CEH Group 3

Name: ARYAN (6604675)

Group: 03

Network Penetration Testing with Real-World Exploits and Security Remediation

Project objectives

Introduction

Theory about the project

Project requirements

Two Operating System

1. Kali Linux (Attacking machine)
2. Metasploitable machine (Target Machine)

Tools Details

1. Scanned a range of network using nmap and its different switches
2. Machine exploit exampled by Metaspoitable and Kali Linux
    a. Exploit through vsftpd 2.3.4
    b. Exploit through brute-force ssh login
    c. Exploit through VNC login and VNC Window
3. Created a new user and cracked the password with John The Reaper

Tasks

Network Scanning

Task 1: Basic Network Scan

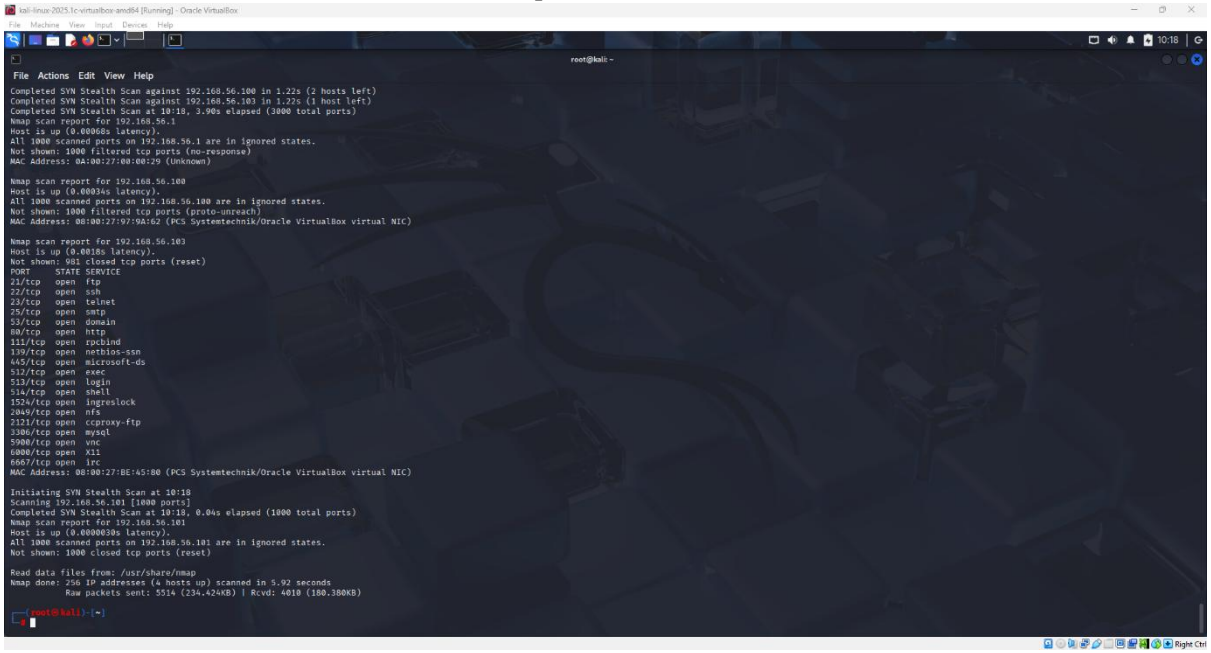
Step 1: Open a terminal on your Kali Linux machine.

Step 2: Run a basic scan on your local network.

nmap -v 192.168.56.0/24

Expected Output: A list of devices on the network, their IP addresses, and the open ports. This -v Option will show a detailed view of the running scan.

