EPICODE

Laboratorio giorno 3 - Cisco CyberOps

By Xian Long Qiu

EPICODE

WireShark richiesta dns

1.L'indirizzo MAC di origine è 08:00:27:96:c2:10.
L'indirizzo MAC di destinazione è 1a:e5:e0:f0:b7:ba.

2.L'indirizzo MAC di origine è associato all’interfaccia di rete VirtualBox (VM guest), cioè la mia macchina, che ha inviato una richiesta DNS.
L'indirizzo MAC di destinazione è associato all'interfaccia del gateway o del server DNS a cui è stata inviata la richiesta.

3.L'indirizzo IP di origine è 192.168.208.151.
L'indirizzo IP di destinazione è 192.168.208.147.

4.L'indirizzo IP 192.168.208.151 è associato all'interfaccia di rete con MAC 08:00:27:96:c2:10 (cioè la mia macchina).
L'indirizzo IP 192.168.208.147 è associato all'interfaccia di rete con MAC 1a:e5:e0:f0:b7:ba (probabilmente il router o il server DNS).

EPICODE

5.La porta di origine è 56922.
La porta di destinazione è 53.

6.Il numero di porta DNS predefinito è 53.

7.Ho confrontato gli indirizzi MAC e IP ottenuti tramite ipconfig /all e arp -a con quelli visibili in Wireshark: sono perfettamente corrispondenti. Questo conferma che Wireshark sta catturando correttamente il traffico di rete in uscita dalla mia macchina.

8.L’indirizzo IP di origine è 192.168.208.147 con MAC 1a:e5:e0:f0:b7:ba.
L’indirizzo IP di destinazione è 192.168.208.151 con MAC 08:00:27:96:c2:10.

9.Gli indirizzi sono invertiti rispetto alla richiesta iniziale perché si tratta della risposta alla query DNS.
Questo scambio conferma il corretto funzionamento del protocollo DNS.

EPICODE

10.Sì, il server può eseguire query ricorsive, come indicato dalla flag Recursion Desired (RD) nella richiesta.
Nella risposta è presente la flag Recursion Available (RA), che conferma che il server supporta e accetta richieste ricorsive.

11.I risultati ottenuti tramite nslookup e quelli visibili nei pacchetti DNS in Wireshark sono coerenti e corrispondenti.

EPICODE

Riflessione

12.Rimuovendo il filtro in Wireshark, ho potuto osservare molti più dettagli della rete.
Questo permette di imparare e analizzare vari aspetti, tra cui:

- Quanti dispositivi sono attivi e chi comunica con chi
- Quali protocolli vengono utilizzati (es. ARP, DHCP, ICMP, HTTP)
- Come avviene la risoluzione dei nomi, l'assegnazione degli IP e il routing
- Eventuali segnali di problemi o comportamenti sospetti

Questa visione completa è fondamentale per l'analisi e la comprensione del traffico di rete.

13.Un attaccante può usare Wireshark (o altri sniffer) come strumento per spiare, analizzare e compromettere la sicurezza di una rete, soprattutto in ambienti non cifrati o mal configurati.
I principali rischi includono:

- 🚨 Sniffing del traffico non cifrato: es. password in chiaro su HTTP, FTP, Telnet
- 🎣 Raccolta di informazioni: identificazione di IP, MAC, servizi attivi e versioni
- 🕴️ Attacchi MITM (Man-in-the-Middle): combinati con ARP spoofing o access point falsi
- 🪝 Sfruttamento di debolezze: es. LLMNR, NetBIOS, DHCP insicuro, protocolli vulnerabili