Aplicación de técnicas de análisis forense en paquetes de redes domésticas sospechosos para confirmar la presencia de intrusos

Manuel Alejandro Archila Morán

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

UNIVERSIDAD DEL VALLE DE GUATEMALA
Facultad de Ingeniería

Aplicación de técnicas de análisis forense en paquetes de redes domésticas sospechosos para confirmar la presencia de intrusos

Trabajo de graduación en modalidad de trabajo profesional presentado por
Manuel Alejandro Archila Morán
para optar al grado académico de Licenciado en Ingeniería en Ciencias de la Computación y Tecnologías de la Información

Guatemala
2024

UNIVERSIDAD DEL VALLE DE GUATEMALA
Facultad de Ingeniería

Aplicación de técnicas de análisis forense en paquetes de redes domésticas sospechosos para confirmar la presencia de intrusos

Trabajo de graduación en modalidad de trabajo profesional presentado por
Manuel Alejandro Archila Morán
para optar al grado académico de Licenciado en Ingeniería en Ciencias de la Computación y Tecnologías de la Información

Guatemala
2024

Vo.Bo.:

(f) 

Ing. Juan Pedro Cáceres

Tribunal Examinador:

(f) 

Ing. Melinton Navas

(f) 

Ing. Juan Pedro Cáceres

(f) 

PhD. Gabriel Barrientos

Fecha de aprobación: Guatemala, 02 de diciembre de 2024.

Índice general

Lista de figuras

Lista de cuadros

Resumen

Este proyecto, titulado "Aplicación de técnicas de análisis forense en paquetes de redes domésticas sospechosos para confirmar la presencia de intrusos", aborda la creciente necesidad de proteger las redes domésticas utilizadas en entornos de teletrabajo. Se enfoca en la aplicación de técnicas avanzadas de análisis forense para detectar patrones de tráfico anómalos que podrían indicar intrusiones maliciosas.

El proyecto emplea herramientas como Wireshark para inspección y visualización detallada de los paquetes capturados, así como Python y la biblioteca dpkt para procesar archivos PCAP de forma programática. La metodología incluye la detección de actividades sospechosas como beaconing, escaneo de puertos, spoofing de ARP, y exfiltración de datos. Las visualizaciones juegan un papel importante al facilitar la interpretación de los resultados mediante gráficos de tráfico por IP, solicitudes DNS, y transferencias de datos.

Esta investigación subraya la relevancia de implementar medidas preventivas para mitigar vulnerabilidades en redes domésticas y fortalecer la seguridad en entornos de teletrabajo. Se documentan patrones maliciosos y se generan recomendaciones para optimizar la ciberseguridad, beneficiando tanto a individuos como a organizaciones.

Abstract

This project, titled "Application of Forensic Analysis Techniques in Suspicious Home Network Packets to Confirm the Presence of Intruders", investigates the forensic analysis of network traffic in home networks, focusing on those used for remote work environments. Advanced techniques are applied to detect and confirm intrusions by identifying suspicious patterns such as beaconing, port scanning, ARP spoofing, and data exfiltration.

The research utilizes Wireshark for detailed inspection and visualization of captured network packets, alongside Python and the dpkt library to process PCAP files programmatically. Data visualizations assist in interpreting findings through traffic flow charts, DNS requests, and large data transfers.

The results highlight the importance of implementing preventive measures to mitigate vulnerabilities in home networks and improve intrusion detection. The study offers actionable recommendations that enhance cybersecurity, contributing valuable insights for individuals and organizations engaged in remote work.

CAPÍTULO 1

Introducción

En la era del teletrabajo, la seguridad de las redes domésticas ha adquirido una importancia crítica. Según Seguridad360, un total del 25,9 % de los bots maliciosos operó a un nivel sofisticado, imitando con éxito el comportamiento humano y eludiendo los métodos de detección de nivel superior [1].Este proyecto se centra en el análisis forense de paquetes de red, ya marcados como potencialmente maliciosos, puede confirmar la presencia de instrusos en estas redes. La proliferación de dispositivos conectados en entornos domésticos, junto con la falta de protocolos de seguridad robustos, presenta un problema significativo: la vulnerabilidad ante ataques generados por intrusos que pueden comprometer datos personales y corporativos.

El propósito de esta investigación es desarrollar un método confiable y detallado para el análisis forense de paquetes de red que identifique efectivamente intrusos en entornos de teletrabajo. Al aplicar técnicas avanzadas y herramientas especializadas, aspiramos a mejorar la detección y mitigación de estas amenazas.

Esta propuesta incluye la implementación de un conjunto de estrategias forenses detalladas, combinando teoría y práctica para identificar intrusos en redes domésticas a traves del tráfico previamente catalogado como malicioso. Los resultados esperados buscan ofrecer un marco mejorado para la seguridad en el teletrabajo, proporcionando conocimientos valiosos sobre la detección de usuarios extraños y fortaleciendo las defensas de las redes domésticas contra futuros ataques.

CAPÍTULO 2

Justificación

El trabajo remoto se ha convertido en una forma dominante de empleo en la sociedad actual, especialmente impulsado por situaciones globales recientes que han forzado a las empresas y sus empleados a adaptarse a entornos digitales desde casa. La transición representó entre el 20 y el 30 % de los asalariados trabajando desde casa durante la pandemia, según datos de la Organización Internacional del Trabajo, lo que significó un aumento significativo desde menos del 3 % antes de la misma [2]. El incremento en la dependencia de las redes domésticas para actividades profesionales incrementa el riesgo de intrusión y compromiso cibernético, ya que estas redes suelen ser menos seguras que las redes corporativas y con frecuencia carecen de las mismas medidas robustas de seguridad y protocolos de gestión del riesgo. Es crucial implementar estrategias específicas para asegurar que estos nuevos entornos de trabajo no se conviertan en el punto débil de la seguridad de la información corporativa.

La detección de intrusos es una necesidad crítica en este contexto. Según un estudio realizado por Ponem Institute las empresas tardan un promedio de 98 días en detectar un brecha de seguridad [3]. Durante este tiempo los intrusos pueden obtener acceso no autorizado a datos personales y empresariales, interrumpir operaciones y servir como plataforma para ataques más complejos. La recolección de esta información sensible es el principal objetivo de estos atacantes, ya que según IBM el 44 % de los datos robados en el año 2020 fueron credenciales de usuarios [4]. En las redes domésticas, la falta de herramientas adecuadas para el análisis y la conciencia sobre la seguridad deja a los individuos y organizaciones vulnerables a estos ataques. El análisis forense de paquetes de red se presenta como una técnica esencial para detectar y analizar patrones de tráfico anómalos y actividades sospechosas que pueden indicar la presencia de intrusos.

Un ejemplo impactante es el de un banco global que creía imposible la extracción de información sensible de su entorno. Sin embargo, una prueba dirigida sobre los controles de punto final y de datos reveló más de 70 brechas de seguridad, muchas de ellas directamente relacionadas con el entorno de trabajo remoto [5]. Este caso subraya la necesidad crítica de desarrollar metodologías adaptadas a las redes domésticas usadas para el teletrabajo, que puedan proporcionar diagnósticos valiosos para mitigar estos riesgos de seguridad de manera efectiva. Implementar estrategias de seguridad adecuadas a las redes domésticas no solo protegerá la información sensible y la infraestructura de las empresas, sino que también fortalecerá la confianza en el teletrabajo como un modelo viable a largo plazo. Al identificar la presencia de intrusos y tomar medidas adecuadas, las organizaciones pueden decidir qué pasos tomar para asegurar la continuidad del negocio y fomentar un entorno de trabajo seguro para sus empleados. Este proyecto no solo atiende a una necesidad inmediata de seguridad

en el contexto del teletrabajo, sino que también contribuye al desarrollo de mejores prácticas para la gestión de la ciberseguridad en entornos no tradicionales.

CAPÍTULO 3

Objetivos

3.1. Objetivo general

Implementar técnicas de análisis forense de paquetes de red para confirmar la presencia de intrusos en redes domésticas empleadas para el teletrabajo.

3.2. Objetivos específicos

- Aplicar técnicas de análisis forense para descomponer y examinar paquetes de red seleccionados, con el fin de identificar patrones de tráfico anómalos
- Optimizar los procesos de detección y respuesta ante incidentes de seguridad, desarrollando e implementando reglas de detección basadas en los patrones de tráfico anómalos identificados.
- Reportar los hallazgos del análisis forense de la red, identificando y documentando detalladamente las vulnerabilidades descubiertas en el tráfico de datos.

CAPÍTULO 4

Marco teórico

4.1. Redes domésticas y seguridad del teletrabajo

El avance tecnológico y la creciente dependencia del teletrabajo han transformado las redes domésticas en componentes críticos del entorno digital actual. Estas redes permiten a los empleados acceder remotamente a sistemas y recursos corporativos, lo cual facilita la continuidad laboral desde el hogar. Sin embargo, esta conectividad también introduce una serie de riesgos de ciberseguridad, que convierten a las redes domésticas en objetivos atractivos para los atacantes [6]. A medida que aumenta el uso de redes domésticas para el trabajo remoto, también crecen las amenazas que afectan a estos entornos, tales como ataques de phishing, malware, y vulnerabilidades en las conexiones de red. Por ello, resulta esencial implementar medidas de seguridad específicas para proteger tanto los datos personales como los recursos empresariales accesibles desde el hogar [7].

4.1.1. Importancia de la seguridad en redes domésticas

La seguridad de las redes domésticas es un aspecto crítico para proteger la privacidad y la integridad de la información personal. Con el incremento de dispositivos conectados en los hogares, como computadoras, teléfonos inteligentes, televisores y cámaras de seguridad, las redes domésticas se han convertido en un blanco atractivo para los ciberdelincuentes. Los atacantes pueden aprovecharse de configuraciones de seguridad deficientes, dispositivos no actualizados o el desconocimiento del usuario para ejecutar diferentes tipos de ataques [8]. A pesar de la percepción de que las redes domésticas no son objetivos prioritarios, los riesgos asociados a ellas pueden ser tan significativos como en las redes empresariales. La falta de una segmentación adecuada y la utilización de credenciales por defecto facilitan el acceso no autorizado a la red y, con ello, la captura de tráfico sensible [9].

4.1.2. Vulnerabilidades comunes en redes domésticas

Las redes domésticas presentan diversas vulnerabilidades que pueden ser explotadas por los atacantes para acceder a datos confidenciales o comprometer el funcionamiento de los dispositivos conectados. Entre las vulnerabilidades más comunes se encuentran las contraseñas débiles o predeterminadas en los routers, la falta de actualizaciones de firmware, y la exposición de servicios no seguros

como Telnet o FTP, los cuales permiten accesos remotos sin encriptación [10]. Muchos dispositivos domésticos, como cámaras de seguridad y asistentes virtuales, vienen configurados con credenciales por defecto, lo que facilita que los atacantes utilicen diccionarios de contraseñas predefinidas para obtener acceso [9]. Además, la configuración incorrecta de redes Wi-Fi, como la utilización de protocolos de seguridad obsoletos como WEP, puede permitir que intrusos se conecten a la red sin ser detectados [11].

Otro problema importante es la falta de segmentación de las redes, lo que significa que una vez que un atacante compromete un dispositivo, como un televisor inteligente o un termostato conectado, puede moverse lateralmente dentro de la red y atacar otros dispositivos más críticos, como computadoras o servidores personales [12]. El uso de técnicas como el escaneo de puertos y la captura de paquetes permite a los atacantes identificar dispositivos y servicios vulnerables dentro de la red doméstica, lo que facilita el despliegue de ataques como la interceptación de tráfico (sniffing), la manipulación de paquetes (spoofing) y la suplantación de direcciones (ARP poisoning) [13].

Finalmente, la falta de concientización de los usuarios es una vulnerabilidad significativa en las redes domésticas. Muchos usuarios no cambian las configuraciones predeterminadas ni implementan medidas básicas de seguridad como la autenticación de dos factores o la creación de redes segmentadas para dispositivos sensibles, lo que aumenta el riesgo de intrusiones y filtraciones de datos [14].

4.2. Análisis de tráfico de red

El análisis de tráfico de red es un componente esencial del análisis forense en entornos domésticos y se emplea para comprender el flujo de datos que circula a través de la red, detectar actividades sospechosas y responder a posibles incidentes de seguridad. Este proceso consiste en la captura, inspección y evaluación de los datos que se transmiten a través de la red, permitiendo a los investigadores identificar patrones de tráfico que puedan indicar la presencia de amenazas, como intentos de escaneo de puertos, conexiones a servidores maliciosos o transferencias de datos no autorizadas [15]. En un entorno doméstico, donde múltiples dispositivos como computadoras, televisores inteligentes y dispositivos IoT se encuentran conectados simultáneamente, el monitoreo de tráfico puede proporcionar información valiosa sobre el comportamiento de cada dispositivo y sus comunicaciones con el exterior.

El uso de herramientas especializadas para la captura de paquetes, como Wireshark y tcpdump, permite realizar un análisis detallado de cada paquete de red, observando campos específicos como direcciones IP de origen y destino, números de puerto y datos del payload. A través de la aplicación de filtros, estas herramientas permiten identificar patrones anómalos, como intentos de conexión a puertos inusuales, repetidos intentos de autenticación fallida, o incluso la presencia de tráfico encriptado que podría indicar un túnel VPN no autorizado. Además, el análisis de tráfico también se puede utilizar para detectar la manipulación de datos, suplantación de identidad (spoofing), y la redirección de tráfico mediante técnicas como ARP poisoning [16].

El análisis de tráfico de red en redes domésticas es particularmente útil para identificar ataques dirigidos a dispositivos IoT, que a menudo carecen de controles de seguridad robustos y pueden ser comprometidos para formar parte de botnets [17]. Por ejemplo, una captura de tráfico que muestre un dispositivo doméstico intentando conectarse repetidamente a direcciones IP externas no relacionadas podría ser un indicio de que el dispositivo ha sido comprometido y está participando en actividades maliciosas. En general, el análisis de tráfico de red permite a los administradores y usuarios domésticos obtener una visión detallada del comportamiento de la red y detectar posibles amenazas antes de que se conviertan en incidentes de seguridad [18].

4.2.1. Estructura de paquetes y su análisis forense

Cada paquete de red contiene información valiosa que puede ser utilizada para determinar la naturaleza de una conexión y su legitimidad. La estructura de los paquetes se organiza en capas, basándose en los modelos de referencia OSI (Open Systems Interconnection) y TCP/IP (Transmission Control Protocol/Internet Protocol). El modelo OSI es un estándar teórico desarrollado por la ISO (International Organization for Standardization), que define siete capas para describir el flujo de datos en una red [19]. Sin embargo, en la práctica, el modelo TCP/IP, que se compone de solo cuatro capas (acceso a la red, internet, transporte y aplicación), es el más ampliamente utilizado en redes domésticas y la mayoría de los dispositivos y protocolos están diseñados en función de este modelo [20].

