INTERNSHIP ASSIGNMENT REPORT

Title: Network Scanning and Security Analysis Using Nmap

Student Details
Name: Bhuvan Kumar HM
Tools Used: Nmap, Wireshark
Operating System: Windows 11

1. Introduction
Network security is a critical aspect of cybersecurity. Identifying active devices and open ports helps in understanding potential risks. This assignment focuses on using Nmap to analyze a local network.

2. Objective
- Install and use Nmap
- Identify live hosts
- Detect open ports and services
- Analyze network traffic
- Identify security risks

3. Tools Used
Nmap – Network scanning
Wireshark – Packet analysis
Command Prompt – Execution

4. Network Information
Local IP Address: 172.17.0.1
Subnet Mask: 255.255.0.0
Network Range: 172.17.0.1/24

22/tcp → SSH (remote shell)

23/tcp → Telnet (insecure remote shell)

21/tcp → FTP (file transfer)

80/tcp → HTTP (web server)

443/tcp → HTTPS (secure web server)

3389/tcp → RDP (Windows Remote Desktop)

445/tcp → SMB (file sharing / Windows shares)

3306/tcp → MySQL database

5432/tcp → PostgreSQL database

5. Methodology:-
Installed Nmap from the official website and verified installation.
Used ipconfig to find the local network range.
Performed a TCP SYN scan using nmap -sS.
Recorded discovered hosts and open ports.

6. 10 Nmap Commands:-

1.Basic Ping Scan :- nmap -sn 81.161.178.68

Checks if a host is up without scanning ports.

2. Full Port Scan (1–65535) :-nmap -p- 81.161.178.68

Scans all 65,535 ports on the host.

3. Scan Specific Ports :-nmap -p 22,80,443 81.161.178.68

Scans only the selected ports.

4. Service & Version Detection:-nmap -sV 81.161.178.68

Shows software version running on each open port.

5. Aggressive Scan:-nmap -A 81.161.178.68

Performs OS detection, version detection, traceroute, script scanning.

6. Operating System Detection:-nmap -O 81.161.178.68

Identifies the OS (Windows/Linux) of the target.

7. Stealth SYN Scan (Default Scan):-nmap -sS 81.161.178.68

Fast and less detectable by firewalls.

8. Scan an Entire Network:-nmap   81.161.178.68

Scans all 256 devices in the subnet.

9. Vulnerability Scan (Using NSE Scripts) :-nmap --script=vuln 81.161.178.68

Runs vulnerability detection scripts.

