Cyber Security

Class no 07

28 Sep 2024

┌──(root㉿kali)-[/home/kali]

└─# ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.0.9 netmask 255.255.255.0 broadcast 192.168.0.255

inet6 fe80::a00:27ff:febf:85f0 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:bf:85:f0 txqueuelen 1000 (Ethernet)

RX packets 653 bytes 370860 (362.1 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 654 bytes 76819 (75.0 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 4 bytes 240 (240.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 4 bytes 240 (240.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

┌──(root㉿kali)-[/home/kali]

└─# nmap -sn 192.168.0.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 05:09 EST

Nmap scan report for 192.168.0.1

Host is up (0.095s latency).

MAC Address: 58:D5:6E:AB:76:5C (D-Link International)

Nmap scan report for 192.168.0.3

Host is up (0.16s latency).

MAC Address: 9C:2E:A1:D6:58:77 (Xiaomi Communications)

Nmap scan report for 192.168.0.8

Host is up (0.00056s latency).

MAC Address: 74:04:F1:11:0E:86 (Intel Corporate)

Nmap scan report for 192.168.0.10

Host is up (0.00097s latency).

MAC Address: 08:00:27:1B:FC:30 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.0.9

Host is up.

Nmap done: 256 IP addresses (5 hosts up) scanned in 9.05 seconds

┌──(root㉿kali)-[/home/kali]

└─# nmap -sT 192.168.0.10

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 05:12 EST

Nmap scan report for 192.168.0.10

Host is up (0.0039s latency).

Not shown: 977 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

8009/tcp open ajp13

8180/tcp open unknown

MAC Address: 08:00:27:1B:FC:30 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds

┌──(root㉿kali)-[/home/kali]

└─# nmap -sV 192.168.0.10

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 05:29 EST

Nmap scan report for 192.168.0.10

Host is up (0.00036s latency).

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

53/tcp open domain ISC BIND 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

111/tcp open rpcbind 2 (RPC #100000)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login OpenBSD or Solaris rlogind

514/tcp open tcpwrapped

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp open vnc VNC (protocol 3.3)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd (Admin email admin@Metasploitable.LAN)

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

MAC Address: 08:00:27:1B:FC:30 (Oracle VirtualBox virtual NIC)

Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 11.82 seconds

┌──(root㉿kali)-[/home/kali]

└─# nmap -A 192.168.0.10 -p 80

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 05:32 EST

Nmap scan report for 192.168.0.10

Host is up (0.0018s latency).

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|\_http-title: Metasploitable2 - Linux

|\_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

MAC Address: 08:00:27:1B:FC:30 (Oracle VirtualBox virtual NIC)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

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

TRACEROUTE

HOP RTT ADDRESS

1 1.78 ms 192.168.0.10

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 7.93 seconds

┌──(root㉿kali)-[/home/kali]

└─# nmap -O 192.168.0.10

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 06:19 EST

Nmap scan report for 192.168.0.10

Host is up (0.0016s latency).

Not shown: 977 closed tcp ports (reset)

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

MAC Address: 08:00:27:1B:FC:30 (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 2.6.13 - 2.6.32

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds