Task 9: Network Vulnerability Scanning – Short Report

Objective:

The objective of this task is to identify active hosts, open ports, running services, operating system details, and potential security risks in the local network using Nmap

Steps Performed :

1. Identified local network range using ipconfig.
2. Discovered active hosts using Nmap ping scan.
3. Performed port scanning on the selected host.
4. Detected running services and versions.
5. Attempted operating system detection.
6. Conducted vulnerability analysis using default Nmap scripts.
7. Saved complete scan results for reporting.

Findings :

- The target system (192.168.31.205) was active and reachable.
- Open ports detected include 80 (HTTP), 135 (MSRPC), 139 (NetBIOS), and 445 (SMB).
- Microsoft IIS 10.0 web server was running on port 80.
- The HTTP TRACE method was enabled, which is potentially risky.
- SMB message signing was enabled, indicating secure configuration.
- The operating system was identified as Microsoft Windows.

Conclusion :

The network vulnerability scan successfully identified active services and minor security risks in the system. No critical vulnerabilities were found. It is recommended to disable unnecessary services and risky HTTP methods, and to keep the system updated with the latest security patches.

Attachments:

```
Microsoft Windows [Version 10.0.26200.7623]
(c) Microsoft Corporation. All rights reserved.

C:\Users\gayat>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   IPv6 Address. . . . . . . . . . . : 2409:40f4:3088:6638:24df:aa6d:a45b:b7af
   Temporary IPv6 Address. . . . . . : 2409:40f4:3088:6638:842f:e378:6095:1648
   Link-local IPv6 Address . . . . . : fe80::d90e:305d:16f4:2318%4
   IPv4 Address. . . . . . . . . . . : 192.168.31.205
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::feb0:deff:fec2:2ca7%4
                                       192.168.31.1

Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter Ethernet:

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

C:\Users\gayat>nmap -sn 192.168.31.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2026-01-29 14:02 +0530
Stats: 0:00:15 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
Parallel DNS resolution of 255 hosts. Timing: About 0.78% done
Nmap scan report for jiofiber.local.html (192.168.31.1)
Host is up (0.0056s latency).
MAC Address: FC:B0:DE:C2:2C:A7 (Cloud Network Technology Singapore PTE.)
Nmap scan report for moto-g45-5G.lan (192.168.31.45)
Host is up (0.16s latency).
MAC Address: 56:E6:FC:82:71:01 (Unknown)
Nmap scan report for 192.168.31.161
Host is up (0.073s latency).
```

```
MAC Address: 84:C8:A0:04:05:58 (Hui Zhou Gaoshengda Technology)
Nmap scan report for GAYATHRI.lan (192.168.31.205)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 38.94 seconds

C:\Users\gayat>192.168.31.205 (GAYATHRI.lan)
'192.168.31.205' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\gayat>nmap 192.168.31.205
Starting Nmap 7.97 ( https://nmap.org ) at 2026-01-29 14:08 +0530
Nmap scan report for GAYATHRI.lan (192.168.31.205)
Host is up (0.00085s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds

C:\Users\gayat>nmap -sV 192.168.31.205
Starting Nmap 7.97 ( https://nmap.org ) at 2026-01-29 14:09 +0530
Nmap scan report for GAYATHRI.lan (192.168.31.205)
Host is up (0.00098s latency).
```

```
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
80/tcp  open  http          Microsoft IIS httpd 10.0
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.25 seconds

C:\Users\gayat>nmap -O 192.168.31.205
Starting Nmap 7.97 ( https://nmap.org ) at 2026-01-29 14:10 +0530
Nmap scan report for GAYATHRI.lan (192.168.31.205)
Host is up (0.00040s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
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=7.97%E=4%D=1/29%OT=80%CT=1%CU=35258%PV=Y%DS=0%DC=L%G=Y%TM=697
B1D0
OS:C%P=i686-pc-windows-windows)SEQ(SP=104%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S
OS:%TS=A)SEQ(SP=105%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=106%GCD=1
OS:%ISR=106%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=106%GCD=1%ISR=109%TI=I%CI=I%II=
OS:I%SS=S%TS=A)SEQ(SP=FC%GCD=1%ISR=10F%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MFFD
OS:7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8ST1
OS:1%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R
OS:=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W
OS:=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=
OS:O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80
OS:%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 10.56 seconds

C:\Users\gayat>nmap -sC 192.168.31.205
Starting Nmap 7.97 ( https://nmap.org ) at 2026-01-29 14:12 +0530
```

```
Nmap scan report for GAYATHRI.lan (192.168.31.205)
Host is up (0.000098s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
80/tcp  open  http
|_http-title: Site doesn't have a title.
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2026-01-29T08:42:57
|_  start_date: N/A
|_clock-skew: -1s

Nmap done: 1 IP address (1 host up) scanned in 19.45 seconds

C:\Users\gayat>nmap -sV -O -sC 192.168.31.205 -oN final_scan_report.txt
Starting Nmap 7.97 ( https://nmap.org ) at 2026-01-29 14:14 +0530
Nmap scan report for GAYATHRI.lan (192.168.31.205)
```

```
Host is up (0.00056s latency).

Not shown: 996 closed tcp ports (reset)

PORT    STATE SERVICE       VERSION

80/tcp  open  http          Microsoft IIS httpd 10.0

|_http-server-header: Microsoft-IIS/10.0

| http-methods:

|_  Potentially risky methods: TRACE

|_http-title: Site doesn't have a title.

135/tcp open  msrpc         Microsoft Windows RPC

139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn

445/tcp open  microsoft-ds?

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=7.97%E=4%D=1/29%OT=80%CT=1%CU=35298%PV=Y%DS=0%DC=L%G=Y%TM=697B1DF

OS:E%P=i686-pc-windows-windows)SEQ(SP=104%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S

OS:%TS=A)SEQ(SP=106%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=FD%GCD=1%

OS:ISR=103%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=FD%GCD=1%ISR=108%TI=I%CI=I%II=I%

OS:SS=S%TS=A)SEQ(SP=FF%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MFFD7N

OS:W8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8ST11%

OS:O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y

OS:%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%R

OS:D=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0
OS:%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
%Q=)T5(

OS:R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A
%A=O%

OS:F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y
%DF=N

OS:%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80
%C

OS:D=Z)


Network Distance: 0 hops

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows


Host script results:

| smb2-time:

|   date: 2026-01-29T08:44:37

|_  start_date: N/A

| smb2-security-mode:

|   3.1.1:

|_    Message signing enabled and required


OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 31.46 seconds
```