

Name: Alok Bhawankar

Roll No: CSE-37

PRN: 1032170126

Lab Assignment 4

NMap

1) TCP SYN port scan

```
Command Prompt

Connection-specific DNS Suffix . : 
IPv6 Address. . . . . : 2409:4042:79c:21f3:e118:6705:f9d2:bfbe
Temporary IPv6 Address. . . . . : 2409:4042:79c:21f3:498d:af05:6059:799d
Link-local IPv6 Address . . . . . : fe80::e118:6705:f9d2:bfbe%18
IPv4 Address. . . . . : 192.168.43.61
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::f6f5:dbff:fe82:a39%18
                          192.168.43.162

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 

C:\Users\alokb>nmap 192.168.43.61 -sS
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-09 00:18 India Standard Time
Nmap scan report for 192.168.43.61
Host is up (0.0019s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
808/tcp   open  ccproxy-http
5357/tcp  open  wsddapi

Nmap done: 1 IP address (1 host up) scanned in 4.85 seconds
C:\Users\alokb>
```

2) UDP Port Scan

```
Command Prompt

139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
808/tcp   open  ccproxy-http
5357/tcp  open  wsddapi

Nmap done: 1 IP address (1 host up) scanned in 4.85 seconds

C:\Users\alokb>nmap 192.168.43.61 -sU
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-09 00:21 India Standard Time
Nmap scan report for 192.168.43.61
Host is up (0.00072s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
123/udp   open|filtered ntp
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
1900/udp  open|filtered upnp
3702/udp  open|filtered ws-discovery
4500/udp  open|filtered nat-t-ike
5050/udp  open|filtered mmcc
5353/udp  open|filtered zeroconf
5355/udp  open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 55.60 seconds

C:\Users\alokb>nmap 192.168.43.61 -A
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-09 00:23 India Standard Time
Nmap scan report for 192.168.43.61
Host is up (0.00044s latency).
Not shown: 995 closed ports
```

3) Remote OS Detection using TCP/IP stack fingerprint

```
Command Prompt
C:\Users\alokb>nmap 192.168.43.61 -O
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-09 00:24 India Standard Time
Nmap scan report for 192.168.43.61
Host is up (0.00050s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
808/tcp    open  ccproxy-http
5357/tcp   open  wsddapi
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=6/9%OT=135%CT=1%CU=35140%PV=Y%DS=0%DC=L%G=Y%TM=608FBCE
OS:6%P=i686-pc-windows-windows)SEQ(SP=102%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S
OS:%TS=U)OPS(O1=MFFD7NW8NNS%O2=MFFD7NW8NNS%O3=MFFD7NW8%O4=MFFD7NW8NNS%O5=MF
OS:FD7NW8NNS%O6=MFFD7NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF7
OS:0)ECN(R=Y%DF=Y%T=40%W=0%S=Z%A=0%RD=0%Q=)T1(R=Y%DF=Y%T=40%S=0%A=
OS:S+VF=AS%RD=0%Q=)T2(R=Y%DF=Y%T=40%W=0%S=Z%A=0%RD=0%Q=)T3(R=Y%DF=Y
OS:%T=40%W=0%S=Z%A=0%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=Z%A=0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%
OS:%S=A%A=0%F=R%O=0%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:%S=A%A=0%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%RD=0%Q=)U1
OS:(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=N%T=40%CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.98 seconds
```

4) Scan with default NSE scripts

```
Command Prompt

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.98 seconds

C:\Users\alokb>nmap 192.168.43.61 -sC
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-09 00:24 India Standard Time
Nmap scan report for 192.168.43.61
Host is up (0.0028s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
808/tcp    open  ccproxy-http
5357/tcp   open  wsddapi

Host script results:
|_clock-skew: -1s
|_smb2-security-mode:
|   2.02:
|_   Message signing enabled but not required
|_smb2-time:
|   date: 2021-06-08T18:54:47
|_   start_date: N/A

Nmap done: 1 IP address (1 host up) scanned in 16.93 seconds

C:\Users\alokb>
```

5) Service and Version Detection

