

Information Security Management

Lab Assignment 4

Name: Devi Sree Pendyala

1. Command : mkdir

Solution :

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

2. Command : nslookup <targethost>

Solution :

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

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

Solution :

```
(kali㉿kali)-[~/Desktop/Devisree_pendyala]
$ 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[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
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
```

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

Solution :

```
(kali㉿kali)-[~/Desktop/Devisree_pendyala]
$ nmap -sn 17.253.144.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 23:48 EST
Nmap scan report for apple.com.bo (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/Devisree_pendyala]
$ nmap -sn 17.253.144.10/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 23:53 EST
Nmap scan report for apple.com.cn (17.253.144.10)
Host is up (0.027s latency).
Nmap scan report for primephonic.com (17.253.144.11)
Host is up (0.027s latency).
Nmap scan report for ads-apple.com.cn (17.253.144.12)
Host is up (0.027s latency).
Nmap scan report for 17.253.144.13
Host is up (0.027s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.55 seconds
```

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

Solution:

```
(kali㉿kali)-[~/Desktop/Devisree_pendyala]
$ nmap -sL 17.253.144.10/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 23:54 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.co (17.253.144.10)
Nmap scan report for maps.apple (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
Nmap scan report for 17.253.144.29
Nmap scan report for 17.253.144.30
Nmap scan report for 17.253.144.31
Nmap scan report for 17.253.144.32
Nmap scan report for 17.253.144.33
Nmap scan report for 17.253.144.34
Nmap scan report for 17.253.144.35
Nmap scan report for 17.253.144.36
Nmap scan report for 17.253.144.37
```

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

Solution:

```
(kali㉿kali)-[~/Desktop/Devisree_pendyala]
$ nmap 17.253.144.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 23:56 EST
Nmap scan report for apple.com.do (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 4.07 seconds
```

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

Solution :

```
(kali㉿kali)-[~/Desktop/Devisree_pendyala]
$ nmap -p443 17.253.144.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 10:31 EST
Nmap scan report for livepage.apple.com (17.253.144.10)
Host is up (0.040s latency).

PORT      STATE SERVICE
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

8.Command : nmap -sV<target>

Solution:

