REPORT S11/L2

Studente: Vincenzo Zarola
Corso: Cybersecurity Specialist

1. Analisi Primo Pacchetto (Richiesta Client)

Domanda: Qual è il numero di porta TCP di origine?
Risposta: 40662

Domanda: Come classificheresti la porta di origine?
Risposta: Porta Dinamica o Privata (Dynamic/Private Port).

Domanda: Qual è il numero di porta TCP di destinazione?
Risposta: 80

Domanda: Come classificheresti la porta di destinazione?
Risposta: Porta Ben Nota (Well-Known Port).

Domanda: Quale flag è impostato?
Risposta: 0x002 **(SYN)**

Domanda: A quale valore è impostato il numero di sequenza relativo?
Risposta: 0

---

2. Analisi Secondo Pacchetto (Risposta Server)

Domanda: Quali sono i valori delle porte di origine e destinazione?
Risposta: Porta di Origine: **80**; Porta di Destinazione: **40662**.

Domanda: Quali flag sono impostati?
Risposta: 0x012 **(SYN, ACK)**

Domanda: A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?
Risposta:

- Numero di sequenza relativo (Seq): **0**
- Numero di acknowledgment relativo (Ack): **1**.

Domanda: Cosa fa l’opzione -r?
Risposta: Legge i pacchetti dal file (creato con l'opzione -w o da altri strumenti che scrivono file pcap o pcapng). L'input standard

viene utilizzato se il file è ‘’-"

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.

Comando: ***ip.addr***
Ci permette di visualizzare il traffico sia in entrata che in uscita, relativo ad un singolo dispositivo o ad un server.

Comando: ***tcp.port***
Ci permette di analizzare solo il traffico relativo a un servizio specifico, in modo da poter escludere tutto il resto del ‘rumore’ in rete.

Comando: ***tcp.analysis.falg***
Questo filtro ci aiuta a capire se ci sono anomalie, problemi di prestazioni o stati insoliti nelle connessioni TCP, in quanto Wireshark li evidenzia.

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

Risoluzione dei Problemi di Prestazioni (Network Troubleshooting): Capire perché un'applicazione è lenta. Analizzando i timestamp e le ritrasmissioni TCP, si può capire se la lentezza è dovuta alla rete (latenza alta, perdita pacchetti) o al server (che ci mette troppo a rispondere).

Analisi di Sicurezza e Forensics (Threat Hunting): Dopo un incidente di sicurezza, si usa Wireshark per analizzare i file ***.pcap*** e capire cosa ha fatto l'attaccante: quali dati ha esfiltrato, quali comandi ha inviato a un server o se ci sono credenziali passate in chiaro.