

**Vulnerability Assessment & Penetration
Testing**

LAB MANUAL

Subject Code: **18PC0CY05**

Regulation: R 18

Class: IV Year B. Tech. I Sem CSE (Cyber
Security)

Experiment No. 1

Aim: Monitoring the network traffic using Wireshark

2. Objectives: To observe the performance in promiscuous & non-promiscuous mode & to find the packets based on different filters.

3. Outcomes: The learner will be able to:-

Identify different packets moving in/out of network using packet sniffer for network analysis.

Understand professional, ethical, legal, security and social issues and responsibilities. Also will be able to analyze the local and global impact of computing on individuals, organizations, and society.

Match the industry requirements in the domains of Database management, Programming and Networking with the required management skills.

4. Hardware / Software Required: Wireshark, Ethereal and tcpdump.

5. Theory:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets.

Applications:

Network administrators use it to troubleshoot network problems

Network security engineers use it to examine security problems

Developers use it to debug protocol implementations

People use it to learn network protocol internals beside these examples can be helpful in many other situations too. **Features:**

The following are some of the many features wireshark provides:

Available for UNIX and Windows.

Capture live packet data from a network interface.

Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.

Import packets from text files containing hex dumps of packet data.

Display packets with very detailed protocol information.

Export some or all packets in a number of capture file formats.

Filter packets on many criteria.

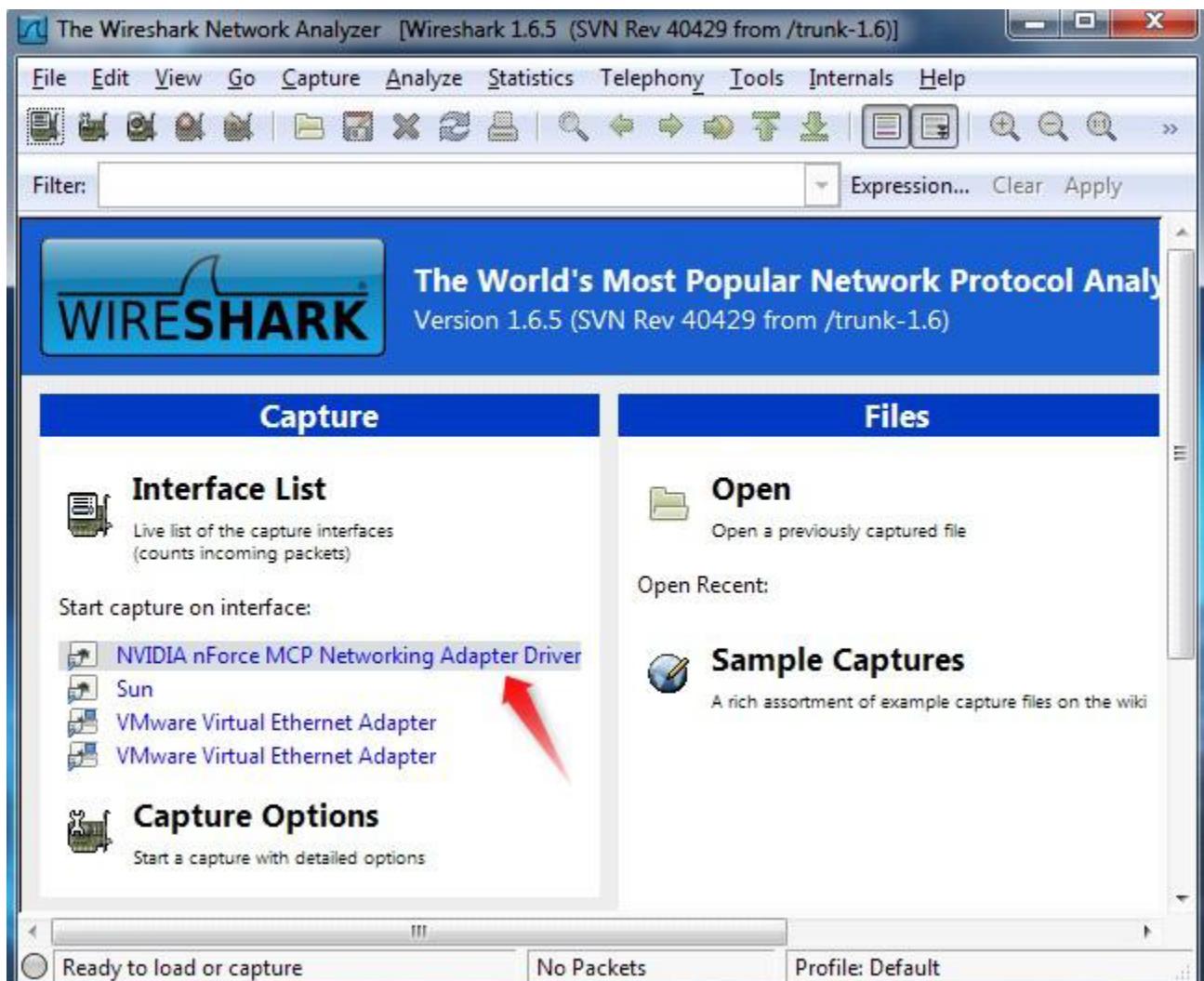
Search for packets on many criteria.

Colorize packet display based on filters.

Create various statistics.

Capturing Packets

After downloading and installing wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by clicking Capture Options.



As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system. If you're capturing on a wireless interface and have promiscuous mode enabled in your capture options, you'll also see other the other packets on the network

Capturing from NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev ...)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length
1038	40.422312	192.168.1.77	173.194.33.1	TCP	54
1039	40.659611	fe80::bdca:e67b:5eb7:ffff02::c		SSDP	208
1040	41.550320	192.168.1.77	207.8.65.23	HTTP	51
1041	41.580992	207.8.65.23	192.168.1.77	TCP	60
1042	42.051665	192.168.1.76	239.255.255.250	UDP	50
1043	42.104199	Actionte_d8:a3:88	Msi_74:82:e6	ARP	60
1044	42.104226	Msi_74:82:e6	onte_d8:a3:88	ARP	42
1045	42.119803	192.168.1.74	239.255.255.250	UDP	56
1046	42.910321	192.168.1.77	74.125.53.125	Jabber/	51
1047	42.929318	74.125.53.125	192.168.1.77	TCP	60
1048	43.659423	fe80::bdca:e67b:5eb7:ffff02::c		SSDP	208
1049	45.052365	192.168.1.76	239.255.255.250	UDP	50
1050	45.121318	192.168.1.74	239.255.255.250	UDP	56
1051	45.418680	192.168.1.77	72.165.61.176	UDP	126
1052	46.659410	fe80::bdca:e67b:5eb7:ffff02::c		SSDP	208

Frame 924: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: CiscoSpv_4a:df:be (60:2a:d0:4a:df:be), Dst: IPv4mcast_6f:00 (232.239.0.1)
Internet Protocol Version 4, Src: 192.168.1.76 (192.168.1.76), Dst: 232.239.0.1
Internet Group Management Protocol

Hex	Dec	ASCII
0000	01 00 5e 6f 00 0a 60 2a	d0 4a df be 08 00 46 a0 ..^o...`* .J....F.
0010	00 20 57 53 00 00 01 02	21 f7 c0 a8 01 4c e8 ef . WS.... !....L..
0020	00 0a 94 04 00 00 16 00	01 06 e8 ef 00 0a 00 00
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00

Click the stop capture button near the top left corner of the window when you want to stop capturing traffic.

Capturing from NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev ...)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

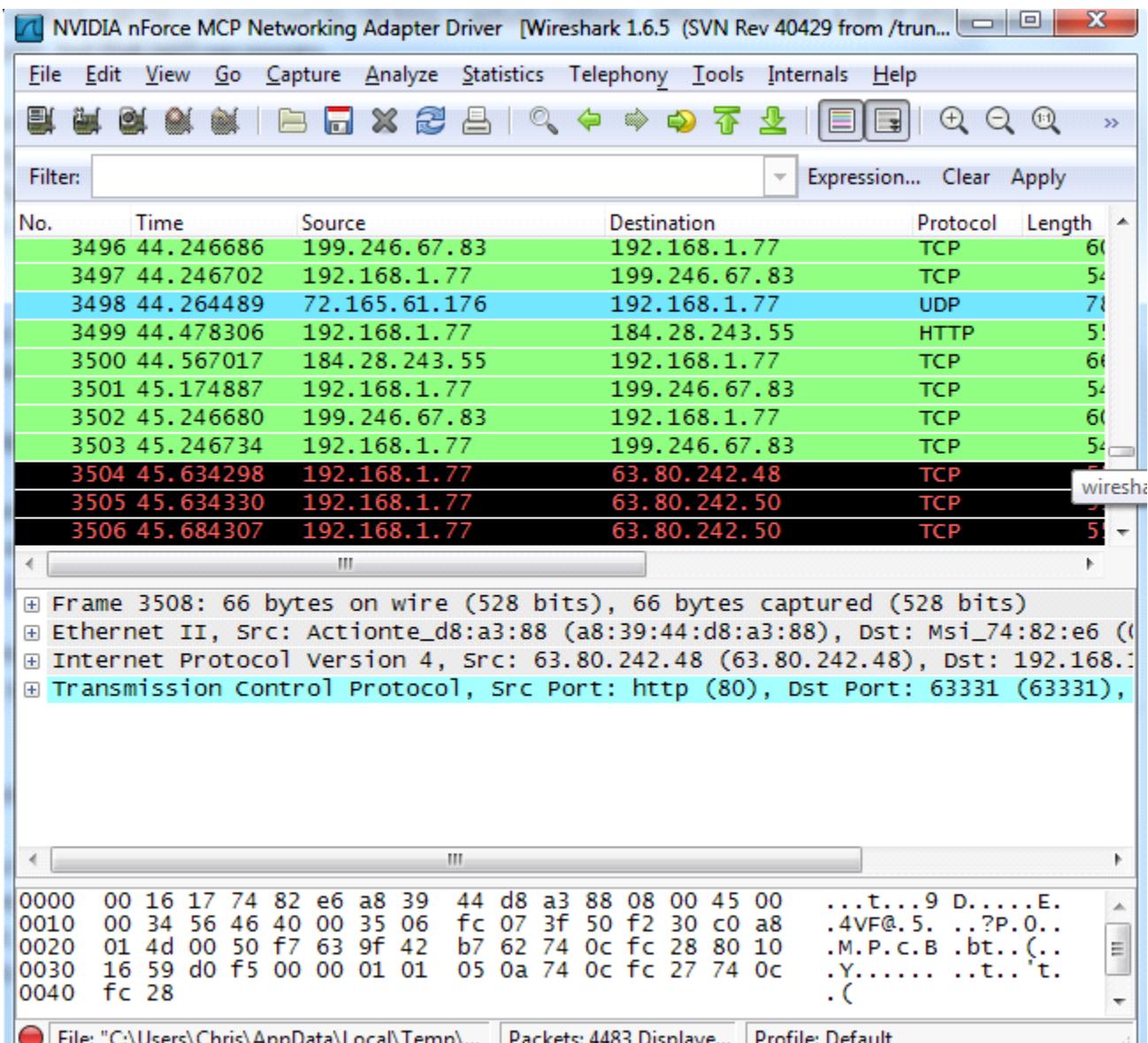
No.	Time	Source	Destination	Protocol	Length
1196	69.066042	192.168.1.76	239.255.255.250	UDP	50
1197	69.134051	192.168.1.74	239.255.255.250	UDP	56
1198	69.739231	173.194.33.1	192.168.1.77	TLSv1	13!
1199	69.829177	192.168.1.77	63.80.4.133	TCP	92
1200	69.862702	192.168.1.77	207.8.65.23	TCP	115
1201	69.862750	192.168.1.77	207.8.65.23	HTTP	344
1202	69.863851	192.168.1.77	207.8.65.23	TCP	115
1203	69.863895	192.168.1.77	207.8.65.23	HTTP	28!
1204	69.896441	207.8.65.23	192.168.1.77	TCP	60
1205	69.897417	207.8.65.23	192.168.1.77	TCP	60
1206	69.900444	207.8.65.23	192.168.1.77	TCP	60
1207	69.901173	207.8.65.23	192.168.1.77	TCP	60
1208	69.912970	207.8.65.23	192.168.1.77	HTTP	280
1209	69.917987	207.8.65.23	192.168.1.77	HTTP	321
1210	69.940316	192.168.1.77	173.194.33.1	TCP	54

Frame 924: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: CiscoSpv_4a:df:be (60:2a:d0:4a:df:be), Dst: IPv4mcast_6f:00 (01:00:5e:6f:00:0a)
Internet Protocol Version 4, Src: 192.168.1.76 (192.168.1.76), Dst: 232.239.1.1 (173.194.33.1)
Internet Group Management Protocol

0000 01 00 5e 6f 00 0a 60 2a d0 4a df be 08 00 46 a0 ..^o...`* .J....F.
0010 00 20 57 53 00 00 01 02 21 f7 c0 a8 01 4c e8 ef . WS.... !....L..
0020 00 0a 94 04 00 00 16 00 01 06 e8 ef 00 0a 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

NVIDIA nForce MCP Networking Adapter Driver | Packets: 1210 Displaved | Profile: Default

Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems – for example, they could have been delivered out-of-order.



Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type `-dns||` and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trunk...)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: dns

No.	Time	Source	Destination	Protocol	Length
1019	9.161980	192.168.1.77	8.8.8.8	DNS	86
1020	9.161988	192.168.1.77	8.8.8.8	DNS	76
1021	9.164656	192.168.1.77	8.8.8.8	DNS	102
1029	9.181951	8.8.8.8	192.168.1.77	DNS	102
1031	9.191415	8.8.8.8	192.168.1.77	DNS	109
1032	9.204042	192.168.1.77	8.8.8.8	DNS	79
1034	9.224022	8.8.8.8	192.168.1.77	DNS	284
1035	9.239748	192.168.1.77	8.8.8.8	DNS	80
1050	9.260332	8.8.8.8	192.168.1.77	DNS	274
1296	21.095831	192.168.1.77	8.8.8.8	DNS	83
1297	21.115981	8.8.8.8	192.168.1.77	DNS	99
1222	22.244702	192.168.1.75	224.0.0.251	MDNS	20

Frame 1021: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
Ethernet II, Src: Msi_74:82:e6 (00:16:17:74:82:e6), Dst: Actionte_d8:a3:88 (00:16:17:d8:a3:88)
Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 8.8.8.8
User Datagram Protocol, Src Port: 58168 (58168), Dst Port: domain (53)
Domain Name System (query)

File: "C:\Users\Chris\AppData\Local\Temp\...\Packets: 4483 Displave..." Profile: Default

Another interesting thing you can do is right-click a packet and select Follow TCP Stream

NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trunk...)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length
1031	9.191415	8.8.8.8	192.168.1.77	DNS	109
1032	9.204042	192.168.1.77	8.8.8.8	DNS	79
1033	9.204306	192.168.1.77	96.6.193.244	TCP	54
1034	9.224022	8.8.8.8	192.168.1.77	DNS	284
1035	9.239748	192.168.1.77	8.8.8.8	DNS	80
1036	9.243917	192.168.1.77	172.104.22.41	HTTP	758
1037	9.245027	192.168.1.77		TCP	66
1038	9.245665	192.168.1.77		TCP	66
1039	9.255815	63.80.4.133		TCP	1514
1040	9.256284	63.80.4.133		TCP	1514
1041	9.256314	192.168.1.77		TCP	52

Frame 1036: 758 bytes on wire (6064 bits)
Ethernet II, Src: MSI_74:82:e6 (08:00:22:41:74:82), Dst: 173.194.1.1 (0a:00:27:01:00:01)
Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 173.194.1.1 (173.194.1.1)
Transmission Control Protocol, Src Port: http (80), Dst Port: http (80), Seq: 1, Ack: 1, Len: 758
Hypertext Transfer Protocol

Follow TCP Stream

Follow UDP Stream

Follow SSL Stream

Copy

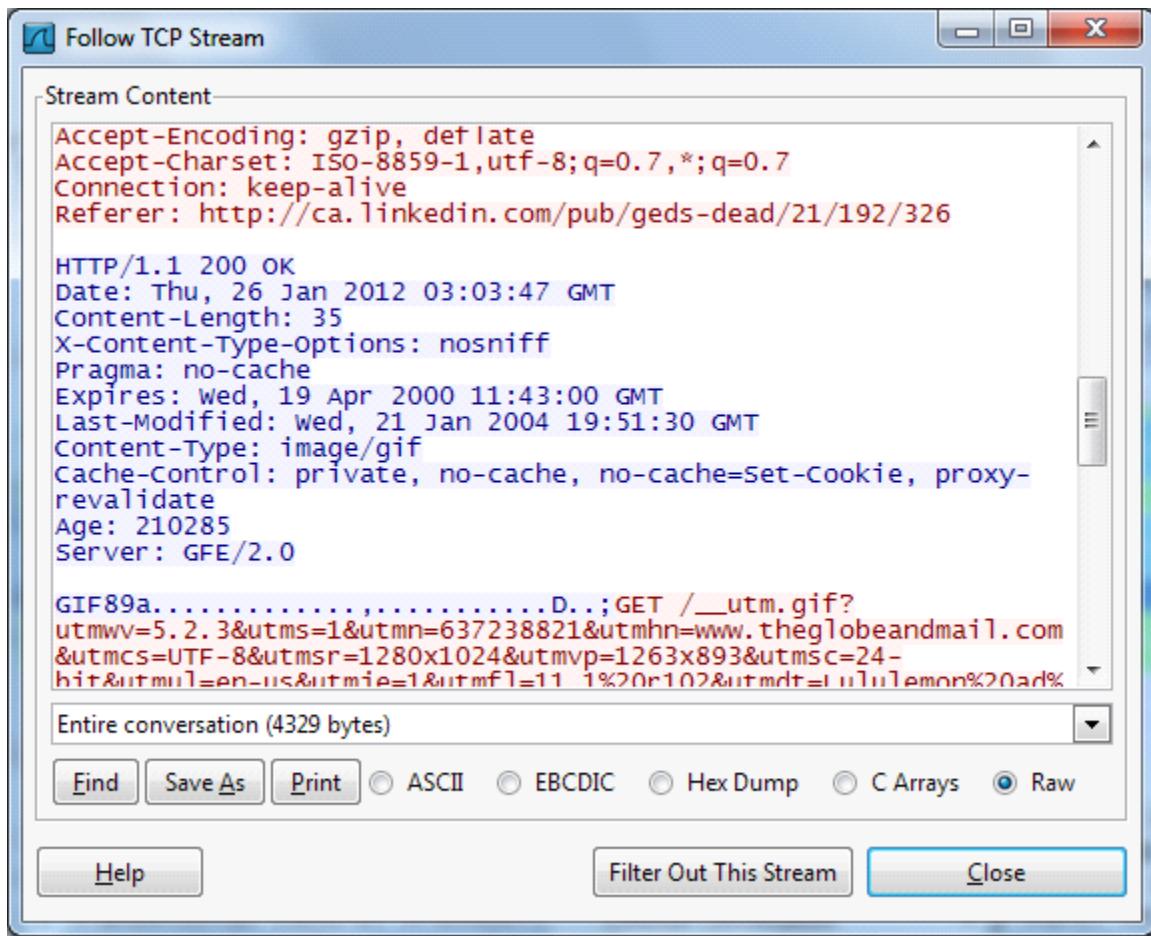
Decode As...

Print...

Show Packet in New Window

File: "C:\Users\Chris\AppData\Local\Temp\..." | Packets: 4483 Displayed | Profile: Default

You'll see the full conversation between the client and the server.



Close the window and you'll find a filter has been applied automatically – Wireshark is showing you the packets that make up the conversation.

NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trunk...)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 67 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length
1036	9.243917	192.168.1.77	173.194.33.41	HTTP	758 G
1046	9.258497	173.194.33.41	192.168.1.77	HTTP	430 H
1048	9.258920	192.168.1.77	173.194.33.41	HTTP	1120 G
1059	9.273910	173.194.33.41	192.168.1.77	HTTP	430 H
1096	9.473301	192.168.1.77	173.194.33.41	TCP	54 6
2307	29.191953	192.168.1.77	173.194.33.41	TCP	1484 D
2308	29.191961	192.168.1.77	173.194.33.41	HTTP	55 G
2309	29.210835	173.194.33.41	192.168.1.77	TCP	60 h
2310	29.211104	173.194.33.41	192.168.1.77	HTTP	430 H
2374	29.411299	192.168.1.77	173.194.33.41	TCP	54 6

+ Frame 1036: 758 bytes on wire (6064 bits), 758 bytes captured (6064 bits)
+ Ethernet II, Src: Msi_74:82:e6 (00:16:17:74:82:e6), Dst: Actionte_d8:a3:88 (00:16:17:74:d8:a3)
+ Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 173.194.33.41 (173.194.33.41)
+ Transmission Control Protocol, Src Port: 63752 (63752), Dst Port: http (80),
+ Hypertext Transfer Protocol

Hex	Dec	ASCII
0000	a8 39 44 d8 a3 88 00 16	..9D..... .t....E.
0010	17 74 82 e6 08 00 45 00	. .#.@... C....M..
0020	43 a4 c0 a8 01 4d ad c2	!)...P.1 T.....P.
0030	54 ad 8f 0f 98 97 50 18	?..Ev..GE T /__utm
0040	54 20 2f 5f 75 74 6d	.gif?utm wv=5.2.3
0050	77 76 3d 35 2e 32 2e 33	_utmrc-18 utmn-200

File: "C:\Users\Chris\AppData\Local\Temp\..." Packets: 4483 Displayed Profile: Default

Inspecting Packets

Click a packet to select it and you can dig down to view its details.

NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trunk...)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

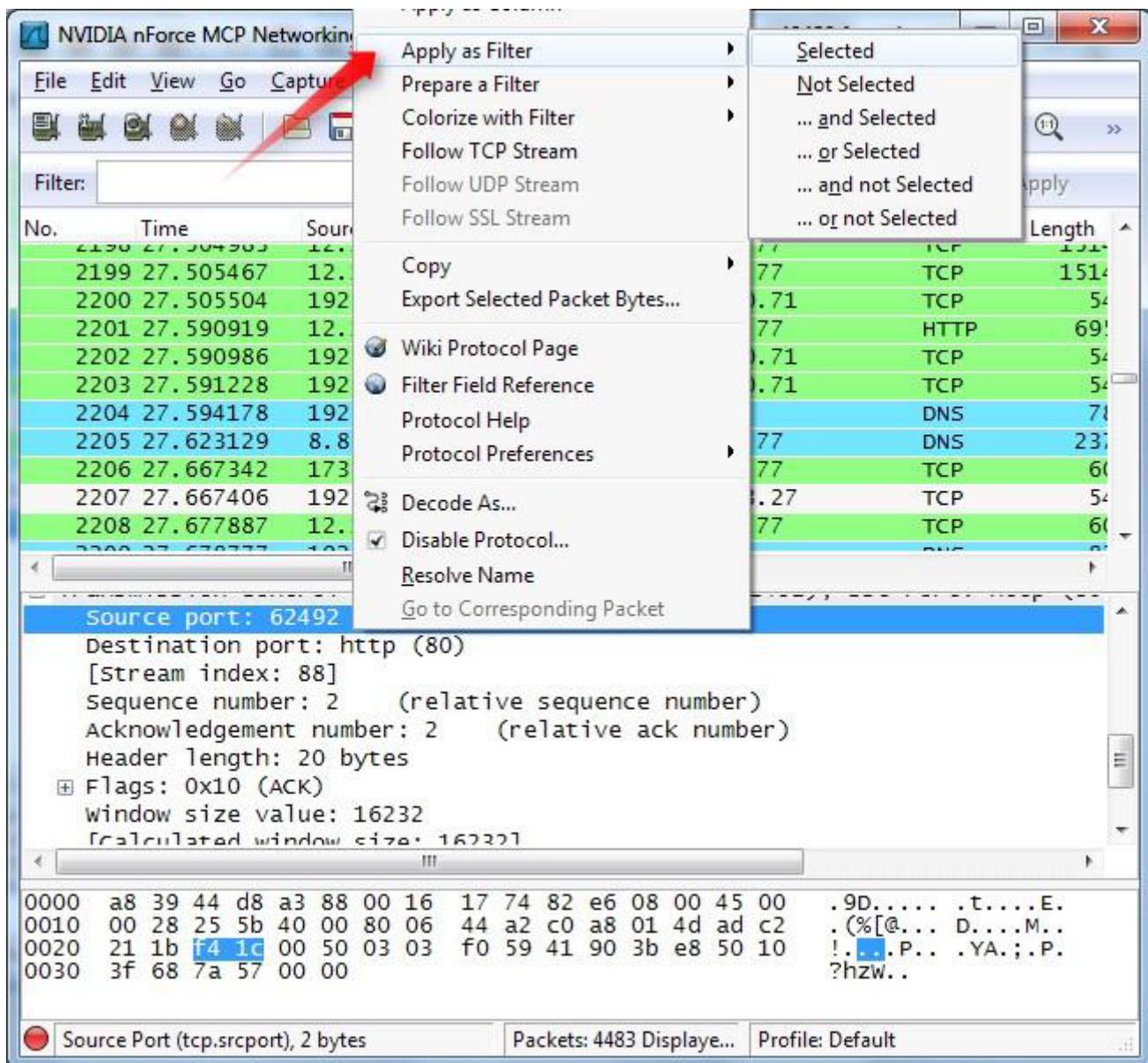
No.	Time	Source	Destination	Protocol	Length
2198	27.504563	12.129.210.71	192.168.1.77	TCP	151
2199	27.505467	12.129.210.71	192.168.1.77	TCP	151
2200	27.505504	192.168.1.77	12.129.210.71	TCP	54
2201	27.590919	12.129.210.71	192.168.1.77	HTTP	69
2202	27.590986	192.168.1.77	12.129.210.71	TCP	54
2203	27.591228	192.168.1.77	12.129.210.71	TCP	54
2204	27.594178	192.168.1.77	8.8.8.8	DNS	70
2205	27.623129	8.8.8.8	192.168.1.77	DNS	23
2206	27.667342	173.194.33.27	192.168.1.77	TCP	60
2207	27.667406	192.168.1.77	173.194.33.27	TCP	54
2208	27.677887	12.129.210.71	192.168.1.77	TCP	60
2209	27.677887	192.168.1.77	8.8.8.8	DNS	23

Frame 2207: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Arrival Time: Jan 28, 2012 05:28:58.189043000 Pacific Standard Time
Epoch Time: 1327757338.189043000 seconds
[Time delta from previous captured frame: 0.000064000 seconds]
[Time delta from previous displayed frame: 0.000064000 seconds]
[Time since reference or first frame: 27.667406000 seconds]
Frame Number: 2207
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)

Hex	Dec	Text
0000	a8 39 44 d8 a3 88 00 16	.9D..... t....E.
0010	17 74 82 e6 08 00 45 00	. (%[@... D....M..
0020	00 28 25 5b 40 00 80 06	!....P... .YA.;.P.
0030	44 a2 c0 a8 01 4d ad c2	?hzw..
	f0 59 41 90 3b e8 50 10	
	3f 68 7a 57 00 00	

Frame (frame), 54 bytes Packets: 4483 Displayed... Profile: Default

You can also create filters from here – just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

6. Conclusion:

In this experiment we analyze various packet sniffing tools that monitor network traffic transmitted between legitimate users or in the network. The packet sniffer is network monitoring tool. It is opted for network monitoring, traffic analysis, troubleshooting, Packet grapping, message, protocol analysis, penetration testing and many other purposes.

Experiment -2

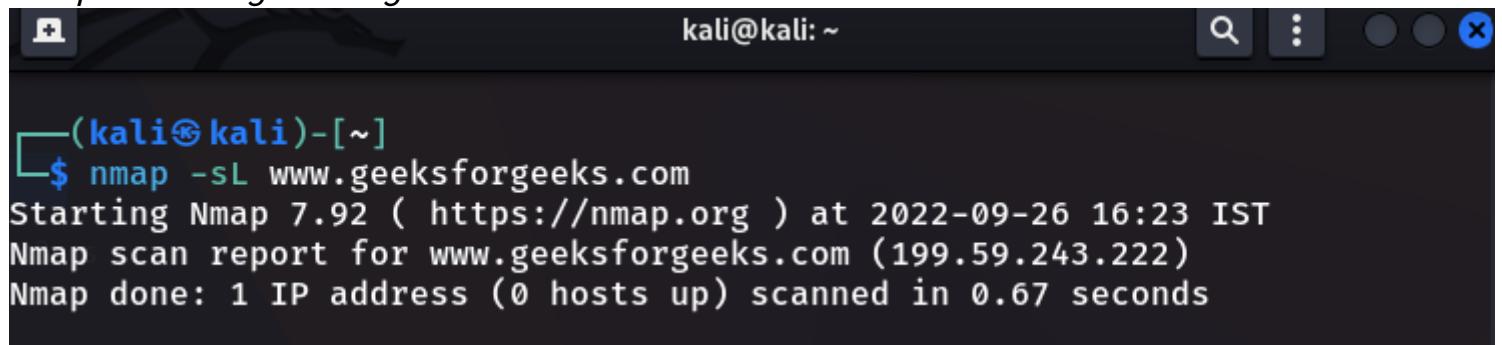
Host Discovery in Nmap Network Scanning

Nmap becomes the primary tool for scanning the network, while other scanner tools still compete with Nmap. Many hosts in the organization are filtered by the firewall which is not detectable in the network. But this can be possible using host discovery using Nmap. Host discovery in Nmap is the process of gathering information about the host in the respective network. Host discovery is also known as [ping scan](#). Nmap uses options like ping or built-in script to look after ports, services, and running servers on respective IPs using [TCP](#) and [UDP](#). This may lead to further enumeration.

The function of Host discovery in Nmap:

- **List Scan:** A list scan generally lists the possible host without sending any packets to the targeted host.

```
nmap -sL www.geeksforgeeks.com
```

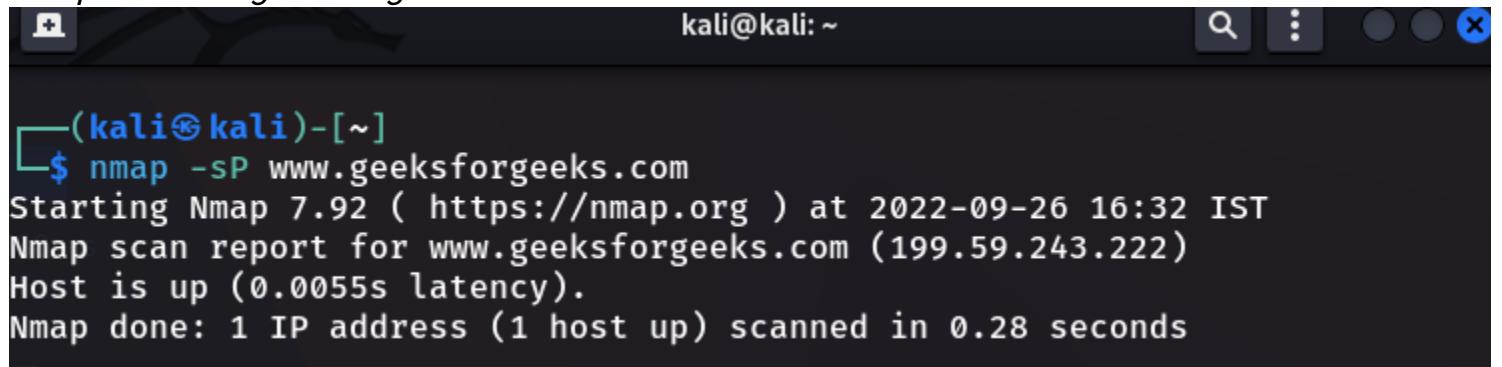


A terminal window titled 'kali@kali: ~' showing the command \$ nmap -sL www.geeksforgeeks.com. The output indicates that Nmap 7.92 is starting at 2022-09-26 16:23 IST, scanning the IP 199.59.243.222, and has completed the scan in 0.67 seconds, reporting 1 IP address (0 hosts up).

```
(kali㉿kali)-[~]
$ nmap -sL www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:23 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Nmap done: 1 IP address (0 hosts up) scanned in 0.67 seconds
```

- **Ping Sweep:** Ping sweep discovers on the basis the host is powered on.

```
nmap -sP www.geeksforgeeks.com
```



A terminal window titled 'kali@kali: ~' showing the command \$ nmap -sP www.geeksforgeeks.com. The output indicates that Nmap 7.92 is starting at 2022-09-26 16:32 IST, scanning the IP 199.59.243.222, and has completed the scan in 0.28 seconds, reporting 1 IP address (1 host up). It also notes that the host is up with 0.0055s latency.

```
(kali㉿kali)-[~]
$ nmap -sP www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:32 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0055s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

- **Disable ARP Ping:** Nmap mostly uses [ARP](#) ping to discover the other host in the network. To disable ARP Ping, use option –disable-arp-ping.

```
nmap -sn www.geeksforgeeks.com --disable-arp-ping
```

kali@kali: ~

```
└─(kali㉿kali)-[~]
$ nmap -sn www.geeksforgeeks.com --disable-arp-ping
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:40 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0099s latency).
Nmap done: 1 IP address (1 host up) scanned in 5.95 seconds
```

- **TCP SYN Ping:** Nmap checks whether a host is online.

nmap -PS www.geeksforgeeks.com

```
└─(kali㉿kali)-[~]
$ nmap -PS www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:45 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0093s latency).

Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 6.19 seconds
```

- **TCP ACK Ping:** Nmap checks whether the host is responding.

nmap -sA www.geeksforgeeks.com

```
root@kali: /home/kali
└─(root㉿kali)-[/home/kali]
# nmap -sA www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:51 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.011s latency).

All 1000 scanned ports on www.geeksforgeeks.com (199.59.243.222) are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.85 seconds
```

- **ICMP Echo Ping:** Nmap sends ICMP packets to the available host.

nmap -PE www.geeksforgeeks.com

```
[+] root@kali:[/home/kali]
# nmap -PE www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 17:00 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0071s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 5.38 seconds
```

- **UDP Ping:** Nmap sends the UDP packets to the targeted port.

```
nmap -sU www.geeksforgeeks.com
```

```
[+] root@kali:[/home/kali]
# nmap -sU www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 12:38 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0078s latency).
All 1000 scanned ports on www.geeksforgeeks.com (199.59.243.222) are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.92 seconds
```

- **IP Protocol Ping:** Nmap tries to send different packets using different protocols.

```
nmap -v -PO www.geeksforgeeks.com
```

```
ser pentestlab
└─(root㉿kali)-[~/home/kali]
└─# nmap -v -PO www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 13:04 IST
Initiating Ping Scan at 13:04
Scanning www.geeksforgeeks.com (199.59.243.222) [3 ports]
Completed Ping Scan at 13:04, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:04
Completed Parallel DNS resolution of 1 host. at 13:04, 0.41s elapsed
Initiating SYN Stealth Scan at 13:04
Scanning www.geeksforgeeks.com (199.59.243.222) [1000 ports]
Discovered open port 443/tcp on 199.59.243.222
Discovered open port 80/tcp on 199.59.243.222
Completed SYN Stealth Scan at 13:04, 4.56s elapsed (1000 total ports)
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0073s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
t3r

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.21 seconds
    Raw packets sent: 2003 (88.076KB) | Rcvd: 5 (236B)
```

- **ARP Ping:** ARP ping scan is used to discover the host devices in the same network. sometimes it will not visible due to [firewall](#) filtering.

nmap -PR www.geeksforgeeks.com

```
pdfparser pentestlab
└─(root㉿kali)-[~/home/kali]
└─# nmap -PR www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 13:20 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0062s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 23.55 seconds
```

- **Traceroute:** Traceroute helps to discover the following hops or pathways to the targeted host.

nmap -sn -traceroute www.geeksforgeeks.com

```
root@kali: /home/kali
└# nmap -sn --traceroute www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 13:27 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0069s latency).

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1  1.82 ms   192.168.1.1
2  10.54 ms  223.177.143.255
3  9.04 ms   122.186.81.173
4  6.70 ms   116.119.42.213
5  7.64 ms   99.83.64.164
6  8.19 ms   150.222.217.64
7  ...
8  4.95 ms   150.222.217.210
9  3.85 ms   150.222.217.93
10 ...
11 7.77 ms   150.222.255.45
12 public...
13 12.22 ms  52.93.116.142
14 7.05 ms   199.59.243.222

Nmap done: 1 IP address (1 host up) scanned in 16.45 seconds
```

Experiment- 3

OpenVAS, short for Open Vulnerability Assessment System, is an open-source network security scanner and vulnerability management tool. It is designed to identify and assess potential security vulnerabilities in computer systems, networks, and applications. OpenVAS helps organizations detect and mitigate security risks by scanning their infrastructure for known vulnerabilities and providing detailed reports on the findings.

Key features of OpenVAS include:

Vulnerability Scanning: OpenVAS scans target systems to identify security vulnerabilities, including software vulnerabilities, misconfigurations, and potential weaknesses that could be exploited by attackers.

Regular Updates: OpenVAS uses a regularly updated database of known vulnerabilities and checks for the latest security threats. This ensures that it can identify even the most recent vulnerabilities.

Customizable Scans: Users can configure and customize scans based on their specific requirements, including the choice of scan targets, scan timing, and the types of vulnerabilities to look for.

Reporting: OpenVAS provides comprehensive reports on scan results, including details about identified vulnerabilities, severity levels, and recommendations for remediation. These reports can be valuable for security teams and system administrators.

Integration: OpenVAS can be integrated into other security tools and processes to streamline vulnerability management and remediation efforts. It supports various formats for exporting scan results, making it compatible with other security software.

Web-based Interface: OpenVAS offers a web-based interface that allows users to manage and configure scans, view scan results, and generate reports through a user-friendly dashboard.

Scalability: OpenVAS is suitable for both small and large organizations and can be scaled to meet the needs of complex network infrastructures.

OpenVAS is widely used by security professionals, system administrators, and organizations to proactively identify and address security vulnerabilities in their IT environments. It is known for its effectiveness in helping organizations maintain the security of their systems and networks by providing insights into potential risks that need to be addressed promptly.

Installing Openvas on Kali Linux

To install Openvas and its dependencies on our Kali Linux system run the following command:

```
sudo apt update  
sudo apt upgrade -y  
sudo apt dist-upgrade -y
```

sudo apt install openvas

The next step is to run the installer, which will configure OpenVAS and download various network vulnerability tests (NVT) or signatures. Due to a large number of NVTs (50.000+), the setting process may take some time and consume a lot of data. In the test setup we used for this tutorial, the complete setup process took 10 minutes, which is not bad.

Run the following command to start the setup process:

```
gvm-setup
```

```
phantom@kali:~  
File Actions Edit View Help  
[>] Creating database  
CREATE ROLE  
GRANT ROLE  
CREATE EXTENSION  
CREATE EXTENSION  
[>] Migrating database  
[>] Checking for admin user  
[*] Creating user admin for gvm  
[*] Please note the generated admin password:  
[*] User created with password 'c273c26d-28d3-485b-9865-5c96e30acf6d'.  
[*] Define Feed Import Owner  
[>] Updating OpenVAS feeds  
[*] Updating: NVT  
Greenbone community feed server - http://feed.community.greenbone.net/  
This service is hosted by Greenbone Networks - http://www.greenbone.net/  
All transactions are logged.  
If you have any questions, please use the Greenbone community portal.  
See https://community.greenbone.net for details.  
By using this service you agree to our terms and conditions.  
Only one sync per time, otherwise the source ip will be temporarily blocked.  
/
```

