



Cyber Security & Ethical Hacking

Laboratorio giorno 2 – Cisco CyberOps

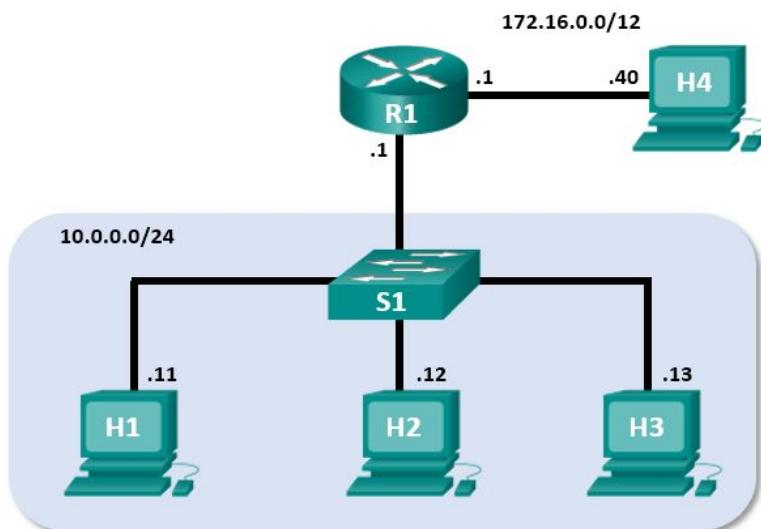


Usare Wireshark per Osservare l'Handshake a 3 Vie TCP



Usare Wireshark per Osservare l'Handshake a 3 Vie TCP

Topologia Mininet



Risorse Richieste: Macchina virtuale CyberOps Workstation

Obiettivi

- Parte 1: Preparare gli Host per Catturare il Traffico
- Parte 2: Analizzare i Pacchetti usando Wireshark
- Parte 3: Visualizzare i Pacchetti usando tcpdump

Contesto / Scenario

In questo laboratorio, userai Wireshark per catturare ed esaminare i pacchetti generati tra il browser del PC che utilizza il protocollo HTTP (HyperText Transfer Protocol) e un server web, come www.google.com. Quando un'applicazione, come HTTP o FTP (File Transfer Protocol), si avvia per la prima volta su un host, TCP utilizza l'handshake a tre vie per stabilire una sessione TCP affidabile tra i due host. Ad esempio, quando un PC utilizza un browser web per navigare in internet, viene avviato un handshake a tre vie e viene stabilita una sessione tra l'host del PC e il server web. Un PC può avere più sessioni TCP attive simultaneamente con vari siti web.



ISTRUZIONI

Parte 1: Preparare gli Host per Catturare il Traffico

- a. Avviare la VM CyberOps. Accedere con nome utente analyst e password cyberops.
- b. Avviare Mininet.

```
[analyst@sec0ps ~]$ sudo lab.support.files/scripts/cyberops_topo.py
```

- c. Avviare gli host H1 e H4 in Mininet.

```
*** Starting CLI:  
mininet> xterm H1  
mininet> xterm H4
```

- d. Avviare il server web su H4.

```
[root@sec0ps analyst]# /home/analyst/lab.support.files/scripts/reg_server_start.sh
```



e. Per motivi di sicurezza, non è possibile eseguire Firefox dall'account utente root. Sull'host H1, usare il comando su (switch user) per passare dall'utente root all'account utente analyst:

```
[root@sec0ps analyst]# su analyst
```

f. Avviare il browser web su H1. Ci vorrà qualche momento.

```
[analyst@sec0ps ~]$ firefox &
```

g. Dopo l'apertura della finestra di Firefox, avviare una sessione tcpdump nel terminale Node: H1 e inviare l'output a un file chiamato capture.pcap. Con l'opzione -v, è possibile osservare l'avanzamento. Questa cattura si fermerà dopo aver catturato 50 pacchetti, poiché è configurata con l'opzione -c 50.

```
[analyst@sec0ps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap
```

h. Dopo l'avvio di tcpdump, navigare rapidamente a 172.16.0.40 nel browser web Firefox.



Parte 2: Analizzare i Pacchetti usando Wireshark

Passo 1: Applicare un filtro alla cattura salvata.

- Premere INVIO per vedere il prompt. Avviare Wireshark su Node: H1. Fare clic su OK quando viene richiesto l'avviso riguardante l'esecuzione di Wireshark come superutente.

```
[analyst@secOps ~]$ wireshark-gtk &
```

- In Wireshark, fare clic su File > Open. Selezionare il file pcap salvato situato in /home/analyst/capture.pcap.
- Applicare un filtro tcp alla cattura. In questo esempio, i primi 3 frame rappresentano il traffico di interesse.

