## **Practical 2**

Name: Saloni Vishwakarma

Wireless LAN adapter Wi-Fi:

**Roll no:**C1-13

Aim: Network Scanning and vulnerability assessment using NMAP PS C:\Users\acer> ipconfig WindowsIP Configuration Ethernet adapter Ethernet: Media State......Media disconnected Connection-specific DNS Suffix .: Wireless LAN adapter Local Area Connection\* 9: Media State..... Media disconnected Connection-specific DNS Suffix .: Wireless LAN adapter Local Area Connection\* 10: Media State..... Media disconnected Connection-specific DNS Suffix .: Ethernet adapter VMware Network Adapter VMnet1: Connection-specific DNS Suffix .: Link-local IPv6 Address .....: fe80::2673:c387:40ab:8403%11 IPv4 Address .....: 192.168.198.1 Subnet Mask.....: 255.255.255.0 Default Gateway . . . . . . . : Ethernet adapter VMware Network Adapter VMnet8: Connection-specific DNS Suffix .: Link-local IPv6 Address ..........: fe80::19e4:5967:44db:57d7%5 IPv4 Address .....: 192.168.246.1 Subnet Mask.....: 255.255.255.0 Default Gateway . . . . . . . :

Connection-specific DNS Suffix .: rknec.edu

Link-local IPv6 Address .....: fe80::6fec:f58:a45b:1205%18

IPv4 Address .....: 172.16.146.130 Subnet Mask ....: 255.255.254.0 Default Gateway ....: 172.16.146.1

## **Open Command Prompt or PowerShell or ZENMAP IDE**

## 1. Perform a Basic Ping Scan:

Starting Nmap 7.94 ( <code>https://nmap.org</code> ) at 2023-09-11 15:48 India Standard Time Nmap scan report for 192.168.198.1

Host is up.

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

#### 2. Perform a Full Port Scan:

PS C:\Users\acer> nmap -p- 192.168.198.1

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 15:48 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.000014s latency).

Not shown: 65518 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh
80/tcp open http
135/tcp open msrpc
137/tcp filtered netbios-ns
139/tcp open netbios-ssn
445/tcp open microsoft-ds
903/tcp open iss-console-r

903/tcp open iss-console-mgr 913/tcp open apex-edge 5040/tcp open unknown 7680/tcp open pando-pub 49664/tcp open unknown 49666/tcp open unknown

49667/tcp open unknown 49668/tcp open unknown 49670/tcp open unknown

49671/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 3.06 seconds

### 3. Specify Specific Ports:

PS C:\Users\acer> nmap -p 80,22 192.168.198.1

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 15:49 India Standard Time Nmap scan report for 192.168.198.1

Host is up (0.00s latency).

#### PORT STATE SERVICE

22/tcp open ssh 80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

## 4. Save Output to a File:

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 15:50 India Standard Time Nmap scan report for 192.168.198.1 Host is up (0.00011s latency). Not shown: 65518 closed tcp ports (reset) **PORT** STATE SERVICE 22/tcp open ssh 80/tcp open http 135/tcp open msrpc 137/tcp filtered netbios-ns 139/tcp open netbios-ssn 445/tcp open microsoft-ds iss-console-mgr 903/tcp open 913/tcp open apex-edge unknown 5040/tcp open

PS C:\Users\acer> nmap -p- 192.168.198.1 -oN scan results.txt

7680/tcp open pando-pub 49664/tcp open unknown 49665/tcp open unknown 49666/tcp open unknown 49667/tcp open unknown 49668/tcp open unknown 49670/tcp open unknown 49671/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 3.07 seconds

### 5. View Results:

```
# Nmap 7.94 scan initiated Mon Sep 11 15:50:03 2023 as: "C:\\Program Files (x86)\\Nmap\\nmap.exe" -p- -oN scan_results.txt 192.168.198.1
Nmap scan report for 192.168.198.1
Host is up (0.00011s latency).
Not shown: 65518 closed tcp ports (reset)
PORT
          STATE
                   SERVICE
22/tcp
          open
                    ssh
80/tcp
135/tcp open msrpc
137/tcp filtered netbios-ns
139/tcp
                   netbios-ssn
445/tcp
          open
                    microsoft-ds
903/tcp
                   iss-console-mgr
          open
913/tcp
                    apex-edge
5040/tcp open
                    unknown
7680/tcp open
                    pando-pub
49664/tcp open
                    unknown
49665/tcp open
                    unknown
49666/tcp open
                    unknown
49667/tcp open
                    unknown
49668/tcp open
                    unknown
49670/tcp open
                    unknown
49671/tcp open
# Nmap done at Mon Sep 11 15:50:06 2023 -- 1 IP address (1 host up) scanned in 3.07 seconds
```

### 6. Service Version Detection:

PS C:\Users\acer> nmap -sV 192.168.198.1

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 15:50 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.00065s latency).

Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH for\_Windows\_8.6 (protocol 2.0)

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?

903/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)

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 7.01 seconds

### 7. Operating System Detection:

PS C:\Users\acer> nmap -O 192.168.198.1

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 15:51 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.00062s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh 80/tcp open http 135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

903/tcp open iss-console-mgr

Device type: general purpose

Running: Microsoft Windows 10

OS CPE: cpe:/o:microsoft:windows\_10:1607 OS details: Microsoft Windows 10 1607

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 1.24 seconds

#### 8. Aggressive Scan:

PS C:\Users\acer> nmap -A 192.168.198.1

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 15:51 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.00075s latency).

Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH for Windows 8.6 (protocol 2.0)

ssh-hostkey:

3072 c5:60:50:9f:fd:16:04:99:d9:2c:19:c5:68:e4:2e:8f (RSA) 256 4c:64:69:28:55:dd:89:32:d0:be:51:d0:97:e5:77:d4 (ECDSA) \_ 256 ce:8b:83:e9:8a:7e:dd:00:aa:27:1d:e4:b4:b1:9a:9a (ED25519) 80/tcp open http Microsoft IIS httpd 10.0

| http-methods:

\_ Potentially risky methods: TRACE |\_http-title: Site doesn't have a title. \_http-server-header: Microsoft-IIS/10.0

135/tcp open msrpc Microsoft Windows RPC

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

445/tcp open microsoft-ds?

903/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)

Device type: general purpose Running: Microsoft Windows 10

OS CPE: cpe:/o:microsoft:windows\_10:1607 OS details: Microsoft Windows 10 1607

Network Distance: 0 hops

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

Host script results:

| smb2-time:

| date: 2023-09-11T10:22:09

\_ start\_date: N/A | smb2-security-mode:

| 3:1:1:

Message signing enabled but not 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 22.36 seconds

### 9.Scan Multiple Targets:

PS C:\Users\acer> nmap 192.168.198.1 192.168.210.1

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 15:55 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.000031s latency).

Not shown: 994 closed top ports (reset)

PORT STATE SERVICE

22/tcp open ssh 80/tcp open http 135/tcp open msrpc 139/tcp open netbios-ssn

445/tcp open microsoft-ds

903/tcp open iss-console-mgr

# 10. You can also scan a range of IP addresses:

PS C:\Users\acer> nmap 192.168.198.1-50

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 16:39 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.00098s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh 80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

903/tcp open iss-console-mgr

Nmap done: 50 IP addresses (1 host up) scanned in 2.45 seconds

# 11. Exclude Hosts from Scanning:

PS C:\Users\acer> nmap 192.168.198.1-50 --exclude 192.168.198.10

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 16:39 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.000014s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh 80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

903/tcp open iss-console-mgr

Nmap done: 49 IP addresses (1 host up) scanned in 2.46 seconds

### 12. UDP Port Scan:

PS C:\Users\acer> nmap -sU 192.168.198.1

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 16:10 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.00032s latency).

Not shown: 992 closed udp ports (port-unreach)

PORT STATE SERVICE

137/udp open|filtered netbios-ns

138/udp open|filtered netbios-dgm

500/udp open|filtered isakmp

1900/udp open|filtered upnp

4500/udp open|filtered nat-t-ike

5050/udp open|filtered mmcc

5353/udp open|filtered zeroconf

5355/udp open|filtered llmnr

## 13. Timing and Performance Options:

PS C:\Users\acer> nmap -T4 --max-rtt-timeout 500ms 192.168.198.1

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 16:12 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.00038s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh 80/tcp open http 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 903/tcp open iss-console-mgr

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds

# 14. Output to XML or Other Formats:

PS C:\Users\acer> nmap -oX scan\_results.xml 192.168.198.1

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 16:12 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.00018s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh 80/tcp open http 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds

903/tcp open iss-console-mgr

### 15. Scan a Network Range:

PS C:\Users\acer> nmap 192.168.198.0/24

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 16:21 India Standard Time

Nmap scan report for 192.168.198.254

Host is up (0.00067s latency).

All 1000 scanned ports on 192.168.198.254 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response) MAC Address: 00:50:56:E4:D5:4F (VMware)

Nmap scan report for 192.168.198.1

Host is up (0.000025s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh 80/tcp open http 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 903/tcp open iss-console-mgr

Nmap done: 256 IP addresses (2 hosts up) scanned in 31.50 seconds

## 16. Scan for Specific Protocols:

PS C:\Users\acer> nmap -sU 192.168.198.1 # UDP scan

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 16:22 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.00046s latency).