```
phantom@kali:~  
File Actions Edit View Help  
dfn-cert-2019.xml  
    3,549,005 100% 367.22kB/s 0:00:09 (xfr#22, to-chk=6/29)  
dfn-cert-2020.xml  
    3,659,131 100% 363.89kB/s 0:00:09 (xfr#23, to-chk=5/29)  
dfn-cert-2021.xml  
    1,749,636 100% 374.37kB/s 0:00:04 (xfr#24, to-chk=4/29)  
sha1sums  
    1,419 100% 3.99kB/s 0:00:00 (xfr#25, to-chk=3/29)  
sha256sums  
    2,019 100% 5.68kB/s 0:00:00 (xfr#26, to-chk=2/29)  
sha256sums.asc  
    819 100% 1.78kB/s 0:00:00 (xfr#27, to-chk=1/29)  
timestamp  
    13 100% 0.03kB/s 0:00:00 (xfr#28, to-chk=0/29)  
  
sent 711 bytes received 76,459,880 bytes 403,485.97 bytes/sec  
total size is 76,439,315 speedup is 1.00  
[*] Checking Default scanner  
08b69003-5fc2-4037-a479-93b440211c73 OpenVAS /var/run/ospd/ospd.sock 0 OpenVAS Default  
[*] Done  
[*] Please note the password for the admin user  
[*] User created with password 'c273c26d-28d3-485b-9865-5c96e30acf6d'.  
phantom@kali:[~]
```

After the configuration process is complete, all the necessary OpenVAS processes will start and the web interface will open automatically. The web interface is running locally on port 9392 and can be accessed through <https://localhost:9392>.

OpenVAS will also set up an admin account and automatically generate a password for this account which is displayed in the last section of the setup output:

Verify the Installation

You can verify your installation with.

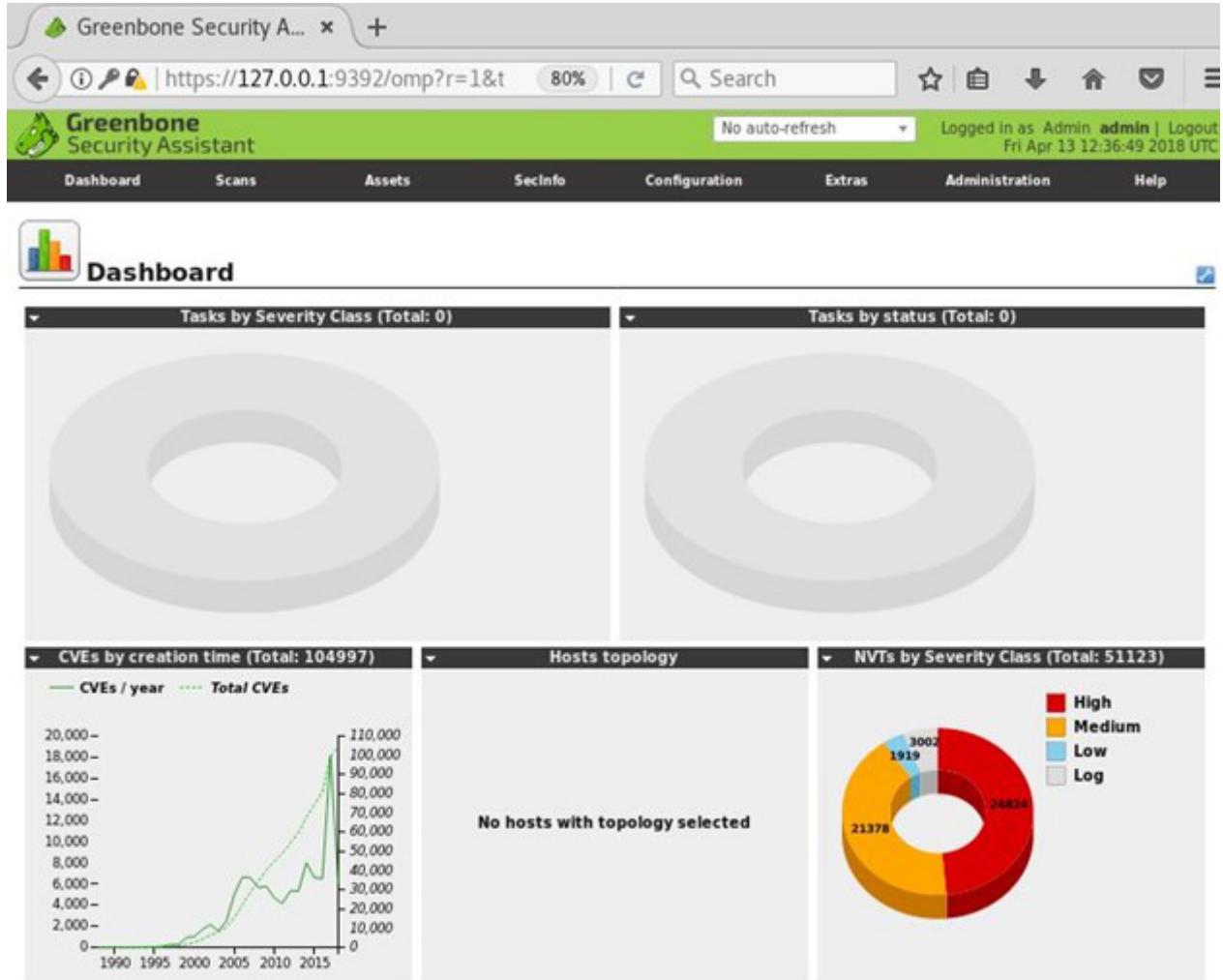
gvm-check-setup

Password reset

Did you forget to note down the password? You can change the admin password using the following commands:

gvmd --user=admin --new-password=passwd;

The next step is to accept the self-signed certificate warning and use the automatically generated admin credentials to login on to the web interface:



Starting and stopping OpenVAS

Before starting to install the virtual appliance, the last step I have to consider is to start and stop the OpenVAS service. OpenVAS services consume a lot of unnecessary resources, so it is recommended that you disable these services when you are not using OpenVAS.

Run the following command to start the services:

Sudo gvm-start

```
(phantom㉿kali)-[~]
$ sudo gvm-start
[sudo] password for phantom:
[-] Something is already using port: 9392/tcp
COMMAND PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
gsad  861 _gvm  10u  IPv4  17527      0t0  TCP localhost:9392 (LISTEN)

UID  siations w PID  re PPID C STIME TTY      STAT   TIME CMD
_gvm     861        1  0 14:02 ?
               861           1  0 14:02 ?          Sl    0:00 /usr/sbin/gsad --listen=127.0.0.1 --port=9392
Install the new version.

(phantom㉿kali)-[~]
$
```

To stop the OpenVAS services again, run:

sudo gvm-stop

```
phantom@kali: ~
File Actions Edit View Help
(phantom@kali)~]
$ sudo gvm-stop
[sudo] password for phantom:
[>] Stopping OpenVAS services
● greenbone-security-assistant.service - Greenbone Security Assistant (gsad)
   Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; enabled; vendor preset: disabled)
     Active: inactive (dead) since Sat 2021-06-26 14:23:35 EDT; 505ms ago
       Docs: man:gsad(8)
          https://www.greenbone.net
      Process: 834 ExecStart=/usr/sbin/gsad --listen=127.0.0.1 --port=9392 (code=exited, status=0/SUCCESS)
   Main PID: 836 (code=killed, signal=TERM)
     CPU: 17ms

Jun 26 14:22:22 kali systemd[1]: Starting Greenbone Security Assistant (gsad) ...
Jun 26 14:22:22 kali gsad[834]: Oops, secure memory pool already initialized
Jun 26 14:22:22 kali systemd[1]: Started Greenbone Security Assistant (gsad).
Jun 26 14:23:35 kali systemd[1]: Stopping Greenbone Security Assistant (gsad) ...
Jun 26 14:23:35 kali systemd[1]: greenbone-security-assistant.service: Succeeded.
Jun 26 14:23:35 kali systemd[1]: Stopped Greenbone Security Assistant (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
   Loaded: loaded (/lib/systemd/system/gvmd.service; enabled; vendor preset: disabled)
     Active: inactive (dead) since Sat 2021-06-26 14:23:35 EDT; 547ms ago
       Docs: man:gvmd(8)
      Process: 812 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock (code=exited, status=0/SUCCESS)
   Main PID: 813 (code=killed, signal=TERM)
     CPU: 600ms

Jun 26 14:22:21 kali systemd[1]: Starting Greenbone Vulnerability Manager daemon (gvmd) ...
```

*Note: To create a new user :

sudo runuser -u _gvm -- gvmd --create-user=admin2 --new-password=12345

To change the password of the existing user:

**sudo runuser -u _gvm -- gvmd --user=admin
--new-password=new_password**

Perform Vulnerability Scanning using OpenVAS.

In the Terminal window, type the following and press Enter:

```
sudo /usr/bin/gvm-feed-update
```

Executing this command will update the Greenbone database.

This process will take up to 15 minutes to complete.

Type the following in the **Terminal** window and press Enter:

```
sudo gvm-start
```

The **Firefox** browser will open automatically.

Click **Advanced**.

Scroll down and click **Accept the Risk and Continue**.

The **Greenbone Security Assistant** login page is displayed.

Type the credentials in the Username and Password text box and click **Login**.

The dashboard for OpenVAS is displayed.

Click **Scans** and select **Tasks**.

The **Tasks** page is displayed. Click **Task Wizard** on the upper left side – just below the menu.

In the **Task Wizard** pop-up window, enter the following in the **IP address or hostname** field:

```
192.168.0.4
```

Click **Start Scan**

Wait for the scan to complete. This may take up to 10 minutes.

On **Task 1 of 1**, click **1** in the **Reports** field.

Click the entry in the **Date** field.

Select the **Results** field on the **Immediate scan of IP 192.168.0.4** task results window.

Select **Ports** on the **Immediate scan of IP 192.168.0.4** task results window.

In the **Ports** field, the open ports of the scanned host are displayed.

Select **Operating Systems** on the **Task** window.

The scanned host's operating system is identified as Microsoft Windows. Several other fields of information gathered from the scanned host can b

Aim: Vulnerability Scanning using with Nessus

DESCRIPTION:

Nessus

Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. This article will focus on this vulnerability scanner, discussing the fundamentals that one needs to have before getting started with the tool, the different scanning capabilities that it provides, what it takes to run the tool and how results appear once scans are complete.

Vulnerability scanning with Nessus

Nessus performs its scans by utilizing plugins, which run against each host on the network in order to identify vulnerabilities. Plugins can be thought of as individual pieces of code that Nessus uses to conduct individual scan types on targets. Plugins are numerous and wide in their capabilities. For instance, a plugin could be launched and targeted at a host to:

- 1) Identify which operating systems and services are running on which ports
- 2) Identify which software components are vulnerable to attacks (FTP, SSH, SMB and more)
- 3) Identify if compliance requirements are met on various hosts

When you launch a scan, Nessus goes through a series of steps.

Step 1: Nessus will retrieve the scan settings. The settings will define the ports to be scanned, the plugins to be enabled and policy preferences definitions.

Step 2: Nessus will then perform host discovery to determine the hosts that are up. The protocols used in host

discovery will be ICMP, TCP, UDP and ARP. You can specify these per your desires.

Step 3: Nessus then performs a port scan of each host that is discovered to be up. You can also define which

ports you will want to be scanned. Ports can be defined in ranges or individually, with valid ports ranging from

1 to 65535.

Step 4: Nessus will then perform service detection to determine the services that are running behind each port

on each host discovered

Step 5: Nessus then performs operating system detection.

Step 6: Once all the steps are complete, Nessus runs each host against a database of known vulnerabilities in an

attempt to discover which host contains which vulnerabilities.

Experiment -5

Aim : To perform internal penetration testing – Mapping, Scanning, Gaining Access through CVE's, Sniffing POP3/FTP/Telnet passwords, ARP Poisoning , DNS poisoning

Description:

1. Mapping:

During the mapping phase, pen testers gain better insight into the most exposed and critical elements of an organization's infrastructure. This particular phase is essential, especially if you are looking at vulnerabilities within the entire framework, rather than just one particular aspect (such as, say, guest wi-fi).

Installing Nmap

To install Nmap on Red Hat Enterprise Linux 8 or Fedora, you'd run:

```
# dnf -y install nmap
```

Substitute dnf for yum if you are on Red Hat Enterprise Linux 7 or newer. After installing Nmap, you can run the nmap command without arguments to display all of its options. You also should consult the Nmap man page by running man nmap.

Using Nmap

Let's assume your local network is 192.168.0.0/24, and you want to run a scan on this network. Running a scan without any argument except the network address yields the following:

```
# nmap 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-06 21:00 CET
Nmap scan report for Archer.lan (192.168.0.1)
Host is up (0.0046s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1900/tcp  open  upnp
20005/tcp open  btx
MAC Address: 50:ff:BF:ff:AC (Tp-link Technologies)
```

