

Assignment

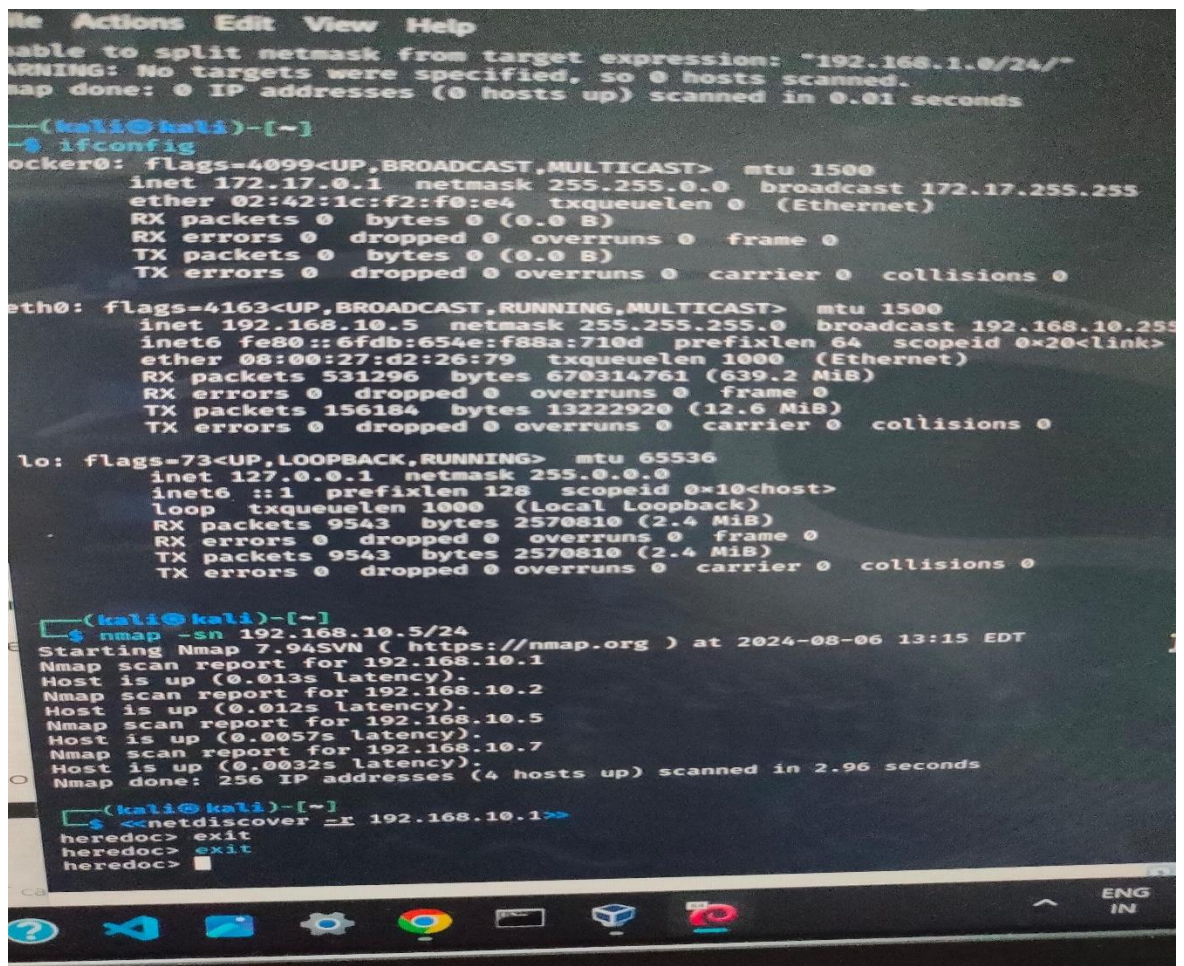
Name: Tanishq Kanare

Batch: CS-EH July 2024 batch

Task: To hack the username and password of SkyTower Virtual machine

Procedure:

