LA CORPORACIÓN

Descargamos el zip de la plataforma de los

amigos de The Hackers Labs.

Nos aparecen 4 archivos (3 .pcap y 1 .pdf)

Leemos el pdf

evince '¡Tu primer desafío como analista de ciberseguridad!.pdf'

¡Tu primer desafío como analista de
ciberseguridad!
Es tu primer día como analista junior en el departamento de ciberseguridad de La Corporación, una organización tecnológica que maneja datos críticos y confidenciales para clientes en todo el mundo. La Corporación ha sido objeto de constantes intentos de intrusión en las últimas semanas, y el equipo de seguridad está bajo presión para evitar cualquier brecha.
Tu jefe, un veterano de la ciberseguridad conocido por su actitud directa y su poca paciencia para los novatos, te ha dado tu primera tarea. Mientras te entrega tres registros de tráfico de red capturados durante el fin de semana, te dice con una sonrisa

irónica:
"Estos logs podrían contener algo interesante… o no. Es tu trabajo averiguarlo. Si logras identificar algún incidente o actividad sospechosa, tal vez merezcas estar aquí. Si no encuentras nada… bueno, siempre hay trabajo en el departamento de soporte."
Con los ojos de tus compañeros observándote y el reloj corriendo, sabes que esta es tu oportunidad para demostrar que tienes lo necesario para formar parte de este equipo.
Objetivo
Tu tarea como nuevo analista es:
1. Analizar los tres registros(viernes.pcap, sabado.pcap, domingo.pcap)
2. Responder a preguntas clave basadas en tus hallazgos.

Necesitamos analizar los archivos de captura de tráfico de red

(viernes.pcap, sabado.pcap, y domingo.pcap) para identificar

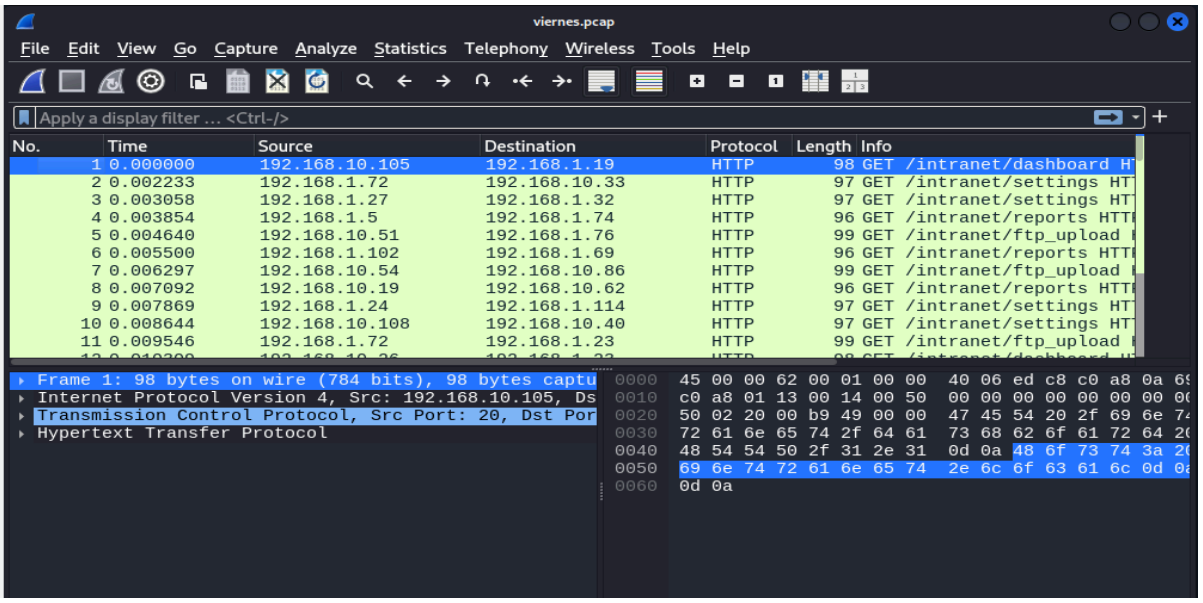
cualquier incidente sospechoso.

