

Pratica CyberOps 2

Nella giornata di oggi ci è richiesto si rispondere alle seguenti domande dopo aver svolto l'esercizio su macchina virtuale CyberOps workstation.

Rispondiamo di seguito alle sei domande legate a questo primo screenshot.

No.	Time	Source	Destination	Protocol	Length	Info
14	1.464102	10.0.0.11	172.16.0.40	TCP	66	47970 → 80 [ACK] Seq=1 Ack=1 Win=64 Len=0 TSval=2951933703 TSecr=3084809895
15	1.464141	172.16.0.40	10.0.0.11	TCP	66	[TCP ACKed unseen segment] 80 → 47970 [ACK] Seq=1 Ack=2 Win=61 Len=0 TSval=3084820135 TSecr=2951913435
50	11.704463	10.0.0.11	172.16.0.40	TCP	66	[TCP Dup ACK 14#1] 47970 → 80 [ACK] Seq=1 Ack=1 Win=64 Len=0 TSval=2951943943 TSecr=3084820135

Frame 14: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: aa:15:f9:50:ed:07 (aa:15:f9:50:ed:07), Dst: 36:94:0d:7b:41:d5 (36:94:0d:7b:41:d5)

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

Transmission Control Protocol, Src Port: 47970, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 47970

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

Next sequence number: 1 (relative sequence number)

Acknowledgment number: 1 (relative ack number)

1000 ... = Header Length: 32 bytes (8)

Flags: 0x010 (ACK)

Window size value: 64

[calculated window size: 64]

[Window size scaling factor: -1 (unknown)]

Checksum: 0xb669 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

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

[Timestamps]

- **Qual è il numero di porta TCP di origine?**

R: Il numero di porta TCP di origine è 47970.

- **Come classificheresti la porta di origine?**

R: La porta di origine (47970) è una porta effimera o dinamica. Queste porte vengono assegnate temporaneamente dai sistemi operativi quando un client avvia una connessione. Poiché è superiore a 1023, non è una porta ben nota (well-known port).

- **Qual è il numero di porta TCP di destinazione?**

R: Il numero di porta TCP di destinazione è 80.

- **Come classificheresti la porta di destinazione?**

R: La porta di destinazione (80) è una porta "ben nota" (well-known port). È la porta standard utilizzata per il traffico HTTP (Hypertext Transfer Protocol).

- **Quale flag è impostato?**

R: Il flag impostato è ACK (Acknowledgment). Questo è indicato da Flags: 0x010 (ACK).

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

R: Il numero di sequenza relativo è impostato a 1. Questo è indicato da Sequence number: 1

Andiamo adesso a svolgere la seconda parte dell'esercizio rispondendo alle tre domande legate al secondo screenshot:

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 47970, Seq: 1, Ack: 2, Len: 0

Source Port: 80
Destination Port: 47970
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 2 (relative ack number)
1000 = Header Length: 32 bytes (8)
▼ Flags: 0x010 (ACK)
000. = Reserved: Not set
...0 = Nonce: Not set
....0... = Congestion Window Reduced (CWR): Not set
....0... = ECN-Echo: Not set
....0... = Urgent: Not set
....1... = Acknowledgment: Set
....0... = Push: Not set
....0... = Reset: Not set
....0... = Syn: Not set
....0... = Fin: Not set
[TCP Flags:A...]
Window size value: 61
[Calculated window size: 61]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xb669 [unverified]

- **Quali sono i valori delle porte di origine e destinazione? R:**
 - Porta di origine: 80
 - Porta di destinazione: 47970
- **Quali flag sono impostati? R:**
 - Il flag impostato è ACK (Acknowledgment). Questo è indicato da Acknowledgment: Set e Flags: 0x010 (ACK).
- **A quali valori sono impostati i numeri relativi di sequenza e acknowledgment? R:**
 - Numero di sequenza relativo: 1
 - Numero di acknowledgment relativo: 2

Andiamo ora ad analizzare il terzo screenshot:

No.	Time	Source	Destination	Protocol	Length	Info
14	1.464102	10.0.0.11	172.16.0.40	TCP	66	47970 → 80 [ACK] Seq=1 Ack=1 Win=64 Len=0 TSval=2951933703 TSecr=3084809895
15	1.464141	172.16.0.40	10.0.0.11	TCP	66	[TCP ACKed unseen segment] 80 → 47970 [ACK] Seq=1 Ack=2 Win=61 Len=0 TSval=3084820135 TSecr=2951913435
50	11.704463	10.0.0.11	172.16.0.40	TCP	66	[TCP Dup ACK 14#1] 47970 → 80 [ACK] Seq=1 Ack=1 Win=64 Len=0 TSval=2951943943 TSecr=3084820135

▼ Transmission Control Protocol, Src Port: 47970, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 47970
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1000 = Header Length: 32 bytes (8)
▼ Flags: 0x010 (ACK)
000. = Reserved: Not set
...0 = Nonce: Not set
....0... = Congestion Window Reduced (CWR): Not set
....0... = ECN-Echo: Not set
....0... = Urgent: Not set
....1... = Acknowledgment: Set
....0... = Push: Not set
....0... = Reset: Not set
....0... = Syn: Not set
....0... = Fin: Not set
[TCP Flags:A...]
Window size value: 64
[Calculated window size: 64]
[Window size scaling factor: -1 (unknown)]

- **Flags: 0x010 (ACK)**
- **[TCP Flags:A...]**

Domanda: **Quale flag è impostato? R:**

Analizzando lo screenshot, il flag impostato è ACK (Acknowledgment).