En el análisis forense de paquetes de red, se examinan los datos de cada una de estas capas para extraer información relevante y detectar anomalías. Por ejemplo, la capa de enlace de datos, equivalente a la capa de acceso a la red en TCP/IP, proporciona direcciones físicas (MAC) que permiten rastrear la procedencia y el destino de los dispositivos dentro de una red local [21]. Esto es particularmente útil para identificar si un dispositivo está suplantando la identidad de otro mediante técnicas como ARP spoofing. La capa de red, equivalente a la capa de internet en TCP/IP, contiene direcciones IP y detalles de enrutamiento, lo que permite seguir el camino que toman los paquetes a través de la red y detectar posibles intentos de redireccionamiento malicioso [22].

La capa de transporte, que abarca los protocolos TCP y UDP, permite identificar las aplicaciones y servicios que se están comunicando a través de números de puerto. Analizar los encabezados de esta capa puede ayudar a detectar intentos de manipulación de sesiones (session hijacking), fragmentación anómala de paquetes, o incluso ataques de denegación de servicio (DoS) que intentan saturar un servicio específico [23]. Finalmente, la capa de aplicación es crucial para el análisis forense, ya que contiene la carga útil (payload) del paquete, la cual puede incluir información como solicitudes HTTP, comandos DNS, o contenido de mensajes en protocolos como SMTP o FTP [22].

4.2.2. Herramientas y técnicas de análisis forense de tráfico

Existen numerosas herramientas para realizar análisis forense de tráfico de red, cada una con funcionalidades especializadas para capturar, filtrar y analizar el contenido de los paquetes. Entre las herramientas más utilizadas se encuentra **Wireshark**, una aplicación gráfica ampliamente conocida en el campo de la seguridad informática, que permite inspeccionar cada detalle de los paquetes capturados en tiempo real. Wireshark permite a los investigadores visualizar el contenido de cada capa del paquete y aplicar filtros avanzados para centrarse en patrones específicos, como intentos de conexión a puertos conocidos por vulnerabilidades, respuestas anómalas en protocolos DNS o tráfico sospechoso hacia dominios desconocidos [16].

Por otro lado, el uso de lenguajes de programación como **Python** en el análisis de tráfico forense ha ganado popularidad, gracias a la flexibilidad y poder de las librerías disponibles. Entre estas se encuentran **dpkt**, **pyshark** y **scapy**, las cuales permiten automatizar la captura y análisis de paquetes de red, así como desarrollar scripts personalizados para casos específicos de análisis [24]. La librería **dpkt** es particularmente útil para procesar grandes volúmenes de tráfico rápidamente, ya que permite parsear archivos de captura (`.pcap`) y extraer datos relevantes como direcciones IP, puertos y protocolos sin necesidad de una interfaz gráfica [25].

Otra librería popular es **pyshark**, que actúa como un *wrapper* para Wireshark y permite utilizar las funciones de captura y filtrado de esta herramienta desde un entorno de Python . Con **pyshark**, los investigadores pueden aplicar los mismos filtros que usarían en Wireshark y acceder a cada campo del paquete de manera programática, facilitando la automatización de tareas repetitivas y el análisis de grandes volúmenes de datos en poco tiempo [26].

Finalmente, **scapy** es una de las librerías más potentes y versátiles para el análisis y manipulación de tráfico de red. A diferencia de **dpkt** y **pyshark**, **scapy** no solo se limita a analizar el tráfico, sino que también permite crear y enviar paquetes personalizados, lo cual la hace ideal para pruebas de penetración y simulaciones de ataques [27].

4.3. Técnicas de detección de intrusiones

La detección de intrusiones es una técnica esencial para identificar actividades no autorizadas o maliciosas dentro de una red, especialmente en entornos domésticos donde la seguridad suele ser menos robusta que en entornos empresariales. Los **Sistemas de Detección de Intrusiones** (IDS) juegan un papel crucial en este proceso, ya que monitorean continuamente el tráfico de la red y generan alertas cuando se detectan patrones sospechosos o actividades que se desvían del comportamiento normal [28]. Estos sistemas permiten a los usuarios detectar posibles ataques antes de que comprometan la seguridad de la red, lo cual es especialmente importante en redes domésticas donde múltiples dispositivos, como cámaras de seguridad, asistentes virtuales y otros dispositivos IoT, se conectan simultáneamente.

Existen dos enfoques principales para la detección de intrusiones: la detección basada en firmas y la detección basada en el comportamiento. La **detección basada en firmas** se enfoca en identificar patrones de ataque conocidos que han sido previamente catalogados y registrados en una base de datos de firmas. Este tipo de IDS compara el tráfico de red con firmas predefinidas de ataques conocidos, como intentos de escaneo de puertos, inyecciones de código SQL o intentos de fuerza bruta para acceder a contraseñas [29]. Si el sistema detecta una coincidencia con una firma en su base de datos, genera una alerta. Aunque este método es efectivo para detectar ataques conocidos, su principal limitación es la incapacidad para identificar nuevas amenazas o ataques de día cero [30].

Por otro lado, la **detección basada en el comportamiento** no se limita a patrones de ataque predefinidos, sino que analiza el comportamiento habitual de la red para identificar cualquier anomalía que pueda indicar una intrusión. Este enfoque es útil en redes domésticas, donde el tráfico de los dispositivos conectados tiende a seguir patrones consistentes. Un IDS basado en el comportamiento puede detectar actividades sospechosas cuando, por ejemplo, un dispositivo IoT comienza a enviar grandes volúmenes de datos a un servidor externo no autorizado [31]. A través de técnicas como el análisis estadístico y el aprendizaje automático, estos sistemas pueden aprender el comportamiento "normal"de la red y detectar desviaciones que podrían representar una amenaza [32].

Además, algunos sistemas modernos combinan ambos enfoques, lo que se conoce como **detección híbrida**, para aumentar la precisión y cobertura en la detección de intrusiones [33]. En redes domésticas, el uso de soluciones híbridas puede optimizar el balance entre la detección de ataques conocidos y la capacidad de identificar comportamientos anómalos.

4.3.1. Monitoreo y detección de anomalías

El monitoreo y la detección de anomalías se centran en el análisis continuo del tráfico de red para identificar comportamientos que se desvían de la norma establecida. En esta técnica, se utiliza una línea base del tráfico legítimo o normal, que representa el comportamiento esperado de los dispositivos conectados en la red. Esta línea base es crucial para identificar cambios abruptos o inusuales que puedan señalar la presencia de un incidente de seguridad, como intentos de exfiltración de datos, accesos no autorizados o la conexión de dispositivos no reconocidos a la red [34]. A diferencia de los sistemas de detección basados en firmas, que dependen de la identificación de patrones predefinidos de ataques, la detección de anomalías tiene la ventaja de ser efectiva para descubrir comportamientos previamente desconocidos, como ataques de día cero [35].

El monitoreo de anomalías es particularmente útil en redes domésticas, donde los patrones de tráfico suelen ser más estables y predecibles que en entornos empresariales. Los dispositivos conectados en el hogar, como televisores inteligentes, asistentes virtuales y cámaras de seguridad, tienden a seguir rutinas de comunicación que pueden ser fácilmente monitoreadas y analizadas. Por ejemplo, si un dispositivo IoT, que normalmente solo se comunica con servidores de su proveedor, de repente comienza a enviar grandes volúmenes de datos a un servidor externo no autorizado, esto podría ser una señal de que el dispositivo ha sido comprometido [36]. De manera similar, un aumento inesperado en el tráfico saliente durante horas inusuales puede indicar intentos de exfiltración de datos o actividades de malware en la red.

Las técnicas de detección de anomalías suelen apoyarse en herramientas y algoritmos de aprendizaje automático que permiten al sistema aprender el comportamiento normal de la red con el tiempo y adaptarse a los cambios graduales en los patrones de tráfico [37]. Algoritmos como redes neuronales, análisis estadístico y *clustering* no supervisado se utilizan para identificar estas desviaciones, permitiendo la detección de amenazas emergentes que podrían pasar desapercibidas para otros sistemas basados en reglas estáticas [38]. Esta capacidad de adaptación es crucial para detectar ataques de día cero, en los que no existen firmas predefinidas ni referencias previas para identificarlos.

A pesar de las ventajas del monitoreo de anomalías, uno de los desafíos más comunes es el riesgo de generar falsos positivos. Dado que esta técnica se basa en la identificación de desviaciones, eventos legítimos pero inusuales, como la instalación de un nuevo dispositivo o una actualización de software que provoca un cambio en los patrones de tráfico, podrían generar alertas falsas [39]. Sin embargo, al combinar el monitoreo de anomalías con otros métodos de detección, como la detección basada en firmas, los administradores pueden minimizar estos falsos positivos y obtener un panorama más completo del estado de la red.

4.4. Análisis forense de paquetes capturados

El análisis forense de paquetes capturados es un proceso clave en la investigación de incidentes de seguridad en redes. A diferencia del monitoreo en tiempo real, este análisis se realiza de manera retrospectiva sobre datos que fueron previamente capturados durante un período específico. El análisis forense de estos paquetes permite a los investigadores examinar con detalle el tráfico de red, identificar patrones anómalos y reconstruir los eventos que llevaron a un incidente de seguridad . Esta técnica es especialmente valiosa para descubrir ataques que no fueron detectados en tiempo real, como actividades maliciosas ocultas entre el tráfico legítimo o ataques sofisticados que involucran múltiples fases . Al examinar los diferentes tipos de paquetes y protocolos, los analistas pueden rastrear la fuente y el destino de los datos, detectar intentos de suplantación de identidad o de manipulación de paquetes, y encontrar evidencia de tráfico sospechoso que podría haber comprometido la seguridad de la red . El análisis forense de paquetes es una herramienta fundamental para comprender las causas y consecuencias de un ataque, proporcionando información detallada para prevenir futuros incidentes y garantizar la integridad de la red [40].

4.4.1. Tipos de paquetes y protocolos comunes en el análisis forense

En el análisis forense de redes, uno de los aspectos más críticos es la correcta identificación y análisis de los tipos de paquetes y protocolos que se encuentran presentes en el tráfico de red. Los tipos de paquetes y los protocolos de comunicación juegan un papel fundamental en la determinación de los eventos que llevaron a un incidente de seguridad, ya que cada uno aporta información valiosa sobre el origen, destino y la naturaleza de los datos transmitidos. A continuación, se describen los tipos de paquetes más comunes en el análisis forense y los protocolos más relevantes en redes domésticas.

- **Paquetes IP (Internet Protocol)**: El protocolo IP es responsable del direccionamiento y la fragmentación de los datos que se transmiten a través de redes basadas en TCP/IP. En el contexto del análisis forense, los paquetes IP son de gran importancia, ya que contienen las direcciones IP de origen y destino, lo que permite a los analistas rastrear el origen de una conexión sospechosa o identificar dispositivos dentro de la red que pudieran haber sido comprometidos [41].
- **Paquetes TCP (Transmission Control Protocol)**: TCP es un protocolo orientado a la conexión, lo que significa que garantiza la entrega de los datos en el orden correcto y sin pérdidas. Los paquetes TCP incluyen información como el número de secuencia y el número de acuse de recibo, lo que facilita el análisis detallado de las sesiones establecidas entre dispositivos. En el análisis forense, los analistas pueden reconstruir sesiones completas utilizando los datos de los paquetes TCP, lo que es crucial para determinar cómo un atacante interactuó con los sistemas comprometidos [42].
- **Paquetes UDP (User Datagram Protocol)**: A diferencia de TCP, el protocolo UDP no garantiza la entrega de datos, lo que lo hace más rápido pero menos fiable. UDP se utiliza comúnmente en aplicaciones que requieren alta velocidad, como el streaming de video o los juegos en línea. Los paquetes UDP son relevantes en el análisis forense porque suelen ser utilizados en ataques como los de denegación de servicio (DoS) y en aplicaciones que generan grandes volúmenes de tráfico no confiable [43].
- **Protocolo HTTP (Hypertext Transfer Protocol)**: HTTP es el protocolo base para la transferencia de datos en la web. En el análisis forense, el tráfico HTTP es de gran interés, ya que puede revelar sitios web a los que se accedió, datos enviados a través de formularios y otros contenidos sensibles que podrían haberse filtrado durante un ataque. Los analistas pueden investigar encabezados HTTP, solicitudes GET/POST y la respuesta del servidor para identificar patrones anómalos de comportamiento [44].
- **Protocolo HTTPS (Hypertext Transfer Protocol Secure)**: HTTPS es una versión segura de HTTP, que utiliza SSL/TLS para cifrar los datos transmitidos entre el cliente y el servidor. Aunque el tráfico HTTPS es más difícil de analizar debido a su cifrado, los metadatos como las direcciones IP, puertos y los certificados pueden proporcionar pistas sobre conexiones sospechosas, incluso sin acceso al contenido de la comunicación cifrada [44].
- **Protocolo DNS (Domain Name System)**: El sistema DNS es crucial para resolver nombres de dominio en direcciones IP. Los ataques como el envenenamiento de caché DNS y la suplantación de servidores DNS pueden desviar el tráfico legítimo hacia sitios maliciosos. El análisis forense de paquetes DNS puede revelar intentos de redireccionamiento o actividad sospechosa relacionada con dominios fraudulentos [45].

Cada uno de estos tipos de paquetes y protocolos aporta información crítica durante el análisis forense de un incidente de seguridad. Los analistas pueden extraer direcciones IP, números de puerto, datos de aplicaciones y otras características clave para identificar patrones de tráfico malicioso, reconstruir el flujo de un ataque y tomar decisiones informadas sobre las contramedidas a implementar.

4.4.2. Extracción de información de paquetes

La extracción de información de paquetes es un proceso fundamental en el análisis forense de redes, ya que permite a los investigadores identificar y rastrear datos clave que pueden revelar la naturaleza y el alcance de un incidente de seguridad. Cada paquete de red contiene múltiples campos que transportan información valiosa sobre el origen, destino y contenido de los datos transmitidos. A continuación, se describe el proceso de extracción de la información más relevante durante un análisis forense de paquetes.

- **Direcciones IP (Internet Protocol)**: Las direcciones IP de origen y destino son fundamentales para rastrear la procedencia y el destino del tráfico en la red. Estas direcciones permiten identificar los dispositivos implicados en una conexión o ataque. En el contexto del análisis forense, las direcciones IP pueden ayudar a localizar los servidores a los que se conectó un dispositivo comprometido o desde donde se originó un ataque [46]. Las direcciones IP también se pueden utilizar para identificar intentos de suplantación de identidad, como en ataques de IP spoofing, en los que un atacante falsifica la dirección IP de origen para hacerse pasar por otro dispositivo.

- **Direcciones MAC (Media Access Control)**: Las direcciones MAC son identificadores únicos asignados a las tarjetas de red y permiten rastrear la identidad de dispositivos dentro de una red local. En un análisis forense, la dirección MAC puede ser útil para identificar dispositivos conectados a la red en un momento específico. Las direcciones MAC son esenciales para analizar la autenticidad de los dispositivos y detectar intentos de suplantación en la red local [47].