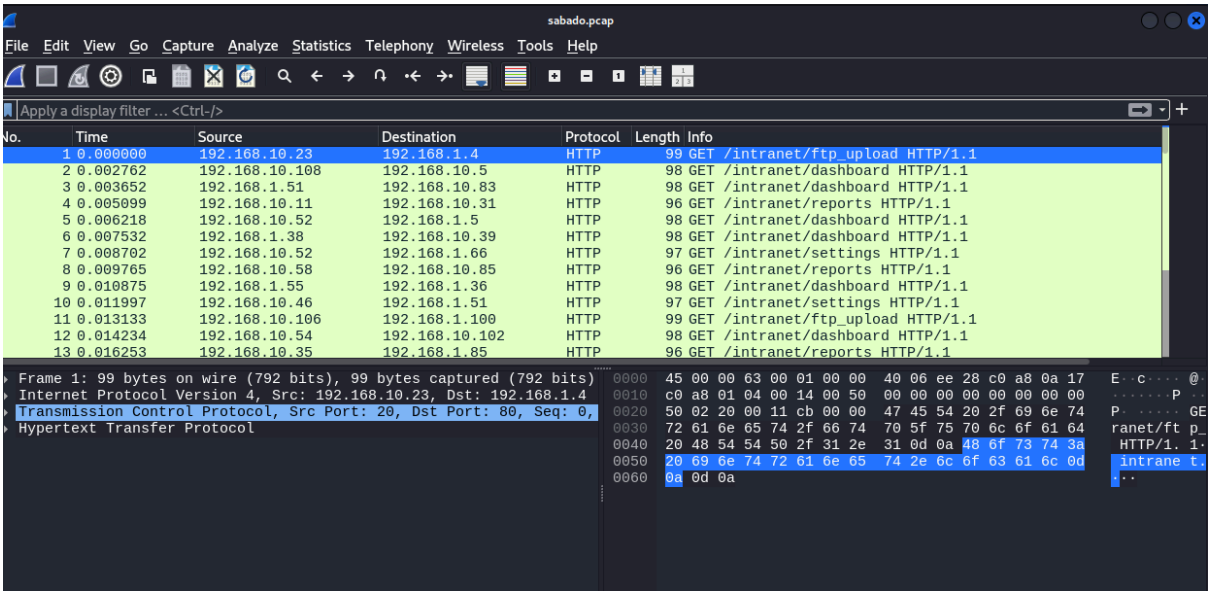
Para ello, utilizamos la herramienta wireshark

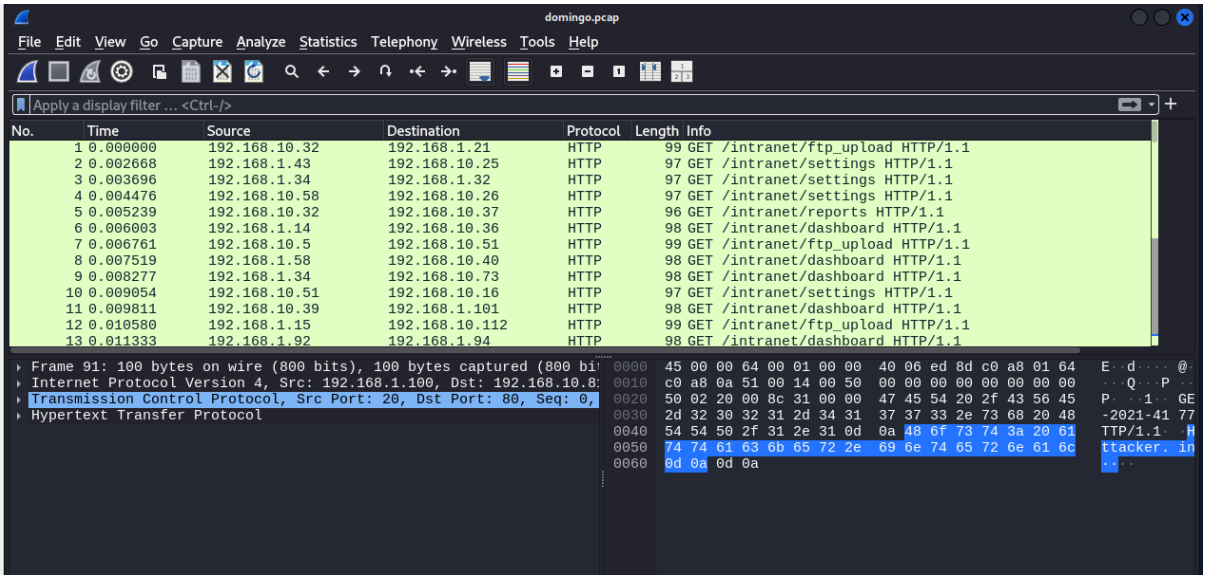
1 - Abrimos wireshark

2- Cargamos el archivo viernes.pcap

En Wireshark, ve a File > Open....







