Report di Cattura Wireshark: Scansione Nmap da Kali a Metasploitable

1. Dettagli della rete

Host sorgente: 192.168.50.100

Host destinatario: 192.168.50.101

MAC sorgente: 08:00:27:ad:25:87

MAC destinatario: 08:00:27:5c:bf:f2

2. ARP Request/Reply

Pacchetto	Sorgente	Destinazione	Info
1	Broadcast	192.168.50.101	Who
2	192.168.50.101	192.168.50.100	192.1

3. Pacchetti TCP SYN (Porte Scansionate)

Frame No.	Sorgente	Destinazione	Risposta
5	59813	3389	RST-ACK
8	59813	256	RST-ACK
12	59813	1025	RST-ACK

4. Pacchetti Frammentati

Frame No.	Offset	ID	Descrizione
3, 4	0, 8	420e	Riassemblato in pacchetto completo
6, 7	0, 8	c2c4	Riassemblato in pacchetto completo

5. Conclusioni

La scansione Nmap ha utilizzato il flag -f per frammentare i pacchetti, come confermato dall'analisi dei frammenti catturati. Diversi pacchetti TCP SYN sono stati inviati verso porte aperte e chiuse, con risposte RST-ACK indicative delle porte chiuse. Il traffico frammentato potrebbe essere utile per eludere sistemi IDS/IPS poco sofisticati.