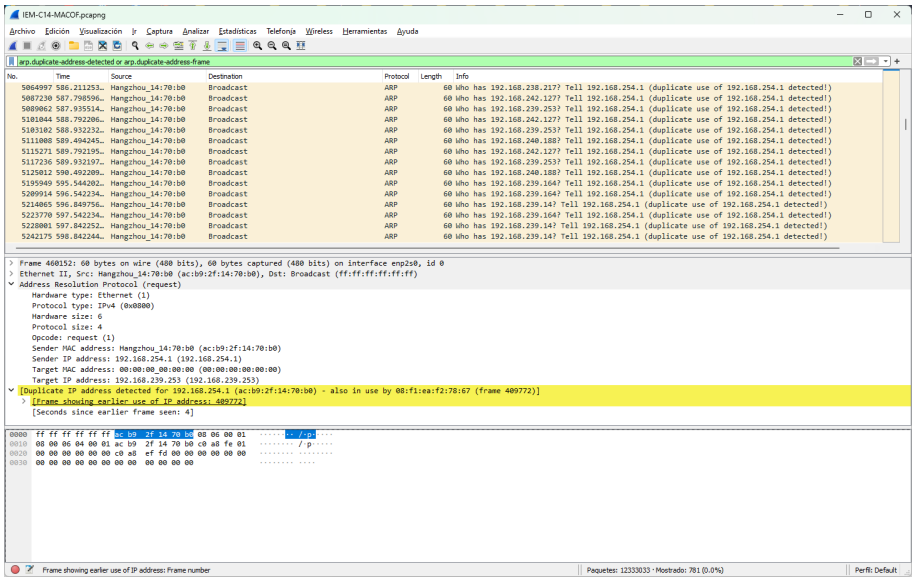


Figura 5.31: Suplantación ARP.

Finalmente, el último filtro a aplicar es `tcp.analysis.lost_segment || tcp.analysis.retransmission`, el cual muestra los paquetes perdidos y retransmitidos. Se observa en la Figura 5.32 que los paquetes llegan a 1012. Estos paquetes filtrados indican que existe congestión en la red que podría afectar la calidad del servicio o la disponibilidad de la red.

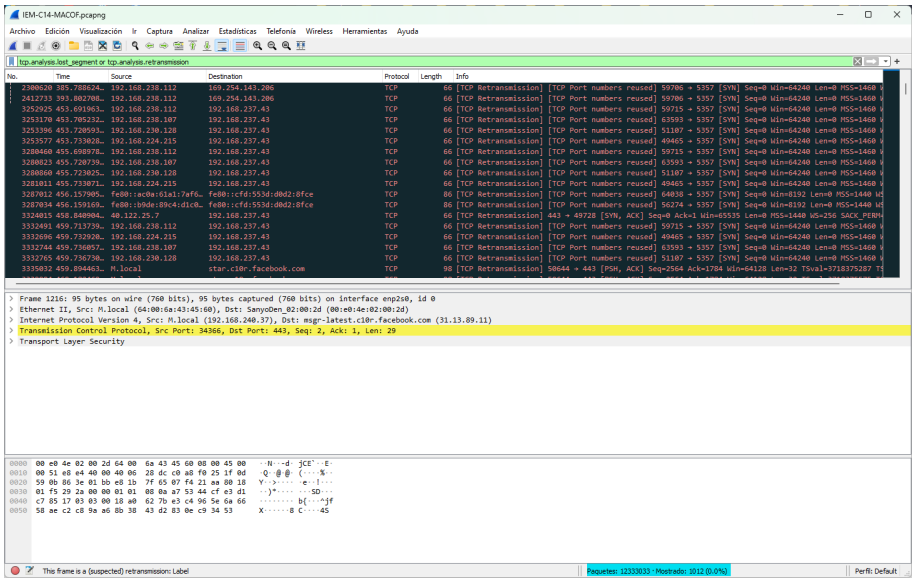


Figura 5.32: Paquetes TCP perdidos y retransmitidos.

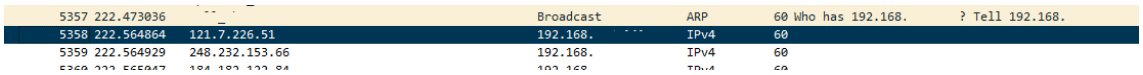
Durante la etapa de captura de paquetes con Wireshark, se tuvo la oportunidad de capturar un evento fortuito. Un ataque con la herramienta *macof* (inundación de direcciones

MAC) de la paquetería DSNIF.[2] Resulta ser un ataque fácil de detectar, ya que consiste en enviar múltiples paquetes falsificados a través de un puerto con el objetivo de saturar la tabla de asignación del conmutador.

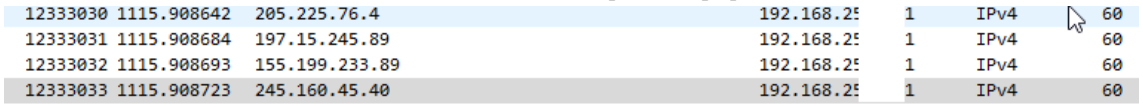
Generalmente, un conmutador dispone de una memoria interna denominada CAM (Memoria de Contenido de Direcciones, *Content-Addressable Memory*) donde asigna puertos a direcciones MAC. Cuando una trama llega a un puerto, la CAM añade una entrada a la tabla especificando la MAC del equipo que transmitió la trama junto con el puerto en el que se encuentra. De esta forma, cuando el conmutador recibe una trama dirigida a ese equipo sabrá por qué puerto debe enviarla [37]. En algunas ocasiones, se desconoce el destino del paquete, esto sucede debido a que el equipo no logra generar tráfico o porque la entrada asociada al equipo ha expirado. El conmutador copia la trama y la envía por todos lo puertos excepto por el que fue recibido. Por consiguiente, todos los equipos conectados al conmutador recibirán dicha trama y únicamente el equipo correspondiente, aquel que tenga la MAC que coincida con la MAC destino de la trama, contestará. Esta acción permite al conmutador añadir una entrada a su tabla CAM con la nueva asociación MAC/puerto. Con base en lo anterior, los puertos del conmutador no serán inundados con futuros paquetes dirigidos a este equipo.

Sí se envían cientos de tramas falsificando la MAC origen del equipo y llenando la tabla CAM. Ante este caso, el comportamiento depende del fabricante. Los conmutadores de gama baja no contienen tablas CAM virtualizadas, esto quiere decir que si la tabla dispone de un número *n* de asociaciones MAC/puerto, y un equipo consigue llenar dicha tabla con *n* entradas, la tabla se llenará y todas las VLANs se verán afectadas. Detectar este tipo de ataque resulta sencillo, únicamente mirando el tráfico generado, se observa gran cantidad de tramas con valores aleatorios. Lo que se visualizó con Wireshark fue lo siguiente:

- Genera demasiado tráfico *broadcast* utilizando el protocolo ARP.
- Genera tráfico utilizando el protocolo IPv4 comenzando desde el paquetes 5358 hacia una dirección destino específica mientras que la direcciones IP fuentes son aleatorias y termina en el paquete 12 333 033 (véase Figura 5.33).



(a) Inicio del tráfico aleatorio a partir del paquete 5358.



(b) Fin del tráfico aleatorio en el paquete 12333033.

Figura 5.33: Inició y fin de direcciones IP aleatorias hacia una dirección específica.

Al abrir el archivo con la herramienta NetworkMiner se presentan algunos eventos no comunes, estos se mencionan a continuación:

- Al inicializar el archivo la memoria RAM del equipo portátil se satura (véase Figura 5.34).

[2]Conjunto de herramientas para la auditoría de red y pruebas de penetración que permiten analizar diferentes protocolos de aplicación y extraer información relevante. `dsniff`, `filesnarf`, `mailsnarf`, `msgsnarf`, `urlsnarf`, y `webspy` monitorean pasivamente una red para obtener datos interesantes como contraseñas, correo electrónico o archivos. `arpspoof`, `dnsspoof` y `macof` facilitan la intercepción del tráfico de red [57].

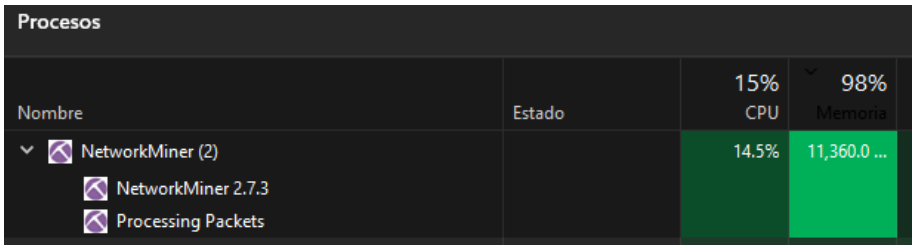


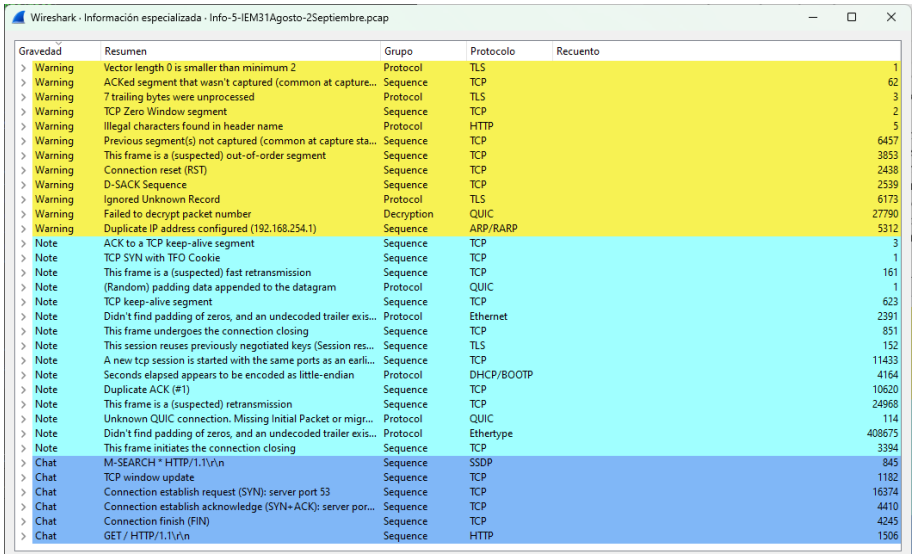
Figura 5.34: Problemas al abrir el archivo utilizando NetworkMiner.

- La ventana de NetworkMiner muestra el proceso de carga (abrir el archivo) y se detiene al 13 % (véase Figura 5.35).

Figura 5.35: Ventana de NetworkMiner al momento de saturar la memoria RAM del equipo.

Ante estos eventos, es claro que la cantidad de tráfico generado es demasiado, por lo tanto, no es posible visualizarlo detalladamente con la herramienta NetworkMiner. Al presentarse este caso, es necesario utilizar equipo de cómputo con características técnicas apropiadas para analizar este tipo de archivos.

Continuando con la siguiente captura de paquetes, la Figura 5.36 muestra que no existe ningún caso en la sección de Error, sin embargo, al observar la sección de Advertencias la mayoría de casos pertenece al protocolo TCP lo cual aumenta la posibilidad de que se trate de un ataque DDoS o escaneo de puertos. Así mismo, se observa que existe una caso que tiene que ver con el protocolo HTTP y uno más que incluye al protocolo ARP, en este último es necesario utilizar el filtro de suplantación ARP.



Gravedad	Resumen	Grupo	Protocolo	Recuento
Warning	Vector length 0 is smaller than minimum 2	Protocol	TLS	1
Warning	ACKed segment that wasn't captured (common at capture...	Sequence	TCP	62
Warning	7 trailing bytes were unprocessed	Protocol	TLS	3
Warning	TCP Zero Window segment	Sequence	TCP	2
Warning	Illegal characters found in header name	Protocol	HTTP	5
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	6457
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	3853
Warning	Connection reset (RST)	Sequence	TCP	2438
Warning	D-SACK Sequence	Sequence	TCP	2539
Warning	Ignored Unknown Record	Protocol	TLS	6173
Warning	Failed to decrypt packet number	Decryption	QUIC	27790
Warning	Duplicate IP address configured (192.168.254.1)	Sequence	ARP/RARP	5312
Note	ACK to a TCP keep-alive segment	Sequence	TCP	3
Note	TCP SYN with TFO Cookie	Sequence	TCP	1
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	161
Note	(Random) padding data appended to the datagram	Protocol	QUIC	1
Note	TCP keep-alive segment	Sequence	TCP	623
Note	Didn't find padding of zeros, and an undecoded trailer exis...	Protocol	Ethernet	2391
Note	This frame undergoes the connection closing	Sequence	TCP	851
Note	This session reuses previously negotiated keys (Session res...	Sequence	TLS	152
Note	A new tcp session is started with the same ports as an earli...	Sequence	TCP	11433
Note	Seconds elapsed appears to be encoded as little-endian	Protocol	DHCP/BOOTP	4164
Note	Duplicate ACK (#1)	Sequence	TCP	10620
Note	This frame is a (suspected) retransmission	Sequence	TCP	24968
Note	Unknown QUIC connection. Missing Initial Packet or migr...	Protocol	QUIC	114
Note	Didn't find padding of zeros, and an undecoded trailer exis...	Protocol	Ethertype	408675
Note	This frame initiates the connection closing	Sequence	TCP	3394
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	845
Chat	TCP window update	Sequence	TCP	1182
Chat	Connection establish request (SYN): server port 53	Sequence	TCP	16374
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	4410
Chat	Connection finish (FIN)	Sequence	TCP	4245
Chat	GET / HTTP/1.1\r\n	Sequence	HTTP	1506

Figura 5.36: Resumen de la quinta captura de paquetes en la UTM.

Para el análisis de este archivo se comienza por la suplantación ARP, la Figura 5.37

muestra los paquetes filtrados en donde posiblemente exista suplantación, cabe mencionar que estas peticiones las hace el servidor de la UTM, ante esto, la opción de ataque queda descartada y por lo tanto se clasifica como falso positivo.

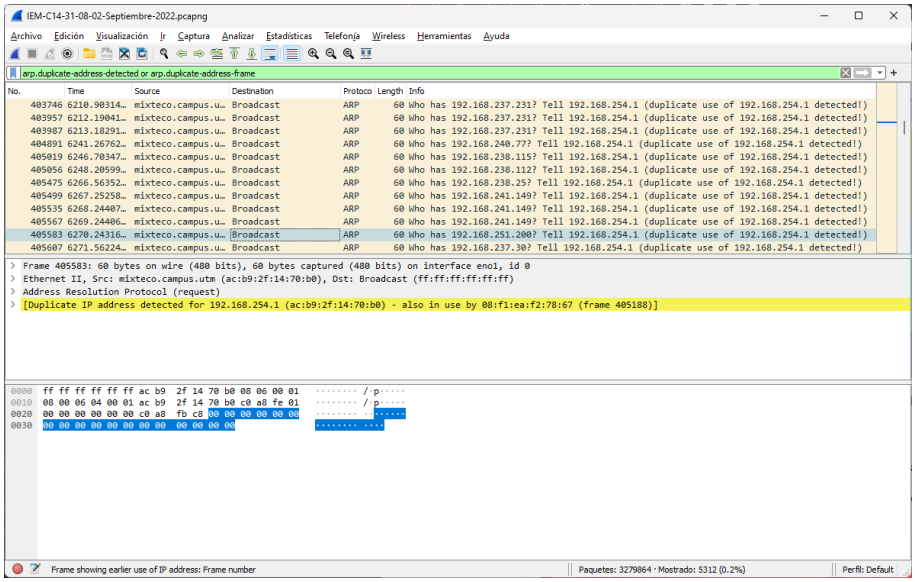


Figura 5.37: Posible suplantación ARP.

Otra de las amenazas comunes que puede existir en una red es el barrido *ping* ICMP. Como se observa en la Figura 5.38, el huésped origen busca un destino con alguna dirección IP disponible, también se puede utilizar para observar el comportamiento de las demás redes. La figura en cuestión informa que el origen no recibió ninguna respuesta del huésped destino. De igual manera, se observa que el huésped destino es una dirección IP desconocida, probablemente se trate de servidores que pertenecen al proveedor de servicio de Internet. Ante esta premisa, este caso se clasifica como falso positivo.

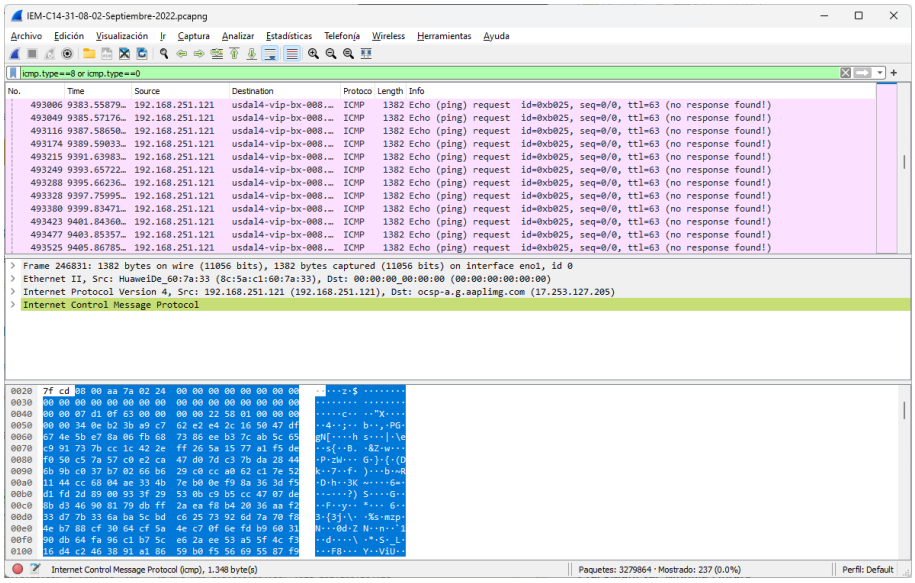


Figura 5.38: Barrido *ping* ICMP.

Continuando con el análisis, la Figura 5.39 muestra paquetes filtrados asociados a un escaneo ARP, la mayoría de las direcciones IP pertenecen a conmutadores, enrutadores y servidores de la UTM, sin embargo, si se detecta tráfico que cumple con este filtro, se

puede analizar más a fondo para determinar si es un problema de seguridad o simplemente un error de configuración de red.

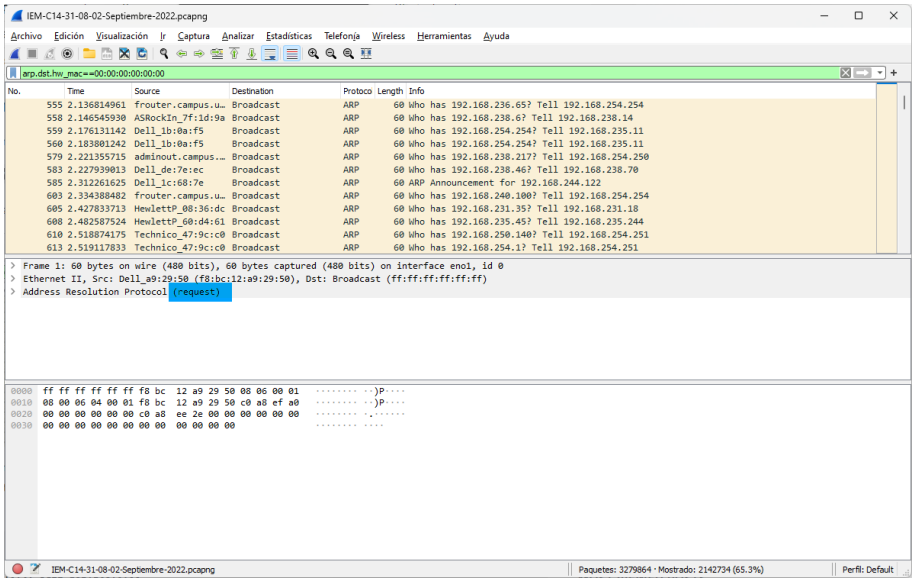


Figura 5.39: Escaneo ARP.