Ouput of the Scan



<u>RECON</u>

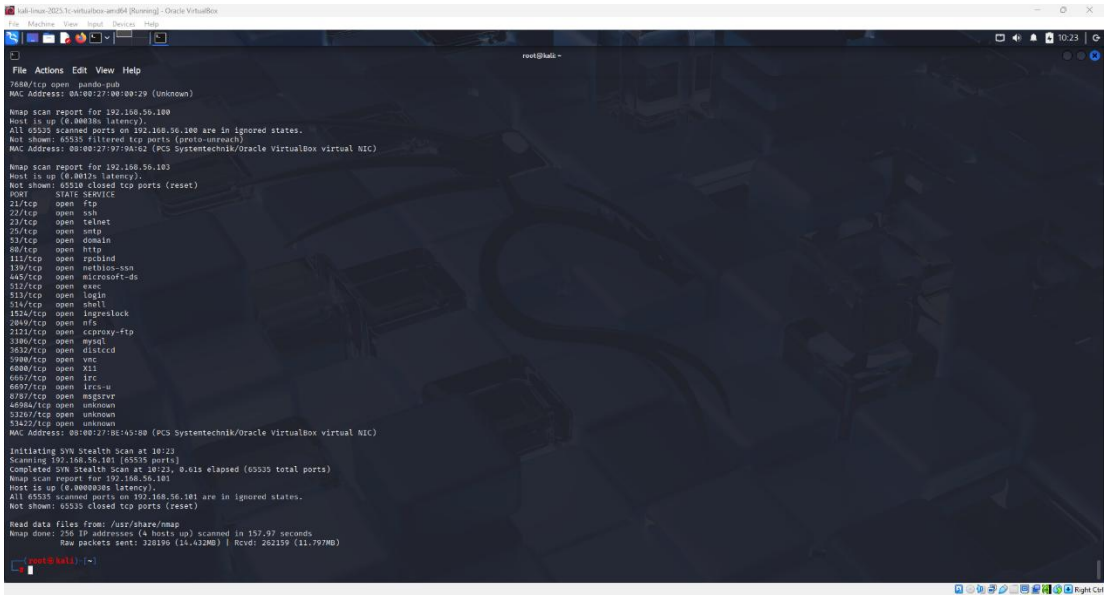
Task 1: Scanning for hidden Ports

Step 1: To scan for hidden ports, we have to scan whole range of ports on that specific targeted ip address.

nmap -v -p- 192.168.56.103

Expected Output: A list of hidden ports with services.

Output



Total Hidden Ports = 7

List of hidden ports

1

2

3

4

5

6

7

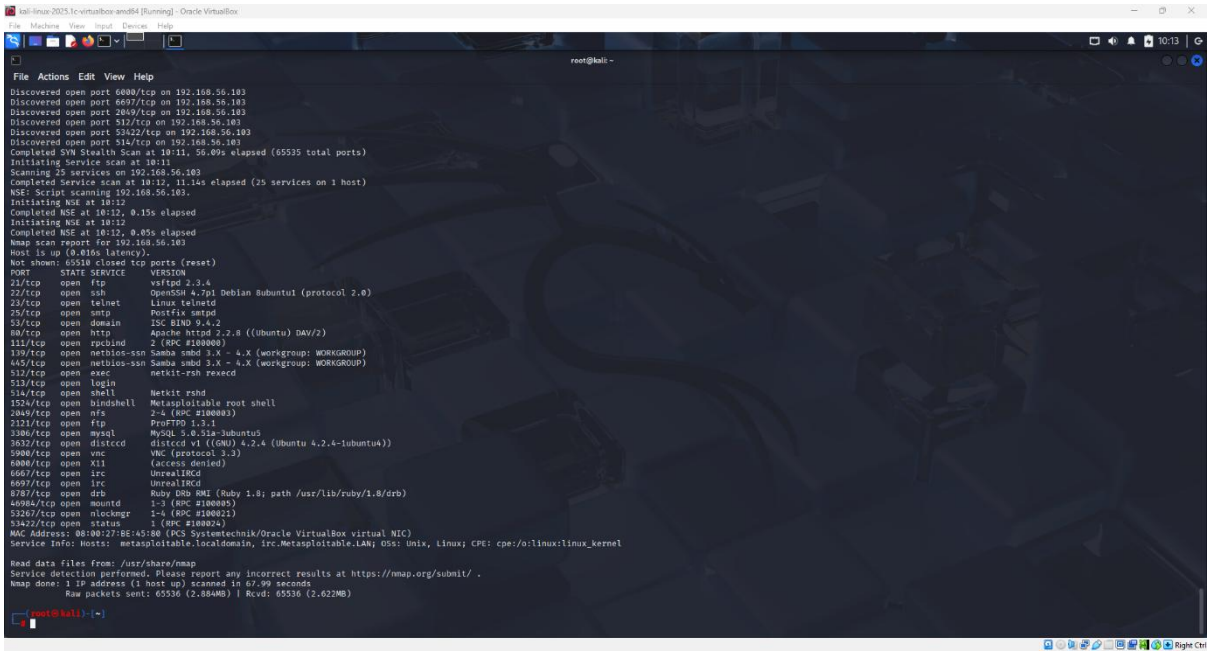
Task 2: Service Version Detection

Step 1: Use the -sV option to detect the version of services running on open ports:

nmap -v -sV 192.168.56.103

Expected Output: A detailed list of open ports and the services running on them, including version information.

