

Lab Assignment - 4

Name: Anushareddy Ramachandra Reddy

1.Command: mkdir

Solution:

```
(kali㉿kali)-[~]  
$ cd Desktop  
  
(kali㉿kali)-[~/Desktop]  
$ cd Anushareddy_Ramachandra_reddy  
  
(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]  
$
```

2.Command : nslookup<targethost>

Solution:

```
(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]  
$ nslookup amazon.com  
Server:      129.120.210.235  
Address:     129.120.210.235#53  
  
Non-authoritative answer:  
Name:   amazon.com  
Address: 52.94.236.248  
Name:   amazon.com  
Address: 205.251.242.103  
Name:   amazon.com  
Address: 54.239.28.85  
  
(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]  
$ nslookup apple.com  
Server:      129.120.210.235  
Address:     129.120.210.235#53  
  
Non-authoritative answer:  
Name:   apple.com  
Address: 17.253.144.10  
  
(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]  
$
```

3.Command : nmap -h(Help Summary page)

Solution:

```
File Actions Edit View Help
(kali@kali) - [~/Desktop/Anushareddy_Ramachandra_reddy]
$ nmap -h
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sl: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
```

4.Command: nmap -sn<target>(Ping Scan)

Solution:

```
(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]
└─$ nmap -sn 17.253.144.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:21 EST
Nmap scan report for apple.com (17.253.144.10)
Host is up (0.027s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds

(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]
└─$ nmap -sn 17.253.144.10/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:23 EST
Nmap scan report for apple.com.ai (17.253.144.10)
Host is up (0.027s latency).
Nmap scan report for itunes.com (17.253.144.11)
Host is up (0.026s latency).
Nmap scan report for ads-apple.com.cn (17.253.144.12)
Host is up (0.031s latency).
Nmap scan report for 17.253.144.13
Host is up (0.026s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.73 seconds

(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]
└─$
```

5.Command: nmap -sL <target> (List Scan)

Solution:

```
(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]
└─$ nmap -sL 17.253.144.10/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:26 EST
Nmap scan report for 17.253.144.0
Nmap scan report for 17.253.144.1
Nmap scan report for 17.253.144.2
Nmap scan report for 17.253.144.3
Nmap scan report for 17.253.144.4
Nmap scan report for 17.253.144.5
Nmap scan report for 17.253.144.6
Nmap scan report for 17.253.144.7
Nmap scan report for 17.253.144.8
Nmap scan report for 17.253.144.9
Nmap scan report for apple.com.au (17.253.144.10)
Nmap scan report for primephonic.com (17.253.144.11)
Nmap scan report for ads-apple.apple.com.cn (17.253.144.12)
Nmap scan report for 17.253.144.13
Nmap scan report for 17.253.144.14
Nmap scan report for 17.253.144.15
Nmap scan report for 17.253.144.16
Nmap scan report for 17.253.144.17
Nmap scan report for 17.253.144.18
Nmap scan report for 17.253.144.19
Nmap scan report for 17.253.144.20
Nmap scan report for 17.253.144.21
Nmap scan report for 17.253.144.22
Nmap scan report for 17.253.144.23
Nmap scan report for 17.253.144.24
Nmap scan report for 17.253.144.25
Nmap scan report for 17.253.144.26
Nmap scan report for 17.253.144.27
Nmap scan report for 17.253.144.28
```

6.Command : nmap <target> (Scan all Ports)

Solution:

```
(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]
$ nmap 17.253.144.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:31 EST
Nmap scan report for aperturetrialbuy.apple.com (17.253.144.10)
Host is up (0.028s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.09 seconds

(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]
$
```

7.Command: nmap <port#><target> (Scan Specific Ports)

Solution:

```
(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]
$ nmap -p443 17.253.144.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:34 EST
Nmap scan report for vipd-healthcheck.a01.3banana.com (17.253.144.10)
Host is up (0.027s latency).

PORT      STATE SERVICE
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds

(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]
$
```

