Traccia:
Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:
-OS fingerprint
-Syn Scan
-TCP connect
-Version detection

Ambiente:
Macchina attaccante Kali Linux VM con ip 192.168.1.100 e scheda di rete bridged
Macchina target Windows 7 VM con ip 192.168.1.102 e scheda di rete bridged

Svolgimento:
-IP: 192.168.1.102
-S.O.: Microsoft Windows 7|2008|8.1
-Porte aperte e servizi attivi:

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
5357/tcp	open	wsdapi
49152/tcp	open	unknown
49153/tcp	open	unknown
49154/tcp	open	unknown
49155/tcp	open	unknown
49156/tcp	open	unknown
49157/tcp	open	unknown