Not shown: 992 closed udp ports (port-unreach)

PORT STATE SERVICE 137/udp open|filtered netbios-ns

138/udp open|filtered netbios-dgm

500/udp open|filtered isakmp

1900/udp open|filtered upnp

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 50.12 seconds

PS C:\Users\acer> nmap -sT 192.168.198.1 # TCP scan

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 16:24 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.0014s latency).

Not shown: 994 filtered tcp ports (no-response)

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

903/tcp open iss-console-mgr

Nmap done: 1 IP address (1 host up) scanned in 5.79 seconds

## 17. Scripting Engine (NSE) Categories:

PS C:\Users\acer> nmap --script vuln 192.168.198.1 Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-11 16:25 India Standard Time Nmap scan report for 192.168.198.1 Host is up (0.000019s latency). Not shown: 994 closed tcp ports (reset) PORT STATE SERVICE 22/tcp open ssh 80/tcp open http \_http-dombased-xss: Couldn't find any DOM based XSS. \_http-csrf: Couldn't find any CSRF vulnerabilities. \_http-stored-xss: Couldn't find any stored XSS vulnerabilities. 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 903/tcp open iss-console-mgr Host script results: \_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR |\_smb-vuln-ms10-054: false Nmap done: 1 IP address (1 host up) scanned in 137.31 seconds nmap --script discovery <target> Group: 224.0.0.252 PS C:\Users\acer> nmap --script discovery 192.168.198.1 Description: Link-local Multicast Name Starting Nmap 7.94 (https://nmap.org) at Resolution (rfc4795) 2023-09-11 16:40 India Standard Time | 172.16.146.81 Pre-scan script results: Interface: eth5 | broadcast-igmp-discovery: Version: 2 | 172.16.146.27 Group: 224.0.0.252 Interface: eth5 Description: Link-local Multicast Name Version: 2 Resolution (rfc4795) Group: 224.0.0.252 | 172.16.146.94 Description: Link-local Multicast Name Interface: eth5 Resolution (rfc4795) Version: 2 | 172.16.146.33 Group: 224.0.0.252 Interface: eth5 Description: Link-local Multicast Name Version: 2 Resolution (rfc4795) | 172.16.146.111 Group: 224.0.0.252 Description: Link-local Multicast Name Interface: eth5 Resolution (rfc4795) Version: 2 | 172.16.146.41 Group: 224.0.0.252 Interface: eth5 Description: Link-local Multicast Name Version: 2 Resolution (rfc4795) Group: 224.0.0.252 | 172.16.146.119 Description: Link-local Multicast Name Interface: eth5 Resolution (rfc4795) Version: 2 | 172.16.146.58 Group: 224.0.0.252 Interface: eth5 Description: Link-local Multicast Name

Resolution (rfc4795)

Version: 2

172.16.146.121	Interface: eth5
Interface: eth5	Version: 2
Version: 2	Group: 224.0.0.252
Group: 224.0.0.252	Description: Link-local Multicast Name
Description: Link-local Multicast Name	Resolution (rfc4795)
Resolution (rfc4795)	172.16.146.193
172.16.146.134	Interface: eth5
Interface: eth5	Version: 2
Version: 2	Group: 224.0.0.252
Group: 224.0.0.252	Description: Link-local Multicast Name
Description: Link-local Multicast Name	Resolution (rfc4795)
Resolution (rfc4795)	172.16.146.197
172.16.146.146	Interface: eth5
Interface: eth5	Version: 2
Version: 2	Group: 224.0.0.251
Group: 224.0.0.252	Description: mDNS (rfc6762)
Description: Link-local Multicast Name	172.16.146.197
Resolution (rfc4795)	Interface: eth5
172.16.146.156	Version: 2
Interface: eth5	Group: 224.0.0.252
Version: 2	Description: Link-local Multicast Name
Group: 224.0.0.252	Resolution (rfc4795)
Description: Link-local Multicast Name	172.16.146.206
Resolution (rfc4795)	Interface: eth5
172.16.146.157	Version: 2
Interface: eth5	Group: 224.0.0.252
Version: 2	Description: Link-local Multicast Name
Group: 224.0.0.252	Resolution (rfc4795)
Description: Link-local Multicast Name	172.16.146.210
Resolution (rfc4795)	Interface: eth5
172.16.146.169	Version: 2
Interface: eth5	Group: 224.0.0.252
Version: 2	Description: Link-local Multicast Name
Group: 224.0.0.252	Resolution (rfc4795)
Description: Link-local Multicast Name	172.16.146.211
Resolution (rfc4795)	Interface: eth5
172.16.146.179	Version: 2
Interface: eth5	Group: 224.0.0.252
Version: 2	Description: Link-local Multicast Name
Group: 224.0.0.252	Resolution (rfc4795)
Description: Link-local Multicast Name	172.16.146.245
Resolution (rfc4795)	Interface: eth5
172.16.146.182	Version: 2
Interface: eth5	Group: 224.0.0.252
Version: 2	Description: Link-local Multicast Name
Group: 224.0.0.252	Resolution (rfc4795)
Description: Link-local Multicast Name	172.16.146.251
Resolution (rfc4795)	Interface: eth5
172.16.146.186	Version: 2

