



Examen Parcial

Module	IT - Cibersecurity
Teacher,-s	Chrystian Ruiz Diaz
Student,-s	Tobías Emanuel González Vera
Career,-s	Ingeniería en Tecnologías de la Información Empresarial
Date	@July 5, 2024
Wochentage	Freitag
Deadline	@July 5, 2024
Status	Done
Attached files	<u>Unidad_40_GuiaExamenParcialPractico.pdf</u>

Introducción

Metodología

Configurar la Red de la VM

Instalación y configuración de Apache

Monitoreo del tráfico de Red

Siendo atacado sin piedad

Configuración del Sistema de Detección de Intrusos (IDS) y Wireshark

Análisis detallado del ataque

Conclusión

Introducción

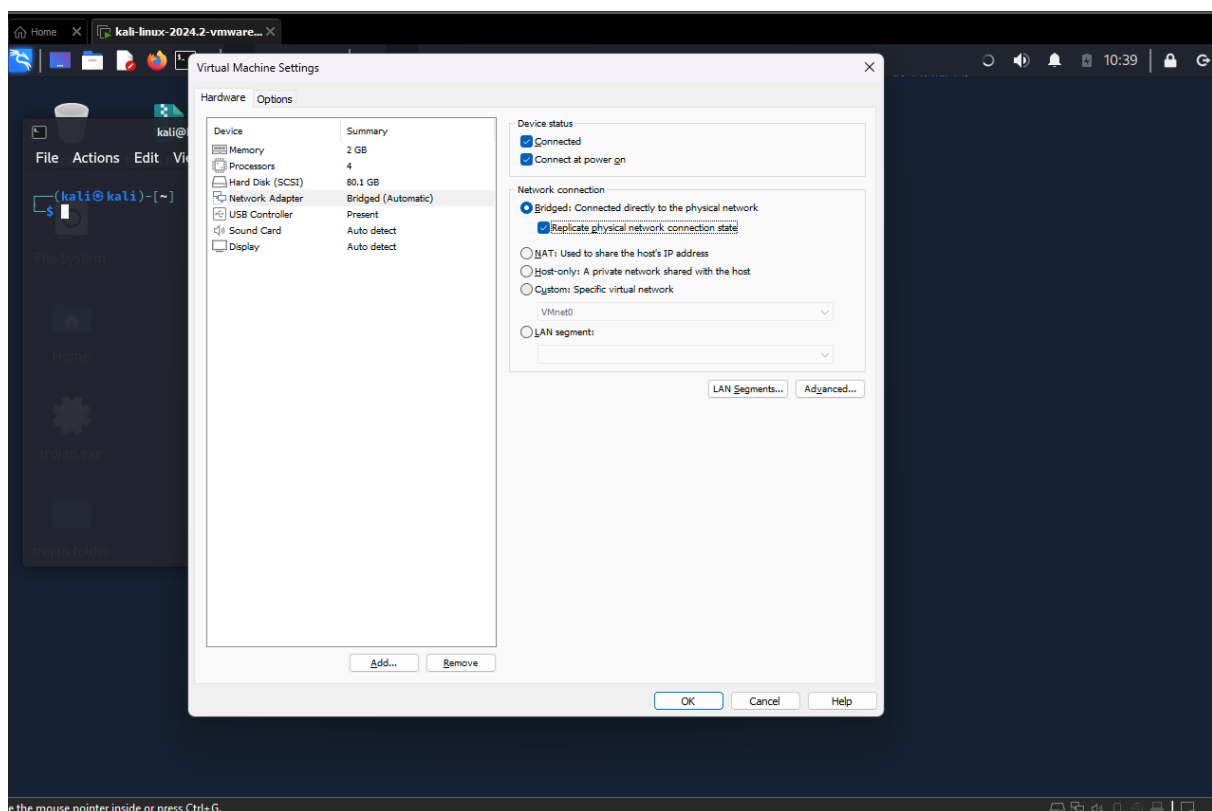
En la investigación de seguridad informática, es crucial utilizar herramientas avanzadas para detectar y analizar posibles amenazas a la integridad de los sistemas. En este caso, se emplearon Wireshark y Snort para monitorear el tráfico de red en busca de actividad sospechosa. Estas herramientas permiten capturar y analizar paquetes de datos en tiempo real, facilitando la identificación temprana de intentos de intrusión y vulnerabilidades potenciales en la red.