- **Números de puerto**: Los números de puerto son utilizados para identificar qué servicio o aplicación está siendo utilizado en una comunicación. El análisis de los números de puerto permite a los investigadores determinar qué tipo de tráfico está fluyendo en la red. Por ejemplo, los puertos 80 y 443 suelen estar asociados con el tráfico web (HTTP y HTTPS), mientras que el puerto 21 indica tráfico FTP [48]. Identificar los puertos utilizados por los atacantes puede ayudar a los analistas a reconstruir la actividad de un ataque, como el acceso a servidores web no autorizados o la transferencia de datos maliciosos.

- **Protocolo de transporte (TCP/UDP)**: El protocolo de transporte utilizado en un paquete también proporciona información crítica. El protocolo TCP, por ejemplo, incluye datos sobre el número de secuencia y el acuse de recibo, lo que permite a los analistas reconstruir sesiones de comunicación completas [49]. En el caso de UDP, aunque carece de garantías de entrega, es común en ataques de denegación de servicio (DoS), ya que puede ser utilizado para saturar un servidor con grandes volúmenes de tráfico.

- **Encabezados de paquetes (Headers)**: Los encabezados de los paquetes proporcionan metadatos valiosos sobre la estructura del paquete y la información de control utilizada para dirigir el tráfico. Estos encabezados contienen detalles como la versión del protocolo, la longitud del paquete, el TTL (Time to Live) y los protocolos de nivel superior utilizados [50]. El análisis detallado de los encabezados puede ayudar a los investigadores a detectar intentos de manipulación de paquetes, como la fragmentación maliciosa de datos o la alteración de los campos de control para desviar o interrumpir la entrega de datos.

- **Contenido del paquete (Payload)**: El payload o contenido del paquete es la porción de datos que transporta la información que está siendo intercambiada entre los dispositivos. En el análisis forense, inspeccionar el contenido de los paquetes es esencial para identificar comandos enviados, credenciales transmitidas en texto plano, o incluso archivos maliciosos que se hayan transferido a través de la red [51]. Aunque los payloads pueden estar cifrados, los metadatos y otros datos adjuntos pueden proporcionar pistas sobre la naturaleza de la comunicación. El análisis de payloads no cifrados es una fuente de evidencia clave para comprender el propósito de la comunicación en cuestión.

La combinación de esta información permite a los analistas forenses crear una imagen detallada de las actividades que ocurrieron en la red durante un período determinado. Al extraer direcciones IP, números de puerto, protocolos y contenido de los paquetes, los investigadores pueden rastrear los movimientos de los atacantes, reconstruir el flujo de los ataques y determinar el impacto potencial sobre la red y los dispositivos comprometidos.

4.4.3. Detección de actividades maliciosas

La detección de actividades maliciosas en el análisis forense de paquetes capturados es esencial para identificar ataques que comprometen la seguridad de una red. Existen varios patrones de tráfico que pueden ser indicativos de actividades maliciosas, como el escaneo de puertos, el tráfico inusual y los ataques de suplantación de identidad (ARP poisoning). Estos patrones pueden ser detectados a través de un análisis exhaustivo de los paquetes capturados y la correlación de eventos dentro del tráfico de red.

- **Escaneo de puertos**: El escaneo de puertos es una técnica utilizada por los atacantes para descubrir servicios activos en una red. Al enviar múltiples paquetes dirigidos a diferentes puertos de un sistema, los atacantes pueden identificar qué puertos están abiertos y qué servicios están disponibles, lo que les permite encontrar vulnerabilidades explotables [13]. Un patrón común de escaneo de puertos incluye un alto volumen de paquetes dirigidos a puertos consecutivos en un corto período de tiempo. Herramientas como Nmap son frecuentemente utilizadas para realizar este tipo de ataques. En el análisis forense, detectar un escaneo de puertos implica observar conexiones repetitivas desde la misma dirección IP hacia varios puertos de un dispositivo, lo cual puede señalar el intento de mapear la red en busca de vulnerabilidades.

- **Tráfico inusual o anómalo**: El tráfico inusual es una señal clave de una actividad maliciosa. Este tipo de tráfico puede incluir un aumento inesperado en el volumen de datos transmitidos, tráfico generado en horarios inusuales o conexiones a direcciones IP sospechosas o desconocidas [52]. El análisis forense puede detectar estos patrones al comparar el tráfico actual con una línea base de comportamiento normal. Por ejemplo, si un dispositivo IoT que normalmente genera poco tráfico comienza a enviar grandes volúmenes de datos a un servidor externo, esto podría indicar una exfiltración de datos o un ataque de malware. Además, el tráfico hacia sitios web o servidores que están asociados con actividades maliciosas puede ser un signo claro de una infracción de seguridad.

- **Ataques de Suplantación de Identidad (ARP Spoofing)**: ARP (Address Resolution Protocol) spoofing es un ataque en el que un atacante falsifica mensajes ARP para asociar su dirección MAC con la dirección IP de otro dispositivo en la red, permitiendo interceptar o modificar el tráfico destinado a esa dirección [53]. Este ataque es particularmente peligroso en redes domésticas, donde el control sobre el tráfico ARP suele ser mínimo. Los analistas forenses pueden detectar ARP spoofing mediante la inspección de paquetes ARP inconsistentes o duplicados en la red, donde una dirección IP está asociada a múltiples direcciones MAC. Al observar patrones de tráfico anómalos relacionados con la resolución de direcciones, los analistas pueden identificar y mitigar los efectos de este ataque, como el secuestro de sesiones (session hijacking) o la intercepción de datos sensibles.

- **Ataques de Denegación de Servicio (DoS)**: Un ataque de Denegación de Servicio (DoS) o de Denegación de Servicio Distribuida (DDoS) ocurre cuando un atacante sobrecarga un servidor o dispositivo con una gran cantidad de tráfico para agotar sus recursos y hacer que sea inaccesible para los usuarios legítimos [54]. Los ataques DoS suelen estar caracterizados por un alto volumen de paquetes, a menudo generados a través de protocolos como UDP, ICMP o TCP SYN. En el análisis forense, la identificación de un ataque DoS puede implicar la detección de una avalancha de paquetes desde múltiples direcciones IP hacia un único servidor o servicio. Este tipo de análisis permite a los investigadores identificar el origen del ataque y, en algunos casos, filtrar el tráfico malicioso para restaurar la funcionalidad del sistema afectado.

- **Exfiltración de datos**: La exfiltración de datos es el proceso por el cual un atacante extrae información confidencial de una red comprometida. Este tipo de actividad maliciosa a menudo se lleva a cabo mediante la transmisión de datos sensibles a servidores externos controlados por el atacante [55]. En el análisis forense, la detección de la exfiltración de datos puede implicar la identificación de conexiones a direcciones IP sospechosas, así como un análisis de

las transferencias de archivos o grandes volúmenes de datos fuera de la red, que no corresponden a las actividades normales del usuario. Los analistas también pueden detectar intentos de evadir la detección mediante el uso de cifrado o protocolos menos comunes.

El análisis de estos patrones de actividad maliciosa proporciona a los investigadores forenses las herramientas necesarias para identificar, rastrear y mitigar los ataques en redes domésticas. Detectar anomalías como el escaneo de puertos, el tráfico inusual o los ataques de suplantación de identidad es esencial para prevenir mayores daños y asegurar la red contra futuras amenazas.

4.4.4. Reconstrucción de incidentes de seguridad

La reconstrucción de incidentes de seguridad es un proceso crítico en el análisis forense de redes. Utilizando la información contenida en los paquetes capturados, los analistas forenses pueden recrear la secuencia de eventos que llevaron a un incidente de seguridad, identificar los métodos utilizados por los atacantes y evaluar el impacto total del ataque. Este enfoque permite comprender no solo lo que sucedió, sino también cómo y cuándo se produjo, lo que facilita la implementación de medidas preventivas para evitar incidentes similares en el futuro. A continuación, se describen algunas de las principales técnicas para la reconstrucción de incidentes de seguridad.

- **Identificación de la secuencia de eventos**: La primera etapa en la reconstrucción de un incidente es identificar la secuencia de eventos clave que ocurrieron durante el ataque. Esto implica analizar el tráfico de red capturado para seguir las conexiones establecidas, las solicitudes enviadas y las respuestas recibidas entre el atacante y los dispositivos comprometidos. Por ejemplo, mediante el análisis de las direcciones IP de origen y destino, los números de puerto y las marcas de tiempo de los paquetes, los analistas pueden determinar cuándo y cómo se estableció la conexión inicial. Posteriormente, pueden seguir el rastro de las acciones tomadas por el atacante, como el escaneo de vulnerabilidades, la explotación de una vulnerabilidad y la instalación de malware.
- **Análisis de cronología**: El análisis de la cronología del incidente es crucial para determinar el momento exacto en que ocurrió el ataque y para identificar el punto de entrada. Utilizando los **timestamps** asociados a los paquetes capturados, los analistas pueden reconstruir el orden en el que se realizaron las acciones maliciosas y correlacionarlas con otros eventos en la red. Por ejemplo, si un servidor web fue atacado, la cronología de los paquetes HTTP podría revelar cuándo el atacante envió una solicitud maliciosa, cuándo el servidor respondió y cuándo se extrajeron datos confidenciales. El análisis de la cronología también permite identificar patrones de comportamiento malicioso que ocurrieron durante un periodo prolongado, lo que es útil en casos de ataques persistentes avanzados (APT, por sus siglas en inglés).
- **Correlación con otros eventos de seguridad**: La correlación de la información de los paquetes capturados con otros eventos de seguridad es fundamental para obtener una visión completa del incidente. Esto incluye la relación entre el tráfico de red y otros eventos como accesos no autorizados a sistemas, modificaciones en archivos o intentos de autenticación fallidos. Los analistas pueden correlacionar los datos de los paquetes con registros de auditoría, logs de sistemas y otros eventos, lo que les permite identificar si el tráfico malicioso coincidió con actividades sospechosas en los sistemas internos. Por ejemplo, si se detecta un aumento en el tráfico hacia un servidor, esto podría coincidir con un intento de acceso no autorizado en los registros del sistema, lo que indicaría un intento de exfiltración de datos.
- **Reconstrucción de sesiones**: Una de las técnicas más avanzadas para la reconstrucción de incidentes es la capacidad de reconstruir sesiones completas de comunicación a partir de los paquetes capturados. Esto es particularmente útil en casos donde los atacantes interactúan directamente con sistemas comprometidos durante un período prolongado. La reconstrucción de

sesiones TCP, por ejemplo, permite a los analistas ver exactamente qué datos fueron enviados y recibidos durante una sesión, lo que ayuda a determinar las acciones específicas realizadas por el atacante. Esta técnica también es útil para detectar ataques de suplantación de sesiones o intentos de manipulación de datos.

- **Detección de indicadores de compromiso (IoCs)**: Los Indicadores de Compromiso (IoCs) son rastros de actividad maliciosa que los atacantes dejan tras realizar un ataque. Estos pueden incluir direcciones IP sospechosas, nombres de archivos maliciosos o comportamientos anómalos en el tráfico de red. La detección y el análisis de estos indicadores en los paquetes capturados es esencial para identificar qué sistemas fueron comprometidos, cómo se llevó a cabo el ataque y qué medidas deben tomarse para evitar que vuelva a ocurrir. Los IoCs pueden ser utilizados tanto para la detección temprana de futuros ataques como para la recuperación de sistemas comprometidos.
- **Documentación y generación de informes forenses**: Tras la reconstrucción del incidente, es crucial que los analistas forenses documenten sus hallazgos de manera clara y completa. Esta documentación incluye la cronología de los eventos, las técnicas utilizadas por los atacantes y las vulnerabilidades explotadas. La generación de informes forenses no solo facilita la comprensión de los hechos por parte de otros equipos de seguridad o por el personal de gestión, sino que también proporciona evidencia para posibles acciones legales o regulatorias. Además, los informes forenses permiten a las organizaciones aprender del incidente y mejorar sus defensas frente a futuros ataques.

El seguimineto de esotos pasos es imperativo para poder realizar una buena reconstruccipon de los eventos ocurridos durante el ataque. Es necesario conocer el procedimiento adecuado para documentar cada uno de los hallazgos sin dañar o alterar la evidencia. La reconstrucción de incidentes de seguridad es esencial para comprender completamente el alcance y el impacto de un ataque. Mediante el análisis de la secuencia de eventos, la cronología de los ataques y la correlación con otros eventos de seguridad, los analistas pueden obtener una visión completa del incidente, lo que les permite responder de manera efectiva y prevenir futuros compromisos [56].

4.4.5. Preservación y documentación de la evidencia

En el análisis forense de redes, la preservación y documentación de la evidencia es esencial para garantizar que los datos capturados puedan ser utilizados de manera confiable en investigaciones futuras. La integridad de los paquetes capturados debe ser mantenida en todo momento para asegurar que la evidencia no sea manipulada o alterada, lo que podría comprometer su validez en un contexto legal o de auditoría. A continuación, se discuten las principales técnicas y mejores prácticas para preservar y documentar adecuadamente la evidencia forense.

- **Métodos de preservación de capturas**: Uno de los primeros pasos en el proceso de análisis forense es garantizar que los paquetes capturados estén preservados de manera que no puedan ser modificados ni corrompidos. Para ello, se deben utilizar técnicas que mantengan la integridad de los datos capturados. Entre las técnicas más comunes se encuentran el uso de algoritmos de hashing, como MD5 o SHA-256, para generar una huella digital del archivo de captura (`.pcap`), lo que permite verificar que no se ha alterado en ningún momento. Adicionalmente, los analistas forenses suelen trabajar con copias de las capturas originales, almacenando el archivo original en un medio de solo lectura (como un disco duro externo o DVD) para evitar cualquier modificación accidental . Otras técnicas incluyen el sellado de tiempo (*timestamping*) de los archivos, que proporciona una marca temporal verificable del momento en que se capturó y almacenó la evidencia [57].
- **Cadena de custodia**: En cualquier investigación forense, es fundamental mantener una cadena de custodia para rastrear quién tuvo acceso a la evidencia, cuándo y qué se hizo con ella.

La cadena de custodia es un registro detallado que documenta todos los movimientos y accesos a la evidencia digital, desde su captura hasta su análisis y almacenamiento final. Este registro debe incluir detalles como la identidad de las personas que manejaron la evidencia, el propósito de su acceso y cualquier acción realizada sobre ella. Mantener una cadena de custodia robusta asegura que la evidencia no haya sido manipulada y, por lo tanto, se puede presentar de manera confiable en procedimientos legales o auditorías [58].

