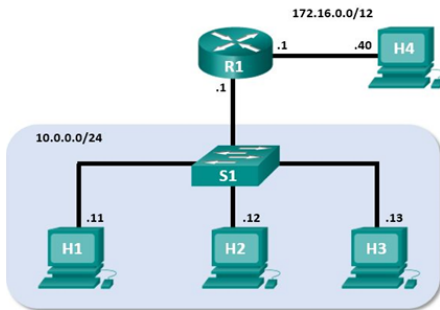


S11L2

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.

- Qual è il numero di porta TCP di origine?

Il numero di porta TCP di origine è 48856

43	16.810732	10.0.0.11	172.16.0.40	TCP	74	48856 → 80 [SYN] Seq=0 Win=42340
44	16.810751	172.16.0.40	10.0.0.11	TCP	74	80 → 48856 [SYN, ACK] Seq=0 Ack=
45	16.810757	10.0.0.11	172.16.0.40	TCP	66	48856 → 80 [ACK] Seq=1 Ack=1 Win=
46	16.810820	10.0.0.11	172.16.0.40	HTTP	397	GET / HTTP/1.1
47	16.810828	172.16.0.40	10.0.0.11	TCP	66	80 → 48856 [ACK] Seq=1 Ack=332 W
48	16.810899	172.16.0.40	10.0.0.11	TCP	304	80 → 48856 [PSH, ACK] Seq=1 Ack=
49	16.810904	10.0.0.11	172.16.0.40	TCP	66	48856 → 80 [ACK] Seq=332 Ack=239
50	16.810923	172.16.0.40	10.0.0.11	HTTP	681	HTTP/1.1 200 OK (text/html)

Frame 43: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: fa:69:24:e1:77:03 (fa:69:24:e1:77:03), Dst: de:6b:ca:b9:67:da (de:6b:ca:b9:67:da)

Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40

Transmission Control Protocol, Src Port: 48856, Dst Port: 80, Seq: 0, Len: 0

- Come classifichereesti la porta di origine?

La porta di origine (48856/tcp) rientra nell'intervallo di porte effimere/dinamiche. Viene tipicamente assegnata in modo temporaneo dal sistema operativo quando un client apre una connessione tcp verso un server

- Qual è il numero di porta TCP di destinazione?

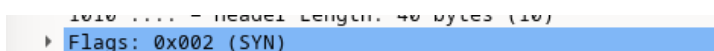
La porta TCP di destinazione è la porta 80

- Come classifichereesti la porta di destinazione?

La porta di destinazione (80/tcp) rientra tra le well-known port, il servizio principale di questa porta è HTTP

- Quale flag è impostato?

Il flag impostato è il SYN, il primo dei tre passi del triple-handshake



- A quale valore è impostato il numero di sequenza relativo?

Il numero di sequenza relativo è 0

Sequence Number: 0 (relative sequence number)

43	16.810732	10.0.0.11	172.16.0.40	TCP	74	48856 → 80	[SYN]	Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM TSval=1346012345 TSecr=0 WS...
44	16.810751	172.16.0.40	10.0.0.11	TCP	74	80 → 48856	[SYN, ACK]	Seq=0 Ack=1 Win=43440 Len=0 MSS=1460 SACK_PERM TSval=3877695113...
45	16.810757	10.0.0.11	172.16.0.40	TCP	66	48856 → 80	[ACK]	Seq=1 Ack=1 Win=42496 Len=0 TSval=1346012345 TSecr=3877695113
46	16.810820	10.0.0.11	172.16.0.40	HTTP	397	GET / HTTP/1.1		
47	16.810828	172.16.0.40	10.0.0.11	TCP	66	80 → 48856	[ACK]	Seq=1 Ack=332 Win=43520 Len=0 TSval=3877695113 TSecr=1346012345
48	16.810899	172.16.0.40	10.0.0.11	TCP	304	80 → 48856	[PSH, ACK]	Seq=1 Ack=332 Win=43520 Len=238 TSval=3877695113 TSecr=13460123...
49	16.810904	10.0.0.11	172.16.0.40	TCP	66	48856 → 80	[ACK]	Seq=332 Ack=239 Win=42496 Len=0 TSval=1346012345 TSecr=3877695113
50	16.810923	172.16.0.40	10.0.0.11	HTTP	681	HTTP/1.1 200 OK	(text/html)	

- Quali sono i valori delle porte di origine e destinazione?

La porta di origine è la porta 80 e la porta di destinazione è la porta 48856

- Quali flag sono impostati?

I flag impostati sono SYN, ACK. La seconda fase del triple-handshake

Flags: 0x012 (SYN, ACK)

- A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?

I valori impostati ai numeri relativi di sequenza e acknowledgment è 1


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

- Quale flag è impostato?