- I have hacked the username and password of SkyTower Virtual Machine using Kali Linux vm.
- Firstly, I found out the ip address of kali linux which came out as attached in screenshot below:



```
File Actions Edit View Help
Unable to split netmask from target expression: "192.168.1.0/24/"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.01 seconds

--(kali@kali)-[~]
$ ifconfig
lo: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 127.0.0.1 netmask 255.255.0.0 broadcast 127.0.0.1
    ether 02:42:1c:f2:f0:e4 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

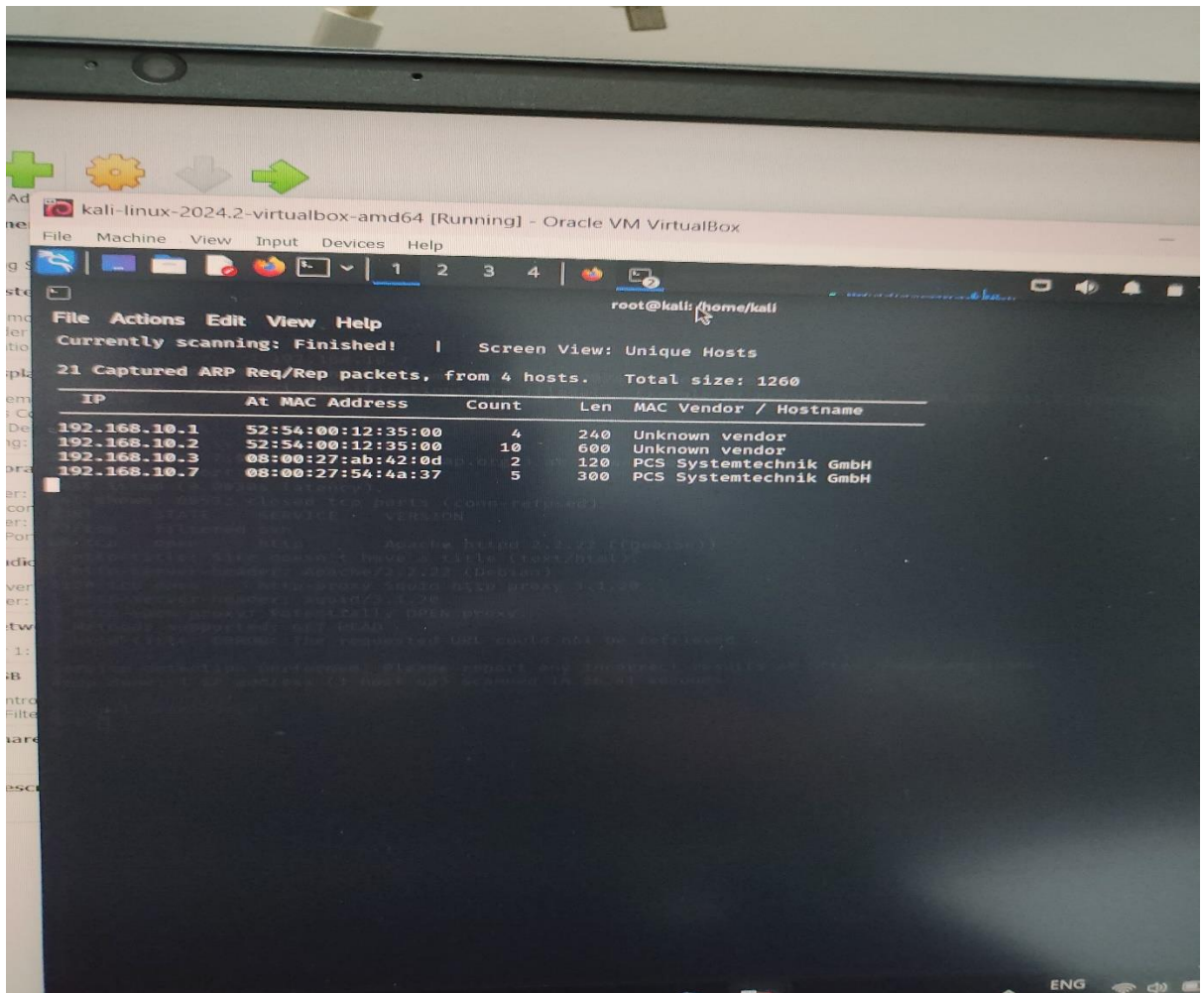
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.5 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::6fdb:654e:f88a:710d prefixlen 64 scopeid 0<link>
    ether 08:00:27:d2:26:79 txqueuelen 1000 (Ethernet)
    RX packets 531296 bytes 670314761 (639.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 156184 bytes 13222920 (12.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 9543 bytes 2570810 (2.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9543 bytes 2570810 (2.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

--(kali@kali)-[~]
$ nmap -sn 192.168.10.5/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 13:15 EDT
Nmap scan report for 192.168.10.1
Host is up (0.013s latency).
Nmap scan report for 192.168.10.2
Host is up (0.012s latency).
Nmap scan report for 192.168.10.5
Host is up (0.0057s latency).
Nmap scan report for 192.168.10.7
Host is up (0.0032s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.96 seconds

--(kali@kali)-[~]
$ <<netdiscover -r 192.168.10.1>>
heredoc> exit
heredoc> exit
heredoc> █
```

