Practical 2

Name: Saloni Vishwakarma
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 . . . . . :

Wireless LAN adapter Wi-Fi:

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 (https://nmap.org) 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-mgr
913/tcp	open	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	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:

PS C:\Users\acer> nmap -p- 192.168.198.1 -oN scan_results.txt
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
903/tcp	open	iss-console-mgr
913/tcp	open	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	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    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-mgr
913/tcp   open     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     unknown

# 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 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

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>

PS C:\Users\acer> nmap --script discovery 192.168.198.1
Starting Nmap 7.94 (https://nmap.org) at 2023-09-11 16:40 India Standard Time
Pre-scan script results:
| broadcast-igmp-discovery:
| 172.16.146.27
| Interface: eth5
| Version: 2
| Group: 224.0.0.252
| Description: Link-local Multicast Name Resolution (rfc4795)
| 172.16.146.33
| Interface: eth5
| Version: 2
| Group: 224.0.0.252
| Description: Link-local Multicast Name Resolution (rfc4795)
| 172.16.146.41
| Interface: eth5
| Version: 2
| Group: 224.0.0.252
| Description: Link-local Multicast Name Resolution (rfc4795)
| 172.16.146.58
| Interface: eth5
| Version: 2
| Group: 224.0.0.252
| Description: Link-local Multicast Name Resolution (rfc4795)
| 172.16.146.81
| Interface: eth5
| Version: 2
| Group: 224.0.0.252
| Description: Link-local Multicast Name Resolution (rfc4795)
| 172.16.146.94
| Interface: eth5
| Version: 2
| Group: 224.0.0.252
| Description: Link-local Multicast Name Resolution (rfc4795)
| 172.16.146.111
| Interface: eth5
| Version: 2
| Group: 224.0.0.252
| Description: Link-local Multicast Name Resolution (rfc4795)
| 172.16.146.119
| Interface: eth5
| Version: 2
| Group: 224.0.0.252
| Description: Link-local Multicast Name Resolution (rfc4795)

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

```
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name
Resolution (rfc4795)
| 172.16.147.10
|     Interface: eth5
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
| 172.16.147.10
|     Interface: eth5
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name
Resolution (rfc4795)
| 172.16.147.19
|     Interface: eth5
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name
Resolution (rfc4795)
| 172.16.147.21
|     Interface: eth5
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name
Resolution (rfc4795)
| 172.16.147.33
|     Interface: eth5
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
| 172.16.147.33
|     Interface: eth5
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name
Resolution (rfc4795)
| 172.16.147.40
|     Interface: eth5
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name
Resolution (rfc4795)
| 172.16.147.69
|     Interface: eth5
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name
Resolution (rfc4795)
|  172.16.146.58
|     Interface: eth5
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope
(rfc2365)
|_  Use the newtargets script-arg to add the
results as targets
| ipv6-multicast-mld-list:
| fe80::9c7b:f2b6:595c:6605:
|     device: eth5
|     mac: 18:cc:18:cd:80:39
|     multicast_ips:
|       ff02::1:3              (Link-local Multicast
Name Resolution)
|       ff02::fb               (mDNSv6)
|       ff02::c                (SSDP)
| fe80::3db1:ec11:fd4a:76c:
|     device: eth5
|     mac: 2c:33:58:20:f5:b7
|     multicast_ips:
|       ff02::fb               (mDNSv6)
|       ff02::1:3              (Link-local Multicast
Name Resolution)
|       ff02::c                (SSDP)
| fe80::5c7a:257c:ff37:8747:
|     device: eth5
|     mac: 58:ce:2a:64:3e:17
|     multicast_ips:
|       ff02::1:3              (Link-local Multicast
Name Resolution)
|       ff02::fb               (mDNSv6)
|       ff02::c                (SSDP)
| fe80::e9d9:e014:eee3:d0c8:
|     device: eth5
|     mac: 18:cc:18:ce:79:7b
|     multicast_ips:
|       ff02::fb               (mDNSv6)
|       ff02::1:3              (Link-local Multicast
Name Resolution)
|       ff02::c                (SSDP)
| fe80::567e:c82a:77:918b:
|     device: eth5
|     mac: 58:ce:2a:64:24:1d
|     multicast_ips:
|       ff02::1:3              (Link-local Multicast
Name Resolution)
|       ff02::fb               (mDNSv6)
|       ff02::c                (SSDP)
```

