

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint
- Syn Scan
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection

A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un report contenente le seguenti info (dove disponibili):

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

PORTE APERTE:

Nmap scan report for 192.168.0.101 (192.168.0.101)

Host is up (0.0013s latency).

Not shown: 978 closed tcp ports (conn-refused)

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  
8180/tcp open unknown  
MAC Address: 08:00:27:B1:7C:1D (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux\_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
Network Distance: 1 hop

Host script results:

| smb-os-discovery:  
| OS: Unix (Samba 3.0.20-Debian)  
| Computer name: metasploitable  
| NetBIOS computer name:  
| Domain name: localdomain  
| FQDN: metasploitable.localdomain  
|\_ System time: 2024-04-30T13:41:07-04:00