Group: 224.0.0.252	172.16.146.58	
Description: Link-local Multicast Name	Interface: eth5	
Resolution (rfc4795)	Version: 2	
172.16.147.10	Group: 239.255.255.250	
Interface: eth5		nization-Local Scope
Version: 2	(rfc2365)	•
Group: 224.0.0.251	'	s script-arg to add the
Description: mDNS (rfc6762)	results as targets	5 compress 9 co asses and
172.16.147.10	ipv6-multicast-mld-lis	st:
Interface: eth5	fe80::9c7b:f2b6:595	
Version: 2	device: eth5	
Group: 224.0.0.252	mac: 18:cc:18:cd:	80:39
Description: Link-local Multicast Name	multicast_ips:	30.00
Resolution (rfc4795)	ff02::1:3	(Link-local Multicast
172.16.147.19	Name Resolution)	(Ziiiit ioodi mailiodot
Interface: eth5	ff02::fb	(mDNSv6)
Version: 2	ff02::c	(SSDP)
Group: 224.0.0.252	fe80::3db1:ec11:fd4	` '
Description: Link-local Multicast Name	device: eth5	a.700.
Resolution (rfc4795)	mac: 2c:33:58:20:	f5·h7
172.16.147.21	multicast_ips:	13.07
Interface: eth5	ff02::fb	(mDNSv6)
Version: 2	ff02::1:3	` '
•	•	(Link-local Multicast
Group: 224.0.0.252	Name Resolution)	(CCDD)
Description: Link-local Multicast Name	ff02::c	(SSDP)
Resolution (rfc4795)	fe80::5c7a:257c:ff37:8747:	
172.16.147.33	device: eth5	
Interface: eth5	mac: 58:ce:2a:64:3e:17	
Version: 2	multicast_ips:	/1.2 - 1. 1 1. N.A 1/2 4
Group: 224.0.0.251	ff02::1:3	(Link-local Multicast
Description: mDNS (rfc6762)	Name Resolution)	(~ DNO 0)
172.16.147.33	ff02::fb	(mDNSv6)
Interface: eth5	ff02::c (SSDP)	
Version: 2	fe80::e9d9:e014:eee3:d0c8:	
Group: 224.0.0.252	device: eth5	
Description: Link-local Multicast Name	mac: 18:cc:18:ce:79:7b	
Resolution (rfc4795)	multicast_ips:	
172.16.147.40	ff02::fb	(mDNSv6)
Interface: eth5	ff02::1:3	(Link-local Multicast
Version: 2	Name Resolution)	
Group: 224.0.0.252	ff02::c	(SSDP)
Description: Link-local Multicast Name	fe80::567e:c82a:77:918b:	
Resolution (rfc4795)	device: eth5	
172.16.147.69	mac: 58:ce:2a:64:24:1d	
Interface: eth5	multicast_ips:	
Version: 2	ff02::1:3	(Link-local Multicast
Group: 224.0.0.252	Name Resolution)	
Description: Link-local Multicast Name	ff02::fb	(mDNSv6)
Resolution (rfc4795)	ff02::c	(SSDP)