| fe80::76dd:a644:e79e:be3e:
| device: eth5
| mac: 2c:33:58:20:ff:a8
| multicast_ips:
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::fb (mDNSv6)
| ff02::c (SSDP)
| fe80::f758:6ef9:20fe:c691:
| device: eth5
| mac: a4:6b:b6:c8:38:09
| multicast_ips:
| ff02::fb (mDNSv6)
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::c (SSDP)
| fe80::bc31:cf79:1f86:e44a:
| device: eth5
| mac: 58:ce:2a:64:50:05
| multicast_ips:
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::fb (mDNSv6)
| ff02::c (SSDP)
| fe80::d911:38a5:d378:29e8:
| device: eth5
| mac: 50:c2:e8:c2:8d:bd
| multicast_ips:
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::fb (mDNSv6)
| ff02::c (SSDP)
| fe80::f595:fa31:7599:291d:
| device: eth5
| mac: 30:d1:6b:fa:0e:cd
| multicast_ips:
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::fb (mDNSv6)
| ff02::c (SSDP)
| fe80::aaf9:fa3e:31be:7f6b:
| device: eth5
| mac: 58:ce:2a:63:37:92
| multicast_ips:
| ff02::1:3 (Link-local Multicast Name Resolution)
| fe80::7b20:2592:c1d7:a1e6:
| device: eth5
| mac: 2c:33:58:20:f9:31
| multicast_ips:
| ff02::fb (mDNSv6)
| fe80::f205:8925:cbeb:aeec:
| device: eth5
| mac: 58:ce:2a:63:7c:ca
| multicast_ips:
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::fb (mDNSv6)
| ff02::c (SSDP)
| fe80::9356:5e97:1dd6:6d8a:
| device: eth5
| mac: 2c:33:58:21:00:8e
| multicast_ips:
| ff02::fb (mDNSv6)
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::c (SSDP)
| fe80::b7cd:e517:b9ad:c83b:
| device: eth5
| mac: c0:3c:59:77:a7:d6
| multicast_ips:
| ff02::c (SSDP)
| ff02::fb (mDNSv6)
| ff02::1:3 (Link-local Multicast Name Resolution)
| fe80::3587:6106:687:3d72:
| device: eth5
| mac: 2c:33:58:20:fe:09
| multicast_ips:
| ff02::fb (mDNSv6)
| ff02::1:3 (Link-local Multicast Name Resolution)
| fe80::d0e0:14df:dbc6:b0b1:
| device: eth5
| mac: 00:e0:2d:93:19:e4
| multicast_ips:
| ff02::fb (mDNSv6)
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::c (SSDP)
| fe80::1626:3b35:601e:c2cc:
| device: eth5
| mac: 18:cc:18:2d:d8:e5
| multicast_ips:
| ff02::c (SSDP)
| ff02::fb (mDNSv6)
| ff02::1:3 (Link-local Multicast Name Resolution)

| fe80::3ceb:4d2:9707:e2b7:
| device: eth5
| mac: 30:03:c8:83:a3:4d
| multicast_ips:
| ff02::fb (mDNSv6)
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::c (SSDP)
| fe80::c274:adff:fec2:415:
| device: eth5
| mac: c0:74:ad:c2:04:15
| multicast_ips:
| ff02::fb (mDNSv6)
| fe80::6482:5c63:9eb2:a331:
| device: eth5
| mac: 2c:33:58:21:00:07
| multicast_ips:
| ff02::fb (mDNSv6)
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::c (SSDP)
| fe80::decd:2fff:fe01:dc9c:
| device: eth5
| mac: dc:cd:2f:01:dc:9c
| multicast_ips:
| ff02::c (SSDP)
| fe80::1a08:bab:278a:3f0d:
| device: eth5
| mac: 2c:33:58:20:fc:e2
| multicast_ips:
| ff02::fb (mDNSv6)
| ff02::1:3 (Link-local Multicast Name Resolution)
| fe80::8062:168:7fb:f3ff:
| device: eth5
| mac: 50:5a:65:fa:fa:64
| multicast_ips:
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::c (SSDP)
| fe80::2cf3:5dae:5efc:e2c3:
| device: eth5
| mac: 2c:33:58:20:fd:0f
| multicast_ips:
| ff02::fb (mDNSv6)
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::c (SSDP)
| fe80::4a70:ea17:f73b:3a35:
| device: eth5
| mac: 2c:33:58:20:ff:49
| multicast_ips:
| ff02::c (SSDP)
| fe80::8e75:9050:76a6:ad42:
| device: eth5
| mac: 14:18:c3:05:9f:dd
| multicast_ips:
| ff02::fb (mDNSv6)
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::c (SSDP)
| fe80::966e:2702:127b:c3d7:
| device: eth5
| mac: 14:18:c3:02:97:b1
| multicast_ips:
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::fb (mDNSv6)
| ff02::c (SSDP)
| fe80::703e:e4cc:99e1:d20e:
| device: eth5
| mac: f4:b5:20:47:25:b7
| multicast_ips:
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::fb (mDNSv6)
| ff02::c (SSDP)
| fe80::f38a:2592:5e3:1c5e:
| device: eth5
| mac: 3c:91:80:93:75:59
| multicast_ips:
| ff02::fb (mDNSv6)
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::c (SSDP)
| fe80::d8fd:cf0e:3691:86c0:
| device: eth5
| mac: 2c:33:58:20:f5:a8
| multicast_ips:
| ff02::1:3 (Link-local Multicast Name Resolution)
| ff02::c (SSDP)
| fe80::68b8:cd7b:3572:220f:
| device: eth5
| mac: 2c:33:58:20:ff:4e
| multicast_ips:
| ff02::fb (mDNSv6)

```
|      ff02::1:3                (Link-local Multicast
Name Resolution)
|      ff02::c                  (SSDP)
| fe80::cbe4:d8be:428e:9fde:
|    device: eth5
|    mac: 10:a5:1d:f9:0d:e4
|    multicast_ips:
|      ff02::fb                 (mDNSv6)
|      ff02::1:3                (Link-local Multicast
Name Resolution)
|      ff02::c                  (SSDP)
|  fe80::ecd0:5823:967a:4361:
|    device: eth5
|    mac: f4:b5:20:48:91:02
|    multicast_ips:
|      ff02::1:3                (Link-local Multicast
Name Resolution)
|      ff02::fb                 (mDNSv6)
|      ff02::c                  (SSDP)
|  fe80::c0e9:a889:1565:3e0d:
|    device: eth5
|    mac: 2c:33:58:20:fb:11
|    multicast_ips:
|      ff02::fb                 (mDNSv6)
|      ff02::1:3                (Link-local Multicast
Name Resolution)
|      ff02::c                  (SSDP)
| fe80::c274:adff:fec2:416:
|    device: eth5
|    mac: c0:74:ad:c2:04:16
|    multicast_ips:
|      ff02::fb                 (mDNSv6)
| fe80::f32e:b9e0:3ec2:a:
|    device: eth5
|    mac: 18:cc:18:2d:d8:3b
|    multicast_ips:
|      ff02::1:3                (Link-local Multicast
Name Resolution)
|      ff02::fb                 (mDNSv6)
|      ff02::c                  (SSDP)
| fe80::59b:5208:5e6f:753e:
|    device: eth5
|    mac: 2c:33:58:20:f5:ad
|    multicast_ips:
|      ff02::fb                 (mDNSv6)
|_     ff02::1:3                (Link-local Multicast
Name Resolution)
| targets-ipv6-multicast-mld:
| IP: fe80::1626:3b35:601e:c2cc  MAC:
18:cc:18:2d:d8:e5  IFACE: eth5
| IP: fe80::1a08:bab:278a:3f0d  MAC:
2c:33:58:20:fc:e2  IFACE: eth5
| IP: fe80::2cf3:5dae:5efc:e2c3  MAC:
2c:33:58:20:fd:0f  IFACE: eth5
| IP: fe80::3587:6106:687:3d72  MAC:
2c:33:58:20:fe:09  IFACE: eth5