- **Generación de informes forenses**: La creación de informes forenses detallados es una parte crucial del proceso de análisis. Estos informes no solo documentan los hallazgos de los analistas, sino que también proporcionan una explicación clara y comprensible del incidente investigado, que puede ser utilizada por otros equipos técnicos, auditores o en procedimientos judiciales [59]. Un informe forense debe incluir varios elementos clave, como:
  - Descripción del incidente de seguridad.
  - Cronología detallada de los eventos identificados.
  - Métodos utilizados para analizar los paquetes capturados.
  - Resultados del análisis, incluyendo cualquier actividad maliciosa detectada.
  - Medidas recomendadas para mitigar el ataque y prevenir futuros incidentes.
- **Uso de herramientas forenses certificadas**: Para garantizar que la evidencia digital sea aceptada en procedimientos legales, los analistas forenses deben utilizar herramientas y métodos que sean reconocidos y certificados por la comunidad forense. Herramientas como Wireshark, tcpdump, y otros softwares especializados en análisis de paquetes están ampliamente aceptadas en la comunidad de análisis forense. El uso de herramientas validadas y certificadas garantiza que los datos extraídos sean confiables y que los métodos de análisis cumplan con los estándares aceptados por los tribunales y otras instituciones regulatorias.
- **Almacenamiento seguro de la evidencia**: Después de que los datos han sido capturados y analizados, es fundamental almacenarlos de manera segura para garantizar que puedan ser utilizados en el futuro si es necesario. Esto implica el uso de medios de almacenamiento seguro y de solo lectura, como discos duros externos cifrados o sistemas de almacenamiento en la nube con autenticación robusta y control de acceso [60]. Además, las copias de seguridad de los archivos de captura deben realizarse regularmente para prevenir la pérdida accidental de datos. Mantener la evidencia en un ambiente seguro garantiza que esté disponible para investigaciones futuras o auditorías.

La preservación y documentación de la evidencia es una parte crítica del análisis forense, ya que asegura que los datos capturados puedan ser utilizados de manera efectiva en investigaciones futuras. Al emplear técnicas adecuadas de preservación, mantener una cadena de custodia clara y generar informes forenses detallados, los analistas pueden proporcionar una visión completa del incidente y garantizar que la evidencia sea admitida en procedimientos legales.

CAPÍTULO 5

Metodología

5.1. Requisitos previos para el análisis forense

Para integrar esta metodología de análisis forense de paquetes de red, es fundamental contar previamente con un sistema de captura de paquetes configurado en el entorno de la red objetivo. Este sistema debe ser capaz de registrar de manera continua o bajo demanda el tráfico que circula por la red, generando archivos en formatos estándar como PCAP para su posterior análisis. La disponibilidad de estas capturas permite realizar un análisis detallado en cualquier momento, facilitando la identificación de anomalías y patrones sospechosos en caso de incidentes de seguridad o auditorías forenses.

5.2. Preparación para el análisis

Se estableció un entorno controlado y seguro en una máquina virtual aislada para el análisis forense de los paquetes de red capturados. Este entorno fue configurado con herramientas clave como Python y las bibliotecas `dpkt`, `socket`, `pandas`, `matplotlib`, y `requests`, que permiten un análisis detallado de los datos contenidos en los archivos PCAP. Las bibliotecas fueron seleccionadas por su robustez y amplia adopción en la comunidad de análisis forense de redes. Se verificó que todos los archivos estuvieran en un formato compatible con las herramientas, realizando conversiones necesarias para preservar la integridad de los datos.

5.3. Identificación de anomalías

El análisis forense de los paquetes capturados se centró en la detección de patrones sospechosos que podrían indicar la presencia de intrusos en la red. Los siguientes parámetros y herramientas fueron seleccionados por su relevancia en la identificación de amenazas comunes:

- **Paquetes SYN (escaneo de puertos):** Se empleó la detección de paquetes SYN sin respuestas ACK, los cuales son indicativos de intentos de escaneo de puertos o ataques SYN flood. Este tipo de ataque suele emplearse para detectar servicios abiertos en un sistema antes

de realizar un ataque más dirigido. Se utilizó `dpkt` para analizar el tráfico TCP y detectar este tipo de actividad, con un umbral de 10 paquetes SYN por IP para considerar el tráfico sospechoso.

- **Transferencias de datos grandes:** Se analizaron los tamaños de los paquetes TCP, estableciendo un umbral de 1000 bytes para identificar posibles fugas de datos o exfiltraciones de información. Este parámetro es esencial para detectar transferencias masivas no autorizadas desde la red.
- **Solicitudes DNS:** Se monitorearon las solicitudes DNS en busca de patrones anómalos o consultas repetitivas a dominios sospechosos. Se utilizó `dpkt` para extraer las consultas DNS y `matplotlib` para representar visualmente los resultados. Se consideró como sospechoso cualquier dominio que recibiera más de 5 solicitudes, indicando posibles intentos de phishing o actividad maliciosa.
- **Beaconing:** Se implementó la detección de patrones de beaconing, analizando la cantidad de solicitudes enviadas a una misma IP destino. El beaconing es característico de malware que se comunica con servidores de comando y control. Se estableció un umbral de más de 50 solicitudes para identificar estas actividades.
- **ARP Spoofing:** Se implementó la detección de ataques de ARP spoofing, en los que un atacante asocia múltiples direcciones MAC a una dirección IP con el fin de interceptar tráfico. Se analizaron los paquetes ARP para verificar si una misma IP tenía múltiples direcciones MAC asociadas, lo que indicaría un ataque.

La selección de estos parámetros y herramientas fue basada en las mejores prácticas de análisis forense de tráfico de red, donde el objetivo es detectar actividades maliciosas como escaneos, ataques de denegación de servicio, exfiltración de datos y tráfico hacia servidores no autorizados.

5.4. Representación de hallazgos

Se realizaron representaciones visuales de los resultados obtenidos para facilitar su interpretación y análisis posterior:

- **Gráficos de tráfico por IP destino:** Se generaron gráficos de barras que mostraron la cantidad de solicitudes enviadas a cada IP, lo que permitió identificar patrones de beaconing.
- **Gráficos de paquetes SYN por IP origen:** Estos gráficos mostraron la cantidad de paquetes SYN enviados por cada IP origen, lo que ayudó a identificar intentos de escaneo de puertos.
- **Gráficos de transferencias de datos grandes por IP:** Se visualizó el volumen de datos transferidos por IP, ayudando a detectar posibles fugas de información.
- **Gráficos de solicitudes DNS por dominio:** Este gráfico facilitó la identificación de dominios sospechosos al mostrar visualmente las solicitudes DNS recibidas por cada dominio.
- **Gráficos de protocolos detectados:** Se representaron los protocolos observados en el tráfico, permitiendo detectar protocolos no estándar o inusuales que podrían indicar tráfico malicioso.

La visualización de los datos se implementó utilizando `matplotlib`, una biblioteca robusta y flexible que permite generar gráficos detallados y personalizables, facilitando la comprensión de los resultados del análisis.

5.5. Análisis con Wireshark

Wireshark fue utilizado como complemento al análisis automatizado realizado en Python, permitiendo una inspección más detallada y manual de los hallazgos detectados en los paquetes PCAP. Esta herramienta facilitó la validación de anomalías previamente identificadas y permitió reconstruir secuencias de eventos en la red mediante la aplicación de filtros avanzados y la opción **"Follow TCP/UDP Stream"**.

5.6. Documentación de resultados

Se documentaron todos los hallazgos, incluyendo detalles sobre las direcciones IP y los tipos de tráfico involucrados en las anomalías detectadas. El informe final incluyó un resumen detallado de los patrones sospechosos identificados, como escaneos de puertos, solicitudes DNS inusuales, ataques de ARP spoofing, `strings` sospechosos en el contenido del paquete, transferencias de datos grandes y ataques de beaconing, análisis realizado con Python. Además, se documentaron los hallazgos en los puertos inusuales detectados con la herramienta Wireshark, incluyendo un posible ataque de phishing y la descarga de un ejecutable malicioso. El informe concluye con recomendaciones para mitigar posibles vulnerabilidades y prevenir futuros incidentes de seguridad.

CAPÍTULO 6

Resultados

6.1. Detección de anomalías

La detección de anomalías fue un proceso fundamental en el análisis forense del tráfico de red realizado, ya que permitió identificar patrones inusuales o comportamientos sospechosos que podrían haber indicado la presencia de intrusos en la red. En esta sección, se analizaron los paquetes capturados utilizando la librería `dpkt` en Python, la cual facilitó la extracción y procesamiento de información clave, como los encabezados de protocolos, patrones de comunicación y datos transferidos. A través de este análisis, se identificaron indicadores de compromiso, tales como beaconing, escaneo de puertos, ARP spoofing, tráfico DNS inusual y transferencias de datos atípicas. La detección de estas anomalías no solo evidenció posibles ataques, sino que también proporcionó información relevante para mitigar vulnerabilidades y mejorar la seguridad de la red.

6.1.1. Hash del archivo de capturas

Hash SHA-256 del archivo: `bc4913e7823995dc6fcfeeeb1450ee391aa91b44af2bd09da4e93f79b681a4c4`

6.1.2. Solicitudes por IP

El análisis de las solicitudes realizadas por cada dirección IP fue esencial para identificar patrones de comportamiento que pudieran sugerir actividades maliciosas dentro del tráfico de red. Esta parte se enfoca en examinar la cantidad y destinos de las diferentes solicitudes que realizaban las IPs para identificar patrones sospechosos. Uno de estos siendo `beaconing`, un tipo de comunicación repetitiva que los atacantes utilizan para mantener control sobre dispositivos comprometidos.

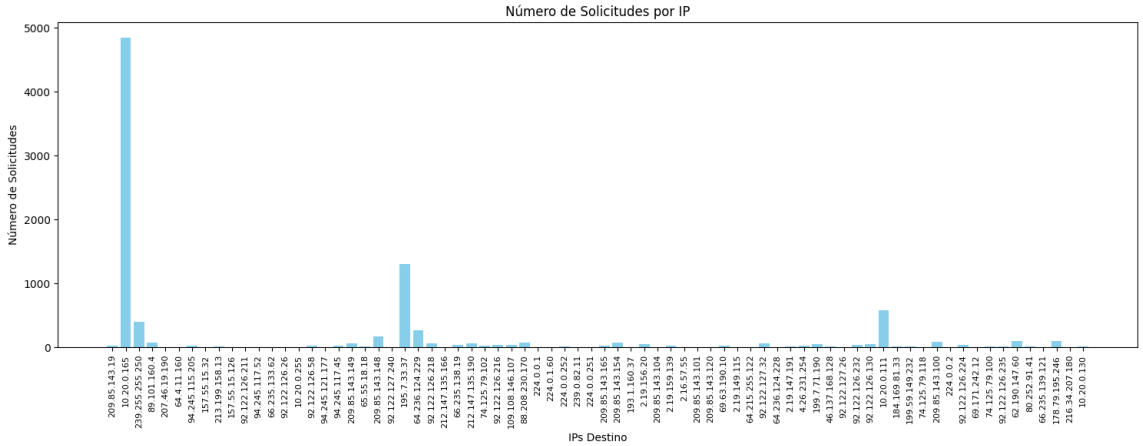


Figura 6.1: Solicitudes por IP

La Figura 6.1 muestra las solicitudes realizadas por cada una de las IPs encontradas dentro del archivo analizado.

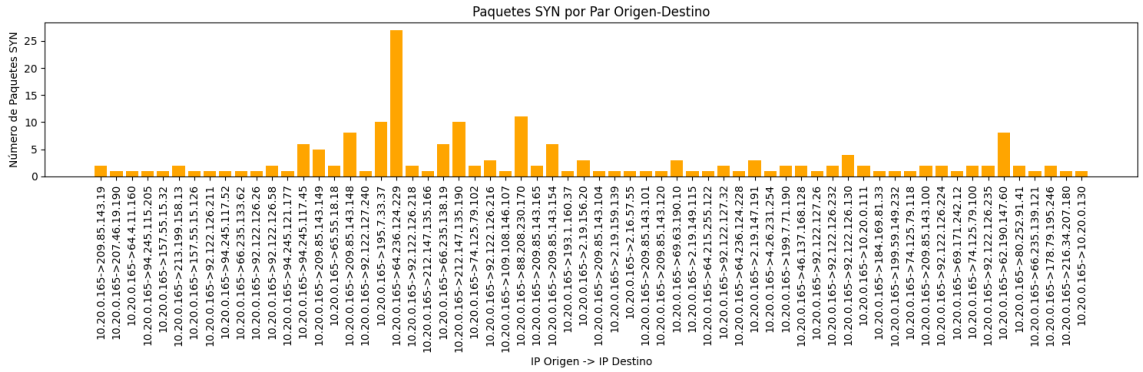


Figura 6.2: Paquetes SYN por par de origen-destino

La Figura 6.2 muestra la cantidad de paquetes SYN que existe entre cada par de IPs origen-destino. Esto se ocurre cuando dos dispositivos estan estableciendo una nueva conexión.

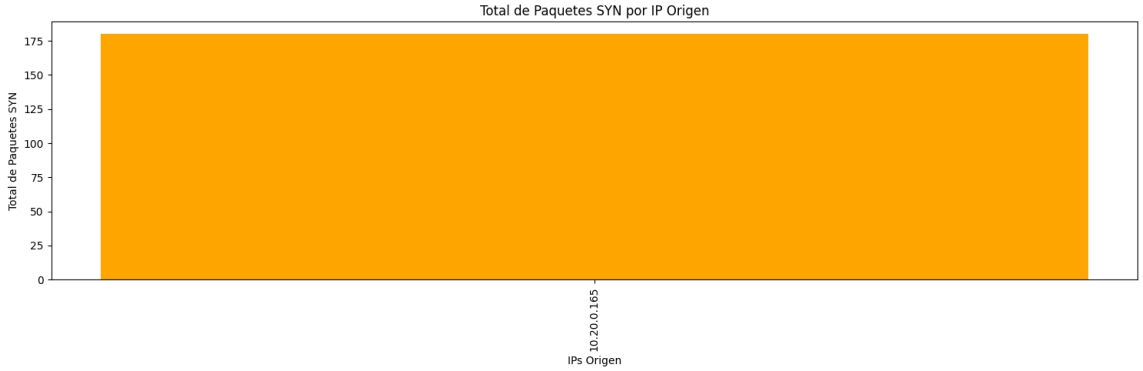


Figura 6.3: Total de paquetes SYN por origen

En la Figura 6.3 muestra la cantidad de paquetes SYN que una IP ha enviado.

6.1.3. Escaneo de puertos

En esta sección se presentan los resultados relacionados con el escaneo de puertos, una técnica empleada tanto por administradores de red como por atacantes para identificar puertos abiertos y servicios activos en los dispositivos de la red. Durante el análisis del tráfico capturado, se estudiaron las peticiones que cada IP hacia los puertos de otras para identificar posibles ataques de este tipo, caracterizados por múltiples solicitudes consecutivas dirigidas a diferentes puertos en breves intervalos de tiempo.