Los paquetes que se observan en la Figura 5.40 son 186, los cuales no se consideran como un ataque a la red comparado con los paquetes capturados, sin embargo, también existe la posibilidad que las herramientas de defensa funcionaron adecuadamente para rechazar el ataque.

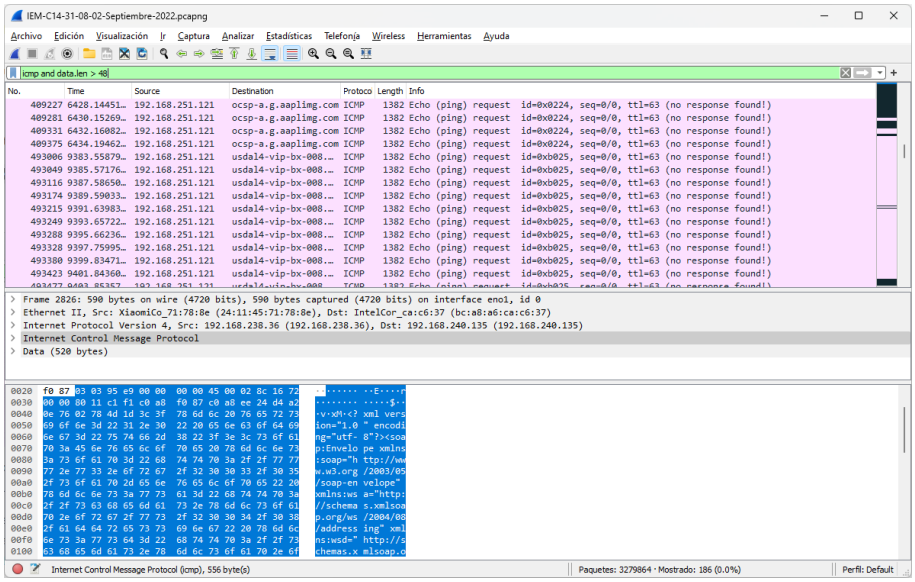


Figura 5.40: Inundación ICMP.

Finalmente, la Figura 5.41 filtra paquetes que presentan características de retransmisión y pérdida. El recuento de paquetes llega al 1 % equivalente a 31423 de 3279864 paquetes capturados. Se observa también que en la sección de características del paquete, TCP presenta problemas en la sección Nota, esto indica errores inusuales sobre TCP.

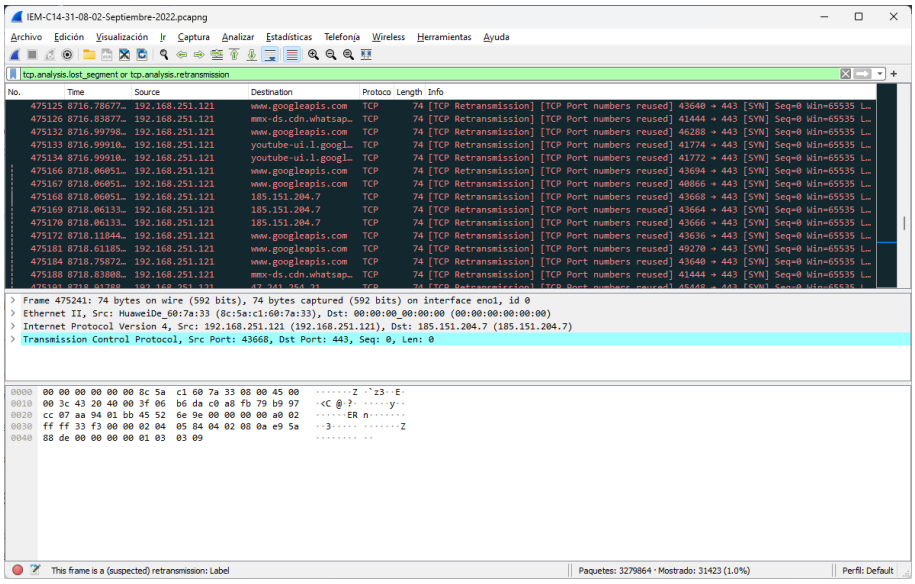


Figura 5.41: Pérdida y transmisión de paquetes TCP.

Continuando con el análisis de paquetes, el archivo que analizó NetworkMiner es el quinto archivo de captura. La Figura 5.42 muestra que durante la captura de este archivo hubo 2637 huéspedes, se realizaron 12790 inicios de sesión a diferentes sitios web y en la pestaña Anomalies se muestra un resumen de las posibles amenazas que tiene el archivo en cuestión.

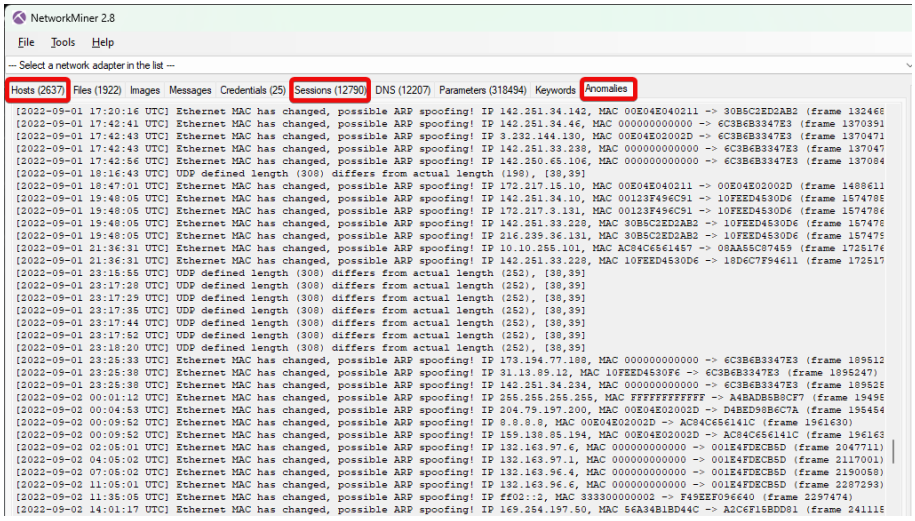


Figura 5.42: Resumen de anomalías desde NetworkMiner.

En la Figura 5.42 se observa un número extenso de posibles suplantaciones ARP, sin embargo, la mayoría se trata de problemas con la administración de la red específicamente de tráfico *broadcast*. Del mismo modo, se aplicó el filtro `169.254.` para que filtrará todas las direcciones APIPA, y así determinar qué se asigna cuando los equipos no encuentran su servidor DHCP, esto sucede porque de alguna forma las direcciones pertenecientes a la red no encontraron su servidor destino y se asignaron a la dirección APIPA (véase Figura 5.43).

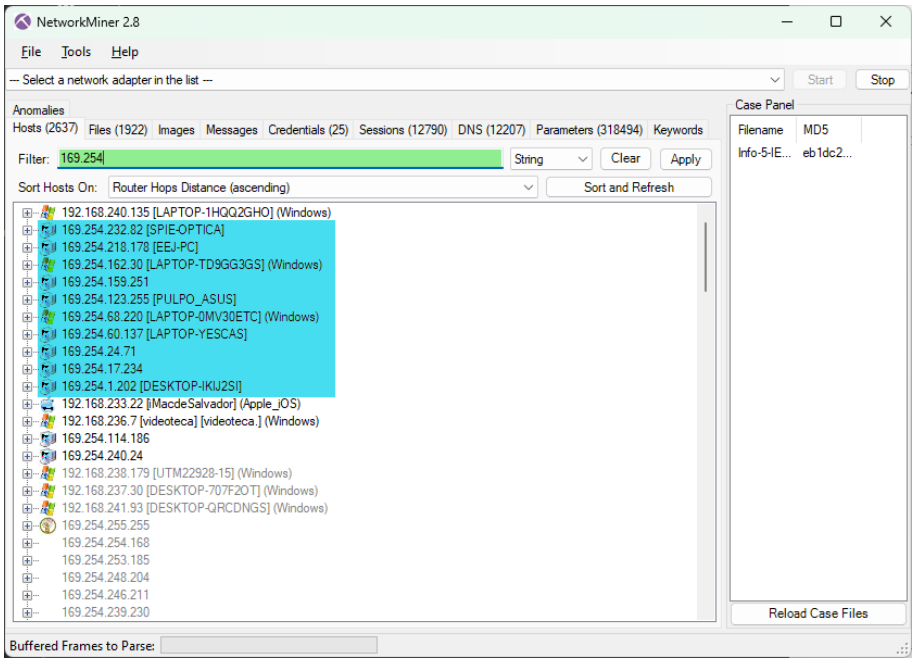


Figura 5.43: Problemas con el servidor DHCP.

Para iniciar la detección de amenazas en el sexto archivo de captura, en la Figura 5.44 se observan cuatro casos en la sección Error, de los cuales únicamente TLS y HTTP son de interés para el desarrollo de esta investigación. Mientras que en la sección Advertencias el protocolo que predomina es TCP; es necesario analizar mediante Gráficas de Flujo para descartar posibles ataques DDoS, otros protocolos son TLS y HTTP. En esta captura no se presenta ninguna suplantación de ARP, sin embargo, se debe aplicar el filtro para descartar totalmente.

Gravedad	Resumen	Grupo	Protocolo	Recuento
Error	Incorrect Mailbox data length(Expected:17700 Actual:1440)	Malformed	ECAT_MAILBOX	3
Error	TLSCiphertext length MUST NOT exceed 2^14 + 2048	Protocol	TLS	1
Error	Malformed Packet (Exception occurred)	Malformed	HTTP	23
Error	Bad checksum [should be 0xef6e]	Checksum	HIP	220
Warning	DNS response retransmission. Original response in frame 6...	Protocol	mDNS	4
Warning	Illegal characters found in header name	Protocol	HTTP	7302
Warning	DNS query retransmission. Original request in frame 5683	Protocol	mDNS	168
Warning	Failed to create decryption context: Unable to retrieve ciph...	Decryption	QUIC	73
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	12674
Warning	D-SACK Sequence	Sequence	TCP	112
Warning	Ignored Unknown Record	Protocol	TLS	522
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	12582
Warning	Connection reset (RST)	Sequence	TCP	165
Note	This session reuses previously negotiated keys (Session res...	Sequence	TLS	1
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	37
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	127
Note	ACK to a TCP keep-alive segment	Sequence	TCP	97
Note	TCP keep-alive segment	Sequence	TCP	211
Note	(Random) padding data appended to the datagram	Protocol	QUIC	25
Note	Seconds elapsed appears to be encoded as little-endian	Protocol	DHCP/BOOTP	10
Note	Duplicate ACK (#1)	Sequence	TCP	44748
Note	"Time To Live" only 1	Sequence	IPv4	1
Note	This frame undergoes the connection closing	Sequence	TCP	440
Note	Didn't find padding of zeros, and an undecoded trailer exis...	Protocol	Ethertype	2322
Note	This frame initiates the connection closing	Sequence	TCP	549
Note	A new tcp session is started with the same ports as an earli...	Sequence	TCP	312
Note	This frame is a (suspected) retransmission	Sequence	TCP	4519
Chat	Possible traceroute: hop #10, attempt #2	Sequence	UDP	2
Chat	TCP window update	Sequence	TCP	4633
Chat	GET / HTTP/1.1\r\n	Sequence	HTTP	600
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	514
Chat	Connection finish (FIN)	Sequence	TCP	989
Chat	Connection establish request (SYN): server port 7680	Sequence	TCP	926

Figura 5.44: Resumen de la sexta captura de paquetes en la UTM.

Para iniciar este análisis se comienza con un escaneo ARP con el fin de observar los paquetes que presentan estas características. La Figura 5.45 muestra que el origen de estos paquetes pertenece a diferentes conmutadores con destino *broadcast*.

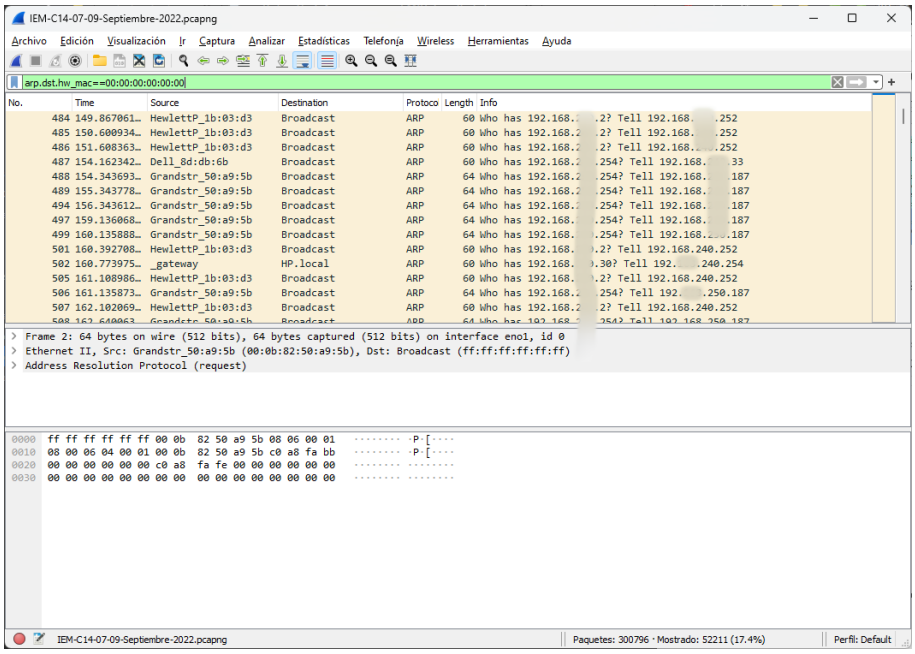


Figura 5.45: Escaneo ARP.

Por lo tanto, con base al resumen general mostrado por Wireshark, no existe ninguna advertencia sobre ARP, esto quiere decir que el archivo no presenta alguna suplantación ARP, para verificar es necesario aplicar el filtro de visualización de suplantación ARP. En la Figura 5.46 se observa que en efecto, el archivo de captura se encuentra limpio de paquetes con posible suplantación ARP. Lo que se muestra en la Figura 5.46 es el escenario ideal que todo administrador de red desea.

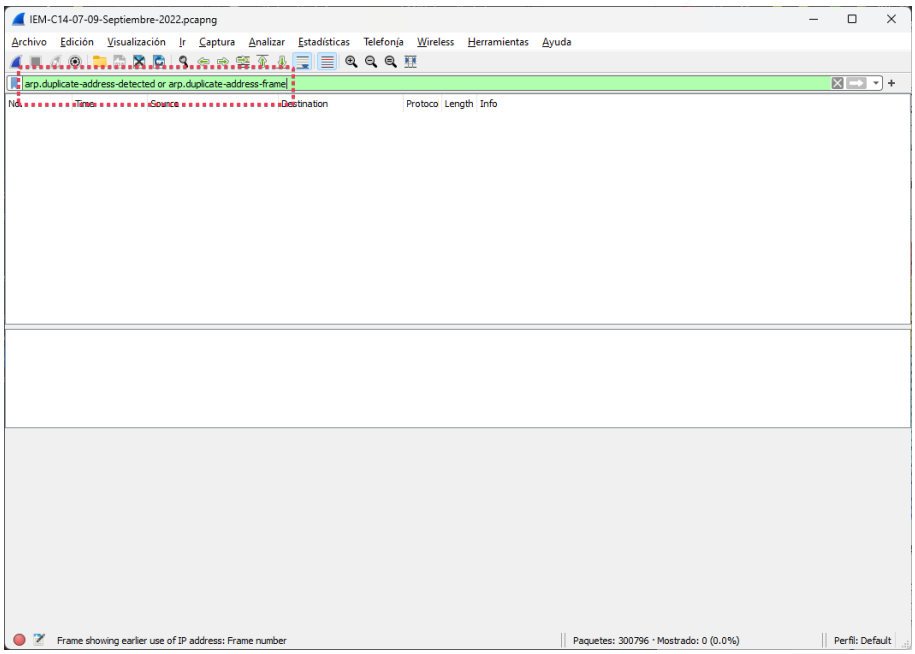


Figura 5.46: Paquete libre de suplantaciones ARP.

En la Figura 5.47 se observa que existen dos paquetes; solicitud y respuesta de ICMP. Esta comunicación involucra a un usuario del IEM que realizó una solicitud *ping* hacia un equipo y éste respondió. Lo anterior fue el proceso inicial de un escaneo ICMP para

descubrir los huéspedes activos en la red y posteriormente efectuar un ataque. Por lo anterior, este caso se clasifica como verdadero positivo.

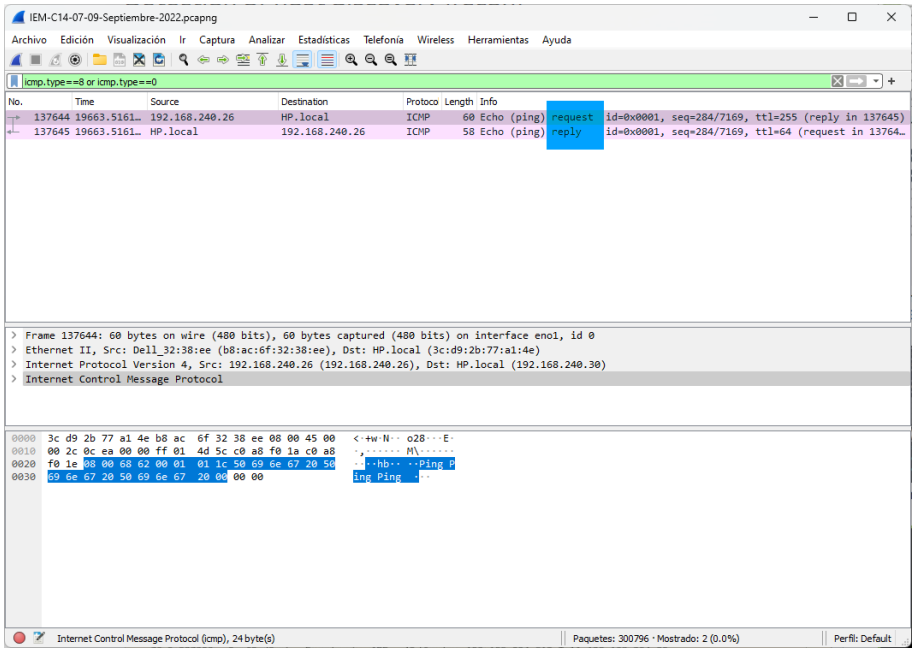


Figura 5.47: Barrido *ping* ICMP, solicitud y respuesta.

Finalmente, para visualizar los paquetes que han sido retransmitidos y perdidos se utiliza el filtro `tcp.analysis.lost_segment || tcp.analysis.retransmission`. En la Figura 5.48 se observa que el porcentaje mostrado equivale a un 5.7 %. Esta cifra indica que el rendimiento de la red se ha visto afectado. Ante este porcentaje alto comparado con los demás archivos analizados, es posible que existan problemas en la red o intentos de ataque como denegación de servicio o simplemente una explotación de vulnerabilidades con respecto a TCP. Los paquetes perdidos o retransmitidos pueden ser causados por una variedad de factores como problemas en los nodos de red, problemas de software o simplemente congestión en la red.

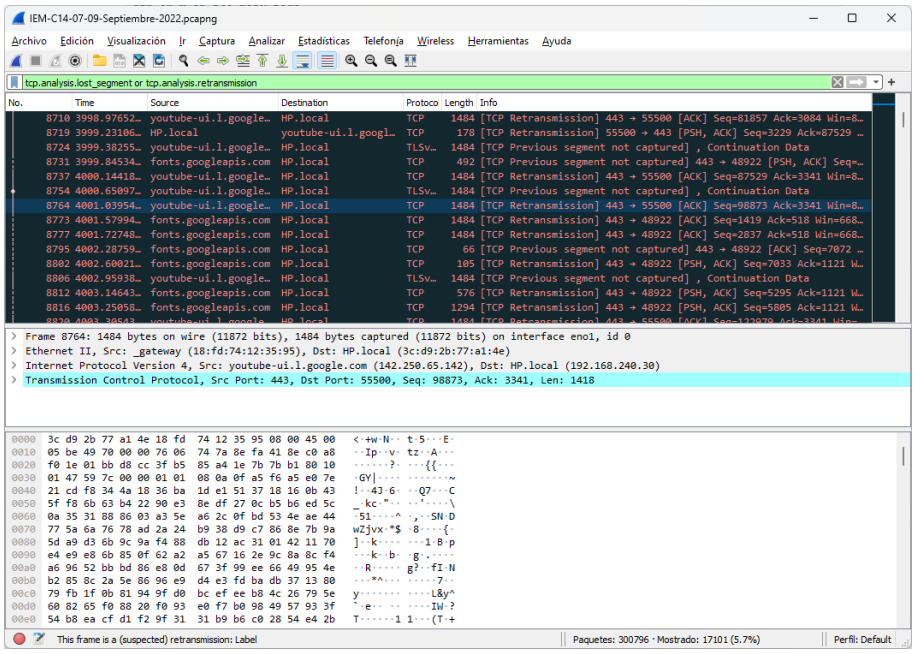


Figura 5.48: Paquetes TCP perdidos y retransmitidos.

