Parshvanath Charitable Trust's
A. P. SHAH INSTITUTE OF TECHNOLOGY
(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)
(Religious Jain Minority)

Department of Information Technology

Semester: V
Academic Year: 2021-22
Class / Branch: TE IT
Subject: Security Lab (SL)
Name of Instructor: Prof. Kiran Deshpande

Name of Student:Vishal Bangar
Student ID: 20104084

EXPERIMENT NO. 4

Aim : To Use Nmap for Network discovery and security Auditing.

TCP SYN Scan Output :

```
root@apsit-HP-245-G4-Notebook-PC:~# nmap -sS 127.0.0.1 -p  80

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-15 17:43 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
 with --dns-servers
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
root@apsit-HP-245-G4-Notebook-PC:~#
```

Tcpdump capture to analyze working of TCP SYN Scan or Half Scan :

```
root@apsit-HP-245-G4-Notebook-PC:~# tcpdump  -v -n -e -i lo   port 80
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
17:43:37.408302 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 58: (tos 0x0, ttl 43, id 62862, offset 0,
 flags [none], proto TCP (6), length 44)
    127.0.0.1.37324 > 127.0.0.1.80: Flags [S], cksum 0x689a (correct), seq 3120685419, win 1024, options [mss 1460], length 0
17:43:37.408335 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 58: (tos 0x0, ttl 64, id 0, offset 0, fla
gs [DF], proto TCP (6), length 44)
    127.0.0.1.80 > 127.0.0.1.37324: Flags [S.], cksum 0xfe20 (incorrect -> 0xe101), seq 3188795559, ack 3120685420, win 43690, o
ptions [mss 65495], length 0
17:43:37.408359 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 54: (tos 0x0, ttl 64, id 22508, offset 0,
 flags [DF], proto TCP (6), length 40)
    127.0.0.1.37324 > 127.0.0.1.80: Flags [R], cksum 0x8453 (correct), seq 3120685420, win 0, length 0
17:43:56.679701 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 58: (tos 0x0, ttl 48, id 7196, offset 0,
flags [none], proto TCP (6), length 44)
```

TCP connect() scan Output :

```
root@apsit-HP-245-G4-Notebook-PC:~# nmap -sT 127.0.0.1 -p  80

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-15 17:50 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
 with --dns-servers
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00019s latency).
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@apsit-HP-245-G4-Notebook-PC:~#
```

Tcpdump capture to analyze working of TCP Connect Scan or Full Scan :

```
root@apsit-HP-245-G4-Notebook-PC:~# tcpdump  -v -n -e -i lo  port 80
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
17:50:08.956533 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 74: (tos 0x0, ttl 64, id 16651, offset 0,
 flags [DF], proto TCP (6), length 60)
    127.0.0.1.41420 > 127.0.0.1.80: Flags [S], cksum 0xfe30 (incorrect -> 0x95d1), seq 3200808602, win 43690, options [mss 65495
,sackOK,TS val 5060497 ecr 0,nop,wscale 7], length 0
17:50:08.956570 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 74: (tos 0x0, ttl 64, id 0, offset 0, fla
gs [DF], proto TCP (6), length 60)
    127.0.0.1.80 > 127.0.0.1.41420: Flags [S.], cksum 0xfe30 (incorrect -> 0xffde), seq 3913118917, ack 3200808603, win 43690, o
ptions [mss 65495,sackOK,TS val 5060497 ecr 5060497,nop,wscale 7], length 0
17:50:08.956602 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 64, id 16652, offset 0,
 flags [DF], proto TCP (6), length 52)
    127.0.0.1.41420 > 127.0.0.1.80: Flags [.], cksum 0xfe28 (incorrect -> 0xd223), ack 1, win 342, options [nop,nop,TS val 50604
97 ecr 5060497], length 0
17:50:08.956655 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 64, id 16653, offset 0,
 flags [DF], proto TCP (6), length 52)
    127.0.0.1.41420 > 127.0.0.1.80: Flags [R.], cksum 0xfe28 (incorrect -> 0xd21f), seq 1, ack 1, win 342, options [nop,nop,TS v
al 5060497 ecr 5060497], length 0
```

TCP FIN scan Output :

```
root@apsit-HP-245-G4-Notebook-PC:~# nmap -sF 127.0.0.1 -p  80

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-15 17:54 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
 with --dns-servers
Nmap scan report for localhost (127.0.0.1)
Host is up.
PORT   STATE         SERVICE
80/tcp open|filtered http

Nmap done: 1 IP address (1 host up) scanned in 2.19 seconds
root@apsit-HP-245-G4-Notebook-PC:~#
```