Output



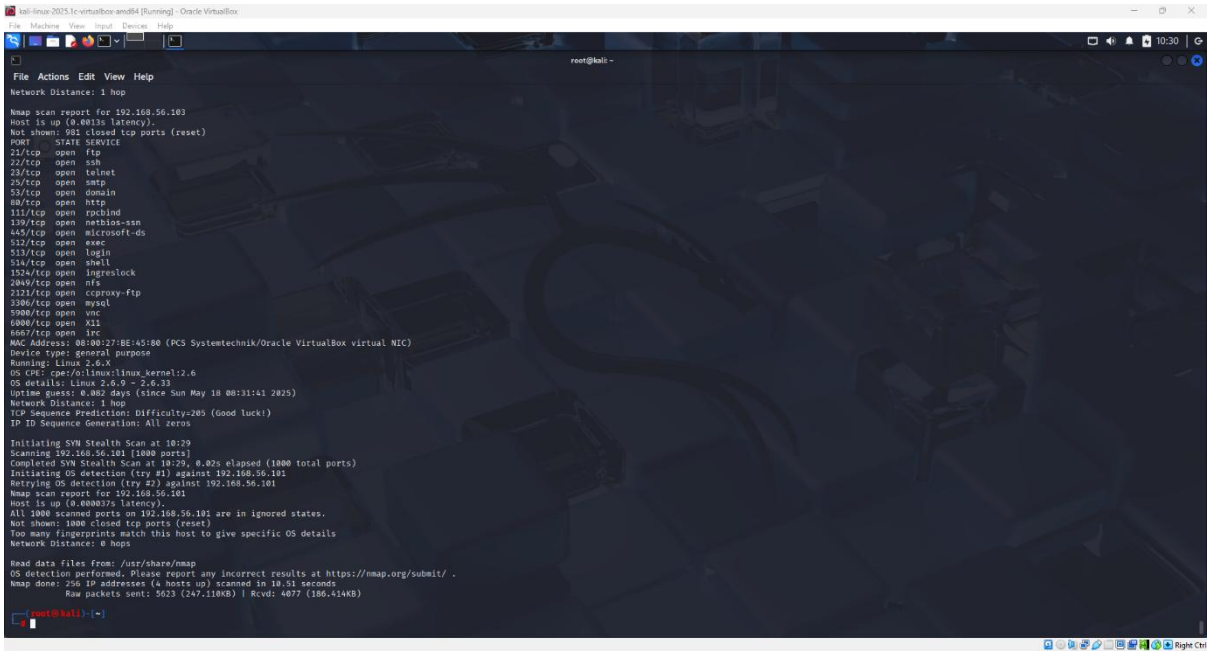
Task 3: Operating System Detection

Step 1: Use the -O option to detect the operating systems of devices on the network:

Nmap -v -O 192.168.56.103

Expected Output: The operating system details of the devices on the network.

Output



<u>ENUMERATION</u>

Target IP Address ENTER_192.168.56.103

Operating System Details (Nmap scan report for 192.168.56.103

Host is up (0.0013s latency).

```
Not shown: 981 closed tcp ports (reset)
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
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
MAC Address: 08:00:27:BE:45:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.082 days (since Sun May 18 08:31:41 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=205 (Good luck!)
IP ID Sequence Generation: All zeros

Initiating SYN Stealth Scan at 10:29
Scanning 192.168.56.101 [1000 ports]
Completed SYN Stealth Scan at 10:29, 0.02s elapsed (1000 total ports)
```

Initiating OS detection (try #1) against 192.168.56.101

Retrying OS detection (try #2) against 192.168.56.101

Nmap scan report for 192.168.56.101

Host is up (0.000037s latency).