- Then I tried to find out the IP address of SkyTower VM.
- For this I checked the MAC address of skytower from the network settings in virtual box and noted it down.
- Then I ran the command “netdiscover -r <ip of kali/24>”
- By this command I got the list of all the machines connected to NAT Network same as that of kali linux, as shown below.



- Then I matched the MAC Address of skytower with the corresponding ip and I found out that the ip address of skytower is: 192.168.10.7
- Then I ran the nmap scan for this ip to find out which ports are open which can be enumerated
- Then I found out that port 80 was open. The results are shown below:

```
(kali㉿kali)-[~]
└─$ nmap -sV --script=default, safe 192.168.10.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 16:41 EDT
Failed to resolve "safe".
Nmap scan report for 192.168.10.7
Host is up (0.0060s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    filtered ssh
80/tcp    open  http         Apache httpd 2.2.22 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Debian)
3128/tcp  open  http-proxy   Squid http proxy 3.1.20
|_http-server-header: squid/3.1.20
|_http-open-proxy: Potentially OPEN proxy.
|_Methods supported: GET HEAD
|_http-title: ERROR: The requested URL could not be retrieved

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 14.73 seconds

(kali㉿kali)-[~]
└─$
```

- Then I have done an automated vulnerability scan using the command :
sudo apt install openvas
sudo gvm-setup
sudo gvm-start

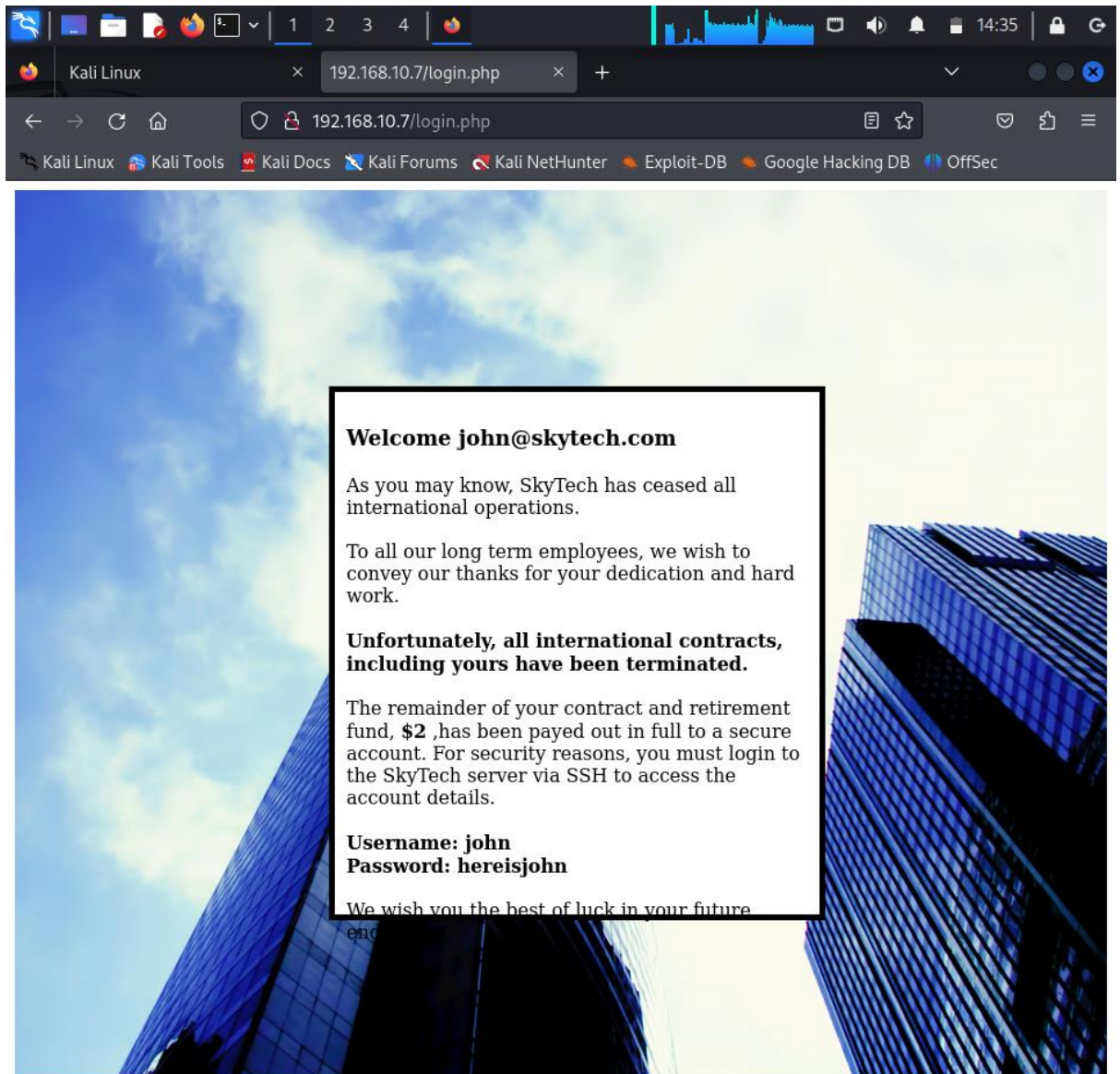
```
kali@kali: ~
File Actions Edit View Help
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.

(kali㉿kali)-[~]
└─$ sudo gvm-setup
[>] Starting PostgreSQL service
[>] Creating GVM's certificate files
[>] Creating PostgreSQL database
[*] Creating database user
[*] Creating database
[*] Creating permissions
CREATE ROLE
[*] Applying permissions
GRANT ROLE
[*] Creating extension uuid-oss
CREATE EXTENSION
[*] Creating extension pgcrypto
CREATE EXTENSION
[*] Creating extension pg-gvm
CREATE EXTENSION
[>] Migrating database
[*] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '03e079c2-38e1-4e61-ae2d-43c9b233887e'. Pass the
[*] Configure Feed Import Owner
[*] Define Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
[*] Downloading Notus files from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/notus/ to /var/lib/notus
rsync: read error: Connection reset by peer (104)
rsync error: error in socket IO (code 10) at io.c(806)
rsync: connection unexpectedly closed (31249 bytes received so far)
rsync error: error in rsync protocol data stream (code 12) at io.c(231)
[*] Downloading NASL files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/nasl/
to /var/lib/openvas/plugins
```

