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.

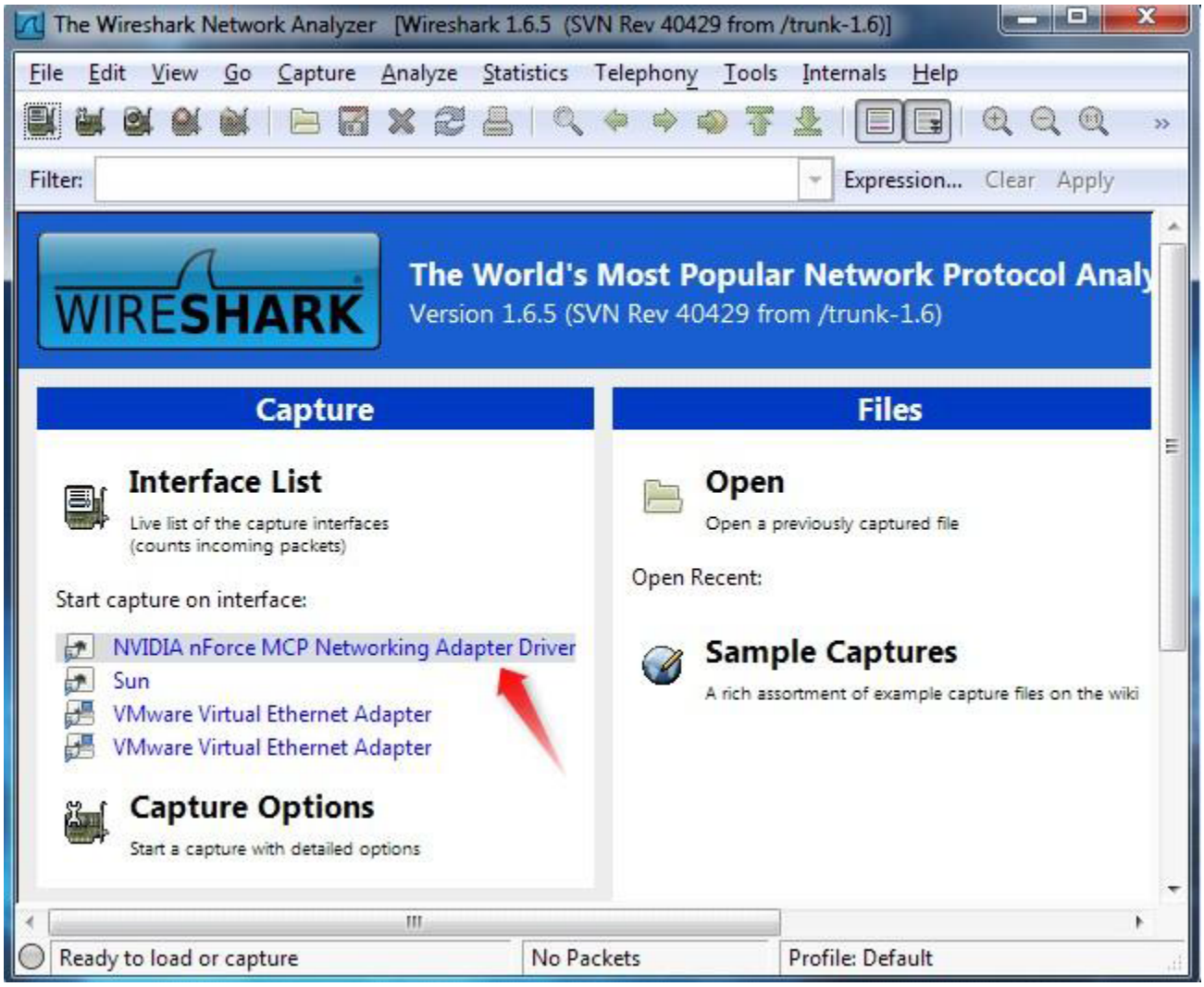
Search for packets on many criteria.

Colorize packet display based on filters.

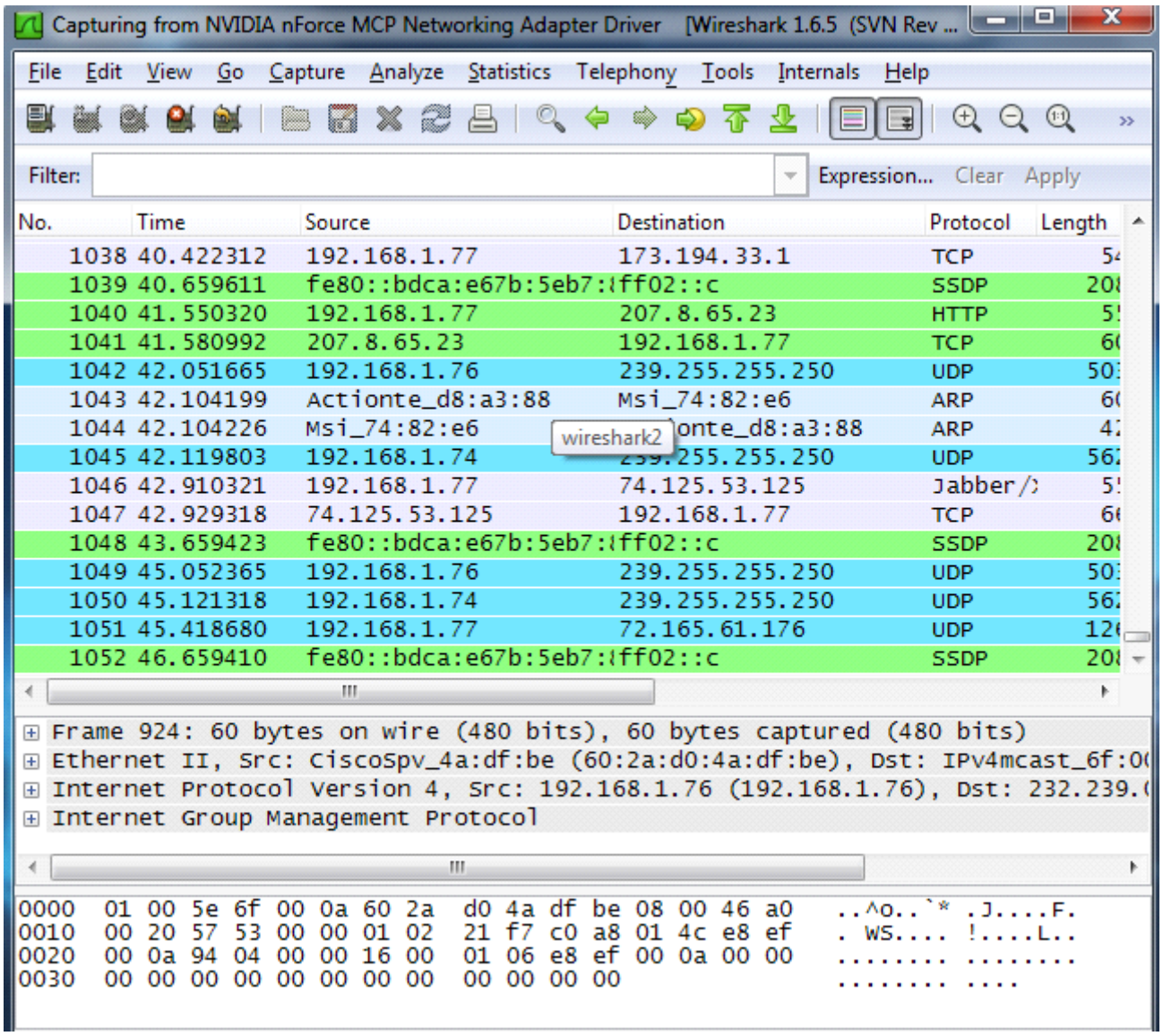
Create various statistics.

Capturing Packets

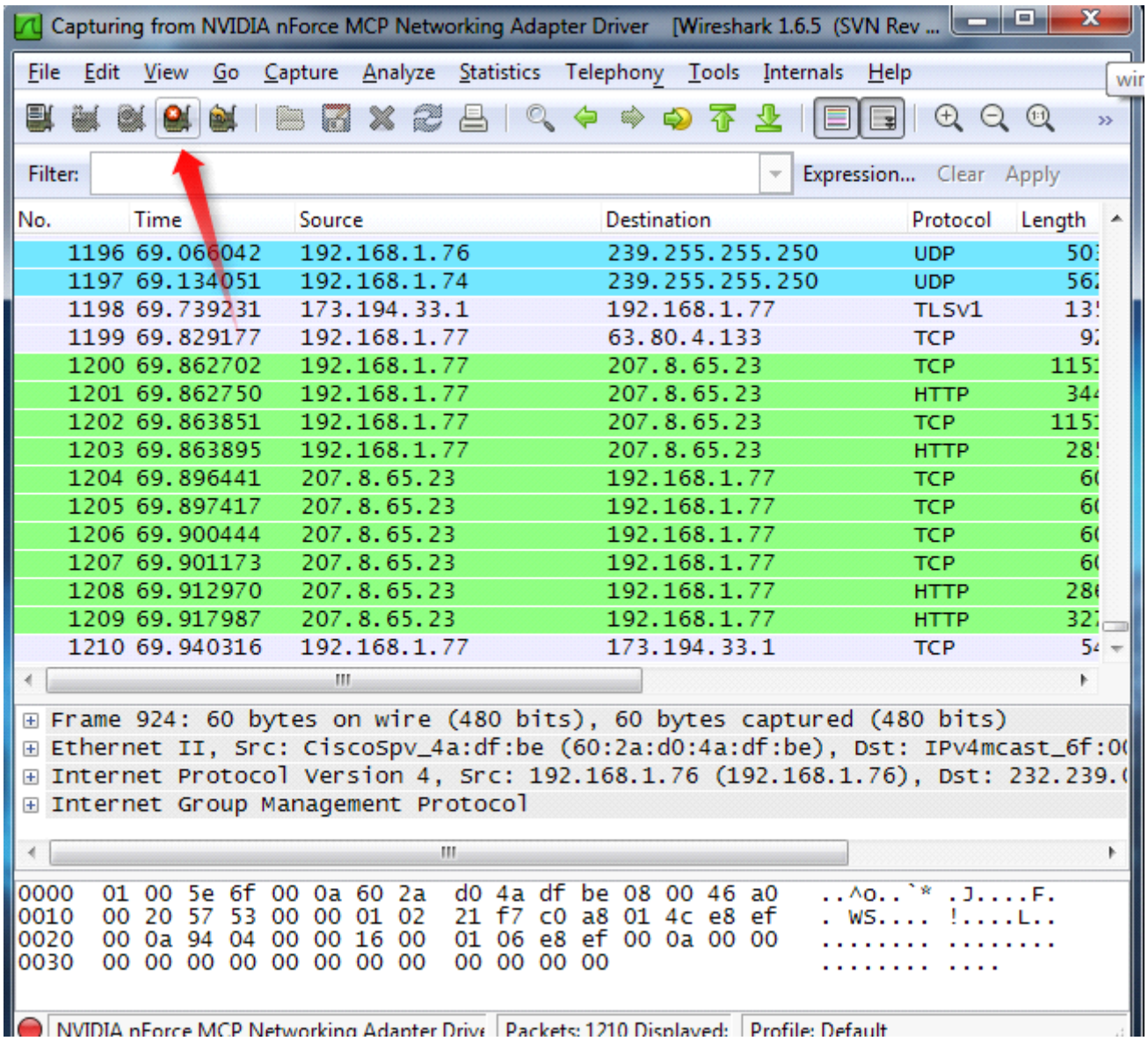
After downloading and installing wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by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



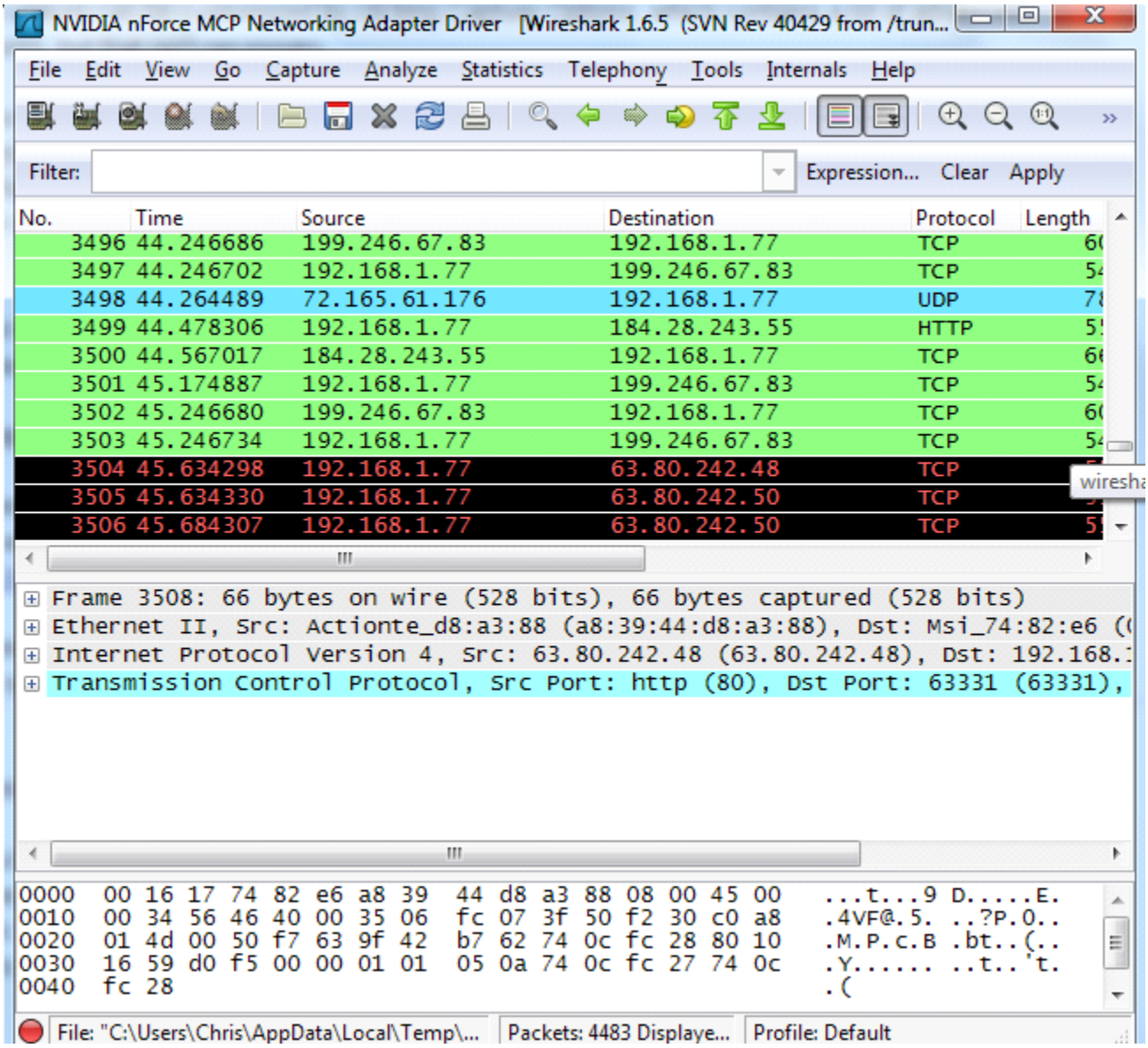
As soon as you click the interface‘s name, you‘ll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system. If you‘re capturing on a wireless interface and have promiscuous mode enabled in your capture options, you‘ll also see other the other packets on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



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



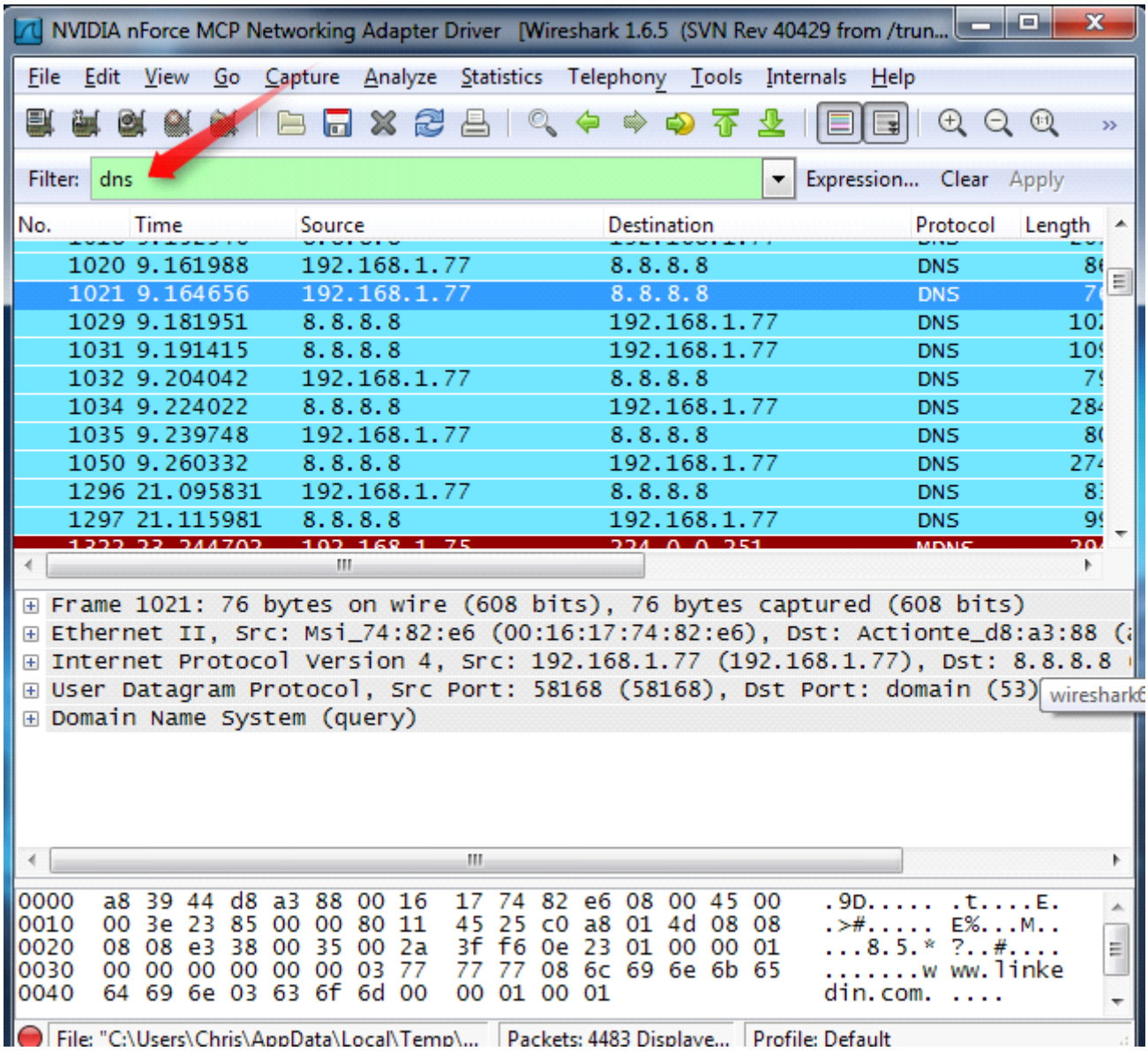
Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.