All 1000 scanned ports on 192.168.56.101 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

Read data files from: /usr/share/nmap

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

Nmap done: 256 IP addresses (4 hosts up) scanned in 10.51 seconds

Raw packets sent: 5623 (247.110KB) | Rcvd: 4077 (186.414KB))

MAC Address: 00:0C:29:5D:FE:0B (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

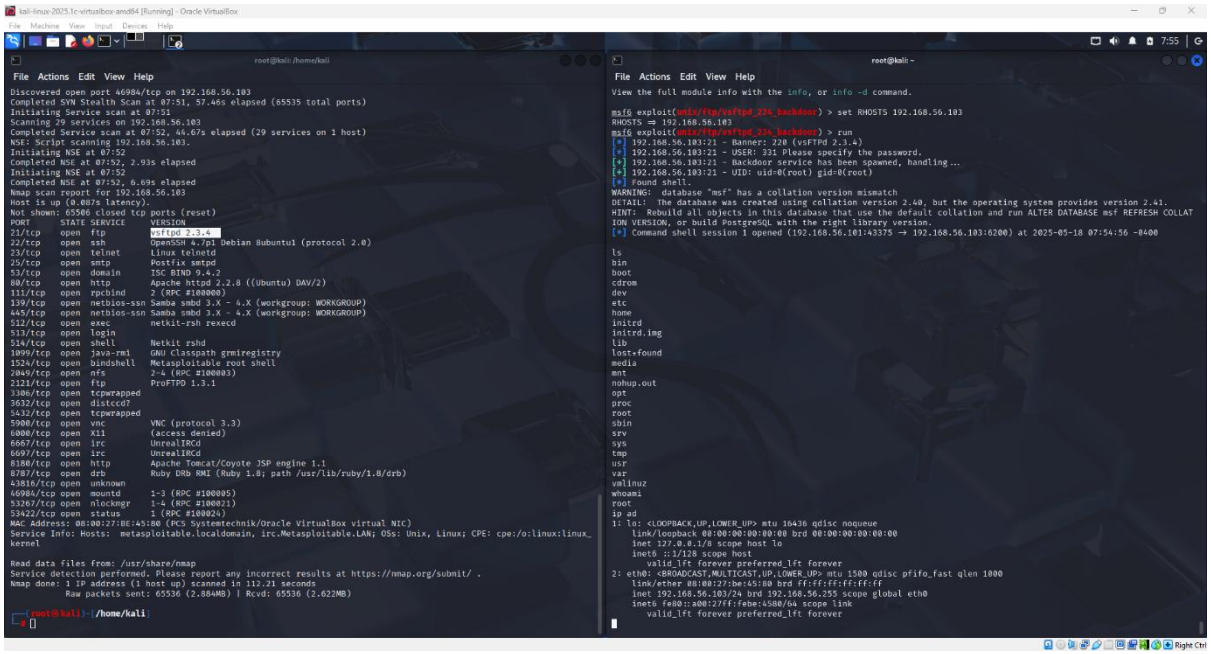
OS details: Linux 2.6.9 - 2.6.33

Services Version with open ports (LIST ALL THE OPEN PORTS EXCLUDING HIDDEN PORTS)