```
Nmap scan report for Lyric-1111C2.lan (192.168.0.101)
Host is up (0.013s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE0
```

80/tcp open http

MAC Address: B8:dd:A0:dd:dd:C2 (Resideo)

Multiple networks can be scanned at once. For example

nmap 192.168.0.0/24 10.80.0.0/24

Multiple networks can be scanned at once.

For example:

nmap 192.168.0.0/24 10.80.0.0/24

If we want to run a quick scan of machines in our network without trying to see if any port is open, we run:

nmap -sn 192.168.0.0/24

The output of the above command produces something like:

nmap -sn 192.168.0.0/24

Starting Nmap 7.80 (https://nmap.org) at 2020-03-06 21:24 CET

Nmap scan report for Archer.lan (192.168.0.1)

Host is up (0.016s latency).

MAC Address: 50:C7:FF:FF:15:FF (Tp-link Technologies)

Nmap scan report for Lyric-1111C2.lan (192.168.0.101)

Host is up (0.96s latency).

MAC Address: B8:FF:FF:11:FF:C2 (Resideo)

MAC Address: 88:DD:EA:DD:CE:37 (Texas Instruments)

Nmap scan report for SoundTouch-Kitchen.lan (192.168.0.160)

Host is up (0.39s latency).

MAC Address: 5C:DD:DD:FF:FF:B5 (Texas Instruments)

Nmap scan report for 192.168.0.181

Host is up (0.60s latency).

MAC Address: 40:DD:DD:8F:FF:F5 (Asustek Computer)

Nmap scan report for TL-WPA4220.lan (192.168.0.225)

Host is up (0.61s latency).

MAC Address: 50:DD:FF:AA:DD:BA (Tp-link Technologies)

Nmap scan report for f3d0r4.lan (192.168.0.165)

Host is up.

Nmap done: 256 IP addresses (7 hosts up) scanned in 9.11 seconds

Mind you that -sn was known as -sP in the previous versions of Nmap. The use of -sP is still backward compatible and should work in the recent versions of Nmap.

So running:

nmap -sn 192.168.0.0/24 -oG nmap_output

produces the following output:

cat nmap_output

Nmap 7.80 scan initiated Fri Mar 6 22:01:57 2020 as: nmap -sn -oG nmap_output 192.168.0.0/24

Host: 192.168.0.1 (Archer.lan) Status: Up

Host: 192.168.0.101 (Lyric-1111C2.lan) Status: Up

Host: 192.168.0.151 (SoundTouch-VW-benee.lan) Status: Up

Host: 192.168.0.160 (SoundTouch-VW-keuken.lan) Status: Up

```
Host: 192.168.0.181 ()      Status: Up
Host: 192.168.0.225 (TL-WPA4220.lan)    Status: Up
Host: 192.168.0.165 (f3d0r4.lan)      Status: Up
# Nmap done at Fri Mar   6 22:02:06 2020 -- 256 IP addresses (7 hosts up)
scanned in 9.45 seconds
```

2. Scanning specific ports:

Nmap has the option to scan specific ports on specific targets. If we were interested in checking the state of ports 22 and 443 (which by default use the TCP protocol), we'd run the following:

```
# nmap -sV -p 22,443 192.168.0.0/24
```

If you are unsure what -sV does, just run:

```
# nmap | grep -- -sV
```

The above command displays the ports regardless of their state: open, closed, filtered, etc. Most of the time, we're interested in open ports, and so we can add the -open flag to achieve this. We'll slightly modify the above command and run:

```
# nmap -sV -p 22,443 192.168.0.0/24 -open
```

Instead of using a comma to specify a port, it is also possible to use a range of ports, which is much more flexible and easier to read. For example:

```
# nmap -p 54-111 192.168.0.0/2
```

3. Gaining Access through CVE's

The nmap command-line to scan for CVE-2017-0143 (EternalBlue) is the following:
nmap.exe -Pn -p445 --open --max-hostgroup 3 --script smb-vuln-ms17-010 -oN ms17-010 192.168.1.17

The command-line options that we specify mean the following:

-Pn: Treat all hosts as online -- skip host discovery

-p445: This indicates the port that we want to scan. Here we only scan port 445 which is the smb file sharing port.

--script smb-vuln-ms17-010: This indicates that the MS17-010 script should be executed on every found open port.

-oN ms17-010: Output scan in normal format to the given filename (in this case the filename will be ms17-010.nmap)

192.168.1.17: This indicates the machine to scan.

--open: Only show open (or possibly open) ports.

--max-hostgroup 3: Parallel host scan group size is set to 3. It has been found that this is the ideal setting when using this script.

If nmap detects that a machine is vulnerable for CVE-2017-0143 (EternalBlue), then the output will look as follows:

```
C:\Tools\nmap-7.50>nmap.exe -Pn -p445 --open --max-hostgroup 3 --script smb-vuln-ms17-010 192.168.1.17
```

Starting Nmap 7.50 (https://nmap.org) at 2017-07-01 10:00 Romance Summer Time

Nmap scan report for 192.168.1.17

Host is up (0.22s latency).

PORt STATE SERVICE
445/tcp open microsoft-ds

Host script results:

| smb-vuln-ms17-010:

| | VULNERABLE:

| | | Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

| | | State: VULNERABLE

| | | IDs: CVE:CVE-2017-0143

| | | Risk factor: HIGH

| | | A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).

| | | Disclosure date: 2017-03-14

| | | References:

| | | https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

| | | https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

| | | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 10.82 seconds

If nmap detects that a machine is not vulnerable for CVE-2017-0143 (EternalBlue), then the output will look as follows:

