

Parte 1:

In questo laboratorio, completa i seguenti obiettivi:

- Parte 1 Preparare gli host per catturare il traffico
- Parte 2: Analizzare i pacchetti utilizzando Wireshark
- Parte 3 Visualizzare i pacchetti utilizzando tcpdump

Parte 2:

In questo laboratorio, completa i seguenti obiettivi:

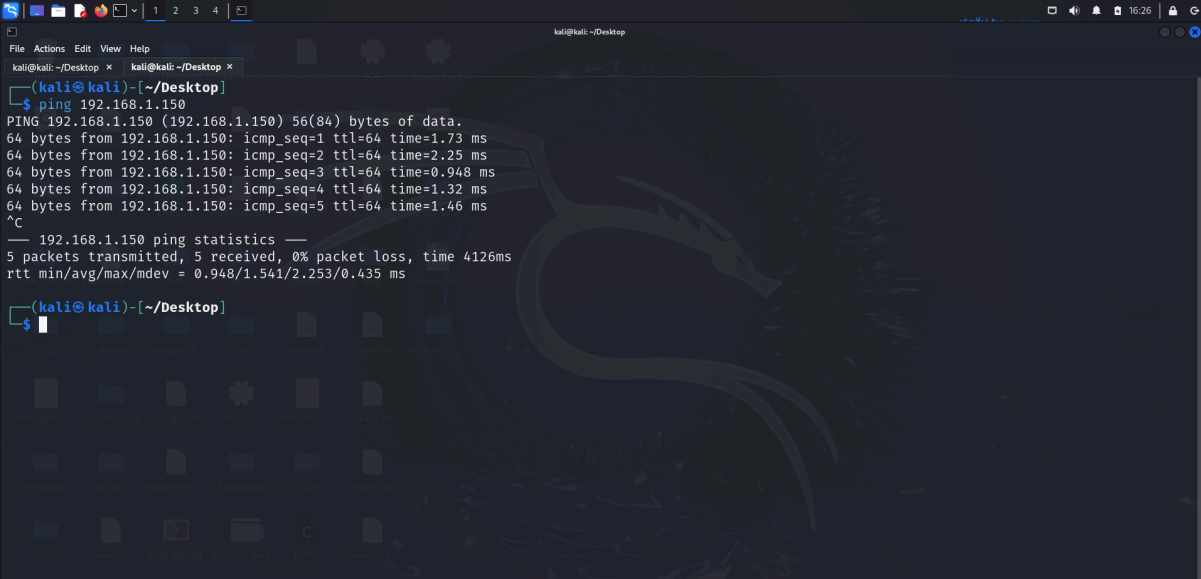
- Identificare i campi dell'intestazione TCP e il funzionamento utilizzando una cattura di sessione FTP in Wireshark.
- Identificare i campi dell'intestazione UDP e il funzionamento utilizzando una cattura di sessione TFTP in Wireshark.

Per quanto riguarda la prima parte dell'esercizio ho deciso di utilizzare due macchine

la prima macchina utilizzata è una macchina che utilizza **Kali** come sistema operativo

mentre la seconda macchina utilizzata è la macchina **cyberops workstation**.

Ho avviato entrambe le macchine e una volta accese ho verificato se ci sia connettività utilizzando il comando ping:



```
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali:~/Desktop x kali@kali:~/Desktop x
(kali@kali)~[~/Desktop]
$ ping 192.168.1.150
PING 192.168.1.150 (192.168.1.150) 56(84) bytes of data.
64 bytes from 192.168.1.150: icmp_seq=1 ttl=64 time=1.73 ms
64 bytes from 192.168.1.150: icmp_seq=2 ttl=64 time=2.25 ms
64 bytes from 192.168.1.150: icmp_seq=3 ttl=64 time=0.948 ms
64 bytes from 192.168.1.150: icmp_seq=4 ttl=64 time=1.32 ms
64 bytes from 192.168.1.150: icmp_seq=5 ttl=64 time=1.46 ms
^C
--- 192.168.1.150 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4126ms
rtt min/avg/max/mdev = 0.948/1.541/2.253/0.435 ms
(kali@kali)~[~/Desktop]
$
```

Una volta aver verificato che ci sia connettività procedo con l'enumerazione dei vari servizi utilizzando **Nmap**.