Para finalizar el análisis de este archivo de captura, se utilizó la herramienta NetworkMiner; al abrir el archivo, se observa que se capturaron 238 huéspedes, se realizaron 681 inicios de sesión a diferentes sitios web y en la pestaña Anomalies se muestra un resumen de las posibles amenazas que tiene el archivo en cuestión, sin embargo, para este archivo se encontró un mensaje explicando que no se pudo analizar el protocolo DHCP (véase Figura 5.49), esto quiere decir que coincide con la Información especializada de Wireshark al no presentarse ninguna amenaza de suplantación ARP.

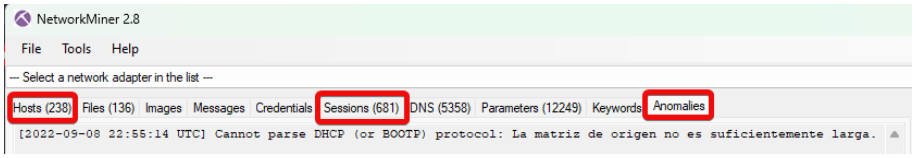


Figura 5.49: Resumen de anomalías desde NetworkMiner.

Para dar inicio al análisis del séptimo archivo de captura, la Figura 5.50 podría ser el caso ideal de una captura de paquetes en la que no existen errores, sin embargo, no se descarta el uso de filtros para verificar que se trate de un archivo libre de amenazas. Como se mencionó en el apartado 2.13.3, la gravedad de la sección Nota reporta algunos errores inusuales; existe una duplicación de ACK y se encuentra en el protocolo TCP, es necesario analizarlas para descartar amenazas y afirmar que se trata de una captura perfecta.

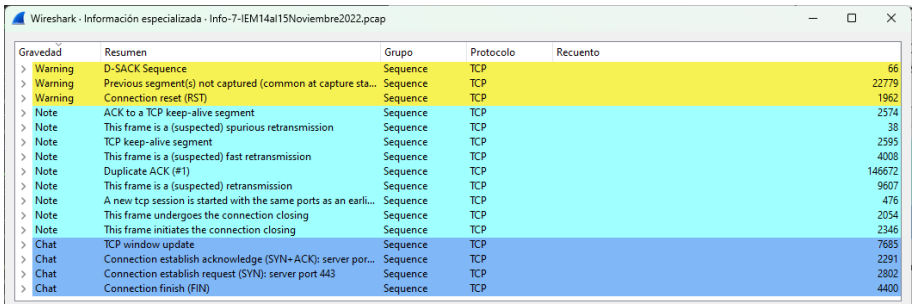


Figura 5.50: Resumen de la séptima captura de paquetes en la UTM.

Comenzando con el filtro de suplantación ARP, los paquetes filtrados se observan en la Figura 5.51 resultando contradictorio puesto que en la Figura 5.50 la Información Especializada arroja que no existe advertencia. Ante esto, es necesario implementar los demás filtros para descartar cualquier amenaza.

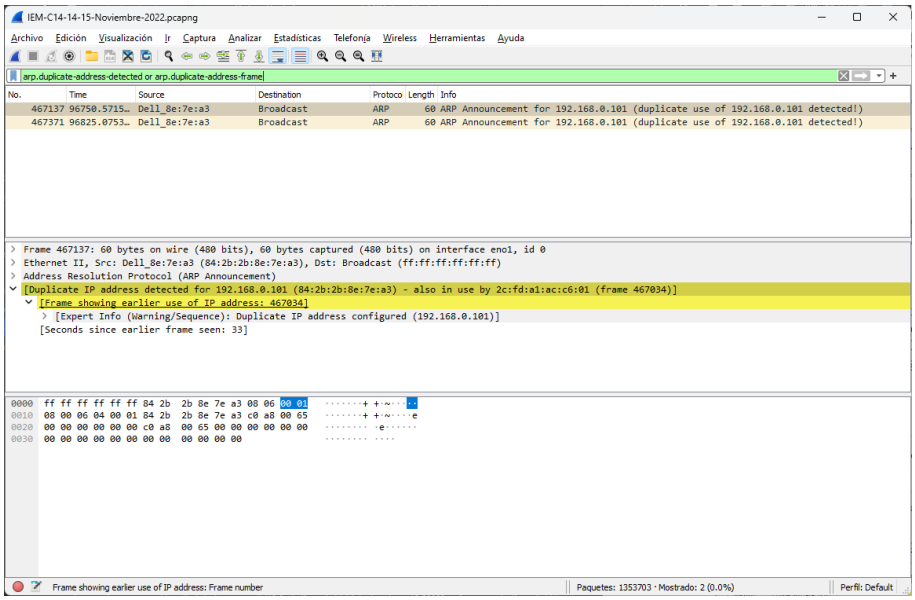


Figura 5.51: Posible suplantación ARP.

Al aplicar los filtros relacionados con el escaneo de puertos no se encontraron amenazas, no obstante, se aplicó el filtro para mostrar paquetes perdidos y retransmitidos. Las Figuras 5.52 muestra un porcentaje de 1.7 % que equivale a 22779 paquetes mostrados, esto quiere decir que existe algún factor que causa este tipo de pérdida de paquetes.

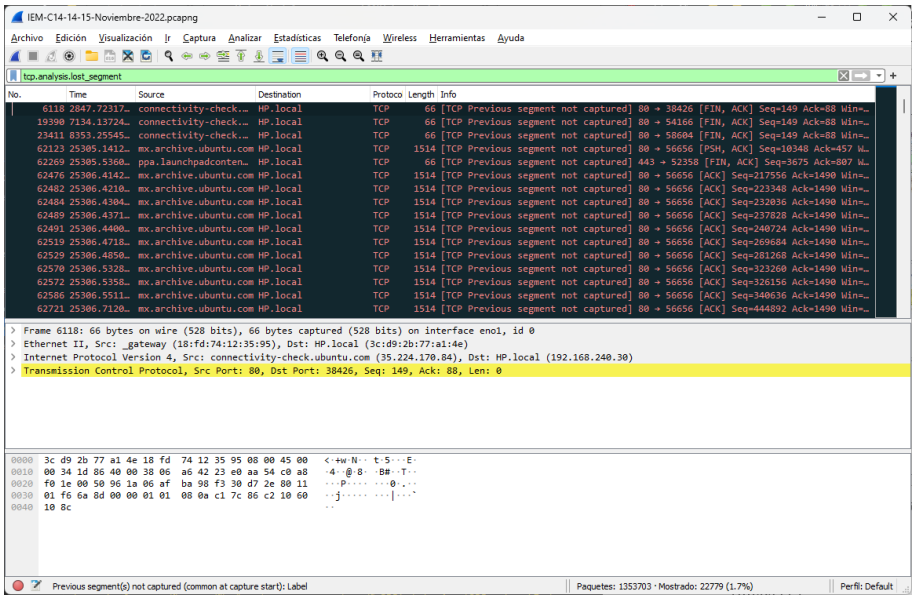


Figura 5.52: Paquetes perdidos.

En la figura 5.53 se muestran los paquetes retransmitidos, el porcentaje es de 0.7 % que equivale a 9607 paquetes, de la misma manera que en los paquetes perdidos.

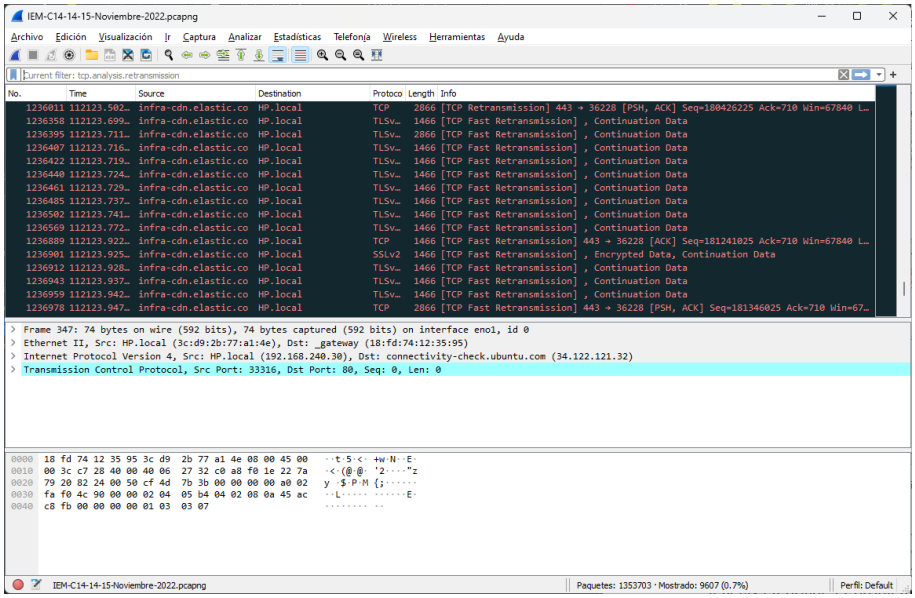


Figura 5.53: Paquetes retransmitidos.

Para este archivo la herramienta NetworkMiner indica que se capturaron 1791 huéspedes, se registraron 2966 inicios de sesión a diferentes sitios web y en la pestaña Anomalies se muestra un resumen de las posibles amenazas que tiene el archivo en cuestión (véase Figura 5.54):

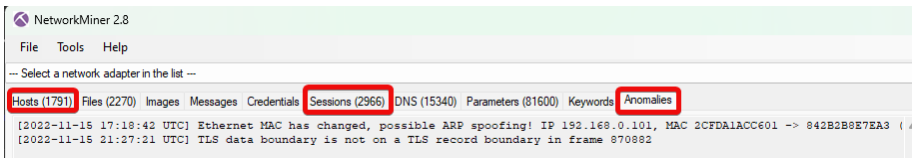


Figura 5.54: Resumen de anomalías desde NetworkMiner.

Detallando el análisis, se filtró la dirección MAC que presenta una suplantación ARP y se observan tres direcciones IP de las cuales, la primera tiene los primeros dos bytes en `169.254`, significa que dicha dirección IP corresponde al direccionamiento privado automático del protocolo de Internet, esta dirección IP se asigna cuando los equipos no encuentran su servidor DHCP. A la hora de que estos dispositivos encontraron su servidor se les volvió a asignar la dirección de `192.168.*.*` y comenzó el envío de paquetes con dicha dirección, sin embargo, al salir de la misma interfaz poseen la misma dirección MAC (véase Figura 5.55).

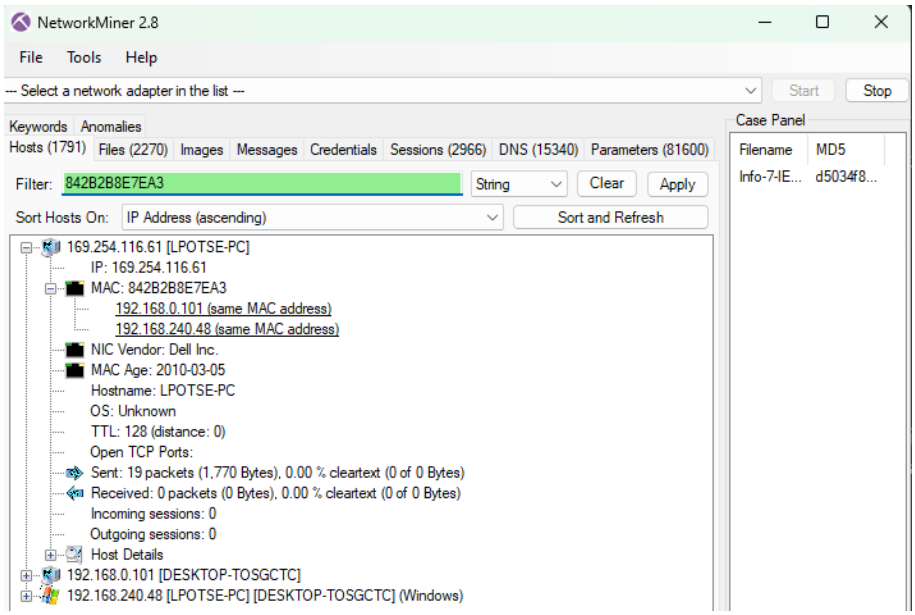


Figura 5.55: Error en el servidor DHCP.

Para concluir la detección de amenazas en la red de la UTM, la Figura 5.56 pertenece al archivo 8 de la Tabla 5.1. Se observa la Información especializada y con ello un error que pertenece a un protocolo que se encuentra fuera del alcance de esta investigación, seguido de este, aparecen cuatro casos en la sección Advertencias en donde el problema se enfoca en al rendimiento de la red o un posible ataque de denegación de servicio. Es necesario implementar funciones extras para descartar cualquier amenaza.

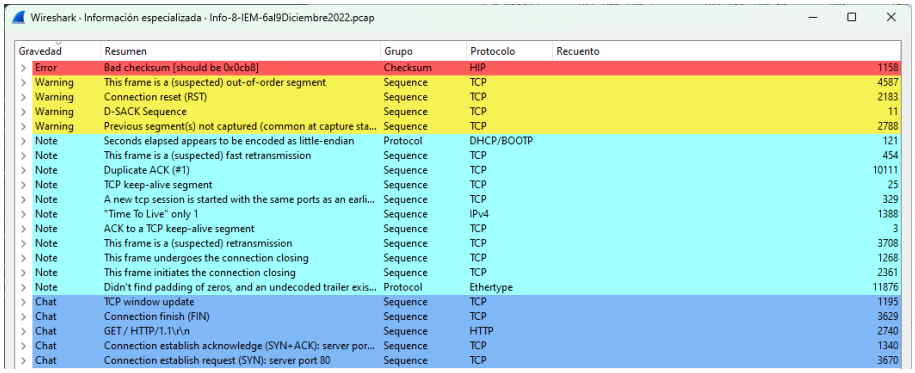


Figura 5.56: Resumen de la octava captura de paquetes en la UTM.

Con el fin de confirmar la ausencia de cualquier posible amenaza derivada de la suplantación ARP, se procede a aplicar el filtro `arp.duplicate-address-detected || arp.duplicate-address-frame`, la Figura 5.57 muestra que en efec-

to, no existe presencia de amenazas relacionadas con la suplantación ARP.

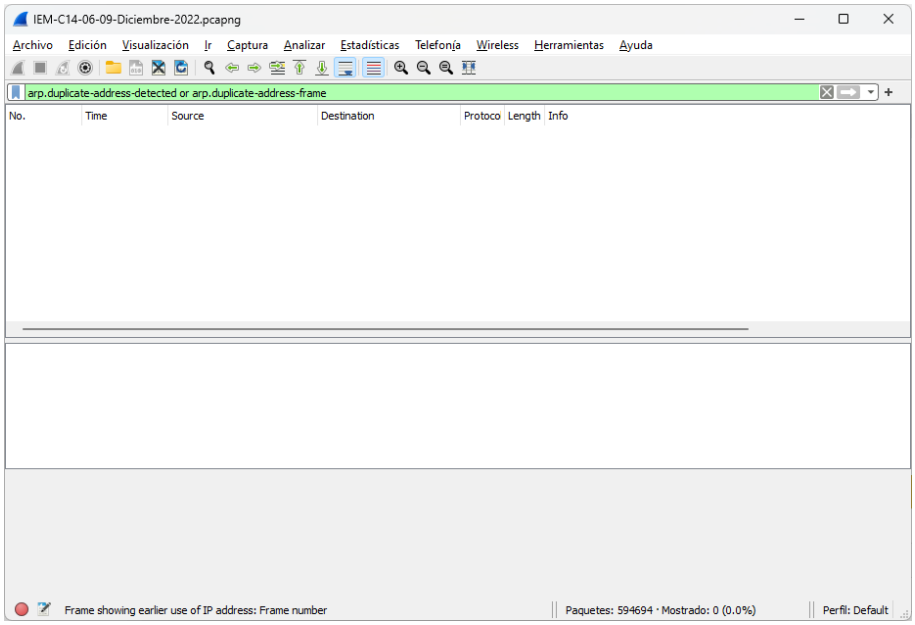


Figura 5.57: Posible suplantación ARP.

Con base a la Figura 5.56 existen varios paquetes que pertenecen al protocolo TCP y están agrupados ya sea en las secciones Advertencias, Nota y Conversaciones. Al aplicar filtros de escaneo de puertos específicamente para el protocolo TCP, la mayoría de los paquetes que muestra están relacionados con la pérdida o retransmisión. La mayoría de las amenazas encontradas son el resultado de muchos factores, no necesariamente se deben a errores de configuración o administración.

La Figura 5.58 muestra un 0.5 % de paquetes que equivalen a 2788 paquetes, es probable que esto se deba a una congestión en la red, se observa que los paquetes perdidos están relacionados con la actualización de software de seguridad de una distribución de Linux.

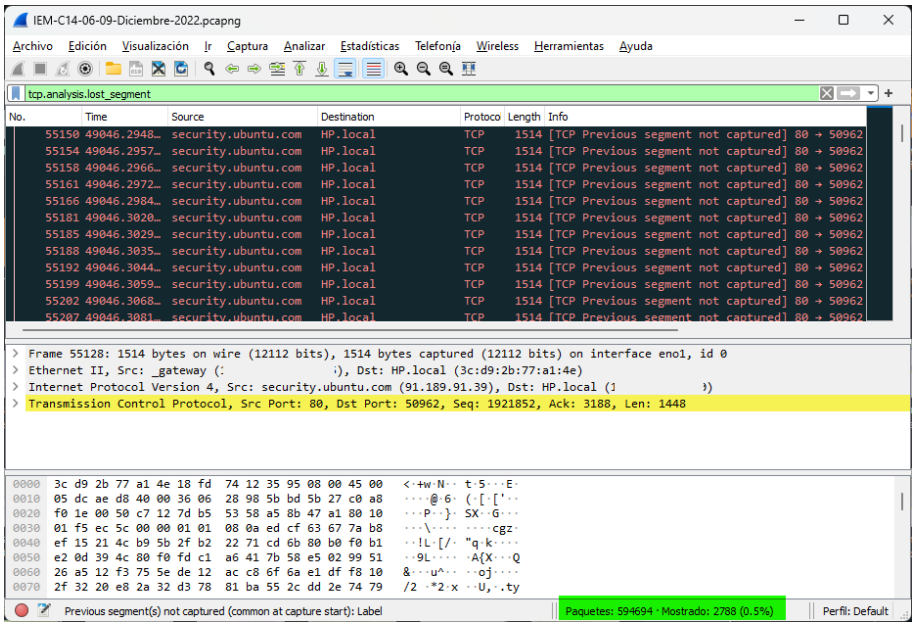


Figura 5.58: Paquetes perdidos durante la conexión TCP.

En cuanto a los paquetes retransmitidos, la Figura 5.59 muestra un 0.6 % que equivale a 3708 paquetes, es posible que la retransmisión de estos paquetes se deba a la congestión y problemas de latencia en la red, así mismo, estas retransmisiones indican posibles intentos de ataque de denegación de servicio o intrusión, en donde los atacantes intentan saturar la red mediante el envío de paquetes de retransmisión, no obstante esta premisa no es válida debido a que el número de paquetes es mínimo.

