Lab 2 - BlackBox Nmap Scanning

Scanning

Perform an active discovery analysis of the Pentesting VM using Kali VM (Nmap) to gather the following information. Use methods that minimize firewall detection, but do not worry about time and rate limit factors when constructing Nmap queries. (5 points)

1. **IP Address and MAC Address of the Pentesting VM**: To find the IP address and MAC address of the Pentesting VM, you can run the following Nmap command:

   ```
   nmap -sn 10.0.2.0/24
   ```

   This will perform a simple ping scan (`-sn`), which will only determine whether the target is online and will provide you with the IP address and MAC address of the Pentesting VM = **10.0.2.15**. Refer Figure 2.1 and 2.1.2
2. **All open TCP ports on the Pentesting VM**: Use the following Nmap command to scan for open TCP ports:

   ```
   nmap -sT -p- -T4 10.0.2.15 --packet-trace
   ```

   This command will scan all 65535 TCP ports (`-p-`) aggressively (`-T4`) to find open ports on the Pentesting VM. Refer Figure 2.2
3. **All open UDP ports on the Pentesting VM**: Run the following Nmap command to scan for open UDP ports:

   ```
   nmap -sU -PS -p- 10.0.2.15 --packet-trace
   ```

   This command will scan all 65535 UDP ports to find open ports on 10.0.2.15. Refer Figure 2.3
4. **Detect actual services and their respective versions**: Once you have identified open TCP and UDP ports, you can use Nmap's service version detection feature to determine the services running on those ports along with their versions. Refer Figure 2.4 Use the following command:

   ```
   nmap -sV -p- 10.0.2.15 --packet-trace
   ```

5. **Operating System of the Pentesting VM**: To identify the operating system of the Pentesting VM, you can use Nmap's OS detection feature. Refer Figure 2.5 Run the following command:

   ```
   nmap -O 10.0.2.15 --packet-trace
   ```

Wireshark or --packet-trace

Regarding how Nmap collects this data using packet trace or Wireshark:

a. **Identify the IP Address and MAC Address**: Nmap sends out ARP requests and analyzes the responses to determine the IP and MAC addresses of hosts on the network. Refer Figure 2.1 and 2.1.2

b. **Identify an open TCP port**: Nmap sends SYN packets to various ports and analyzes the responses. If a SYN/ACK is received, it indicates an open port. if RST is received it is considered as closed port. Using packet trace we can deduce if a connection is successful (open) or refused (closed). Refer the below screenshot for reference. Refer Figure 2.2

c. **Identify an open UDP port**: Nmap sends UDP packets to various ports and analyzes the responses. If an ICMP port unreachable message is not received, it indicates an open port.

Here using `-PS` we are also sending TCP SYN packets to see if any ports responds to UDP and TCP SYN packets while running UDP scan. Refer Figure 2.3

d. **Detect the service and service version on an open TCP port**: Nmap sends probes tailored to specific services and analyzes the responses to determine the service and its version. we use `-sV` to detect the services and their versions running. Nmap has its `nmap-services` database of about 2,200 well-known services, Nmap would report that those ports probably corresponding services like SMB, HTTP etc., Refer Figure 2.4

e. **Detect the specific operating system**: Nmap analyzes various aspects of network communication, including TCP/IP stack behavior and responses to specific probes, to make an educated guess about the target's operating system. Refer Figure 2.5

