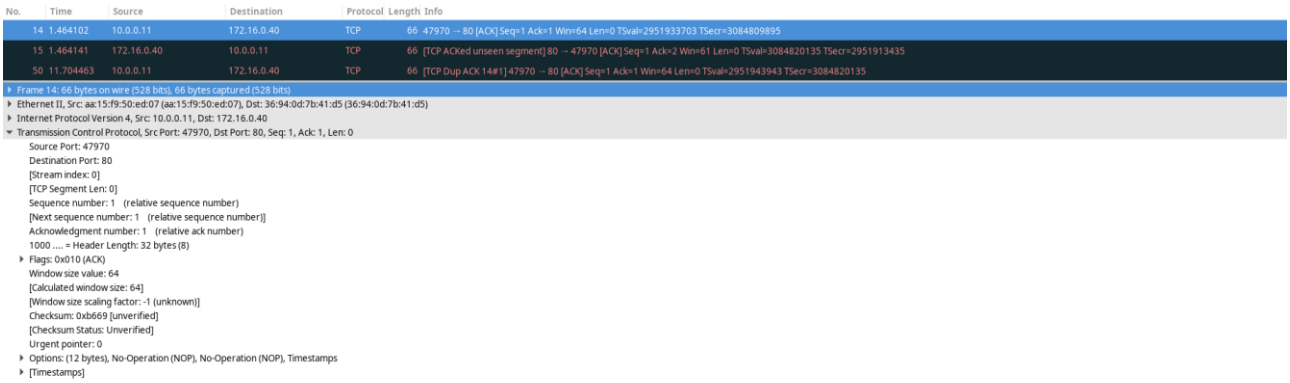
Pratica CyberOps 2

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

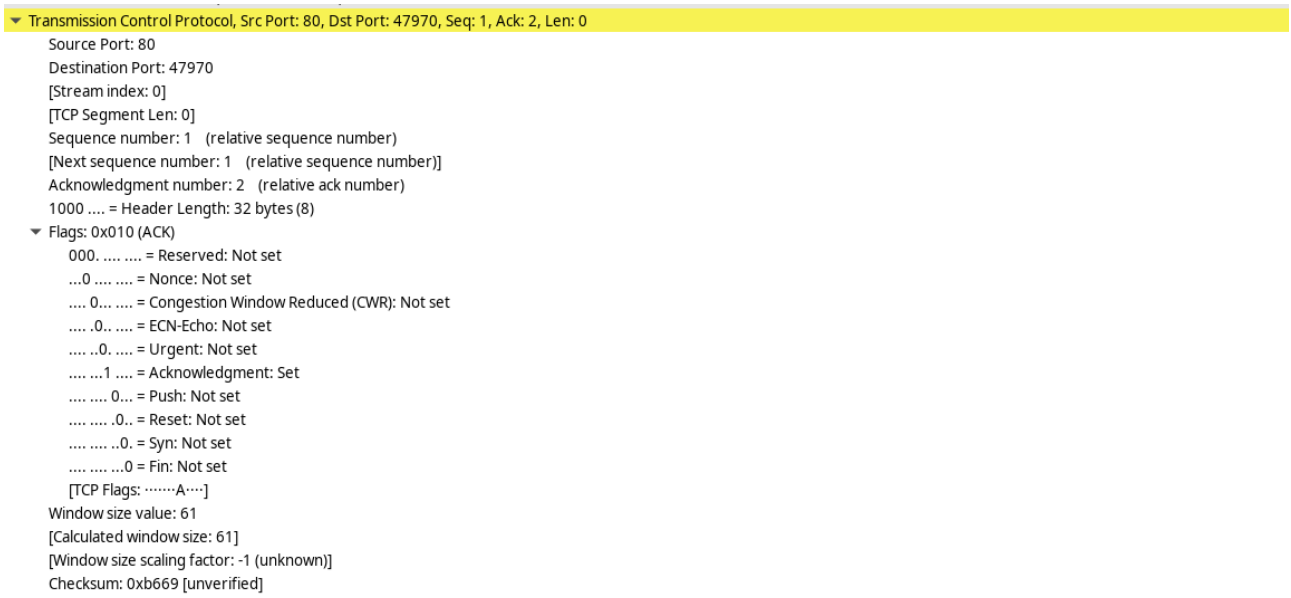
Rispondiamo di seguito alle sei domande legate a questo primo screenshot.



- **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).

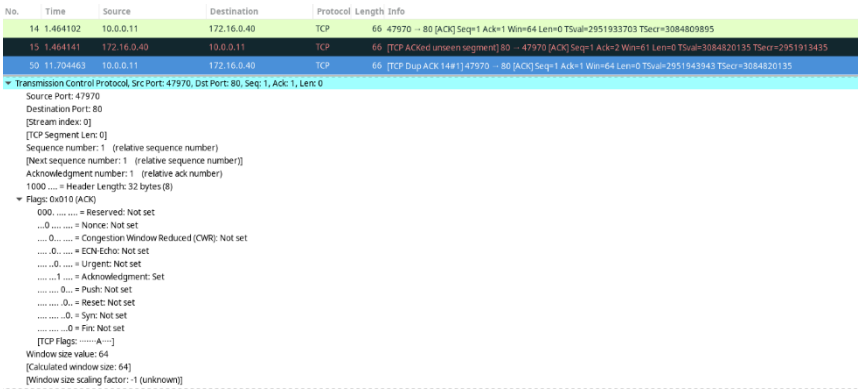
- **Qual è il numero di porta TCP di destinazione?**
  R: Il numero di porta TCP di destinazione è 80.
- **Come classificheresti la porta di destinazione?**
  R: La porta di destinazione (80) è una porta "ben nota" (well-known port). È la porta standard utilizzata per il traffico HTTP (Hypertext Transfer 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:



- **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:



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

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

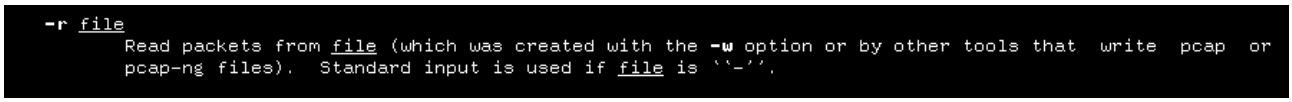
Questo è indicato da:

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

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

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

Cosa fa l'opzione -r?



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.

Fabriani Anais
10/06/2025