Tabla 6.1: Análisis de puertos por IP

IP Origen	IP Destino	Puerto	Solicitudes
10.20.0.165	209.85.143.19	443	32
10.20.0.165	207.46.19.190	80	5
10.20.0.165	64.4.11.160	80	5
10.20.0.165	94.245.115.205	80	23
10.20.0.165	157.55.15.32	80	4
10.20.0.165	213.199.158.13	80	10
10.20.0.165	157.55.15.126	80	4
10.20.0.165	92.122.126.211	80	5
10.20.0.165	94.245.117.52	80	5
10.20.0.165	66.235.133.62	80	4
10.20.0.165	92.122.126.26	80	5
10.20.0.165	92.122.126.58	80	29
10.20.0.165	94.245.121.177	80	5
10.20.0.165	94.245.117.45	80	32
10.20.0.165	209.85.143.149	80	67
10.20.0.165	65.55.18.18	80	11
10.20.0.165	209.85.143.148	80	174
10.20.0.165	92.122.127.240	80	5
10.20.0.165	195.7.33.37	80	1307
10.20.0.165	64.236.124.229	80	271
10.20.0.165	92.122.126.218	80	68
10.20.0.165	212.147.135.166	80	5
10.20.0.165	66.235.138.19	80	33
10.20.0.165	212.147.135.190	80	59
10.20.0.165	74.125.79.102	80	21
10.20.0.165	92.122.126.216	80	44
10.20.0.165	109.108.146.107	80	42
10.20.0.165	88.208.230.170	80	76
10.20.0.165	209.85.143.165	80	26
10.20.0.165	209.85.143.154	80	63
10.20.0.165	209.85.143.154	443	10
10.20.0.165	193.1.160.37	80	6
10.20.0.165	2.19.156.20	80	51
10.20.0.165	209.85.143.104	80	5
10.20.0.165	2.19.159.139	80	23
10.20.0.165	2.16.57.55	80	7
10.20.0.165	209.85.143.101	80	6

IP Origen	IP Destino	Puerto	Solicitudes
10.20.0.165	209.85.143.120	443	8
10.20.0.165	69.63.190.10	80	25
10.20.0.165	2.19.149.115	80	6
10.20.0.165	64.215.255.122	80	5
10.20.0.165	92.122.127.32	80	63
10.20.0.165	64.236.124.228	80	5
10.20.0.165	2.19.147.191	80	13
10.20.0.165	4.26.231.254	80	27
10.20.0.165	199.7.71.190	80	46
10.20.0.165	46.137.168.128	80	14
10.20.0.165	92.122.127.26	80	5
10.20.0.165	92.122.126.232	80	39
10.20.0.165	92.122.126.130	80	51
10.20.0.165	10.20.0.111	8080	13
10.20.0.165	10.20.0.111	4444	569

La Tabla 6.1 presenta un resumen de las solicitudes realizadas desde una IP origen a otras IPs destino, especificando el puerto involucrado en cada conexión y el número total de conexiones realizadas.

6.1.4. Análisis de solicitudes DNS

En esta sección se presentan los resultados del análisis de las solicitudes DNS, un componente esencial para detectar patrones sospechosos en el tráfico de red. Este análisis permite identificar dominios consultados, los cuales pueden mostrar comportamientos maliciosos, como el uso de dominios generados algorítmicamente.

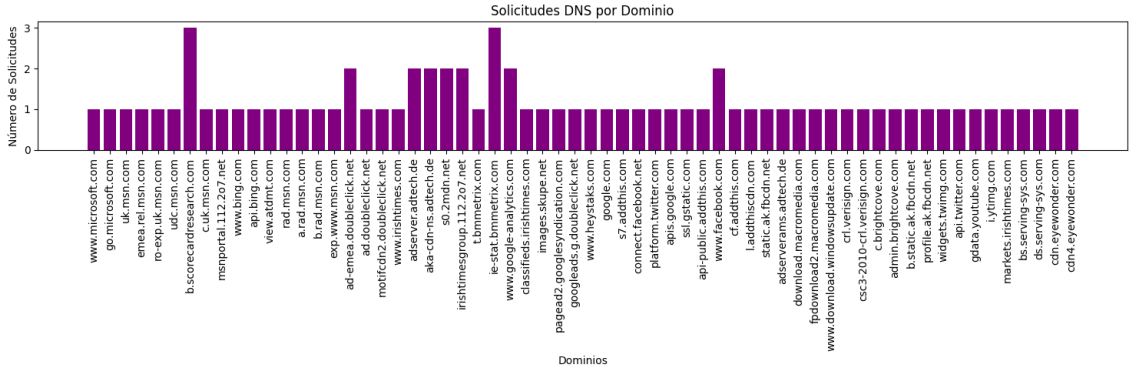


Figura 6.4: Solicitudes DNS por dominio

La Figura 6.4 muestra el número de solicitudes DNS realizadas por las distintas IPs involucradas en el análisis.

6.1.5. Transferencia de datos grandes

En este apartado se presentan los resultados del análisis de transferencias grandes de datos, un indicador grande para detectar comportamiento malicioso. Las existencia de gtransferencia de

grandes volumenes puede asociarse con exfiltración de información sensible.

Tabla 6.2: Transferencias grandes de datos

IP Origen	IP Destino	Bytes Transferidos
10.20.0.165	195.7.33.37	151002
209.85.143.148	10.20.0.165	256549
195.7.33.37	10.20.0.165	2287931
92.122.126.218	10.20.0.165	116435
92.122.127.32	10.20.0.165	101161
10.20.0.111	10.20.0.165	1153000
209.85.143.100	10.20.0.165	146931
62.190.147.60	10.20.0.165	118291
178.79.195.246	10.20.0.165	135385

La Tabla 6.2 presenta un resumen de la cantidad de bytes tranferidos de una IP origen a un IP destino.

6.2. Detección de Strings sospechosos

Finalmente este apartado cubre los hallazgos tras realizar el análisis de *strings* sospechosos en los payloads de los paquetes capturados.

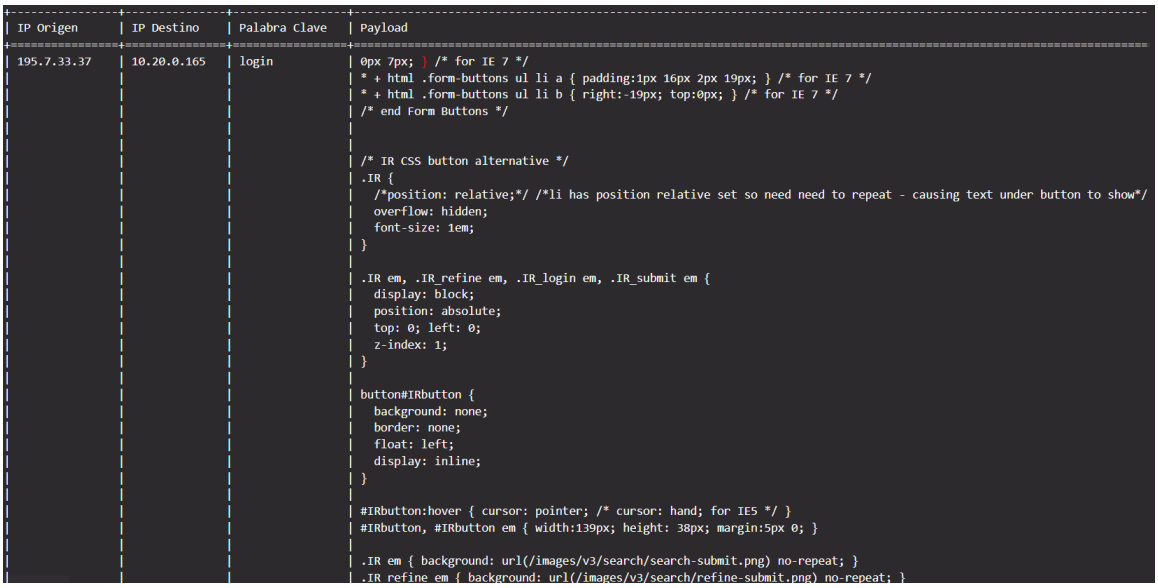


Figura 6.5: String sospechosos 1

Desde la Figura 6.5 hasta la Figura 6.10 se presenta el uso de palabras claves para encontrar tráfico malicioso dentro del contenido de los paquetes estudiados para filtrar posibles casos de exfiltración de datos.

Desde la Figura 6.5 hasta la Figura 6.10 se presenta el uso de palabras claves para encontrar tráfico malicioso dentro del contenido de los paquetes estudiados para filtrar posibles casos de exfiltración de datos.