Figures

Figure 2.1

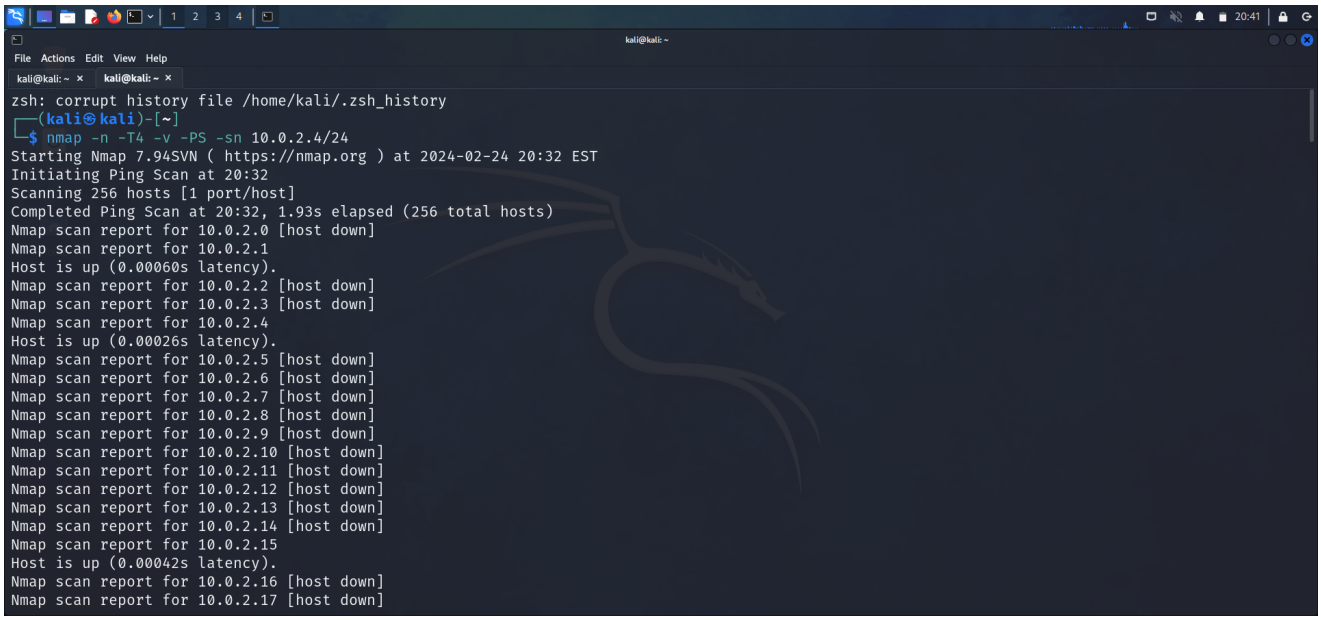


Figure 2.1.2