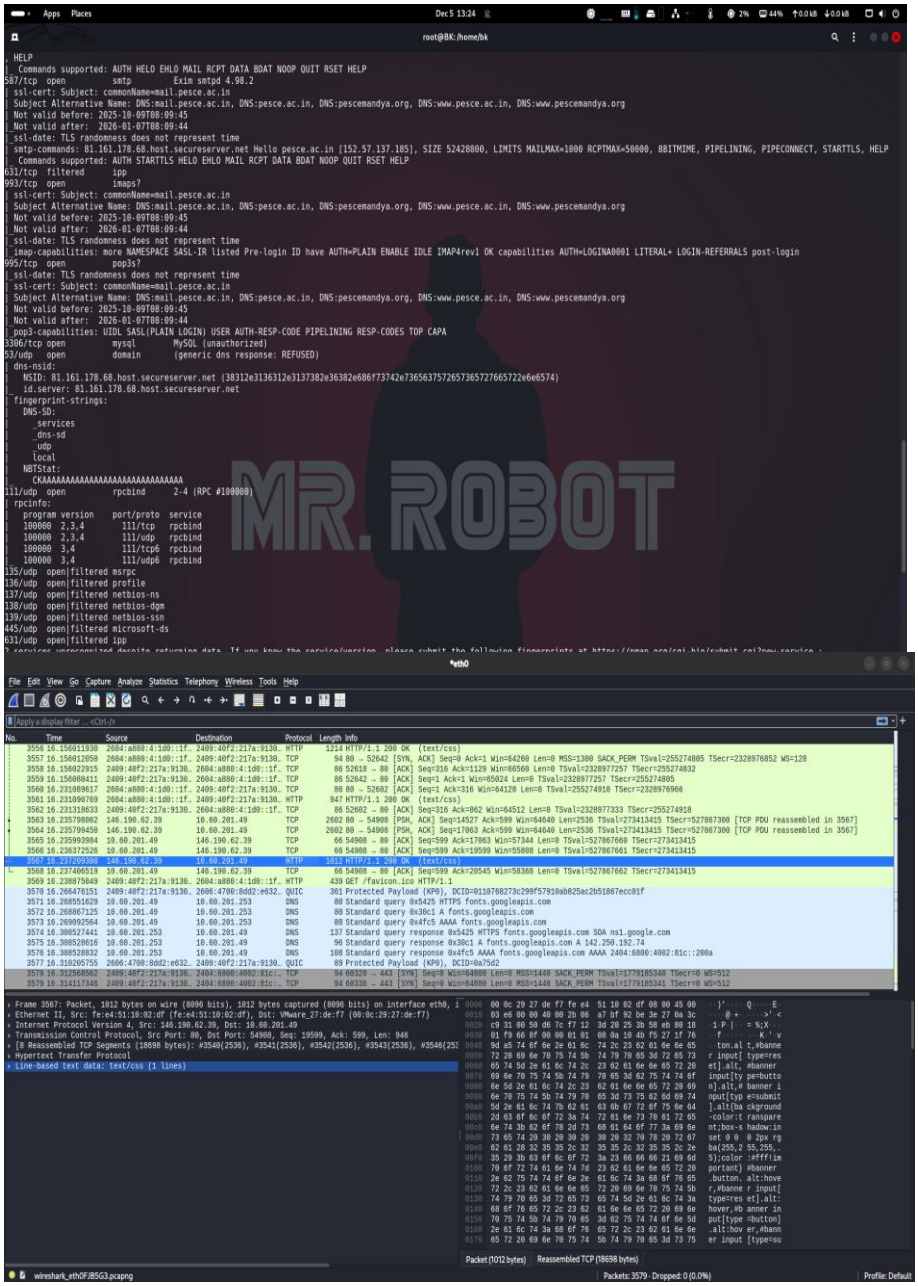
10. Output Scan Results to a File:-nmap -oN scan_result.txt 81.161.178.681

7. Results and Findings

Multiple hosts and services were discovered. Some open ports could pose security risks if not secured.

8. Conclusion

Nmap is an effective tool for understanding network exposure and improving security posture.


Apps Places
Dec 5 13:24
root@BK: /home/bk
| HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
587/tcp open smtp Exim smtpd 4.98.2
| ssl-cert: Subject: commonName=mail.pesce.ac.in
| Subject Alternative Name: DNS:mail.pesce.ac.in, DNS:pesce.ac.in, DNS:pescemandya.org, DNS:www.pesce.ac.in, DNS:www.pescemandya.org
| Not valid before: 2025-10-09T08:09:45
|_Not valid after: 2026-01-07T08:09:44
|_ssl-date: TLS randomness does not represent time
| smtp-commands: 81.161.178.68.host.secureserver.net Hello pesce.ac.in [152.57.137.185], SIZE 52428800, LIMITS MAILMAX=1000 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
631/tcp filtered ipp
993/tcp open imaps?
| ssl-cert: Subject: commonName=mail.pesce.ac.in
| Subject Alternative Name: DNS:mail.pesce.ac.in, DNS:pesce.ac.in, DNS:pescemandya.org, DNS:www.pesce.ac.in, DNS:www.pescemandya.org
| Not valid before: 2025-10-09T08:09:45
|_Not valid after: 2026-01-07T08:09:44
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: more NAMESPACE SASL-IR listed Pre-login ID have AUTH=PLAIN ENABLE IDLE IMAP4rev1 OK capabilities AUTH=LOGINA0001 LITERAL+ LOGIN-REFERRALS post-login
995/tcp open pop3s?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mail.pesce.ac.in
| Subject Alternative Name: DNS:mail.pesce.ac.in, DNS:pesce.ac.in, DNS:pescemandya.org, DNS:www.pesce.ac.in, DNS:www.pescemandya.org
| Not valid before: 2025-10-09T08:09:45
|_Not valid after: 2026-01-07T08:09:44
| pop3-capabilities: UIDL SASL(PLAIN LOGIN) USER AUTH-RESP-CODE PIPELINING RESP-CODES TOP CAPA
3306/tcp open mysql MySQL (unauthorized)
53/udp open domain (generic dns response: REFUSED)
| dns-nsid:
| NSID: 81.161.178.68.host.secureserver.net (38312e3136312e3137382e36382e686f73742e7365637572657365727665722e6e6574)
|_ id.server: 81.161.178.68.host.secureserver.net
| fingerprint-strings:
| DNS-SD:
| services
| _dns-sd
| _udp
| local
| NBTStat:
| CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
111/udp open rpcbind 2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind
|_ 100000 3,4 111/udp6 rpcbind
135/udp open|filtered msrpc
136/udp open|filtered profile
137/udp open|filtered netbios-ns
138/udp open|filtered netbios-dgm
139/udp open|filtered netbios-ssn
445/udp open|filtered microsoft-ds
631/udp open|filtered ipp
MR. ROBOT

