

# **PROOF OF CONCEPT**

By V.R.Devanand 181MC117

**Nmap:** Nmap or Network Mapper is a free and open source built-in tool in Kali Linux which allows us to map the users in our network and consists of various utilities such as host discovery, operating system detection, service detection etc..

**Nmap is a pre-installed tool in Kali Linux and thus doesn't require installation**

**To launch Nmap just type nmap in terminal**

**Major arguments/commands in Nmap:**

```
Applications ▾ Places ▾ Terminal ▾ Wed 1:30 PM
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~# nmap
Nmap 7.70 ( 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/PU[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 consecutively - 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)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
```

-p --> port

--top-ports -->scans for top ports

-iL --> read from txt file

-O --> os detection

-sV --> service detection

-sT --> send tcp packets

-sS --> send tcp SYN (half open scanning)

-sU --> send udp packets

--script --> use its scripting engine.

-A --> aggressive scan (os detection,version detection)

## Usage: nmap -arguments (victims' ip)

By this way Nmap is used as a Information gathering tool to find the

```
Applications ▾ Places ▾ Terminal ▾ Wed 1:33 PM
root@localhost: ~

File Edit View Search Terminal Help
OS: 5=7)SEQ(SP=FD%GCD=1%ISR=110%CI=I%II=I%TS=7)OPS(O1=M5B45T11NW8%02=M5B45T1
OS: 1NW8%03=M5B45T11NW8%04=M5B45T11NW8%05=M5B45T11NW8%06=M5B45T11)WIN(W1=FF
OS: FFW2=FFFFW3=FFFFW4=FFFFW5=FFFFW6=FFFF)ECN(R=Y%DF=N%T=40%W=FFFF%O=M
OS: B4NN5NW8%CC=Y%Q=)T1(R=Y%DF=N%T=40%W=0%AS=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4
OS: (R=Y%DF=Y%T=40%W=0%AS=A%Z=F=R%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=
OS: F%AR%Q=RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%Z=F=R%Q=)T7(R=Y%DF=Y%
OS: T=40%W=0%S=Z%A=S+F=AR%Q=RD=0%Q=)UI(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%R
OS: ID=G%RIPL=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

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 16.34 seconds
root@localhost:~# nmap -O -F 192.168.43.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-07 13:32 IST
Nmap scan report for 192.168.43.1
Host is up (0.0059s latency).
Not shown: 99 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 28:A6:0C:BC:6C:A3 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprints:
OS: 5CAN(V=7.70%E=4%Q=0/7%OT=53%CT=7%CU=34061%PV=Y%DS=1%DC=0%G=Y%M=20A60C%TM
OS: =5D4A85AF%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=107%TI=I%CI=I%II=I%
OS: TS=7)SEQ(SP=104%GCD=1%ISR=107%TI=I%CI=I%II=I%SS=0%TS=7)SEQ(SP=104%GCD=1%
OS: ISR=107%CI=I%II=I%TS=7)OPS(O1=M5B45T11NW8%02=M5B45T11NW8%03=M5B45T11NW8
OS: %04=M5B45T11NW8%05=M5B45T11NW8%06=M5B45T11)WIN(W1=FFFFW2=FFFFW3=FFFFW
OS: 4=FFFFW5=FFFFW6=FFFF)ECN(R=Y%DF=N%T=40%W=FFFF%O=M5B4NN5NW8%CC=Y%Q=)T1(
OS: R=Y%DF=N%T=40%W=0%AS=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%
OS: S=A%Z=F=R%Q=RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%Q=RD=0%Q=)T6(R
OS: =Y%DF=Y%T=40%W=0%S=A%Z=F=R%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=
OS: AR%Q=RD=0%Q=)UI(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPL=G%RUCK=G%
OS: RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

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 12.24 seconds
root@localhost:~# nmap help
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-07 13:33 IST
Failed to resolve "help".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.48 seconds
root@localhost:~# nmap -h
```

vulnerabilities in victims' machine to use the apt exploits.