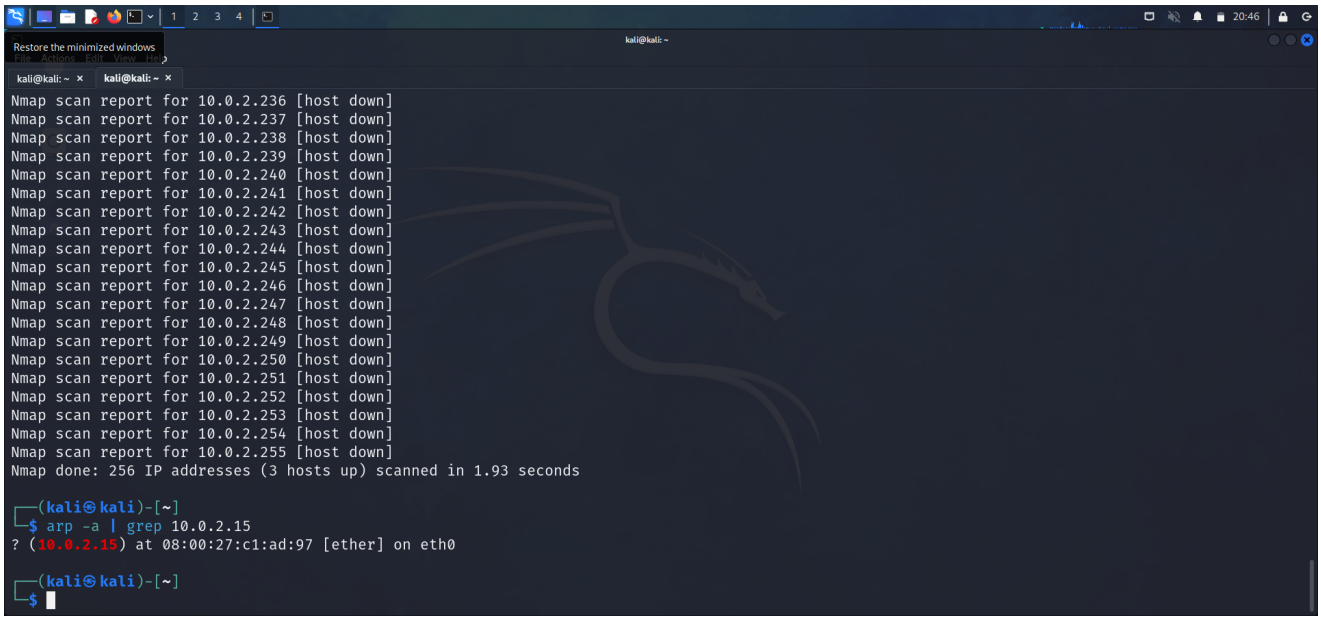


Figure 2.2

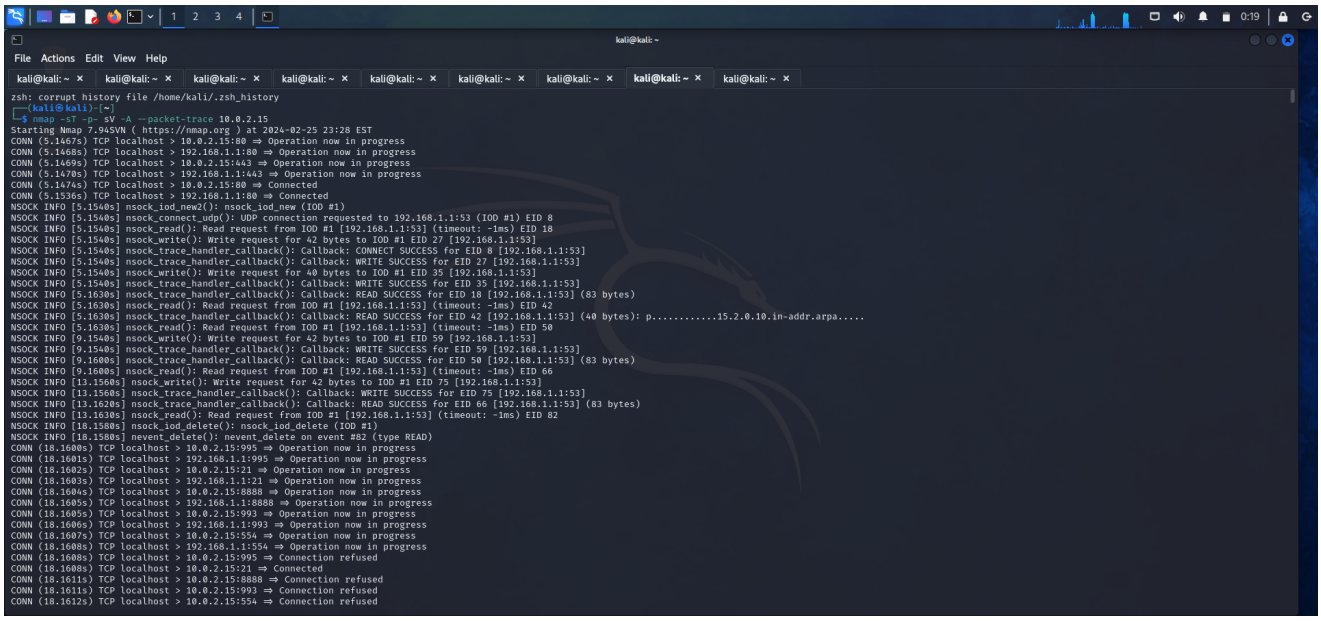


Figure 2.3