fe80::76dd:a644:e79e	·he3e·	multicast_ips:		
device: eth5		ff02::fb (mDNSv6)		
mac: 2c:33:58:20:ff:a8		fe80::f205:8925:cbeb:aeec:		
multicast_ips:		device: eth5	b.acc.	
· -·	(Link-local Multicast	mac: 58:ce:2a:63:	7c:ca	
Name Resolution)	(Link local Mattodot	multicast_ips:	7 0.00	
•	(mDNSv6)	ff02::1:3	(Link-local Multicast	
	SSDP)	Name Resolution)	(Elitik loodi Walloast	
fe80::f758:6ef9:20fe:c	•	ff02::fb	(mDNSv6)	
device: eth5	001.	ff02::c (SSDP)		
mac: a4:6b:b6:c8:38	8·∩9	fe80::9356:5e97:1dd6:6d8a:		
multicast_ips:		device: eth5		
•	mDNSv6)	mac: 2c:33:58:21:	00:8e	
	(Link-local Multicast	multicast_ips:		
Name Resolution)	(	ff02::fb	(mDNSv6)	
,	SSDP)	ff02::1:3	(Link-local Multicast	
fe80::bc31:cf79:1f86:e	•	Name Resolution)	(=	
device: eth5		ff02::c	(SSDP)	
mac: 58:ce:2a:64:50	0:05	fe80::b7cd:e517:b9	` '	
multicast_ips:		device: eth5		
· ·	(Link-local Multicast	mac: c0:3c:59:77:	a7:d6	
Name Resolution)	(	multicast_ips:		
•	mDNSv6)	ff02::c	(SSDP)	
•	SSDP)	ff02::fb	(mDNSv6)	
fe80::d911:38a5:d378	•	ff02::1:3	(Link-local Multicast	
device: eth5		Name Resolution)		
mac: 50:c2:e8:c2:8d	l:bd	fe80::3587:6106:687:3d72:		
multicast_ips:		device: eth5		
· ·	(Link-local Multicast	mac: 2c:33:58:20:fe:09		
Name Resolution)		multicast_ips:		
•	mDNSv6)		(mDNSv6)	
•	SSDP)	ff02::1:3	(Link-local Multicast	
fe80::f595:fa31:7599:2	·	Name Resolution)		
device: eth5		fe80::d0e0:14df:dbc6:b0b1:		
mac: 30:d1:6b:fa:0e:cd		device: eth5		
multicast_ips:		mac: 00:e0:2d:93:19:e4		
· ·	(Link-local Multicast	multicast_ips:		
Name Resolution)		ff02::fb	(mDNSv6)	
	mDNSv6)	ff02::1:3	(Link-local Multicast	
•	SSDP)	Name Resolution)	•	
fe80::aaf9:fa3e:31be:7	7f6b:	ff02::c	(SSDP)	
device: eth5		fe80::1626:3b35:601e:c2cc:		
mac: 58:ce:2a:63:37:92		device: eth5		
multicast_ips:		mac: 18:cc:18:2d:d8:e5		
ff02::1:3 (Link-local Multicast		multicast_ips:		
Name Resolution)	•	ff02::c	(SSDP)	
fe80::7b20:2592:c1d7	:a1e6:	ff02::fb	(mDNSv6)	
device: eth5		ff02::1:3	(Link-local Multicast	
mac: 2c:33:58:20:f9:31		Name Resolution)		

fe80::3ceb:4d2:97	07:e2b7:	device: eth5	
device: eth5		mac: 2c:33:58:20	):ff:49
mac: 30:03:c8:8	3:a3:4d	<pre>  multicast_ips:</pre>	
multicast_ips:		ff02::c	(SSDP)
ff02::fb	(mDNSv6)	fe80::8e75:9050:7	6a6:ad42:
ff02::1:3	(Link-local Multicast	device: eth5	
Name Resolution)		mac: 14:18:c3:05	5:9f:dd
ff02::c	(SSDP)	multicast_ips:	
fe80::c274:adff:fed	2:415:	ff02::fb	(mDNSv6)
device: eth5		ff02::1:3	(Link-local Mu
mac: c0:74:ad:c	2:04:15	Name Resolution)	
multicast_ips:		ff02::c	(SSDP)
ff02::fb	(mDNSv6)	fe80::966e:2702:1	27b:c3d7:
fe80::6482:5c63:9	eb2:a331:	device: eth5	
device: eth5		mac: 14:18:c3:02	2:97:b1
mac: 2c:33:58:2	1:00:07	multicast_ips:	
multicast_ips:	· -	ff02::1:3	(Link-local Mu
ff02::fb	(mDNSv6)	Name Resolution)	\
ff02::1:3	(Link-local Multicast	ff02::fb	(mDNSv6)
Name Resolution)	(Ziiiit 1884) Mailieast	ff02::c	(SSDP)
ff02::c	(SSDP)	fe80::703e:e4cc:9	,
fe80::decd:2fff:fe01:dc9c:		device: eth5	
device: eth5	1.4000.	mac: f4:b5:20:47:25:b7	
mac: dc:cd:2f:01	·dc·9c	multicast_ips:	.20.07
multicast_ips:	.46.36	ff02::1:3	(Link-local Mu
ff02::c	(SSDP)	Name Resolution)	(LITIK-IOCAL IVIU
fe80::1a08:bab:27	` '	ff02::fb	(mDNSv6)
device: eth5	6a.310d.	ff02::i0	(SSDP)
mac: 2c:33:58:2	Orforo?	fe80::f38a:2592:5e	` '
	0.16.62	device: eth5	5.105e.
multicast_ips:	(mDNIC) (C)		0.75.50
ff02::fb	(mDNSv6)	mac: 3c:91:80:93	3.75.59
ff02::1:3	(Link-local Multicast	multicast_ips:	( DNO - 0)
Name Resolution)	<b>1011</b>	ff02::fb	(mDNSv6)
fe80::8062:168:7fb	D:T3TT:	ff02::1:3	(Link-local Mu
device: eth5		Name Resolution)	(2255)
mac: 50:5a:65:fa	a:fa:64	ff02::c	(SSDP)
multicast_ips:		fe80::d8fd:cf0e:369	91:86c0:
ff02::1:3	(Link-local Multicast	device: eth5	
Name Resolution)		mac: 2c:33:58:20	):f5:a8
ff02::c	(SSDP)	multicast_ips:	
fe80::2cf3:5dae:5e	efc:e2c3:	ff02::1:3	(Link-local Mu
device: eth5		Name Resolution)	
mac: 2c:33:58:20:fd:0f		ff02::c	(SSDP)
multicast_ips:		fe80::68b8:cd7b:35	572:220f:
ff02::fb	(mDNSv6)	device: eth5	
ff02::1:3	(Link-local Multicast	mac: 2c:33:58:20	):ff:4e
Name Resolution)		multicast_ips:	
ff02::c	(SSDP)	ff02::fb	(mDNSv6)
	73b:3a35:		•

