Práctica Cinco

Análisis de captura de tráfico en la red

Jesús Alejandro Rosales González

Seguridad en Redes - *Maestría en Ciberseguridad*

lunes, 21 de julio de 2025

Tabla de contenidos

Introducción

El presente análisis se basa en una captura de tráfico de red realizada con el complemento NPCAP y analizada mediante la herramienta Wireshark. El objetivo principal es examinar la información contenida en los paquetes capturados, incluyendo fecha y hora de transmisión, direcciones IP de origen y destino, direcciones MAC, nombres de host, y demás datos relevantes. A partir de esta información, se busca interpretar el comportamiento de la red durante el período de captura, identificar posibles patrones de comunicación, y comprender mejor el flujo de datos entre los dispositivos involucrados.

Análisis

2015-02-24-traffic-analysis-exercise.pcap

Fecha y hora de la captura

La captura de tráfico analizada se llevó a cabo el *23 de febrero de 2015*, comenzando a las *22:04:07* y finalizando a las *22:07:47*, con una duración total de aproximadamente *219.4 segundos* (poco más de tres minutos y medio).

Direcciones IP y sus respectivos *Hosts*

Durante el análisis se identificaron múltiples direcciones IP, tanto privadas, pertenecientes a la red local, como públicas, asociadas a servidores externos. Las direcciones privadas permiten identificar dispositivos internos como estaciones de trabajo o puertas de enlace, mientras que las IP públicas revelan los destinos con los que la red se comunicó a través de Internet. En muchos casos, se logró asociar estas direcciones a nombres de host mediante solicitudes DNS, lo cual facilita su identificación. En la siguiente tabla se detalla cada dirección detectada, su nombre de host (cuando estuvo disponible), y si corresponde a un rango privado o público, con el fin de clarificar el alcance y origen del tráfico observado.

Dirección IP	Dirección Host	Tipo
10.10.100.139	Stephanie-PC	private
10.10.100.1	isatap.mshome.net	private
2.16.162.26		public
65.55.56.206		public
173.194.113.164		public
173.194.113.191		public
134.170.189.4		public
204.79.197.200		public
173.194.113.175		public
119.18.61.253		public
74.125.136.95		public
69.64.49.212		public
173.194.113.183		public
2.16.162.35		public
23.10.250.48		public
207.46.101.93		public
23.10.250.18		public
194.165.16.67		public
108.58.117.78		public
89.144.2.20		public
190.93.240.200		public
54.74.60.167		public
190.93.241.200		public
194.165.16.72		public
199.182.165.25		public
162.244.34.110		public
173.239.42.219		public
69.172.216.161		public
173.194.113.179		public
69.172.216.56		public
69.172.216.58		public
199.212.255.136		public
199.212.255.224		public
93.184.220.20		public
104.67.51.113		public
5.149.250.194		public
50.7.74.66		public
8.19.136.250		public

199.212.255.139		public
69.172.216.111		public
173.194.113.168		public
46.252.196.1		public
78.129.138.60		public
199.96.57.6		public
173.194.113.173		public
173.194.113.166		public
104.67.54.166		public
92.123.196.84		public
94.31.29.153		public
179.60.192.3		public
185.31.19.196		public
199.30.80.32		public
91.225.248.129		public
78.129.138.69		public
62.51.0.35		public
37.252.162.84		public
68.232.35.121		public
23.251.136.159		public
130.211.103.172		public
62.51.0.45		public
216.178.47.73		public
173.194.113.188		public
83.138.170.197		public
182.189.225.65		public
87.248.222.176		public
2.16.162.25		public
188.226.247.5		public
37.157.6.227		public
216.38.172.159		public
179.60.192.10		public
185.29.133.33		public
216.38.172.153		public
185.31.128.232		public
63.135.90.161		public
93.184.220.12		public
148.251.24.67		public
93.184.220.74		public
23.215.60.197		public
46.51.170.181		public
23.49.14.117		public
148.251.24.69		public
173.194.113.186		public
23.215.60.227		public
104.67.35.160		public
46.228.164.11		public

194.165.16.146		public

La tabla anterior muestra las direcciones IP detectadas durante la captura, clasificadas según su tipo (pública o privada) y, cuando fue posible, el nombre de host asociado. Esta información permite vincular los flujos de tráfico con entidades específicas dentro y fuera de la red analizada.