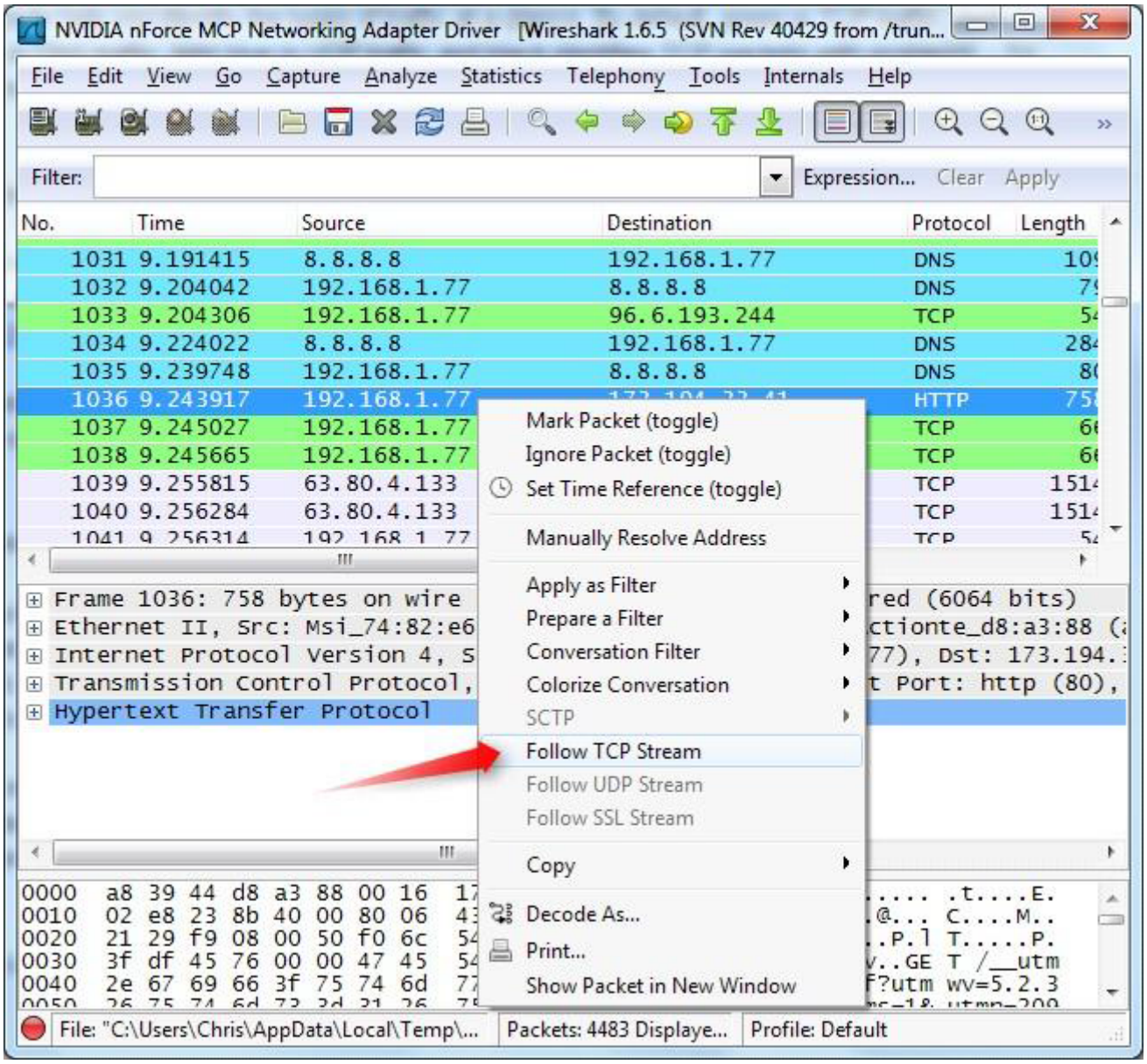
Filtering Packets

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.

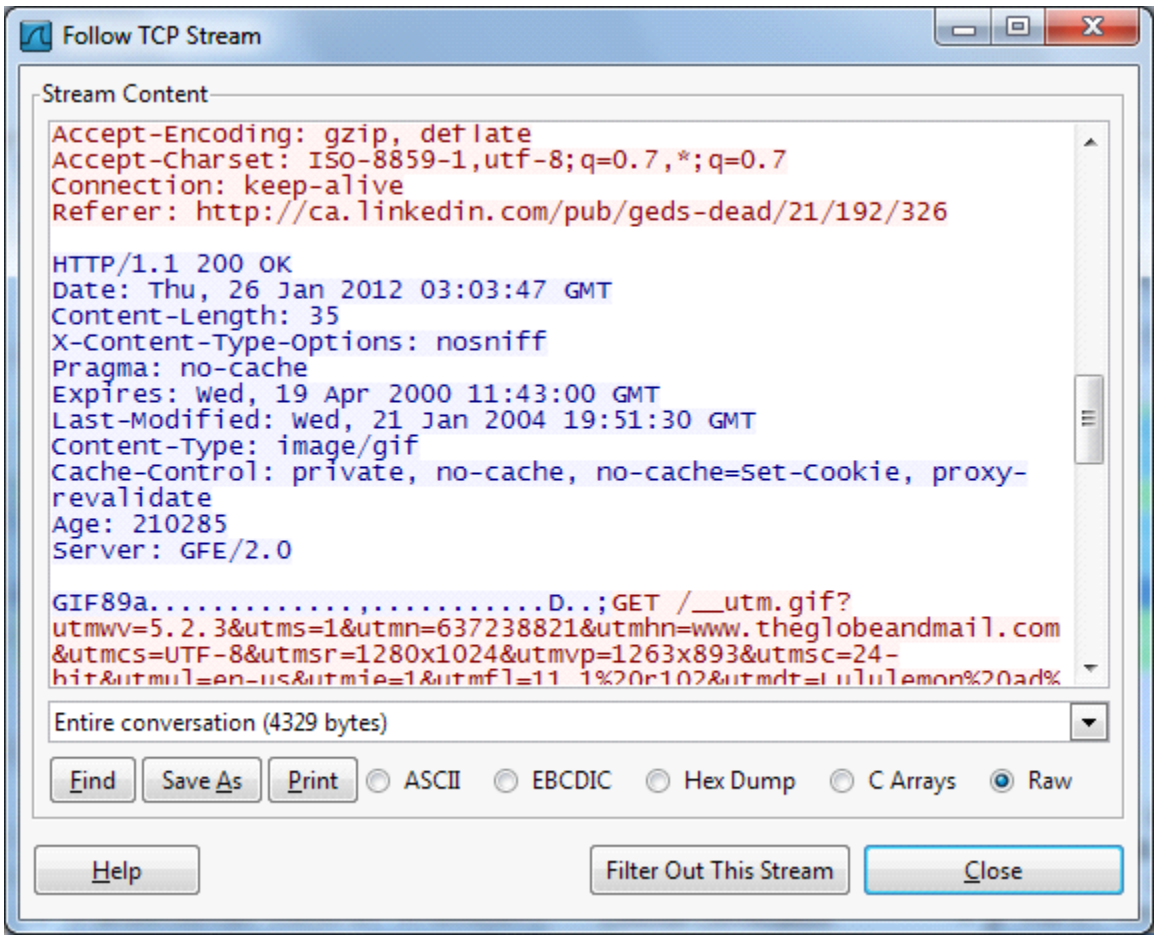
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type —dns‖ and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



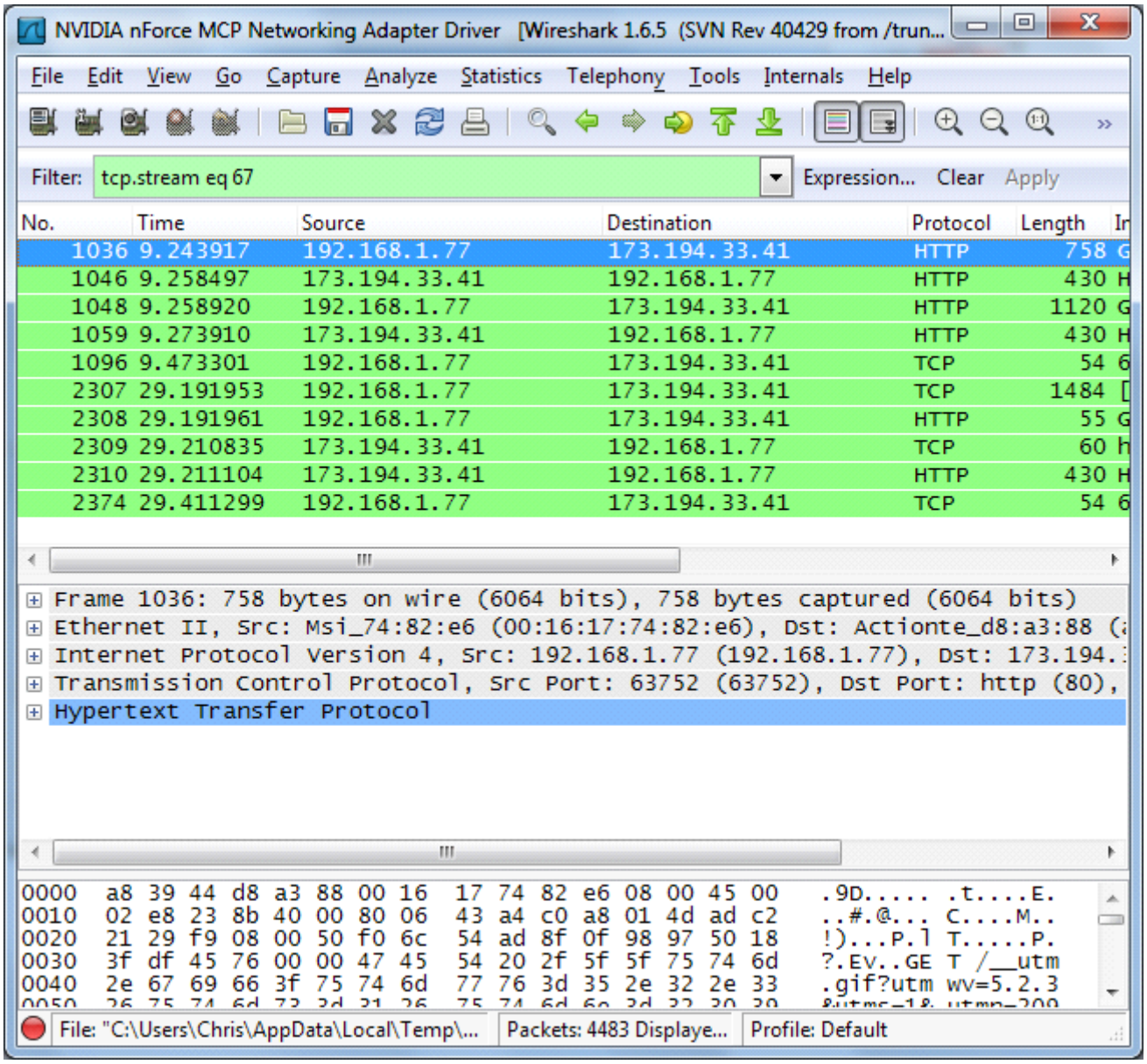
Another interesting thing you can do is right-click a packet and select Follow TCP Stream



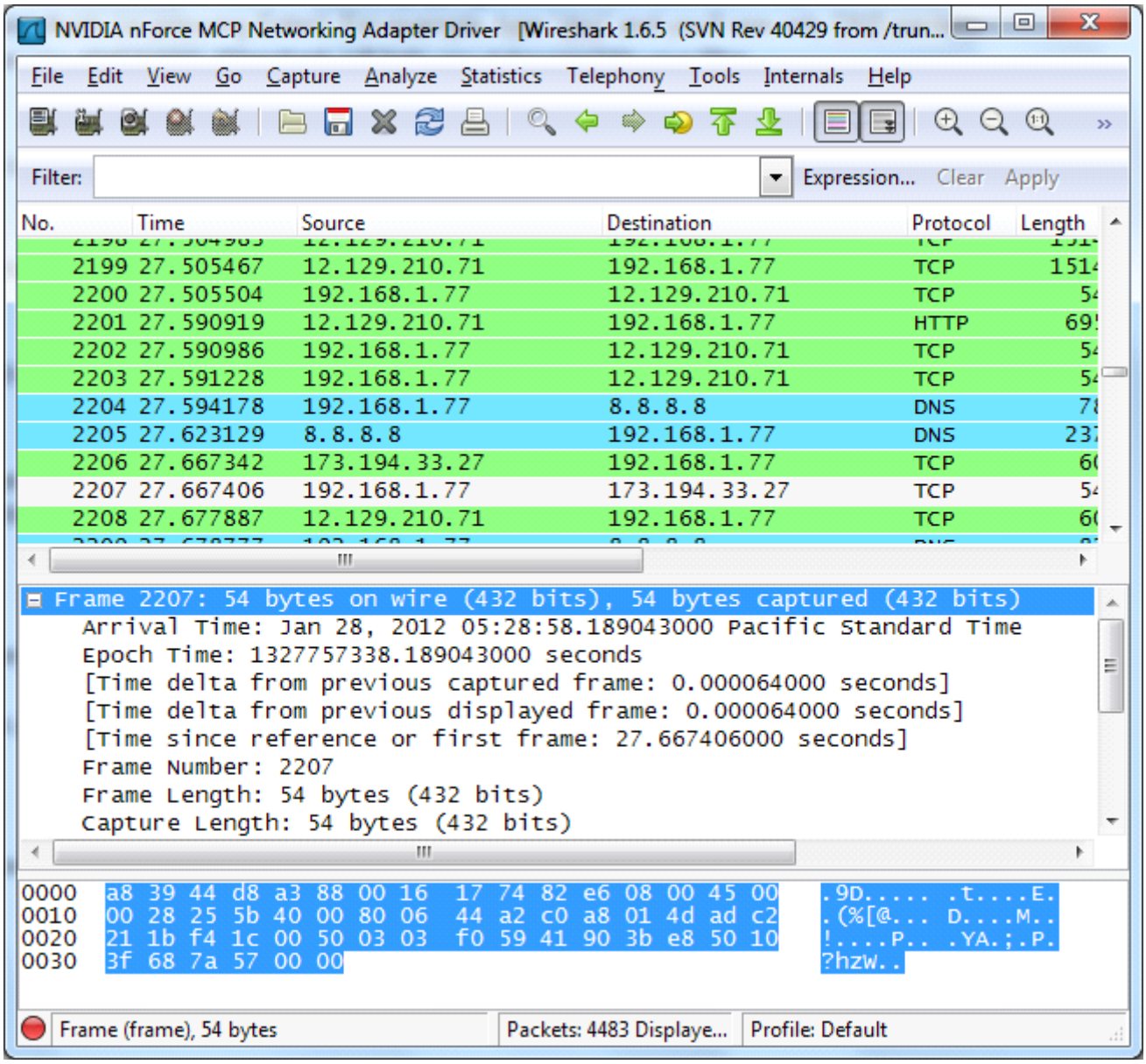
You'll see the full conversation between the client and the server.