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
3556 16.156011930 2604:a880:4:1d0::1f.. 2409:40f2:217a:9130.. HTTP 1214 HTTP/1.1 200 OK (text/css)
3557 16.156012850 2604:a880:4:1d0::1f.. 2409:40f2:217a:9130.. TCP 94 80 → 52642 [SYN, ACK] Seq=0 Ack=1 Win=64260 Len=0 MSS=1380 SACK_PERM TSval=255274805 TSecr=2328976852 WS=128
3558 16.156022915 2409:40f2:217a:9130.. 2604:a880:4:1d0::1f.. TCP 86 52618 → 80 [ACK] Seq=316 Ack=1129 Win=66560 Len=0 TSval=2328977257 TSecr=255274832
3559 16.156089411 2409:40f2:217a:9130.. 2604:a880:4:1d0::1f.. TCP 86 52642 → 80 [ACK] Seq=1 Ack=1 Win=65024 Len=0 TSval=2328977257 TSecr=255274805
3560 16.231089617 2604:a880:4:1d0::1f.. 2409:40f2:217a:9130.. TCP 86 80 → 52602 [ACK] Seq=1 Ack=316 Win=64128 Len=0 TSval=255274918 TSecr=2328976966
3561 16.231090769 2604:a880:4:1d0::1f.. 2409:40f2:217a:9130.. HTTP 947 HTTP/1.1 200 OK (text/css)
3562 16.231318633 2409:40f2:217a:9130.. 2604:a880:4:1d0::1f.. TCP 86 52602 → 80 [ACK] Seq=316 Ack=962 Win=64512 Len=0 TSval=2328977333 TSecr=255274918
3563 16.235790062 146.190.62.39 10.60.201.49 TCP 2602 80 → 54908 [PSH, ACK] Seq=14527 Ack=599 Win=64640 Len=2536 TSval=2734413415 TSecr=527867309 [TCP PDU reassembled in 3567]
3564 16.235799450 146.190.62.39 10.60.201.49 TCP 2602 80 → 54908 [PSH, ACK] Seq=17063 Ack=599 Win=64640 Len=2536 TSval=2734413415 TSecr=527867309 [TCP PDU reassembled in 3567]
3565 16.235993984 10.60.201.49 146.190.62.39 TCP 66 54908 → 80 [ACK] Seq=599 Ack=17063 Win=57344 Len=0 TSval=527867660 TSecr=273413415
3566 16.236372526 10.60.201.49 146.190.62.39 TCP 66 54908 → 80 [ACK] Seq=599 Ack=19599 Win=55808 Len=0 TSval=527867661 TSecr=273413415
3567 16.237209208 146.190.62.39 10.60.201.49 HTTP 1012 HTTP/1.1 200 OK (text/css)
3568 16.237406519 10.60.201.49 146.190.62.39 TCP 66 54908 → 80 [ACK] Seq=599 Ack=20545 Win=58368 Len=0 TSval=527867662 TSecr=273413415
3569 16.238075049 2409:40f2:217a:9130.. 2604:a880:4:1d0::1f.. HTTP 439 GET /favicon.ico HTTP/1.1
3570 16.266476151 2409:40f2:217a:9130.. 2606:4700:8dd2:e632.. QUIC 361 Protected Payload (KP0), DCID=011076827 3c299f57910ab825ac2b51867ecc01f
3571 16.268551629 10.60.201.49 10.60.201.253 DNS 80 Standard query 0x5425 HTTPS fonts.googleapis.com
3572 16.268867125 10.60.201.49 10.60.201.253 DNS 80 Standard query 0x30c1 A fonts.googleapis.com
3573 16.269092564 10.60.201.49 10.60.201.253 DNS 80 Standard query 0x4fc5 AAAA fonts.googleapis.com
3574 16.308527441 10.60.201.253 10.60.201.49 DNS 137 Standard query response 0x5425 HTTPS fonts.googleapis.com SOA ns1.google.com