Esta práctica tiene como objetivo configurar y utilizar una máquina virtual (VM) Kali Linux en modo de red bridged, conectada a la red de la universidad, para analizar y responder a intentos de intrusión. Se usará Apache como servidor web para recibir intentos de login por parte de un atacante.

Metodología

Configurar la Red de la VM

Configurar el modo Bridged y obtener el IP



Al comienzo, tuve (y tuvimos) problemas para obtener el ip, ya que solo aparecía el IPv6

```
IPv6: fe80::7b99:f9df:8fde:50ef
```

Luego de poner el Bridged en mis OS Windows, pude habilitar la conexión Bridge en mi Kali

```
IPv4: 192.168.18.187
```

```
(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.18.187  netmask 255.255.254.0  broadcast
    inet6 fe80::7b99:f9df:8fde:50ef  prefixlen 64  scopeid
    ether 00:0c:29:82:7d:f2  txqueuelen 1000  (Ethernet)
    RX packets 1042  bytes 380658 (371.7 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 39  bytes 4533 (4.4 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisi

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop  txqueuelen 1000  (Local Loopback)
    RX packets 8  bytes 480 (480.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 8  bytes 480 (480.0 B)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisi
```

Instalación y configuración de Apache

Instalar Apache

```
sudo apt install apache2
```

```
(kali㉿kali)-[~]
$ # instalar apache

(kali㉿kali)-[~]
$ sudo apt install apache2
[sudo] password for kali:
apache2 is already the newest version (2.4.59-2).
The following packages were automatically installed and are no longer required:
  libdaxctl1 libndctl6 libpmem1
Use 'sudo apt autoremove' to remove them.

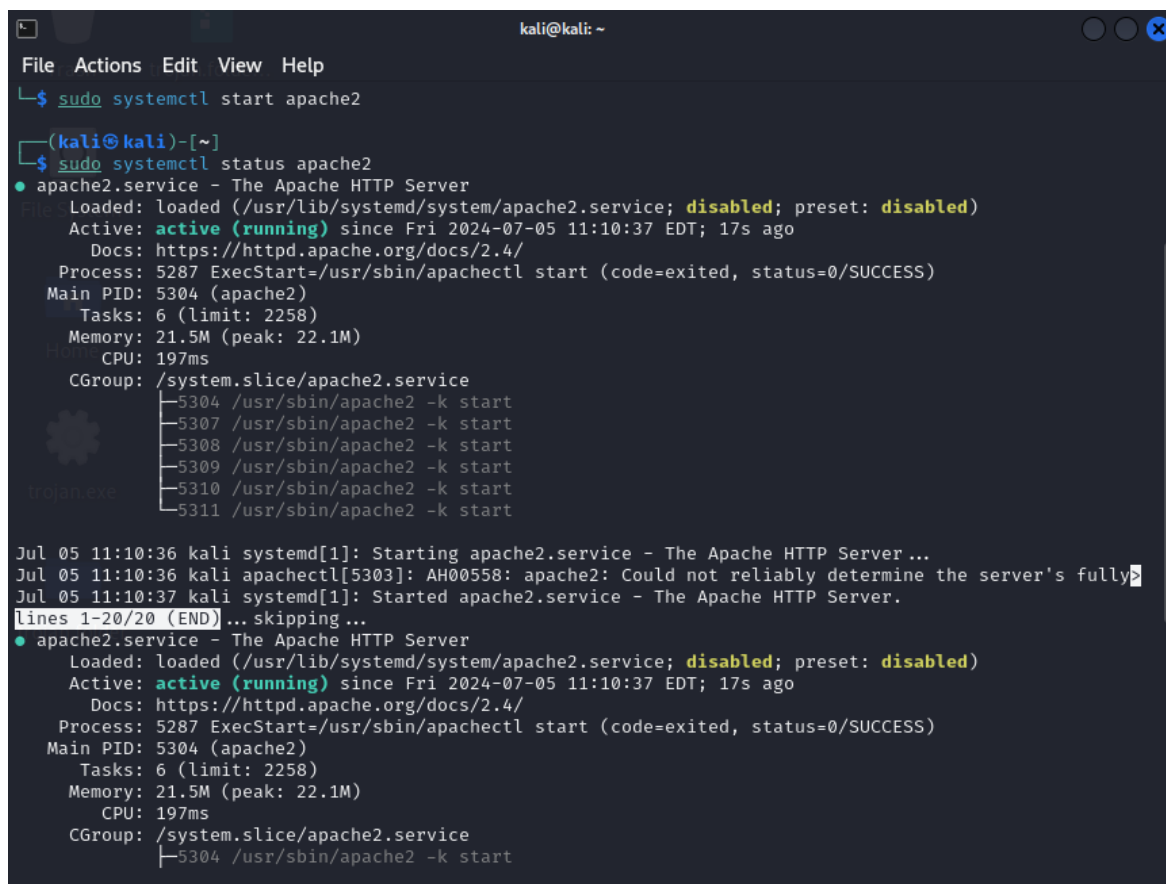
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 475
```