		1.5 ( 00 (000 0) 07 00 ( 0 0 0)
ff02::1:3	(Link-local Multicast	IP: fe80::1626:3b35:601e:c2cc MAC:
Name Resolution)	(0055)	18:cc:18:2d:d8:e5
•	(SSDP)	IP: fe80::1a08:bab:278a:3f0d MAC:
fe80::cbe4:d8be:4286	e:9fde:	2c:33:58:20:fc:e2 IFACE: eth5
device: eth5		IP: fe80::2cf3:5dae:5efc:e2c3 MAC:
mac: 10:a5:1d:f9:0d	d:e4	2c:33:58:20:fd:0f IFACE: eth5
multicast_ips:		IP: fe80::3587:6106:687:3d72 MAC:
ff02::fb	(mDNSv6)	2c:33:58:20:fe:09 IFACE: eth5
ff02::1:3	(Link-local Multicast	IP: fe80::3ceb:4d2:9707:e2b7 MAC:
Name Resolution)		30:03:c8:83:a3:4d IFACE: eth5
ff02::c	(SSDP)	IP: fe80::3db1:ec11:fd4a:76c MAC:
fe80::ecd0:5823:967	a:4361:	2c:33:58:20:f5:b7 IFACE: eth5
device: eth5		IP: fe80::4a70:ea17:f73b:3a35 MAC:
mac: f4:b5:20:48:91	1:02	2c:33:58:20:ff:49 IFACE: eth5
multicast_ips:		IP: fe80::567e:c82a:77:918b MAC:
ff02::1:3	(Link-local Multicast	58:ce:2a:64:24:1d IFACE: eth5
Name Resolution)	•	IP: fe80::59b:5208:5e6f:753e MAC:
,	(mDNSv6)	2c:33:58:20:f5:ad IFACE: eth5
•	(SSDP)	IP: fe80::5c7a:257c:ff37:8747 MAC:
fe80::c0e9:a889:156	'	58:ce:2a:64:3e:17 IFACE: eth5
device: eth5		IP: fe80::6482:5c63:9eb2:a331 MAC:
mac: 2c:33:58:20:fb	o:11	2c:33:58:21:00:07 IFACE: eth5
multicast_ips:		IP: fe80::68b8:cd7b:3572:220f MAC:
	(mDNSv6)	2c:33:58:20:ff:4e IFACE: eth5
ff02::1:3	(Link-local Multicast	IP: fe80::703e:e4cc:99e1:d20e MAC:
Name Resolution)	(Ellin local Manicact	f4:b5:20:47:25:b7 IFACE: eth5
,	(SSDP)	IP: fe80::76dd:a644:e79e:be3e MAC:
fe80::c274:adff:fec2:4	` '	2c:33:58:20:ff:a8 IFACE: eth5
device: eth5	FIO.	IP: fe80::7b20:2592:c1d7:a1e6 MAC:
mac: c0:74:ad:c2:0	<b>√.16</b>	2c:33:58:20:f9:31 IFACE: eth5
multicast_ips:	4.10	IP: fe80::8062:168:7fb:f3ff   MAC:
•	(mDNSv6)	50:5a:65:fa:fa:64 IFACE: eth5
'	(mDNSv6)	
fe80::f32e:b9e0:3ec2	.a.	IP: fe80::8e75:9050:76a6:ad42 MAC:
device: eth5	0.01-	14:18:c3:05:9f:dd IFACE: eth5
mac: 18:cc:18:2d:da	8:30	IP: fe80::9356:5e97:1dd6:6d8a MAC:
multicast_ips:	71 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	2c:33:58:21:00:8e IFACE: eth5
ff02::1:3	(Link-local Multicast	IP: fe80::966e:2702:127b:c3d7 MAC:
Name Resolution)	( 50.5 5)	14:18:c3:02:97:b1 IFACE: eth5
·	(mDNSv6)	IP: fe80::9c7b:f2b6:595c:6605 MAC:
•	(SSDP)	18:cc:18:cd:80:39 IFACE: eth5
fe80::59b:5208:5e6f:7	753e:	IP: fe80::aaf9:fa3e:31be:7f6b MAC:
device: eth5		58:ce:2a:63:37:92 IFACE: eth5
mac: 2c:33:58:20:f5	5:ad	IP: fe80::b7cd:e517:b9ad:c83b MAC:
multicast_ips:		c0:3c:59:77:a7:d6 IFACE: eth5
ff02::fb	(mDNSv6)	IP: fe80::bc31:cf79:1f86:e44a MAC:
_ ff02::1:3	(Link-local Multicast	58:ce:2a:64:50:05 IFACE: eth5
Name Resolution)		IP: fe80::c0e9:a889:1565:3e0d MAC:
targets-ipv6-multicast-	-mld:	2c:33:58:20:fb:11 IFACE: eth5

```
| IP: fe80::c274:adff:fec2:415 MAC:
                                                      | encryption_algorithms: (6)
c0:74:ad:c2:04:15 IFACE: eth5
                                                      | mac_algorithms: (10)
| IP: fe80::c274:adff:fec2:416 MAC:
                                                      |_ compression_algorithms: (2)
c0:74:ad:c2:04:16 IFACE: eth5
                                                      ssh-hostkey:
| IP: fe80::cbe4:d8be:428e:9fde MAC:
                                                      | 3072
10:a5:1d:f9:0d:e4 IFACE: eth5
                                                      c5:60:50:9f:fd:16:04:99:d9:2c:19:c5:68:e4:2e:8f
| IP: fe80::d0e0:14df:dbc6:b0b1 MAC:
                                                      (RSA)
00:e0:2d:93:19:e4 IFACE: eth5
                                                      | 256
IP: fe80::d8fd:cf0e:3691:86c0 MAC:
                                                      4c:64:69:28:55:dd:89:32:d0:be:51:d0:97:e5:77:d
2c:33:58:20:f5:a8 IFACE: eth5
                                                      4 (ECDSA)
| IP: fe80::d911:38a5:d378:29e8 MAC:
                                                      |_ 256
50:c2:e8:c2:8d:bd IFACE: eth5
                                                      ce:8b:83:e9:8a:7e:dd:00:aa:27:1d:e4:b4:b1:9a:9