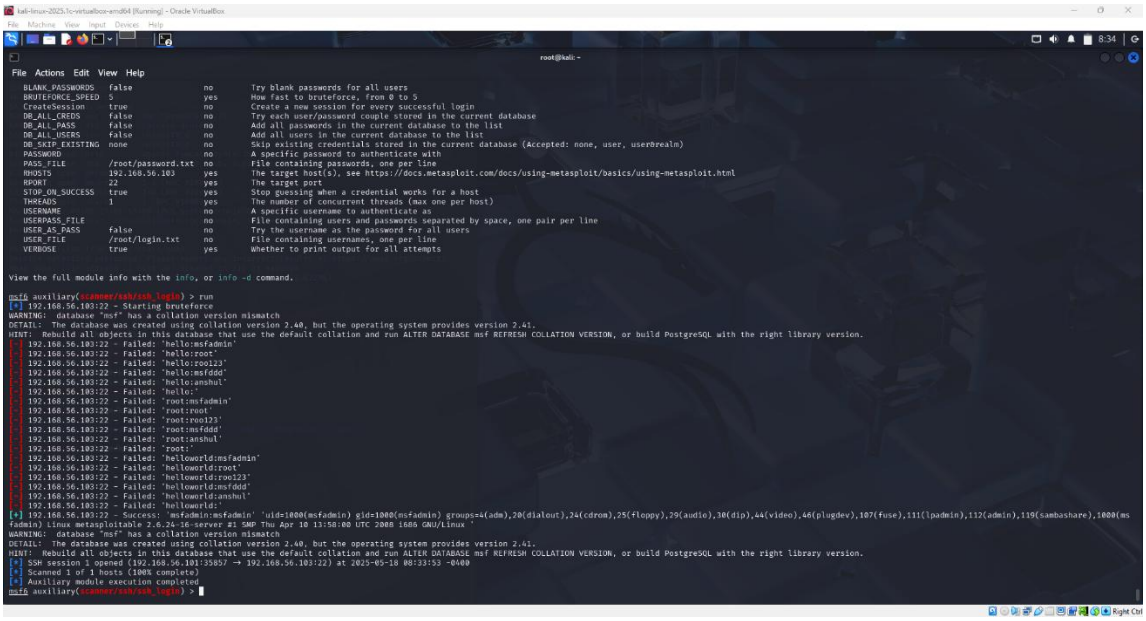
PORT	STATE	SERVICE VERSION
21/tcp	open ftp	vsftpd 2.3.4
22/tcp	open ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