Iniciar el servicio Apache

```
sudo systemctl start apache2
```

Verificar el estado del servicio Apache

```
sudo systemctl status apache2
```



```
kali@kali: ~
File Actions Edit View Help
$ sudo systemctl start apache2

(kali㉿kali)-[~]
$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-07-05 11:10:37 EDT; 17s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 5287 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 5304 (apache2)
       Tasks: 6 (limit: 2258)
      Memory: 21.5M (peak: 22.1M)
         CPU: 197ms
    CGroup: /system.slice/apache2.service
            └─5304 /usr/sbin/apache2 -k start

Jul 05 11:10:36 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Jul 05 11:10:36 kali apachectl[5303]: AH00558: apache2: Could not reliably determine the server's fully
Jul 05 11:10:37 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END) ... skipping ...
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-07-05 11:10:37 EDT; 17s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 5287 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 5304 (apache2)
       Tasks: 6 (limit: 2258)
      Memory: 21.5M (peak: 22.1M)
         CPU: 197ms
    CGroup: /system.slice/apache2.service
            └─5304 /usr/sbin/apache2 -k start
```

Monitoreo del tráfico de Red

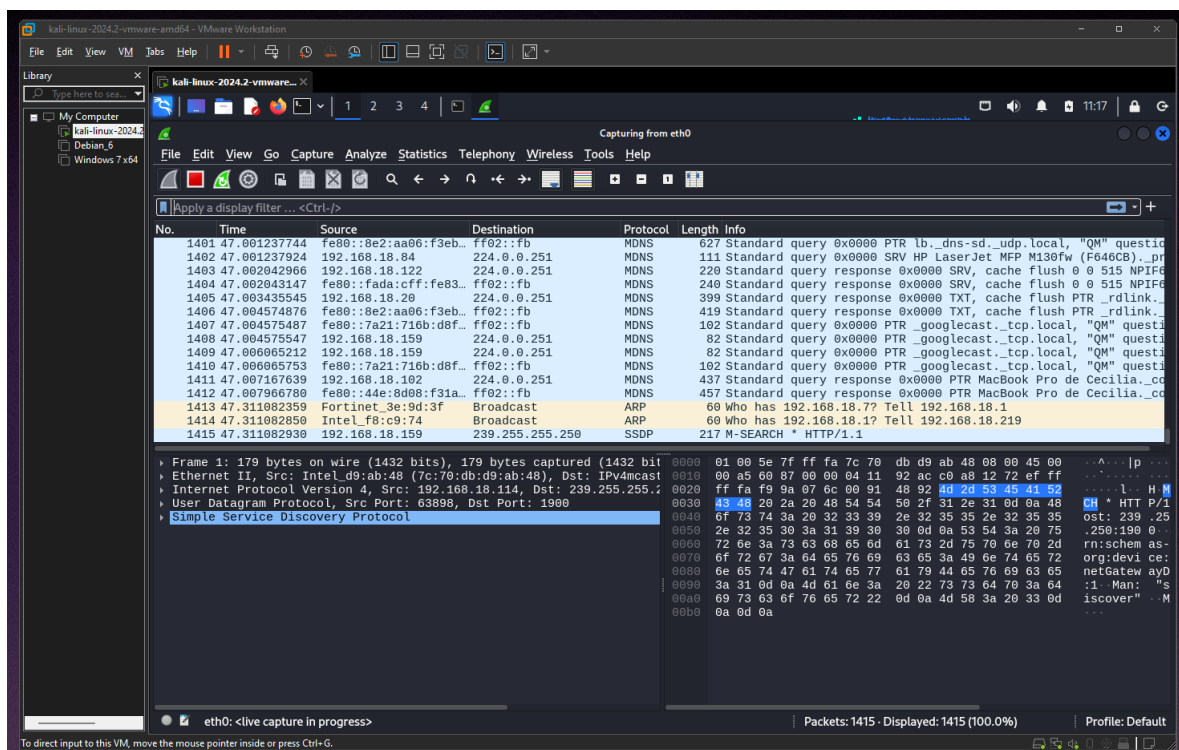
Creando un tráfico de red

```
(kali@kali)-[~]  
$ # trafico de red
```

```
(kali@kali)-[~]  
$ sudo tcpdump -i eth0 -w captura.pcap  
[sudo] password for kali:  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 65536 bytes  
4222 packets received by filter  
0 packets dropped by kernel
```