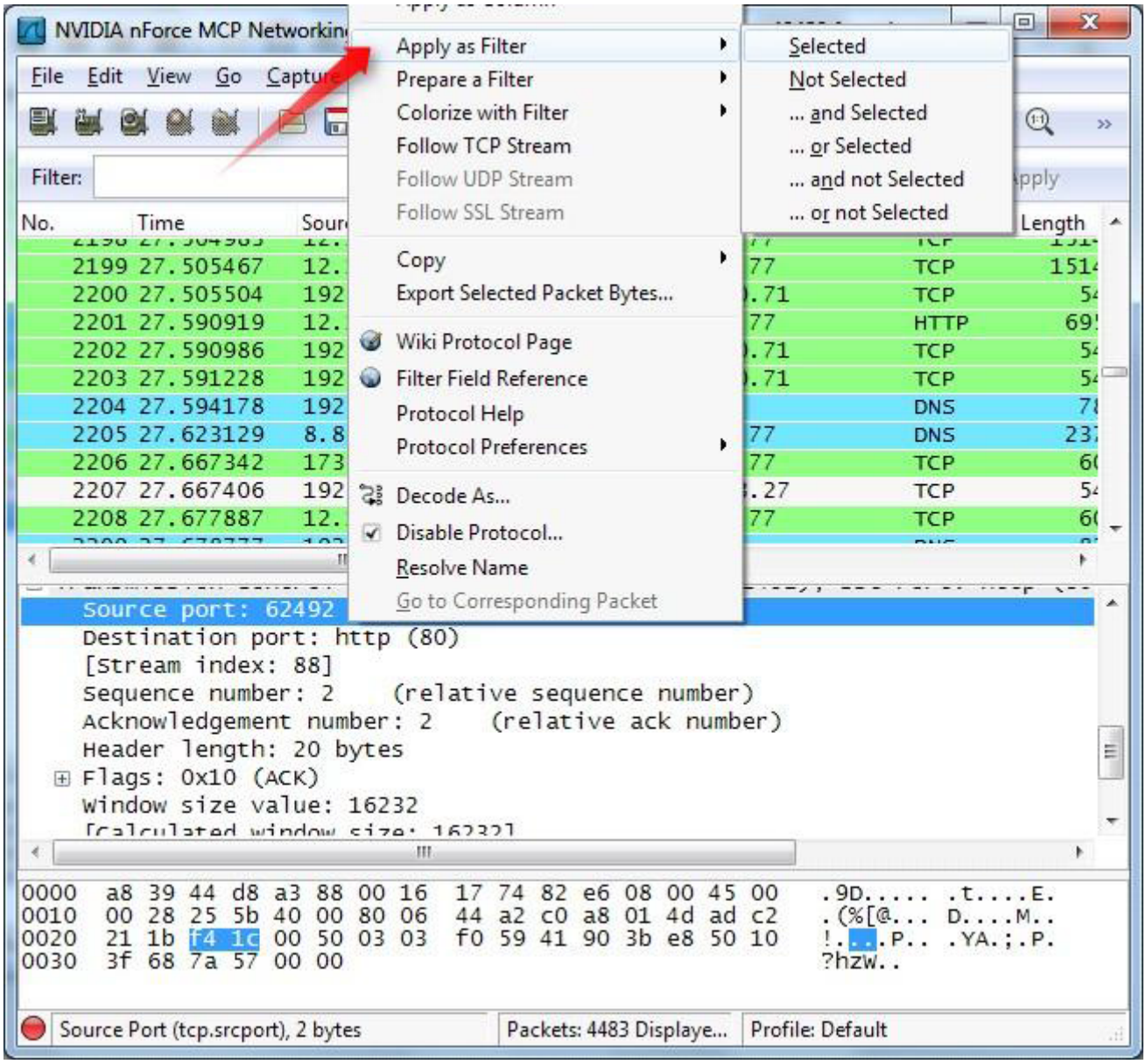
Close the window and you'll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation.



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



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

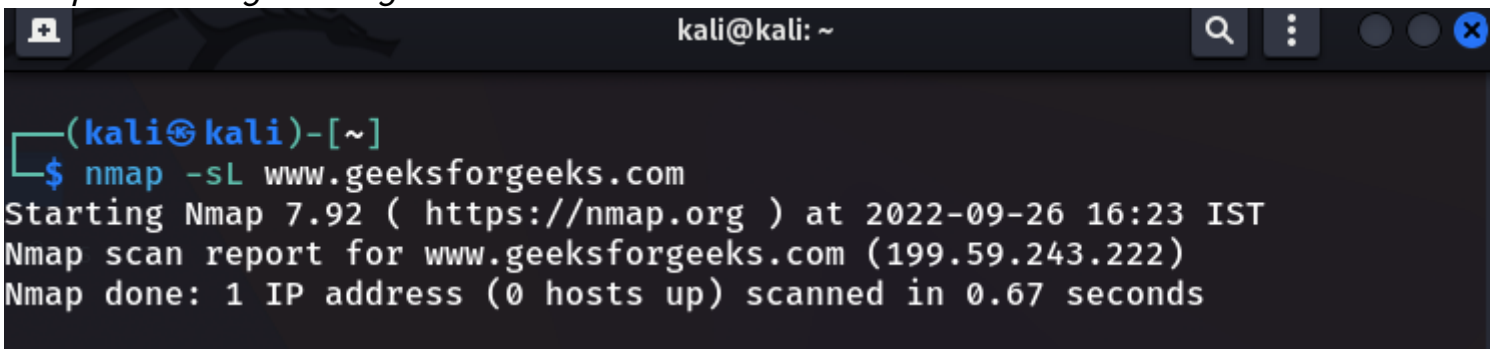
Host Discovery in Nmap Network Scanning

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:

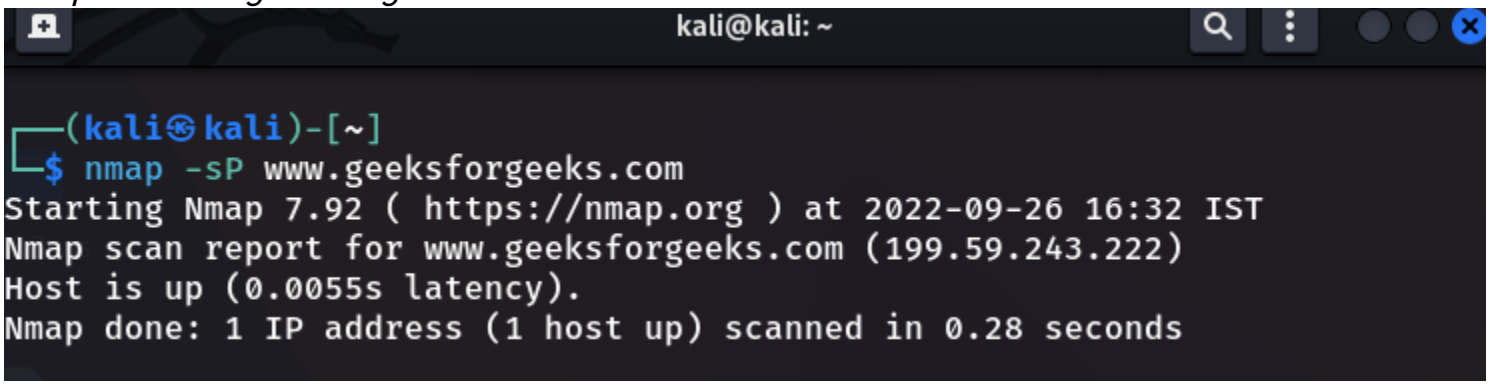
- **List Scan:** A list scan generally lists the possible host without sending any packets to the targeted host.

nmap -sL www.geeksforgeeks.com



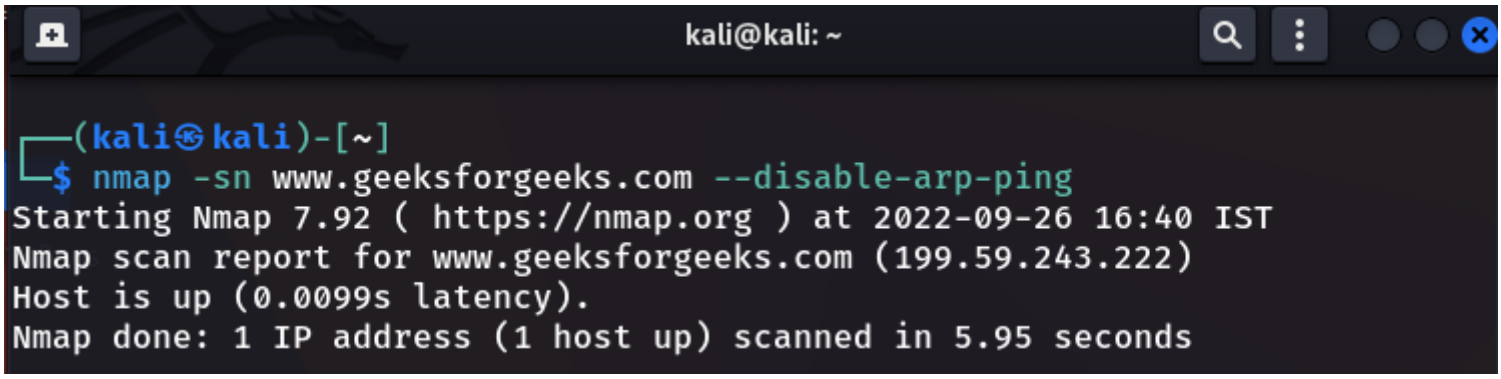
- **Ping Sweep:** Ping sweep discovers on the basis the host is powered on.

nmap -sP www.geeksforgeeks.com



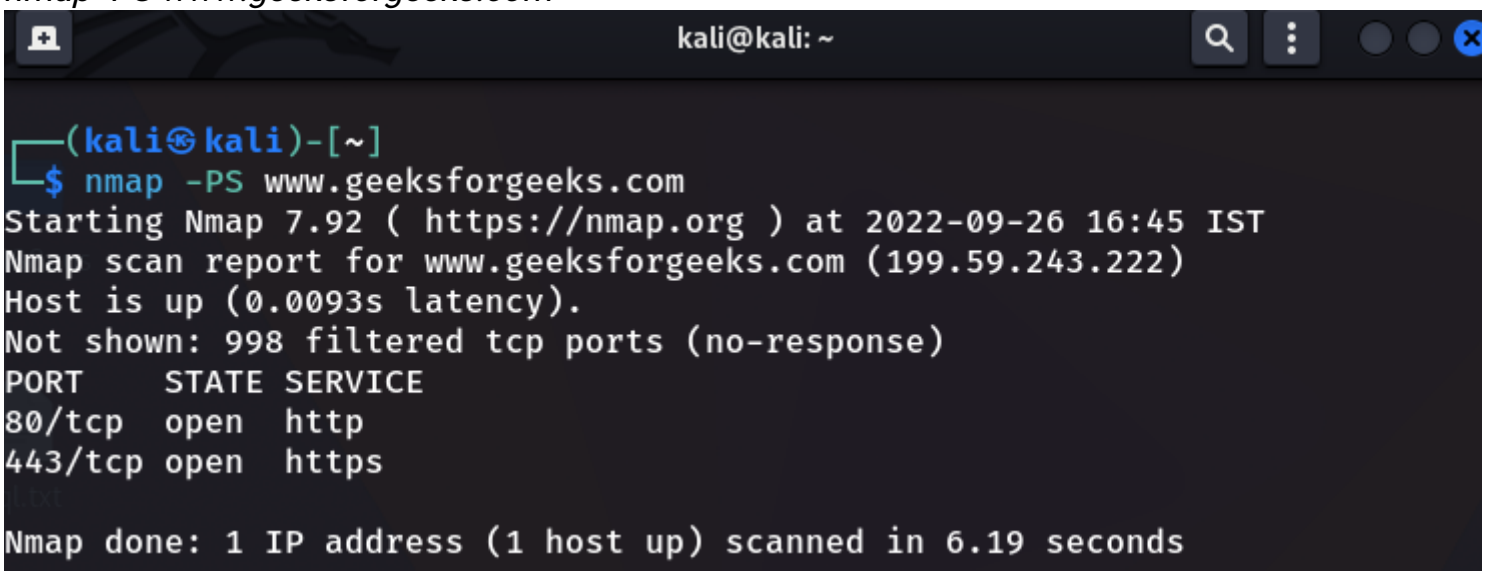
- **Disable ARP Ping:** Nmap mostly uses ARP ping to discover the other host in the network. To disable ARP Ping, use option –disable-arp-ping.

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



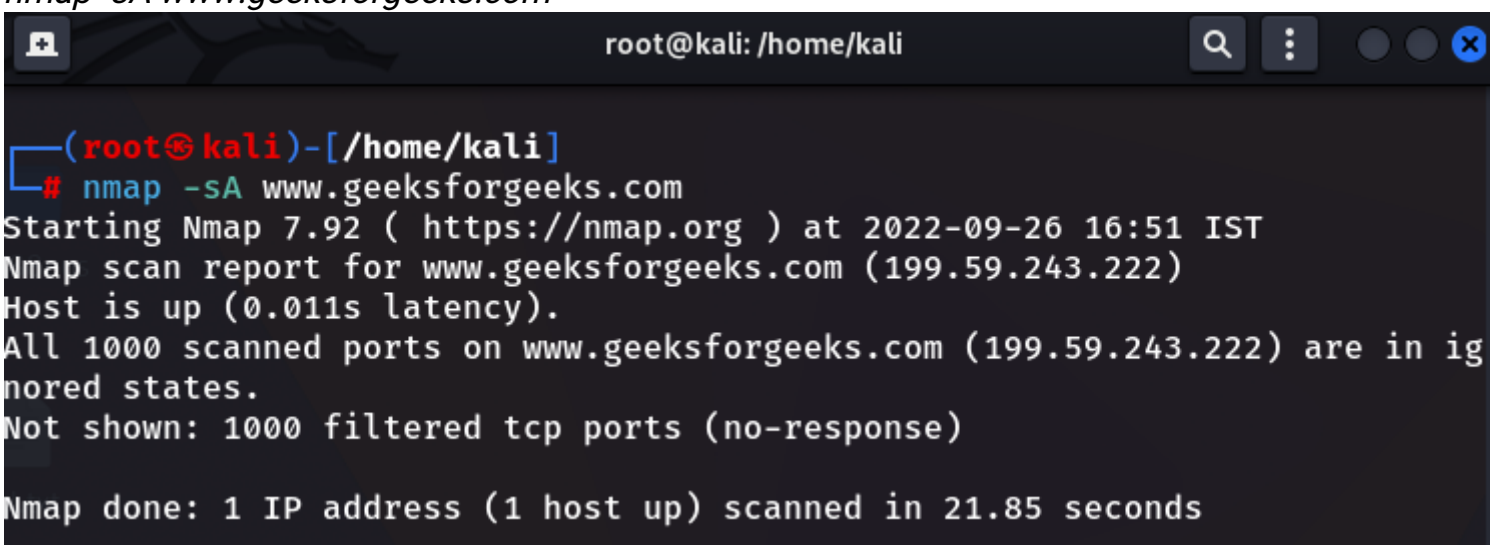
- **TCP SYN Ping:** Nmap checks whether a host is online.

nmap -PS www.geeksforgeeks.com



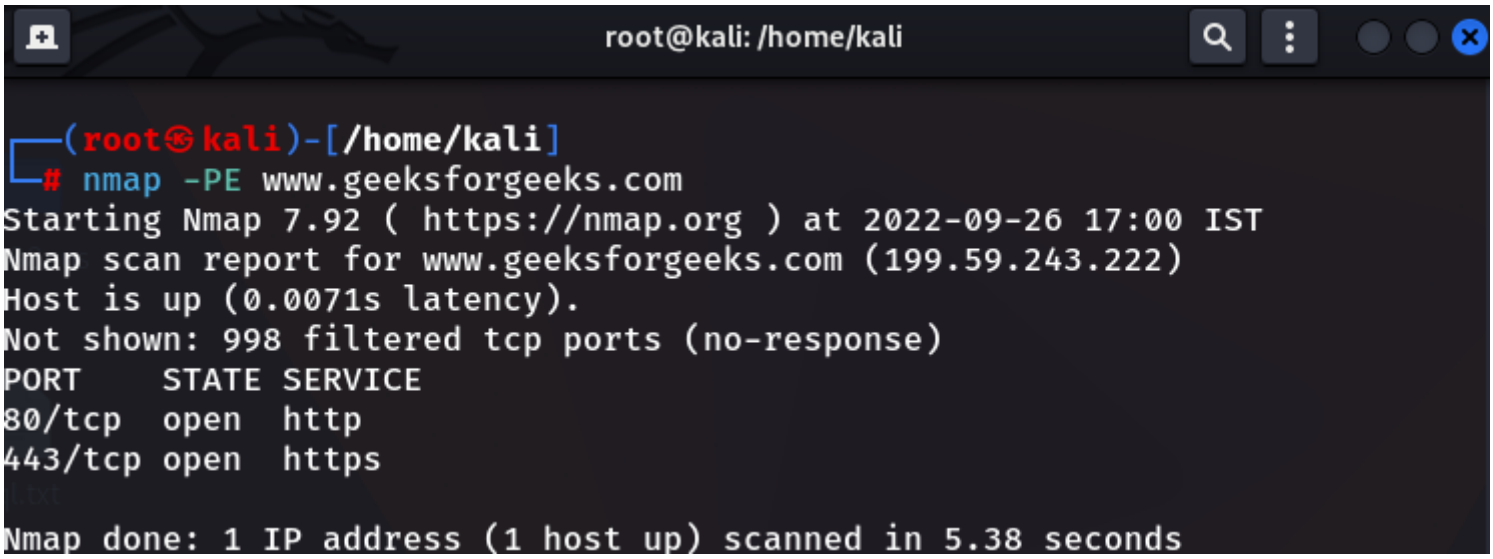
- **TCP ACK Ping:** Nmap checks whether the host is responding.