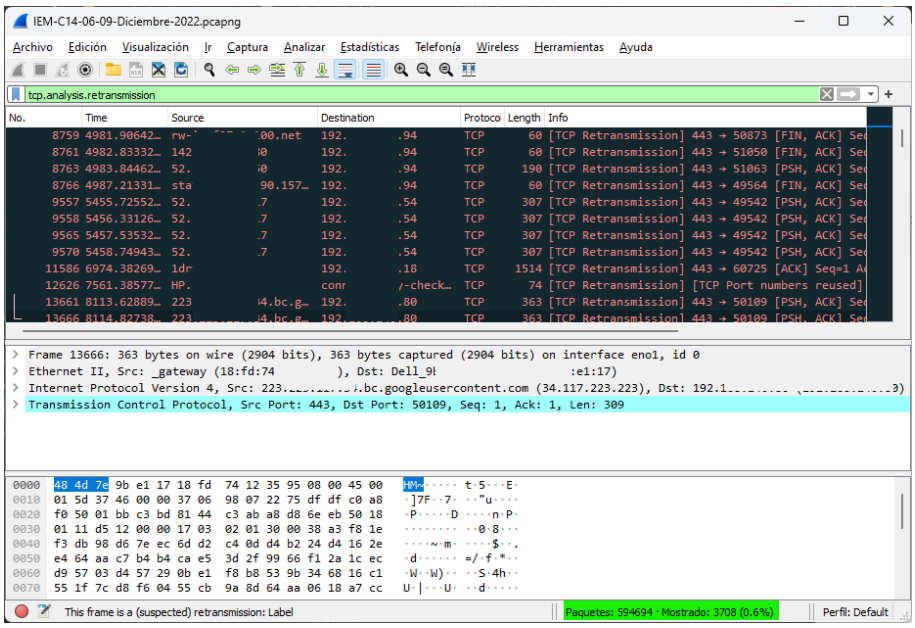


Figura 5.59: Paquetes retransmitidos durante la conexión TCP.

A continuación, la Figura 5.60 es el resultado de NetworkMiner, mostrando que se conectaron 494 huéspedes, se realizaron 4127 inicios de sesión y en la pestaña Anomalies se observa un resumen de las posibles. Convienen subrayar que las posibles suplantaciones ARP se tratan de problemas con el tráfico *broadcast*. A simple vista, este caso se clasifica como verdadero positivo

Figura 5.60: Resumen de anomalías desde NetworkMiner.

Del resumen general mostrado en la Figura 5.60, se contempla la dirección IP APIPA que tiene que ver con la configuración inapropiada del servidor DHCP. En la Figura 5.61 se percibe que la dirección APIPA se asignó a *broadcast*. Por lo tanto, este caso se clasifica como falso positivo.

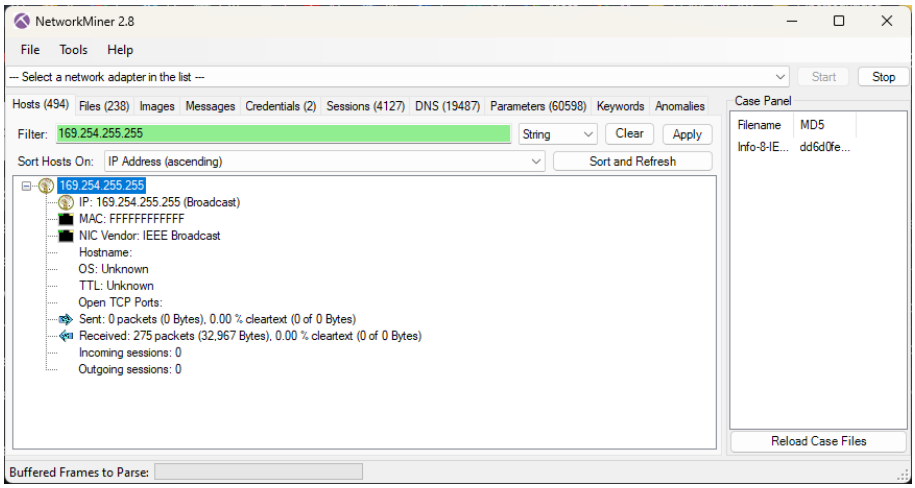


Figura 5.61: Dirección IP APIPA relacionada con el servidor DHCP.

En la pestaña *Parameters* donde se muestran que existen 60536 datos, es necesario revisar detalladamente las direcciones IP destino debido a que las computadoras cuando no están siendo utilizadas por el usuario (acceso a Internet) se enlazan a diferentes servidores, en la mayoría de los casos ocurre para actualizar el sistema operativo.

Para un análisis minucioso, es necesario apoyarse de herramientas como geolocalizadores[3] de IP.

Al analizar el huésped destino se observó una dirección IP en particular a la cual diferentes huéspedes del IEM accedían (véase Figura 5.62).

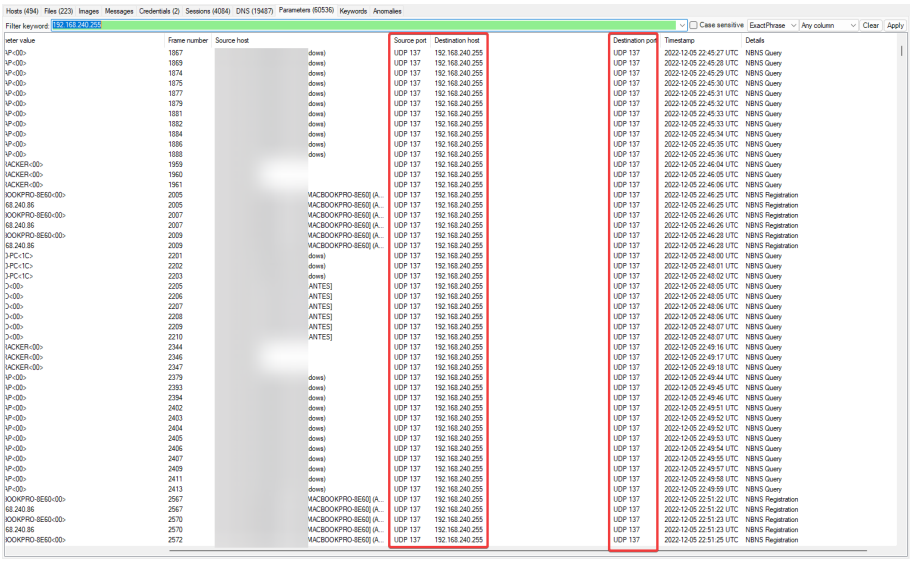


Figura 5.62: Direcciones IP bogon.

Al buscar la dirección IP en un programa de geolocalización arrojó lo que se muestra en la Figura 5.63.

[3]Estos sirven para conocer la dirección IP de un DNS, el país de ubicación, latitud, longitud y zona horaria, entre otros datos.

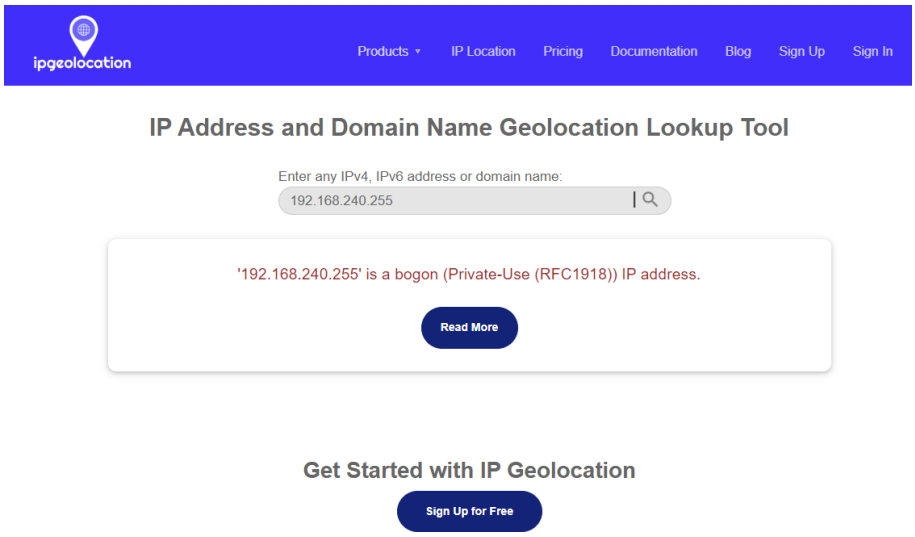


Figura 5.63: Herramienta que define a una dirección IP como bogon.

Una dirección IP bogon es una dirección IP que no se puede utilizar en una red privada o pública, ya que se encuentra en una serie de bloques de direcciones IP que no han sido asignados o reservados para su uso en Internet. Por lo tanto, cualquier tráfico que se origine o se dirija a una dirección IP bogon se considera sospechoso o no válido y puede ser bloqueado o filtrado por los dispositivos de seguridad de la red.

Es posible que exista una dirección IP falsa como resultado de una configuración incorrecta (ya sea intencional o no) que engaña al destinatario acerca de la dirección IP legítima del remitente. Las direcciones IP bogon son populares en piratería o actividades maliciosas y son utilizadas para iniciar ataques distribuidos de denegación de servicio. Como tal, muchos proveedores de servicios de Internet y cortafuegos bloquean las direcciones bogon [58]. Se observa en la Figura 5.62 que utiliza el puerto 137 de UDP. Dicho lo anterior, en la pestaña de huéspedes se filtró la dirección bogon (véase Figura 5.64).

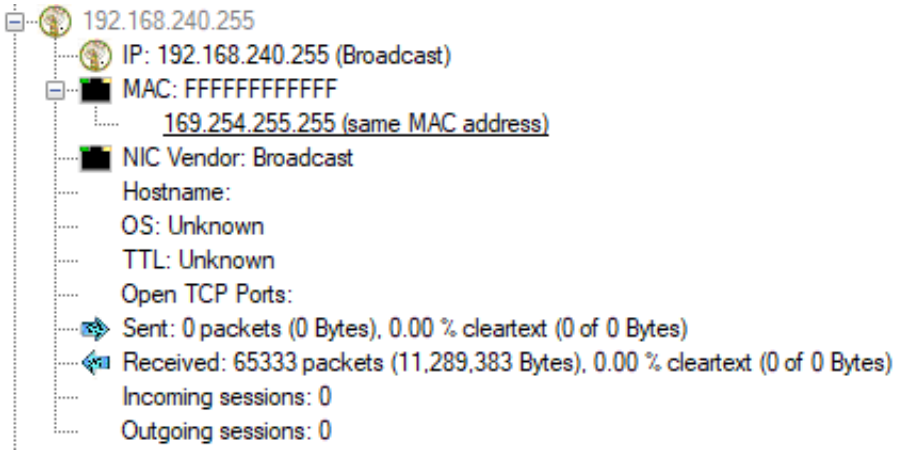


Figura 5.64: Dirección APIPA y tráfico *broadcast*.

5.4. Estadísticas de la red

Existen otras amenazas que son detectadas utilizando diferentes funciones de Wireshark. Si bien estas amenazas no presentan un riesgo para la información de una LAN

universitaria, si afectan su rendimiento. A continuación, se describe la latencia y el *broadcast*, los cuales son características que permite ver estadísticamente el estado de la red.

5.4.1. Latencia

Latencia es el término que se refiere al tiempo que tarda en pasar la información de un punto a otro. Esto se puede determinar de manera gráfica utilizando la gráfica tiempo de ida y vuelta (RTT, *Round Trip Time*). El RTT es la duración en la que se recibe el ACK de un paquete enviado, es decir, por cada paquete enviado desde un huésped, se recibe un ACK que determina el éxito de la entrega del paquete. El tiempo total que se consume desde la transferencia del paquete hasta el ACK del mismo se denomina tiempo de ida y vuelta [59].

Para observar el RTT es necesario seguir los siguientes pasos:

- En el archivo de captura, aplicar el filtro `tcp.stream eq 0`.
- Ir a la pestaña Estadísticas, luego Gráficas de E/S.
- Automáticamente se muestra la gráfica del filtro aplicado.
- En la configuración de esta gráfica, en la columna Y Axis se selecciona la opción AVG (Y field).
- En la columna Y field se agrega el filtro `frame.time_delta`.
- En la interfaz de Wireshark, en la pestaña Estadísticas en la opción Gráficas de Flujo TCP se selecciona Round Trip Time.

5.4.2. *Broadcast*

Para visualizar de manera gráfica en Wireshark el tráfico *broadcast* que se generó durante la captura de paquetes en los diferentes archivos, se siguen los siguientes pasos:

1. Ir a la pestaña Estadísticas.
2. Luego seleccionar la herramienta Gráficas de E/S.
3. Crear una nueva gráfica.
4. Aplicar el filtro `eth.dst==ff:ff:ff:ff:ff:ff` a la gráfica creada.

Con los pasos mencionados, se obtiene la gráfica del tráfico *broadcast* generado por los archivos de captura tanto de la UTM como de la universidad de la capital del estado.

Se debe agregar el filtro `arp.opcode == 1` para visualizar gráficamente peticiones ARP con el fin de demostrar que el tráfico *broadcast* muestra un patrón fijo en los archivos de captura, es decir, que cada determinado tiempo que hay tráfico se presenta una ráfaga de peticiones ARP.

Así mismo se utiliza la función Conversaciones, dirigiéndose a la pestaña de Estadísticas luego Conversaciones. Esta función muestra información de todos los huéspedes que se conectaron a la red, el número de paquetes que se transmitió así como el número de bytes. Se utilizó debido a que muestra los equipos en la red que generaron excesivo tráfico *broadcast*.

5.4.3. Análisis de *Broadcast*

Las figuras que se muestran a continuación pertenecen a los archivos de la Tabla 5.1 y muestran las conversaciones generadas entre diferentes dispositivos así como el número de paquetes que compartieron y el tamaño en bytes. Así mismo, se observan diferentes gráficas que corresponden al tráfico *broadcast* y peticiones ARP generado por distintos dispositivos en la red de la UTM.

Para comenzar el análisis, en la Figura 5.65 se observan las estadísticas que presentó la función Conversaciones de Wireshark con el fin visualizar qué dispositivo en la red generó más tráfico *broadcast*, número de paquetes y tamaño en bytes.

En el caso de la Figura 5.66 se observan dos tipos de gráficas; la primera pertenece al tráfico *broadcast* (color rojo) y la segunda se trata de peticiones ARP (puntos de color verde), en particular se observa que existe un patrón fijo que sobrepasa los 20 000 paquetes por segundo y ocurre cada 60 minutos durante seis horas, sin embargo, otro impulso que resulta constante es el que alcanza a generar 15 000 paquetes con intervalos de 60 minutos durante dos horas. A partir de las 02:00 p.m. el tráfico *broadcast* y las peticiones ARP comienzan a disminuir. Así, a las 03:00 p.m. tanto el tráfico broadcast como las peticiones ARP vuelven a incrementarse. Por otra parte, se observa que las peticiones ARP generan menor número de paquetes comparado con el tráfico *broadcast*.

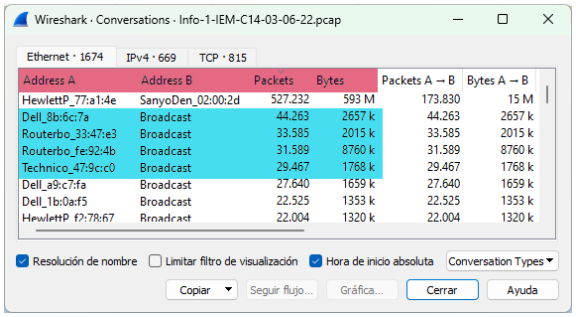


Figura 5.65: Datos estadísticos de los dispositivos que generaron mayor tráfico *broadcast* y número de paquetes.

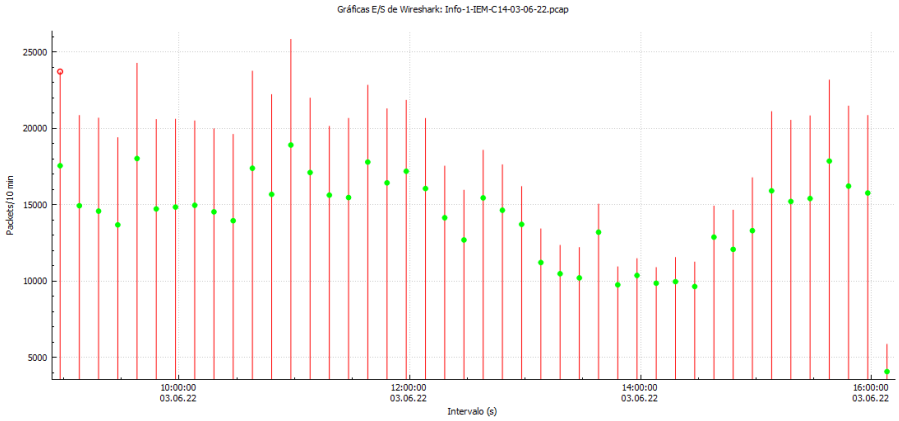


Figura 5.66: Gráfica en donde las peticiones ARP generan menor número de paquetes que el tráfico *broadcast*.

La Figura 5.67 muestra los datos estadísticos de los dispositivos que generaron más tráfico *broadcast* así como el número de paquetes y el número de bytes, en este archivo es posible que se traten de conmutadores y enrutadores quienes generaron mayor tráfico.

En el caso de la Figura 5.68 se observan dos tipos de gráficas, la de color rojo muestra los impulsos generados por el tráfico *broadcast* mientras que los puntos verdes representan las peticiones ARP. Nótese que no todo el tráfico *broadcast* es generado por las peticiones ARP. Así mismo, se observa que el archivo se guardó durante tres días, por tal motivo a lo largo del primer día 18 000 paquetes por un lapso de cinco horas, a partir de las 01:30 p.m. el tráfico disminuyó y volvió a incrementar a partir de las 03:20 p.m, se mantuvo estable durante dos horas; a partir de las 06:00 pm disminuyó. En el segundo día, el tráfico *broadcast* inició a las 07:30 a.m. y registró un incremento demasiado alto generando 38 000 paquetes por diez minutos, posterior a este incremento se presentaron variaciones sobrepasando los 14 000 paquetes por diez minutos, a partir de las 01:00 p.m. disminuyó el tráfico y las 03:20 p.m. se reanudó el incremento de paquetes hasta las 06:00 p.m. en donde el tráfico comenzó a disminuir. Finalmente, durante el último día únicamente se generaron 18 000 paquetes por diez minutos durante seis horas.

Un dato a considerar es que se generó más tráfico *broadcast* que peticiones ARP, esto representa una posible amenaza.

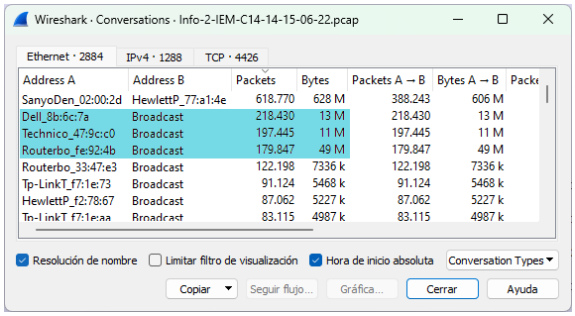


Figura 5.67: Dispositivos que generaron más tráfico *broadcast*.

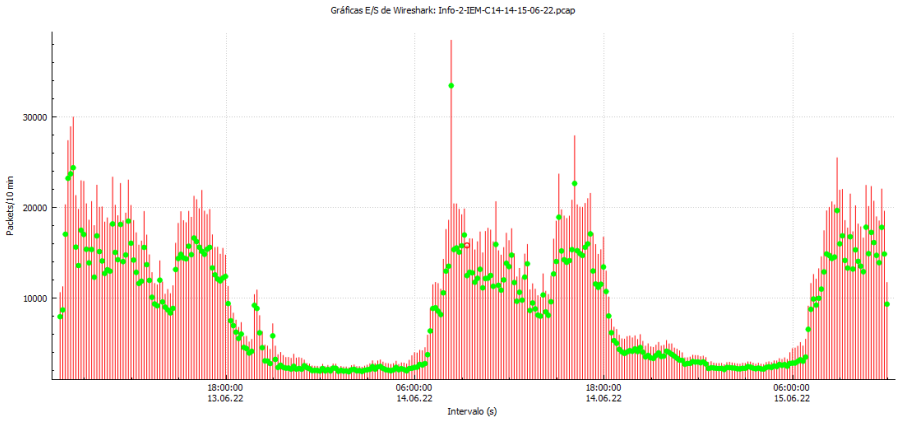


Figura 5.68: Gráfica con tráfico *broadcast* y peticiones ARP que presentan un patrón fijo.