Revisando los tres .pcap lo que vamos a hacer

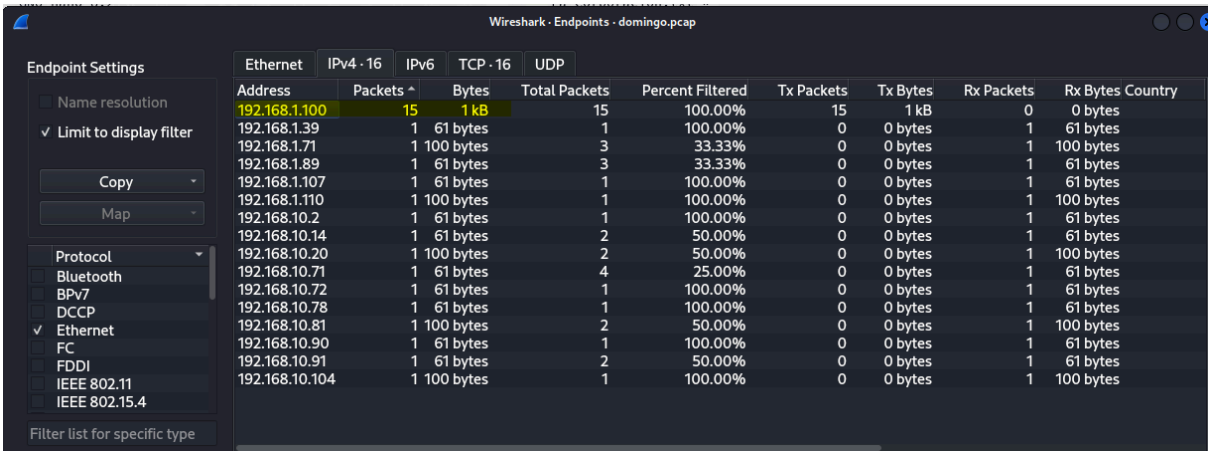
es buscar en wireshark la ip con mayor actividad

Vamos a Statistics > Endpoints.

En la ventana emergente:

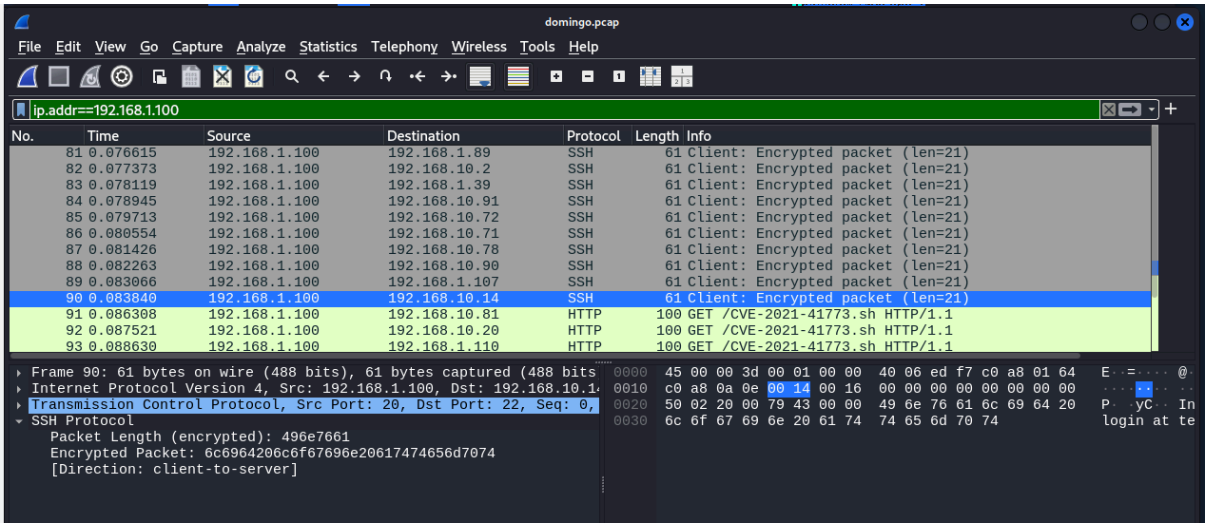
Seleccionamos la pestaña IPv4.
Ordenamos la columna Packets o Bytes de mayor a menor para identificar:
Packets: Número total de paquetes enviados/recibidos por cada IP.
Bytes: Cantidad de datos transferidos por cada IP.