| IP: fe80::decd:2fff:fe01:dc9c MAC:
                                                      a (ED25519)
                                                      80/tcp open http
dc:cd:2f:01:dc:9c IFACE: eth5
| IP: fe80::e9d9:e014:eee3:d0c8 MAC:
                                                      | http-useragent-tester:
                                                      | Status for browser useragent: 404
18:cc:18:ce:79:7b IFACE: eth5
| IP: fe80::ecd0:5823:967a:4361 MAC:
                                                      | Allowed User Agents:
f4:b5:20:48:91:02 IFACE: eth5
                                                          Mozilla/5.0 (compatible; Nmap Scripting
                                                      Engine; https://nmap.org/book/nse.html)
| IP: fe80::f205:8925:cbeb:aeec MAC:
                                                          libwww
58:ce:2a:63:7c:ca IFACE: eth5
| IP: fe80::f32e:b9e0:3ec2:a MAC:
                                                          lwp-trivial
18:cc:18:2d:d8:3b IFACE: eth5
                                                          libcurl-agent/1.0
| IP: fe80::f38a:2592:5e3:1c5e MAC:
                                                          PHP/
3c:91:80:93:75:59 IFACE: eth5
                                                          Python-urllib/2.5
                                                          GT::WWW
| IP: fe80::f595:fa31:7599:291d MAC:
30:d1:6b:fa:0e:cd IFACE: eth5
                                                          Snoopy
                                                          MFC_Tear_Sample
| IP: fe80::f758:6ef9:20fe:c691 MAC:
a4:6b:b6:c8:38:09 IFACE: eth5
                                                          HTTP::Lite
                                                          PHPCrawl
                                                          URI::Fetch
_ Use --script-args=newtargets to add the
                                                          Zend Http Client
results as targets
| hostmap-robtex: *TEMPORARILY DISABLED*
                                                          http client
due to changes in Robtex's API. See
                                                          PECL::HTTP
                                                          Wget/1.13.4 (linux-gnu)
https://www.robtex.com/api/
| http-robtex-shared-ns: *TEMPORARILY
                                                          WWW-Mechanize/1.34
DISABLED* due to changes in Robtex's API.
                                                      http-xssed: No previously reported XSS vuln.
See https://www.robtex.com/api/
                                                      _http-title: Site doesn't have a title.
| targets-asn:
                                                      | http-errors:
_ targets-asn.asn is a mandatory parameter
                                                      | Spidering limited to: maxpagecount=40;
Nmap scan report for 192.168.198.1
                                                      withinhost=192.168.198.1
Host is up (0.000069s latency).
                                                      | Found the following error pages:
Not shown: 994 closed tcp ports (reset)
Bug in http-security-headers: no string output.
                                                      | Error Code: 404
PORT STATE SERVICE
                                                            http://192.168.198.1:80/
22/tcp open ssh
                                                      |_http-chrono: Request times for /; avg:
| banner: SSH-2.0-OpenSSH for Windows 8.6
                                                      122.20ms; min: 46.00ms; max: 164.00ms
| ssh2-enum-algos:
                                                      _http-mobileversion-checker: No mobile version
                                                      detected.
| kex algorithms: (9)
server_host_key_algorithms: (5)
```