Para continuar con el análisis de tráfico *broadcast* se debe revisar la función Conversaciones, donde se muestran datos estadísticos como el número de paquetes transmitidos y el tamaño en bytes, además clasifica a los dispositivos que generaron mayor tráfico *broadcast*. La Figura 5.69 muestra los dispositivos que generaron mayor tráfico *broadcast*; es posible que estos dispositivos sean conmutadores y/o enrutadores.

Considerando ahora la Figura 5.70 se observan dos gráficas; la primera se trata del tráfico *broadcast* (impulsos de color rojo) y la segunda pertenece a las peticiones ARP (puntos de color verde). Se visualizan dos impulsos más altos que alcanzan los 16 paquetes corresponde a 16 paquetes por 20 ms. El patrón fijo constante que se observa pertenece

a las peticiones ARP y el tráfico *broadcast* que durante toda la captura generaron un paquete por 20 ms; posteriormente, el número de paquete aumentó a dos paquetes por 20 ms, sin embargo, al estar generando tres paquetes por 20 ms comenzaron a surgir iteraciones y dejo de ser constante. A pesar de que se trata de un archivo que capturó paquetes durante tres días, la información generado no fue suficiente para mostrar una gráfica más modesta. Se debe destacar que la captura se realizó durante un fin de semana y por tal motivo el número de paquetes de tráfico *broadcast* y peticiones ARP es extremadamente bajo.

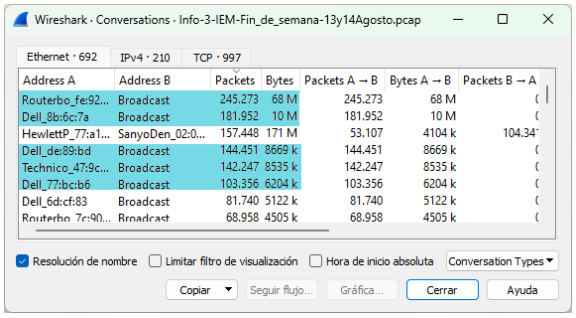


Figura 5.69: Dispositivos con mayor tráfico *broadcast*.

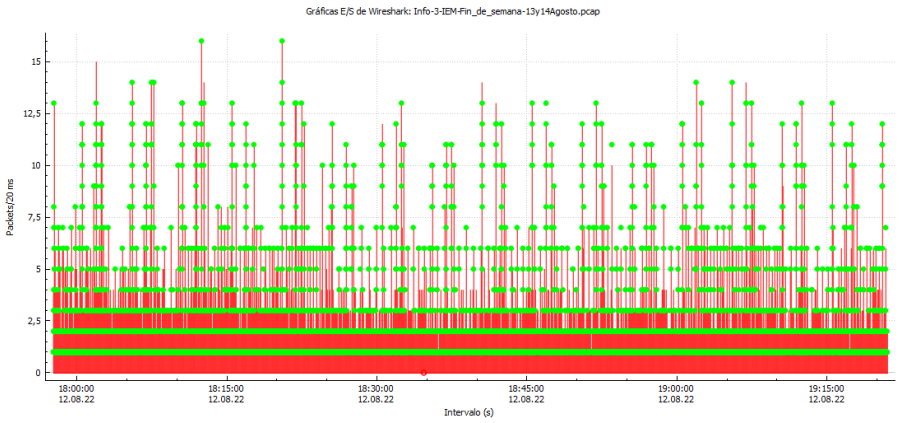


Figura 5.70: Gráfica de fin de semana donde el número de paquetes de tráfico *broadcast* y peticiones ARP es extremadamente bajo.

En el caso particular del ataque DDoS tipo inundación MAC que se logró capturar con la herramienta Wireshark, por las razones mencionadas anteriormente no fue posible analizarlo detalladamente y para este caso no se logró ejecutar la función Conversaciones que muestra de manera detallada las estadísticas de los dispositivos que generaron demasiado tráfico *broadcast*.

Dicho lo anterior, sí fue posible visualizar gráficamente el comportamiento del tráfico *broadcast* así como las peticiones ARP, esto se observa en la Figura 5.71. Aunque este ataque ocurrió durante 18 minutos lo que se inhabilitó fue la CAM del conmutador realizando peticiones con direcciones MAC falsas. El número de paquetes más grande que genera en diez segundos es de 850, posteriormente presenta un impulso de 750 paquetes por diez minutos y finalmente un impulso de 550 paquetes por diez segundos. Se puede notar que se generó más tráfico *broadcast* que peticiones ARP y que en los impulsos de tráfico *broadcast* más altos no se detectaron peticiones ARP.

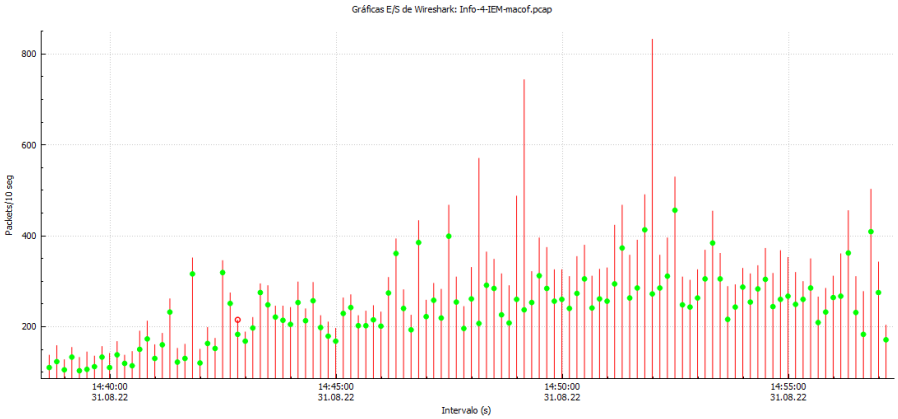


Figura 5.71: Ataque de inundación MAC con tráfico *broadcast* y peticiones ARP.

En el caso de la Figura 5.72, esta muestra datos estadísticos de los dispositivos que generaron mayor tráfico *broadcast*, así como el número de paquetes y el tamaño en bytes, por la resolución del nombre que presentan los dispositivos es probable que se trate de conmutadores y/o enrutadores.

Para iniciar el análisis de la Figura 5.73 se visualizan dos gráficas, la de color rojo pertenece al tráfico *broadcast* y la de color verde trata las peticiones ARP. A simple vista se nota que existe un patrón fijo que duró 11 horas. En el primer bloque se observa que los paquetes generados por tráfico *broadcast* alcanzan los 16 000 paquetes durante diez minutos, después de las 06:00 p.m. el tráfico disminuyó y se mantuvo con pequeñas variaciones entre 4 000 y 4 500 paquetes por 10 minutos. A partir de las 07:00 a.m. del día siguiente comenzó a incrementar el tráfico llegando al punto más alto con 20 000 paquetes por diez minutos. A las 02:00 p.m se presentó un descenso llegando a 10 000 paquetes por diez minutos, a partir de las 03:00 p.m comenzó a incrementar el número de paquetes en su mayoría por tráfico *broadcast*. Finalmente a las 06:00 p.m. el tráfico disminuyó hasta los 3 000 paquetes. Este patrón se visualiza al siguiente día con pequeñas variaciones en los paquetes. Se debe hacer notar que para este archivo existió más tráfico *broadcast* que peticiones ARP.

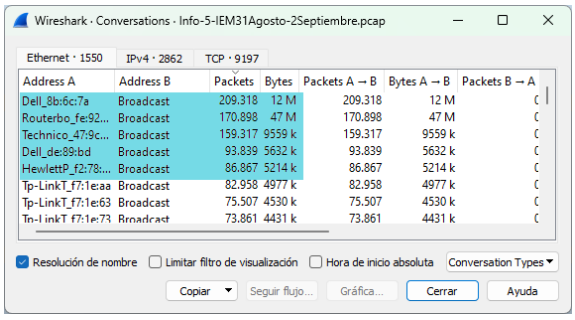


Figura 5.72: Datos estadísticos de los dispositivos con elevado número de paquetes y mayor tráfico *broadcast*.

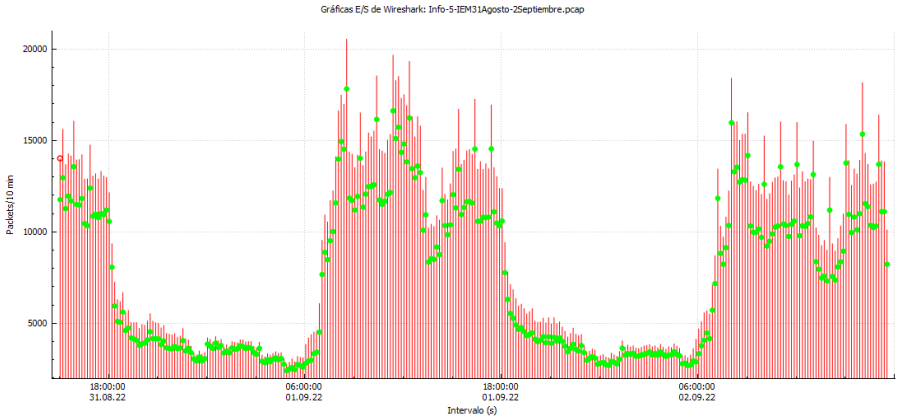


Figura 5.73: Gráfica con tráfico *broadcast* y peticiones ARP mostrando un patrón con pequeñas variaciones.

La Figura 5.74 muestra datos estadísticos de los dispositivos que generaron mayor tráfico dentro de la red, por la resolución de nombres se cree que dos dispositivos son conmutadores y uno de ellos es un enrutador. Así mismo, se observa el número de bytes que generaron por el tráfico *broadcast* de igual modo se visualiza el número de paquetes difundidos.

En el caso de la Figura 5.75 se observa que generó tráfico *broadcast* en menor cantidad comparado con otros archivos, esto se deduce debido a que el impulso más alto llegó a 2 600 paquetes por diez minutos. Por otro lado, las peticiones ARP variaron durante las primeras siete horas, después se mantuvieron constante a partir de las 10:00 p.m., también se visualiza que el número de tráfico *broadcast* durante las primeras siete horas es mayor que las peticiones ARP.

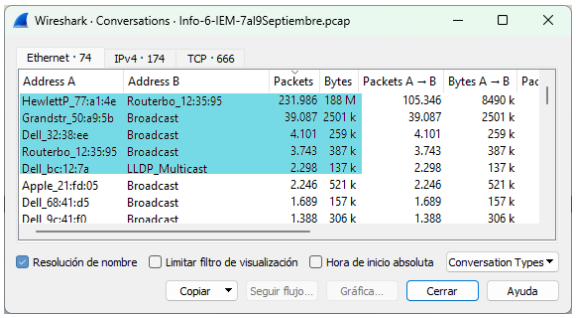


Figura 5.74: Dispositivos que generaron mayor número de paquetes y tráfico *broadcast*.

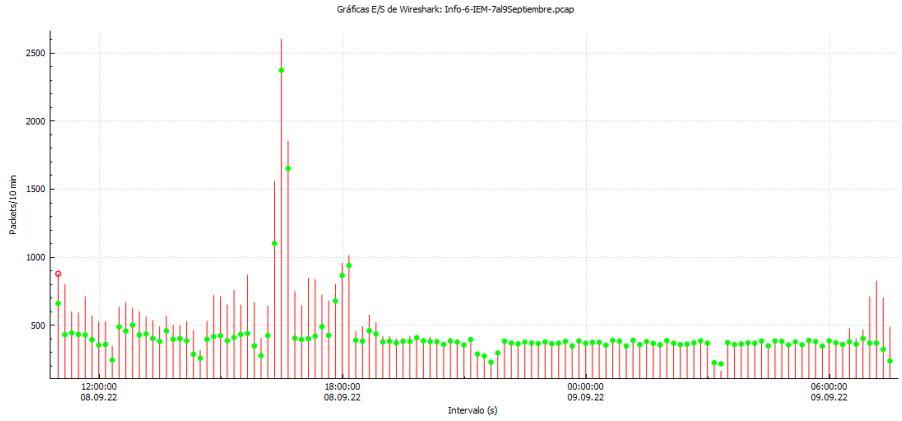


Figura 5.75: Gráfica del tráfico *broadcast* con peticiones ARP constantes.

Por lo que se refiere a la Figura 5.76, esta muestra datos estadísticos de los cinco dispositivos que generaron excesivo tráfico *broadcast*, de igual manera el número de paquetes y el tamaño en bytes. Por la resolución de nombre, se tratan de dos conmutadores y el resto se desconoce el tipo de dispositivo.

Considerando la Figura 5.77 se visualiza gráficamente el comportamiento del tráfico *broadcast* (impulsos de color rojo) y de las peticiones ARP (puntos de color verde). En particular, se observa que las peticiones ARP son constantes llegando a 10 000 paquetes por diez minutos durante nueve horas, se observa que el tráfico *broadcast* presenta varias iteraciones en donde el impulso con el mayor número de paquetes llega a 2 600 paquetes por diez minutos mientras que en ese mismo el impulso la petición ARP alcanza 1 400 paquetes por diez minutos.

A grandes rasgos, se observa que el tráfico *broadcast* fue excesivamente alto.

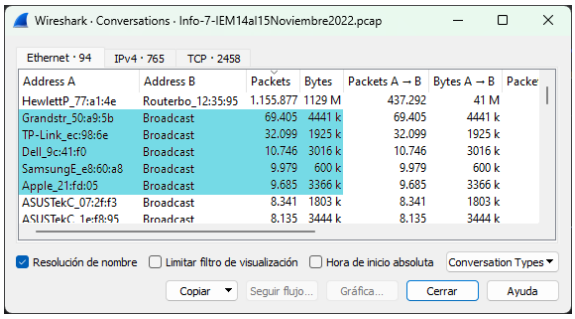


Figura 5.76: Conversaciones entre dispositivos con mayor número de tráfico *broadcast*.

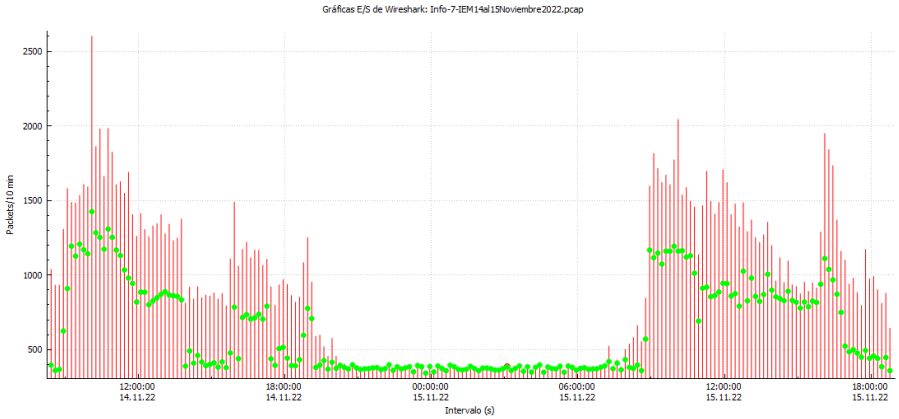


Figura 5.77: Gráfica con excesivo tráfico *broadcast* y con peticiones ARP constantes y variables.

La Figura 5.78 muestra los dispositivos que generaron más tráfico *broadcast*, de igual modo el número de paquetes y el tamaño en bytes. Por la resolución de nombre se considera que dos dispositivos son conmutadores y el resto se desconoce el tipo de dispositivo.

Respecto al análisis gráfico del tráfico *broadcast* (impulsos de color rojo) y las peticiones ARP (puntos de color verde) mostrado en la Figura 5.79, a simple vista se visualiza que las peticiones ARP se mantienen constantes durante las horas inactivas de la red (07:00 p.m a 08:00 a.m.), sin embargo, cuando el tráfico *broadcast* genera los impulsos superando los 1 500 paquetes por diez minutos las peticiones ARP algunas apenas superan los 600 paquetes por diez minutos. Aunado a esto, el archivo capturó paquetes durante cuatro días, esto permite que se visualice un patrón en el horario laboral, de receso e inactivo.

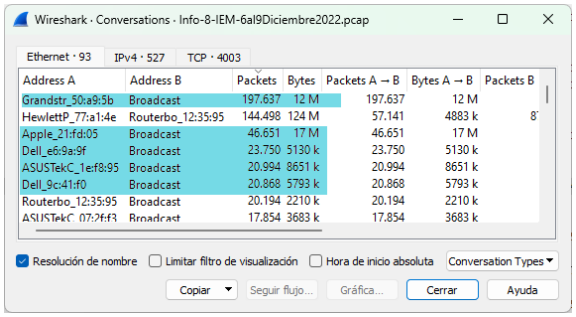


Figura 5.78: Dispositivos con mayor tráfico *broadcast*.

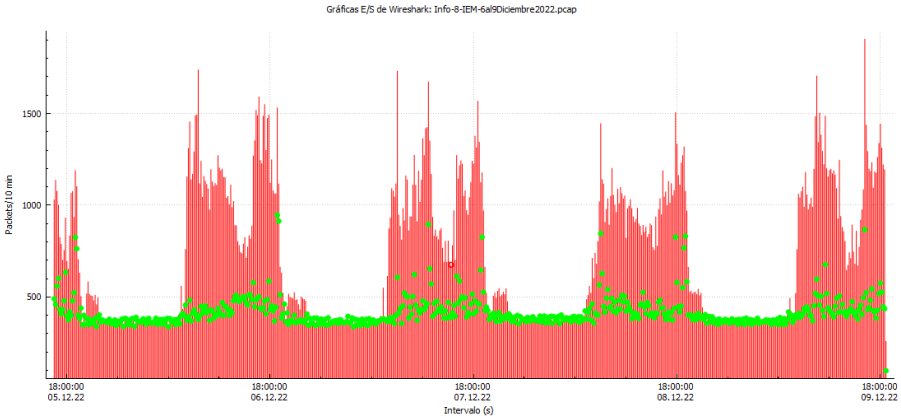


Figura 5.79: Gráfica con mayor tráfico *broadcast* y peticiones ARP constantes mostrando un patrón en el horario laboral, de receso e inactivo.

5.5. Casos Especiales

A continuación se describen dos casos especiales que ilustran las diversas vulnerabilidades que existen en la red de la UTM.

El primero de ellos consiste en la identificación completa de las diferentes subredes asociadas a una dirección IP. Algunas de estas subredes están vinculadas a departamentos que manejan información sensible, como bases de datos de profesores, alumnos y datos bancarios. Por esta razón, se convierten en un punto crítico para posibles ataques y accesos no autorizados a dicha información.

En el segundo caso, se trata de una captura de paquetes utilizando Wireshark en donde se muestra el nombre de usuario y contraseña de un profesor para acceder a la plataforma de NES UTM, donde se albergan los datos académicos de los alumnos. Si esta información llegara a manos de terceros no autorizados, podría causar un daño significativo y afectar gravemente la reputación de la universidad.

Para el primer caso, mediante un escaneo utilizando la herramienta *ping* se logró crear un mapa (véase Figura 5.80) y obtener la dirección IP de algunos departamentos de la universidad.