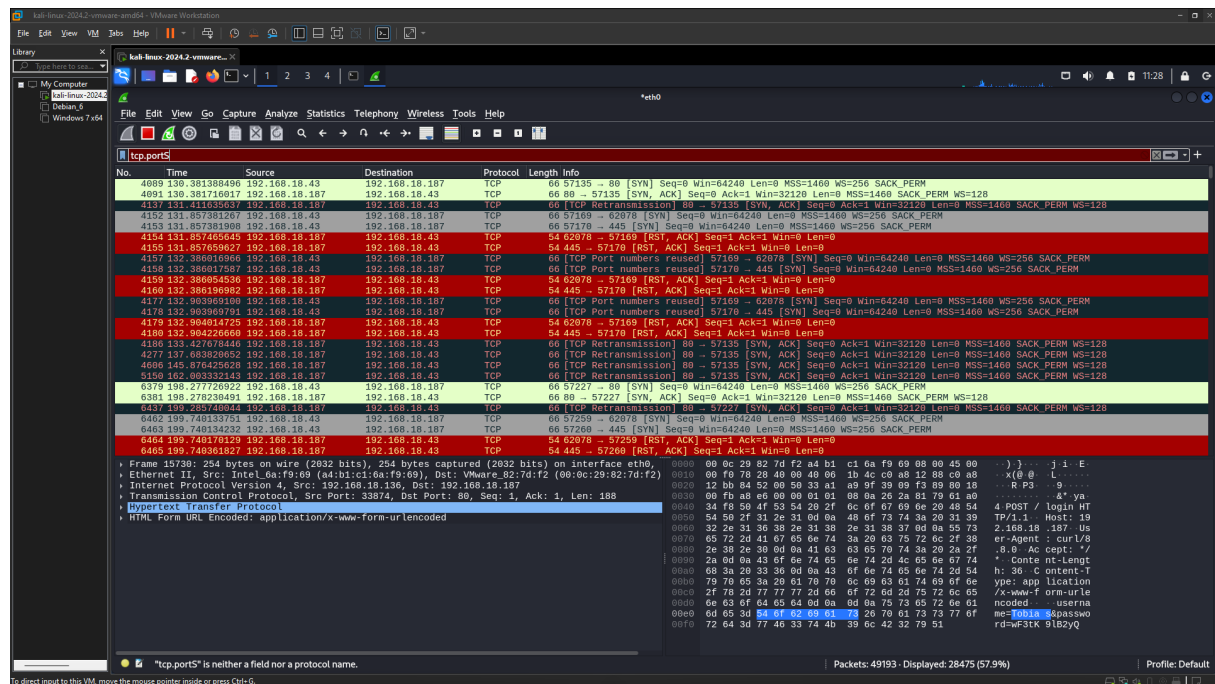


Verificando con Wireshark



@July 5, 2024 11:18 AM - esperando el ataque >:)

Siendo atacado sin piedad



Configuración del Sistema de Detección de Intrusos (IDS) y Wireshark

IDS Snort

Configurar

```
sudo nano /etc/snort/snort.conf
```

```
var HOME_NET 192.168.18.0/23
var EXTERNAL_NET !$HOME_NET
```

Reglas del Snort

dentro de:

```
sudo nano /etc/snort/snort-rules.conf
```

Reglas de Escaneo de Puertos

```
alert tcp any any -> $HOME_NET 21 (msg:"SCAN FIN"; flags:F; c
alert tcp any any -> $HOME_NET 22 (msg:"SCAN FIN"; flags:F; c