nmap -sA www.geeksforgeeks.com



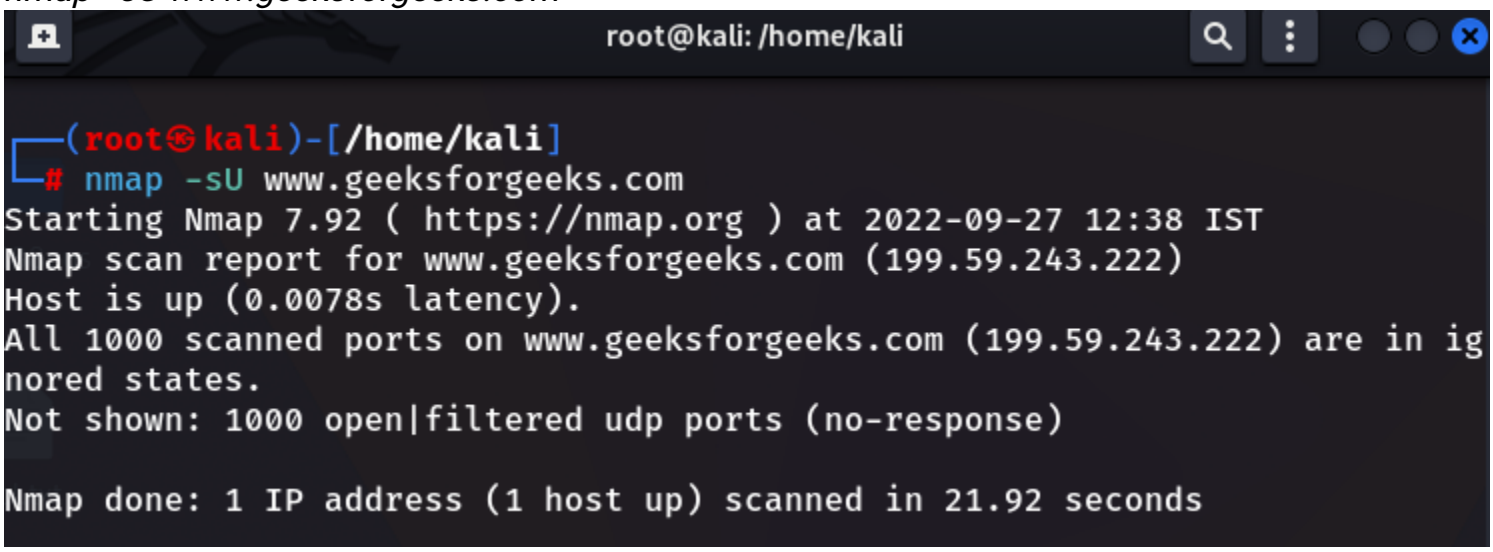
- **ICMP Echo Ping:** Nmap sends ICMP packets to the available host.

nmap -PE www.geeksforgeeks.com



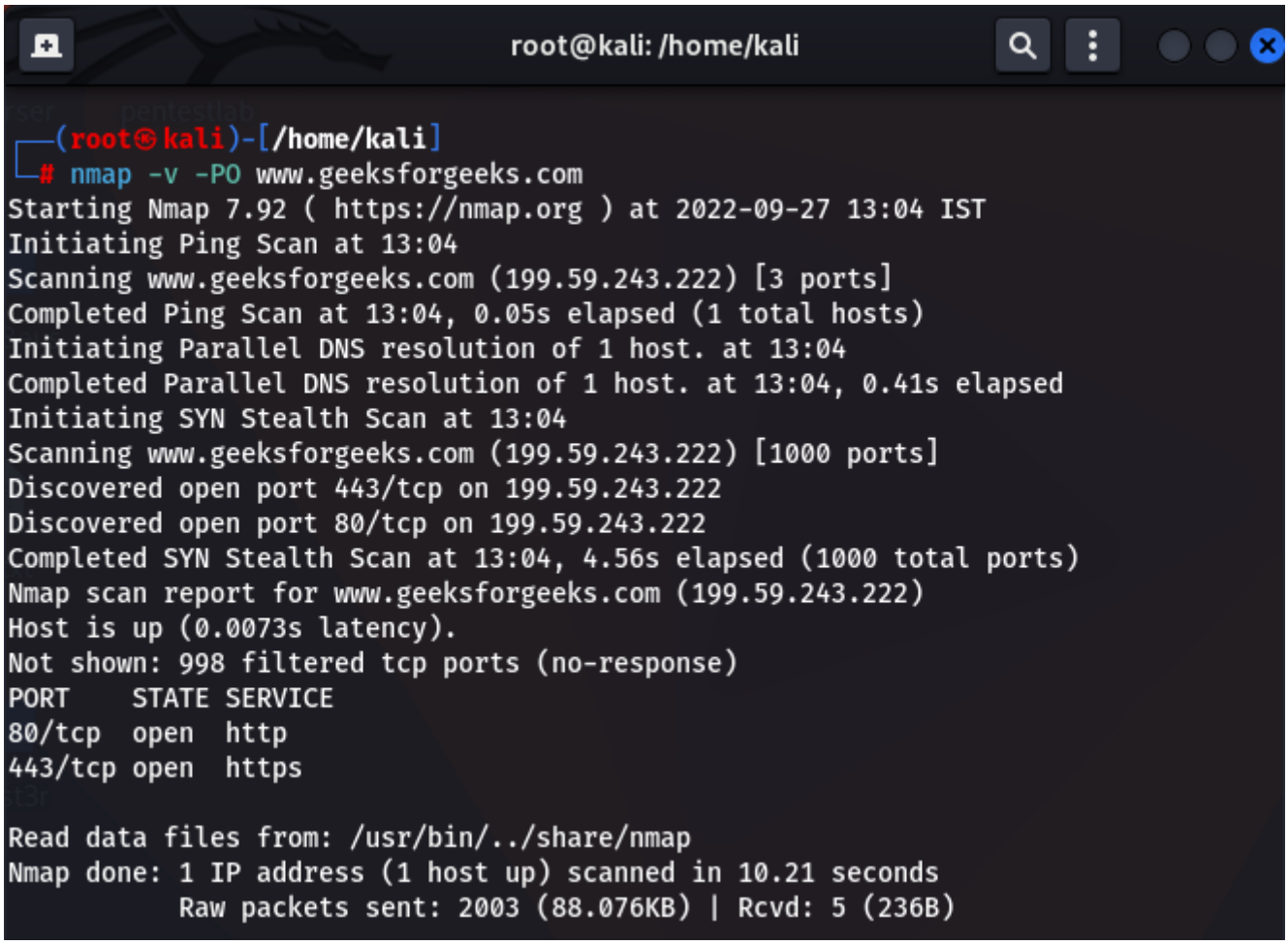
- **UDP Ping:** Nmap sends the UDP packets to the targeted port.

nmap -sU www.geeksforgeeks.com



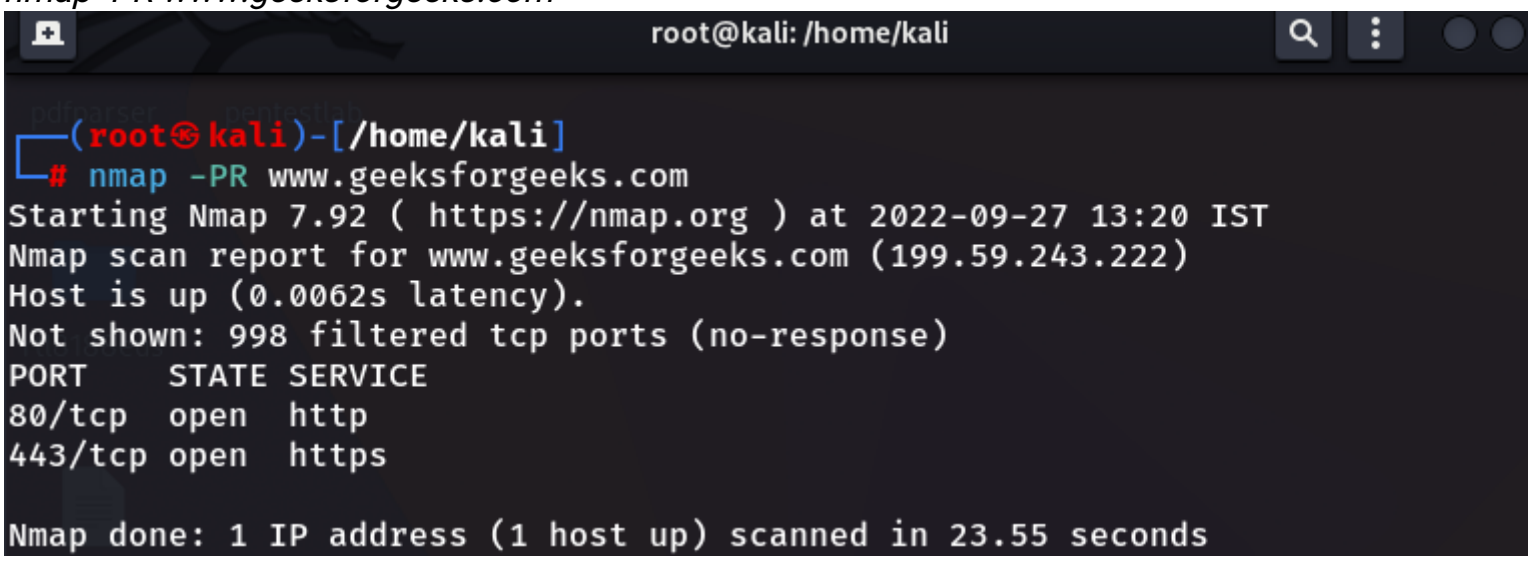
- **IP Protocol Ping:** Nmap tries to send different packets using different protocols.

nmap -v -PO www.geeksforgeeks.com



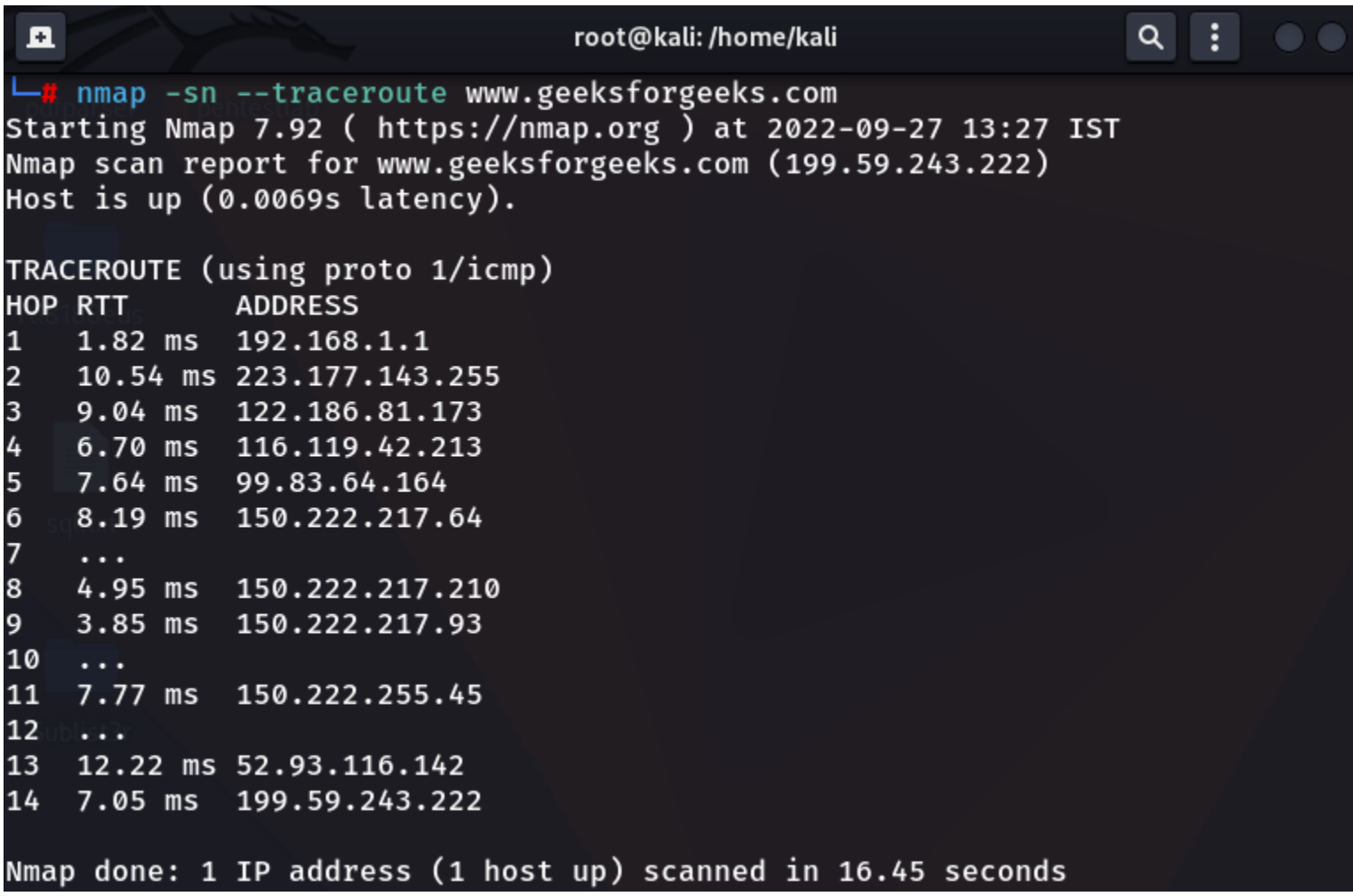
- **ARP Ping:** ARP ping scan is used to discover the host devices in the same network. sometimes it will not visible due to firewall filtering.

nmap -PR www.geeksforgeeks.com



- **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 ...
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:

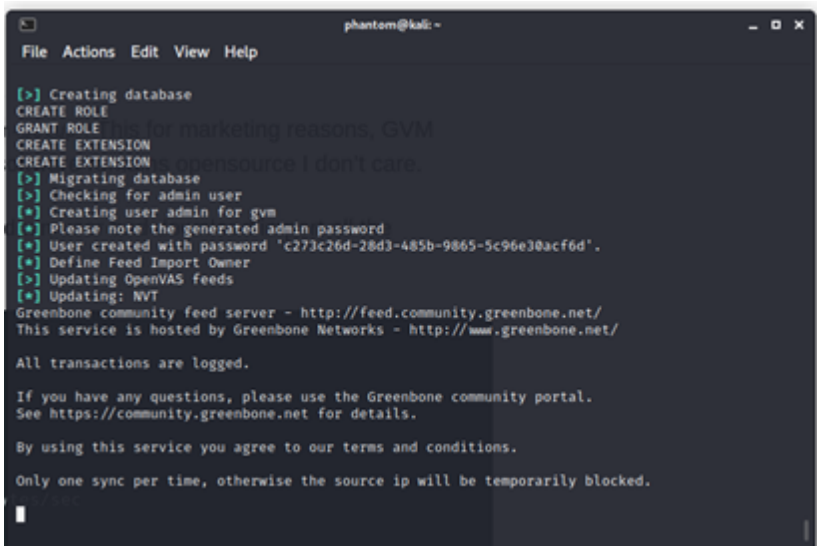
```
sudo apt update
sudo apt upgrade -y
sudo apt dist-upgrade -y
```