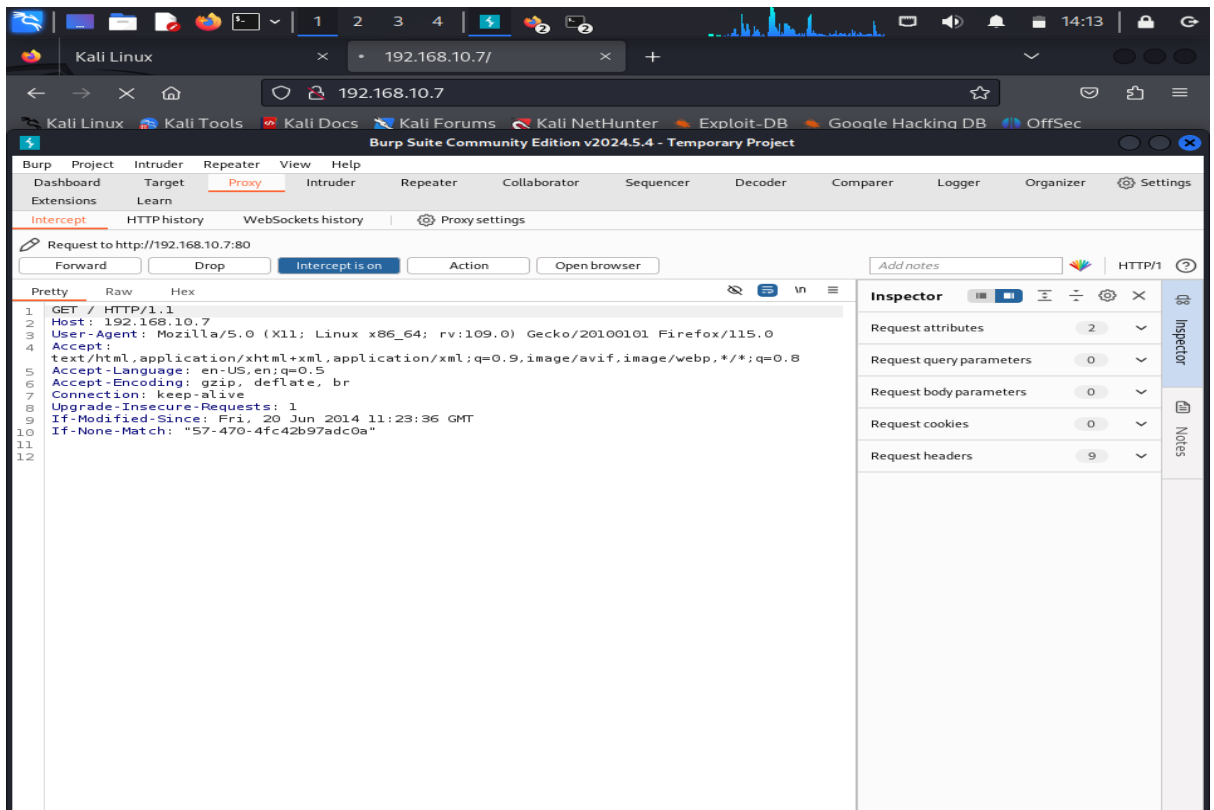

- Then I have done the exploitation using Metasploit framework and used the following commands:

```
kali@kali: ~  
File Actions Edit View Help  
└─27397 /usr/bin/python3 /usr/bin/osspd-openvas --config /etc/gvm/osspd-openvas.conf --log-config /etc/g  
vm/osspd-logging.conf  
└─27399 /usr/bin/python3 /usr/bin/osspd-openvas --config /etc/gvm/osspd-openvas.conf --log-config /etc/g  
vm/osspd-logging.conf  
  
Aug 06 16:54:29 kali systemd[1]: Starting ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas  
) ...  
Aug 06 16:54:31 kali systemd[1]: Started ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)  
. .  
  
[>] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...  
  
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: Use the edit command to open the currently active module  
in your editor  
  
.,;lx00KXXXXX0x!:. Welcome john@skytech.com  
o0WMMMMMMMMMMMMMMMMMMMMMMkd,  
'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,  
:KMHHHHHHHHHHHHHHHHHHHHHMMk:  
,KMHHHHHHHHHHHHHHHHHHHNNNNMMMMMMMMMMMMMMkX,  
lWMHHHHHHHHHHMMXd: .. :dKMHHHHHHHHMMMo  
xMHHHHHHHHMMMd. :oNMMMMMMMMMMk long term employees, we wish to  
oMMMMHHMMMX. dMMMMMMMMMx thanks for your dedication and hard  
.WMHHHHHHMM: :MMMMMMMMMM,  
xMMMMHHMMMo :lMMMMMMMMMO  
NMHHHHHHMMW ,cccccoMMMMMMMMWWlcccc;  
MMHHHHMMAX ;KMHHHHHHHHHHHHMMX: ll international contracts,  
NMHHHHHHMMW ;KMHHHHHHHHHHHHMMX: as have been terminated.  
xMHHHHHHMMMd ,OMMMMMMMMMMK;  
.WMHHHHHHMMMc 'OMMMMMMMO  
lMMMMHHMMMK. 'KMMO'  
dMMMMHHMMMd' eMMMMMMMMMMMNxc'.  
cMMMMMMMMMMMMMMWc  
;OMMMMMMMMMMMMMMMMo.  
.dNMMMMMMMMMMMo  
'oOWMMMMMMMo  
cdKO0K;  
  
Metasploit  
  
=[ metasploit v6.4.15-dev ]  
+ -- ==[ 2433 exploits - 1254 auxiliary - 428 post ]  
+ -- ==[ 1471 payloads - 47 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 >
```

- Also I have tried another method that was logging onto the skytech login page on firefox by searching <http://192.168.10.7>
- The below webpage appeared