alert tcp any any -> $HOME_NET 23 (msg:"SCAN FIN"; flags:F; c
alert tcp any any -> $HOME_NET 80 (msg:"SCAN FIN"; flags:F; c
alert tcp any any -> $HOME_NET 443 (msg:"SCAN FIN"; flags:F; c
alert tcp any any -> $HOME_NET 445 (msg:"SCAN FIN"; flags:F; c
```

Reglas de Detección de Ping de la Muerte (DoS)

```
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping of Death"
alert icmp any any -> $HOME_NET any (msg:"ICMP Large ICMP Pac
```

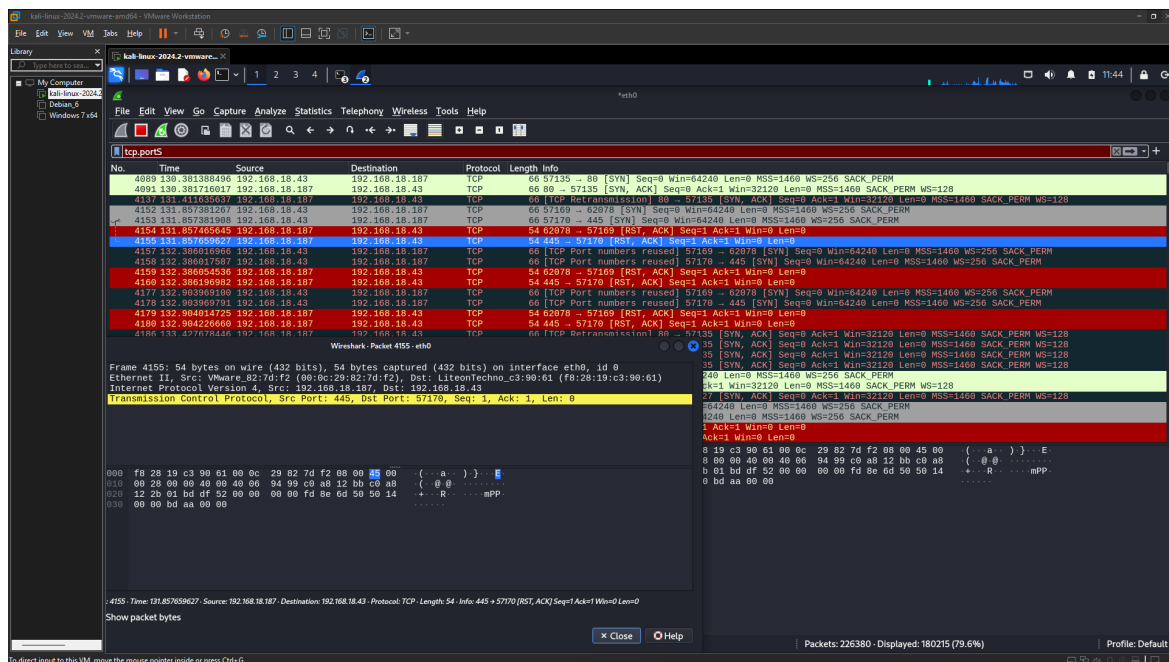
Reglas de Detección de Shellcode

```
alert tcp any any -> $HOME_NET any (msg:"Shellcode Detectado"
```