The screenshot shows the Wireshark interface with a packet list. The filter bar at the top has 'tcp' typed into it. The packet list table has columns: No., Time, Source, Destination, Protocol, Length, and Info. There are four visible rows of data:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	58716 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM
2	0.000081	172.16.0.40	10.0.0.11	TCP	74	80 → 58716 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 TSval=38645
3	0.000082	10.0.0.11	172.16.0.40	TCP	66	58716 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=38645
4	0.000194	10.0.0.11	172.16.0.40	HTTP	356	GET /favicon.ico HTTP/1.1



Passo 2: Esaminare le informazioni all'interno dei pacchetti, inclusi indirizzi IP, numeri di porta TCP e flag di controllo TCP.

a. In questo esempio, il frame 1 è l'inizio dell'handshake a tre vie tra il PC e il server su H4. Nel riquadro dell'elenco dei pacchetti (sezione superiore della finestra principale), selezionare il primo pacchetto, se necessario.

b. Fare clic sulla freccia a sinistra del Transmission Control Protocol nel riquadro dei dettagli del pacchetto per espanderlo ed esaminare le informazioni TCP. Localizzare le informazioni sulla porta di origine e destinazione.

c. Fare clic sulla freccia a sinistra dei Flags. Un valore di 1 significa che il flag è impostato. Localizzare il flag impostato in questo pacchetto.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	58716 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM
2	0.000081	172.16.0.40	10.0.0.11	TCP	74	80 → 58716 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM
3	0.000082	10.0.0.11	172.16.0.40	TCP	66	58716 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=38645 TSecr=1
4	0.000194	10.0.0.11	172.16.0.40	HTTP	356	GET /favicon.ico HTTP/1.1

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 ▶ Ethernet II, Src: a6:a1:15:2c:d8:de (a6:a1:15:2c:d8:de), Dst: a2:86:17:7c:c3:65 (a2:86:17:7c:c3:65)
 ▶ Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40
 ▶ Transmission Control Protocol, Src Port: 58716, Dst Port: 80, Seq: 0, Len: 0
 Source Port: 58716
 Destination Port: 80
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 0 (relative sequence number)
 Acknowledgment number: 0
 Header Length: 40 bytes
 Flags: 0x002 (SYN)
 Window size value: 29200
 [Calculated window size: 29200]
 Checksum: 0xb671 [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 ▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale

Nota: Potrebbe essere necessario regolare le dimensioni delle finestre superiore e centrale all'interno di Wireshark per visualizzare le informazioni necessarie.



- Qual è il numero di porta TCP di origine?
- Come classificheresti la porta di origine?
- Qual è il numero di porta TCP di destinazione?
- Come classificheresti la porta di destinazione?
- Quale flag è impostato?
- A quale valore è impostato il numero di sequenza relativo?

d. Selezionare il pacchetto successivo nell'handshake a tre vie. In questo esempio, è il frame 2. Questa è la risposta del server web alla richiesta iniziale di avviare una sessione.

- Quali sono i valori delle porte di origine e destinazione?
- Quali flag sono impostati?
- A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	58716 → 80 [SYN] Seq=0 Win=
2	0.000081	172.16.0.40	10.0.0.11	TCP	74	80 → 58716 [SYN, ACK] Seq=0
3	0.000082	10.0.0.11	172.16.0.40	TCP	66	58716 → 80 [ACK] Seq=1 Ack=
4	0.000194	10.0.0.11	172.16.0.40	HTTP	356	GET /favicon.ico HTTP/1.1

▶ Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 ▶ Ethernet II, Src: a2:86:17:7c:c3:65 (a2:86:17:7c:c3:65), Dst: a6:a1:15:2c:d8:de (a6:
 ▶ Internet Protocol Version 4, Src: 172.16.0.40, Dst: 10.0.0.11
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 58716, Seq: 0, Ack: 1, Len: 0
 Source Port: 80
 Destination Port: 58716
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 0 (relative sequence number)
 Acknowledgment number: 1 (relative ack number)
 Header Length: 40 bytes
 Flags: 0x012 (SYN, ACK)
 Window size value: 28960
 [Calculated window size: 28960]
 Checksum: 0xc85a [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation



e. Infine, selezionare il terzo pacchetto nell'handshake a tre vie.