```
C:\Tools\nmap-7.50>nmap.exe -Pn -p445 --open --max-hostgroup 3 --script smb-vuln-ms17-010 192.168.1.17
```

Starting Nmap 7.50 (https://nmap.org) at 2017-07-01 10:00 Romance Summer Time

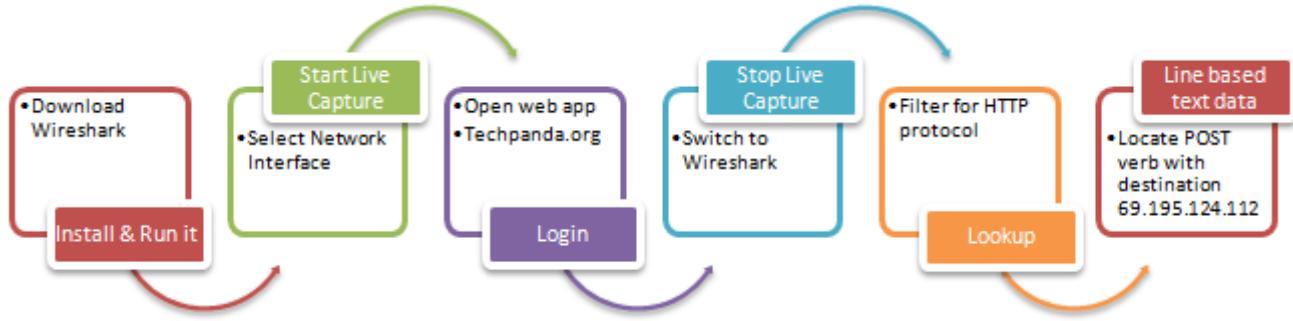
Nmap scan report for 192.168.1.17

Host is up (0.0020s latency).

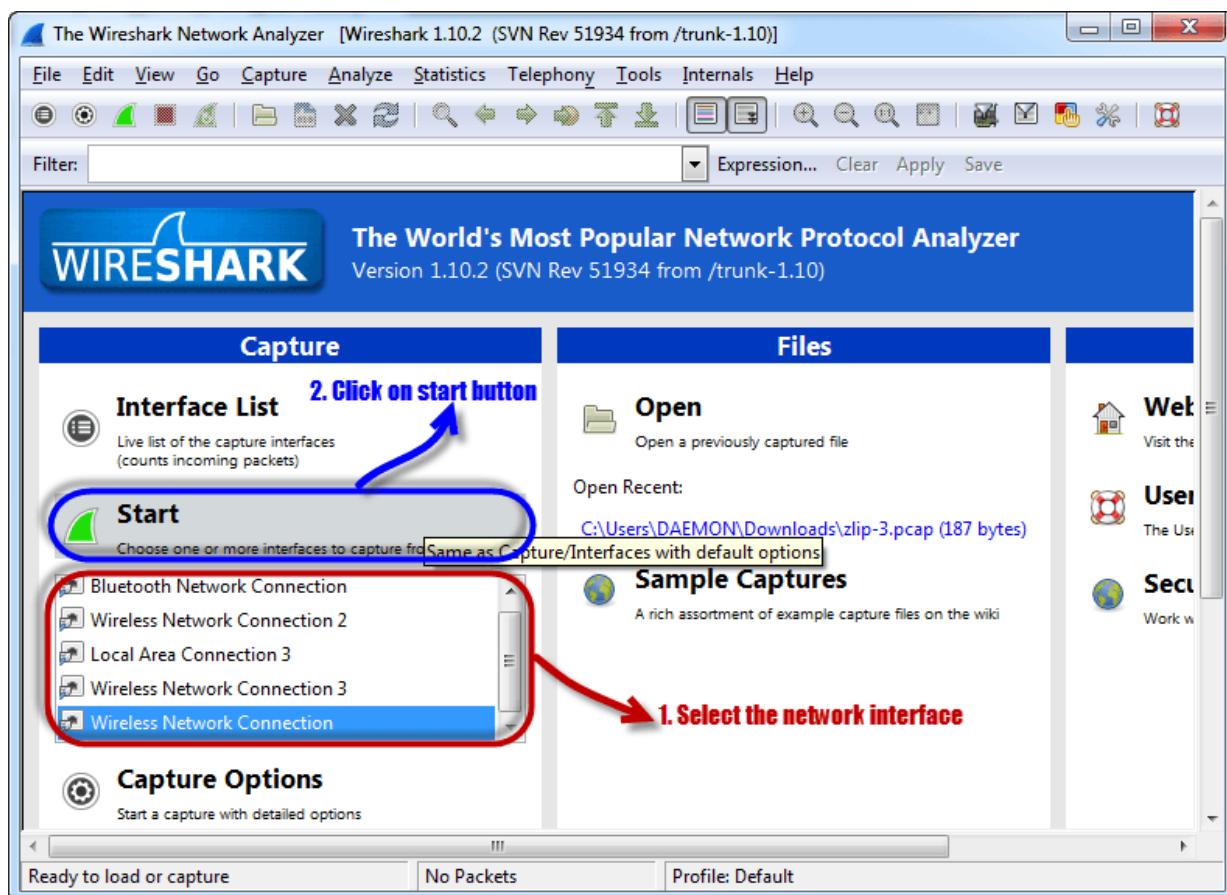
PORt STATE SERVICE
445/tcp open microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 11.00 seconds

4. Sniffing POP3/FTP/Telnet passwords:



- Open Wireshark
- You will get the following screen



- Select the network interface you want to sniff. Note for this demonstration, we are using a wireless network connection. If you are on a local area network, then you should select the local area network interface.
- Click on start button as shown above

Capturing from Wireless Network Connection [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Stop the running live capture

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
539	38.6764890	192.168.43.42	69.21.135.64	UDP	62	Source port: 28409 Desti
540	38.7158980	69.21.135.64	192.168.43.42	UDP	1466	Source port: 12846 Desti
541	38.7166550	192.168.43.42	69.21.135.64	UDP	62	Source port: 28409 Desti
542	39.0935740	fe80::b889:74a:33df:ff02::1:3		LLMNR	89	Standard query 0x3eec A
543	39.0940840	192.168.43.42	224.0.0.252	LLMNR	69	Standard query 0x3eec A
544	39.1860910	69.21.135.64	192.168.43.42	UDP	1466	Source port: 12846 Desti
545	39.1863260	192.168.43.42	69.21.135.64	UDP	62	Source port: 28409 Desti
546	39.1938200	fe80::b889:74a:33df:ff02::1:3		LLMNR	89	Standard query 0x3eec A
547	39.1940520	192.168.43.42	224.0.0.252	LLMNR	69	Standard query 0x3eec A
548	39.3950270	192.168.43.42	192.168.43.255	NBNS	92	Name query NB DAEMON-PC<0
549	39.5278640	192.168.43.42	85.74.22.253	UDP	94	Source port: 49521 Desti
550	40.1447820	192.168.43.42	192.168.43.255	NBNS	92	Name query NB DAEMON-PC<0
551	40.8948090	192.168.43.42	192.168.43.255	NBNS	92	Name query NB DAEMON-PC<0
552	41.3883420	192.168.43.42	192.168.43.1	DNS	84	Standard query 0x7037 A
553	41.4232860	192.168.43.42	85.74.22.253	TCP	66	57807 > 26339 [SYN] Seq=0
554	41.5278740	192.168.43.42	85.74.22.253	UDP	94	Source port: 49521 Desti

Frame 1: 1322 bytes on wire (10576 bits), 1322 bytes captured (10576 bits) on interface 0

Ethernet II, Src: SamsungE_51:12:f3 (10:d5:42:51:12:f3), Dst: IntelCor_a6:c5:43 (60:36:dd:a6)

0000 60 36 dd a6 c5 43 10 d5 42 51 12 f3 08 00 45 00 `6...C.. BQ....E.
0010 05 1c 7b 70 00 00 71 11 71 47 55 4a 16 fd c0 a8 ..{p..q. qGUJ....
0020 2b 2a f6 e7 c1 71 05 08 73 fb 60 00 00 00 04 d8 +*...q.. S.
0030 11 80 20 01 00 00 9d 38 78 cf 24 ec 09 18 aa b58 x. \$....
0040 e9 02 20 01 00 00 5e f5 79 fb 2c 55 3e 8e 3a 44^ y., U>.:D
0050 61 cd 66 c2 60 fo o1 d8 ab 17 01 00 b7 2d 9c o2 A f n

Wireless Network Connection: <live capture i... Packets: 554 Disp... Profile: Default

- Open your web browser and type in <http://www.techpanda.org/>

Login | Personal Contacts x

← → C ⌂ www.techpanda.org/index.php ⌂ Share Media Torrent ⌂ ⌂ ⌂

Login | Personal Contacts Manager v1.0

Email*

Password*

Remember me

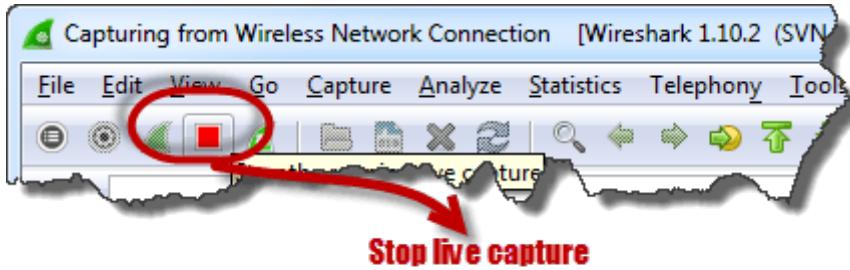
- The login email is **admin@google.com** and the password is **Password2010**
- Click on submit button

- A successful logon should give you the following dashboard

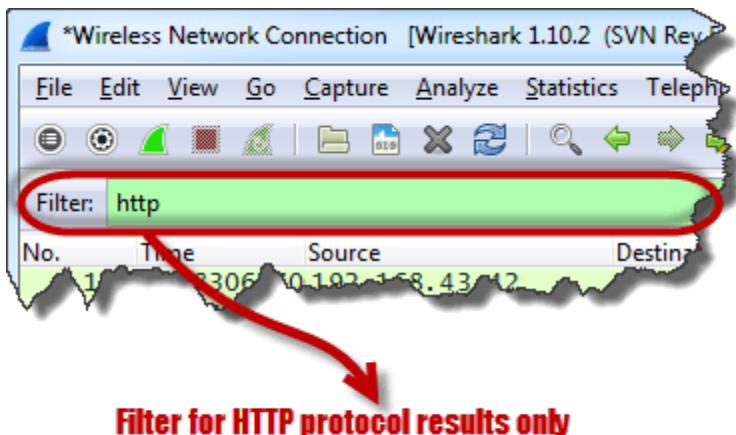
ID	First Name	Last Name	Mobile No	Email	Actions
1	Roderick	Chekoko	9990986	kr@kr.com	Edit
2	Martin	Dawn	111	d@mar.com	Edit
3	Fernie	Ngoma	555	fngoma@yahoo.com	Edit
5	Melody	Kalinda	0758076112	kamel@gmail.com	Edit
6	Smith	Jones	09875465456	sjones@space.com	Edit

Total Records Count: 5

- Go back to Wireshark and stop the live capture



- Filter for HTTP protocol results only using the filter textbox



Locate the Info column and look for entries with the HTTP verb POST and click on it

Protocol	Length	Info
HTTP	433	GET / HTTP/1.1
HTTP	1188	HTTP/1.1 200 OK (text/html)
HTTP	233	HTTP/1.1 200 OK (text/plain)
HTTP	362	GET /subscribe?host_int=74
HTTP	724	POST /index.php HTTP/1.1
HTTP	1234	HTTP/1.1 302 Moved Temporarily
HTTP	567	GET /dashboard.php HTTP/1.1
HTTP	362	[TCP Retransmission] GET /
HTTP	1322	HTTP/1.1 200 OK (text/html)

Look for POST verb under Info column

- Just below the log entries, there is a panel with a summary of captured data. Look for the summary that says Line-based text data: application/x-www-form-urlencoded

*Wireless Network Connection [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
172	10.8306270	192.168.43.42	69.195.124.112	HTTP	433	GET / HTTP/1.1
188	11.6480510	69.195.124.112	192.168.43.42	HTTP	1188	HTTP/1.1 200 OK (text/html)
325	23.5363370	108.160.162.52	192.168.43.42	HTTP	233	HTTP/1.1 200 OK (text/plain)
326	23.5481440	192.168.43.42	108.160.162.52	HTTP	362	GET /subscribe?host_int=74
384	26.8239240	192.168.43.42	69.195.124.112	HTTP	724	POST /index.php HTTP/1.1
400	27.7500490	69.195.124.112	192.168.43.42	HTTP	1234	HTTP/1.1 302 Moved Temporarily
402	27.7534960	192.168.43.42	69.195.124.112	HTTP	567	GET /dashboard.php HTTP/1.1
424	28.5163760	192.168.43.42	108.160.162.52	HTTP	362	[TCP Retransmission] GET /
425	28.7380900	69.195.124.112	192.168.43.42	HTTP	1322	HTTP/1.1 200 OK (text/html)

Frame 384: 724 bytes on wire (5792 bits), 724 bytes captured (5792 bits) on interface 0

Ethernet II, Src: IntelCor_a6:c5:43 (60:36:dd:a6:c5:43), Dst: Samsung_E_51:12:f3 (10:d5:42:51:1)

Internet Protocol Version 4, Src: 192.168.43.42 (192.168.43.42), Dst: 69.195.124.112 (69.195.1)

Transmission Control Protocol, Src Port: 57803 (57803), Dst Port: http (80), Seq: 1, Ack: 1, Len: 5792

Hypertext Transfer Protocol

Line-based text data: application/x-www-form-urlencoded

email=admin%40google.com&password=Password2010&remember_me=Remember+me

all POST variables have been captured in plaintext

Frame (frame), 724 bytes Packets: 666 · Disp... Profile: Default

- You should be able to view the plaintext values of all the POST variables submitted to the server via HTTP protocol.

5. ARP Poisoning:

In this exercise, we have used BetterCAP to perform ARP poisoning in LAN environment using VMware workstation in which we have installed Kali Linux and Ettercap tool to sniff the local traffic in LAN.

For this exercise, you would need the following tools –

VMware workstation

Kali Linux or Linux Operating system

Ettercap Tool

LAN connection

Note – This attack is possible in wired and wireless networks. You can perform this attack in local LAN.

Step 1 – Install the VMware workstation and install the Kali Linux operating system.

Step 2 – Login into the Kali Linux using username pass “root, toor”.

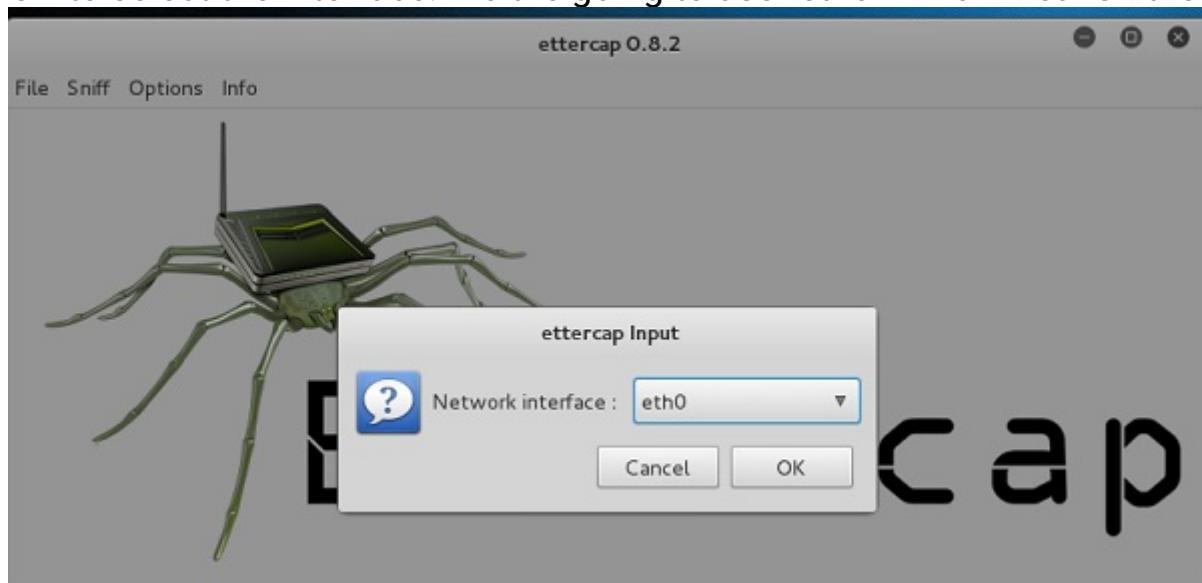
Step 3 – Make sure you are connected to local LAN and check the IP address by typing the command ifconfig in the terminal.

Ifconfig

Step 4 – Open up the terminal and type “Ettercap –G” to start the graphical version of Ettercap.

Ettercap

Step 5 – Now click the tab “sniff” in the menu bar and select “unified sniffing” and click OK to select the interface. We are going to use “eth0” which means Ethernet connection.



Ettercap Input

Step 6 – Now click the “hosts” tab in the menu bar and click “scan for hosts”. It will start scanning the whole network for the alive hosts.

IP Address	MAC Address	Description
192.168.121.1	00:50:56:C0:00:08	
192.168.121.2	00:50:56:FD:27:1D	
192.168.121.129	00:0C:29:AD:8F:25	
fe80::9040:ab7d:ee93:21fc	00:0C:29:AD:8F:25	
192.168.121.254	00:50:56:F2:40:DC	

Delete Host Add to Target 1 Add to Target 2

Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...

Step 7 – Next, click the “hosts” tab and select “hosts list” to see the number of hosts available in the network. This list also includes the default gateway address. We have to be careful when we select the targets.

Host Tab

Step 8 – Now we have to choose the targets. In MITM, our target is the host machine, and the route will be the router address to forward the traffic. In an MITM attack, the attacker intercepts the network and sniffs the packets. So, we will add the victim as “target 1” and the router address as “target 2.”

In VMware environment, the default gateway will always end with “2” because “1” is assigned to the physical machine.

Step 9 – In this scenario, our target is “192.168.121.129” and the router is “192.168.121.2”. So we will add target 1 as victim IP and target 2 as router IP.

Host 192.168.121.129 added to TARGET1

Host 192.168.121.2 added to TARGET2

Target

Step 10 – Now click on “MITM” and click “ARP poisoning”. Thereafter, check the option “Sniff remote connections” and click OK.



Mitm Attack

Step 11 – Click “start” and select “start sniffing”. This will start ARP poisoning in the network which means we have enabled our network card in “promiscuous mode” and now the local traffic can be sniffed.

Note – We have allowed only HTTP sniffing with Ettercap, so don’t expect HTTPS packets to be sniffed with this process.

Step 12 – Now it’s time to see the results; if our victim logged into some websites. You can see the results in the toolbar of Ettercap.

Result

This is how sniffing works. You must have understood how easy it is to get the HTTP credentials just by enabling ARP poisoning.

ARP Poisoning has the potential to cause huge losses in company environments. This is the place where ethical hackers are appointed to secure the networks.

Like ARP poisoning, there are other attacks such as MAC flooding, MAC spoofing, DNS poisoning, ICMP poisoning, etc. that can cause significant loss to a network.

6. DNS Poisoning:

DNS Poisoning is quite similar to ARP Poisoning. To initiate DNS poisoning, you have to start with ARP poisoning, which we have already discussed in the previous chapter. We will use DNS spoof plugin which is already there in Ettercap.

Step 1 – Open up the terminal and type “nano etter.dns”. This file contains all entries for DNS addresses which is used by Ettercap to resolve the domain name addresses. In this file, we will add a fake entry of “Facebook”. If someone wants to open Facebook, he will be redirected to another website.

```
root@kali:~# locate etter.dns
/etc/ettercap/etter.dns
root@kali:~# nano /etc/ettercap/etter.dns
```

Terminal

Step 2 – Now insert the entries under the words “Redirect it to www.linux.org”. See the following example –

```
# redirect it to www.linux.org
#
www.facebook.com    A    216.58.199.174
*.facebook.com      A    216.58.199.174
www.facebook.com    PTR   216.58.199.174
#
microsoft.com        A    107.170.40.56
*.microsoft.com      A    107.170.40.56
www.microsoft.com   PTR   107.170.40.56
# Wildcards in PTR are not allowed
```

Redirect

Step 3 – Now save this file and exit by saving the file. Use “ctrl+x” to save the file.

Step 4 – After this, the whole process is same to start ARP poisoning. After starting ARP poisoning, click on “plugins” in the menu bar and select “dns_spoof”

plugin.

Name	Version	Info
arp_cop	1.1	Report suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
* dns_spoof	1.2	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN
find_ettercap	2.0	Try to find ettercap activity
find_ip	1.0	Search an unused IP address in the subnet

Plugins

Step 5 – After activating the DNS_spoof, you will see in the results that facebook.com will start spoofed to Google IP whenever someone types it in his browser.

