ASSIGNMENT ON NMAP AND WIRESHARK

MC233103

Abdur Rahim

MCSE Network Security

Mobile: 01711152414

Email: rahim.c4d@gmail.com

Wireshark – a sniffing tool

No.	Time	Source	Destination
3505	110.520320392	10.0.2.15	103.163.210.127
3506	110.520414720	103.163.210.127	10.0.2.15
3507	110.520417644	10.0.2.15	103.163.210.127
3508	110.520490159	103.163.210.127	10.0.2.15
3509	110.520492914	10.0.2.15	103.163.210.127
3510	110.520585090	103.163.210.127	10.0.2.15
3511	110.520592531	10.0.2.15	103.163.210.127
3512	110.520879591	103.163.210.127	10.0.2.15
3513	110.520883613	10.0.2.15	103.163.210.127
3514	110.520992211	103.163.210.127	10.0.2.15
3515	110.520992270	103.163.210.127	10.0.2.15
3516	110.520997537	10.0.2.15	103.163.210.127
3517	110.521042666	103.163.210.127	10.0.2.15
3518	110.521045257	10.0.2.15	103.163.210.127
3519	110.521104951	103.163.210.127	10.0.2.15
3520	110.521109142	10.0.2.15	103.163.210.127
3521	110.525229981	103.163.210.127	10.0.2.15
3522	110.525258015	10.0.2.15	103.163.210.127
3523	110.525230233	103.163.210.127	10.0.2.15

```
▸ Frame 10: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▾ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_53:0c:ba (08:00:27:5
  ▸ Destination: PcsCompu_53:0c:ba (08:00:27:53:0c:ba)
  ▸ Source: RealtekU_12:35:02 (52:54:00:12:35:02)
    Type: IPv4 (0x0800)
    Padding: 000000000000
▾ Internet Protocol Version 4, Src: 151.101.1.140, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x1cef (7407)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xb8e1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 151.101.1.140
    Destination Address: 10.0.2.15
```

eth0: <live capture in progress>

3550	110.529101637	10.0.2.15	103.163.210.127
3551	110.529110072	103.163.210.127	10.0.2.15
3552	110.529112752	10.0.2.15	103.163.210.127
3553	110.532019083	103.163.210.127	10.0.2.15
3554	110.532023111	10.0.2.15	103.163.210.127
3555	110.532019132	103.163.210.127	10.0.2.15
3556	110.532019158	103.163.210.127	10.0.2.15
3557	110.532031779	10.0.2.15	103.163.210.127
3558	110.532060210	103.163.210.127	10.0.2.15
3559	110.532060232	103.163.210.127	10.0.2.15

```
Acknowledgment Number: 3945    (relative ack number)
Acknowledgment number (raw): 1860672812
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 65535
[Calculated window size: 65535]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x5d1c [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (5840 bytes)
TCP segment data (262 bytes)
[Reassembled PDU in frame: 3560]
TCP segment data (1460 bytes)
[3 Reassembled TCP Segments (4118 bytes): #3523(976), #3525(2880), #3551(262)]
Transport Layer Security
Transport Layer Security
```

```
0030  ff ff 5d 1c 00 00 a9 4b  28 33 d7 8e 43 eb 07 63   ··]···K (3··C··c
0040  93 73 7d 55 64 0d c1 94  51 7c 93 61 cc d8 c3 97   ·s}Ud··· Q|·a····
0050  87 e3 a4 d3 79 cc 60 ca  09 e5 18 c4 65 42 83 59   ····y·`· ····eB·Y
0060  d8 cd 41 6d bf d5 94 ff  21 fe 81 4c 93 35 6b 75   ··Am···· !··L·5ku
0070  21 89 58 bf c0 6a be f2  c9 62 c4 73 49 7d 71 92   !·X··j·· ·b·sI}q·
0080  00 81 e3 b6 27 8b cb 01  00 fd 41 79 55 ef f2 6b   ····'··· ··AyU··k
0090  98 b4 46 33 e1 af 7d 60  ed 2d 16 a4 b5 cd 2a bd   ··F3··}` ·-····*·
00a0  ba 2e 6e bb 06 9a d7 04  e0 a7 52 70 ea 7c 25 e1   ··n····· ··Rp·|%·
00b0  9e af c8 bd c7 e5 4c e7  70 8b 1b 4e 47 45 a3 ad   ======L· p··NGE··
00c0  31 99 9a 46 e0 5b 11 d6  c7 64 07 fc 69 fb 93 86   1··F·[·· ·d··i···
00d0  05 25 27 5a 82 18 a9 17  cf 7f e4 52 2f 2e 1b a8   ·%'Z···· ···R/···
00e0  05 47 d1 e5 93 e9 1b 89  d0 60 d0 b2 48 38 0d 1c   ·G====== ·`··H8··
00f0  d8 5f eb 5e 03 84 38 56  cb 58 7d ac 89 e7 62 75   ·_·^··8V ·X}···bu
0100  64 35 de b4 06 0c 3d 7b  bc 51 3e cd 83 2d c2 48   d5····={ ·Q>···-·H
0110  57 4a 8b 6f 2a 72 7a 7b  a6 9b 6a b5 64 7d 08 8b   WJ·o*rz{ ··j·d}··
0120  0c 1f 94 1f 9a 98 ea c4  18 69 3f fa 23 52 fe 2a   ======== ·i?·#R·*
0130  fd 7c 3d 31 1a 3d e0 de  82 19 3a ee 17 03 03 10   ·|=1·=·· ··:·····
0140  11 30 26 62 09 dd f8 f7  26 59 f8 03 3c 61 aa 03   ·0&b···· &Y··<a··
0150  9f 2b 28 52 8a a9 66 4f  9c 47 f4 d6 5f 45 92 17   ·+(R··fO ·G··_E··
```

