ESERCITAZIONE: ESPLORAZIONE DEL TRAFFICO DNS CON WIRESHARK
Corso: Cyber Security & Ethical Hacking

PARTE 2: ESPLORARE IL TRAFFICO DELLE QUERY DNS

1. Quali sono gli indirizzi MAC di origine e destinazione rilevati?
[RISPOSTA]: (08:00:27:1f:b7:23 Origine) (64:da:ed:37:9f:0d Destinazione)

2. A quali interfacce di rete sono associati questi indirizzi MAC?
[RISPOSTA]: (PCSSystemtec Origine) (eero Destinazione)

3. Quali sono gli indirizzi IP di origine e destinazione?
[RISPOSTA] 192.168.6.9 / 192.168.4.1

4. A quali interfacce di rete sono associati questi indirizzi IP?
[RISPOSTA]:(PCSSYSTEMTEC Origine)(eero Destinazione)

5. Quali sono le porte (UDP) di origine e destinazione?
[RISPOSTA]:40621/53

6. Qual è il numero di porta DNS predefinito?
[RISPOSTA]:53

7. Confrontando gli indirizzi del tuo PC (ipconfig/ifconfig) con i risultati di Wireshark, qual è la tua osservazione?
[RISPOSTA]:i dati corrispondono agli ip del gateway e l'ip della macchina

PARTE 3: ESPLORARE IL TRAFFICO DELLE RISPOSTE DNS

8. Nel pacchetto "Standard query response", quali sono gli indirizzi MAC, IP e le porte di origine e destinazione?
[RISPOSTA]:(64:da:ed:37:9f:0d Origine) (08:00:27:1f:b7:23 Destinazione) 192.168.4.1 / 192.168.6.9

9. Come si confrontano questi indirizzi con quelli dei pacchetti di query? (Noti inversioni?)
[RISPOSTA]:si sono invertiti

10. Osservando i Flags della risposta, il server DNS è abilitato a fare query ricorsive?
[RISPOSTA]:si risulta abilitato in quanto il flag è su 1

11. Osservando i record CNAME e A nelle Answers, come si confrontano i risultati con quelli del comando nslookup?
[RISPOSTA]:danno le stesse info

RIFLESSIONE E ANALISI CRITICA

12. Rimuovendo il filtro "udp.port == 53", quali altre informazioni sulla rete puoi dedurre dal traffico catturato?

[RISPOSTA]:Rimuovendo il filtro udp.port == 53, si vedrebbe tutto il "rumore" di fondo: traffico HTTP/HTTPS, protocolli di routing (ARP, ICMP), o messaggi di sistema

13. In ottica Ethical Hacking, come può un attaccante usare Wireshark (o lo sniffing DNS) per compromettere la sicurezza della rete?

[RISPOSTA]:Un attaccante può usare Wireshark per la ricognizione (sniffing). Vedendo le query DNS, può capire quali servizi usa la vittima, mappare l'architettura della rete o preparare attacchi di DNS Spoofing/Poisoning reindirizzando l'utente su siti malevoli

---