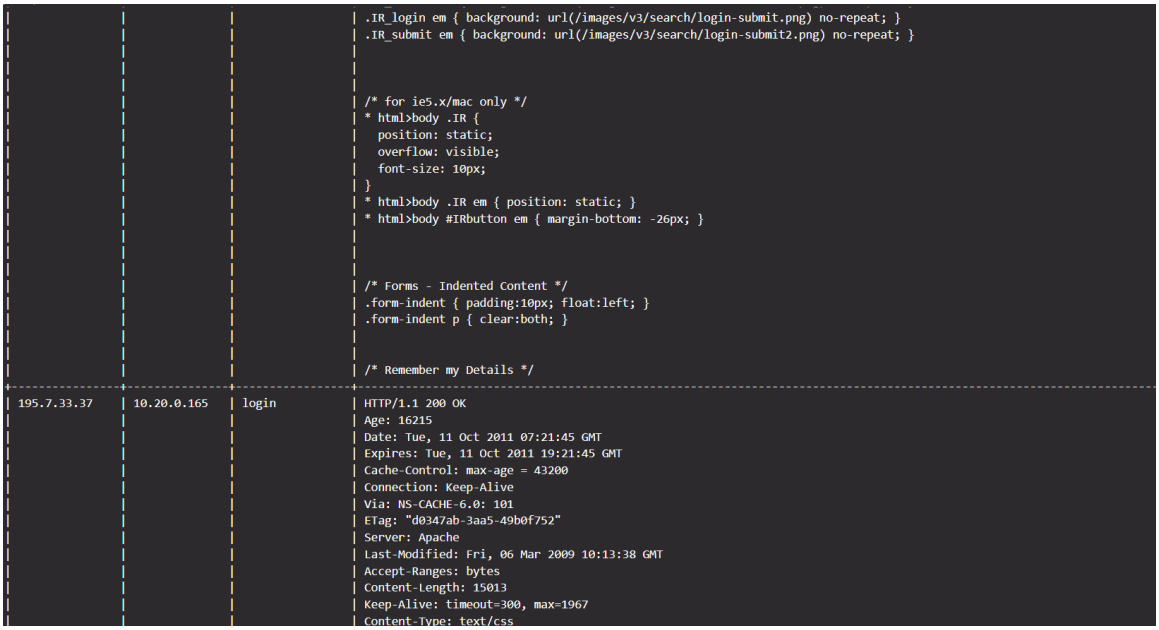


Figura 6.6: String sospechosos 2

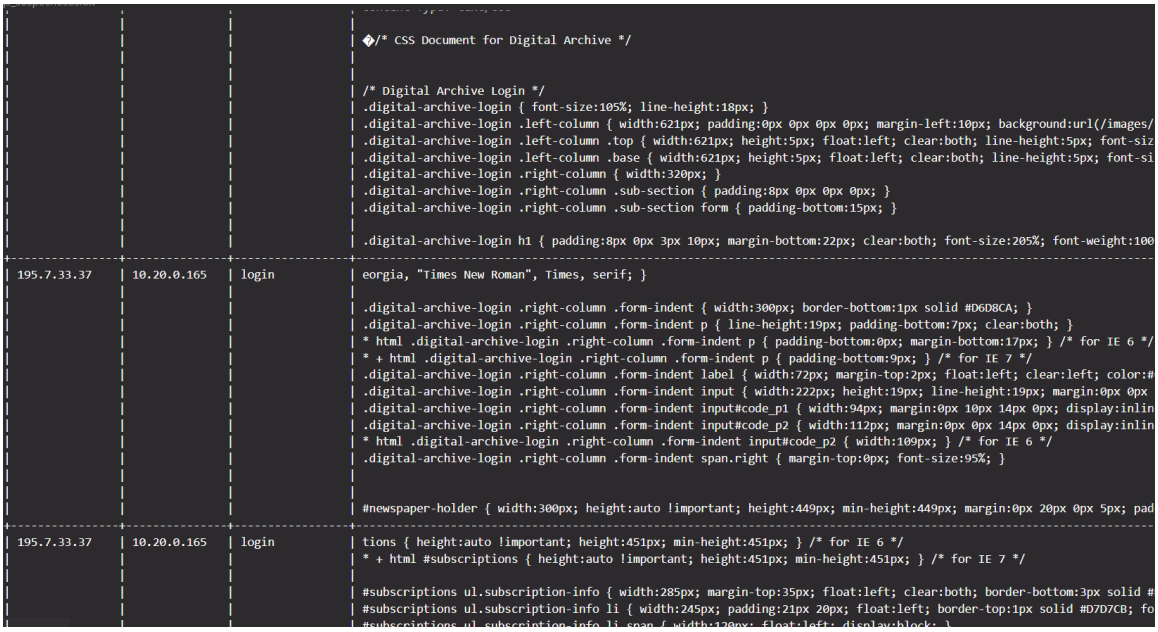


Figura 6.7: String sospechosos 3

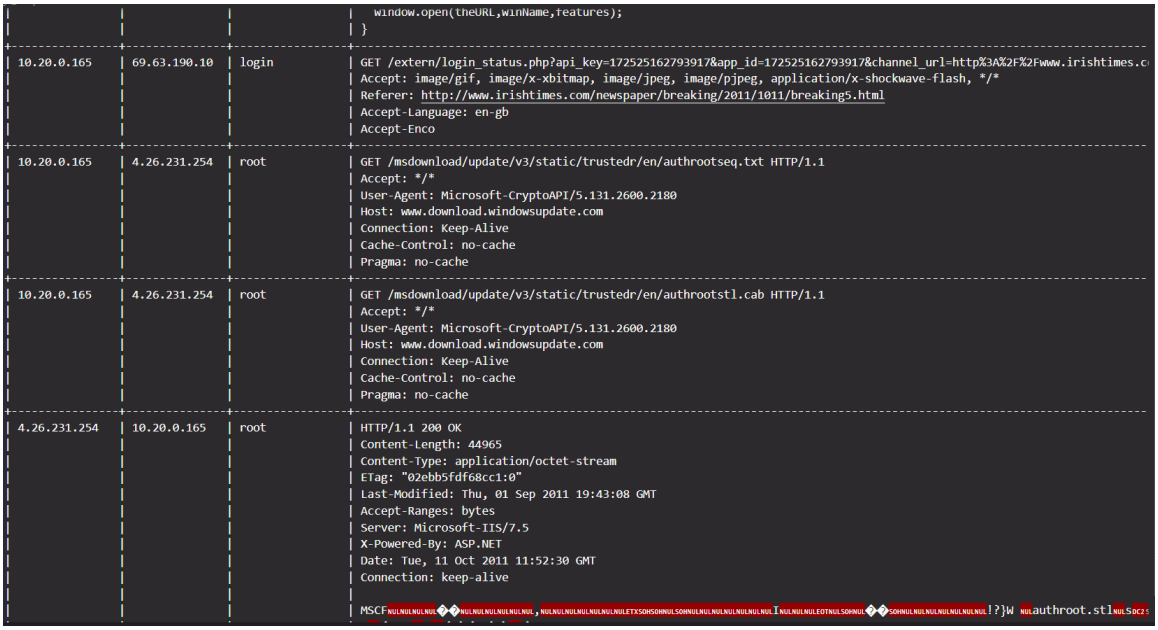


Figura 6.8: String sospechosos 4

Figura 6.9: String sospechosos 5

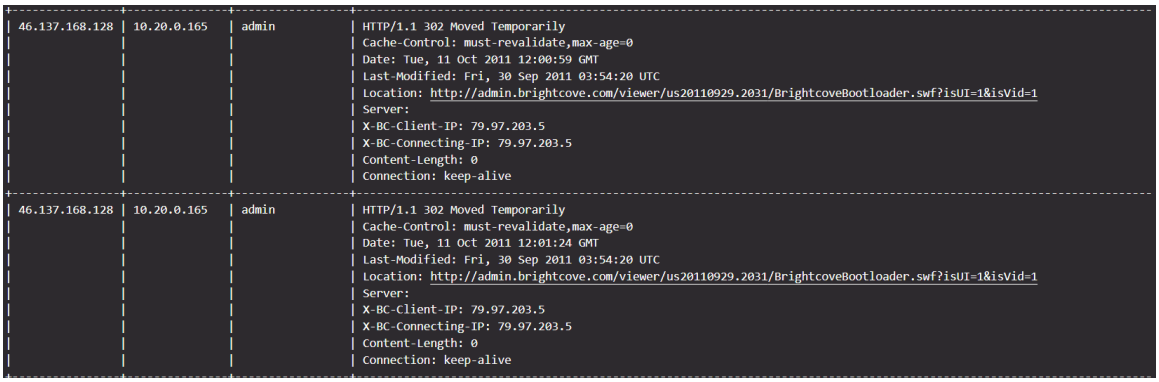


Figura 6.10: String sospechosos 6

6.3. Visualización en Wireshark

En esta sección se presentan los resultados obtenidos mediante la visualización del tráfico de red utilizando Wireshark. Esta herramienta proporcionó una inspección más detallada para analizar los anomalías detectadas con el script.

6.3.1. Análisis del puerto 8080

Este análisis involucra todo el tráfico relacionado a puerto 8080, que presentaba tráfico inusal en el proceso de detección de anomalías.

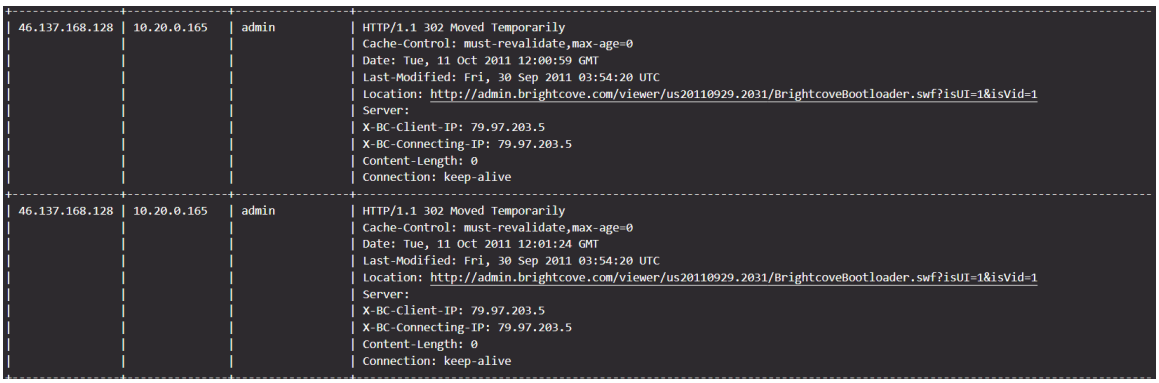
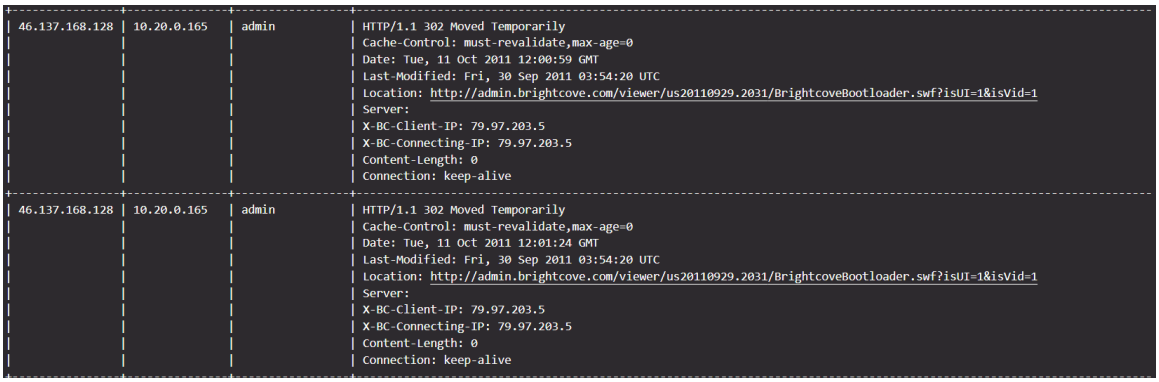


Figura 6.11: Stream TCP malicioso en el puerto 8080 parte 1

Las figuras 6.11 y 6.12 muestran el `tcp stream` de lo enviaba y recibía el puerto 8080.

6.3.2. Análisis del puerto 4444

Este análisis involucra todo el tráfico relacionado a puerto 4444, que presentaba tráfico inusal en el proceso de detección de anomalías.



46.137.168.128	10.20.0.165	admin	HTTP/1.1 302 Moved Temporarily Cache-Control: must-revalidate,max-age=0 Date: Tue, 11 Oct 2011 12:00:59 GMT Last-Modified: Fri, 30 Sep 2011 03:54:20 UTC Location: http://admin.brightcove.com/viewer/us20110929.2031/BrightcoveBootloader.swf?isUI=1&isVid=1 Server: X-BC-Client-IP: 79.97.203.5 X-BC-Connecting-IP: 79.97.203.5 Content-Length: 0 Connection: keep-alive
46.137.168.128	10.20.0.165	admin	HTTP/1.1 302 Moved Temporarily Cache-Control: must-revalidate,max-age=0 Date: Tue, 11 Oct 2011 12:01:24 GMT Last-Modified: Fri, 30 Sep 2011 03:54:20 UTC Location: http://admin.brightcove.com/viewer/us20110929.2031/BrightcoveBootloader.swf?isUI=1&isVid=1 Server: X-BC-Client-IP: 79.97.203.5 X-BC-Connecting-IP: 79.97.203.5 Content-Length: 0 Connection: keep-alive

Figura 6.12: Stream TCP malicioso en el puerto 8080 parte 2

Figura 6.13: Stream TCP malicioso en el puerto 4444 ASCII

Las figuras 6.13 muestra lo que se enviaba y recibia del puerto 4444 en formato ASCII.

Figura 6.14: Stream TCP malicioso en el puerto 4444 raw

La Figura 6.14 muestra lo que se enviaba y recibia del puerto 4444 en formato Raw.

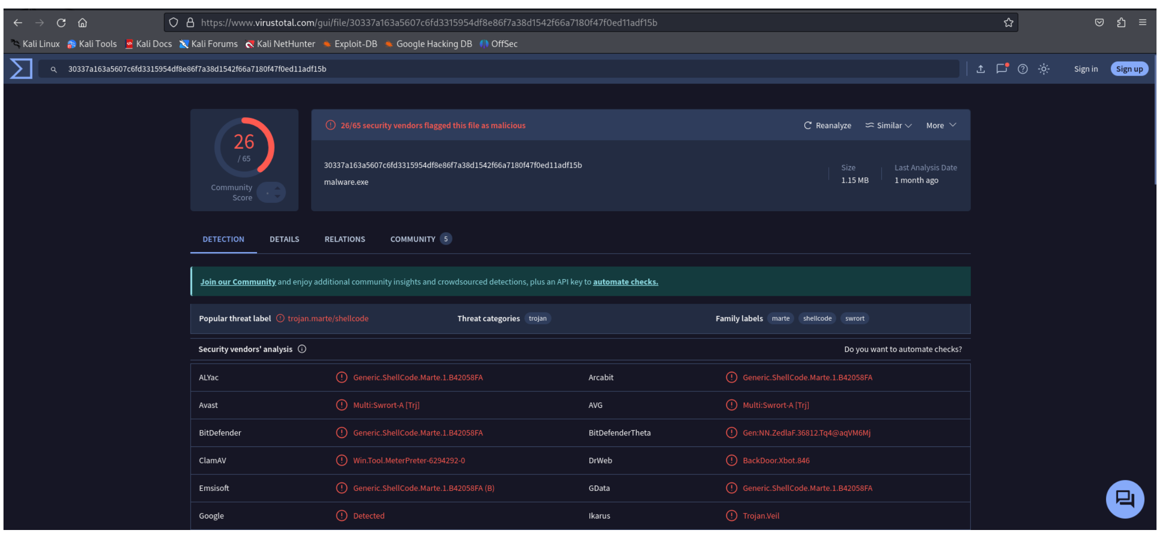


Figura 6.15: Análisis de VirusTotal del archivo recuperado

La Figura 6.15 muestra el análisis realizado en el sitio de Virus Total para determinar si era malicioso o no.

6.3.3. Conexión final

Este apartado muestra los resultados de la última conexión que se encontró de la IP atacante hacia la IP víctima después de logar obtener acesso.

Figura 6.16: Última conexión realizada por la IP atacante

La Figura 6.16 muestra el `tcp stream` de la última conexión realizada por el atacante hacía la víctima luego de obtener acceso a su equipo.

6.4. Reporte final

El reporte, presentado en el anexo 11.1, sintetiza los resultados del análisis forense, presentando de manera estructurada los patrones de tráfico malicioso y las anomalías detectadas en la red. Su objetivo es ofrecer una visión clara y concisa de los hallazgos, incluyendo actividades sospechosas como el beaconing, escaneo de puertos y tráfico DNS inusual.

CAPÍTULO 7

Discusión de resultados

7.1. Anomalías detectadas

El enfoque de este análisis consistía en optimizar el análisis forense utilizando scripts de Python para visualizar de mejor manera las comunicaciones de los dispositivos dentro de la red y gestionar los paquetes de forma más sencilla. De este modo, sería mucho más fácil detectar cualquier actividad inusual en el tráfico, en comparación con el uso exclusivo de una herramienta como Wireshark, sin saber por dónde empezar. Contar con una línea base permitía identificar anomalías en el tráfico y abordar cualquier incidencia de seguridad de manera más directa.

7.1.1. Solicitudes IP y detecciones de Beaconing

La primer característica que se analizaba en el script era cuantas conexiones o solicitudes realizaba una IP. Esto daría un buen punto de partida, ya que si en algún momento alguna dirección mostraba una actividad muy alta resaltaría entre las demás IPs. Como se puede ver en la Figura 6.1, la IP con una cantidad notoria de solicitudes es la 10.20.0.165, la cual contaba con casi 5000 solicitudes. Esto no solo resalta el volumen de actividad de esta IP, sino que también podría tratarse una exploración exhaustiva del etorno. Esto fue el primer indicio de que si había actividad maliciosa, esta IP sería la principal sospechosa.

Para continuar el análisis de solicitudes realizadas se tomó en cuenta revisar posibles ataques de `Beaconing` dentro de los paquetes. Al observar la Figura 6.2, se puede observar que nuevamente la IP 10.20.0.165 es la responsable de enviar solicitudes SYN hacia distintos destinos. Esto es una actividad inusual que podría indicar un escaneo de red o bien un ataque de beaconing, ya que las solicitudes SYN representan intentos de establecer conexiones que, si se hacen de manera continua y hacia múltiples destinos, podrían indicar actividad sospechosa o de reconocimiento.

Para visualizar de mejor manera otras posibles direcciones IP responsables de ataques de beaconing o actividades similares, se realizó un conteo del número de paquetes SYN enviados por cada una de estas direcciones. El conteo de paquetes SYN es esencial, ya que estos paquetes son el primer paso en el proceso de establecimiento de conexión TCP y su uso reiterado puede ser indicativo de intentos de escaneo o reconocimiento de red. Al revisar los resultados del análisis, como se muestra en la Figura 6.3, se encontró que solo una IP fue registrada enviando paquetes SYN: la IP 10.20.0.165.

El hecho de que una única IP haya sido detectada enviando paquetes SYN de manera activa puede ser una señal preocupante. Una posibilidad es que esta IP esté ejecutando un ataque de reconocimiento, como un escaneo de puertos, con el objetivo de identificar servicios disponibles y vulnerables en otros dispositivos de la red.

Es importante resaltar que la ausencia de más direcciones IP enviando paquetes SYN no elimina la posibilidad de que existan otras amenazas latentes en la red. Sin embargo, la concentración del tráfico SYN en una sola IP puede indicar que esta máquina actúa como nodo central de la actividad sospechosa.

7.1.2. Escaneo de puertos

Debido a la sospecha de un posible escaneo de puertos, se decidió tabular cada una de las solicitudes, considerando los siguientes elementos: IP origen, IP destino, el puerto al que se hizo la solicitud y la cantidad de solicitudes. Dentro de la Tabla 6.1 se puede observar todas las solicitudes mencionadas por la IP 10.20.0.165. Sin embargo, a primera vista, no parece haber ninguna irregularidad evidente. La mayoría de estos puertos son el 80 y el puerto 443, comúnmente usados para tráfico HTTP y TCP, respectivamente. Aunque el uso de los puertos 80 y 443 es frecuente y esperado, esto no descarta la posibilidad de actividad sospechosa. Es común que los atacantes aprovechen estos puertos estándar para evadir la detección, ya que muchas redes los mantienen abiertos para permitir el tráfico legítimo de servicios web.

A pesar de esto hay dos puertos inusuales dentro de todo este tráfico, los cuales eran el puerto 8080 y 4444. Estos puertos no están asociados a servicios comunes, lo que genera sospechas sobre la naturaleza del tráfico relacionado. El puerto 8080, aunque se utiliza en algunos casos para servidores proxy o como una alternativa al puerto 80 para servicios web, puede ser aprovechado por atacantes para evadir medidas de seguridad que supervisan únicamente puertos estándar como el 80 y 443. Por otro lado, el puerto 4444 es frecuentemente utilizado por herramientas de ataque como Metasploit, específicamente para establecer conexiones de control remoto. Este hallazgo aumenta la sospecha de que podría haber una actividad maliciosa encubierta, como un intento de obtener acceso remoto al sistema.