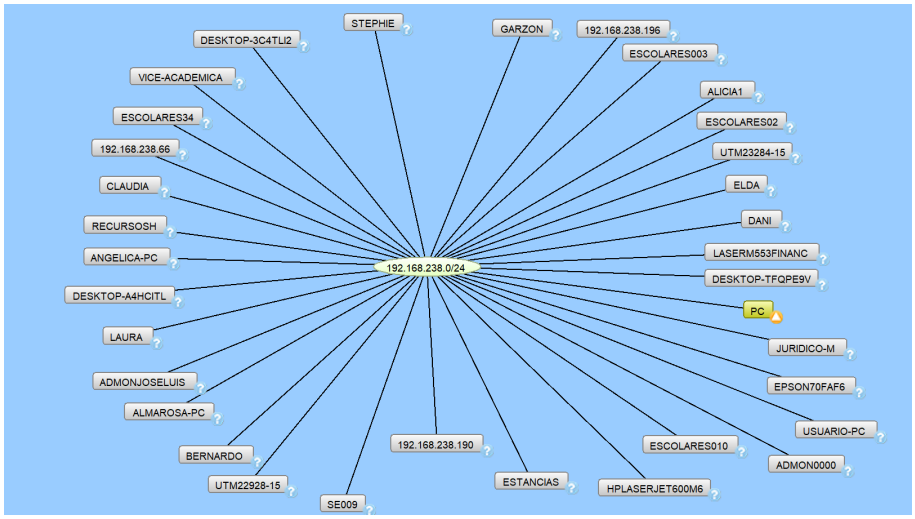


Figura 5.80: Mapeo de direcciones IP asignadas a distintos departamentos de la UTM generado mediante la herramienta *ping*.

En dicha figura se observa que los equipos de la UTM no están configurados para repeler solicitudes *ping* o en su defecto los equipos conectados a la red no tienen configurado un nombre adecuado para mantener la privacidad de los diferentes departamentos de la UTM. Es necesario que se apliquen medidas de seguridad para proteger la identidad de los usuarios debido a que se tienen datos privados de alumnos, profesores y a diario se realizan operaciones confidenciales y que algunas direcciones IP tienen nombre de los departamentos al que pertenecen (RECURSOSH, ESCOLARES34, VICE-ACADEMICA, ESCOLARES003, UTM23284-15 y ESTANCIAS).

El segundo caso tiene que ver con la Figura 5.81 en donde se observa la contraseña y el usuario de la plataforma para asignar calificaciones NES-UTM la cual pertenece a un profesor. Se observa que en el apartado de "`user_session[login]`", el usuario se muestra en texto, el cual es "`ocetxim`". En el apartado de contraseña "`user_session[password]`", el campo se visualiza sin encriptar. Para preservar la confidencialidad y seguridad de la información, se ha ocultado la contraseña en la Figura 5.81, únicamente se pueden apreciar los caracteres "`k0l`". Adicionalmente se muestran otros datos sensibles que son punto de partida para iniciar un ataque. La causa del presente error radica en que los certificados de seguridad, tales como el TLS, no han sido actualizados a la versión más reciente, la 1.3.

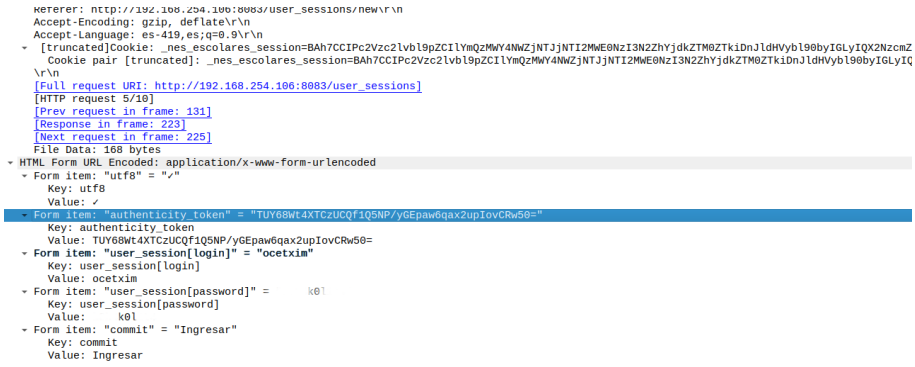


Figura 5.81: Usuario y contraseña mostrada en texto plano para acceder a la plataforma NES-UTM.

Capítulo 6

Recomendaciones

En las redes de computadoras, la seguridad es un aspecto crucial para garantizar la integridad y confidencialidad de la información y de los nodos. A medida que las tecnologías avanzan y las comunicaciones se vuelven más interconectadas, también aumenta la exposición a diversas amenazas y vulnerabilidades.

En el desarrollo de este documento se observaron diferentes amenazas en LANs universitarias, por lo que es necesario que los administradores de red ejecuten programas de monitoreo y escaneo para revisar la situación actual de la red, así mismo, es necesario implementar medidas de seguridad para aplicarlos en dispositivos como conmutadores para repeler cualquier ataque DDoS.

La segmentación de la red es un método infalible con el fin de que el funcionamiento y rendimiento de la red sea altamente eficaz, ante esto es recomendable utilizar redes virtuales (VLANs). Algunos servidores de la UTM no tienen configurado el protocolo TLS, esto significa que cualquier malhechor o curioso puede capturar paquetes y así encontrar direcciones IP de los servidores o incluso de los usuarios que estén conectados a la red.

Otro aspecto a considerar para proteger los equipos de una LAN es configurar adecuadamente el nombre para cada computadora, es decir no asignar nombres de institutos o profesores a las computadoras, cerrar puertos innecesarios. También es recomendable que se configure el nombre de los conmutadores, algunos de los que se encuentran en la UTM es muy fácilmente verlos con Wireshark, se considera necesario diseñar una metodología que se aplique a cada equipo nuevo o formateado para que los encargados del departamento de red o el usuario configure los puertos estrictamente necesarios.

¿Por qué es necesario cambiar el nombre del conmutador? Porque al ser visible la información, los atacantes pueden buscar en la web las características técnicas o posibles *exploits* para infringir la seguridad de los dispositivos.

En este capítulo, se explican algunas recomendaciones para evitar ataques MitM y DDoS las cuales se basan en el libro *The CISO'S next frontier: AI, post-quantum cryptography and advanced security paradigms* [60], así mismo, se explican algunas recomendaciones para mejorar de rendimiento de la red. Es necesario implementar las recomendaciones mencionadas para que la LAN funcione de manera adecuada y se eviten diferentes amenazas que ante cualquier fallo de la red pueden convertirse en ataques de gran importancia afectando la información privada de muchos usuarios.

6.1. Hombre en el Medio

El MitM ocurre cuando un atacante intercepta una conexión cifrada y encriptada entre un cliente y servidor.

6.1.1. Esquemas de protección

- Autenticación mutua: Teóricamente, esta técnica permite que el cliente y el servidor validen y confíen en los certificados antes de que se establezca la conexión SSL/TLS. Sin embargo, la necesidad de revocar y renovar certificados aumenta la complejidad. El proceso de autenticación mutua se describe a continuación:
  - El cliente solicita una conexión cifrada con el servidor y comparte una lista de cifrados criptográficos que puede utilizar para proteger el tráfico.
  - El servidor responde con su lista de cifrados criptográficos que acepta.
  - Se establece un acuerdo entre el cliente y servidor para utilizar una conexión cifrada.
  - El servidor envía su certificado digital y clave pública al cliente, así mismo solicita el certificado del cliente, a lo que este accede.
  - Se verifican los certificados entre el cliente y el servidor, también intercambian claves para negociar un código compartido que se utilizará para cifrar y descifrar el tráfico. Se gestiona uno para cada sesión.
- Asignación de certificados: Esta técnica permite al cliente detectar ataques MitM. Existen dos tipos de asignación de certificados: Asignación de certificados al cliente y Asignación de certificados al servidor.
  - Asignación de certificados al cliente: Implica la emisión de certificados únicos que deben vincularse a cada cliente con una clave privada única correspondiente. Durante la verificación del certificado por parte del servidor, el cliente debe presentar el certificado vinculado o, de lo contrario, el servidor rechazará la conexión. Este enfoque es similar al de la asignación de certificados al servidor, los múltiples pasos que deben dar tanto el cliente como el servidor lo hacen más difícil de aplicar. La necesidad de revocar o enviar un certificado (al cliente) aumenta la complejidad.
  - Asignación de certificados al servidor: Permite al cliente conocer con precisión qué certificado de servidor se necesita exclusivamente para establecer una conexión segura. Aunque el servidor presente un certificado con una cadena de confianza y un nombre de huésped verificables, el cliente rechaza la conexión si no coincide con el certificado de servidor específico que se espera (generalmente, identificado por una clave pública del certificado). De esta manera, todos los clientes que se conecten a un dominio específico pueden utilizar el mismo certificado de servidor.
- Asignación de claves públicas HTTP: El HPKP (*HTTP Public Key Pinning*) ha quedado obsoleto, sin embargo, es bueno referenciarlo para entender la razón por la que fue implementado. El objetivo principal de esta técnica era implementar una clave pseudo-pública en los navegadores (buscadores web) para proporcionar protección contra el uso de certificados fraudulentos o el compromiso de los certificados de la autoridad que emite los certificados de servidor para una determinada aplicación web. En términos sencillos, el servidor enviaba a un cliente un certificado de clave pública que aparecía en la cadena de certificados de futuras conexiones para el mismo nombre de dominio, a través de una cabecera HTTP. El cliente almacenaba la clave en su caché. Posteriormente, si el cliente visitaba el mismo sitio web y el servidor proporciona una clave pública diferente a la obtenida previamente por HPKP, entonces se alertaba al usuario sobre la posibilidad de un ataque MitM. Se descubrió

que la técnica corría el riesgo de verse comprometida si el primer certificado de la clave fuera fraudulenta, o si un atacante realizara un ataque MitM sobre el primer certificado de la clave pública enviado por el servidor, utilizándolo así para enviar al cliente a un dominio fraudulento. HPKP ha sido sustituido por el certificado de transparencia (*Certificate Transparency*).

- Detección de degradación de TLS: Los ataques MitM se vuelven mucho más difíciles de llevar a cabo con TLS 1.3, por lo que los actores de amenazas intentan evitar este problema degradando la conexión TLS 1.3 a TLS 1.2. Los diseñadores del protocolo previeron este problema y han proporcionado un marcador de degradación dentro del propio protocolo. Cuando un cliente (o servidor) TLS 1.3 ve este marcador, debe abortar inmediatamente la conexión *(handshake)*.

6.2. DoS y DDoS

Con base a los ataques encontrados en los archivos de captura en las dos LANs universitarias, se observa que DoS comúnmente ataca a los protocolos que se encuentran en las capas siete y tres del modelo de referencia OSI. Ante esta situación y los resultados encontrados, para prevenir el DoS y DDoS se recomienda utilizar las siguiente técnicas de prevención.

- Depuración de Tráfico (*Traffic Scrubbing*): Permite detectar y depurar paquetes de datos (generalmente UDP o TCP) maliciosos. Por lo general, un proveedor externo se encarga de este servicio, que puede funcionar en dos modos:
  - Modo de monitoreo: Tiene la capacidad para detectar y activar manualmente la depuración de tráfico. El inicio manual del depurado de tráfico puede llevar al menos 15 a 45 minutos. Esta técnica sigue siendo la opción más extendida y requiere mucha intervención manual y coordinación entre los equipos de seguridad de la red local y el proveedor de servicios de depuración. Esta capacidad la suelen ofrecer los proveedores comerciales de servicios o circuitos de Internet como servicio adicional, sin embargo, ya no es muy eficaz, dada la gran cantidad de daños que pueden causar los ataques sofisticados en muy poco tiempo, lo que exige una respuesta proactiva y sostenida en tiempo real. Pueden producirse retrasos adicionales si el equipo de seguridad de la red no tiene derechos para realizar cambios en el enrutamiento de la red.
  - Modo activo: Tiene la capacidad para detectar y depurar dinámicamente el tráfico con un retraso y unos problemas de rendimiento mínimos. Esta es la mejor opción de implementación posible en la actualidad para medianas y grandes empresas con aplicaciones críticas de alto riesgo orientadas a Internet. Proporciona detección y protección casi en tiempo real frente a ataques DDoS grandes y pequeños o equivalentes. Se sabe que esta técnica proporciona protección contra algunos ataques muy grandes (mayores a 1 Tbps).
- Cortafuegos (*Firewalls*): Una generación siguiente de cortafuegos es una llave perimetral activada que tiene la capacidad para bloquear paquetes de datos maliciosos y forma la primera línea de defensa para ataques DDoS. Los cortafuegos son capaces de bloquear pequeños ataques DDoS pero no debería ser utilizado para ataques grandes y de periodos prolongados.
- Limitación (*Throttling*): Esta técnica limita el número de solicitudes que un servidor puede manejar, limitándolas a medida que el volumen aumenta por encima de un

límite configurado. Utilizando esta técnica se puede reducir la velocidad de un ataque para proporcionar cierta mitigación táctica, pero no puede utilizarse como solución estratégica, ya que también afectaría a la conexión entrante de usuarios auténticos.

- Cortafuegos de sitios web: Un cortafuegos para sitios web debe tener una capacidad inherente para proveer protección rudimentaria contra inundaciones TCP o HTTP, pero no puede proporcionar protección contra grandes ataques DDoS. Para que un cortafuegos de sitios web pueda bloquear un ataque, tiene que estar configurado en modo de aplicación y no en el modo de supervisión más habitual.
- Alta Disponibilidad y Recuperación ante Desastres: La mejor práctica consiste en asegurar que todos los sistemas de alto riesgo conectados a Internet cuenten con alta disponibilidad local y recuperación ante desastres en línea remota. Esto tiene como objetivo mitigar los ataques de denegación de servicio distribuido (DDoS) en un sitio o ubicación específica. Esta medida proporcionaría la capacidad de ofrecer redundancia a nivel local o de sitio, lo cual es esencial para garantizar la continuidad del negocio en caso de pérdida de un centro de datos principal o sitio debido a un evento de red catastrófico causado por un ataque DDoS.

6.3. Mejoras de Rendimiento

Una de las recomendaciones importantes para un buen rendimiento en la red es la segmentación, que sirve para garantizar una mayor seguridad y contener amenazas así como para evitar la propagación de las mismas dentro de la red. Esto surge por los puntos de acceso no autorizados (creados desde computadoras portátiles, de escritorio e incluso teléfonos celulares), por ejemplo alumnos o profesores de las universidades utilizan Wi-Fi para realizar compras en Internet, esto representa un punto de acceso difícil de controlar y la dificultad radica en que al momento de que exista una intromisión no autorizada, la arquitectura tradicional de la red permitirá expandirse sin problema a todo el sistema; logrando así una infección total difícil de eliminar. Por esta razón, la mejor estrategia que se puede llevar a cabo es la segmentación de redes.

En cuanto al rendimiento del ancho de banda existen diferentes factores que ocasionan un ineficiente uso del ancho de banda, dentro de éstas destacan: estrategias de cableado inadecuadas, errores de software, aplicaciones mal instaladas que consumen más recursos de almacenamiento, copia de seguridad, red y gestión ineficiente de redes virtuales, entre otras. Dicho esto, para optimizar el ancho banda en una red universitaria es necesario seguir las siguientes recomendaciones:

- Recopilar datos de la red para analizarlos y saber cuánto ancho de banda consumen los usuarios y las aplicaciones. Al realizar esta actividad, los administradores de red percibirán de dónde procede y hacia dónde va el tráfico.
- El mapeo de la red es necesaria para conocer cómo están conectados los dispositivos y ver el tráfico de paquetes que circula a través de ésta. Si se presenta alguna amenaza de rendimiento, los administradores, al conocer su red, pueden re-configurar el diseño para reducir los problemas presentados.
- Crear subredes y redes virtuales con el fin de agilizar las comunicación entre los dispositivos finales, esto se logra conociendo la topología de la red.

- Utilizar los servicios de equilibrio de carga[1] y carga compartida[2] que pueden mejorar el rendimiento distribuyendo el tráfico por diferentes rutas de red.
- El establecer políticas de uso y prioridades son necesarias para tener una mejor prestación de la red, esto consiste en bloquear el acceso a los usuarios a ciertos sitios web, aplicaciones y recursos con el fin de evitar el alto consumo de ancho de banda. Así mismo, para tener un mejor control es necesario utilizar herramientas que permitan supervisar la actividad de los usuarios con el fin de proporcionar información sobre recursos que consumen demasiado ancho de banda.
- Otra recomendación importante para optimizar el ancho de banda es mantener actualizado los sistemas, mejorar constantemente los cambios en la configuración, revisar los parches de seguridad todo esto en horas que sea menos probable que los usuarios estén conectados a la red. Para optimizar esto es necesario verificar si algunos dispositivos de la red tienen la función de hacer las actualizaciones automáticamente.
- El uso de las herramientas de monitoreo permiten a los administradores de red conocer cuánto ancho de banda se está consumiendo, así mismo, se identifican las rutas que son sobrecargadas con exceso de paquetes.
- Tener un plan fiable y flexible para el futuro con el fin de migrar al uso de nuevas tecnologías como cambios de aplicaciones, migración a servidores en la nube así como actualización de sistemas operativos, servidores y hardware. Estos cambios sin duda afectan el crecimiento del tráfico de la red así como las políticas de seguridad.

6.4. Protección para el Escaneo de Puertos

El escaneado de puertos es un método muy utilizado por los atacantes con el fin de encontrar servidores vulnerables. A menudo lo utilizan para descubrir los niveles de seguridad en las organizaciones con el fin de determinar si disponen de cortafuegos eficaces y así detectar redes o servidores vulnerables.

Los atacantes realizan el escaneo para evaluar cómo reaccionan los puertos, lo que les permite conocer los niveles de seguridad del objetivo y los sistemas que despliegan.

Las organizaciones necesitan software de seguridad eficaz, herramientas de escaneo de puertos y alertas de seguridad que vigilen los puertos e impidan que los actores maliciosos lleguen a la red.

Algunos de los mecanismos más importantes contra el escaneo de puertos son [62]:

- Cortafuegos potentes: Puede impedir el acceso no autorizado a la red privada de una empresa. Controla los puertos y su visibilidad, además de detectar cuándo se está realizando un escaneado de puertos antes de cerrarlo.
- Envoltorios TCP: Permiten a los administradores tener la flexibilidad de permitir o denegar el acceso a servidores basándose en direcciones IP y nombres de dominio.
- Descubrir agujeros en la red: Las empresas pueden utilizar un verificador de puertos o un escáner de puertos para determinar si hay más puertos abiertos de los necesarios. Es necesario utilizarlo periódicamente para informar de posibles puntos débiles o vulnerabilidades que podrían ser aprovechados por un atacante.

[1] Ocurre cuando un dispositivo de red reenvía datos hacia el destino de un paquete, este proceso de reenvío incluye la capacidad de enviar los datos a través de múltiples rutas [61].

[2] Divide estáticamente el tráfico de conexión y lo envía a varios destinos de procesamiento. En la mayoría de los casos, el servicio de reparto identifica las conexiones en función de su IP de origen y destino o de su dirección MAC [61].

6.5. Protección para evitar los *pings*

Algunos administradores de red consideran que ICMP resulta una amenaza para la integridad de algunos equipos, por esta razón se bloquean los *pings* externos. Sin embargo, es necesario recalcar que aunque es útil desactivar algunas funciones de ICMP no es bueno hacerlo a todos los equipos pues su función en algunos equipos es fundamental para un funcionamiento adecuado.

6.5.1. MS Windows

Con respecto a las medidas de seguridad que se pueden habilitar en una computadora con sistema operativo MS Windows existen varias maneras de hacerlo. MS Windows tiene su propio cortafuegos, cuando está habilitado impide que otro equipo pueda detectar la computadora activa. Específicamente el cortafuegos de Windows 10 y 11, incluyen una funcionalidad de seguridad avanzada que bloquea dichas peticiones para redes públicas pero las permite para redes privadas.

Para activar el cortafuegos se siguen los siguientes pasos:

1. Acceder al menú de Panel de Control.
2. Ir a Sistema y seguridad.
3. Seleccionar *Firewall* de Windows Defender.
4. Ir a Configuración avanzada.
5. Seleccionar Reglas de entrada.
6. Buscar la regla Compartir archivos e impresoras (solicitud eco: ICMPv4 de entrada).
7. Dar clic derecho y seleccionar Deshabilitar regla.
8. Realizar lo mismo a partir del paso 6 para ICMPv6.

6.5.2. GNU/Linux

En computadoras con distribuciones Linux, por defecto la respuesta *ping* está habilitada a nivel de kernel. Para modificarlo se puede realizar a través de un cortafuegos llamado Iptables, el cual funciona para filtrar los paquetes en la red y configurar reglas que descarten los paquetes ICMP entrantes tanto IPv6 e IPv4.