Reglas de Detección de Backdoors

```
alert tcp any any -> $HOME_NET 31337 (msg:"Backdoor Detectado"
```

Verificando el ataque en Wireshark



Análisis detallado del ataque

Tipo de ataque	Escaneo de Puertos (SYN Scan)
----------------	-------------------------------

IP de origen	192.168.18.43
Protocolo	TCP
Puerto lógico	80

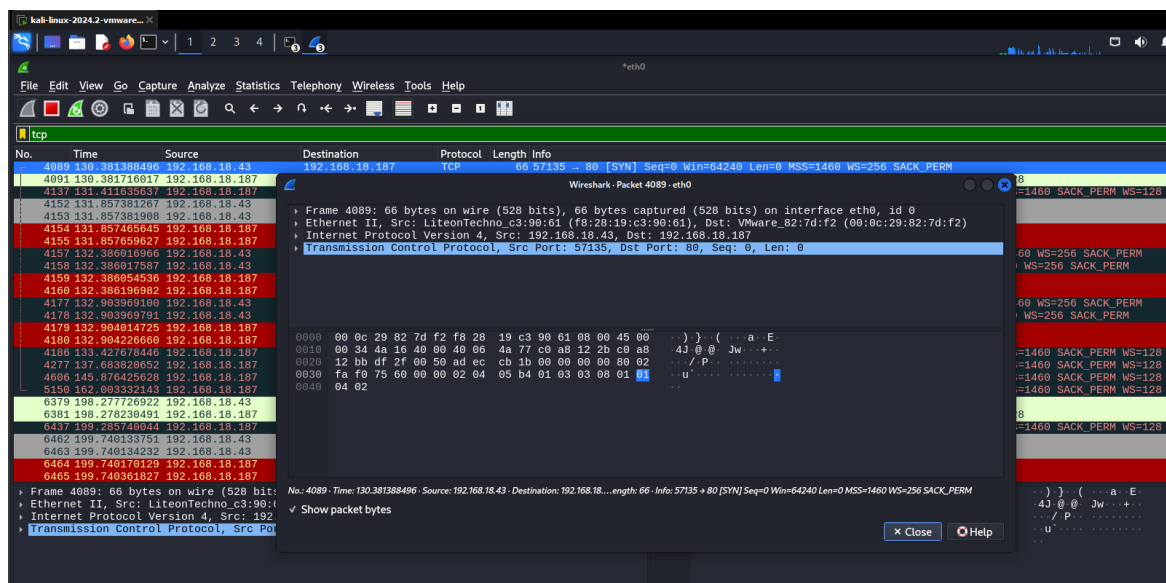
Descripción del Ataque:

- **Tipo de Ataque:** Escaneo de puertos mediante SYN (Synchronized) Scan.

El atacante intenta descubrir qué servicios están disponibles en la red, enviando paquetes SYN a varios puertos de la IP objetivo (192.168.18.187 en este caso, mi kali linux) para determinar cuáles están abiertos y pueden ser vulnerables.

- **Objetivo:** Identificar servicios vulnerables que puedan ser explotados posteriormente.