7.1.3. Análisis de solicitudes DNS

El análisis de solicitudes DNS permite identificar patrones de comunicación entre dispositivos de la red y dominios externos. Este tipo de análisis es clave, ya que las solicitudes DNS pueden revelar intentos de contacto con servidores maliciosos o el uso de servicios legítimos para actividades sospechosas. En la Figura 6.4 se presentan los dominios más consultados en el tráfico analizado, mostrando un patrón variado de solicitudes hacia múltiples dominios conocidos.

Entre los dominios con más solicitudes, se destacan algunos pertenecientes a Microsoft, como microsoft.com, msn.com y windowsupdate.com, lo cual sugiere tráfico relacionado con servicios legítimos de actualización y sincronización de aplicaciones. Sin embargo, también se observan dominios relacionados con publicidad y seguimiento, como doubleclick.net y scorecardresearch.com, que suelen ser utilizados para campañas de marketing, pero también podrían ser aprovechados por atacantes para evadir la detección mediante tráfico aparentemente normal.

Este análisis también fue realizado con el propósito de detectar posibles patrones relacionados con la Generación Dinámica de Dominios (GDA). Los GDAs son técnicas utilizadas por algunos tipos de malware para generar múltiples nombres de dominio en un intento de evadir bloqueos por parte de sistemas de seguridad.

7.1.4. Transferencias de datos grandes

El análisis de las transferencias de datos es esencial para identificar posibles actividades anómalas, como exfiltración de información, transferencia de archivos sospechosos o comunicaciones intensas con servidores externos. En la Tabla 6.2 se muestran las transferencias más significativas entre diferentes IPs, detallando las direcciones de origen y destino junto con la cantidad de bytes transferidos.

Lo más importante de estas transferencias de datos es que la mayoría son realizadas por la IP 10.20.0.165, indicando que este dispositivo esta involucrado en actividades inusuales en la red. La transferencia más notoria era la de 1,573,000 bytes desde 10.20.0.111 hacia 10.20.0.165 por su volumen, lo que podría indicar un movimiento lateral dentro de la red.

7.1.5. Detección de strings sospechosos

La detección de `strings` sospechosos es una técnica fundamental en el análisis forense y de seguridad, ya que permite identificar patrones de texto ocultos en el tráfico de red o en archivos capturados que podrían indicar actividad maliciosa o datos sensibles expuestos. Es por esto que para optimizar este proceso se tomó en cuenta la búsqueda de palabras claves para filtrar los `payloads` más relevantes. A pesar de lograr filtrar el contenido de los paquetes, los resultados fueron poco relevantes. Varios paquetes tenían caracteres que no se podían decodificar con `enconding` con UTF-8 o latin-1. De igual manera había muchos payloads con código que no mostraba información indicativa de un posible intruso dentro de la red.

7.1.6. ARP Spoofing

Uno de los métodos utilizados en el programa que no arrojó resultados fue el análisis de ARP Spoofing. Esta técnica consiste en detectar si una misma IP está asociada a múltiples direcciones MAC, lo que es un claro indicio de suplantación de identidad en la red. Sin embargo, al ejecutar la función encargada de identificar este comportamiento, no se detectaron anomalías: ninguna IP aparecía asociada con más de una dirección MAC.

El ARP Spoofing es una táctica comúnmente utilizada por los atacantes para interceptar, modificar o redirigir el tráfico en redes locales. Consiste en enviar respuestas ARP falsas, logrando que los dispositivos de la red asocien la dirección IP de un atacante con la dirección MAC de otro dispositivo legítimo, como un servidor o router.

7.2. Análisis en Wireshark

Teniendo identificadas las caraterísticas claves del tráfico sospechoso esta captura de paquetes se llevo a la aplicación de Wireshark para realizar un análisis manual y exhaustivo de los paquetes de red. Esta herramienta permite examinar con más profundidad los paquetes con un conjunto de herramientas especializadas, ofrenciendo resultados más precisos.

7.2.1. Puerto 8080

Uno de los puertos inusuales que se identificó en los resultados del script fue el puerto 8080. Como se mencionó anteriormente, este puerto no tiene un uso predefinido y estándar, como sucede

con otros puertos comunes, como el puerto 80 (HTTP) o el puerto 443 (HTTPS). El puerto 8080 se utiliza frecuentemente como alternativa al puerto 80 o para ejecutar servidores proxy y servicios web en aplicaciones de prueba o entornos de desarrollo. Sin embargo, su presencia en una red donde no se espera su uso puede ser un indicio de actividad sospechosa.

Utilizando *Wireshark* y sus opciones para filtrar tráfico por puerto, se analizó todo el flujo relacionado con dicho puerto. Como se puede ver en las figuras 6.11 y 6.12, todo comienza con un `request GET` hacia la ruta `/banking.htm`, que luego es redireccionado a un recurso con el mismo nombre, pero con el parámetro `?UOjiXfyAbAISuH`. Este segundo recurso devuelve un `script` de JavaScript que **decodifica una cadena hexadecimal**, almacenada en la variable `oBUHVaEknwtffNM`, a una cadena de texto mediante la función `String.fromCharCode()`. Luego, aplica un **XOR dinámico** sobre la cadena decodificada, utilizando como clave un valor obtenido del *query string* (`location.search`). Finalmente, el `script` utiliza `window.eval()` para **ejecutar dinámicamente el código descifrado**, lo que representa una amenaza potencial de **phishing** o **ataque XSS**, al permitir la ejecución de código malicioso en el navegador de la víctima. Después de esta ejecución de código se retorna un iframe que carga un archivo `.gif`. Sin embargo, la bandera Referer fue manipulada para apuntar a la persona que interactuó con el recurso malicioso principal, permitiendo un posible rastreo del comportamiento del usuario.

Esto es claramente un análisis de phishing avanzado, ya que involucra múltiples técnicas diseñadas para evadir detección y comprometer al usuario. El uso de redireccionamientos sospechosos desde una URL legítima hacia un recurso con parámetros adicionales sugiere un intento de engañar al usuario y hacer que interactúe con contenido malicioso. Además, la inclusión de un script ofuscado, que decodifica y ejecuta código dinámicamente mediante `eval()`, es una señal clara de un ataque sofisticado. La manipulación de la cabecera Referer para rastrear la actividad de la víctima y la carga de un iframe con contenido adicional refuerzan la hipótesis de que este tráfico forma parte de una campaña de phishing avanzada, con el objetivo de robar información sensible o instalar malware en el dispositivo del usuario sin levantar sospechas inmediatas.

7.2.2. Puerto 4444

El otro puerto que resaltó entre el resto del tráfico fue en el puerto 4444. Para examinar que estaba ocurriendo en esta ubicación se hizo el mismo proceso de filtrado y seguimiento de flujo. En este caso al examinar el `tcp stream` se encontró la salida presente en la Figura 6.13. Al analizar su contenido se encuentra el texto `This porgram cannot be run in DOS mode`, al igual que los encabezados `MZ` y `PE`, indicadores de que se trata de un ejecutable de Windows.

Sabiendo que se trata de un ejecutable de Windows, era necesario categorizar la funcionalidad de este ejecutable que posiblemente era malicioso. Para esto se convirtió el `payload` de un formato `ASCII` a un formato `RAW` como se ve en la Figura 6.14. Usando *Wireshark* se pudo crear un archivo con este contenido crudo.

Contando con el nuevo archivo se utilizó el portal web de Virus Total, un sitio especializado en el análisis estático de archivos para la detección de contenido malicioso. Después de someter el archivo al análisis de esta página web, se obtuvo el resultado presente en la figura 6.15. Esto nos indicaba que el ejecutable proporcionaba una consola al atacante para poder tener acceso al sistema.

7.2.3. Intruso detectado

Finalmente, lo último registrado en el archivo de captura es una conexión realizada desde la IP atacante, 10.20.0.165. Como se puede ver la figura6.16 este atacante logra establecer una comunicación con un sistema de la red, usando SMB. A pesar de que este flujo sea corto y esta ofuscado se puede encontrar la mención de `IPC$` la cual representa una conexión a recursos administrativos.

Esto puede ser un indicador de que el atacante ya conectado esta intentando escalar privilegios por alguna vulnerabilidad de SMB.

7.3. Acciones a tomar

La primera acción inmediata para contener el incidente, se debe desconectar los sistemas comprometidos de la red para evitar que el atacante continúe accediendo a recursos adicionales o propague el ataque a otros dispositivos de la red. El aislamiento de estos sistemas es fundamental para frenar cualquier movimiento lateral y preservar la integridad de los datos y servicios restantes. Adicionalmente, es necesario bloquear la dirección IP atacante, 10.20.0.165, en el firewall y otros sistemas de seguridad, impidiendo futuras conexiones desde esa fuente. Esta acción no solo mitiga el ataque en curso, sino que también previene intentos de reconexión o exfiltración de información.

Otra acción fundamental implementar un programa de concientización y capacitación del personal sobre phishing, dado que este tipo de ataques aprovecha el error humano para comprometer la seguridad de la organización. Los empleados deben ser entrenados para identificar correos electrónicos sospechosos, enlaces maliciosos, y redireccionamientos inusuales, como los detectados en este análisis. Además, se deben realizar simulaciones periódicas de phishing para evaluar el nivel de preparación y reforzar las buenas prácticas.

7.4. Documentar hallazgos

El reporte realizado proporciona una visión de las amenazas y vulnerabilidades presentes en la red doméstica analizada. Los resultados destacan la detección de patrones específicos de tráfico anómalo, como el beaconing, escaneo de puertos y tráfico DNS inusual, que son indicativos de actividad potencialmente maliciosa. Además, el hallazgo de scripts ofuscados y un ejecutable malicioso dentro del tráfico analizado a través de Wireshark, indica posibles ataques de phishing y acceso remoto no autorizado, lo que implica que los dispositivos de la red podrían estar comprometidos. La identificación de estos patrones indica la existencia de un actor externo que logró comunicarse con dispositivos de la red y explotar vulnerabilidades específicas.

CAPÍTULO 8

Conclusiones

- La aplicación de técnicas de análisis forense permitió detectar y validar intrusos en redes domésticas utilizadas en teletrabajo, destacando su eficacia en la identificación de actividades maliciosas. Los resultados revelaron patrones anómalos como beaconing y escaneo de puertos, evidenciados a través de un enfoque que combinó herramientas automatizadas con análisis detallados en Wireshark. Esta metodología no solo expuso las amenazas presentes, sino que también demostró su capacidad para fortalecer las defensas de las redes domésticas, protegiendo tanto los datos personales como los activos corporativos en entornos remotos.
- Mediante el uso de herramientas como Python y bibliotecas especializadas como dpkt, se logró una descomposición detallada y eficiente de los paquetes de red capturados. Este análisis permitió examinar cada componente del tráfico de red, como encabezados de protocolos, direcciones IP, puertos, y contenidos específicos, identificando patrones anómalos y datos atípicos que podrían indicar actividad maliciosa. Este nivel de análisis fue fundamental para comprender la naturaleza del tráfico en redes domésticas y establecer una base sólida para la detección de amenazas.
- A partir de los patrones de tráfico anómalos identificados, se desarrollaron reglas de detección específicas que optimizaron los procesos de respuesta ante incidentes de seguridad. Estas reglas no solo permitieron una reacción más rápida ante eventos sospechosos, sino que también minimizaron el impacto de posibles intrusiones en la red. La integración de estas reglas en el análisis forense proporciona una herramienta efectiva para la prevención de incidentes, marcando un avance significativo en la protección de redes domésticas.
- El análisis forense realizado resultó en una documentación detallada de las vulnerabilidades identificadas en el tráfico de red. Los hallazgos incluyeron direcciones IP maliciosas, patrones de comunicación sospechosos en puertos específicos y transferencias de datos inusuales. Este nivel de documentación, respaldado por visualizaciones claras y datos verificables, facilita no solo la comprensión de las amenazas, sino también la implementación de medidas correctivas y preventivas para fortalecer la seguridad.

CAPÍTULO 9

Recomendaciones

- Reconstruir el GIF para analizar contenido esteganográfico: Dado que el archivo GIF no se pudo recuperar y puede ser utilizado para ocultar información mediante técnicas de esteganografía, sería útil reconstruir el archivo original a partir de los paquetes capturados. Esto permitirá verificar si contiene mensajes ocultos, datos incrustados o comandos cifrados que podrían ser utilizados por un atacante para comunicar instrucciones sin ser detectado.
- Analizar el código fuente del shellcode recuperado: Otro aspecto crucial es realizar un análisis profundo del shellcode recuperado. Examinar el código fuente podría ayudar a identificar las funciones y comportamientos maliciosos que se ejecutaron en el sistema comprometido. Además, esto permitiría reconocer si el shellcode está diseñado para escalar privilegios, realizar conexiones remotas, o abrir backdoors en el sistema.

CAPÍTULO 10

Bibliografía

Bibliografía

[1] Seguridad360. (2023, Apr.) Alerta por incremento de ataques a redes domésticas en américa latina - revista seguridad 360. Accessed: 2024-03-24. [Online]. Available: https://revistaseguridad360.com/noticias/ataques-a-redes-domesticas/

[2] Naciones Unidas. (2021, Jul.) Teletrabajo en américa latina: 23 millones de personas trabajaron desde casa durante la pandemia de COVID-19. [Online]. Available: https://news.un.org/es/story/2021/07/1494012

[3] C. Osborne. (2015, May) Most companies take over six months to detect data breaches. Accessed: 2024-05-31. [Online]. Available: https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/

[4] IBM Newsroom. (2021) *IBM* report: Cost of a data breach hits record high during pandemic. Accessed: 2024-05-31. [Online]. Available: https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic?wpisrc=nl_cybersecurity202

[5] V. Anant, S. Banerjee, J. Boehm, and K. Li. (2020, Jul.) A dual cybersecurity mindset for the next normal. Accessed: 2024-05-31. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-dual-cybersecurity-mindset-for-the-next-normal

[6] I. Porcius, "The rise of telework and the struggle towards cyber security," *Fiat Iustitia*, vol. 1, no. 1, pp. 148–157, 2021, [Online]. Available: https://www.ceeol.com/search/article-detail?id=981807.

[7] M. T. Whitty, N. Moustafa, and M. Grobler, "Cybersecurity when working from home during COVID-19: considering the human factors," *Journal of Cybersecurity*, vol. 10, no. 1, Jan. 2024.

[8] D. Buil-Gil, S. Kemp, S. Kuenzel, L. Coventry, S. Zakhary, D. Tilley, and J. Nicholson, "The digital harms of smart home devices: A systematic literature review," *Computers in Human Behavior*, vol. 145, p. 107770, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0747563223001218

[9] B. Knieriem, X. Zhang, P. Levine, F. Breitinger, and I. Baggili, *An Overview of the Usage of Default Passwords*, 01 2018, pp. 195–203.