Figure 2.4

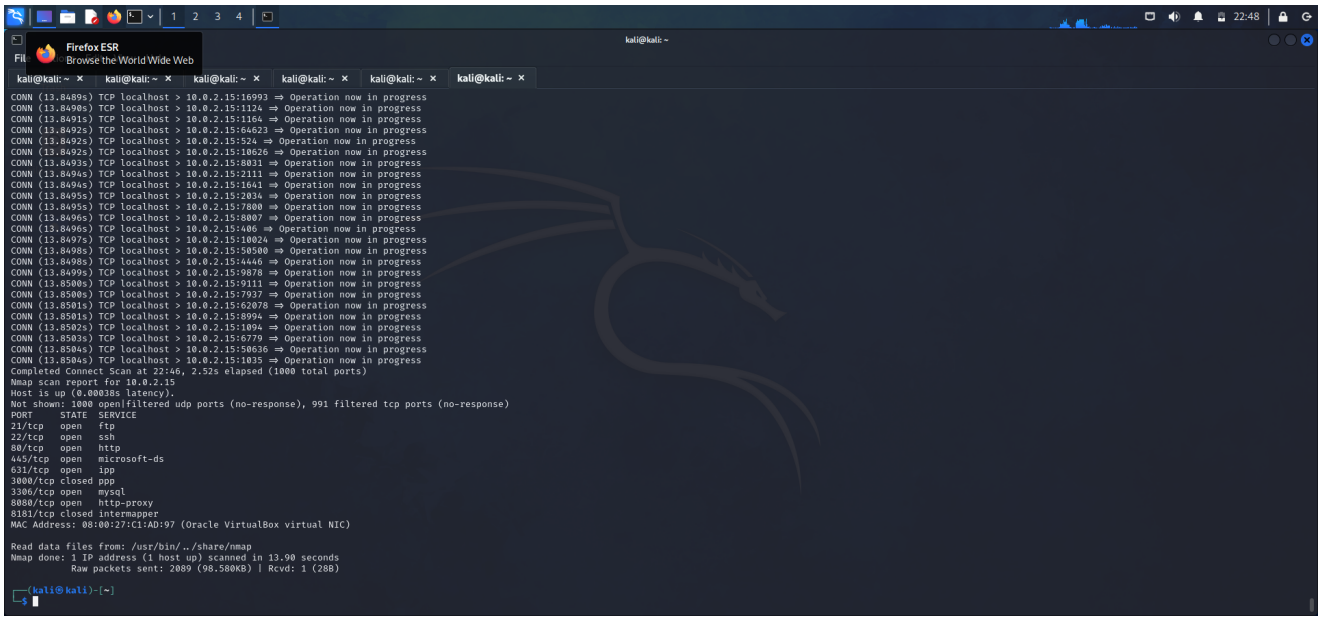
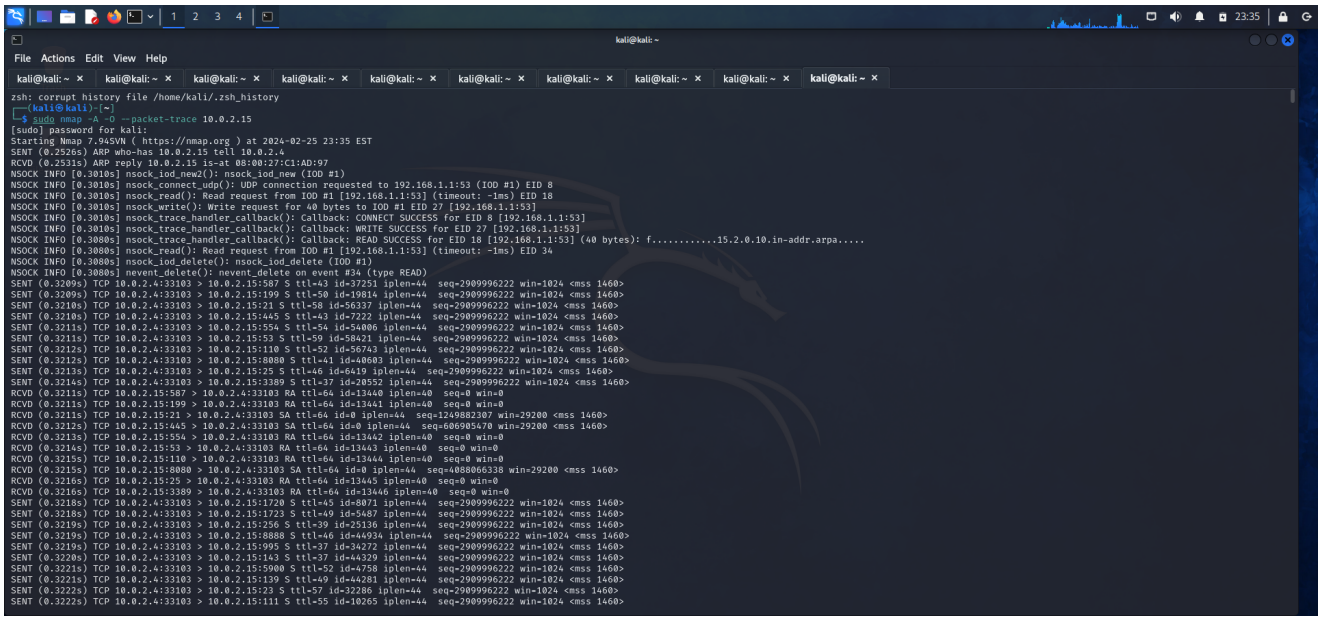