Frame (5894 bytes) | Reassembled TCP (4118 bytes)

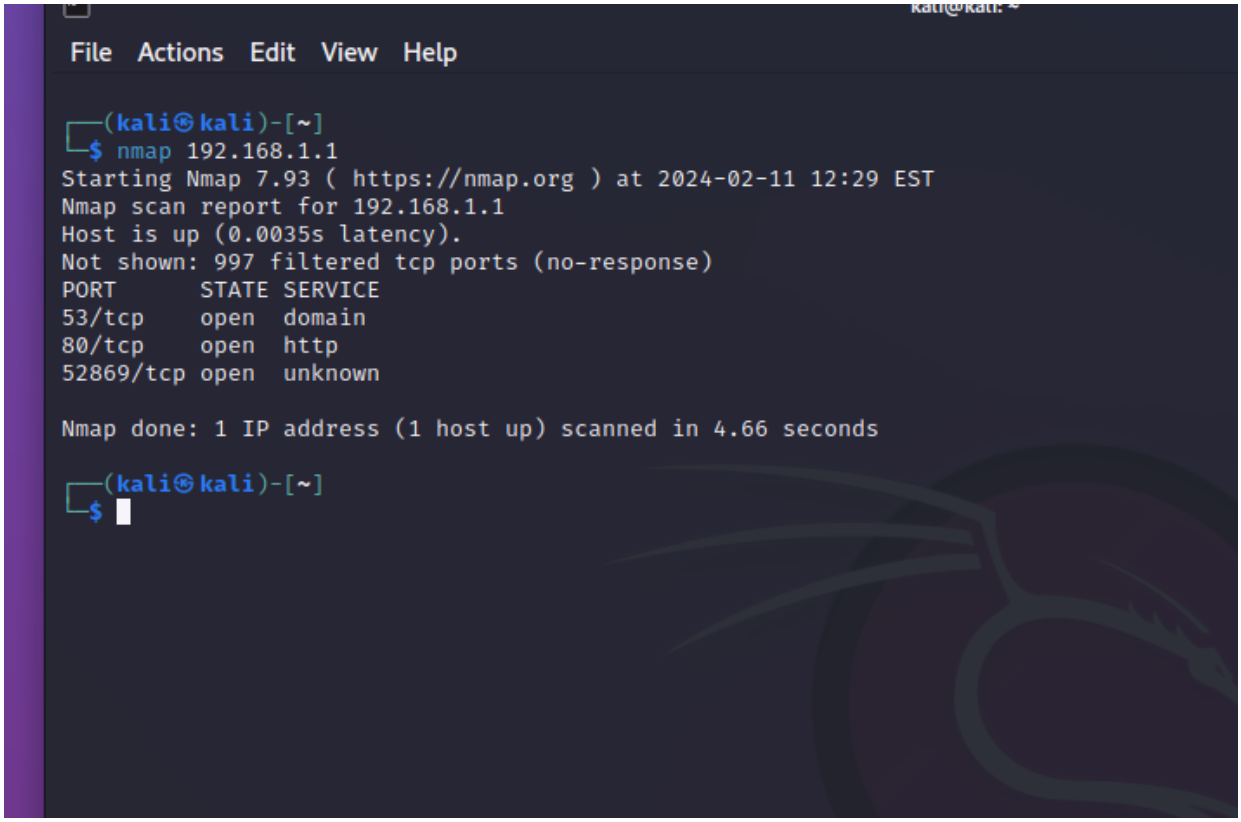
A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 262 bytes