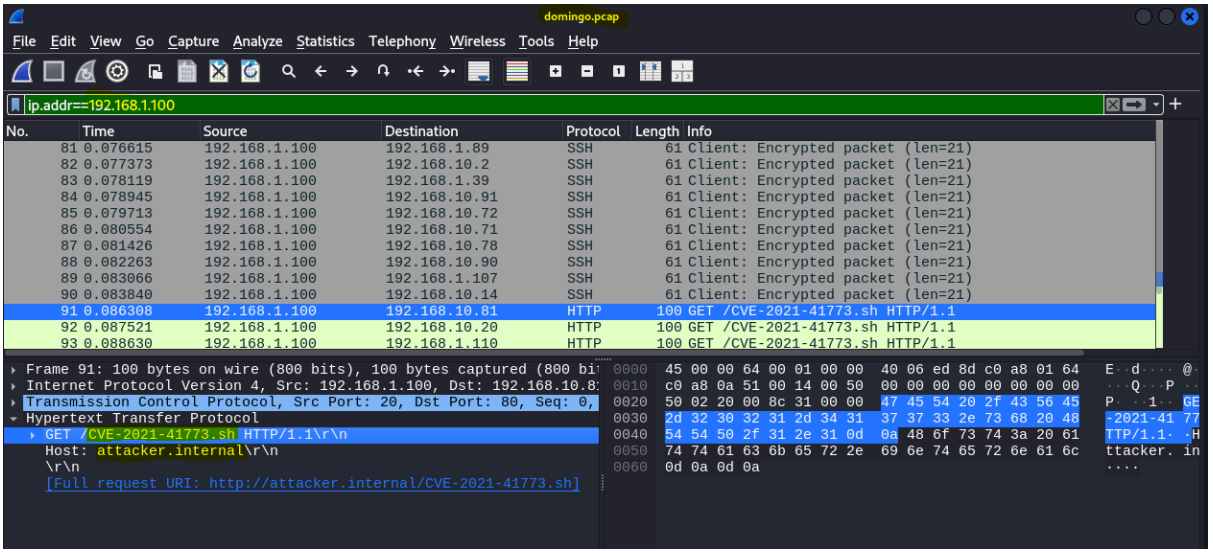
La primera IP en la lista es la que tiene más actividad.



Si usamos el filtro "ip.addr==192.168.1.100"

obtenemos todos los paquetes en que esta IP está involucrada





Podríamos hacer lo mismo con tshark

. tshark -r domingo.pcap -Y "ssh" -T fields -e ip.src | sort | uniq -c | sort -nr

```
Running as user "root" and group "root". This could be dangerous.
          10 192.168.1.100
```

. tshark -r domingo.pcap -Y "ssh" -T fields -e tcp.srcport -e tcp.dstport | sort | uniq -c | sort -nr

```
Running as user "root" and group "root". This could be dangerous.
          10 20   22
```

. tshark -r domingo.pcap -Y "http.request" -T fields -e http.host -e http.request.uri | tail -n 5

```
Running as user "root" and group "root". This could be dangerous.
attacker.internal       /CVE-2021-41773.sh
attacker.internal       /CVE-2021-41773.sh
attacker.internal       /CVE-2021-41773.sh
attacker.internal       /CVE-2021-41773.sh
attacker.internal       /CVE-2021-41773.sh
```

Propuesta de estudio scapy, tcpdump…..

🖖 Buen día.