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 Metasploitable VM con ip 192.168.1.101 e scheda di rete bridged

Svolgimento:
-IP: 192.168.1.101
-S.O.: Linux 2.6.9 - 2.6.33
-Porte aperte e servizi attivi:

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
2121/tcp	open	ccproxy-ftp
3306/tcp	open	mysql
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	open	ajp13
8180/tcp	open	unknown