Equipos MAC

Además del análisis de direcciones IP, se examinaron las direcciones MAC presentes en la captura. Estas direcciones permiten identificar de forma única a los dispositivos en el nivel de enlace de datos (Capa 2 del modelo OSI) y, en muchos casos, también permiten inferir el fabricante del hardware gracias a la porción OUI (Organizationally Unique Identifier). Esta información complementa el análisis, ya que puede vincular actividades específicas con tipos de dispositivos o marcas determinadas. A continuación, se presenta una tabla con las direcciones MAC detectadas y el nombre del fabricante asociado, cuando fue posible resolverlo.

Dirección MAC	*Fabricante*
28:92:4a:3b:5f:cd	Hewlett Packard
20:aa:4b:d0:c5:04	Cisco-Linksys, LLC

En la tabla se listan las direcciones MAC extraídas del tráfico capturado, junto con el nombre del fabricante del dispositivo correspondiente. Esta asociación se realizó mediante la resolución del OUI, permitiendo identificar posibles roles o funciones del hardware involucrado en la red.

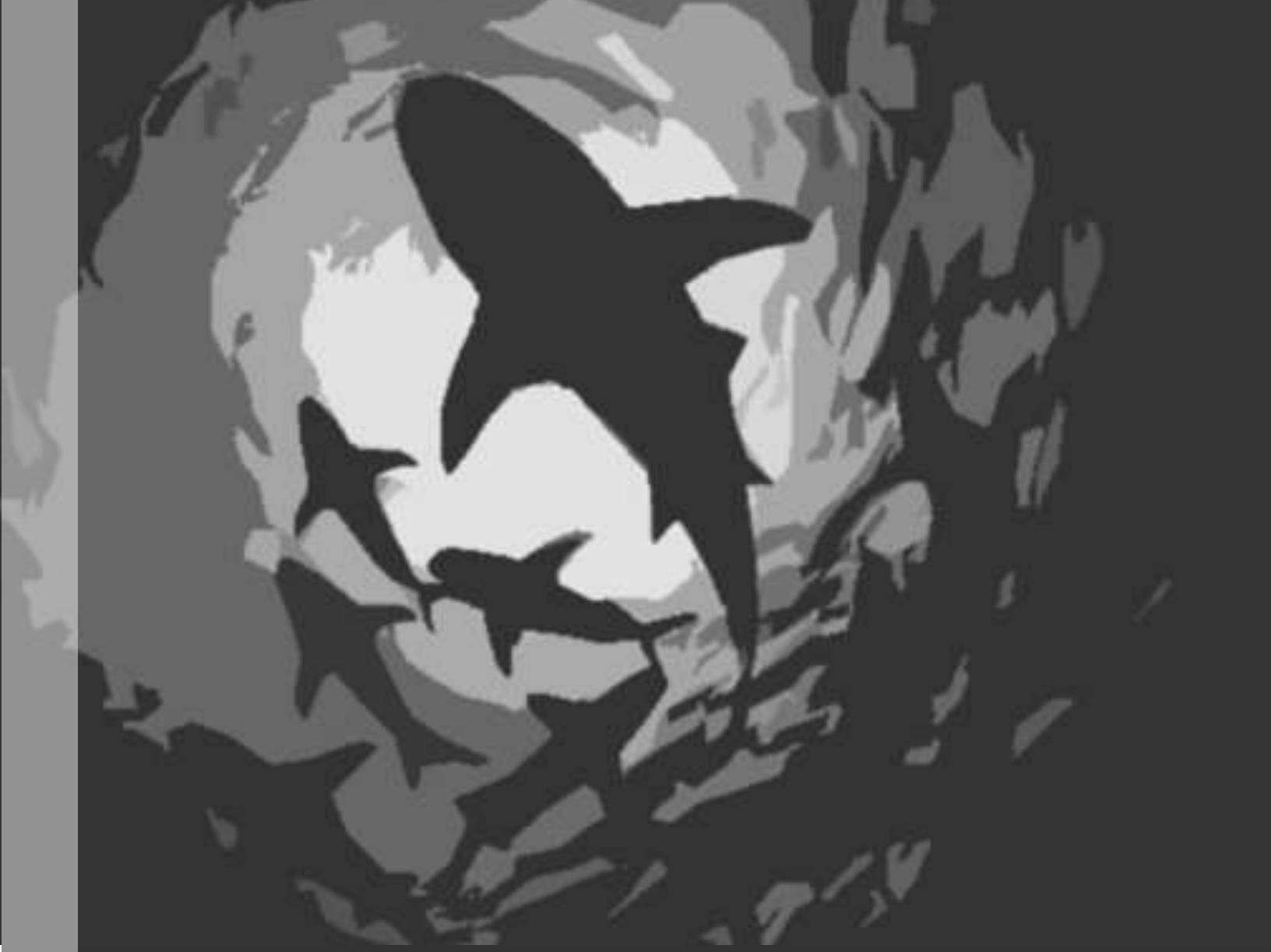
Lista de Protocolos

El análisis del tráfico capturado también se llevó a cabo a nivel de protocolos, con el objetivo de comprender la estructura y el tipo de comunicación que ocurrió durante la sesión de red. La jerarquía de protocolos revela tanto el volumen como la frecuencia de uso de cada capa o protocolo específico, desde Ethernet (Capa 2) y direcciones IP (Capa 3), hasta protocolos de transporte como TCP y UDP (Capa 4), y protocolos de aplicación como HTTP, DNS o TLS (Capa 7). A continuación, se presenta una tabla que resume la cantidad de tramas y el volumen de datos (en bytes) asociados a cada protocolo identificado durante la captura.

Protocolo	Frames	Bytes
eth	9950	7181688
ip	9950	7181688
udp	771	79166
llmnr	16	1104
nbns	36	3528
dns	698	72323

dhcp	2	684
ntp	2	180
data	17	1347
igmp	15	900
tcp	9164	7101622
http	1049	735455
data-text-lines	103	76165
tcp.segments	69	46941
media	57	43191
tcp.segments	43	28862