_http-devframework: Couldn't determine the	2:1:0
underlying framework or CMS. Try increasing	3:0:0
'httpspider.maxpagecount' value to spider more	3:0:2
pages.	3:1:1
http-sitemap-generator:	
Directory structure:	to debug)
Longest directory structure:	smb2-capabilities:
Depth: 0	2:0:2:
Dir: /	Distributed File System
Total files found (by extension):	2:1:0:
	Distributed File System
  _http-referer-checker: Couldn't find any	Leasing
cross-domain scripts.	Multi-credit operations
_http-date: Mon, 11 Sep 2023 11:11:30 GMT;	3:0:0:
-1s from local time.	Distributed File System
_http-comments-displayer: Couldn't find any	Leasing
comments.	Multi-credit operations
_http-feed: Couldn't find any feeds.	3:0:2:
http-vhosts:	Distributed File System
_128 names had status 404	Leasing
http-headers:	Multi-credit operations
Server: Microsoft-IIS/10.0	3:1:1:
Date: Mon, 11 Sep 2023 11:11:30 GMT	Distributed File System
Connection: close	Leasing
Content-Length: 0	Leasing  _ Multi-credit operations
Content-Length. 0	inditi-credit operations  _fcrdns: FAIL (No PTR record)
  _ (Request type: GET)	path-mtu: ERROR: Script execution failed (use
, , , , , , , , , , , , , , , , , , , ,	-d to debug)
135/tcp open msrpc	<u>.</u> ,
139/tcp open netbios-ssn	smb2-security-mode:
_smb-enum-services: ERROR: Script execution failed (use -d to debug)	•
`	<pre> _ Message signing enabled but not required   smb-mbenum:</pre>
445/tcp open microsoft-ds	·
_smb-enum-services: ERROR: Script execution	_ ERROR: Failed to connect to browser
failed (use -d to debug)	service: Could not negotiate a connection:SMB:
903/tcp open iss-console-mgr	Failed to receive bytes: ERROR
_banner: 220 VMware Authentication Daemon	smb2-time:
Version 1.10: SSL Required,	date: 2023-09-11T11:11:15
Lieut e signt us evites	_ start_date: N/A
Host script results:	_msrpc-enum: Could not negotiate a
_ipidseq: ERROR: Script execution failed (use	connection:SMB: Failed to receive bytes:
-d to debug)	ERROR
_dns-brute: Can't guess domain of	Nesses described Decidence (Alberton) consumed in
"192.168.198.1"; use dns-brute.domain script	Nmap done: 1 IP address (1 host up) scanned in
argument.	57.47 seconds
smb-protocols:	
dialects:	

### nmap --script auth <target>

PS C:\Users\acer> nmap --script auth 192.168.198.1 Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 16:43 India Standard Time Nmap scan report for 192.168.198.1 Host is up (0.0000080s latency). Not shown: 994 closed tcp ports (reset) PORT STATE SERVICE 22/tcp open ssh | ssh-auth-methods: | Supported authentication methods: publickey password \_ keyboard-interactive | ssh-publickey-acceptance: Accepted Public Keys: No public keys accepted 80/tcp open http |\_http-config-backup: ERROR: Script execution failed (use -d to debug) 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 5.45 seconds

### nmap --script vuln <target>

903/tcp open iss-console-mgr

PS C:\Users\acer> nmap --script vuln 192.168.198.1

Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 16:47 India Standard Time

Nmap scan report for 192.168.198.1

Host is up (0.000014s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh 80/tcp open http

\_http-csrf: Couldn't find any CSRF vulnerabilities.

http-dombased-xss: Couldn't find any DOM based XSS.

http-stored-xss: Couldn't find any stored XSS vulnerabilities.

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

903/tcp open iss-console-mgr

Host script results:

smb-vuln-ms10-054: false

| smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Lsamba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 136.54 seconds