| IP: fe80::3ceb:4d2:9707:e2b7  MAC:
30:03:c8:83:a3:4d  IFACE: eth5
| IP: fe80::3db1:ec11:fd4a:76c  MAC:
2c:33:58:20:f5:b7  IFACE: eth5
| IP: fe80::4a70:ea17:f73b:3a35  MAC:
2c:33:58:20:ff:49  IFACE: eth5
|  IP: fe80::567e:c82a:77:918b    MAC:
58:ce:2a:64:24:1d  IFACE: eth5
| IP: fe80::59b:5208:5e6f:753e  MAC:
2c:33:58:20:f5:ad  IFACE: eth5
| IP: fe80::5c7a:257c:ff37:8747  MAC:
58:ce:2a:64:3e:17  IFACE: eth5
| IP: fe80::6482:5c63:9eb2:a331  MAC:
2c:33:58:21:00:07  IFACE: eth5
| IP: fe80::68b8:cd7b:3572:220f  MAC:
2c:33:58:20:ff:4e  IFACE: eth5
| IP: fe80::703e:e4cc:99e1:d20e  MAC:
f4:b5:20:47:25:b7  IFACE: eth5
| IP: fe80::76dd:a644:e79e:be3e  MAC:
2c:33:58:20:ff:a8  IFACE: eth5
| IP: fe80::7b20:2592:c1d7:a1e6  MAC:
2c:33:58:20:f9:31  IFACE: eth5
|  IP: fe80::8062:168:7fb:f3ff    MAC:
50:5a:65:fa:fa:64  IFACE: eth5
| IP: fe80::8e75:9050:76a6:ad42  MAC:
14:18:c3:05:9f:dd  IFACE: eth5
| IP: fe80::9356:5e97:1dd6:6d8a  MAC:
2c:33:58:21:00:8e  IFACE: eth5
| IP: fe80::966e:2702:127b:c3d7  MAC:
14:18:c3:02:97:b1  IFACE: eth5
| IP: fe80::9c7b:f2b6:595c:6605  MAC:
18:cc:18:cd:80:39  IFACE: eth5
| IP: fe80::aaf9:fa3e:31be:7f6b  MAC:
58:ce:2a:63:37:92  IFACE: eth5
| IP: fe80::b7cd:e517:b9ad:c83b  MAC:
c0:3c:59:77:a7:d6  IFACE: eth5
| IP: fe80::bc31:cf79:1f86:e44a  MAC:
58:ce:2a:64:50:05  IFACE: eth5
| IP: fe80::c0e9:a889:1565:3e0d  MAC:
2c:33:58:20:fb:11  IFACE: eth5
```

```
| IP: fe80::c274:adff:fec2:415  MAC:
c0:74:ad:c2:04:15  IFACE: eth5
| IP: fe80::c274:adff:fec2:416  MAC:
c0:74:ad:c2:04:16  IFACE: eth5
| IP: fe80::cbe4:d8be:428e:9fde  MAC:
10:a5:1d:f9:0d:e4  IFACE: eth5
| IP: fe80::d0e0:14df:dbc6:b0b1  MAC:
00:e0:2d:93:19:e4  IFACE: eth5
| IP: fe80::d8fd:cf0e:3691:86c0 MAC:
2c:33:58:20:f5:a8  IFACE: eth5
| IP: fe80::d911:38a5:d378:29e8  MAC:
50:c2:e8:c2:8d:bd  IFACE: eth5
| IP: fe80::decd:2fff:fe01:dc9c  MAC:
dc:cd:2f:01:dc:9c  IFACE: eth5
| IP: fe80::e9d9:e014:eee3:d0c8  MAC:
18:cc:18:ce:79:7b  IFACE: eth5
| IP: fe80::ecd0:5823:967a:4361  MAC:
f4:b5:20:48:91:02  IFACE: eth5
| IP: fe80::f205:8925:cbeb:aeec  MAC:
58:ce:2a:63:7c:ca  IFACE: eth5
|  IP: fe80::f32e:b9e0:3ec2:a     MAC:
18:cc:18:2d:d8:3b  IFACE: eth5
| IP: fe80::f38a:2592:5e3:1c5e  MAC:
3c:91:80:93:75:59  IFACE: eth5
| IP: fe80::f595:fa31:7599:291d  MAC:
30:d1:6b:fa:0e:cd  IFACE: eth5
| IP: fe80::f758:6ef9:20fe:c691  MAC:
a4:6b:b6:c8:38:09  IFACE: eth5
|
|_  Use --script-args=newtargets to add the
results as targets
|_hostmap-robtex: *TEMPORARILY DISABLED*
due to changes in Robtex's API. See
https://www.robtex.com/api/
|_http-robtex-shared-ns: *TEMPORARILY
DISABLED* due to changes in Robtex's API.
See https://www.robtex.com/api/
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Nmap scan report for 192.168.198.1
Host is up (0.000069s latency).
Not shown: 994 closed tcp ports (reset)
Bug in http-security-headers: no string output.
PORT    STATE SERVICE
22/tcp  open  ssh
|_banner: SSH-2.0-OpenSSH_for_Windows_8.6
| ssh2-enum-algos:
|  kex_algorithms: (9)
|  server_host_key_algorithms: (5)
|  encryption_algorithms: (6)
|  mac_algorithms: (10)
|_  compression_algorithms: (2)
| 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:d
4 (ECDSA)
|_ 256
ce:8b:83:e9:8a:7e:dd:00:aa:27:1d:e4:b4:b1:9a:9
a (ED25519)
80/tcp  open  http
| http-useragent-tester:
|  Status for browser useragent: 404
|  Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting
Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
|_http-xssed: No previously reported XSS vuln.
|_http-title: Site doesn't have a title.
| http-errors:
| Spidering limited to: maxpagecount=40;
withinhost=192.168.198.1
|  Found the following error pages:
|
|  Error Code: 404
|_      http://192.168.198.1:80/
|_http-chrono: Request times for /; avg:
122.20ms; min: 46.00ms; max: 164.00ms
|_http-mobileversion-checker: No mobile version
detected.
```