[10] O. Soluade, "Security breaches, network exploits and vulnerabilities: A conundrum and an analysis," *International Journal of Cyber-Security and Digital Forensics*, vol. 3, pp. 246–261, 01 2014.

[11] B. I. Reddy and V. Srikanth, "Review on wireless security protocols (wep, wpa, wpa2 & wpa3)," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 28–35, 07 2019.

[12] C. Smiliotopoulos, G. Kambourakis, and C. Kolias, "Detecting lateral movement: A systematic survey," *Heliyon*, vol. 10, no. 4, p. e26317, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S240584402402348X

[13] M. Vivo, L. Ke, G. Isern, and G. Vivo, "A review of port scanning techniques," *Computer Communication Review*, vol. 29, pp. 41–48, 04 1999.

[14] M. Alsharif, S. Mishra, and M. Alshehri, "Impact of human vulnerabilities on cybersecurity," *Computer Systems Science and Engineering*, vol. 40, 09 2021.

[15] A. TechPark. (2023, Apr. 06) Importance of network traffic analysis. Accessed: Nov. 05, 2024. [Online]. Available: https://ai-techpark.com/importance-of-network-traffic-analysis/

[16] R. Soepeno, "*Wireshark*: An effective tool for network analysis," 09 2023.

[17] R. Das and M. Gündüz, "Analysis of cyber-attacks in IoT-based critical infrastructures," *International Journal of Information Security*, vol. 8, pp. 122–133, 12 2019.

[18] N. Mangrulkar, A. Bhagat Patil, and A. Pande, "Network attacks and their detection mechanisms: A review," *International Journal of Computer Applications*, vol. 90, 02 2014.

[19] E. Harmoush. (2016, Jan. 11) OSI model – practical networking. [Online]. Available: https://www.practicalnetworking.net/series/packet-traveling/osi-model/

[20] C. Parker. (2019, Aug. 28) What is a TCP/IP packet? [Online]. Available: https://whatismyipaddress.com/tcp-ip

[21] A. Wijayanto, I. Riadi, Y. Prayudi, and T. Sudinugraha, "Network forensics against address resolution protocol spoofing attacks using trigger, acquire, analysis, report, action method," *Register Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 8, pp. 156–169, 07 2022.

[22] L. F. Sikos, "Packet analysis for network forensics: A comprehensive survey," *Forensic Science International: Digital Investigation*, vol. 32, p. 200892, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287619302002

[23] Y. Guo and M. Simon, "Network forensics in manet: Traffic analysis of source spoofed DoS attacks," in *2010 Fourth International Conference on Network and System Security*, 2010, pp. 128–135.

[24] Paritosh. (2023, Nov. 05) Python libraries and frameworks specifically designed for cybersecurity. [Online]. Available: https://medium.com/@paritoshblogs/python-libraries-and-frameworks-specifically-designed-for-cybersecurity-3da157dd9167

[25] S. Tonight. (2024) Analyzing networking traffic using dpkt library in python | *Studytonight*. [Online]. Available: https://www.studytonight.com/network-programming-in-python/analyzing-network-traffic

[26] S. Selvidge. (2023, Sep. 21) *PyShark*: Python packet parsing with *Wireshark*. [Online]. Available: https://celeryq.org/pyshark/

[27] O. Rosenbaum. (2022, Dec. 21) How to use *Scapy* – python networking tool explained. [Online]. Available: https://www.freecodecamp.org/news/how-to-use-scapy-python-networking/

[28] IBM. (2023, Apr. 19) Sistema de detección de intrusiones. [Online]. Available: https://www.ibm.com/es-es/topics/intrusion-detection-system

[29] C. Pastorino. (2021) Conocimientos generales: ¿cómo entender el funcionamiento de los atacantes para evadir las soluciones de seguridad como un antivirus? – seguridad de la información. [Online]. Available: https://www.uv.mx/infosegura/general/conocimientos_antivirus-3/#:~:text=Detecci%C3%B3n%20reactiva%20(o%20basada%20en%20firmas)&text=Para%20que%20una%20amenaza%20sea,amenazas%20conocidas%20como%200%2Dday

[30] Faster Capital. (2014) Ventajas y limitaciones de la detección basada en firmas - fastercapital. [Online]. Available: https://fastercapital.com/es/tema/ventajas-y-limitaciones-de-la-detecci%C3%B3n-basada-en-firmas.html#:~:text=Un%20problema%20con%20la%20detecci%C3%B3n,cuando%20no%20se%20detecta%20malware

[31] VPN Unlimited. (2024) ¿qué es la detección basada en el comportamiento? - términos y definiciones de ciberseguridad. [Online]. Available: https://www.vpnunlimited.com/es/help/cybersecurity/behavior-based-detection

[32] V. Varadaraj. (2024, Apr. 05) Todo sobre la ia y la detección de amenazas | blog de *McAfee*. [Online]. Available: https://www.mcafee.com/blogs/es-mx/internet-security/todo-sobre-la-ia-y-la-deteccion-de-amenazas/

[33] Paloalto Networks. (2015) ¿qué es un sistema de detección de intrusiones? Accessed: Nov. 05, 2024. [Online]. Available: https://www.paloaltonetworks.es/cyberpedia/what-is-an-intrusion-detection-system-ids#:~:text=Un%20IDS%20h%C3%ADbrido%20combina%20dos,el%20m%C3%A1s%20potente%20de%20todos

[34] J. Svoboda, I. Ghafir, and V. Prenosil, "Network monitoring approaches: An overview," *International Journal of Advances in Computer Networks and Its Security– IJCNS*, vol. 5, pp. 88–93, 10 2015.

[35] AWS. (2022) ¿qué es la detección de anomalías? - explicación de la detección de anomalías en machine learning - *aws*. Accessed: Nov. 05, 2024. [Online]. Available: https://aws.amazon.com/es/what-is/anomaly-detection/#:~:text=La%20detecci%C3%B3n%20de%20anomal%C3%ADas%20ofrece,en%20la%20detecci%C3%B3n%20de%20anomal%C3%ADas

[36] I. Makhdoom, M. Abolhasan, D. Franklin, J. Lipman, C. Zimmermann, M. Piccardi, and N. Shariati, "Detecting compromised IoT devices: Existing techniques, challenges, and a way forward," *Computers & Security*, vol. 132, p. 103384, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823002948

[37] M. Thwaini, "Anomaly detection in network traffic using machine learning for early threat detection," *Data and Metadata*, vol. 1, p. 34, 12 2022.

[38] Ikusi. (2022, Mar. 23) Detección de anomalías basada en el machine learning - ikusi. [Online]. Available: https://www.ikusi.com/mx/blog/deteccion-de-anomalias-basada-en-el-machine-learning/

[39] V. Shutenko. (2024, May 21) AI anomaly detection: Applications and challenges in 2024. [Online]. Available: https://www.techmagic.co/blog/ai-anomaly-detection

[40] ManageEngine. (2024) ¿qué es el análisis forense de red? - *ManageEngine* netflow analyzer. [Online]. Available: https://www.manageengine.com/latam/netflow/que-es-el-analisis-forense-de-red.html

[41] IBM. (2024, Aug. 27) Internet protocol. [Online]. Available: https://www.ibm.com/docs/en/aix/7.1?topic=protocols-internet-protocol

[42] Fortinet. (2023) What is TCP/IP in networking? | fortinet. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/tcp-ip

[43] Cloudflare. (2024) What is the user datagram protocol (UDP)? [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/

[44] ——. (2019) Why is HTTP not secure? | HTTP vs. HTTPS. [Online]. Available: https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/

[45] ——. (2023) What is DNS? | how DNS works. [Online]. Available: https://www.cloudflare.com/learning/dns/what-is-dns/

[46] Kaspersky. (2020, Nov. 07) What is an IP address & what does it mean? [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address

[47] WhatIsMyIPAddress. (2019, Aug. 28) What is a MAC address and how do i find it? [Online]. Available: https://whatismyipaddress.com/mac-address

[48] CBTnuggets. (2024) Common network ports and what they're used for. [Online]. Available: https://www.cbtnuggets.com/common-ports

[49] A. Acharya. (2023, Jul. 06) Understanding TCP and UDP : Building blocks of connectivity. [Online]. Available: https://medium.com/@abhirup.acharya009/understanding-tcp-and-udp-building-blocks-of-connectivity-ec96e208b852

[50] R. Molenaar. (2015, Jul. 15) Ipv4 packet header. Accessed: Nov. 05, 2024. [Online]. Available: https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/ipv4-packet-header

[51] W. John, S. Tafvelin, and T. Olovsson, "Passive internet measurement: Overview and guidelines based on experiences," *Computer Communications*, vol. 33, no. 5, pp. 533–550, Mar. 2010.

[52] ManageEngine. (2022) Apache: Unusual traffic patterns | *ManageEngine*. Accessed: Nov. 05, 2024. [Online]. Available: https://www.manageengine.com/products/eventlog/logging-guide/apache-traffic-control.html

[53] Imperva. (2023, Dec. 20) What is ARP spoofing | ARP cache poisoning attack explained | imperva. [Online]. Available: https://www.imperva.com/learn/application-security/arp-spoofing/

[54] Cloudflare. (2023) What is a denial-of-service (DoS) attack? [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

[55] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. A. Babar, and A. Rashid, "Data exfiltration: A review of external attack vectors and countermeasures," *Journal of Network and Computer Applications*, vol. 101, pp. 18–54, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804517303569

[56] SalvationData Technology. (2024, Jul. 09) Key examination steps for a forensic investigator. [Online]. Available: https://www.salvationdata.com/knowledge/forensic-investigator/

[57] J. L. Brunty, "Best practices for digital forensics," Department of Integrated Science, Marshall University, Huntington, WV, Tech. Rep., May 2013.

[58] EDJ. (2023, Aug. 04) Cadena de custodia digital: Todo lo que un jurista debe saber. [Online]. Available: https://www.edjxtechlawschool.com/post/cadena-de-custodia-digital-todo-lo-que-un-jurista-debe-saber

[59] SalvationData Technology. (2022, Nov. 07) Write a forensic report step by step [examples inside]. [Online]. Available: https://www.salvationdata.com/work-tips/write-a-forensic-report/

[60] J. Lindquist. (2022, Jan. 28) What is the most secure way to store digital evidence? - kustom signals inc. [Online]. Available: https://kustomsignals.com/blog/what-is-the-most-secure-way-to-store-digital-evidence

CAPÍTULO 11

Anexos

11.1. Reporte de vulnerabilidades encontradas

11.1.1. Introducción

Este informe documenta un análisis forense realizado sobre una red doméstica utilizada en teletrabajo, con el objetivo de identificar actividades maliciosas y posibles intrusos. La investigación empleó herramientas avanzadas, como Python y Wireshark, para analizar el tráfico capturado, identificando patrones sospechosos que pudieran indicar la presencia de intrusos o tráfico malicioso.

11.1.2. Metodología

Preparación del análisis: El análisis se llevó a cabo en un entorno controlado, utilizando Python junto con las bibliotecas `dpkt` y `matplotlib` para la extracción, procesamiento y visualización de datos.

Herramientas: Wireshark complementó el análisis con inspecciones manuales detalladas de los paquetes PCAP. Se configuraron filtros avanzados para seguir flujos TCP y UDP, facilitando la reconstrucción de conexiones relevantes.

11.1.3. Resultados del análisis

Hash SHA-256 del archivo de captura:

`bc4913e7823995dc6fcfeeeb1450ee391aa91b44af2bd09da4e93f79b681a4c4`

Beaconing: La dirección IP 10.20.0.165 mostró casi 5000 solicitudes, lo que sugiere un intento de comunicación repetitiva hacia un servidor de comando y control.

Escaneo de puertos: La IP 10.20.0.165 realizó múltiples conexiones a los puertos 8080 y 4444, este último asociado a herramientas de control remoto como Metasploit, lo que indica actividad sospechosa.

Solicitudes DNS: Se identificaron solicitudes a dominios publicitarios.

Transferencias de datos grandes: Se observó una transferencia significativa entre las IP 10.20.0.111 y 10.20.0.165, lo cual podría sugerir una exfiltración de datos.

Detección de strings sospechosos: El análisis de strings no mostró nada interesante o sospechoso.

11.1.4. Análisis en Wireshark

Puerto 8080: El análisis del stream TCP en el puerto 8080 reveló una secuencia sospechosa de redireccionamientos y ejecución de JavaScript ofuscado. Comienza con un request GET hacia `/banking.htm`, que luego se redirige a un recurso con un parámetro adicional, devolviendo un script que decodifica una cadena hexadecimal y utiliza `eval()` para ejecutar código dinámico. Este comportamiento representa una posible amenaza de phishing avanzado o XSS.

Puerto 4444: Al examinar el tráfico en este puerto, se encontró un ejecutable de Windows en el flujo TCP. El archivo identificado contiene encabezados `MZ` y `PE`, indicando un ejecutable de Windows posiblemente malicioso. Tras convertir el contenido de ASCII a RAW, se generó un archivo que, al ser analizado con VirusTotal, mostró que el ejecutable proporcionaba acceso de consola al atacante, permitiéndole control remoto del sistema comprometido.

11.1.5. Discusión de resultados

Anomalías detectadas: La IP 10.20.0.165 demostró ser la principal fuente de actividad sospechosa en la red, tanto en términos de solicitudes repetitivas como de escaneo de puertos inusuales. La detección de beaconing y los patrones de DNS inusuales refuerzan la sospecha de comunicación continua con servidores externos maliciosos.

Análisis manual en Wireshark: La inspección manual permitió identificar scripts maliciosos y archivos ejecutables en puertos sospechosos, reforzando la efectividad de combinar análisis automatizado con inspección detallada.

11.1.6. Acciones recomendadas

Aislamiento de dispositivos comprometidos: Desconectar de la red los dispositivos afectados, particularmente aquellos que interactúan con la IP 10.20.0.165, para detener el movimiento lateral y prevenir la exfiltración de datos.

Bloqueo de la IP sospechosa: Implementar bloqueos a la dirección IP atacante (10.20.0.165) en el firewall y en otros dispositivos de seguridad.

Concientización sobre Phishing: Implementar un programa de concientización para el personal, centrado en técnicas de phishing y redireccionamientos sospechosos, tal como se identificó en este análisis.

11.1.7. Conclusión

Los resultados del análisis indican patrones de actividad maliciosa en la red doméstica, con conexiones reiteradas en puertos inusuales y transferencias de datos anormales. La combinación de

herramientas automatizadas y análisis detallado permitió identificar múltiples amenazas, subrayando la importancia de monitorear el tráfico en redes domésticas. Reforzar la seguridad y aplicar métodos de detección en tiempo real es clave para mitigar este tipo de riesgos en redes de teletrabajo.