8.Command: nmap -sV<target>

Solution:

```
(kali@kali) - [~/Desktop/Anushareddy_Ramachandra_reddy]
$ nmap -sV 17.253.144.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:36 EST
Nmap scan report for squeakytoytrainingcamp.com (17.253.144.10)
Host is up (0.028s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http
443/tcp   open  ssl/https
2-Ports unrecognized despite returning data. If you know the service/version, please submit the following:
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF:Port80-TCP:V=7.94SVN1E=7%D=11/8%Time=672EBC95P=x86_64-pc-linux-gnu%r(G
SF:etRequest,2EF,"HTTP/1.\0\0x20400\0x20Host\0x20Header\0x20Required\r\nDate:
SF:x20Sat,\0x2009\0x20Nov\0x202024\0x2001:36:22\0x20GMT\r\nVia:\0x20http/1.\0x2
SF:0usmsc2-edge-bx-008\0x20ts.apple\0x20\0(acdn/262\0x2014454\0x20)\r\nCache-Con
SF:trol:\0x20no-store\r\nContent-Type:\0x20text/html\r\nContent-Language:\0x2
SF:0en\r\nX-Cache:\0x20none\r\nCDNUUID:\0x2083a2279d-e66b-40a9-8b6d-7e2dfb10
SF:756b-6998504851\r\nContent-Length:\0x20447\r\n\r\n<HTML>\n<HEAD>\n<TITLE
SF>\r\nHost\0x20Header\0x20Required</TITLE>\n<HEAD>\n<BODY\0x20BGCOLOR=\0x20"whit
SF:e"\0x20FGCOLOR=\0x20"black">\n<H1>Host\0x20Header\0x20Required</H1>\n<HR>\n\
SF:n<FONT\0x20FACE=\0x20"Helvetica,Arial">\n<B>\nDescription:\0x20Your\0x20browser
SF:\0x20did\0x20not\0x20send\0x20a\0x20"Host"\0x20HTTP\0x20header\0x20field\0x20and
SF:\0x20therefore\0x20the\0x20virtual\0x20host\0x20being\0x20requested\0x20could\
SF:\0x20not\0x20be\0x20determined\0x20.\nTo\0x20access\0x20this\0x20web\0x20site\0x20co
SF:rectly,\0x20you\0x20will\0x20need\0x20to\0x20upgrade\0x20to\0x20a\0x20browser\
SF:nthat\0x20supports\0x20the\0x20HTTP\0x20"Host"\0x20header\0x20field\0x20.\n</B>
```

9.Command: nmap<target> with*

Solution:

```
(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]
$ nmap 17.253.144.*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:38 EST
Nmap scan report for www.brkgls.com (17.253.144.10)
Host is up (0.035s latency).
Not shown: 997 filtered tcp ports (no-response), 1 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for primephonic.com (17.253.144.11)
Host is up (0.029s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for ads-apple.com.cn (17.253.144.12)
Host is up (0.060s latency).
Not shown: 996 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 17.253.144.13
Host is up (0.029s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 256 IP addresses (4 hosts up) scanned in 49.68 seconds
```

10.Command : nmap -A <target>

Solution:

```
(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]
$ nmap -A 17.253.144.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:42 EST
Nmap scan report for 17.253.144.13
Host is up (0.027s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 400 Host Header Required
|     Date: Sat, 09 Nov 2024 01:43:00 GMT
|     Via: http/1.1 usmsc2-edge-bx-002.ts.apple.com (acdn/262.14454)
|     Cache-Control: no-store
|     Content-Type: text/html
|     Content-Language: en
|     X-Cache: none
|     CDNUUID: f439391b-b173-4d5b-8a06-408d930caddc-7006295715
|     Content-Length: 447
|     <HTML>
|     <HEAD>
|     <TITLE>Host Header Required</TITLE>
|     </HEAD>
|     <BODY BGCOLOR="white" FGCOLOR="black">
|     <H1>Host Header Required</H1>
|     <HR>
|     <FONT FACE="Helvetica,Arial"><B>
|     Description: Your browser did not send a "Host" HTTP header field
|     therefore the virtual host being requested could not be determined.
|     access this web site correctly, you will need to upgrade to a browser
|     that supports the HTTP "Host" header field.
|     </B></FONT>
|     <HR>
```

11.Command : sudo nmap -O<target>

Solution:

```
(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]
$ sudo nmap -O 17.253.144.13
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:46 EST
Nmap scan report for 17.253.144.13
Host is up (0.013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.46 seconds

(kali㉿kali)-[~/Desktop/Anushareddy_Ramachandra_reddy]
$
```