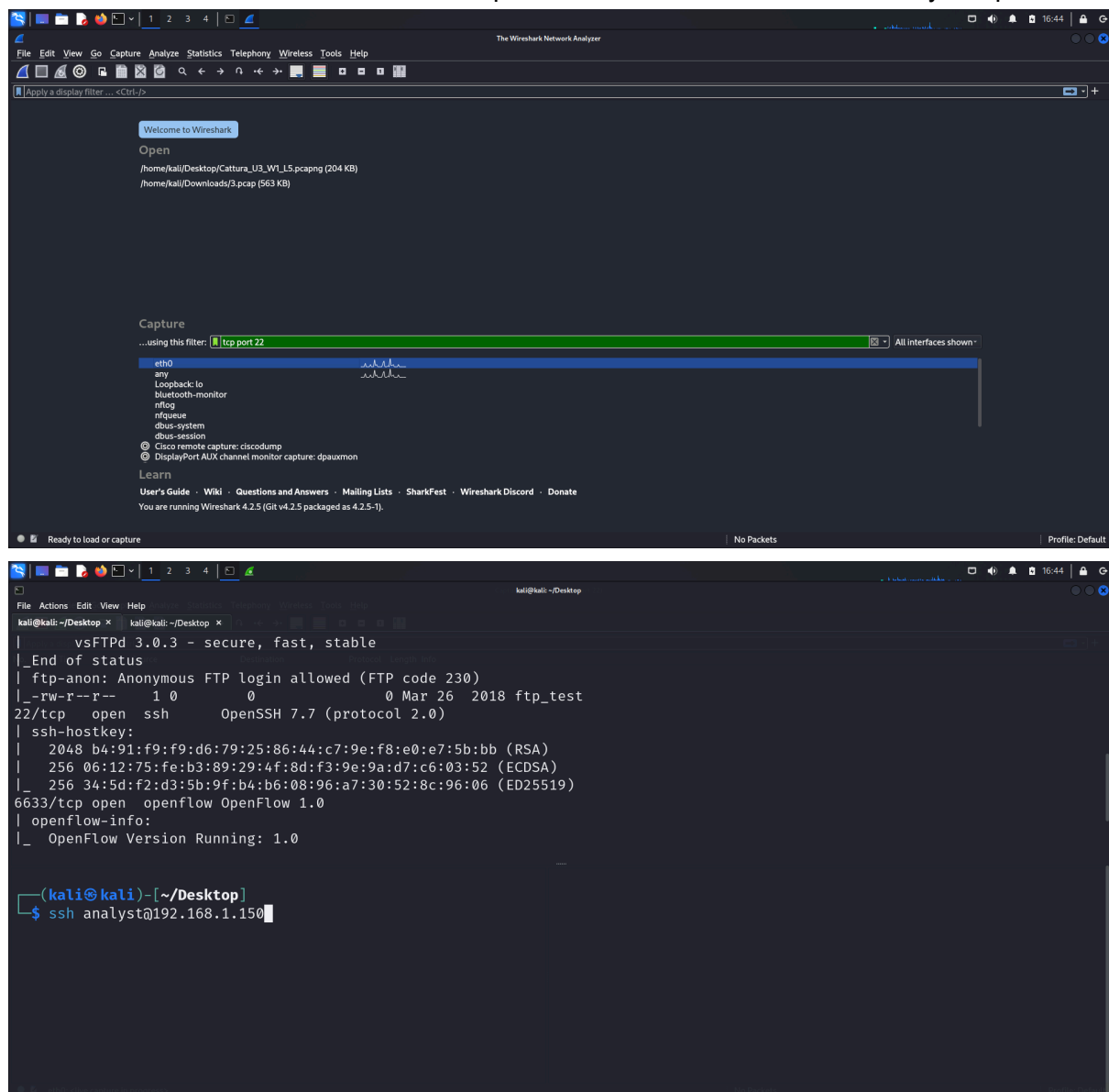
Questo passaggio anche se non richiesto dall'esercizio è stato effettuato, poichè ho deciso di strutturare la risoluzione del problema in maniera diversa rispetto a come riportato sulla guida presente all'interno del pdf

link della guida:

<https://itexamanswers.net/9-2-6-lab-using-wireshark-to-observe-the-tcp-3-way-handshake-answers.html>

Per generare il traffico da analizzare ho deciso di connettermi alla macchina **Cyberops workstation** utilizzando il servizio **ssh**.

Quindi non ci resta altro che far partire lo sniffing del traffico di rete utilizzando **Wireshark** in ascolto sull'interfaccia di rete **eth0** e connetterci alla macchina **cyberops** tramite **ssh** utilizzando le credenziali di default usate per accedere alla workstation della cyberops.