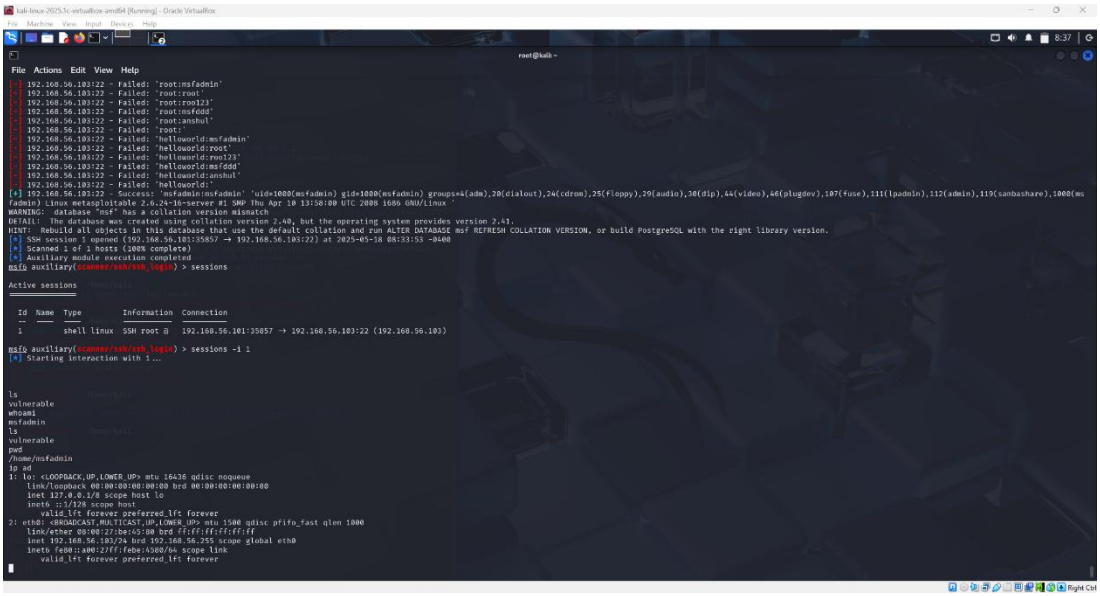
Task 4- Exploitation of services

1. **GAINING ROOT ACCESS THROUGH VSFTPD 2.3.4**

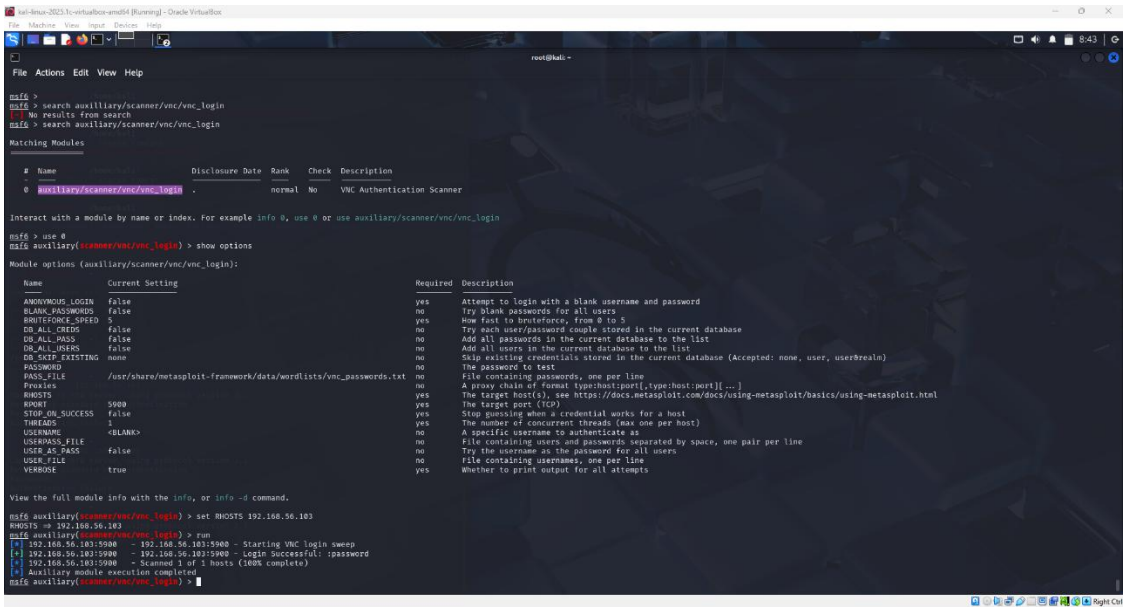


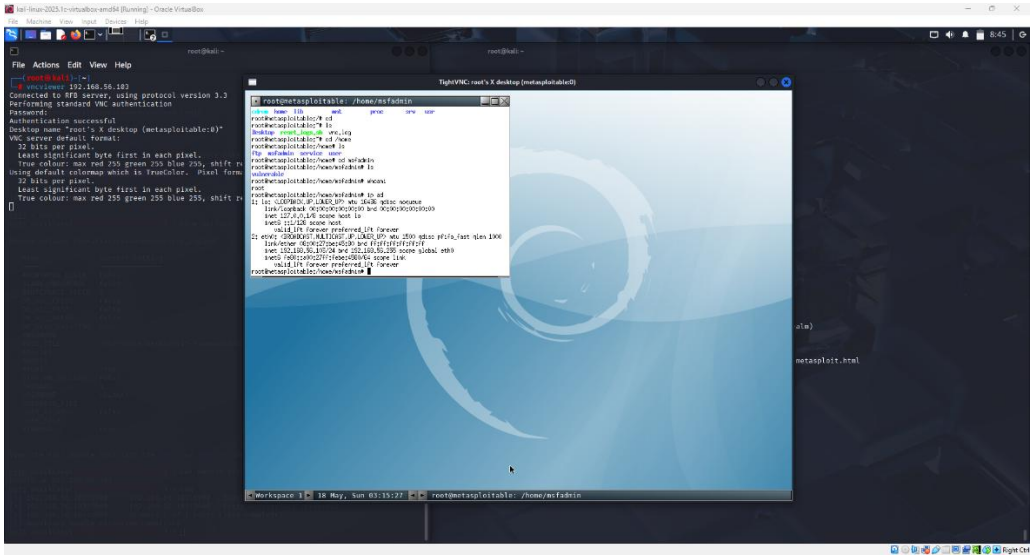
2. GAINING ROOT ACCESS THROUGH SSH AND BRUTE FORCE LOGIN





3. GAINING ACCESS THROUGH VNC LOGIN AND VNC WINDOW





Task 5 - Create user with root permission

adduser **aryan**

Set a simple password example 12345 or hello or 987654321

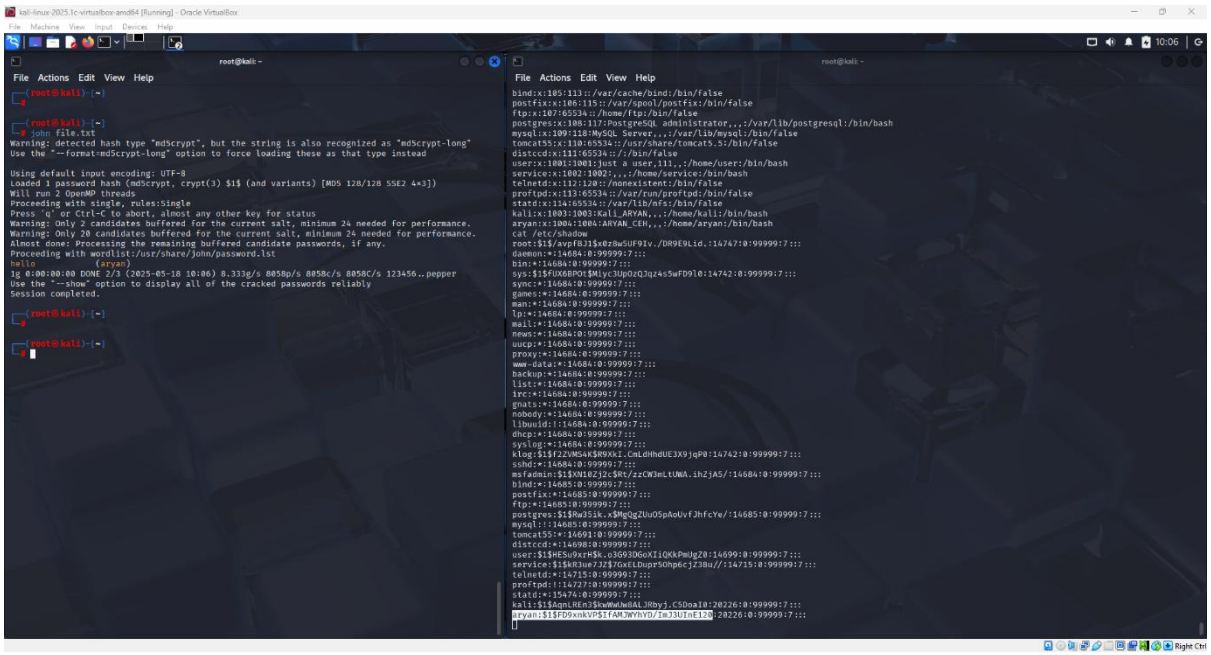
NOTE- Every student have to use different password

Get the details of user in /etc/passwd

Enter details of the new user you have added in Metasploit (example ansh:x:1001:1001:Anshul,,,:/home/ansh:/bin/bash)

Get the details of password hash in /etc/shadow

Hash ansh:$1$8nWuasXV$pk6ZABfqT9NoHv1pPX8Rj.



Task 6 - Cracking password hashes

Store the password hash in a text file

Filename with screenshot attached

Cracking password with prebuilt wordlist of john in default mode

John filename

To display the cracked password of the hash

John filename –show

Attach screenshot of cracked password

Major Learning From this project

When exploiting the **Metasploitable** vulnerable machine using **Kali Linux**, we step into the shoes of a real-world attacker, not to cause harm, but to **understand the anatomy of vulnerability, the fragility of misconfigured services**, and the power of information in the wrong hands. Through **vsftpd**, we learn how **backdoored services** can silently provide attackers with root shells—highlighting the importance of keeping software up-to-date and scanning for malicious code even in "official" packages. **SSH login attacks** teach us the value of **weak or reused credentials**, where brute force and default passwords can crack entry wide open—underscoring why security policies must enforce strong password hygiene and monitoring. When breaking into the **VNC window**, we see how remote desktop services, when **left open without authentication or with default credentials**, become gateways for total GUI-based control—making it painfully obvious how dangerous exposed ports are.

Diving deeper, tools like **John the Ripper** show us the raw reality of password cracking. We learn how **hashes are not enough** if the underlying passwords are weak or commonly used. John teaches us that **passwords are only as strong as the user's imagination**, and that security doesn't end at encryption—it begins with behavior.

In the grand scheme, this entire exercise isn't just about exploiting a machine—it's a brutal **mirror reflecting the laziness, ignorance, and misconfigurations** that plague real-world systems.