Tcpdump capture to analyze working of FIN Scan :

```
root@apsit-HP-245-G4-Notebook-PC:~# tcpdump  -v -n -e -i lo   port 80
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
17:54:09.271747 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 54: (tos 0x0, ttl 51, id 6751, offset 0,
flags [none], proto TCP (6), length 40)
    127.0.0.1.38853 > 127.0.0.1.80: Flags [F], cksum 0x4387 (correct), seq 4091666018, win 1024, length 0
17:54:10.272755 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 54: (tos 0x0, ttl 48, id 852, offset 0, f
lags [none], proto TCP (6), length 40)
    127.0.0.1.38854 > 127.0.0.1.80: Flags [F], cksum 0x4386 (correct), seq 4091600483, win 1024, length 0
```

TCP Null scan Output :

```
root@apsit-HP-245-G4-Notebook-PC:~# nmap -sN 127.0.0.1 -p  81

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-15 17:57 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
 with --dns-servers
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00019s latency).
PORT   STATE  SERVICE
81/tcp closed hosts2-ns

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
root@apsit-HP-245-G4-Notebook-PC:~#
```

Tcpdump capture to analyze working of Null Scan :

```
root@apsit-HP-245-G4-Notebook-PC:~# tcpdump  -v -n -e -i lo   port 81
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
17:57:13.315969 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 54: (tos 0x0, ttl 58, id 8540, offset 0,
flags [none], proto TCP (6), length 40)
    127.0.0.1.53612 > 127.0.0.1.81: Flags [none], cksum 0x787d (correct), win 1024, length 0
17:57:13.316033 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 54: (tos 0x0, ttl 64, id 26669, offset 0,
 flags [DF], proto TCP (6), length 40)
    127.0.0.1.81 > 127.0.0.1.53612: Flags [R.], cksum 0x7c69 (correct), seq 0, ack 1638859256, win 0, length 0
```

TCP Version Scan Output :

```
root@apsit-HP-245-G4-Notebook-PC:~# nmap -sV 127.0.0.1 -p  80

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-15 17:58 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
 with --dns-servers
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00016s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.99 seconds
root@apsit-HP-245-G4-Notebook-PC:~#
```

Tcpdump capture to analyze working of Version Scan :

```
root@apsit-HP-245-G4-Notebook-PC:~# tcpdump  -v -n -e -i lo   port 80
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
17:58:56.267780 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 58: (tos 0x0, ttl 39, id 43635, offset 0,
 flags [none], proto TCP (6), length 44)
    127.0.0.1.58750 > 127.0.0.1.80: Flags [S], cksum 0x9be9 (correct), seq 2077333658, win 1024, options [mss 1460], length 0
17:58:56.267835 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 58: (tos 0x0, ttl 64, id 0, offset 0, fla
gs [DF], proto TCP (6), length 44)
    127.0.0.1.80 > 127.0.0.1.58750: Flags [S.], cksum 0xfe20 (incorrect -> 0x9898), seq 3031281091, ack 2077333659, win 43690, o
ptions [mss 65495], length 0
17:58:56.267866 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 54: (tos 0x0, ttl 64, id 50087, offset 0,
 flags [DF], proto TCP (6), length 40)
    127.0.0.1.58750 > 127.0.0.1.80: Flags [R], cksum 0xb7a2 (correct), seq 2077333659, win 0, length 0
17:58:56.680913 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 74: (tos 0x0, ttl 64, id 15364, offset 0,
 flags [DF], proto TCP (6), length 60)
    127.0.0.1.41426 > 127.0.0.1.80: Flags [S], cksum 0xfe30 (incorrect -> 0x19b4), seq 2805270248, win 43690, options [mss 65495
,sackOK,TS val 5192428 ecr 0,nop,wscale 7], length 0
17:58:56.680948 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 74: (tos 0x0, ttl 64, id 0, offset 0, fla
gs [DF], proto TCP (6), length 60)
    127.0.0.1.80 > 127.0.0.1.41426: Flags [S.], cksum 0xfe30 (incorrect -> 0xe416), seq 91813080, ack 2805270249, win 43690, opt
ions [mss 65495,sackOK,TS val 5192428 ecr 5192428,nop,wscale 7], length 0
17:58:56.680977 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 64, id 15365, offset 0,
 flags [DF], proto TCP (6), length 52)
    127.0.0.1.41426 > 127.0.0.1.80: Flags [.], cksum 0xfe28 (incorrect -> 0xb65b), ack 1, win 342, options [nop,nop,TS val 51924
28 ecr 5192428], length 0
17:59:02.683212 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 84: (tos 0x0, ttl 64, id 15366, offset 0,
 flags [DF], proto TCP (6), length 70)
    127.0.0.1.41426 > 127.0.0.1.80: Flags [P.], cksum 0xfe3a (incorrect -> 0xd1c4), seq 1:19, ack 1, win 342, options [nop,nop,T
S val 5193929 ecr 5192428], length 18: HTTP, length: 18
        GET / HTTP/1.0

17:59:02.683298 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 64, id 46096, offset 0,
 flags [DF], proto TCP (6), length 52)
    127.0.0.1.80 > 127.0.0.1.41426: Flags [.], cksum 0xfe28 (incorrect -> 0xaa8f), ack 19, win 342, options [nop,nop,TS val 5193
929 ecr 5193929], length 0
```