The screenshot shows a Kali Linux terminal window with the following content:

```

analyst@secOps:~$ cat /etc/passwd
vsftpd:vsftpd:1000:1000:vsftpd:/usr/sbin/ftpd:/usr/sbin/passwd
ftp-anon:Anonymous FTP login allowed (FTP code 230):1000:1000:ftp-anon:/usr/lib/ftp:/usr/sbin/passwd
_:system user:1:1:/:/bin:/usr/sbin/passwd
_1:system user:1:1:/:/bin:/usr/sbin/passwd
_2:system user:1:1:/:/bin:/usr/sbin/passwd
_3:system user:1:1:/:/bin:/usr/sbin/passwd
_4:system user:1:1:/:/bin:/usr/sbin/passwd
_5:system user:1:1:/:/bin:/usr/sbin/passwd
_6:system user:1:1:/:/bin:/usr/sbin/passwd
_7:system user:1:1:/:/bin:/usr/sbin/passwd
_8:system user:1:1:/:/bin:/usr/sbin/passwd
_9:system user:1:1:/:/bin:/usr/sbin/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/passwd
bin:x:2:2:bin:/bin:/usr/sbin/passwd
www-data:x:3:3:www-data:/var/www:/usr/sbin/passwd
sys:x:4:65534:sys:/dev:/usr/sbin/passwd
mail:x:8:8:mail:/var/mail:/usr/sbin/passwd
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/passwd

```

The terminal window title is "analyst@secOps~". The prompt is "analyst@secOps:~\$". The output of the command is displayed in a light blue font. The session ends with a successful login from 192.168.1.150.

Wireshark packet capture analysis of an Internet Protocol Version 4 (IP) packet. The packet list shows a SYN packet from 192.168.1.105 to 192.168.1.150. The packet details show the IP header and the TCP segment. The packet bytes show the raw data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.105	192.168.1.150	TCP	74	50990 → 22 [SYN] Seq=0 Win=32768 Len=0 MSS=1460 SACK_PERM TSval=4254360600 TSecr=0 WS=128
2	0.00113993	192.168.1.150	192.168.1.105	TCP	74	22 → 50990 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=3417917480 TSecr=4254360600 WS=128
3	0.00253117	192.168.1.105	192.168.1.150	SSHv2	98	Client: Protocol (SSH-2.0-OpenSSH_9.7p1 debian7)
5	0.00316081	192.168.1.150	192.168.1.105	TCP	66	22 → 50990 [ACK] Seq=1 Ack=3 Win=29056 Len=0 TSval=3417917481 TSecr=4254360602
6	0.00376136	192.168.1.150	192.168.1.105	SSHv2	87	Server: (SSH-2.0-OpenSSH_7.7)
7	0.182620483	192.168.1.105	192.168.1.150	TCP	66	50990 → 22 [ACK] Seq=3 Ack=22 Win=32128 Len=0 TSval=4254360782 TSecr=3417914960
8	0.184731486	192.168.1.105	192.168.1.150	SSHv2	1682	Client: Key Exchange Init
9	0.185203006	192.168.1.150	192.168.1.105	TCP	66	22 → 50990 [ACK] Seq=22 Ack=1569 Win=32128 Len=0 TSval=3417914967 TSecr=4254360784
10	0.193933364	192.168.1.150	192.168.1.105	SSHv2	1146	Server: Key Exchange Init
11	0.195648060	192.168.1.150	192.168.1.105	SSHv2	114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
12	0.205760005	192.168.1.150	192.168.1.105	SSHv2	446	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
13	0.208673854	192.168.1.105	192.168.1.150	SSHv2	82	Client: New Keys
14	0.255105527	192.168.1.150	192.168.1.105	TCP	66	22 → 50990 [ACK] Seq=1482 Ack=1633 Win=32128 Len=0 TSval=3417915033 TSecr=4254360808
15	0.255142023	192.168.1.150	192.168.1.105	SSHv2	118	Client: New Keys
16	0.256417109	192.168.1.150	192.168.1.105	TCP	66	22 → 50990 [ACK] Seq=1482 Ack=1677 Win=32128 Len=0 TSval=3417915034 TSecr=4254360855
17	0.257522776	192.168.1.150	192.168.1.105	SSHv2	110	Server:
18	0.257602772	192.168.1.105	192.168.1.150	SSHv2	134	Client:
19	0.266059551	192.168.1.150	192.168.1.105	SSHv2	118	Server:
20	0.307968472	192.168.1.105	192.168.1.150	TCP	66	50990 → 22 [ACK] Seq=1745 Ack=1578 Win=31872 Len=0 TSval=4254360908 TSecr=3417915045