- I intercepted the traffic using burpsuite as shown below

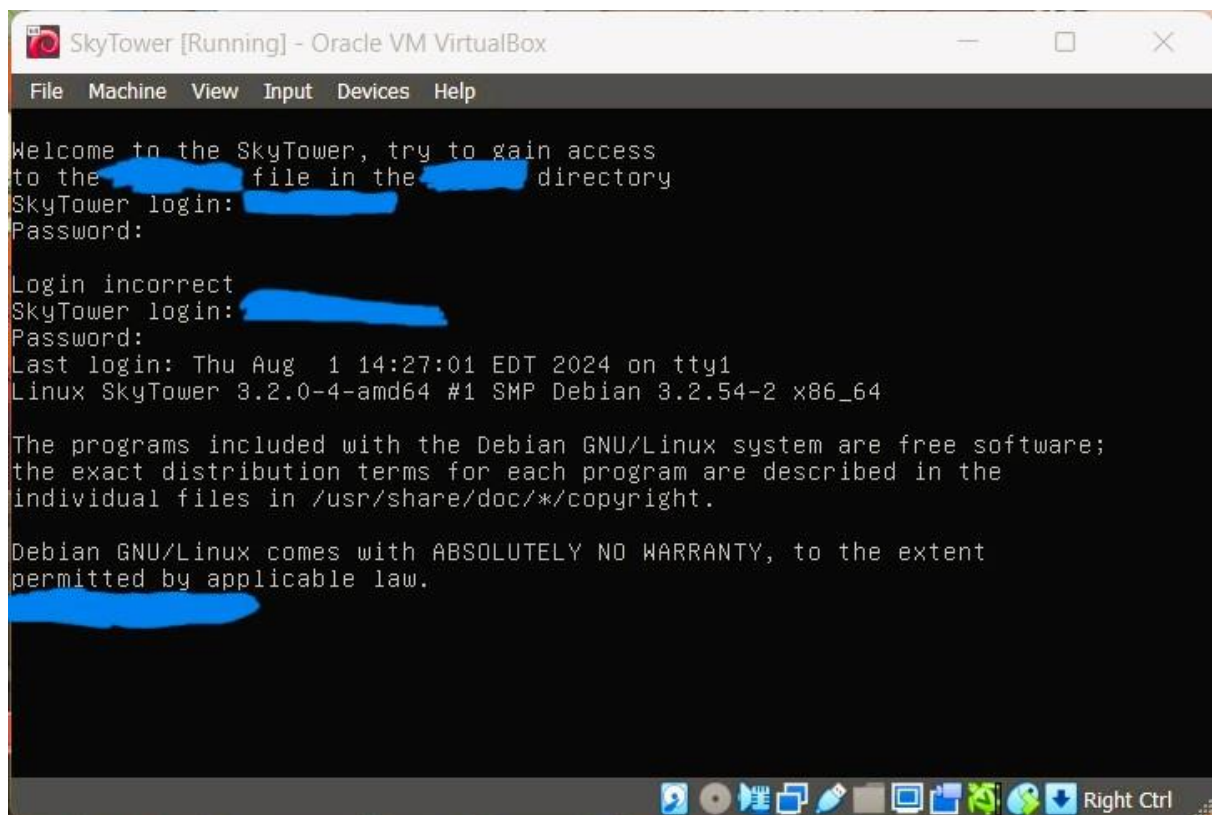


- Then I stored the code into a file and searched for passwords and username using proxychains command
- From the skyTech table I was getting

```
Tables_in_SkyTech bytes 1596 (1.5 KiB)
login errors 0 dropped 0 overruns 0 frame 0
id TX packet email 28 password 1596 (1.5 KiB)
1 TX error john@skytech.com hereisjohn
2 sara@skytech.com ihatethisjob
3 william@skytech.com senseable
```

- Logging in as sara we saw commands were executable
- Then I typed command sudo-l, then
- Sudo ls/accounts/../root
- There I saw flag.txt
- Then I typed sudo ls /accounts../root/flag.txt
- Then I got the root password=theskytower, and then I re-login
- And the final output came as

Congratz, have a cold one to celebrate!
root password is theskytower



The screenshot shows a terminal window titled "SkyTower [Running] - Oracle VM VirtualBox". The terminal displays a login prompt for "SkyTower". The user enters a username (redacted) and a password (redacted). The login is incorrect. The terminal then shows the last login time and the system information: "Linux SkyTower 3.2.0-4-amd64 #1 SMP Debian 3.2.54-2 x86_64". It also displays the Debian GNU/Linux warranty disclaimer. The terminal window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The bottom of the window shows a taskbar with various icons and the text "Right Ctrl".

```
Welcome to the SkyTower, try to gain access
to the [REDACTED] file in the [REDACTED] directory
SkyTower login: [REDACTED]
Password: [REDACTED]

Login incorrect
SkyTower login: [REDACTED]
Password: [REDACTED]
Last login: Thu Aug  1 14:27:01 EDT 2024 on tty1
Linux SkyTower 3.2.0-4-amd64 #1 SMP Debian 3.2.54-2 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
[REDACTED]
```