Nmap OS Detection Output :

```
root@apsit-HP-245-G4-Notebook-PC:~# nmap -O 192.168.200.238

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-15 18:01 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
 with --dns-servers
Nmap scan report for itserver (192.168.200.238)
Host is up (0.0021s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
13/tcp  open  daytime
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
443/tcp open  https
MAC Address: 00:15:17:7E:35:00 (Intel Corporate)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.00 seconds
root@apsit-HP-245-G4-Notebook-PC:~#
```

TCP XMAS Scan Output :

```
root@apsit-HP-245-G4-Notebook-PC:~# nmap -sX 127.0.0.1 -p  80,443

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-15 18:24 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
 with --dns-servers
Nmap scan report for localhost (127.0.0.1)
Host is up.
PORT    STATE         SERVICE
80/tcp  open|filtered http
443/tcp open|filtered https

Nmap done: 1 IP address (1 host up) scanned in 3.19 seconds
root@apsit-HP-245-G4-Notebook-PC:~#
```

Tcpdump capture to analyze working of XMAS Scan :

```
root@apsit-HP-245-G4-Notebook-PC:~# tcpdump  -v -n -e -i lo   port 80
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
18:03:19.883947 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 54: (tos 0x0, ttl 44, id 33883, offset 0,
 flags [none], proto TCP (6), length 40)
    127.0.0.1.49088 > 127.0.0.1.80: Flags [FPU], cksum 0xa3e2 (correct), seq 1913182141, win 1024, urg 0, length 0
18:03:20.884968 00:00:00:00:00:00 > 00:00:00:00:00:00, ethertype IPv4 (0x0800), length 54: (tos 0x0, ttl 59, id 22906, offset 0,
 flags [none], proto TCP (6), length 40)
    127.0.0.1.49089 > 127.0.0.1.80: Flags [FPU], cksum 0xa3e1 (correct), seq 1913247676, win 1024, urg 0, length 0
```

Nmap Output for ports behind firewall (Filtered Ports) :

```
root@apsit-HP-245-G4-Notebook-PC:~# nmap -sV 127.0.0.1 -p  80,443

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-15 18:11 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
 with --dns-servers
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:47127 > 127.0.0.1:80 S ttl=37 id=53917 iplen=44  seq=4203092245 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:47127 > 127.0.0.1:443 S ttl=46 id=23307 iplen=44  seq=4203092245 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:47128 > 127.0.0.1:443 S ttl=50 id=50256 iplen=44  seq=4203157780 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:47128 > 127.0.0.1:80 S ttl=43 id=49462 iplen=44  seq=4203157780 win=1024 <mss 1460>
Nmap scan report for localhost (127.0.0.1)
Host is up.
PORT    STATE    SERVICE VERSION
80/tcp  filtered http
443/tcp filtered https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.95 seconds
root@apsit-HP-245-G4-Notebook-PC:~#
```

Nmap Output for PING Scan :

```
root@apsit-HP-245-G4-Notebook-PC:~# nmap -sP 192.168.200.238

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-15 18:28 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
 with --dns-servers
Nmap scan report for itserver (192.168.200.238)
Host is up (0.0051s latency).
MAC Address: 00:15:17:7E:35:00 (Intel Corporate)
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
root@apsit-HP-245-G4-Notebook-PC:~#
```