Packet Details:

Internet Protocol Version 4, Src: 192.168.1.105, Dst: 192.168.1.150

Transmission Control Protocol, Src Port: 50990, Dst Port: 22, Seq: 1, Ack: 1, Len: 0

Source Port: 50990

Destination Port: 22

[Stream index: 0]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 2161854858

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment Number (raw): 1527159870

1600 ... Window: 32 bytes (8)

Flags: 0x00 (ACK)

Window: 251

[Calculated window size: 32128]

Window size scaling factor: 128

Checksum: 0x84b2 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

Packet bytes:

```

0000  08 00 27 14 76 5a 08 00  27 58 75 24 08 08 45 19  ...vZ...XuS...E...
0010  00 00 24 60 ad 48 00 40  46 4a 7b 03 00 01 a5 c0  ad 4k 00 01 J[...>...
0020  01 96 c7 2e 00 16 80 db  46 6a 5b 08 9c 3e 80 10  ...F[...>...
0030  00 08 fb 84 b2 00 09 01 01  08 0a fd 94 64 61 cb b9  ...d...
0040  3d 5c
  
```

Packets: 39, Displayed: 39 (100.0%)

Profile: Default

Analisi dei Dati Forniti

1. Individuazione dell'Handshake:

- Nella tabella, i primi tre **pacchetti (righe 1-3)** corrispondono alle fasi del triplo handshake.
 - Il pacchetto 1 sia un ****SYN**** dal client (`192.168.1.100`).
 - Il pacchetto 2 sia un ****SYN-ACK**** dal server (`192.168.1.150`).
 - Il pacchetto 3 sia un ****ACK**** finale dal client.
- Le lunghezze dei pacchetti (68-72 byte) sono coerenti con segmenti TCP senza payload, tipici di SYN/SYN-ACK/ACK.
 - Dal pacchetto 4 in poi, si osservano lunghezze stabili (~70 byte), suggerendo pacchetti ACK **“vuoti”** o **“keep-alive”**. Questi mantengono attiva la connessione TCP/SSH dopo l'autenticazione

```
sudo tcpdump -i eth0 'tcp -n' -c 5
```

[illegible]

```

analyst@secOps:~$ ssh analyst@192.168.1.150
analyst@192.168.1.150's password:
Last login: Tue Jan 28 13:00:15 2025 from 192.168.1.165
[kali@kali:~]$ exit
logout
Connection to 192.168.1.150 closed.

(kali@kali)~[~/Desktop]
$ ssh analyst@192.168.1.150
analyst@192.168.1.150's password:
Last login: Tue Jan 28 13:03:12 2025 from 192.168.1.165
[kali@kali:~]$

```

Risultati del tcpdump:

```
(kali㉿kali)-[~/Desktop]
└─$ sudo tcpdump -i eth0 'tcp' -n -c 5
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:35:03.149479 IP 192.168.1.165.39142 > 192.168.1.150.22: Flags [S], seq 4239369034, win 32120, options [mss 1460,sackOK,TS val 4264565622 ecr 0
,nop,wscale 7], length 0
19:35:03.151467 IP 192.168.1.150.22 > 192.168.1.165.39142: Flags [S.], seq 2171300752, ack 4239369035, win 28960, options [mss 1460,sackOK,TS val
3428122475 ecr 4264565622,nop,wscale 7], length 0
19:35:03.151529 IP 192.168.1.165.39142 > 192.168.1.150.22: Flags [.], ack 1, win 251, options [nop,nop,TS val 4264565624 ecr 3428122475], length
0
19:35:03.152199 IP 192.168.1.165.39142 > 192.168.1.150.22: Flags [P.], seq 1:33, ack 1, win 251, options [nop,nop,TS val 4264565624 ecr 342812247
5], length 32: SSH: SSH-2.0-OpenSSH_9.7p1 Debian-7
19:35:03.153955 IP 192.168.1.150.22 > 192.168.1.165.39142: Flags [.], ack 33, win 227, options [nop,nop,TS val 3428122478 ecr 4264565624], length
0
5 packets captured
5 packets received by filter
0 packets dropped by kernel

(kali㉿kali)-[~/Desktop]
└─$
```