data	7	3552
tcp.segments	6	3193
xml	7	4001
png	51	39603
tcp.segments	40	31037
tcp.segments	6	2881
image-jfif	3	2406
tcp.segments	3	2406
image-gif	33	15153
tcp.segments	8	799
tls	770	884104
tcp.segments	214	279847
tls	183	249748
data	4	1546
tcp.segments	4	3109

La tabla resume los protocolos identificados en la captura, indicando el número total de tramas (frames) y la cantidad de datos transmitidos (bytes) por cada uno. Esta distribución permite analizar qué protocolos dominaron el tráfico y evaluar el comportamiento general de la red durante el período observado.



¿Qué ocurre?

It's another evening shift at your organization's Security Operations Center (SOC). One of the analysts is looking through some traffic that occurred while your snort-based Intrusion Detection System (IDS) was off-line. The traffic had triggered a non-specific alert of possible malicious activity from another IDS.

Durante una revisión retrospectiva del tráfico de red, desencadenada por una alerta genérica de posible actividad maliciosa, se detectó un patrón de comportamiento que merece una atención inmediata por parte de la alta gerencia. En lo que a simple vista puede parecer una rutina de navegación o verificación de conectividad, se esconde una secuencia de eventos que revela comportamientos riesgosos y posibles compromisos a la infraestructura de la compañía.

Este informe no busca únicamente describir eventos técnicos, sino ofrecer una interpretación profunda sobre lo que realmente ocurrió en nuestra red, por qué debe preocuparnos y qué pasos recomendamos tomar para mitigar cualquier amenaza subyacente.

Lo que sucedió (una historia en capas)

1. Una computadora que intenta parecer normal

A primera vista, el tráfico proveniente de la computadora "Stephanie-PC" parece legítimo: se observan consultas a Microsoft para verificar conectividad (archivo ncsi.txt), visitas a dominios como Google y otros servicios ampliamente utilizados. Esto podría tranquilizar a cualquier observador superficial.