3575 16.308528616 10.60.201.253 10.60.201.49 DNS 96 Standard query response 0x30c1 A fonts.googleapis.com A 142.250.192.74
3576 16.308528832 10.60.201.253 10.60.201.49 DNS 108 Standard query response 0x4fc5 AAAA fonts.googleapis.com AAAA 2404:6800:4002:81c::200a
3577 16.310265755 2606:4700:8dd2:e632.. 2409:40f2:217a:9130.. QUIC 89 Protected Payload (KP0), DCID=0a75d2
3578 16.312558562 2409:40f2:217a:9130.. 2404:6800:4002:81c::.. TCP 94 60328 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=1779185340 TSecr=0 WS=512
3579 16.314117346 2409:40f2:217a:9130.. 2404:6800:4002:81c::.. TCP 94 60336 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=1779185341 TSecr=0 WS=512
Frame 3567: Packet, 1012 bytes on wire (8096 bits), 1012 bytes captured (8096 bits) on interface eth0, i
Ethernet II, Src: fe:e4:51:10:02:df (fe:e4:51:10:02:df), Dst: VMware_27:de:f7 (00:0c:29:27:de:f7)
Internet Protocol Version 4, Src: 146.190.62.39, Dst: 10.60.201.49
Transmission Control Protocol, Src Port: 80, Dst Port: 54908, Seq: 19599, Ack: 599, Len: 946
[8 Reassembled TCP Segments (18698 bytes): #3540(2536), #3541(2536), #3542(2536), #3543(2536), #3546(25
Hypertext Transfer Protocol
Line-based text data: text/css (1 lines)
0000 00 0c 29 27 de f7 fe e4 51 10 02 df 08 00 45 00
0010 03 e6 00 00 40 00 2b 06 a7 bf 92 be 3e 27 0a 3c
0020 c9 31 00 50 d6 7c f7 12 3d 20 25 3b 58 eb 80 18
0030 01 f9 66 8f 00 00 01 01 08 0a 10 4b f5 27 1f 76
0040 9d a5 74 6f 6e 2e 61 6c 74 2c 23 62 61 6e 6e 65
0050 72 20 69 6e 70 75 74 5b 74 79 70 65 3d 72 65 73
0060 65 74 5d 2e 61 6c 74 2c 23 62 61 6e 6e 65 72 20
0070 69 6e 70 75 74 5b 74 79 70 65 3d 62 75 74 74 6f
0080 6e 5d 2e 61 6c 74 2c 23 62 61 6e 6e 65 72 20 69
0090 6e 70 75 74 5b 74 79 70 65 3d 73 75 62 6d 69 74
00a0 5d 2e 61 6c 74 7b 62 61 63 6b 67 72 6f 75 6e 64
00b0 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65
00c0 6e 74 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e
00d0 73 65 74 20 30 20 30 20 30 20 32 70 78 20 72 67
00e0 62 61 28 32 35 35 2c 32 35 35 2c 32 35 2c 2e
00f0 35 29 3b 63 6f 6c 6f 72 3a 23 66 66 66 21 69 6d
0100 70 6f 72 74 61 6e 74 7d 23 62 61 6e 6e 65 72 20
0110 2e 62 75 74 74 6f 6e 2e 61 6c 74 3a 68 6f 76 65
0120 72 2c 23 62 61 6e 6e 65 72 20 69 6e 70 75 74 5b
0130 74 79 70 65 3d 72 65 73 65 74 5d 2e 61 6c 74 3a
0140 68 6f 76 65 72 2c 23 62 61 6e 6e 65 72 20 69 6e
0150 70 75 74 5b 74 79 70 65 3d 62 75 74 74 6f 6e 5d
0160 2e 61 6c 74 3a 68 6f 76 65 72 2c 23 62 61 6e 6e
0170 65 72 20 69 6e 70 75 74 5b 74 79 70 65 3d 73 75
Packet (1012 bytes)
Reassembled TCP (18698 bytes)
wireshark_eth0FJBSG3.pcapng
Packets: 3579 · Dropped: 0 (0.0%)
Profile: Default