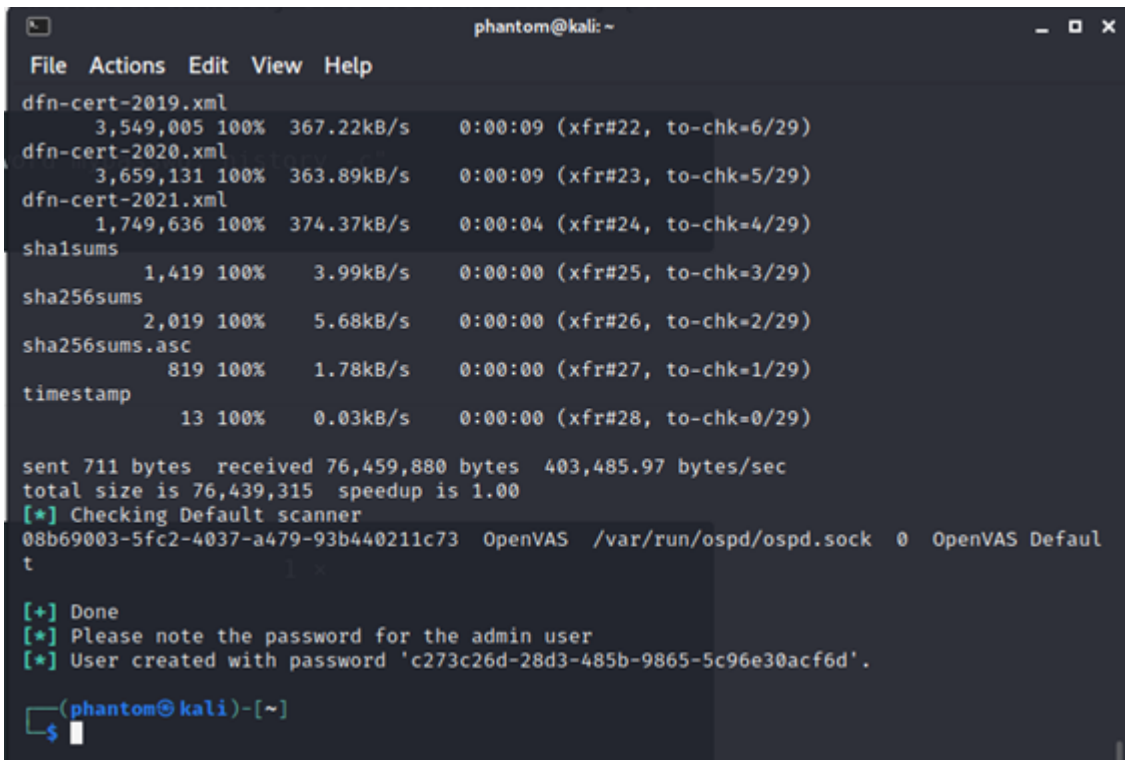
```
sudo apt install openvas
```

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
```





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.

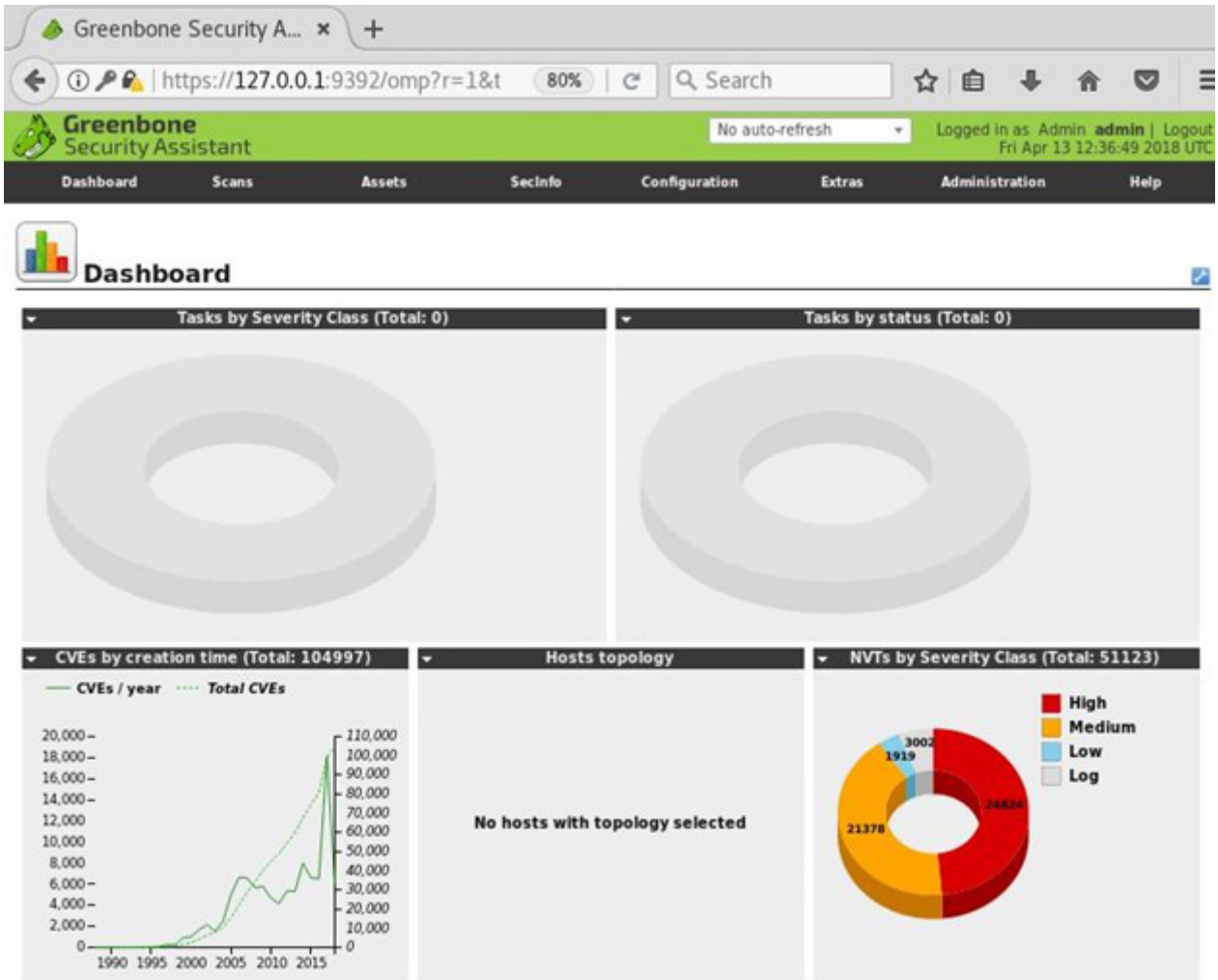
gvm-check-setup

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:

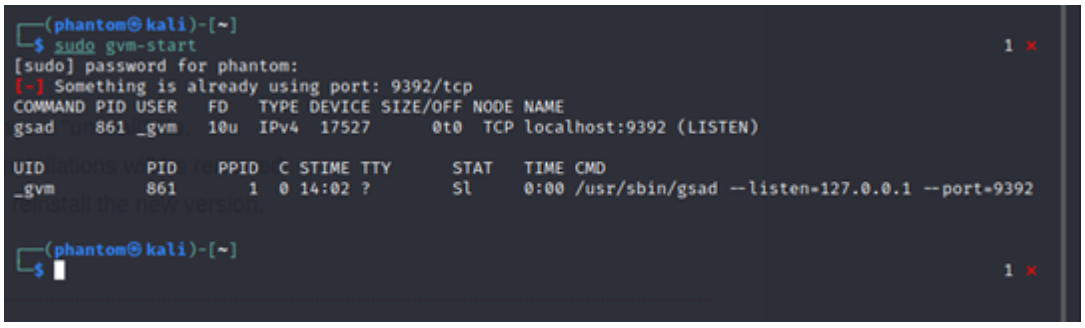


Starting and stopping OpenVAS

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.

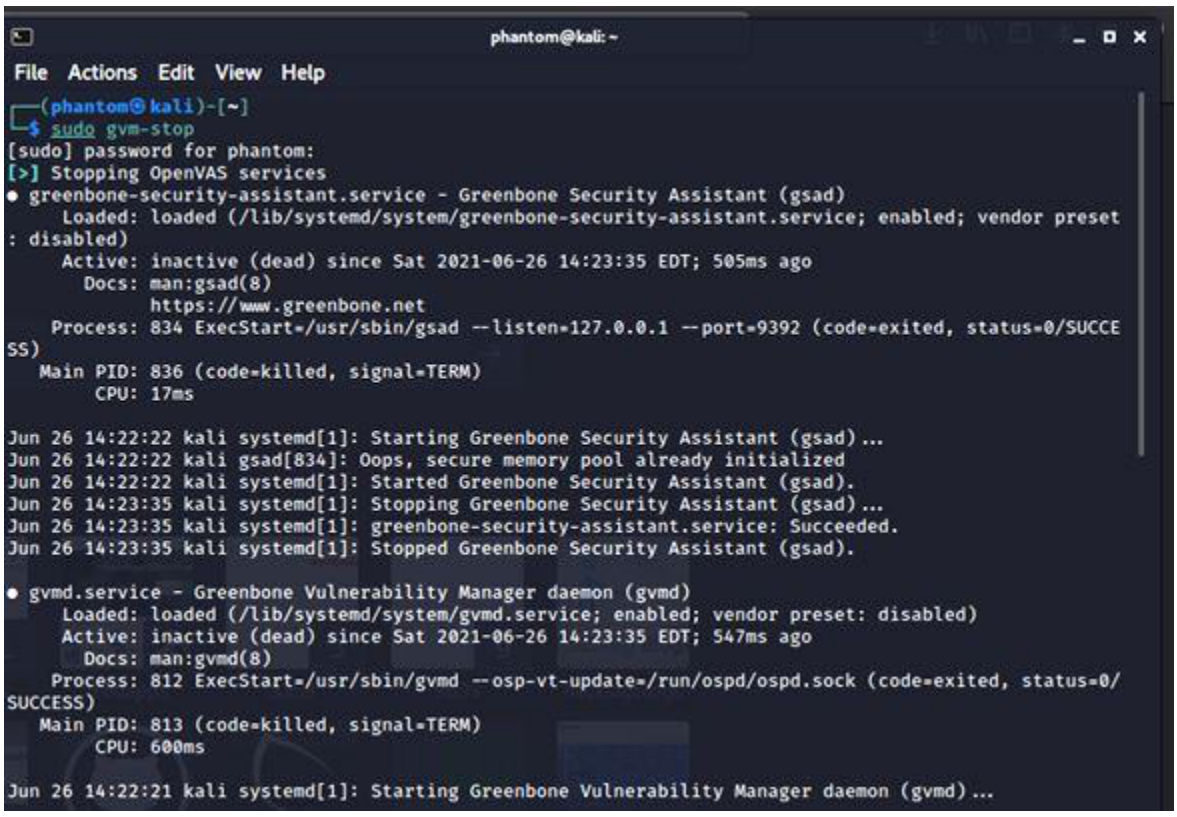
Run the following command to start the services:

Sudo gvm-start



To stop the OpenVAS services again, run:

sudo gvm-stop



*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: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:

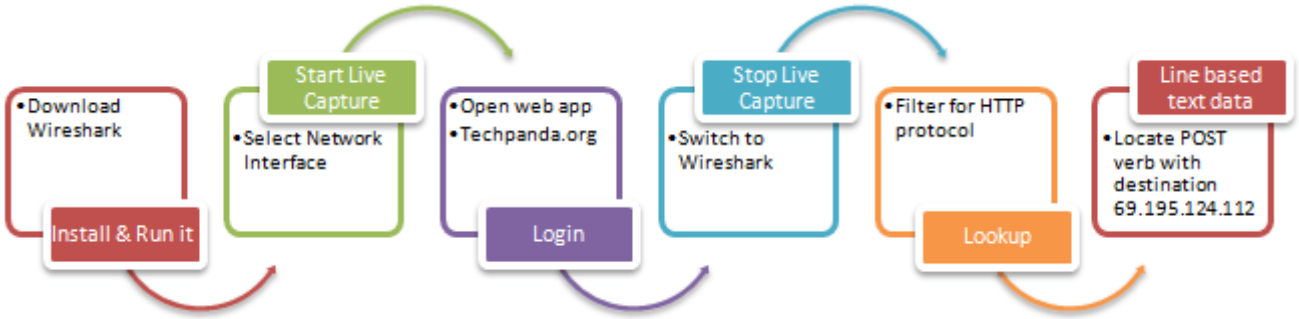
C:\Tools\nmap-7.50>nmap.exe -Pn -p445 --open --max-hostgroup 3 --script smb-vuln-ms17-010 192.168.1.17

```
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
```

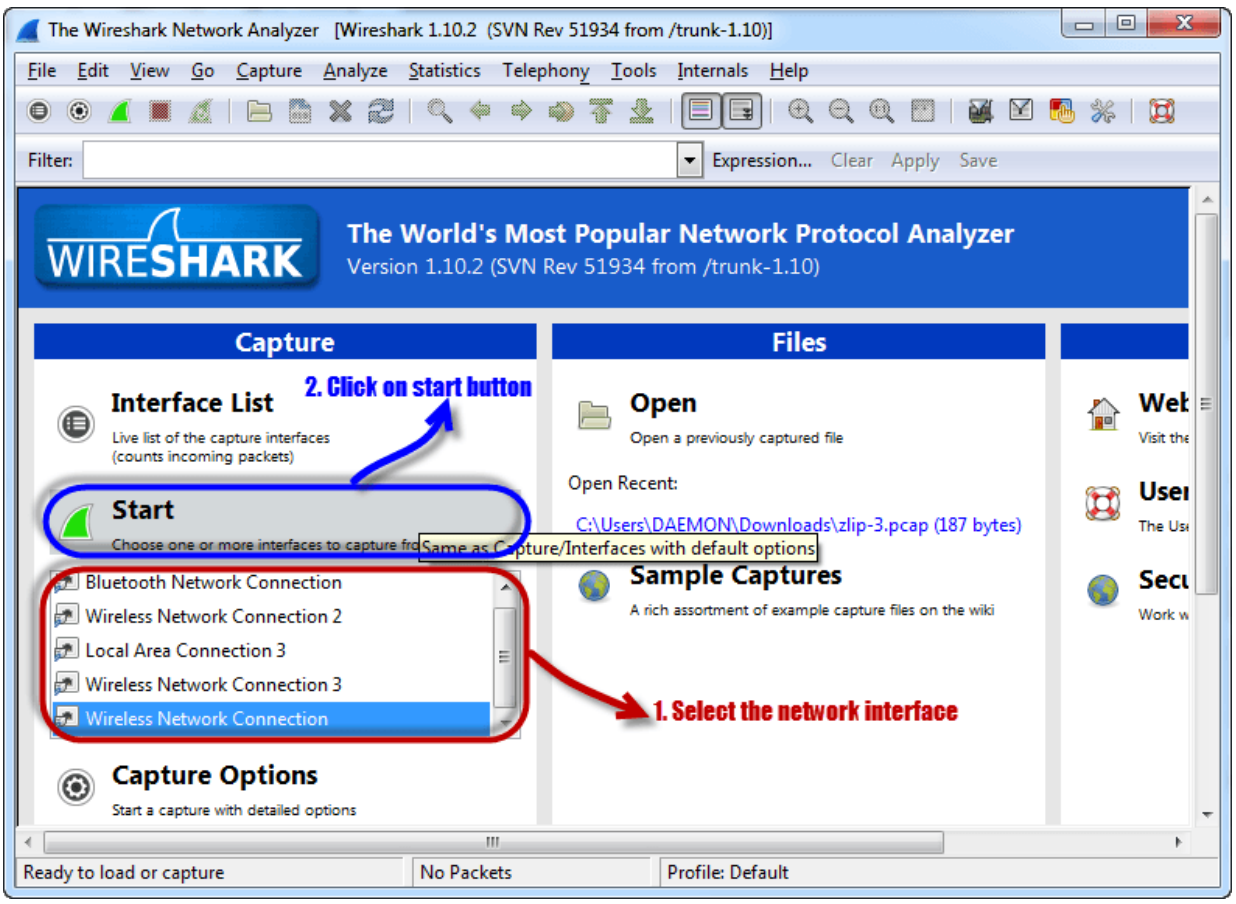
If nmap detects that a machine is not vulnerable for CVE-2017-0143 (EternalBlue), then the output will look as follows:

```
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
```

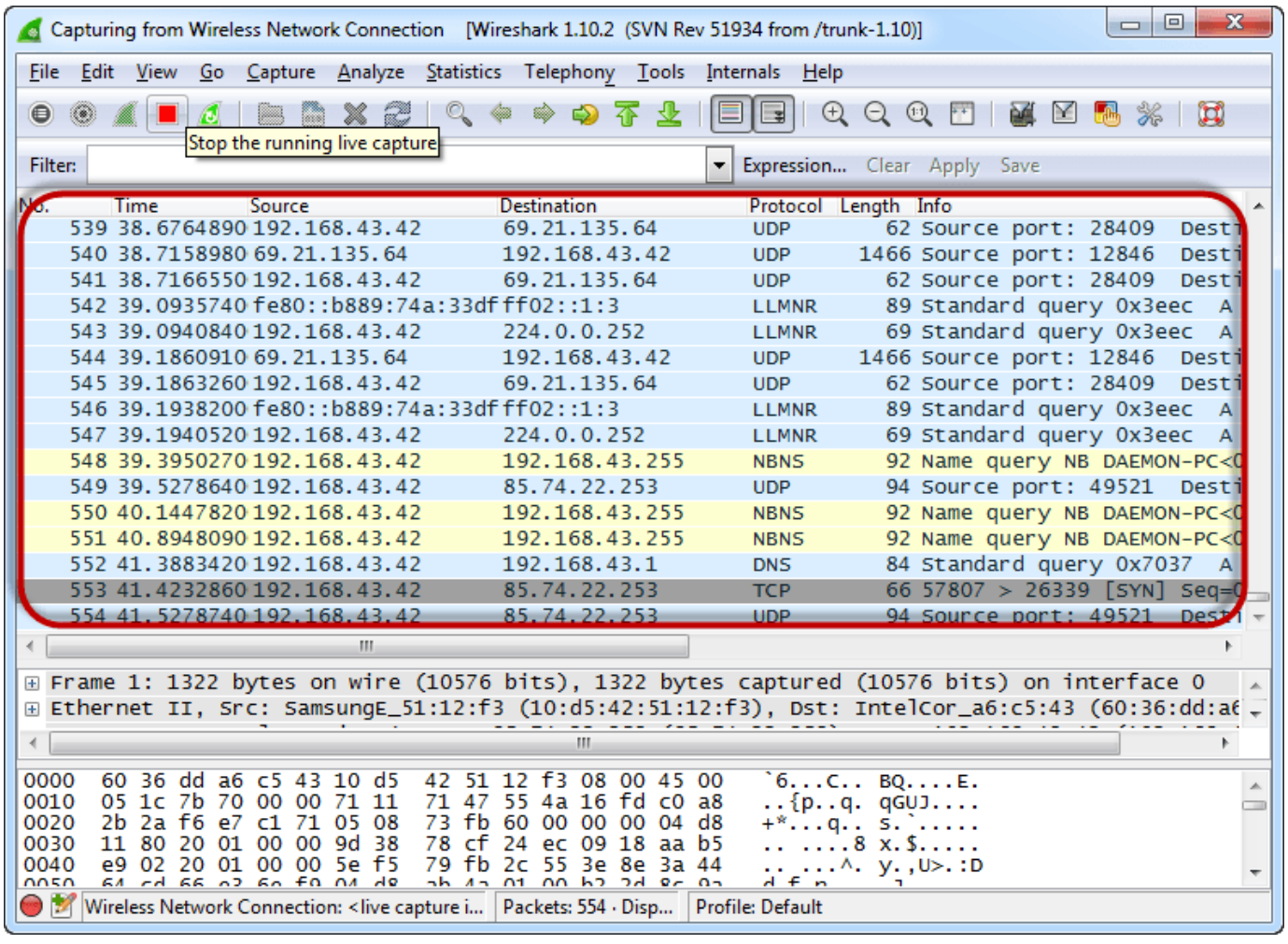
4. **Sniffing POP3/FTP/Telnet passwords:**



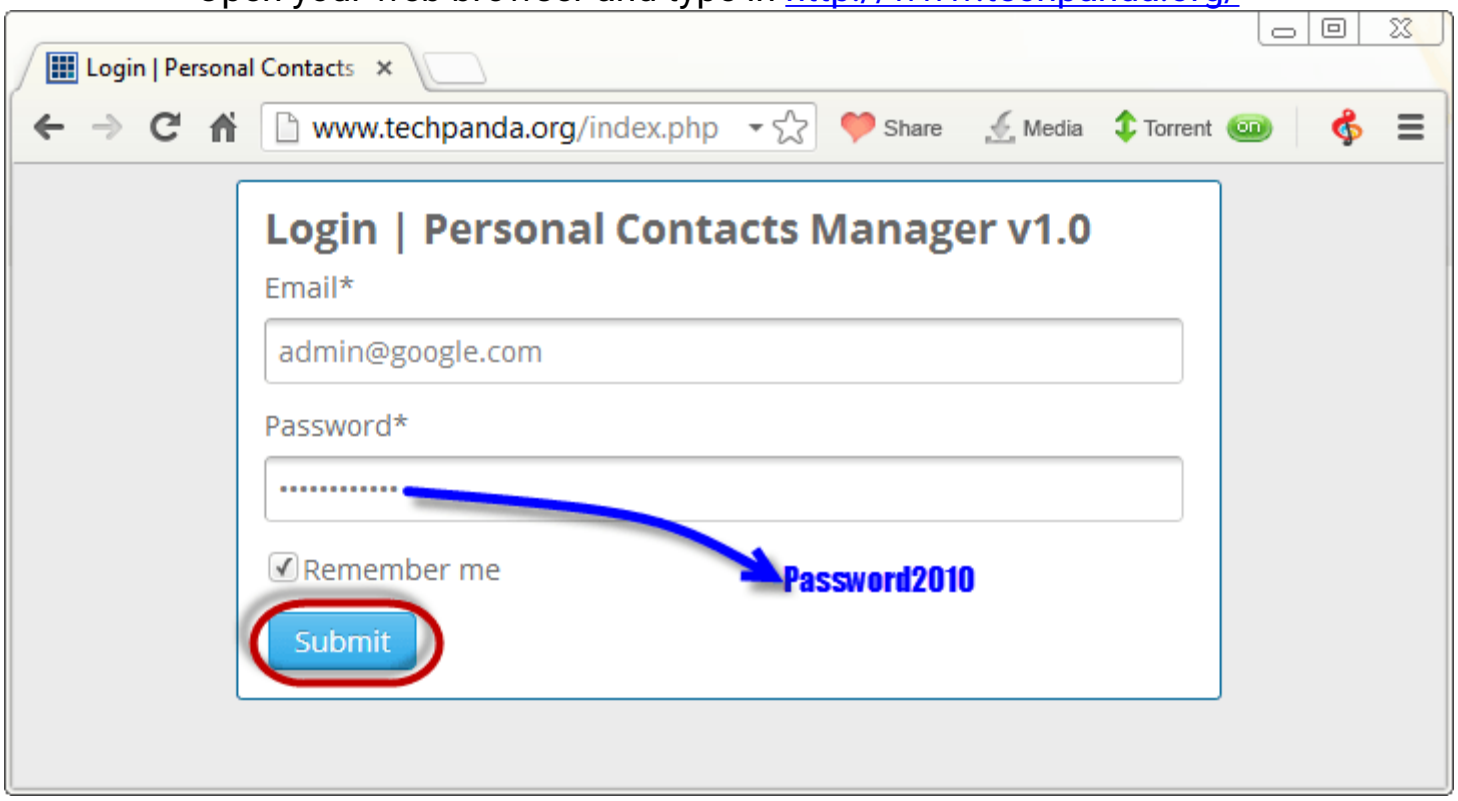
- Open Wireshark
- You will get the following screen



- 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

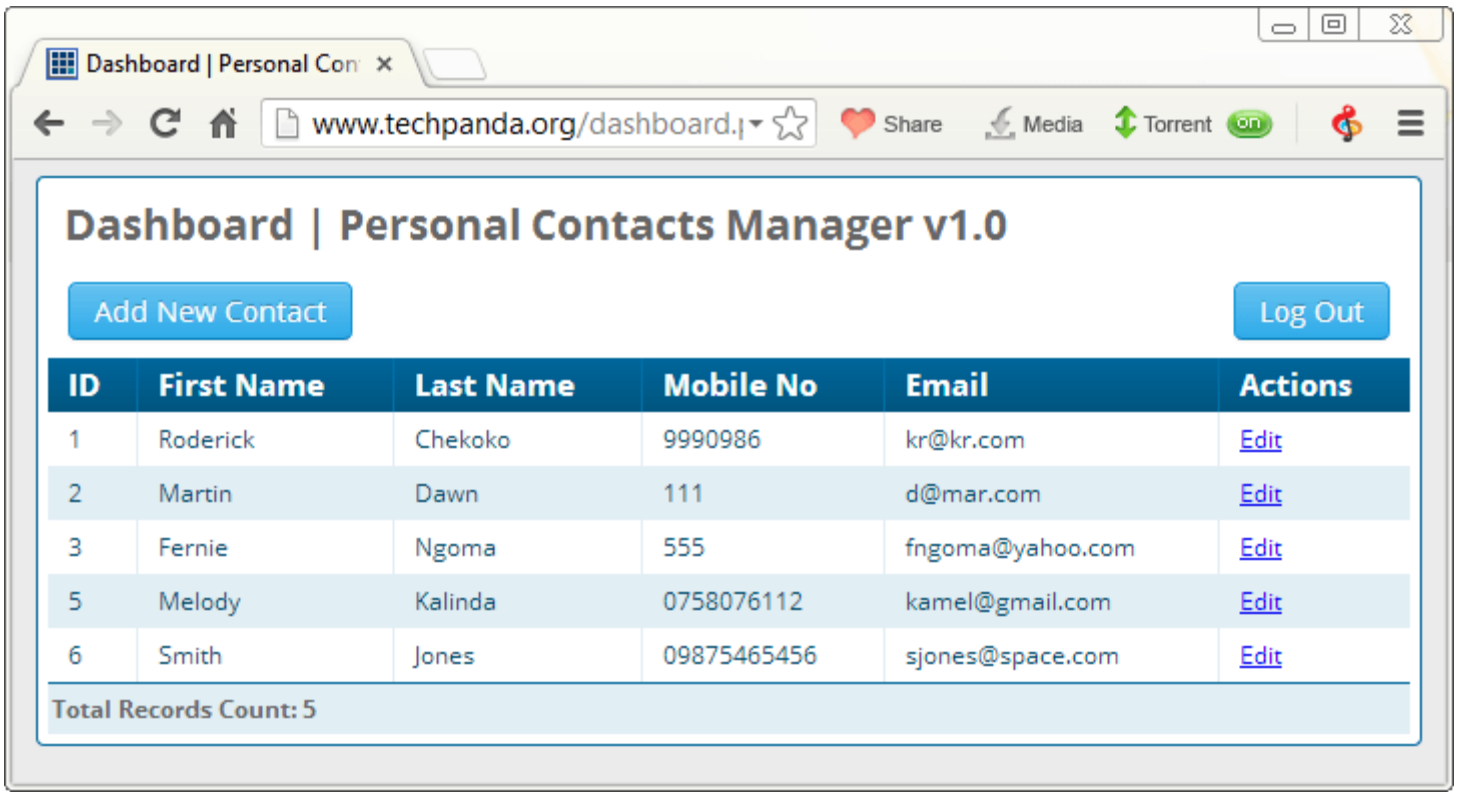


- Open your web browser and type in http://www.techpanda.org/

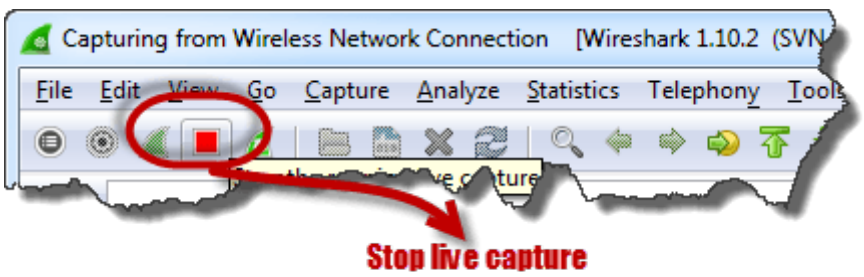


- The login email is **admin@google.com** and the password is **Password2010**
- Click on submit button

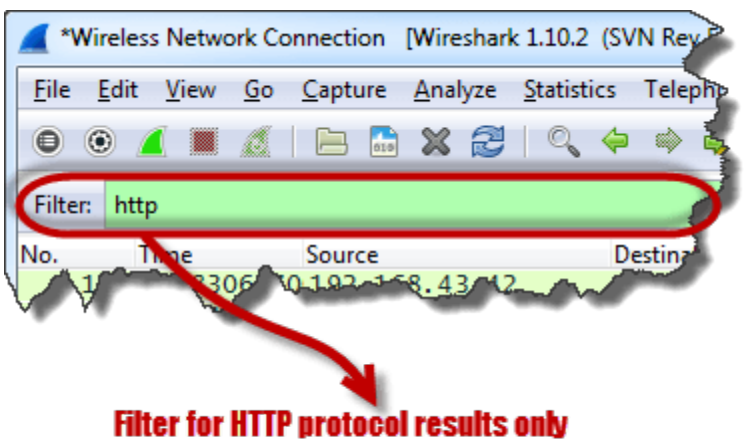
- A successful logon should give you the following dashboard



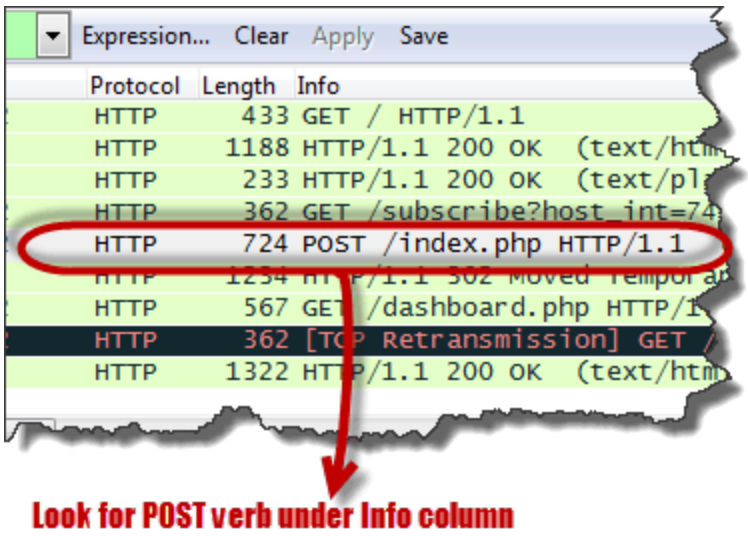
- Go back to Wireshark and stop the live capture



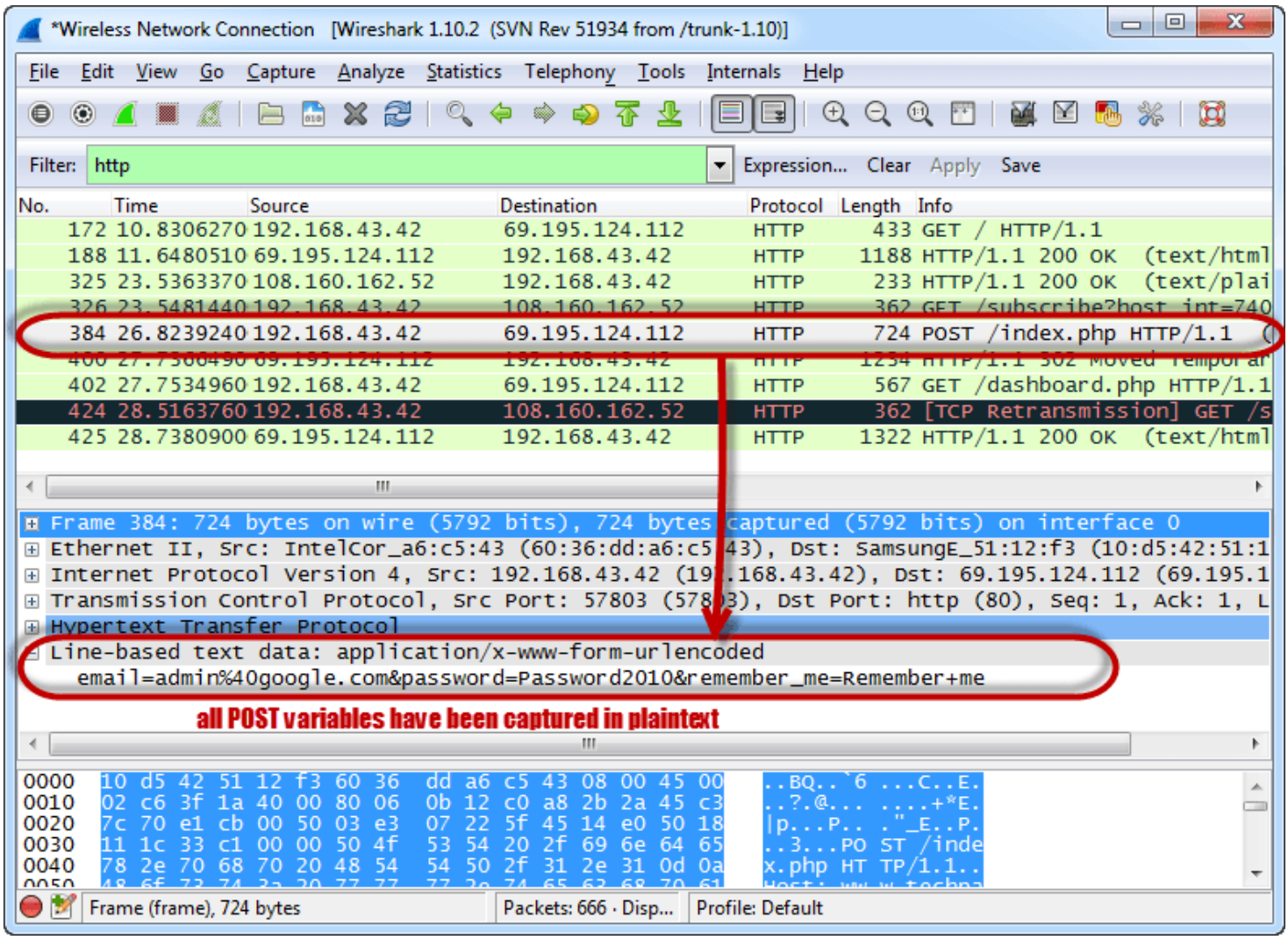
- Filter for HTTP protocol results only using the filter textbox



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



- 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



- 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.

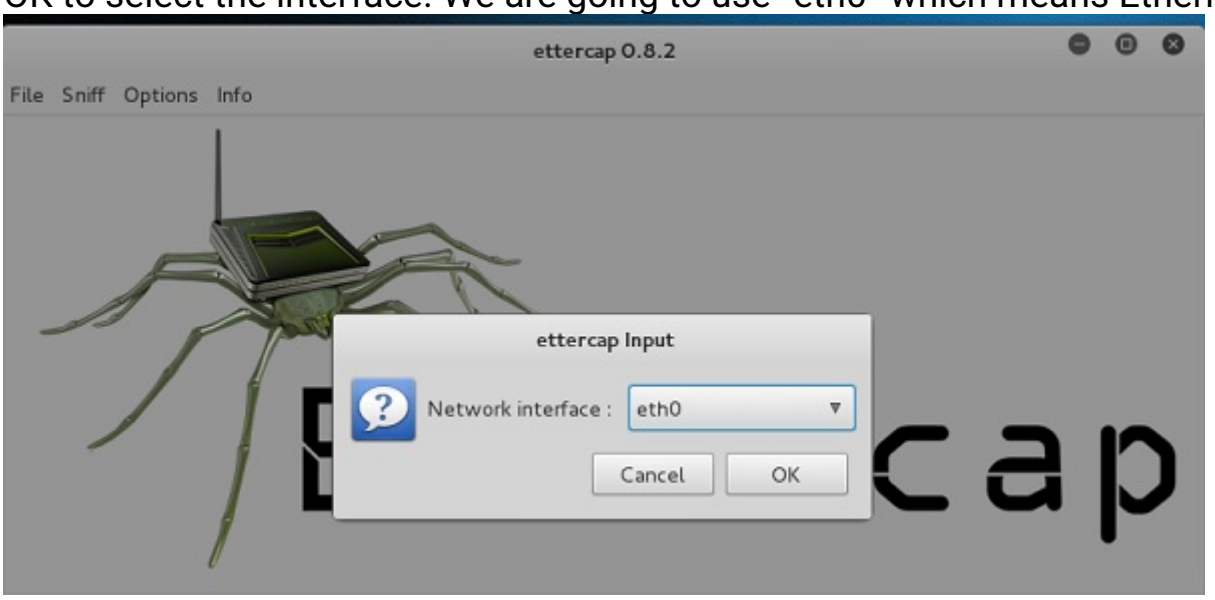
Step 1 − Install the VMware workstation and install the Kali Linux operating system.

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

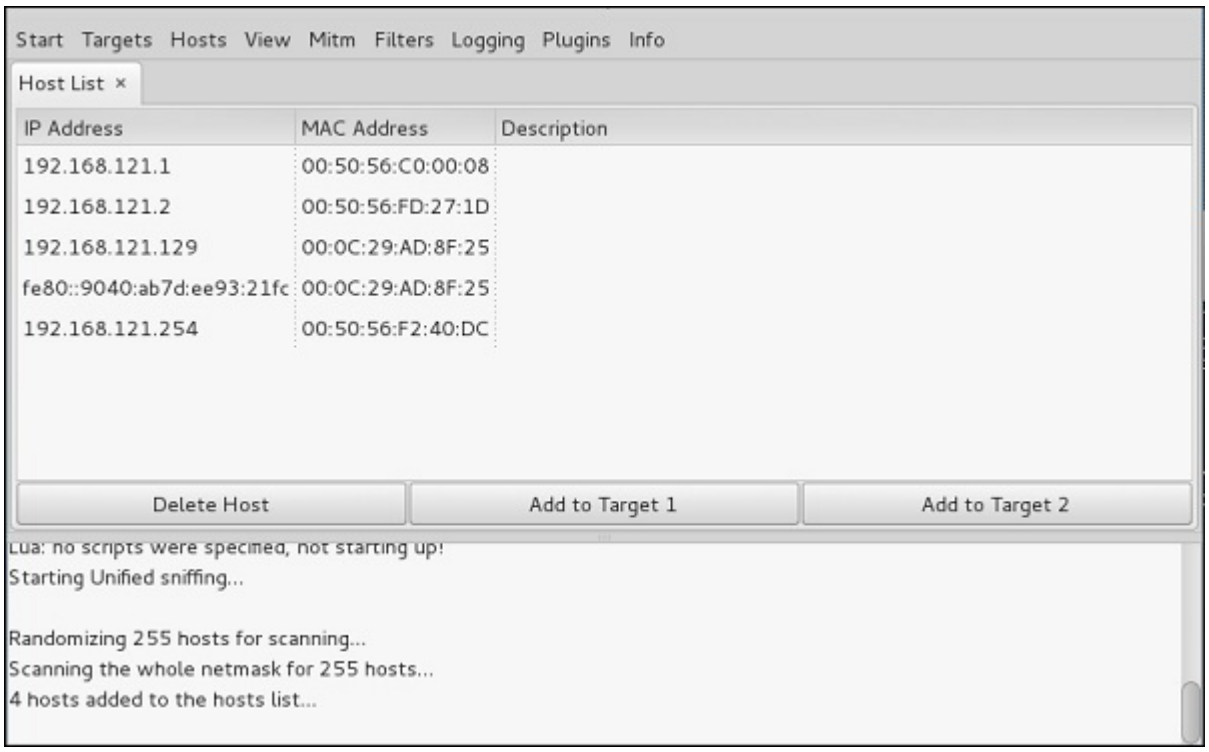
Step 3 − Make sure you are connected to local LAN and check the IP address by typing the command ifconfig in the terminal.

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.



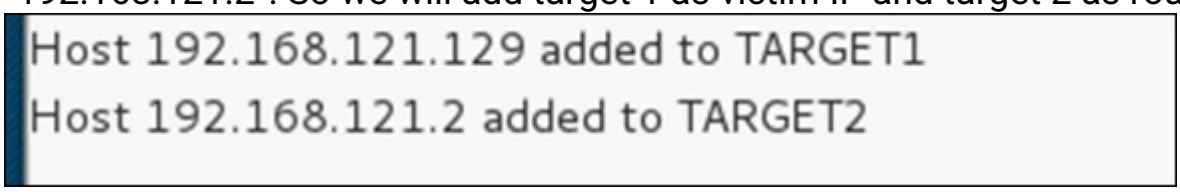
Step 7 – Next, click the “hosts” tab and select “hosts list” to see the number of hosts available in the network. This list also includes the default gateway address. We have to be careful when we select the targets.

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.



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.

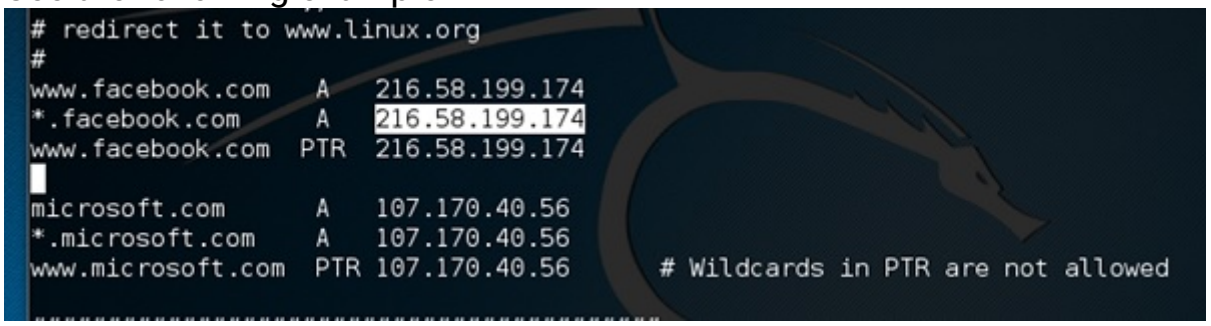
Like ARP poisoning, there are other attacks such as MAC flooding, MAC spoofing, DNS poisoning, ICMP poisoning, etc. that can cause significant loss to a network.

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.

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



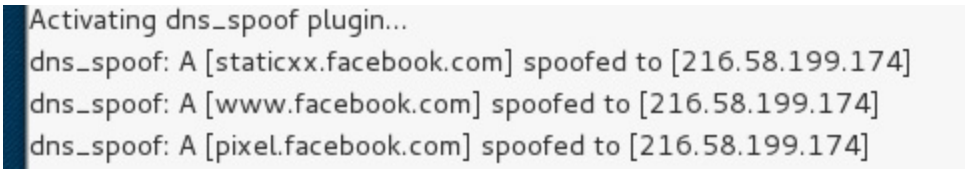
Redirect
Step 3 – Now save this file and exit by saving the file. Use “ctrl+x” to save the file.

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.

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

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.

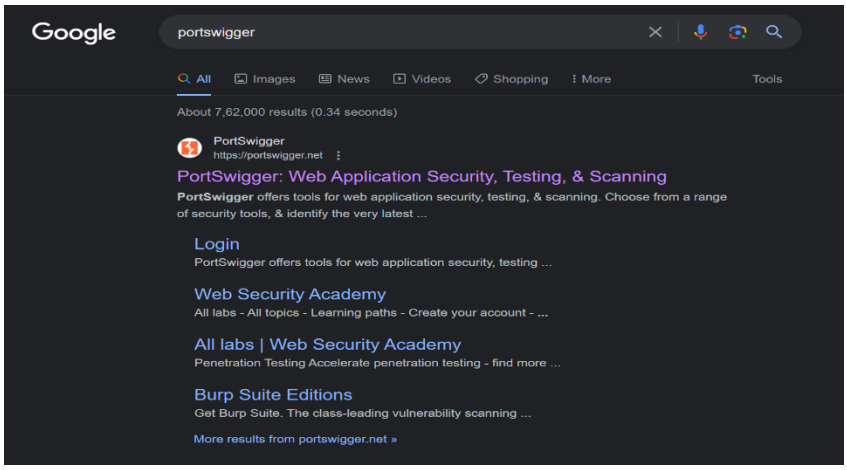
Experiment -6

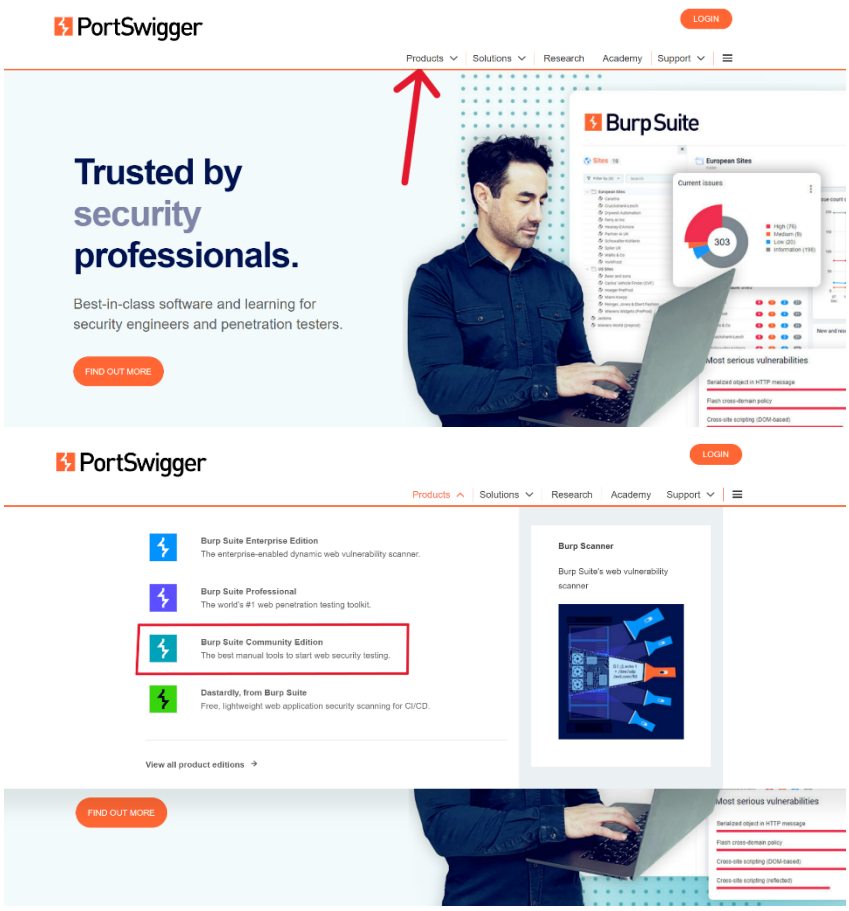
Aim: To Perform Web Application Assessment with Nikto & Burpsuite

Description :

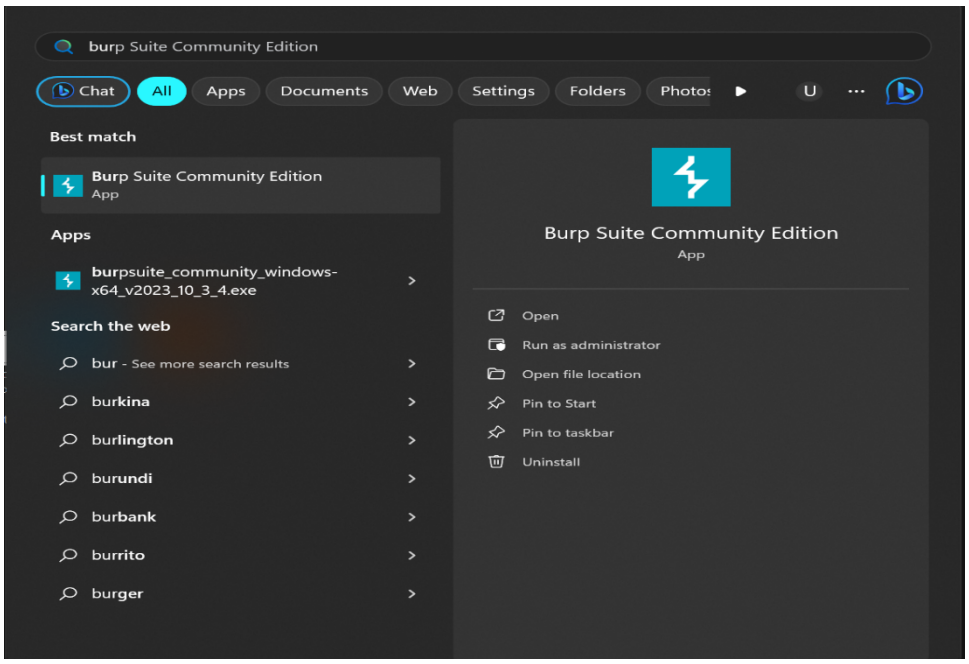
Burp Suite

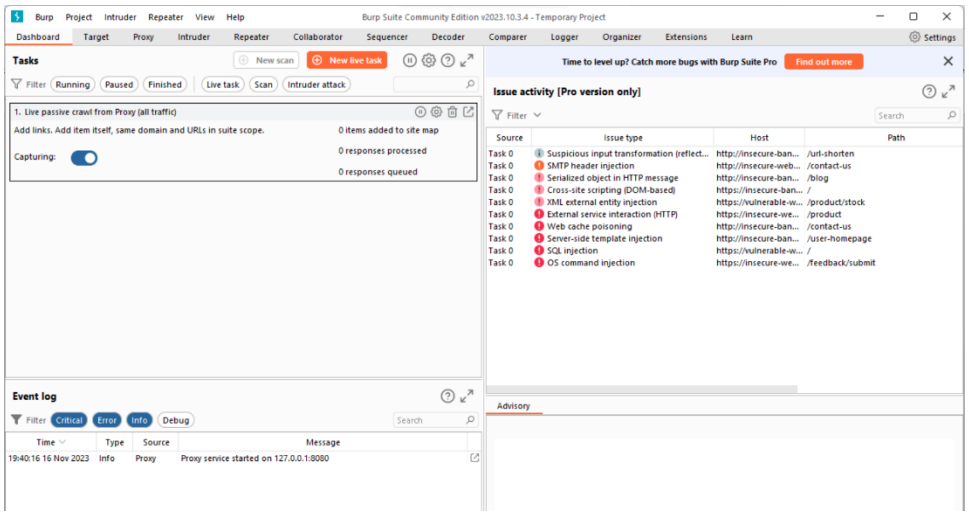
Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger, which is also the alias of its founder Dafydd Stuttard. Burp Suite aims to be an all-in-one set of tools and its capabilities can be enhanced by installing add-ons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





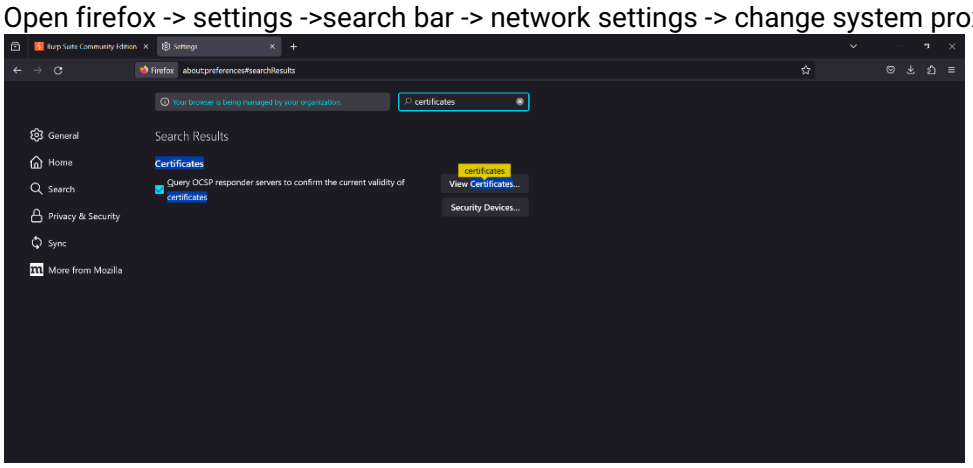
Install Burp suite
Click on Windows button and search burp suite ->Click on Next -> start burp

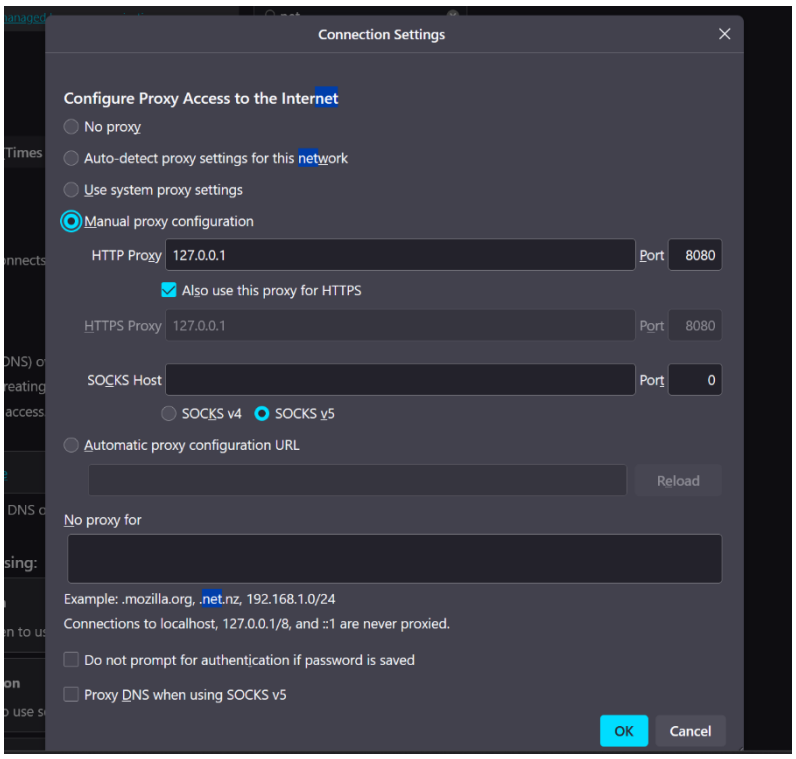




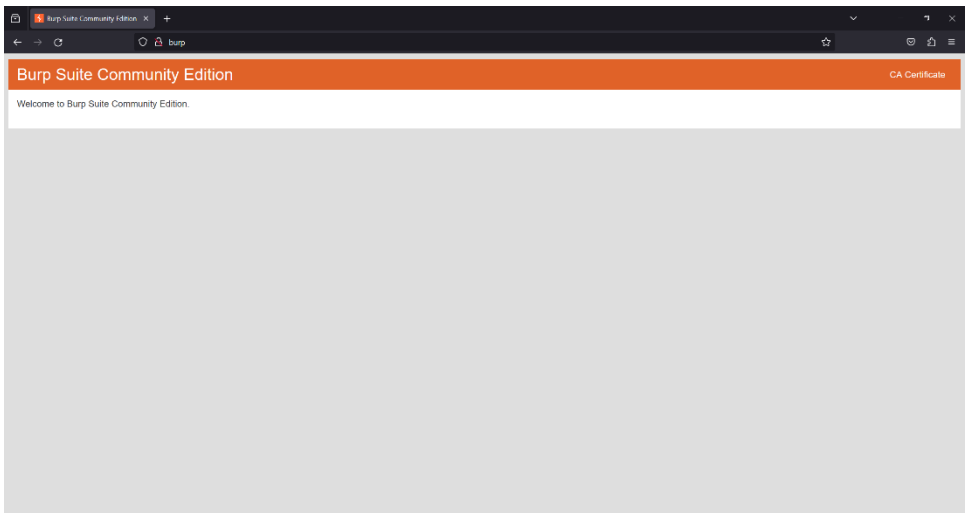
In burp suite window -> Dashboard -> Issue activity -> event log -> Targets display here

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

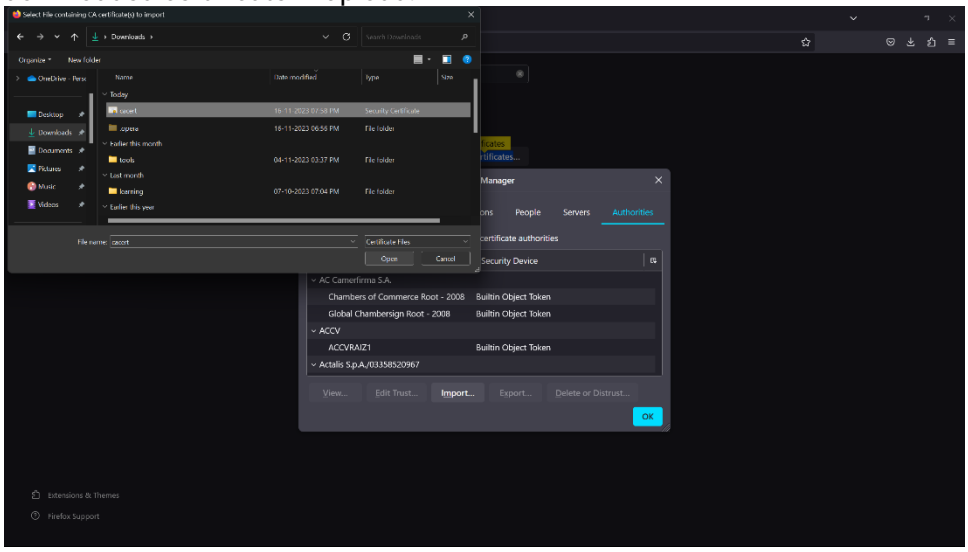




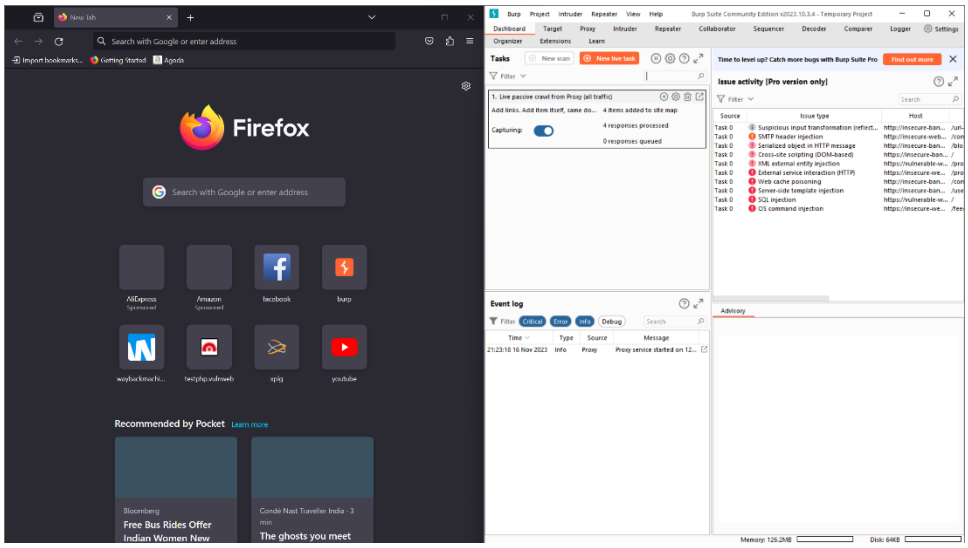
In a new tab url type http://burp -> press enter
Click on CA certificate which is displayed at right top
It downloads the certificate



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

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
```