Pero al mirar con más atención, algo no cuadra.

---

2. El disfraz del comportamiento legítimo

Entre los cientos de conexiones generadas durante apenas tres minutos, detectamos actividad que fue cuidadosamente disfrazada de tráfico normal, pero que encierra otra intención.

El sistema accedió repetidamente a servidores de Facebook sin que existiera una sesión de usuario visible ni actividad interactiva clara. También encontramos solicitudes HTTP que simulaban ser parte de sesiones de Skype —esto fue corroborado por los User-Agent en las cabeceras—, a pesar de que Skype no es un software aprobado ni necesario para las funciones del puesto.

Esto plantea una pregunta clave: ¿qué hace una computadora de trabajo enviando paquetes hacia servidores de comunicación externa enmascarados como tráfico de aplicaciones de uso personal?

---

3. Un patrón claro: comunicación hacia servidores oscuros

Más alarmante aún, identificamos conexiones a direcciones IP incluidas en listas negras globales (como Spamhaus DROP List), que catalogan infraestructura utilizada por botnets, servidores de comando y control (C2) y operadores de malware.

Durante la inspección del payload textual (contenido real de las sesiones), detectamos intentos de descarga y acceso a sitios que presentan un patrón típico de "exploración previa a la infección": comunicación con múltiples servidores, uso de técnicas de redirección encubierta (HTTP 302), y

solicitudes que buscan recursos inusuales que podrían ser utilizados para descargar código malicioso o validar conectividad antes de activar una carga útil.

---

4. El silencio del cifrado: TLS como velo de lo ilícito

También es relevante la cantidad de conexiones TLS (protocolo de cifrado) que ocurrieron hacia destinos no identificados, con anomalías en los registros del protocolo. Esto no es común en tráfico limpio. Las conexiones cifradas con errores de tipo y estructura indican dos cosas posibles:

1. Herramientas personalizadas o maliciosas que usan cifrado pero no siguen los estándares formales (común en malware).
2. Intentos de eludir inspección profunda de paquetes (DPI), al dificultar la lectura del contenido.

El uso de TLS con estructuras inválidas en este contexto no es casualidad. Se trata, probablemente, de comunicaciones deliberadamente ofuscadas, diseñadas para pasar desapercibidas ante mecanismos básicos de defensa.

---

5. Una sesión, múltiples rostros: comportamiento no humano

A nivel de comportamiento, lo observado no se alinea con una sesión de navegación humana típica. Las conexiones ocurrieron en ráfagas, a gran velocidad, con múltiples dominios alcanzados en pocos segundos y sin interacción visible entre peticiones. Esto sugiere:

- Automatización (uso de script o malware).
- Posible beaconing (un malware contactando periódicamente a su servidor de control).
- Exploración en etapas (parte de un framework malicioso en preparación).

Conclusión

Todo lo anterior apunta a una situación preocupante. Aunque no se puede confirmar sin una revisión forense completa, el patrón sugiere que la computadora afectada podría haber sido parte de una cadena de infección que no logró culminarse (por ejemplo, por falta de respuesta del servidor remoto o fallo del vector de ataque).

Este tipo de tráfico es característico de:

- ► Malware en fase de reconocimiento o exfiltración temprana.
- ► Bots intentando contactar con infraestructura de comando y control.
- ► Usuarios empleando herramientas de evasión para navegar sin ser detectados.

Referencias

- Wireshark Foundation. (2024). *Wireshark User Guide*. Recuperado de https://www.wireshark.org/docs/
- Wireshark Manuf File – Organizationally Unique Identifier (OUI) Lookup. Consultado desde: https://gitlab.com/wireshark/wireshark/-/blob/master/manuf
- «2015-02-24-traffic-analysis-exercise.pcap», archivo de captura de tráfico de red utilizado como fuente principal para el análisis. Contiene 9,950 paquetes capturados durante una sesión de aproximadamente 219 segundos, con actividad registrada el 23 de febrero de 2015.