Figure 2.5


kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -O --packet-trace 10.0.2.15
[sudo] password for kali:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-25 23:35 EST
SENT (0.2526s) ARP who-has 10.0.2.15 tell 10.0.2.4
RCVD (0.2531s) ARP reply 10.0.2.15 is-at 08:00:27:C1:AD:97
NSOCK INFO [0.3010s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.3010s] nsock_connect_udp(): UDP connection requested to 192.168.1.1:53 (IOD #1) EID 8
NSOCK INFO [0.3010s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeout: -1ms) EID 18
NSOCK INFO [0.3010s] nsock_write(): Write request for 40 bytes to IOD #1 EID 27 [192.168.1.1:53]
NSOCK INFO [0.3010s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.1.1:53]
NSOCK INFO [0.3010s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [192.168.1.1:53]
NSOCK INFO [0.3080s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.1.1:53] (40 bytes): f...........15.2.0.10.in-addr.arpa.....
NSOCK INFO [0.3080s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeout: -1ms) EID 34
NSOCK INFO [0.3080s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.3080s] nevent_delete(): nevent_delete on event #34 (type READ)
SENT (0.3209s) TCP 10.0.2.4:33103 > 10.0.2.15:587 S ttl=43 id=37251 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3209s) TCP 10.0.2.4:33103 > 10.0.2.15:199 S ttl=50 id=19814 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3210s) TCP 10.0.2.4:33103 > 10.0.2.15:21 S ttl=58 id=56337 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3210s) TCP 10.0.2.4:33103 > 10.0.2.15:445 S ttl=43 id=7222 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3211s) TCP 10.0.2.4:33103 > 10.0.2.15:554 S ttl=54 id=54006 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3211s) TCP 10.0.2.4:33103 > 10.0.2.15:53 S ttl=59 id=58421 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3212s) TCP 10.0.2.4:33103 > 10.0.2.15:110 S ttl=52 id=56743 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3212s) TCP 10.0.2.4:33103 > 10.0.2.15:8080 S ttl=41 id=40603 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3213s) TCP 10.0.2.4:33103 > 10.0.2.15:25 S ttl=46 id=6419 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3214s) TCP 10.0.2.4:33103 > 10.0.2.15:3389 S ttl=37 id=20552 iplen=44 seq=2909996222 win=1024 <mss 1460>
RCVD (0.3211s) TCP 10.0.2.15:587 > 10.0.2.4:33103 RA ttl=64 id=13440 iplen=40 seq=0 win=0
RCVD (0.3211s) TCP 10.0.2.15:199 > 10.0.2.4:33103 RA ttl=64 id=13441 iplen=40 seq=0 win=0
RCVD (0.3211s) TCP 10.0.2.15:21 > 10.0.2.4:33103 SA ttl=64 id=0 iplen=44 seq=1249882307 win=29200 <mss 1460>
RCVD (0.3212s) TCP 10.0.2.15:445 > 10.0.2.4:33103 SA ttl=64 id=0 iplen=44 seq=606905470 win=29200 <mss 1460>
RCVD (0.3213s) TCP 10.0.2.15:554 > 10.0.2.4:33103 RA ttl=64 id=13442 iplen=40 seq=0 win=0
RCVD (0.3214s) TCP 10.0.2.15:53 > 10.0.2.4:33103 RA ttl=64 id=13443 iplen=40 seq=0 win=0
RCVD (0.3215s) TCP 10.0.2.15:110 > 10.0.2.4:33103 RA ttl=64 id=13444 iplen=40 seq=0 win=0
RCVD (0.3215s) TCP 10.0.2.15:8080 > 10.0.2.4:33103 SA ttl=64 id=0 iplen=44 seq=4088066338 win=29200 <mss 1460>
RCVD (0.3216s) TCP 10.0.2.15:25 > 10.0.2.4:33103 RA ttl=64 id=13445 iplen=40 seq=0 win=0
RCVD (0.3216s) TCP 10.0.2.15:3389 > 10.0.2.4:33103 RA ttl=64 id=13446 iplen=40 seq=0 win=0
SENT (0.3218s) TCP 10.0.2.4:33103 > 10.0.2.15:1720 S ttl=43 id=8071 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3218s) TCP 10.0.2.4:33103 > 10.0.2.15:1723 S ttl=49 id=5487 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3219s) TCP 10.0.2.4:33103 > 10.0.2.15:256 S ttl=39 id=25136 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3219s) TCP 10.0.2.4:33103 > 10.0.2.15:8888 S ttl=46 id=44934 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3219s) TCP 10.0.2.4:33103 > 10.0.2.15:995 S ttl=37 id=34272 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3220s) TCP 10.0.2.4:33103 > 10.0.2.15:143 S ttl=37 id=44329 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3221s) TCP 10.0.2.4:33103 > 10.0.2.15:5900 S ttl=52 id=4758 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3221s) TCP 10.0.2.4:33103 > 10.0.2.15:139 S ttl=49 id=44281 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3222s) TCP 10.0.2.4:33103 > 10.0.2.15:23 S ttl=57 id=32286 iplen=44 seq=2909996222 win=1024 <mss 1460>
SENT (0.3222s) TCP 10.0.2.4:33103 > 10.0.2.15:111 S ttl=55 id=10265 iplen=44 seq=2909996222 win=1024 <mss 1460>