6.5.3. macOS X

Con respecto al sistema operativo macOS X al igual que Windows tiene una herramienta por defecto que evita visualizar el equipo logrando no responder a los comandos *pings* ni a los intentos de conexión desde una red TCP o UDP.

Para desplegar esta herramienta, se siguen los siguientes pasos:

1. Acceder al menú Apple.
2. Configuración del Sistema.
3. Red.
4. Ir a la barra lateral y elegir *firewall*.
5. Opciones.
6. Activar modo encubierto.

Capítulo 7

Conclusiones y Líneas Futuras

El presente trabajo de tesis tuvo como objetivo detectar amenazas en los protocolos ARP, ICMP, TCP, DHCP y TLS de una LAN universitaria que pudieran afectar su funcionamiento. La detección de amenazas se realizó mediante la recopilación, identificación y análisis de paquetes utilizando las herramientas de software libre Wireshark y NetworkMiner.

Se lograron capturar paquetes del tráfico de una LAN utilizando Wireshark en dos escenarios distintos a partir de una adecuada configuración del software mencionado. Utilizando los filtros de visualización y las funciones Latencia y *Broadcast* de Wireshark se identificaron amenazas, problemas de rendimiento, inadecuada configuración de equipos de capa 2 y capa 3; posteriormente, se clasificaron los problemas detectados con base a los protocolos ARP, ICMP, TCP, DHCP y TLS. Con la función *Anomalies* de NetworkMiner se analizaron los paquetes identificados y se investigó sobre las amenazas encontradas en los paquetes. Finalmente, se propusieron recomendaciones de seguridad para proteger a los usuarios de una LAN universitaria debido a que las amenazas siempre estarán presentes.

Para realizar el análisis de los archivos capturados se utilizó equipo de cómputo de gama baja, por tal motivo algunos archivos de captura de paquetes que presentaban ataques en la red no pudieron analizarse correctamente. Es recomendable utilizar equipo de gama media o gama alta para realizar este tipo de detección de amenazas.

Es recomendable realizar capturas de paquetes directamente en la oficina de red para generar un análisis más detallado sobre la infraestructura de la red, la conexión de nodos, así como un monitoreo constante de los paquetes.

Son pocos los estudios realizados acerca de amenazas y ataques utilizando herramienta de software libre, la mayoría de organizaciones utiliza software comercial debido a que son programas robustos que presentan funciones complejas como monitoreo y detección de amenazas en tiempo real, clasificación y gravedad de ataques entre otras funciones.

7.1. Líneas Futuras de Investigación

Como líneas futuras de investigación a este documento de tesis se mencionan las siguientes:

- Ampliar el alcance del estudio para abarcar un mayor número de protocolos de red con el fin de identificar amenazas adicionales.
- Simulación de la red de la UTM utilizando simuladores como GNS3 o Packet Tracer, que permitan analizar tanto el tráfico como posibles escenarios que pongan en riesgo la red.

- Diseño y simulación de varios escenarios de segmentación de la LAN de la UTM para optimizar su desempeño.
- Desarrollo de software utilizando la librería `Scapy` del lenguaje Python para captura y filtrado de paquetes de red.
- Detección de amenazas y vulnerabilidades en una LAN universitaria utilizando Nmap y Metasploit.
- Pruebas de *pentesting* a la LAN y WLAN de la UTM.
- Implementación del algoritmo AES utilizando la tarjeta ESP32 para dispositivos IoT.
- Diseño e implementación del algoritmo SHA 256 utilizando la tarjeta FPGA para sistemas embebidos.

Bibliografía

[1] Douglas E. Comer. *Internetworking with TCP/IP Vol 1: Principles, Protocols, and Architecture*. Pearson Education, sixth edition, 2014.

[2] William Stallings. *Data and computer communications*. Pearson Education, tenth edition, 2014.

[3] Mahendra Data. The defense against arp spoofing attack using semi-static arp cache table. *2018 International Conference on Sustainable Information Engineering and Technology (SIET)*, 2018.

[4] Md Shohrab Hossain, Arnob Paul, Hasanul Hasan, and Mohammed Atiquzzaman. Survey of the protection mechanisms to the ssl-based session hijacking attacks. *Network Protocols and Algorithms*, 10, 2018.

[5] Jeewan Bhusal. Network analysis with open source packet analyzers case: Wireshark, 2016.

[6] Vivens Ndatinya, Zhifeng Xiao, Vasudeva Manepalli, Ke Meng, and Yang Xiao. Network forensics analysis using wireshark. *International Journal of Security and Networks*, 10, 2015.

[7] Amanpreet Kaur and Monika Saluja. Investigating tcp/ip, http, arp, icmp packets using wireshark. 2014.

[8] Samir Datt. *Learning network forensics: identify and safeguard your network against both internal and external threats, hackers, and malware attacks*. Packt Publishing, Birmingham, UK, 2016.

[9] James Kurose. *Redes de Computadoras*. Pearson Education, Ciudad de México, 2017.

[10] ¿qué es una caché? `https://www.ionos.mx/digitalguide/hosting/cuestiones-tecnicas/que-es-una-cache/`. Consultado el 14 de Noviembre de 2022.

[11] Chris Sanders. *Practical packet analysis: using Wireshark to solve real-world network problems*. Press, 3rd edition, 2017.

[12] Andrew Zola. What is a ping? `https://www.techtarget.com/searchnetworking/definition/ping`. Consultado el 17 de Marzo de 2023.

[13] Dr. M. Anand Kumar. Troubleshooting networks with internet control message protocol. *CiiT International Journal of Networking and Communication Engineering*, 1, 2009.

[14] Atul Kaushik and R. Joshi. Network forensic system for icmp attacks. *International Journal of Computer Applications*, 2, 2010.

[15] Charles M. Kozierok. The tcp/ip guide. `http://www.tcpipguide.com/free/t_ICMPv4SourceQuenchMessages-3.htm`, 2005. Consultado el 31 de Mayo de 2023.

[16] Lisa Bock. *Learn Wireshark: Confidently Navigate the Wireshark Interface and Solve Real-World Networking Problems.* Packt Publishing, Birmingham, UK, 2019.

[17] Desarrollo de Sistemas Profesionales. Sockets: Protocolos de comunicación tcp y udp. `http://dsp.mx/blog/sistemas-de-informacion/49-sockets-tcp-udp`. Consultado el 20 de Septiembre de 2022.

[18] James H. Baxter. *Wireshark essentials: get up and running with Wireshark to analyze network packets and protocols effectively*. Packt Publishing, Birmingham, U.K., 2014.

[19] John E. Canavan. *Fundamentals of Network Security*. Artech House telecommunications library. Artech House, Boston, 2001.

[20] IBM Documentation. Cortafuegos de nivel de circuito. `https://www.ibm.com/docs/es/db2/11.1?topic=support-circuit-level-firewalls`, 2014. Consultado el 31 de Mayo de 2023.

[21] ¿qué es un puerto de ordenador? | puertos en la red. `https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-computer-port/`. Consultado el 10 de Marzo de 2023.

[22] William R Simpson and Kevin E Foltz. Network segmentation and zero trust architectures. *Lecture Notes in Engineering and Computer Science, Proceedings of the World Congress on Engineering (WCE)*, 2021.

[23] Arthur Salmon, Warun Levesque, and Michael McLafferty. *Applied Network Security*. Packt Publishing, 2017.

[24] Joseph Migga Kizza. *Guide to Computer Network Security*. Springer International Publishing, 2020.

[25] Ali Sadiqui. *Computer Network Security*. ISTE Ltd / John Wiley and Sons Inc, 2019.

[26] James W. Conley Brian Reisman Mitch Ruebush Eric Cole, Ronald L. Krutz and Dieter Gollmann. *Network Security Fundamentals*. John Wiley & Sons, 11 River Street, Hoboken, 2008.

[27] Iso 27001. `https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/`. Consultado el 01 de Marzo de 2023.

[28] Implementación de un marco de ciberseguridad iso 27032. `https://www.isecauditors.com/consultoria-csf-iso-27032`. Consultado el 01 de Marzo de 2023.

[29] Real Academia Española. análisis. https://www.rae.es/drae2001/an%C3%A1lisis. Consultado el 08 de Mayo de 2022.

[30] Ric Messier. *Network Forensics*. Wiley, Indianapolis, Indiana, 2017.

[31] Jessey Bullock and Jeff T. Parker. *Wireshark for security professionals: using Wireshark and the Metasploit framework*. Wiley, Indianapolis, Indiana, 2017.

[32] Robert Shimonski, TotalBoox, and TBX. *The Wireshark Field Guide*. Elsevier Science, 2013.

[33] Piyush Verma. *Wireshark network security a succinct guide to securely administer your network using Wireshark*. Packt Publishing, Birmingham, UK, 2015.

[34] Ulf Lamping Richard Sharpe, Ed Warnicke. *Wireshark User's Guide Version 4.0.4*. Wireshark.

[35] Angela Orebaugh and Gilbert Ramirez. *Wireshark & Ethereal network protocol analyzer toolkit*. Syngress Publishing, Inc, 2007.

[36] Charit Mishra. *Mastering Wireshark: analyze data network like a professional by mastering Wireshark, from 0 to 1337*. O'Reilly, 2016.

[37] Borja Merino. Análisis de tráfico con wireshark. techreport, INTECO-CERT, February 2011.

[38] Networkminer the nsm and network forensics analysis tool. https://www.netresec.com/?page=NetworkMiner. Consultado el 29 de Noviembre de 2022.

[39] Jayant Gadge and Anish Anand Patil. Port scan detection. *16th IEEE international conference on networks*, 2008.

[40] Mauro Conti, Nicola Dragoni, and Viktor Lesyk. A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials*, 2016.

[41] Wesley M. Eddy. Defenses against tcp syn flooding attacks. *The Internet Protocol Journal*, 9, December 2006.

[42] Hao Wu, Xianglei Dang, Lidong Wang, and Longtao He. Information fusion-based method for distributed domain name system cache poisoning attack detection and identification. *IET Information Security*, 10(1), 2016.

[43] Sudhakar and R. K. Aggarwal. A survey on comparative analysis of tools for the detection of arp poisoning. *2017 2nd International Conference on Telecommunication and Networks (TEL-NET)*, 2017.

[44] Mauro Conti, Nicola Dragoni, and Viktor Lesyk. A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials*, 18, 2016.

[45] Session hijacking attack owasp foundation. https://owasp.org/www-community/attacks/Session_hijacking_attack, Abril 2020. Consultado el 09 de Diciembre de 2022.

[46] Anuj Baitha and Smitha Vinod. Session hijacking and prevention technique. *International Journal of Engineering & Technology*, 7, 2018.

[47] Ahmed Sheik. *Certified Ethical Hacker (CEH) preparation guide: lesson-based review of ethical hacking and penetration testing*. Apress L.P., Berkeley, California, 2021.

[48] What is ddos attack - javatpoint. https://www.javatpoint.com/what-is-ddos-attack. Consultado el 17 de Noviembre de 2022.

[49] Ping of death. https://insecure.org/sploits/ping-o-death.html. Consultado el 14 de Noviembre de 2022.

[50] Munther Numan, Fazirulhisyam Hashim, and Nurul Adilah Abdul Latiff. Detection and mitigation of arp storm attacks using software defined networks. *IEEE 13th Malaysia International Conference on Communications (MICC)*, 2017.

[51] Sanjeev Kumar. Smurf-based distributed denial of service (ddos) attack amplification in internet. *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, 2007.

[52] Mac flooding attack. https://linuxhint.com/mac-flooding-attack. Consultado el 18 de Enero de 2023.

[53] What is a distributed denial of service ddos attack netscout. https://www.netscout.com/what-is-ddos, October 2018. Consultado el 08 de Diciembre de 2022.

[54] Phrack magazine. http://phrack.org/issues/48/13.html, Enero 1996. Consultado el 19 de Enero de 2023.

[55] What is a dns flood ddos attack glossary imperva. https://www.imperva.com/learn/ddos/dns-flood/, September 2020. Consultado el 08 de Diciembre de 2022.

[56] What is adsl - internet connections worldwide. https://www.dstny.se/en/glossary/adsl. Consultado el 13 de Febrero de 2023.

[57] José Luis Prieto. dsniff, gti-glosario terminología informática. http://www.tugurium.com/gti/termino.php?Tr=dsniff. Consultado el 11 de Enero de 2023.

[58] ¿qué es un bogon? https://es.theastrologypage.com/bogon. Consultado el 16 de Diciembre de 2022.

[59] Charit Mishra. *Mastering Wireshark: analyze data network like a professional by mastering Wireshark, from 0 to 1337*. Packt Publishing, 2016.

[60] Raj Badhwar. *The CISO'S next frontier: AI, post-quantum cryptography and advanced security paradigms*. Springer, 2021.

[61] Andrew Froehlich. Load sharing vs. load balancing: What's the difference? https://www.techtarget.com/searchnetworking/answer/Load-sharing-vs-load-balancing-Whats-the-difference. Consultado el 15 de Mayo de 2023.

[62] What is a port scan? how to prevent port scan attacks? https://www.fortinet.com/resources/cyberglossary/what-is-port-scan. Consultado el 20 de Febrero de 2023.

[63] Monowar H. Bhuyan, Dhruba K. Bhattacharyya, and Jugal K. Kalita. *Network Traffic Anomaly Detection and Prevention*. Springer International Publishing, 2017.

[64] Charit Mishra. *Wireshark 2 Quick Start Guide: Secure Your Network Through Protocol Analysis*. Packt Publishing, Birmingham, U.K., 2018.

[65] Rahul Awati. What is a uniform resource identifier (uri)? `https://www.techtarget.com/whatis/definition/URI-Uniform-Resource-Identifier`. Consultado el 31 de Octubre de 2022.

[66] Ieee standard computer dictionary: A compilation of ieee standard computer glossaries. *IEEE Std 610*, 1991.

[67] William Stallings. *Comunicaciones y redes de computadores*. Pearson Prentice Hall, Madrid, España, 7ma edition, 2010.

[68] Craig Hunt. *TCP/IP Network Administration*. O'Reilly Media, Inc., third edition, 2002.

[69] High level organization of the standard. `http://www.pentest-standard.org/index.php/Main_Page`. Consultado el 16 de Marzo de 2023.

[70] Cvss v3.1 specification document. `https://www.first.org/cvss/v3.1/specification-document`, 2019. Consultado el 14 de Marzo de 2023.

Anexo A

Protocolos

A.1. Protocolo de Transferencia de Hipertexto

El protocolo de transferencia de hipertexto (HTTP, *Hypertext Transfer Protocol*) se utiliza para proporcionar un servicio que responde a la solicitud de un cliente. Los clientes HTTP (navegadores web) realizan peticiones a un servidor HTTP (servidor web) [63]. Para realizar las peticiones, los clientes utilizan el lenguaje de marcado de hipertexto (HTML, *HyperText Markup Language*).

Los datos en la web son transferidos utilizando los protocolos HTTP/HTTPS mediante la capa de aplicación. La comunicación normal en HTTP sigue un modelo de solicitud/respuesta en donde la comunicación entre el cliente y el servidor es ejecutada por un conjunto de reglas. El cliente solicita un determinado recurso al servidor y luego recibe un código de estado que especifica el estado actual del recurso solicitado. Si está disponible el recurso; se envía junto con el código de estado, de lo contrario el cliente recibe un código de estado no disponible [64].

Siempre que inicia una sesión HTTP existe la conexión de tres vías TCP. Se inicia un canal de comunicación entre los huéspedes a través del cual viajan paquetes HTTP y datos que son enviados y recibidos mientras la sesión está activa. Cuando el cliente hace una solicitud al servidor, éste y la página solicitada son el recurso, para acceder al recurso se necesita de un identificador uniforme de recursos (URI [1], *Identificador Uniforme de Recursos*). Un ejemplo de URI es `https://www.utm.mx/ing_electronica.html`, coloquialmente se conoce como URL, sin embargo existen diferencias técnicas. EL URI está compuesto por:

- El protocolo a usar, en este caso, `https://`
- El servidor a acceder, `www.utm.mx`
- Un número de puerto, si no se indica ninguno se asumirá el puerto 80 para HTTP.
- Una ruta de acceso a la página web. En este caso `/ing_electronica.html`

La comunicación HTTP incluye una línea de inicio, métodos, códigos de estado y modificadores de solicitud. La tabla A.1 muestra los métodos HTTP.

[1] Se trata de una secuencia de caracteres que identifica un recurso lógico (abstracto) o físico, normalmente, pero no siempre, conectado a Internet. Los URI pueden identificar diferentes tipos de recursos, tales como; documentos electrónicos, páginas web, imágenes y fuentes de información con propósito coherente. Un localizador uniforme de recursos (URL), o dirección web, es la forma más común de URI [65].

Método	Descripción
GET	Recupera la infromación definida por el URI
HEAD	Recupera las cabeceras
POST	Envía datos al servidor/aplicación HTTP
OPTIONS	Determina las opciones asociadas con una fuente
PUT	Envía los datos al servidor/aplicación HTTP
DELETE	Elimina la fuente definida por el URI
CONNECT	Utilizado para conectarse a un proxy

Tabla A.1: Descripción de los métodos HTTP.

El huésped identifica el destino y el número de puerto del recurso solicitado. Las solicitudes y respuestas HTTP utilizan modificadores de solicitud con el fin de proporcionar detalles; en la tabla A.2 se explican los modificadores más comunes.

Método	Descripción
Connection	Indica la preferencia de una conexión persistente
Accept	Muestra una lista de formatos de datos aceptados
User-Agent	Muestra una lista de parámetros del navegador y del sistema operativo
Acept-encoding	Es una lista de los esquemas de compresión HTTP aceptables
Acept-language	Los idiomas aceptables
Cookie	Datos enviados desde el sitio web y almacenados en el navegador del usuario

Tabla A.2: Descripción de los modificadores de solicitud.

HTTP tiene una categoría de códigos de estado estandarizados que indican el tipo de respuesta. Por ejemplo, cuando aparece el código `404-page not found` quiere decir que no se encuentra un recurso. En la tabla A.3 se muestran las diferentes categorías y su descripción.

Categoría	Nombre	Descripción
1xx	Informativo	Proveee información general o alguna indicación
2xx	Éxito	Indica si la solicitud del cliente fue recibida, aceptada y procesada con éxito
3xx	Redirección	Indica qué acciones futuras podrían tomarse por el usuario
4xx	Error en el cliente	Indica un error en el cliente
5xx	Error en el servidor	Indica un error en el servidor

Tabla A.3: Descripción de los códigos de estado estandarizados.

Anexo B

Modelos de Referencia

Un modelo de referencia es una estructura formal y lógica que define cómo funcionan e interactúan los dispositivos y software de la red. Así mismo, un modelo de referencia define los protocolos de comunicación, los formatos de los mensajes y los estándares necesarios para su interoperabilidad[1] [63]. Actualmente existen dos arquitecturas que son básicas en el desarrollo de los estándares de comunicación en redes de computadoras, se trata del conjunto de protocolos TCP/IP y del modelo de referencia (OSI). El conjunto de protocolos TCP/IP es la arquitectura empleada para la interconexión de redes de computadoras, mientras que OSI se ha convertido en el modelo estándar para clasificar las funciones de comunicación [67].

B.1. Modelo de referencia OSI

Los estándares son necesarios para promover la interoperatividad entre los equipos de distintos fabricantes. Debido a la complejidad que implican las comunicaciones, un estándar no es suficiente. En su lugar, las distintas funcionalidades deben dividirse en partes más manejables, estructurándose en una arquitectura de comunicaciones. La arquitectura constituye, por tanto, el marco de trabajo para el proceso de normalización.

Esto condujo en 1977 a la Organización Internacional de Estandarización (ISO, *International Organization for Standarization*) a establecer un subcomité para el desarrollo de tal arquitectura. El resultado fue el modelo de referencia OSI (*Open Systems Interconnection*). Aunque los elementos esenciales del modelo se definieron rápidamente, la norma ISO final, ISO 7498, no fue publicada hasta 1984 [67].

El modelo de referencia OSI se caracteriza por tener siete capas, cada una con una función específica (véase Figura B.1).

[1] La capacidad de dos o más sistemas o componentes para intercambiar información y utilizar la información que se ha intercambiado [66]

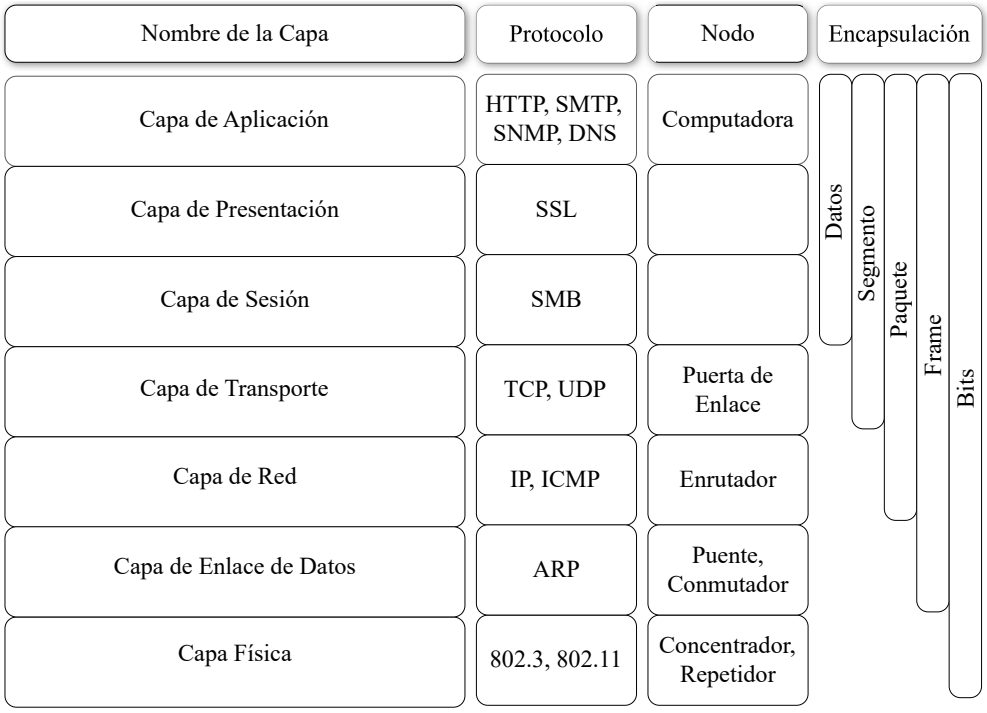


Figura B.1: Modelo de Referencia OSI.

En cada capa, los datos tienen un formato específico llamado unidad de datos de protocolo (PDU, *Protocol Data Unit*) la cual define la forma de los datos cuando pasan a la capa superior o a la capa inferior. Se conoce como datos, segmentos, paquetes, tramas (*frame*) y bits [16].

Entender el funcionamiento del modelo de referencia OSI es fundamental para comprender el flujo de información a través de la red, desde la solicitud en un huésped origen hasta la respuesta del huésped destino, entre los nodos existentes en cada capa, así como asimilar el encapsulamiento, direccionamiento y transporte de paquetes. Por consiguiente, es necesario explicar el funcionamiento de cada capa del modelo de referencia OSI:

1. Capa física: Se encarga de la transmisión de bits a través de un medio y puede ser mediante señales físicas (cable de par trenzado, inalámbrico) u ópticas (cable de fibra óptica). En esta capa se define la tasa de transmisión y sincronización de bits. Los nodos de esta capa son los concentradores, los repetidores y los conectores de cable de par trenzado.

2. Capa de enlace de datos: Se encarga de realizar la detección de errores, combinar los bits en tramas y transmite el paquete de datos a la siguiente capa.

   - Dirección MAC: La dirección de control de acceso al medio (*MAC Address, Media Access Control Address*), es una dirección única para cada dispositivo, está compuesta por 6 bytes. Los primeros tres bytes se utilizan como identificador organizacionalmente único (OUI, *Organizationally Unique Identifier*) y los últimos tres bytes son específicos de la tarjeta de interfaz de red (NIC, *Network Interface Controller*).

   Los nodos de esta capa son los conmutadores, se encargan de reenviar los datos a la siguiente capa basándose en la dirección MAC del dispositivo que va a recibir la trama. Si no se especifica la dirección del destino, la información simplemente se difunde a todos los puertos. También se encuentran los puentes que se encargan de conectar dos LANs y también pueden funcionar como repetidor.

3. Capa de red: Se encarga de realizar el enrutamiento de los paquetes de datos, desde el origen hasta el destino utilizando direccionamiento IP lógico. Encuentra el camino más fácil, más corto y más rápido entre el emisor y el receptor para intercambiar los datos.

   - Direccionamiento IP: La dirección IP es una dirección lógica de red con 32 bits. Tiene dos partes: la dirección de red y la dirección del huésped.
   - Máscara de subred: Es una dirección lógica de 32 bits que se utiliza junto a la dirección IP por los enrutadores para encontrar la ubicación del huésped destino y enrutar los datos

   En esta capa trabajan los enrutadores que facilitan el envío de paquetes de datos entre las redes que no conocen la dirección exacta del huésped.

4. Capa de transporte: En esta capa se determina cuántos paquetes deben enviarse, dónde y a qué velocidad. Mediante el control de flujo, el control de errores y la segmentación o desegmentación ayuda a controlar la fiabilidad. Divide el mensaje recibido por la capa de sesión en segmentos y los enumera para hacer una secuencia. La capa de transporte se asegura de que el mensaje se entregue al proceso correcto en la computadora destino. También se asegura de que el mensaje completo llegue sin ningún error, de lo contrario debe ser retransmitido.

5. Capa de sesión: Establece, mantiene y finaliza una sesión. Se encarga de proporcionar sincronización entre las aplicaciones, esto es necesario para la entrega eficiente de datos sin que existan perdidas.

6. Capa de presentación: Esta capa se encarga de traducir los carácteres ASCII, hacer una compresión de datos para transmitirlos por la red y encriptar los datos para mayor seguridad.

7. Capa de aplicación: En esta capa reside el software de aplicación para proporcionar comunicaciones necesarias. Por ejemplo, en esta capa trabaja el protocolo HTTP que permite la comunicación entre sitios web.

B.2. TCP/IP

En 1969, la Agencia de Proyectos de Investigación Avanzada (ARPA, *Advanced Research Projects Agency*) financió un proyecto de investigación y desarrollo para crear una red experimental de conmutación de paquetes. Esta red, llamada ARPAnet, fue construida para estudiar técnicas que proporcionaran comunicaciones de datos robustas, confiables e independientes de los proveedores. Muchas técnicas de comunicaciones modernas fueron desarrolladas en la ARPAnet mientras que los protocolos básicos TCP/IP fueron desarrollados después de que la red estuviera en funcionamiento [68].

Los protocolos TCP/IP se organizan en cinco capas conceptuales: cuatro capas definen el procesamiento de paquetes y una quinta capa define el hardware de red convencional. La Figura B.2 muestra las capas conceptuales y la encapsulación de los datos que pasan entre cada par sucesivo de capas [1].

1. Capa Física: Se encarga de la transmisión de bits a través de un medio y puede ser mediante señales físicas (cable de par trenzado, inalámbrico) u ópticas (cable de fibra óptica). En esta capa se define la tasa de transmisión y sincronización de bits. Los nodos de esta capa son los concentradores, los repetidores y los conectores de cable de par trenzado.

2. Capa de interfaz de red: Se encarga de aceptar paquetes IP y transmitirlos a través de una red específica. Una interfaz de red puede consistir en un controlador de dispositivo (por ejemplo, cuando la red es una red de área local a la que se conecta la computadora) o un subsistema complejo que implementa un protocolo de enlace de datos [1].

3. Capa de Internet: Es responsable de trasladar los paquetes de un huésped origen al huésped destino. A los paquetes de esta capa de red se les denomina datagramas. En esta capa trabaja IP, que define los campos del datagrama, así como los nodos finales. Contiene protocolos de enrutamiento que determinan las rutas que los datagramas siguen entre el huésped origen y destino.

4. Capa de transporte: Se encarga de transferir los datos a los nodos finales. El TCP y UDP son los protocolos de transporte que utiliza esta capa. TCP se caracteriza por ser un protocolo orientado a conexión mientras que UDP trabaja sin conexión, es decir, no ofrece una fiabilidad, ni control de flujo ni control de congestión. A los paquetes de la capa de transporte se les denomina segmentos.

5. Capa de aplicación: Esta capa reside el software de aplicación para proporcionar comunicaciones necesarias. Por ejemplo, en esta capa trabaja el protocolo HTTP que permite la comunicación entre sitios web.

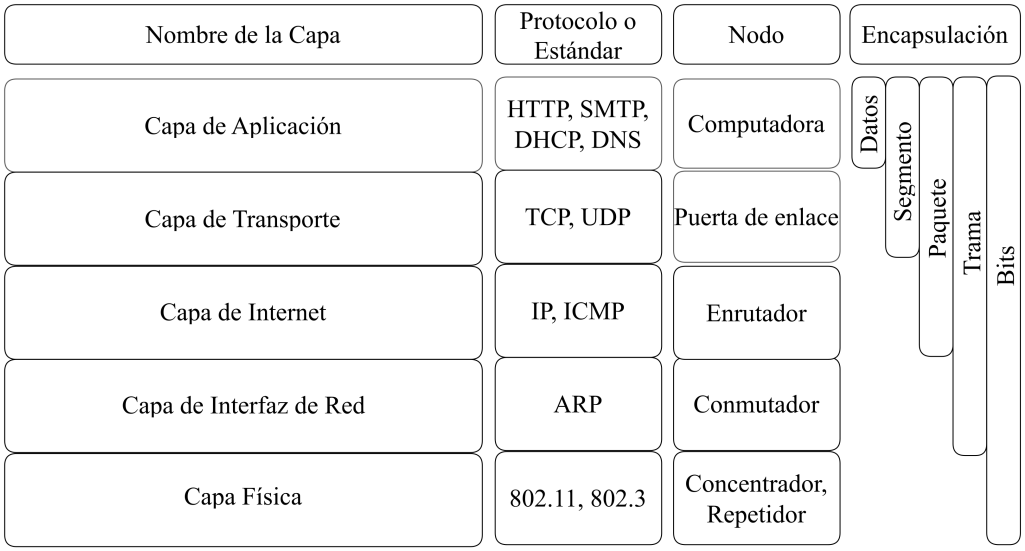


Figura B.2: Modelo TCP/IP.

Anexo C

Nodos

Los nodos están conectados entre sí mediante dispositivos especiales de conexión y conducción que toman el tráfico de red de un nodo y lo pasan al nodo siguiente. Como las LANs son redes pequeñas, sus nodos de conexión son menos potentes y con capacidades limitadas. Se mencionan los dispositivos más comúnmente encontrados en una LAN:

- Un repetidor es un dispositivo de comunicación local de bajo nivel ubicado en la capa física, recibe señales eléctricas que amplifica y luego retransmite hacia otro nodo de la red. Una de sus funciones principales es contrarrestar la atenuación que se produce cuando las señales recorren largas distancias.
- Un concentrador es uno de los dispositivos de red multipuerto básico, permite que todos los dispositivos conectados se comuniquen entre sí. Este dispositivo opera en la capa 1 del modelo OSI y envía el tráfico a todos los puertos. Son excelentes para el análisis de red, cualquiera que esté conectado a un puerto puede ver todo el tráfico de los demás puertos (véase la Figura C.1), en donde la computadora de rastreo puede ver todo el tráfico entre otras computadoras cliente.

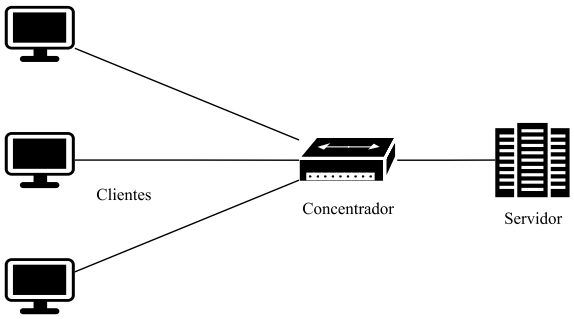


Figura C.1: Ejemplo de conexión con concentrador.

- Un conmutador es un dispositivo de red que conecta segmentos de una red (véase Figura C.2). Este dispositivo opera en la capa 2 del modelo OSI, filtra y reenvía las tramas en la red con la ayuda de una tabla dinámica. Este enfoque punto a punto permite al conmutador conectar varios pares de segmentos, permitiendo que más de una computadora transmita datos a la vez, por tal motivo ofrece un alto rendimiento [24].

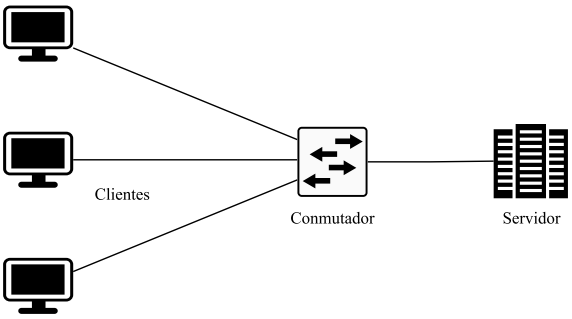


Figura C.2: Ejemplo de conexión con conmutador.

- Los enrutadores son dispositivos de uso general que interconectan dos o más redes representadas por subredes IP o líneas punto a punto no numeradas. Suelen ser computadoras dedicadas de propósito especial con interfaces de entrada y salida separadas para cada red conectada. Se implementa en la capa de red del modelo de referencia OSI (véase Figura C.3).

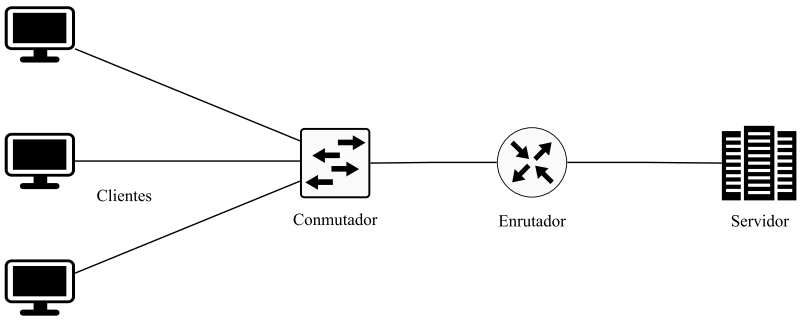


Figura C.3: Ejemplo de conexión para un enrutador.

- Un puente es como un repetidor, pero mientras un repetidor amplifica las señales eléctricas; un puente trabaja en el enlace de datos y amplifica las señales digitales. Copia digitalmente las tramas y permite que las tramas de una LAN, o de una LAN diferente con una tecnología distinta, pasen a otra parte o a otra LAN (véase Figura C.4) [24].

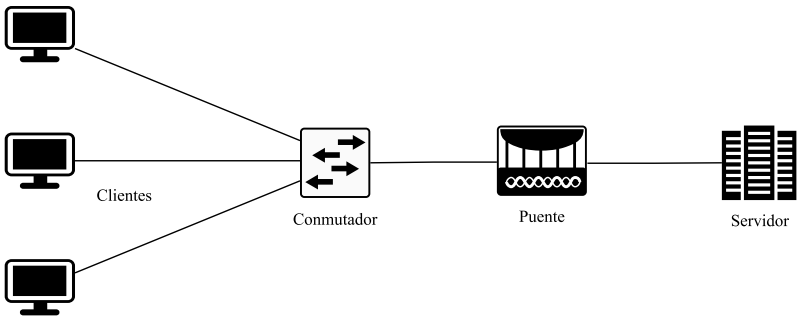


Figura C.4: Ejemplo de conexión para un puente.

- La puerta de enlace realiza la conversión de protocolos entre diferentes tipos de redes, arquitecturas o aplicaciones y sirve como traductor e intérprete para computadoras de red que se comunican con diferentes protocolos y operan en redes diferentes. La funcionalidad de la puerta de enlace, que hace la traducción entre diferentes tecnologías y algoritmos de red, se llama convertidor de protocolos (véase Figura C.5).

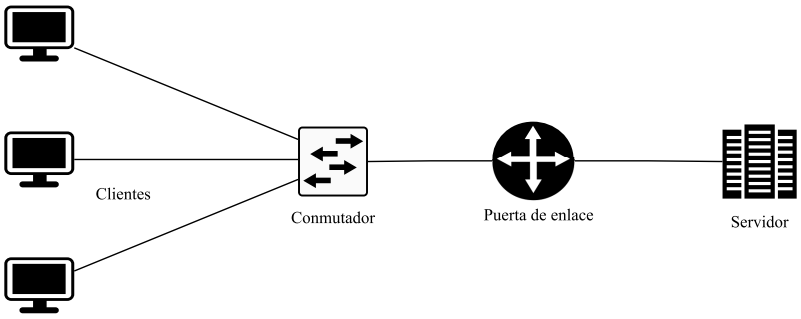


Figura C.5: Ejemplo de conexión para una puerta de enlace.

Anexo D

Formato de Reporte

1. Portada
2. Índice
3. Resumen del Reporte
   Se detalla el nombre de la organización/universidad a la cual se le realizará la detección de amenazas, y el nombre del encargado de realizar la detección de amenazas. Es importante detallar las fechas y las horas de inicio y de finalización. Se agregan las amenazas encontradas y se detalla el nivel de gravedad.
4. Observaciones
   Esta sección sirve como una visión general de alto nivel (véase Figura D.1). Una lista detallada de todas las amenazas descubiertas se puede encontrar en el apartado 6. Es importante señalar que esta lista no es en absoluto exhaustiva y que es muy probable que existan vulnerabilidades no encontradas.

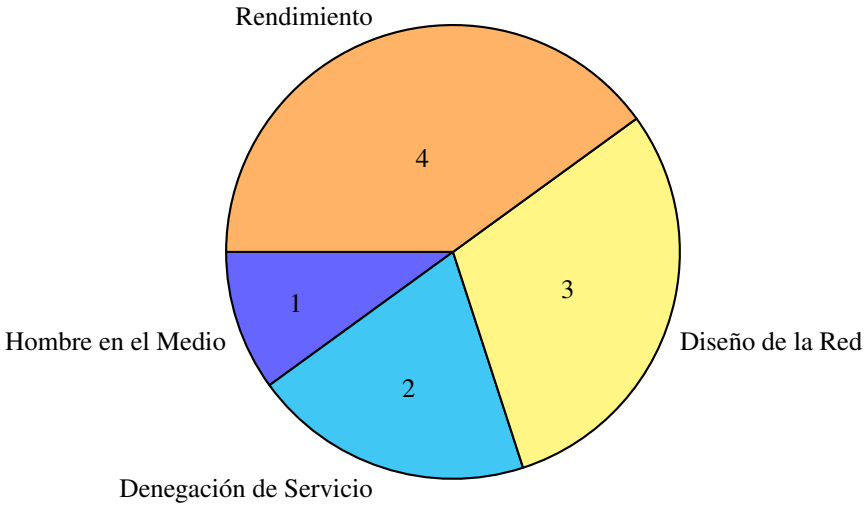


Figura D.1: Resumen de los problemas de la red.

5. Metodología
   Para este reporte, la metodología a utilizar es la Ejecución de Pruebas de Penetración (PTES, *Penetration Testing Execution Standard*) con el fin de detectar amenazas que puedan afectar el rendimiento de una red (véase Figura D.2) [69].

Figura D.2: Metodología PTES.

6. Resultados Técnicos
   Esta tabla tiene el propósito de mostrar el número total de amenazas encontradas durante la detección. Las amenazas se clasifican en función del nivel de riesgo. Los niveles de riesgo se calculan utilizando el Sistema de Puntuación de Vulnerabilidad Común (CVSS, *Common Vulnerability Scoring System*) [70].

Gravedad	Baja (0.1-3.9)	Moderada (4.0-6.9)	Alta (7.0-8.9)	Crítica (9.0-10.0)
Amenaza	1	1	1	1

7. Conclusión
   En esta sección se detallan los problemas que se presentaron al momento de realizar la detección de amenazas, así mismo, se describe el porqué de los problemas encontrados.

8. Anexos - Herramientas de Software utilizadas
   Se nombran las herramientas utilizadas, ya sean software o hardware.