VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering

Lab Assessment-VII, OCTOBER 2020

B.Tech., Fall-2020-2021

NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	CSE3501
COURSE NAME	INFORMATION SECURITY ANALYSIS & AUDIT
SLOT	L19+L20
FACULTY	Prof. THANDEESWARAN R.

Create a Type the following commands in zenmap. Use different IP address and generate a report. Take a screen shot and write your comments on each command.

1. Scan a Host to Detect Firewall: namp –sA vit.ac.in

```
namp -sA vit.ac.in

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 00:46 India Standard Time
Nmap scan report for vit.ac.in (136.233.9.13)
Host is up (0.070s latency).
rDNS record for 136.233.9.13: 136.233.9.13.static.jio.com
All 1000 scanned ports on vit.ac.in (136.233.9.13) are filtered

Nmap done: 1 IP address (1 host up) scanned in 9.74 seconds
```

All the ports are **filtered** meaning there is a **Firewall present**.

2. Scan a host if it is protected by any packet filtering software or Firewalls: nmap -PN vit.ac.in

```
nmap -Pn vit.ac.in

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 00:55 India Standard Time
Nmap scan report for vit.ac.in (136.233.9.13)
Host is up (0.067s latency).
rDNS record for 136.233.9.13: 136.233.9.13.static.jio.com
Not shown: 992 closed ports
PORT    STATE    SERVICE
53/tcp  filtered domain
80/tcp  open     http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open     https
444/tcp filtered snpp
445/tcp filtered microsoft-ds
515/tcp filtered printer

Nmap done: 1 IP address (1 host up) scanned in 4.83 seconds
```

The ports are filtered therefore the host is protected by a **Firewall.**

3. Complete a scan in Stealth Mode: nmap -sS vit.ac.in

```
nmap -sS vit.ac.in

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:23 India Standard Time
Nmap scan report for vit.ac.in (136.233.9.13)
Host is up (0.063s latency).
rDNS record for 136.233.9.13: 136.233.9.13.static.jio.com
Not shown: 992 closed ports
PORT    STATE    SERVICE
53/tcp  filtered domain
80/tcp  open     http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open     https
444/tcp filtered snpp
445/tcp filtered microsoft-ds
515/tcp filtered printer

Nmap done: 1 IP address (1 host up) scanned in 5.03 seconds
```

4. Identify Host Names: nmap -sL vit.ac.in

```
nmap -sL vit.ac.in

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:26 India Standard Time
Nmap scan report for vit.ac.in (136.233.9.13)
rDNS record for 136.233.9.13: 136.233.9.13.static.jio.com
Nmap done: 1 IP address (0 hosts up) scanned in 1.05 seconds
```

5. Scan IPv6 Addresses: nmap -6 ::ffff:c0a8:1

```
nmap -6 fe80::f433:85e9:9870:6cdf%4

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:30 India Standard Time
Nmap scan report for fe80::f433:85e9:9870:6cdf
Host is up (0.0010s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
808/tcp  open  ccproxy-http
2869/tcp open  icslap

Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
```

6. Create Decoys while scanning: nmap -D 192.168.0.1, 192.168.0.2 192.168.101.4

```
nmap -D 192.168.0.1,192.168.0.2 192.168.101.4

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:36 India Standard Time
Nmap scan report for 192.168.101.4
Host is up (0.0035s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
808/tcp  open  ccproxy-http
2869/tcp open  icslap
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 2.11 seconds
```

Used **192.168.0.1 and 192.168.0.2** as **decoys** while **scanning 192.168.101.4**

7. Scan remote Hosts using SCTP: nmap -sZ --top-ports 20 -T4 192.168.101.1/24

Top 20 ports of each host scanned using SCTP.

PTO.

```
nmap -sZ -T4 --top-ports 20 192.168.101.1/24

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:38 India Standard Time
Nmap scan report for 192.168.101.1
Host is up (0.00s latency).

PORT      STATE         SERVICE
7/sctp    open|filtered echo
9/sctp    filtered      discard
20/sctp   open|filtered ftp-data
21/sctp   filtered      ftp
22/sctp   open|filtered ssh
80/sctp   open|filtered http
179/sctp  open|filtered bgp
443/sctp  open|filtered https
1167/sctp open|filtered cisco-ipsla
1812/sctp filtered      radius
1813/sctp open|filtered radacct
2049/sctp filtered      nfs
2225/sctp filtered      rcip-itu
2427/sctp filtered      mgcp-gateway
2904/sctp open|filtered m2ua
2905/sctp open|filtered m3ua
2944/sctp open|filtered megaco-h248
2945/sctp filtered      h248-binary
3097/sctp open|filtered itu-bicc-stc
3565/sctp open|filtered m2pa
MAC Address: E0:67:B3:A8:9F:95 (Shenzhen C-Data Technology)
```

8. Scan output in xml format: nmap -oX scan-report.xml -n 192.168.101.1

```
Administrator: Windows PowerShell
PS C:\> nmap     scan-report.xml    192.168.101.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 02:06 India Standard Time
Nmap scan report for 192.168.101.1
Host is up (0.012s latency).
Not shown: 995 closed ports
PORT    STATE    SERVICE
21/tcp  filtered ftp
23/tcp  open     telnet
80/tcp  open     http
139/tcp open     netbios-ssn
445/tcp open     microsoft-ds
MAC Address: E0:67:B3:A8:9F:95 (Shenzhen C-Data Technology)

Nmap done: 1 IP address (1 host up) scanned in 2.84 seconds
PS C:\> more scan-report.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///C:/Program Files (x86)/Nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.80 scan initiated Sat Oct 17 02:06:48 2020 as: &quot;C:\\Program Files (x8
```

Output is saved as scan-report.xml

9. Save nmap outputs: nmap -n 192.168.101.1 > scan-report

```
Administrator: Windows PowerShell
PS C:\> nmap     192.168.101.1 > scan-report
PS C:\> dir
```

```
-a----        17-10-2020     02:09            918 scan-report
-a----        17-10-2020     02:06           5892 scan-report.xml


PS C:\> more scan-report
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 02:09 India Standard Time
Nmap scan report for 192.168.101.1
Host is up (0.0042s latency).
Not shown: 995 closed ports
PORT    STATE    SERVICE
21/tcp  filtered ftp
23/tcp  open     telnet
80/tcp  open     http
139/tcp open     netbios-ssn
445/tcp open     microsoft-ds
MAC Address: E0:67:B3:A8:9F:95 (Shenzhen C-Data Technology)

Nmap done: 1 IP address (1 host up) scanned in 3.73 seconds
```

10. Using multiple script categories: nmap --script discovery brute 192.168.101.1

```
PS C:\> nmap --script discovery brute 192.168.101.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 02:12 India Standard Time
too short
too short
too short
too short
too short
Pre-scan script results:
| broadcast-igmp-discovery:
|   192.168.101.4
|     Interface: eth3
|     Version: 2
|     Group: 239.255.102.18
|     Description: Organization-Local Scope (rfc2365)
|_  Use the newtargets script-arg to add the results as targets
| ipv6-multicast-mld-list:
|   fe80::1:
|     device: eth3
|     mac: e0:67:b3:a8:9f:95
|     multicast_ips:
|       ff02::1:ff00:0           (Solicited-Node Address)
|       ff02::1:ff00:1           (NDP Solicited-node)
|       ff02::2                  (All Routers Address)
|       ff02::1:ffa8:9f95        (Solicited-Node Address)
|   fe80::4eed:fbff:fe21:c71a:
|     device: eth3
```

****