Filter: tcp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	58716 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM
2	0.000081	172.16.0.40	10.0.0.11	TCP	74	80 → 58716 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM
3	0.000082	10.0.0.11	172.16.0.40	TCP	66	58716 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=38645 TStamp=1400000000.000000
4	0.000194	10.0.0.11	172.16.0.40	HTTP	356	GET /favicon.ico HTTP/1.1

```

Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: a6:a1:15:2c:d8:de (a6:a1:15:2c:d8:de), Dst: a2:86:17:7c:c3:65 (a2:86:17:7c:c3:65)
Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40
Transmission Control Protocol, Src Port: 58716, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
Source Port: 58716
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header Length: 32 bytes
Flags: 0x010 (ACK)
Window size value: 58
[Calculated window size: 29696]
[Window size scaling factor: 512]
Checksum: 0xb669 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

```

Esaminare il terzo e ultimo pacchetto dell'handshake.

Quale flag è impostato?

I numeri relativi di sequenza e acknowledgment sono impostati a 1 come punto di partenza. La connessione TCP è stabilita e la comunicazione tra il computer di origine e il server web può iniziare.



Parte 3: Visualizzare i pacchetti usando tcpdump

È anche possibile visualizzare il file pcap e filtrare per le informazioni desiderate.

a. Aprire una nuova finestra di terminale, inserire `man tcpdump`. Nota: Potrebbe essere necessario premere INVIO per vedere il prompt.

Utilizzando le pagine manuale (man pages) disponibili con il sistema operativo Linux, è possibile leggere o cercare tra le pagine manuale le opzioni per selezionare le informazioni desiderate dal file pcap.

```
[analyst@sec0ps ~]$ man tcpdump
TCPDUMP(1)                               General Commands Manual          TCPDUMP(1)

NAME
    tcpdump - dump traffic on a network

SYNOPSIS
tcpdump [ -AbdDefhHIJKlLnNOpqStuUvxX# ] [ -B buffer_size ]
[ -c count ]
[ -C file_size ] [ -G rotate_seconds ] [ -F file ]
[ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
[ --number ] [ -Q in|out|inout ]
[ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]
[ -W filecount ]
[ -E spi@ipaddr algo:secret,... ]
[ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
[ --time-stamp-precision=tstamp_precision ]
[ --immediate-mode ] [ --version ]
[ expression ]
<output omesso>
```

Per cercare nelle pagine man, è possibile usare / (ricerca in avanti) o ? (ricerca indietro) per trovare termini specifici, n per passare alla corrispondenza successiva e q per uscire. Ad esempio, per cercare informazioni sull'opzione -r, digitare /-r. Digitare n per passare alla corrispondenza successiva.



- b. Nello stesso terminale, aprire il file di cattura usando il seguente comando per visualizzare i primi 3 pacchetti TCP catturati:

```
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3
reading from file capture.pcap, link-type EN10MB (Ethernet)
13:58:30.647462 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [S], seq 2432755549, win 29200, options [mss 1460,sackOK,TS val 3864513189 ecr 0,nop,wscale 9], length 0
13:58:30.647543 IP 172.16.0.40.http > 10.0.0.11.58716: Flags [S.], seq 1766419191, ack 2432755550, win 28960, options [mss 1460,sackOK,TS val 50557410 ecr 3864513189,nop,wscale 9], length 0
13:58:30.647544 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 3864513189 ecr 50557410], length 0
```

Per visualizzare l'handshake a 3 vie, potrebbe essere necessario aumentare il numero di righe dopo l'opzione -c.

- c. Navigare al terminale usato per avviare Mininet. Terminare Mininet inserendo quit nella finestra principale del terminale della VM CyberOps.

```
mininet> quit
*** Stopping 0 controllers

*** Stopping 2 terms
*** Stopping 5 links
....
*** Stopping 1 switches
s1
*** Stopping 5 hosts
H1 H2 H3 H4 R1
*** Done
[analyst@secOps ~]$
```

- d. Dopo aver chiuso Mininet, inserire sudo mn -c per pulire i processi avviati da Mininet. Inserire la password cyberops quando richiesto.

```
[analyst@secOps ~]$ sudo mn -c
[sudo] password for analyst:
```

Domande di Riflessione

1. Ci sono centinaia di filtri disponibili in Wireshark. Una rete di grandi dimensioni potrebbe avere numerosi filtri e molti tipi diversi di traffico. Elenca tre filtri che potrebbero essere utili a un amministratore di rete.
2. In quali altri modi Wireshark potrebbe essere utilizzato in una rete di produzione?



EPCODE

Roma | Milano | Berlino

business@epicode.com