Selected Packet: 3551 · Packets: 20143 · Displayed: 20143 (

3596	110.536796474	103.163.210.127	10.0.2.15
3597	110.536801793	10.0.2.15	103.163.210.127
3598	110.560919214	10.0.2.15	142.250.194.168
3599	110.561409008	142.250.194.168	10.0.2.15
3600	110.573138825	10.0.2.15	142.250.77.206
3601	110.573173191	10.0.2.15	142.250.77.206
3602	110.573183543	10.0.2.15	142.250.77.206
3603	110.573193969	10.0.2.15	142.250.77.206
3604	110.573202635	10.0.2.15	142.250.77.206
3605	110.573249053	10.0.2.15	103.163.210.127
3606	110.573606543	142.250.77.206	10.0.2.15
3607	110.573606937	142.250.77.206	10.0.2.15
3608	110.573606981	142.250.77.206	10.0.2.15
3609	110.573733496	142.250.77.206	10.0.2.15
3610	110.573733606	142.250.77.206	10.0.2.15
3611	110.584361128	10.0.2.15	103.163.210.127
3612	110.588981741	103.163.210.128	10.0.2.15

Nmap

Nmap, short for Network Mapper, is a powerful open-source network scanning tool used for network discovery and security auditing. Here are five commonly used Nmap commands:

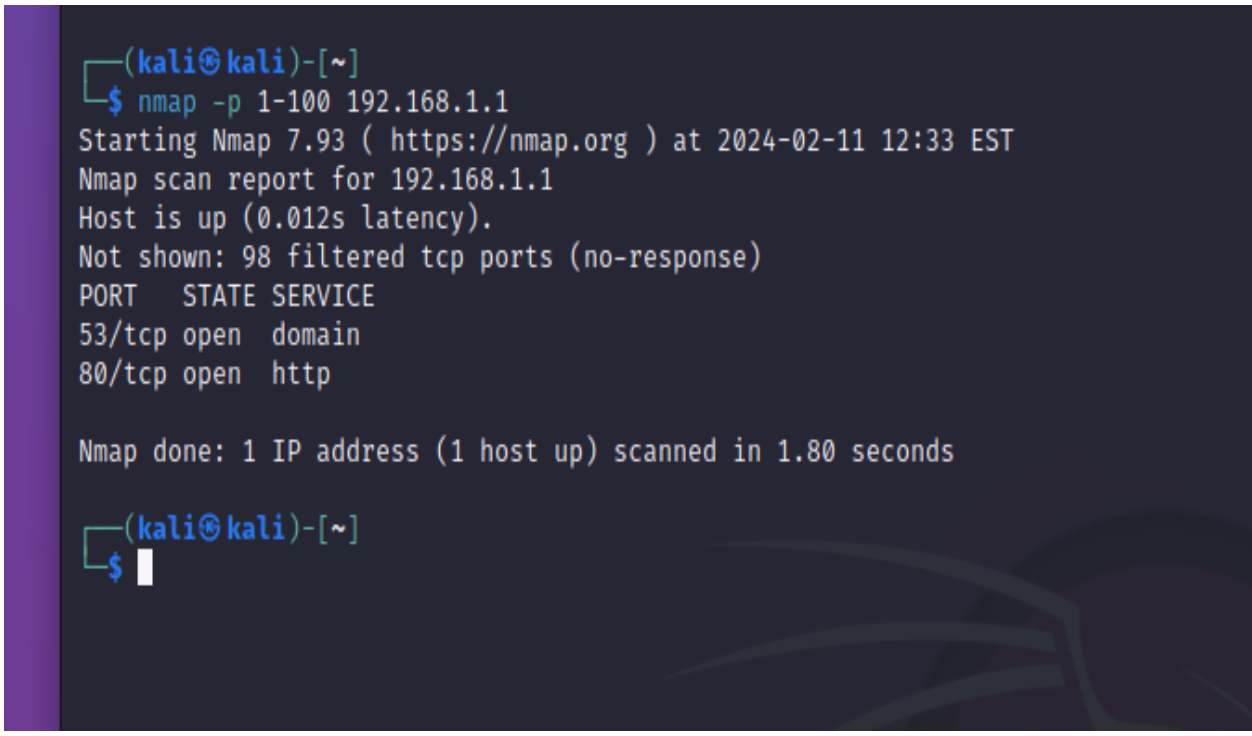
1. **Basic Scan:**
    - Command: **nmap [target]**
    - Description: Performs a basic scan on the specified target(s), identifying open ports, services, and operating system details.
    - Example: **nmap 192.168.1.1**
    - 

2. **Intense Scan:**
    - Command: **nmap -T4 -A -v [target]**

- Description: Conducts a more aggressive scan, including version detection (-A) and operating system detection (-O), with increased timing (-T4) and verbose output (-v).
- Example: **nmap -T4 -A -v 192.168.1.1**
-