```
(kali㉿kali)-[~/Desktop/Devisree_pendyala]
$ nmap -sV 17.253.144.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 10:32 EST
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 10:33 (0:00:13 remaining)
Nmap scan report for seminars.apple.com (17.253.144.10)
Host is up (0.027s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
443/tcp   open  https
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port80-TCP:V=7.94SVN|I=7|D=11/10|Time=6730D22DXP|x86_64-pc-linux-gnu|Xr(
SF-GetRequest,2EF,"HTTP/1.0|x20400|x20Host|x20Header|x20Required\r\nDate:
SF:\x20Sun,\x2010\x20Nov\x202024\x2015:33:01\x20GMT\r\nVia:\x20http/1.1|x
SF:20usmc2-edge-bx-006|.ts|.apple|.com|x20(acdn/262|.14454|)|\r\nCache-Co
SF:ntrol:\x20no-store\r\nContent-Type:\x20text/html\r\nContent-Language:\x
SF:20en\r\nX-Cache:\x20none\r\nCDNUUID:\x201824575c-1e62-46b9-8c21-aba929
SF:f59e4-6873897577\r\nContent-Length:\x20447\r\n\r\n<HTML>\n<HEAD>\n<TITL
SF:E>Host\x20Header\x20Required</TITLE>\n</HEAD>\n<BODY>\x20BGOLOR=\x20whi
SF:te\x20\x20FGCOLOR=\x20black\x20>\n<H1>Host\x20Header\x20Required</H1>\n<HR>\n
SF:\n<FONT\x20FACE=\x20Helvetica,Arial\x20><B>\nDescription:\x20Your\x20browse
SF:r\x20did\x20not\x20send\x20a\x20"Host"\x20HTTP\x20header\x20field\nan
SF:d\x20therefore\x20the\x20virtual\x20host\x20being\x20requested\x20could
SF:\x20not\x20be\x20determined.\n\nTo\x20access\x20this\x20web\x20site\x20c
SF:orrectly,\x20you\x20will\x20need\x20to\x20upgrade\x20to\x20a\x20browser
SF:\nthat\x20supports\x20the\x20HTTP\x20"Host"\x20header\x20field.\n</B
SF:></FONT>\n<HR>\n</BODY>\n")&(HTTPOptions,2EF,"HTTP/1.0|x20400|x20Host
SF:\x20Header\x20Required\r\nDate:\x20Sun,\x2010\x20Nov\x202024\x2015:33:0
SF:1\x20GMT\r\nVia:\x20http/1.1|x20usmc2-edge-bx-006|.ts|.apple|.com|x20
SF:1(acdn/262|.14454|)|\r\nCache-Control:\x20no-store\r\nContent-Type:\x20t
SF:ext/html\r\nContent-Language:\x20en\r\nX-Cache:\x20none\r\nCDNUUID:\x20
SF:8aa5a482-20f1-4870-b734-1f5d7a264152-3845716884\r\nContent-Length:\x204
SF:47\r\n\r\n<HTML>\n<HEAD>\n<TITLE>Host\x20Header\x20Required</TITLE>\n<
SF:HEAD>\n\n<BODY>\x20BGOLOR=\x20white\x20\x20FGCOLOR=\x20black\x20>\n<H1>Host\x20
SF:Header\x20Required</H1>\n<HR>\n\n<FONT\x20FACE=\x20Helvetica,Arial\x20><B>\n
SF:Description:\x20Your\x20browser\x20did\x20not\x20send\x20a\x20"Host"
SF:\x20HTTP\x20header\x20field\nand\x20therefore\x20the\x20virtual\x20host
```

G. Command : nmap <target> with *

Solution:

```
(kali@kali)-[~/Desktop/Devisree_pendyala]
$ nmap 17.253.144.*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-09 00:03 EST
Stats: 0:00:43 elapsed; 252 hosts completed (4 up), 4 undergoing Connect Scan
Connect Scan Timing: About 74.97% done; ETC: 00:04 (0:00:14 remaining)
Nmap scan report for squeakytoytrainingcamp.com (17.253.144.10)
Host is up (0.030s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for maps.apple (17.253.144.11)
Host is up (0.034s 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 swift.org (17.253.144.12)
Host is up (0.033s 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 49.92 seconds
```

10. Command : nmap -A <target>

Solution:

```
(kali@kali)-[~/Desktop/Devisree_pendyala]
$ nmap -A 17.253.144.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-09 00:06 EST
Nmap scan report for 17.253.144.13
Host is up (0.028s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache/2.4.18
|_ fingerprint-strings:
|_   GetRequest:
|_     HTTP/1.0 400 Host Header Required
|_     Date: Sat, 09 Nov 2024 05:06:32 GMT
|_     Via: http/1.1 usmsc2-edge-bx-005.ts.apple.com (acdn/262.14454)
|_     Cache-Control: no-store
|_     Content-Type: text/html
|_     Content-Language: en
|_     X-Cache: none
|_     CDNUUID: 8a4ac5e4-5ef2-4ea0-b0b8-3bc8bcea97bb-7838191835
|_     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>
|_     </BODY>
|_   HTTPOptions:
|_     HTTP/1.0 400 Host Header Required
|_     Date: Sat, 09 Nov 2024 05:06:32 GMT
|_     Via: http/1.1 usmsc2-edge-bx-004.ts.apple.com (acdn/262.14454)
```

11.Command : sudo nmap -O<target>

Solution:

```
(kali@kali) [~/Desktop/Devisree_pendyala]
$ sudo nmap -O 17.253.144.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-09 00:09 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 version 3.1.0.22) (86%)
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 8.15 seconds
```