Risultati delle Scansioni

Fonte dello Scan	Target dello Scan	Tipo di Scan	Porte Aperte
Kali Linux (192.168.50.100)	Metasploitable 2 (192.168.50.101)	nmap -sS -p 0-1023	21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 25/tcp (smtp), 53/tcp (domain), 80/tcp (http), 111/tcp (rpcbind), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 512/tcp (exec), 513/tcp (login), 514/tcp (shell)
Kali Linux (192.168.50.100)	Metasploitable 2 (192.168.50.101)	nmap -sT -p 0-1023	21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 25/tcp (smtp), 53/tcp (domain), 80/tcp (http), 111/tcp (rpcbind), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 512/tcp (exec), 513/tcp (login), 514/tcp (shell)

Considerazioni

1. Le porte aperte rilevate con la scansione SYN e la scansione TCP completa sono le stesse, il che indica che i servizi attivi sono stati rilevati correttamente.
2. Le scansioni di rete possono rivelare porte e servizi aperti che potrebbero essere sfruttati da un attaccante. È importante verificare la necessità di questi servizi e proteggerli adeguatamente.
3. Mantieni una documentazione chiara e organizzata dei risultati delle scansioni per una migliore gestione della sicurezza della rete.