```
Activating dns_spoof plugin...
```

```
dns_spoof: A [staticxx.facebook.com] spoofed to [216.58.199.174]
```

```
dns_spoof: A [www.facebook.com] spoofed to [216.58.199.174]
```

```
dns_spoof: A [pixel.facebook.com] spoofed to [216.58.199.174]
```

Activating

It means the user gets the Google page instead of facebook.com on their browser.

In this exercise, we saw how network traffic can be sniffed through different tools and methods. Here a company needs an ethical hacker to provide network security to stop all these attacks. Let's see what an ethical hacker can do to prevent DNS Poisoning.

Experiment -6

Aim: To Perform Web Application Assessment with Nikto & Burpsuite

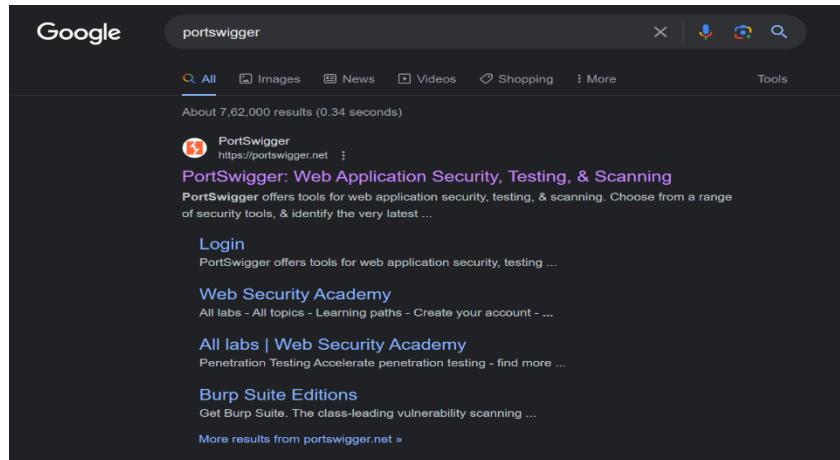
Description :

Burp Suite

Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger, which is also the alias of its founder Dafydd Stuttard. Burp Suite aims to be an all-in-one set of tools and its capabilities can be enhanced by installing add-ons that are called BApps.

It is the most popular tool among professional web app security researchers and bug bounty hunters. Its ease of use makes it a more suitable choice over free alternatives like OWASP ZAP.

Open browser -> portswigger -> click on portswigger.net ->click on products -> Burp suite community edition -> And download.



Trusted by security professionals.

Best-in-class software and learning for security engineers and penetration testers.

[FIND OUT MORE](#)

[LOGIN](#)

[Products](#) [Solutions](#) [Research](#) [Academy](#) [Support](#) [☰](#)

Burp Suite Enterprise Edition
The enterprise-enabled dynamic web vulnerability scanner.

Burp Suite Professional
The world's #1 web penetration testing toolkit.

Burp Suite Community Edition
The best manual tools to start web security testing.

Dastardly, from Burp Suite
Free, lightweight web application security scanning for CI/CD.

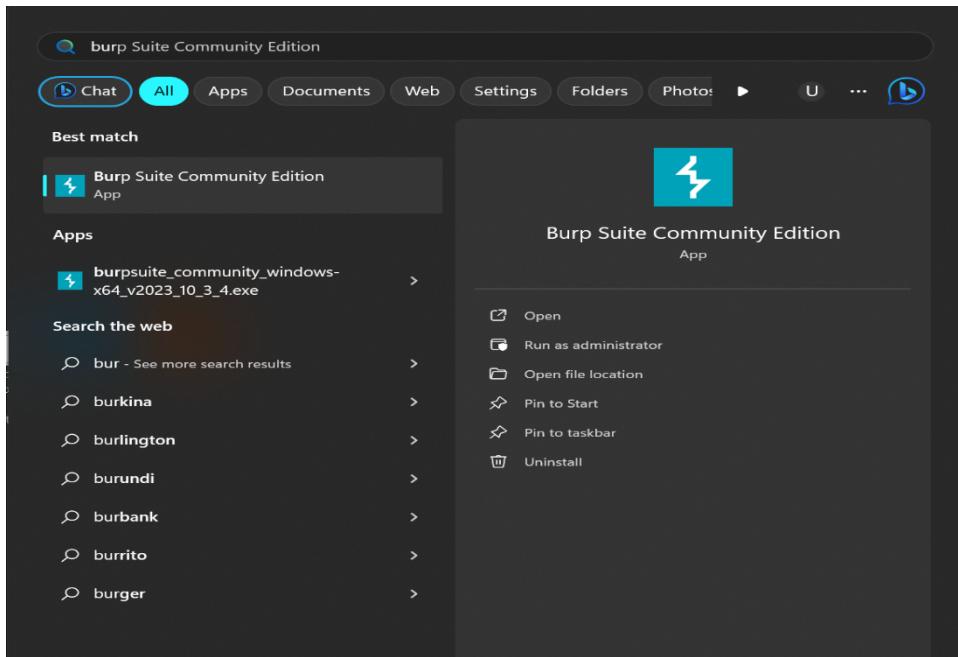
[View all product editions →](#)

[FIND OUT MORE](#)

[LOGIN](#)

Install Burp suite

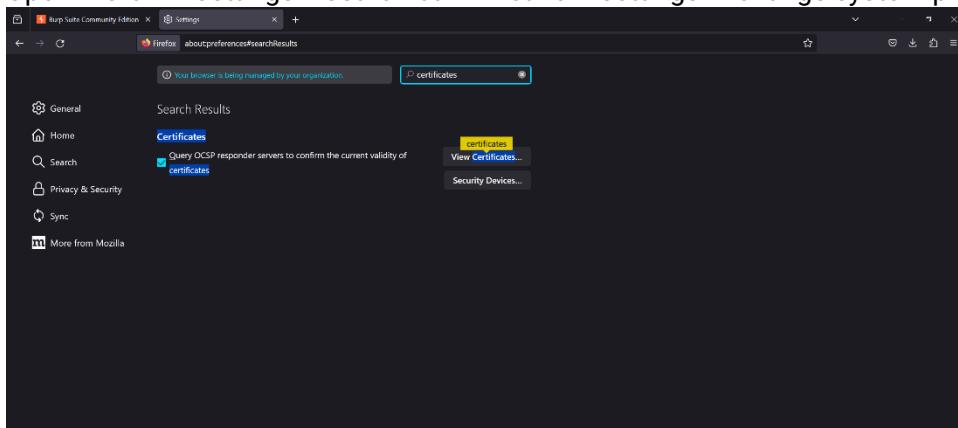
Click on Windows button and search burp suite ->Click on Next -> start burp

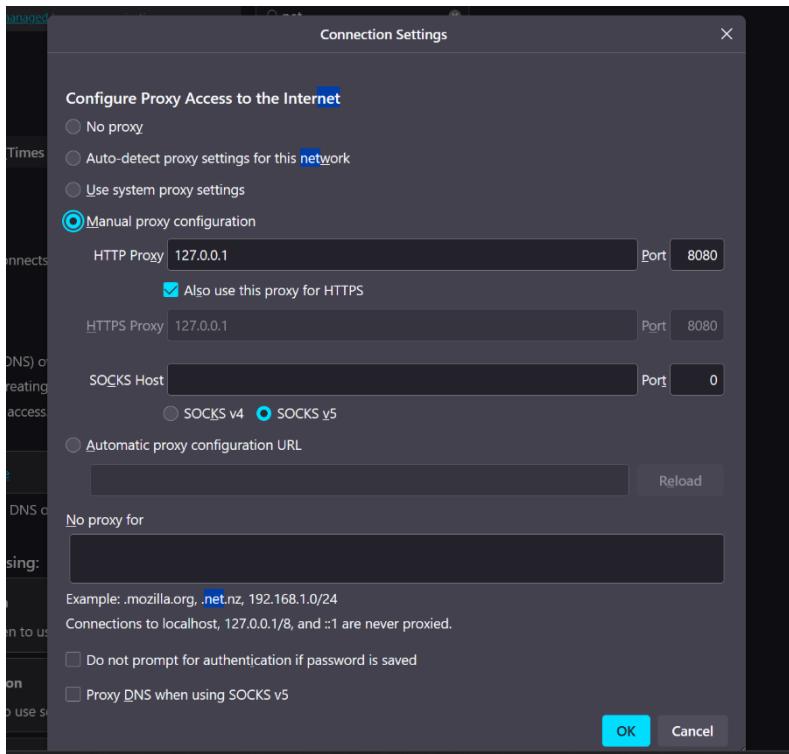


In burp suite window -> Dashboard -> Issue activity -> event log -> Targets display here

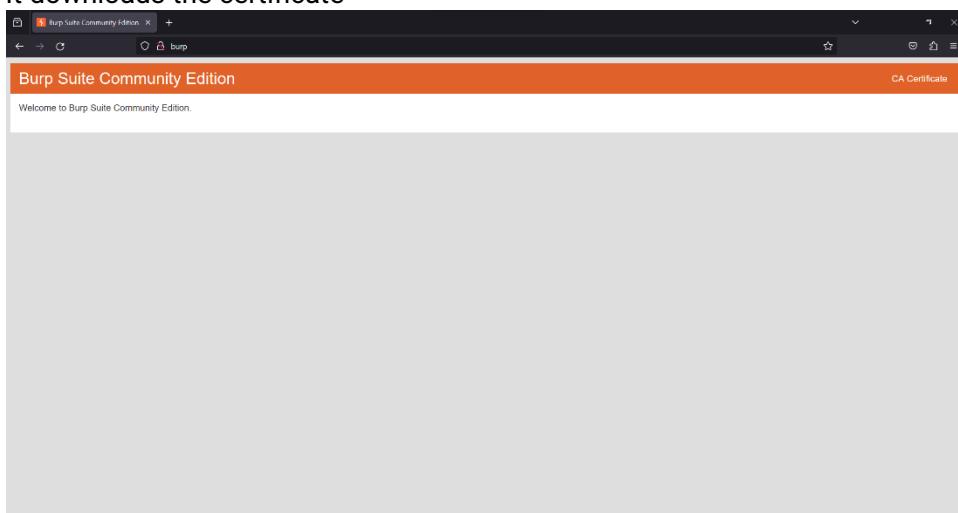
Install Mozilla firefox

Open firefox -> settings ->search bar -> network settings -> change system proxy to manual proxy

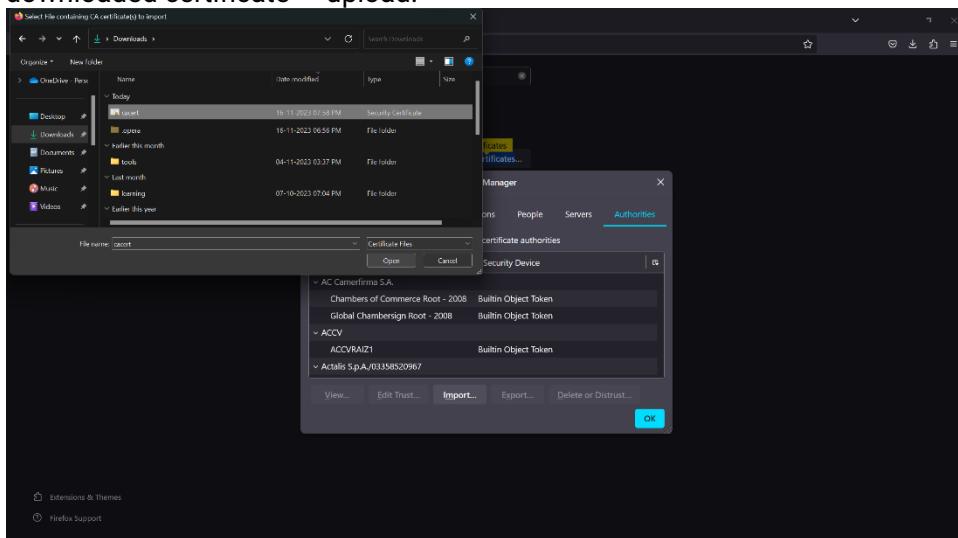




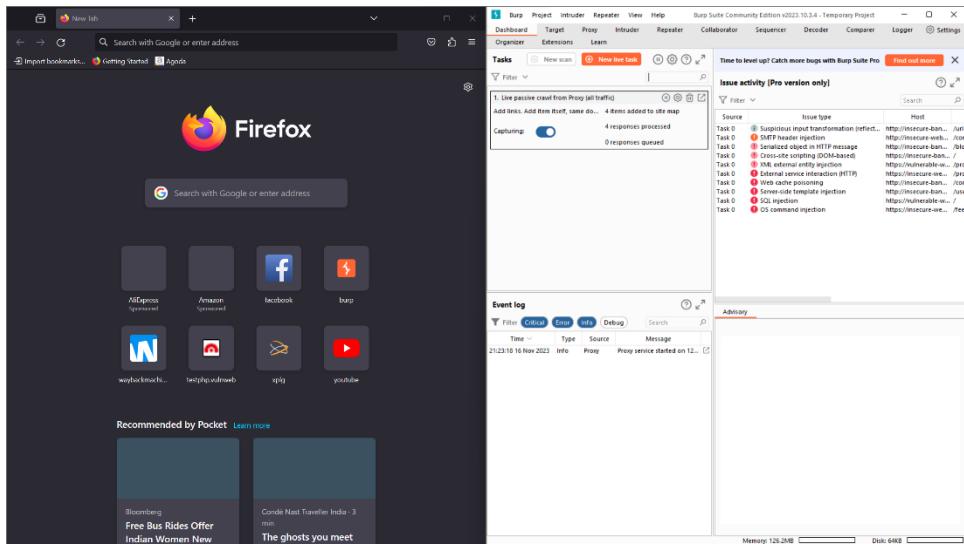
In a new tab url type <http://burp> -> press enter
 Click on CA certificate which is displayed at right top
 It downloads the certificate



Again, go back to settings -> search certificate -> click on view certificate -> authorities -> import -> select the downloaded certificate -> upload.



Open new tab and close the previous tabs and open new tab
 Place Mozilla Firefox and Burp suite on the screen



Burp suite	Mozilla Firefox
Step 1) Proxy -> intercept -> intercept off	Step 2) In url type "testphp.vulnweb.com"
Step 4) Intercept is on	Step 3) In new tab open facebook.com and enter the username and password
Step 6) It will generate all the details like site, username, password etc.,	Step 5) click on login
Step 7) turn off the intercept	Step 8) In testphp.vulnweb.com search art
Step 9) intercept is on	Click on Sign up Username: abcd Password: 1234
Step 11) It generate details and click on forward	Step 10) click on login
Display username: abcd Password:1234	
Plain text format	

Nikto:

Kali Linux is the go-to Linux distribution for users who are into pentesting and security analysis. And adding the Nikto vulnerability scanner to your security analysis tool set on Kali Linux can be achieved with just a couple of commands, as shown below.

First, refresh your APT package lists and install any pending updates:

```
# sudo apt-get update && sudo apt-get upgrade
```

Next, install the Nikto web scanner with the command:

```
# sudo apt-get install nikto -y
```

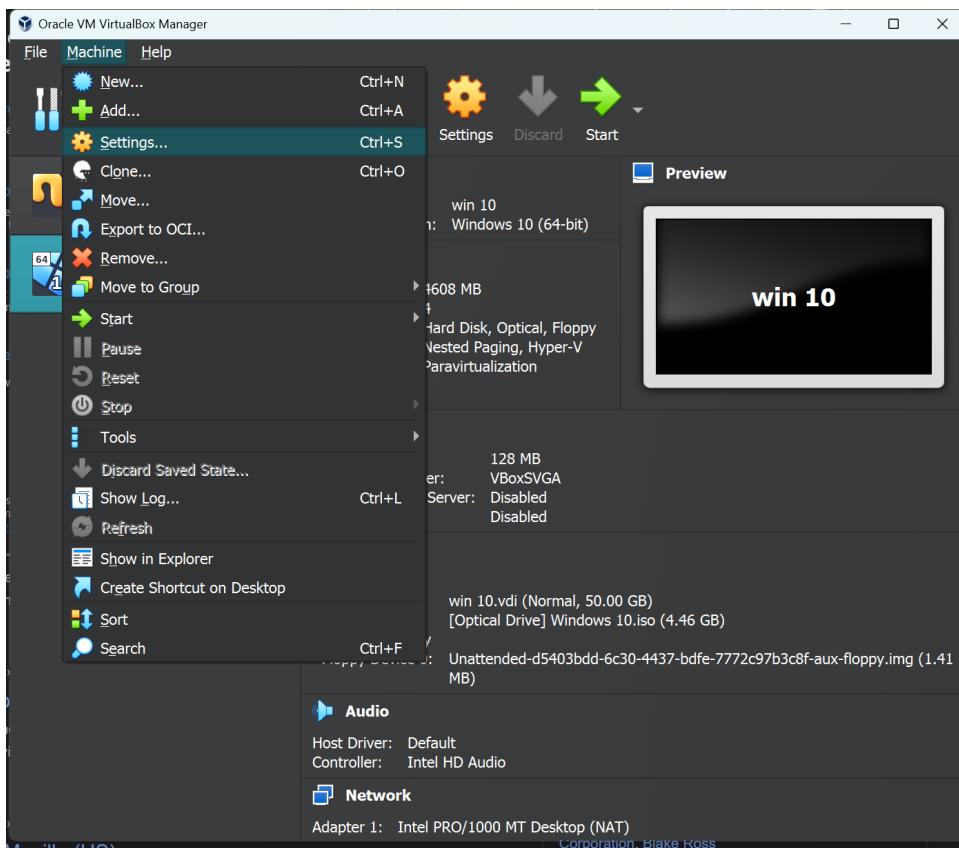
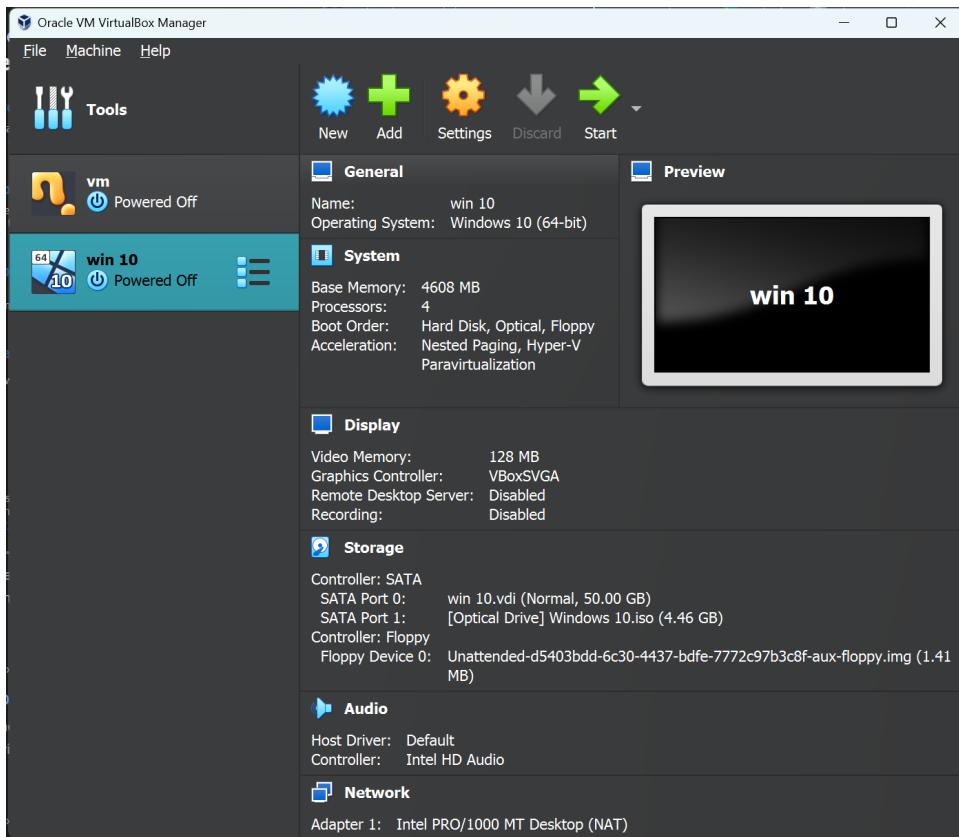
To verify that the Nikto website vulnerability scanner is installed and ready for use, run the command:

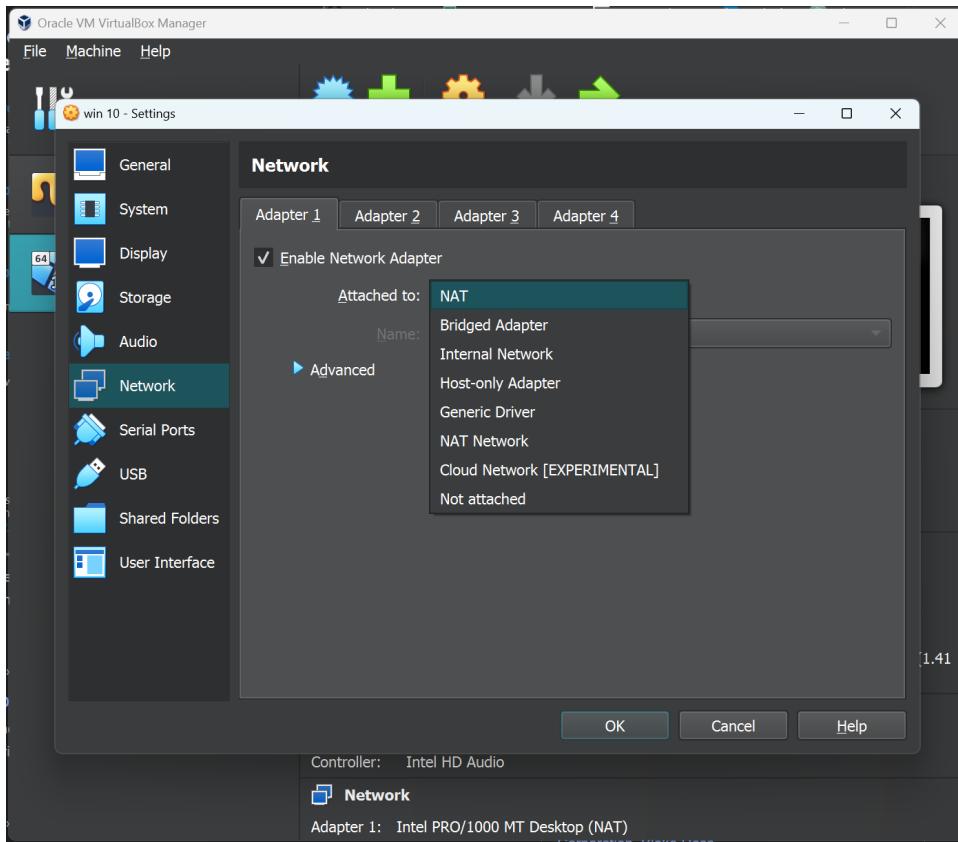
```
# nikto
```

```
~# nikto gniindia.org
```

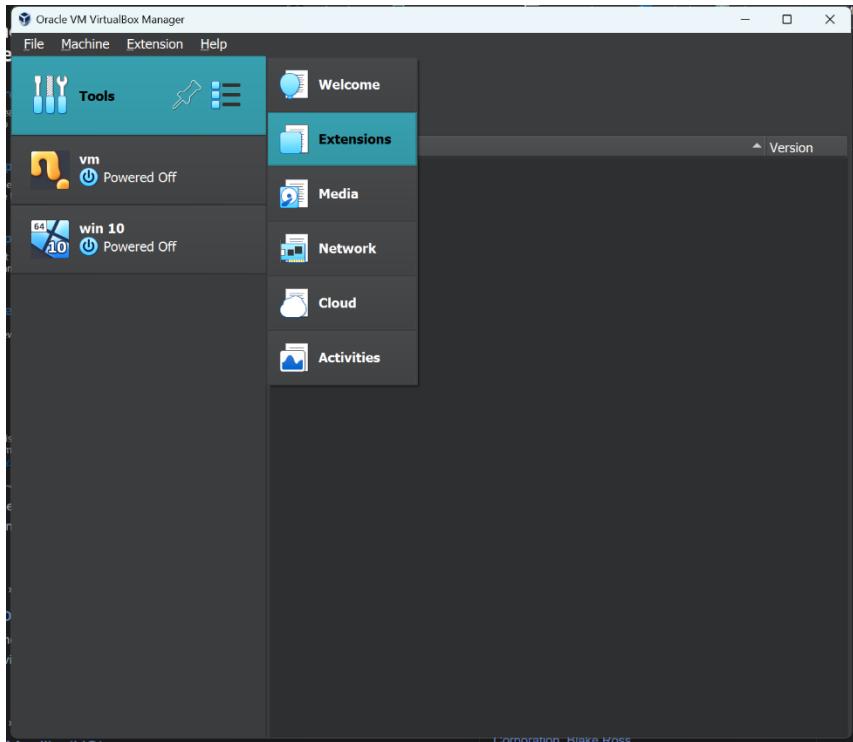
In browser -> nslookup.io -> www.gniindia.org -> find IP address

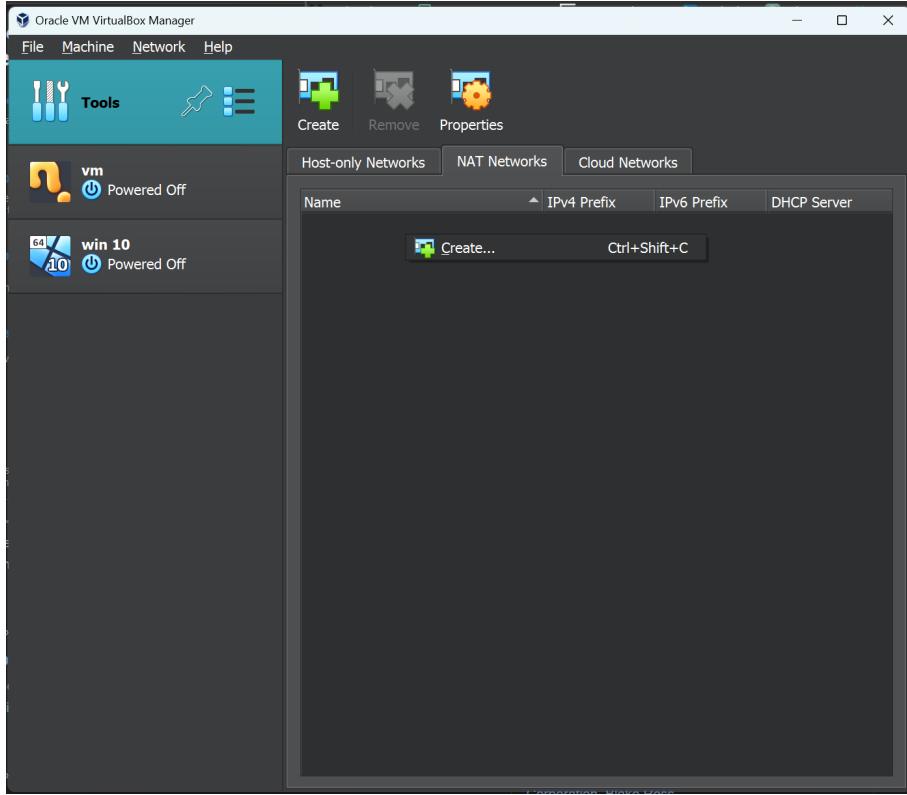
In VM virtual box -> network -> Bridge adapter -> Ok





Tools -> network -> NAT networks -> create





Bridge adapter - [Bridged Adapter is a networking mode in VirtualBox that allows the guest machine to use the physical network adapter of the host system](#)

NAT – All systems in Virtual Box work as a network

Kali Linux -> settings -> go to network tab -> attached to: NAT network

Kali Linux -> click on disconnect -> click wired connection.

After network setting in kali Linux type

```
# nikto -h testphp.vulnweb.com
```

Target IP

Target Host Name: testphp.vulnweb.com

Target port

-> all the details will be displayed

```
# nikto -h vulnweb.com
```

To find or to store it on file we use the following command

```
# nikto -h http://testphp.vulnweb.com -o scan.txt
```

In that txt file it stores the vulnerabilities, we can store o/p

```
# ls - to list the files
```

```
# cat scan.txt
```

It will display the o/p that it stored