Questo è indicato da:

- ...1..... = Acknowledgment: Set

Passiamo alla quarta fase dell'esercizio che prevede la domanda:

Cosa fa l'opzione -r?

```
-r file
Read packets from file (which was created with the -w option or by other tools that write pcap or pcap-ng files). Standard input is used if file is '-'.
```

R:

L'opzione -r viene utilizzata per leggere pacchetti da un file.

Il testo specifica che il file deve essere stato creato con l'opzione -w (presumibilmente di un tool di cattura pacchetti come Wireshark o tcpdump) o da altri strumenti che scrivono file in formato pcap o pcap-ng.

Rispondiamo ora alle ultime due domande di riflessione dell'esercizio quali:

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.

R: Tre filtri Wireshark utili a un amministratore di rete:

1. **ip.addr == X.X.X.X:** Questo filtro permette di visualizzare tutto il traffico (sia di origine che di destinazione) che coinvolge uno specifico indirizzo IP (sostituendo X.X.X.X con l'indirizzo desiderato). È estremamente utile per isolare il traffico di un singolo host o di un gruppo di host.
2. **tcp.port == YYYY o udp.port == YYYY:** Questi filtri consentono di visualizzare il traffico relativo a una specifica porta TCP o UDP (sostituendo YYYY con il numero di porta, ad esempio tcp.port == 80 per il traffico HTTP). Sono fondamentali per analizzare problemi relativi a servizi specifici (es. web server, database, DNS).
3. **http o dns o ftp (o altri protocolli applicativi):** Questi filtri specifici per protocollo permettono di visualizzare solo il traffico di un determinato protocollo applicativo. Sono utili per analizzare il comportamento di applicazioni specifiche e identificare potenziali problemi a livello applicativo.

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

R: Wireshark è uno strumento estremamente versatile in una rete di produzione e può essere utilizzato in diversi modi oltre alla semplice visualizzazione del traffico:

- **Risoluzione dei problemi di connettività:** Identificare se un dispositivo non riesce a raggiungere un altro, verificare la presenza di pacchetti persi o di problemi di routing.
- **Debug di applicazioni:** Comprendere il flusso di comunicazione tra client e server per un'applicazione specifica, identificare errori a livello di protocollo o risposte inattese.
- **Analisi delle prestazioni della rete:** Misurare la latenza, il throughput, identificare colli di bottiglia o ritardi dovuti a problemi di rete o applicazione.
- **Rilevamento di attività anomale o potenziali minacce alla sicurezza:** Sebbene non sia un sistema di rilevamento intrusioni (IDS), un amministratore esperto può notare pattern di traffico insoliti o tentativi di scansione delle porte.

- **Validazione delle configurazioni di rete:** Verificare che le regole del firewall, il NAT, il QoS o il routing funzionino come previsto osservando il traffico effettivo.
 - **Capire il comportamento di nuovi servizi o applicazioni:** Analizzare il traffico generato da nuove implementazioni per assicurarsi che si comportino correttamente e che non ci siano effetti collaterali indesiderati.
 - **Formazione e apprendimento:** È uno strumento eccellente per comprendere come funzionano i protocolli di rete a basso livello.
 - **Analisi forense (post-incidente):** Dopo un incidente di sicurezza, Wireshark può essere utilizzato per analizzare i file di cattura del traffico e capire cosa è successo, come è avvenuto l'attacco o la violazione.
-

Conclusione

In sintesi, l'analisi degli screenshot ci ha permesso di esplorare alcuni aspetti fondamentali del traffico di rete TCP, identificando dettagli cruciali come numeri di porta di origine e destinazione, classificazione delle porte (effimere o ben note), flag impostati (in particolare l'ACK) e valori dei numeri di sequenza e acknowledgment.

Abbiamo anche ripassato l'uso dell'opzione -r per la lettura di file di cattura pacchetti e discusso l'importanza dei filtri in Wireshark, evidenziando il loro ruolo chiave nella risoluzione dei problemi, nell'analisi delle prestazioni e nella sicurezza delle reti di produzione.

Questa comprensione approfondita del traffico di rete è essenziale per qualsiasi amministratore o professionista IT che voglia mantenere una rete efficiente e sicura.