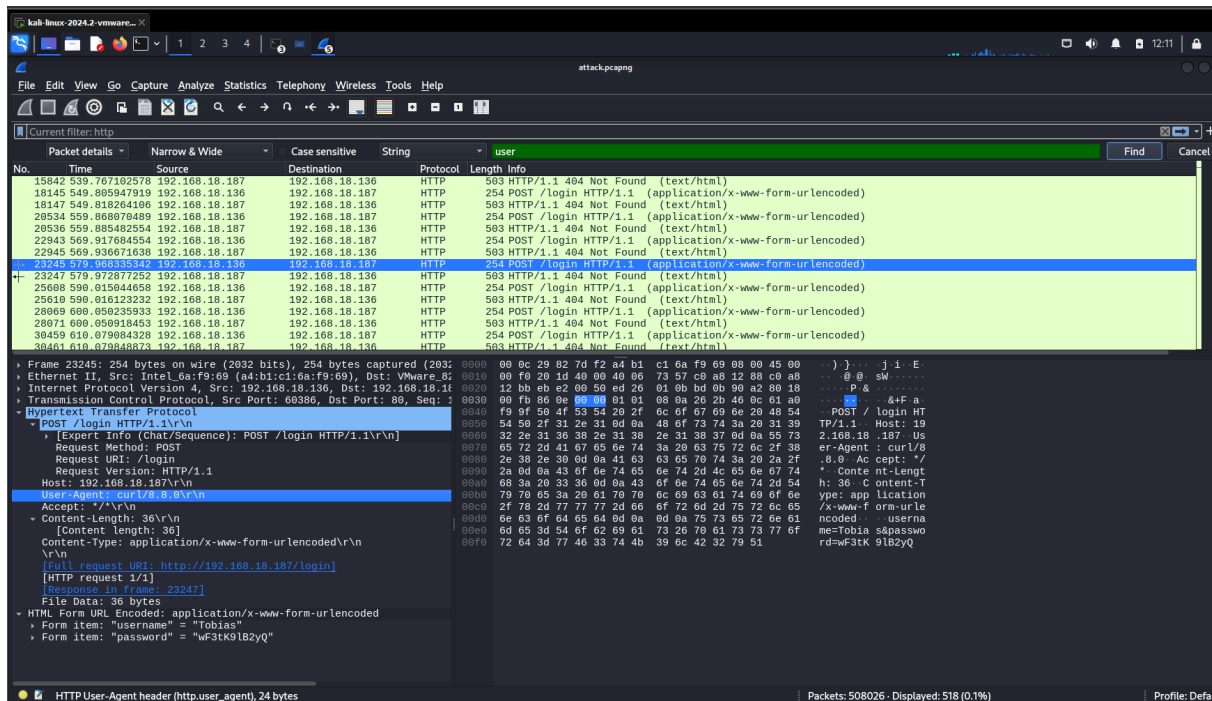
Detalles de un paquete Capturados (Wireshark):



- **Paquete**
 - **Origen:** 192.168.18.187
 - **Destino:** 192.168.18.43
 - **Protocolo:** TCP
 - **Puerto Origen:** 80
 - **Puerto Destino:** 57135
 - **Acción:** SYN-ACK (Solicitud de Sincronización-Acknowledgement)

- **Descripción:** Respuesta al paquete anterior, indicando que el puerto 80 está abierto y esperando una conexión, enviando un SYN-ACK de vuelta.

Credenciales de intento de acceso con el Sniffer



username	Tobias
password	wF3tK9lB2yQ

Conclusión

El análisis detallado de los registros obtenidos revela un patrón de escaneo de puertos SYN dirigido hacia la dirección IP interna 192.168.18.187, con múltiples intentos desde diversas fuentes. Estos eventos indican un posible intento de intrusión para identificar puntos débiles en la red. Es esencial implementar medidas de seguridad adicionales, como la configuración adecuada de firewalls y la actualización de sistemas, para mitigar riesgos y fortalecer la protección contra futuros ataques similares. El uso continuo de herramientas de monitoreo y detección de intrusiones como Wireshark y Snort es fundamental para mantener la seguridad y la integridad de los sistemas en entornos de red.