Il flag impostato è ACK, l'ultima fase del triple-handshake

43	16.810732	10.0.0.11	172.16.0.40	TCP	74	48856 → 80	[SYN]	Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM TSval=1346012345 TSecr=0 WS...
44	16.810751	172.16.0.40	10.0.0.11	TCP	74	80 → 48856	[SYN, ACK]	Seq=0 Ack=1 Win=43440 Len=0 MSS=1460 SACK_PERM TSval=3877695113...
45	16.810757	10.0.0.11	172.16.0.40	TCP	66	48856 → 80	[ACK]	Seq=1 Ack=1 Win=42496 Len=0 TSval=1346012345 TSecr=3877695113
46	16.810820	10.0.0.11	172.16.0.40	HTTP	397	GET / HTTP/1.1		
47	16.810828	172.16.0.40	10.0.0.11	TCP	66	80 → 48856	[ACK]	Seq=1 Ack=332 Win=43520 Len=0 TSval=3877695113 TSecr=1346012345
48	16.810899	172.16.0.40	10.0.0.11	TCP	304	80 → 48856	[PSH, ACK]	Seq=1 Ack=332 Win=43520 Len=238 TSval=3877695113 TSecr=13460123...
49	16.810904	10.0.0.11	172.16.0.40	TCP	66	48856 → 80	[ACK]	Seq=332 Ack=239 Win=42496 Len=0 TSval=1346012345 TSecr=3877695113
50	16.810923	172.16.0.40	10.0.0.11	HTTP	681	HTTP/1.1 200 OK	(text/html)	

- Cosa fa l'opzione -r?



```

[ -s snaplen ] [ -T type ] [ --version ]
[ -V file ] [ -v file ] [ -f filecount ] [ -y datalinktype ]
[ -z postrotate-command ] [ -Z user ]
[ --time-stamp-precision timestamp-precision ]
[ --micro ] [ --nano ]
[ expression ]

```

DESCRIPTION

`tcpdump` prints out a description of the contents of packets on a network interface that match the Boolean `expression` (see `pcap-filter(7)` for the `expression` syntax); the description is preceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight. It can also be run with the `-w` flag, which causes it to save the packet data to a file for later analysis; and/or with the `-r` flag, which causes it to read from a saved packet file rather than to read packets from a network interface. It can also be run with the `-v` flag, which causes it to read a list of saved packet files. In all cases, only packets that match `expression` will be processed by `tcpdump`.

Il flag -r in tcpdump serve a leggere i pacchetti da un file precedentemente salvato in formato pcap

```

analyst@seclips:~$ tcpdump -r /home/analyst/capture.pcap tcp -c 5
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet), snapshot length 262144
07:50:05.684567 IP secOps.48856 > 172.16.0.40,http: Flags [S], seq 2155796878, win 42340, options [mss 1460,sackOK,TS val 1346012345 ecr 0,nop,wscale 9], length 0
07:50:05.684586 IP 172.16.0.40,http > secOps.48856: Flags [S.], seq 3496212570, ack 2155796879, win 43440, options [mss 1460,sackOK,TS val 3877695113 ecr 1346012345,nop,wscale 9], length 0
07:50:05.684592 IP secOps.48856 > 172.16.0.40,http: Flags [.], ack 1, win 83, options [nop,nop,TS val 1346012345 ecr 3877695113], length 0

```

Domande di Riflessione

- 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.

Filtro per IP, ad esempio `ip.addr == 192.168.1.100`.

Filtro per protocollo, ad esempio HTTP, SNMP, TCP.

Filtro per numero di porta, ad esempio `tcp.port == 80`.

2. In quali altri modi Wireshark potrebbe essere utilizzato in una rete di produzione?

-Monitoraggio delle prestazioni

Wireshark può essere utilizzato per identificare i colli di bottiglia e i problemi di latenza della rete. Analizzando i pacchetti, è possibile calcolare il tempo di risposta dei server, il ritardo di e la quantità di perdita di pacchetti.

-Analisi della sicurezza

È un ottimo strumento per individuare attività sospette o traffico dannoso. Può rilevare:

- Scansioni di porte
- Malware o virus
- Comunicazioni in chiaro
- Attacchi DoS/DDoS

-Verifica della conformità

Wireshark aiuta a garantire che la rete sia conforme agli standard aziendali e normativi. Permette di:

- Verificare se le politiche di crittografia sono applicate correttamente (es. HTTPS, SSH).
- Assicurarsi che le applicazioni utilizzino i protocolli e le porte approvati.

-Debugging delle applicazioni

Gli sviluppatori e gli amministratori di sistema possono usare Wireshark per capire esattamente come un'applicazione sta comunicando sulla rete. È uno strumento indispensabile per il troubleshooting di applicazioni distribuite.