

## Report vari tipi di scansione da Kali a Metasploitable

Dopo aver connesso le macchine a rete interna con indirizzi ip statici possiamo iniziare la scansione di Metasploitable da Kali utilizzando Nmap.

### 1) Scansione di tipo -sS

Eseguite da terminale root il comando:

*nmap -sS 192.168.50.101*

Tale scansione viene detta di tipo meno invasivo (o SYN) poiché chiede informazioni sulle porte e servizi all'altra macchina senza stabilire una vera e propria connessione, infatti ottenute le informazioni desiderate resetta la connessione (RST). Possiamo notare tutto ciò dalla schermata di wireshark che catturava i pacchetti durante tale scansione.

1507	9.109691750	192.168.50.100	192.168.50.101	TCP	58 40682 → 7999 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1510	9.109741719	192.168.50.100	192.168.50.101	TCP	58 40682 → 1500 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1511	9.109789876	192.168.50.100	192.168.50.101	TCP	58 40682 → 2049 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1520	9.109855506	192.168.50.100	192.168.50.101	TCP	58 40682 → 4900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1522	9.109873220	192.168.50.100	192.168.50.101	TCP	58 40682 → 8084 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1523	9.109888916	192.168.50.100	192.168.50.101	TCP	58 40682 → 5087 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1524	9.109904451	192.168.50.100	192.168.50.101	TCP	58 40682 → 1216 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1525	9.109920849	192.168.50.100	192.168.50.101	TCP	58 40682 → 1700 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1526	9.109933849	192.168.50.100	192.168.50.101	TCP	58 40682 → 23502 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1527	9.109947292	192.168.50.100	192.168.50.101	TCP	58 40682 → 8011 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1528	9.109959830	192.168.50.100	192.168.50.101	TCP	58 40682 → 40161 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
L 1530	9.109995483	192.168.50.100	192.168.50.101	TCP	54 40682 → 2049 [RST] Seq=1 Win=0 Len=0
1531	9.110015835	192.168.50.100	192.168.50.101	TCP	58 40682 → 1504 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

### 2) Scansione di tipo -sT

A differenza della prima scansione questa utilizza una vera e propria connessione TCP completando il three-way-handshake. Viene considerata più "invasiva" in quanto è più facilmente identificabile.

tcp.dstport == 6000					
No.	Time	Source	Destination	Protocol	Length Info
1624	9.065166976	192.168.50.100	192.168.50.101	TCP	74 57290 → 6000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
1719	9.067720627	192.168.50.100	192.168.50.101	TCP	66 57290 → 6000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
L 1732	9.070948620	192.168.50.100	192.168.50.101	TCP	66 57290 → 6000 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0

In questo caso abbiamo preso come esempio la porta 6000. Possiamo notare la fase di SYN,ACK e RST (sincronizzazione, apprendimento e reset) l'ultima delle tre è utilizzata al posto del finale per non creare connessioni fatte e finite più facilmente identificabili.

Da tali scansioni otteniamo:

Tipo di scansione	Richiedente	Destinatario	Porte e servizi aperti
-sS	192.168.50.100(kali)	192.168.50.101(Metasploitable)	23
-sT	192.168.50.100(kali)	192.168.50.101(Metasploitable)	23