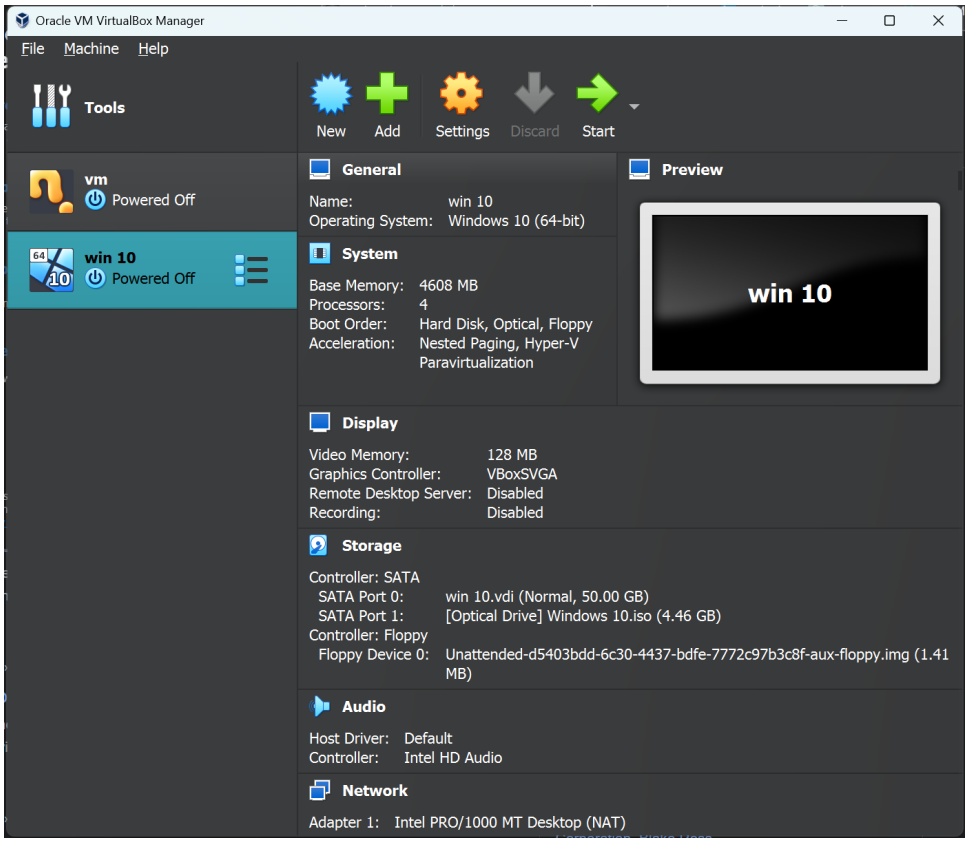
To verify that the Nikto website vulnerability scanner is installed and ready for use, run the command:

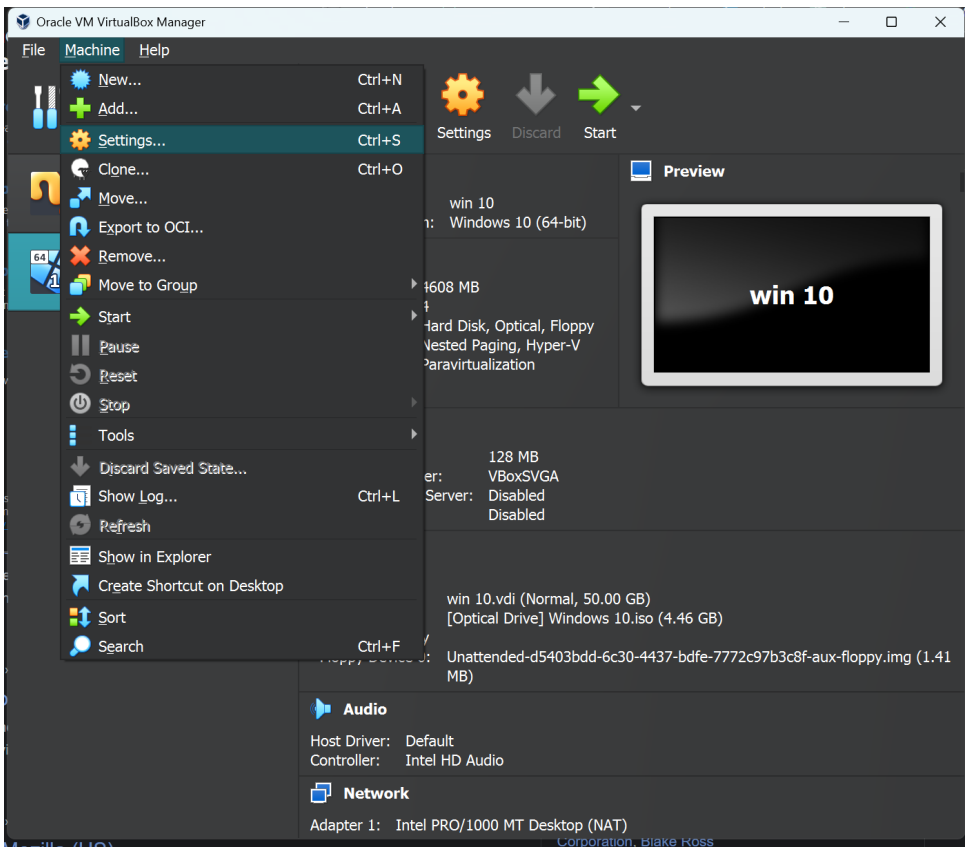
```
# nikto
```

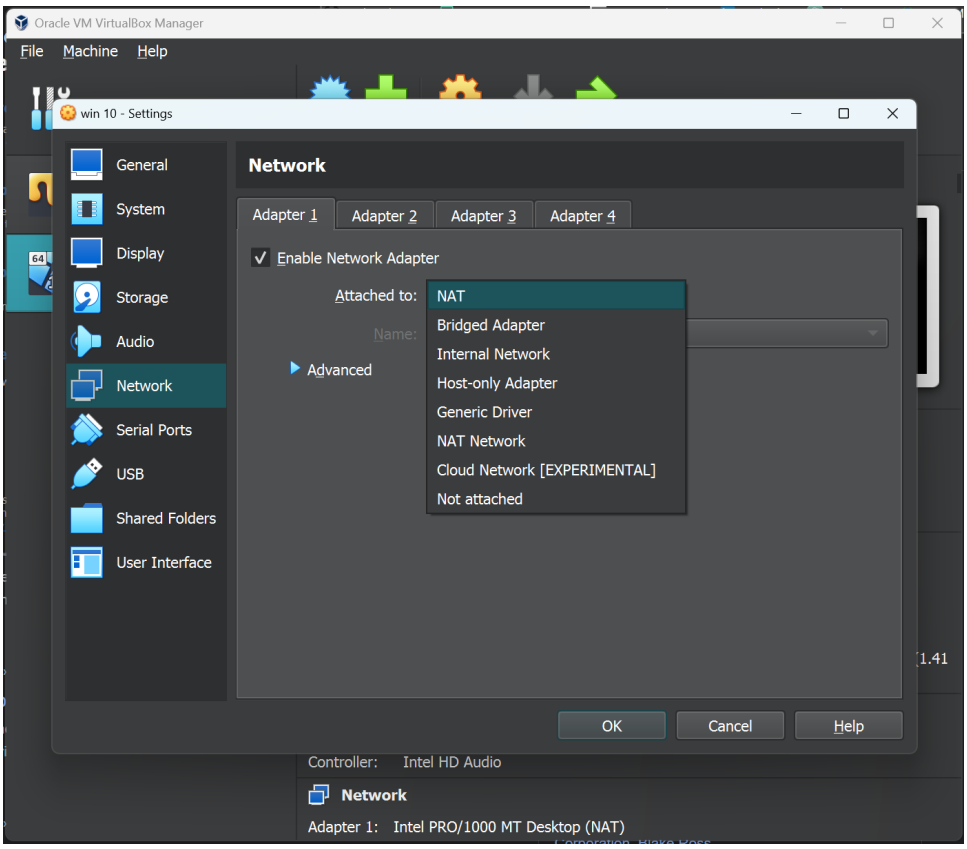
```
~# nikto gniindia.org
```

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

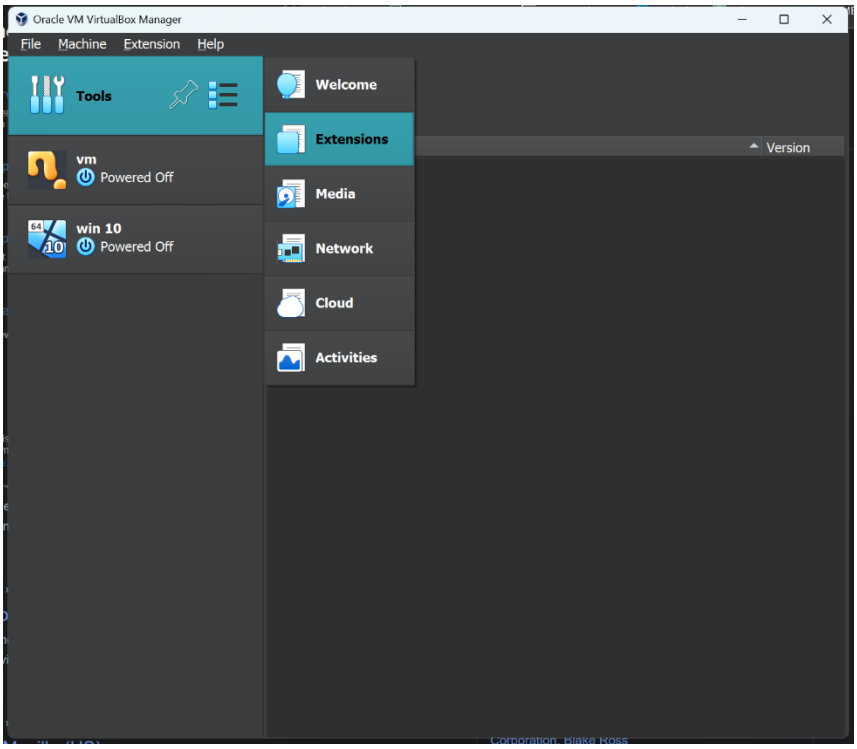
In VM virtual box -> network -> Bridge adapter -> Ok

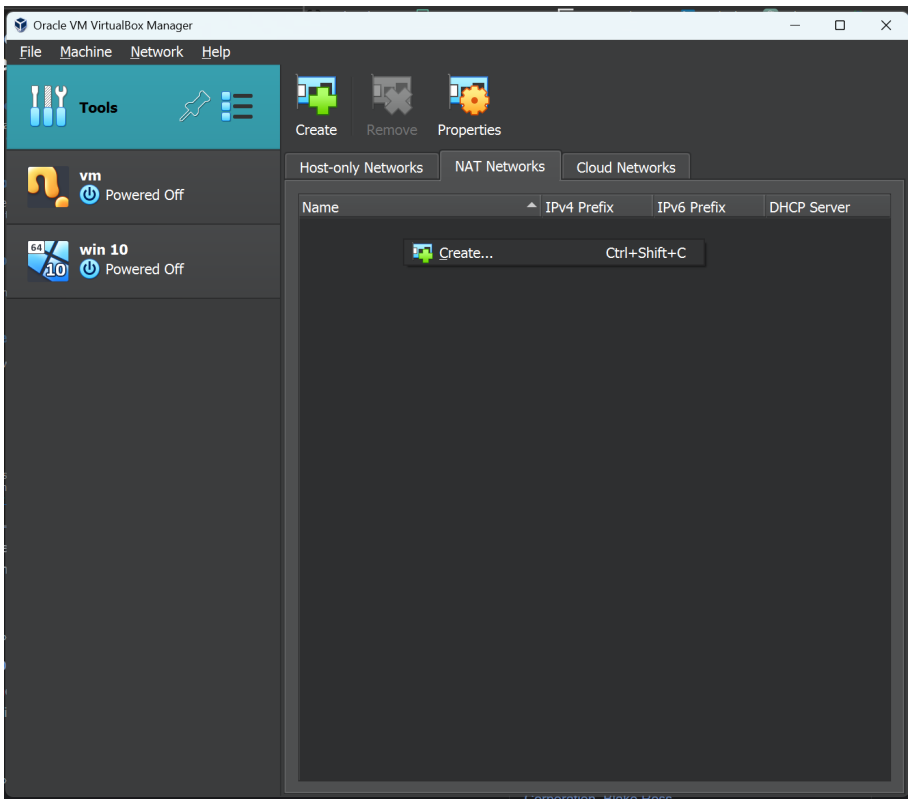

Oracle VM VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Start
vm
Powered Off
win 10
Powered Off
General
Name: win 10
Operating System: Windows 10 (64-bit)
System
Base Memory: 4608 MB
Processors: 4
Boot Order: Hard Disk, Optical, Floppy
Acceleration: Nested Paging, Hyper-V
Paravirtualization
Preview
win 10
Display
Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: win 10.vdi (Normal, 50.00 GB)
SATA Port 1: [Optical Drive] Windows 10.iso (4.46 GB)
Controller: Floppy
Floppy Device 0: Unattended-d5403bdd-6c30-4437-bdfe-7772c97b3c8f-aux-floppy.img (1.41 MB)
Audio
Host Driver: Default
Controller: Intel HD Audio
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)


Oracle VM VirtualBox Manager
File Machine Help
New... Ctrl+N
Add... Ctrl+A
Settings... Ctrl+S
Clone... Ctrl+O
Move...
Export to OCI...
Remove...
Move to Group
Start
Pause
Reset
Stop
Tools
Discard Saved State...
Show Log... Ctrl+L
Refresh
Show in Explorer
Create Shortcut on Desktop
Sort
Search Ctrl+F
Settings Discard Start
Preview
win 10
Audio
Host Driver: Default
Controller: Intel HD Audio
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)



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