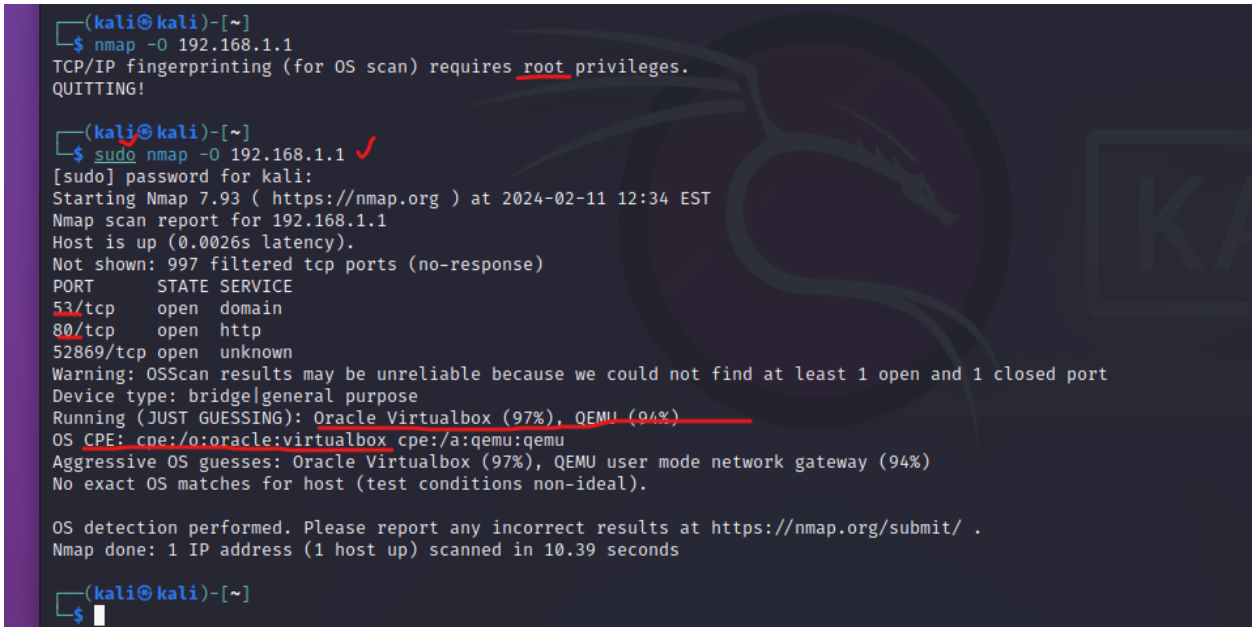
```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -A -v 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 12:31 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:31
Completed NSE at 12:31, 0.00s elapsed
Initiating NSE at 12:31
Completed NSE at 12:31, 0.00s elapsed
Initiating NSE at 12:31
Completed NSE at 12:31, 0.00s elapsed
Initiating Ping Scan at 12:31
Scanning 192.168.1.1 [2 ports]
Completed Ping Scan at 12:31, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:31
Completed Parallel DNS resolution of 1 host. at 12:31, 0.04s elapsed
Initiating Connect Scan at 12:31
Scanning 192.168.1.1 [1000 ports]
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 52869/tcp on 192.168.1.1
Completed Connect Scan at 12:31, 4.98s elapsed (1000 total ports)
Initiating Service scan at 12:31
Scanning 3 services on 192.168.1.1
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 12:32 (0:00:16 remaining)
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 12:32 (0:00:25 remaining)
```

3. **Port Range Scan:**
   - Command: **nmap -p [port range] [target]**
   - Description: Scans a specified range of ports on the target(s).
   - Example: **nmap -p 1-100 192.168.1.1**

- 

4. **Operating System Detection:**

- Command: **nmap -O [target]**
- Description: Attempts to identify the operating system running on the target(s) based on various characteristics and responses.
- Example: **nmap -O 192.168.1.1**

- 

5. Aggressive Timing and Firewall Evasion:
    - Command: nmap -T5 -f [target]
    - Description: Performs an aggressive scan with maximum timing (-T5) and fragmentation (-f) to bypass firewall restrictions and evade intrusion detection systems (IDS).
    - Example: nmap -T5 -f 192.168.1.1

```
┌──(kali㉿kali)-[~]
└─$ nmap -T5 -f 192.168.1.1
Sorry, but fragscan requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -T5 -f 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 12:39 EST
Nmap scan report for 192.168.1.1
Host is up (0.017s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 20.31 seconds

┌──(kali㉿kali)-[~]
└─$
```