|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.
| http-sitemap-generator:
| Directory structure:
| Longest directory structure:
| Depth: 0
| Dir: /
| Total files found (by extension):
|_
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-date: Mon, 11 Sep 2023 11:11:30 GMT; -1s from local time.
|_http-comments-displayer: Couldn't find any comments.
|_http-feed: Couldn't find any feeds.
| http-vhosts:
|_128 names had status 404
| http-headers:
| Server: Microsoft-IIS/10.0
| Date: Mon, 11 Sep 2023 11:11:30 GMT
| Connection: close
| Content-Length: 0
|
|_ (Request type: GET)
135/tcp open msrpc
139/tcp open netbios-ssn
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
445/tcp open microsoft-ds
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
903/tcp open iss-console-mgr
|_banner: 220 VMware Authentication Daemon Version 1.10: SSL Required,...

Host script results:
|_ipidseq: ERROR: Script execution failed (use -d to debug)
|_dns-brute: Can't guess domain of "192.168.198.1"; use dns-brute.domain script argument.
| smb-protocols:
| dialects:

| 2:0:2
| 2:1:0
| 3:0:0
| 3:0:2
|_   3:1:1
|_qscan: ERROR: Script execution failed (use -d to debug)
| smb2-capabilities:
| 2:0:2:
| Distributed File System
| 2:1:0:
| Distributed File System
| Leasing
| Multi-credit operations
| 3:0:0:
| Distributed File System
| Leasing
| Multi-credit operations
| 3:0:2:
| Distributed File System
| Leasing
| Multi-credit operations
| 3:1:1:
| Distributed File System
| Leasing
|_   Multi-credit operations
|_fcrdns: FAIL (No PTR record)
|_path-mtu: ERROR: Script execution failed (use -d to debug)
| smb2-security-mode:
| 3:1:1:
|_   Message signing enabled but not required
| smb-mbenum:
|_ ERROR: Failed to connect to browser service: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| smb2-time:
| date: 2023-09-11T11:11:15
|_ start_date: N/A
|_msrpc-enum: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 57.47 seconds

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
903/tcp open  iss-console-mgr

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

nmap --script vuln <target>

```
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
|_samba-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
```