REPORT S11/L3

Studente: Vincenzo Zarola
Corso: Cybersecurity Specialist

Domanda: Quali sono gli indirizzi MAC di origine e destinazione?
Risposta:

- Indirizzo MAC di origine: 08:00:27:1f:b7:23
- Indirizzo MAC di destinazione: 52:55:0a:00:02:03

Domanda: A quali interfacce di rete sono associati questi indirizzi MAC?
Risposta: Sono associati all'interfaccia **eth0**

Domanda: Quali sono gli indirizzi IP di origine e destinazione?
Risposta:

- Indirizzo IP di origine: 10.0.2.15
- Indirizzo IP di destinazione: 10.0.2.3

Domanda: A quali interfacce di rete sono associati questi indirizzi IP?
Risposta: Sono associati all'interfaccia **eth0**

Domanda: Quali sono le porte di origine e destinazione?
Risposta:

- Porta di origine: 48297
- Porta di destinazione: 53

Domanda: Qual è il numero di porta DNS predefinito?
Risposta: 53

Domanda: Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC. Qual è la tua osservazione?
Risposta: L'osservazione è che l'indirizzo MAC di origine e l'indirizzo IP di origine visibili nel pacchetto corrispondono esattamente agli indirizzi configurati sull'interfaccia eth0 della macchina locale.

Domanda: Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione?
Risposta:

- Indirizzo MAC di origine: 52:55:0a:00:02:03
- Indirizzo MAC di destinazione: 08:00:27:1f:b7:23
- Porta di origine: 53

- Porta di destinazione: 48297

Domanda: Come si confrontano con gli indirizzi nei pacchetti di query DNS?
Risposta: Sono gli stessi indirizzi IP, ma in questo pacchetto sono invertiti (origine e destinazione), in quanto è il pacchetto di risposta

Domanda: Il server DNS può fare query ricorsive?
Risposta: Si, il server DNS può fare query ricorsive. Osservando i flag del pacchetto DNS, si nota che il bit "Recursion Desired" è attivo (impostato a 1). Questo significa che il client (la nostra macchina virtuale) sta chiedendo al server DNS di occuparsi interamente della risoluzione del nome, contattando altri server se necessario, fino a trovare l'indirizzo IP finale.

Domanda: Come si confrontano i risultati con quelli di nslookup?
Risposta: I risultati sono uguali. Wireshark mostra la struttura del pacchetto che corrisponde esattamente alle informazioni restituite dal comando nslookup nel terminale.

Domanda: Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?
Risposta: Quando viene rimosso il filtro, wireshark ci permette di vedere tutto ciò che succede all'interno della rete. In questo caso specifico ci mette a schermo anche il traffico **ARP**, utilizzato per mappare gli indirizzi IP ai MAC address.

Domanda: Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?
Risposta: Un attaccante può utilizzare Wireshark per eseguire attività di **Sniffing** (intercettazione) del traffico di rete. I rischi principali includono:

- **Furto di Credenziali:** Se vengono utilizzati protocolli non crittografati come **Telnet**, **FTP** o **HTTP**, Wireshark può catturare i pacchetti e mostrare in chiaro nomi utente e password.
- **Mappatura della Rete:** Analizzando i pacchetti ARP, DNS e TCP, l'attaccante può identificare gli indirizzi IP attivi, i sistemi operativi in uso e i servizi aperti, informazioni cruciali per preparare un attacco mirato.

Sostanzialmente, se non viene utilizzata la crittografia, Wireshark trasforma la rete in un libro aperto.