CTF Challenge

TDX-Arena: Breaking Hollywood

Ameen Abu Backer - GitHub

January 14, 2025

Contents

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

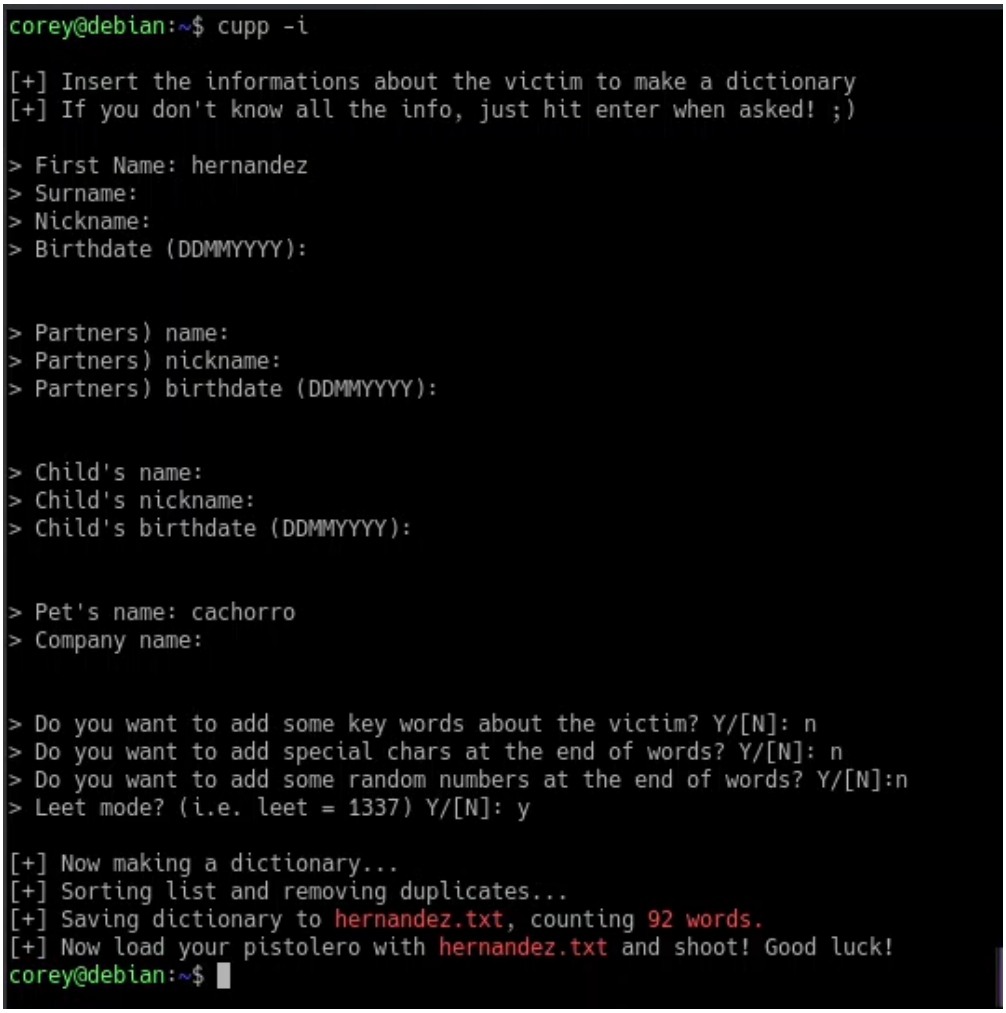
2 Enumeration

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`.



3 Exploitation

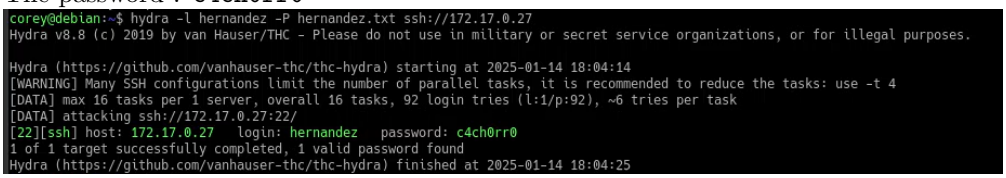
3.0.1 Brute-Forcing the SSH Service

- **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`



3.0.2 Logging into the Web Server

- **Credentials Found**: Username: `hernandez`, Password: `c4ch0rr0`
- **Command Used**:

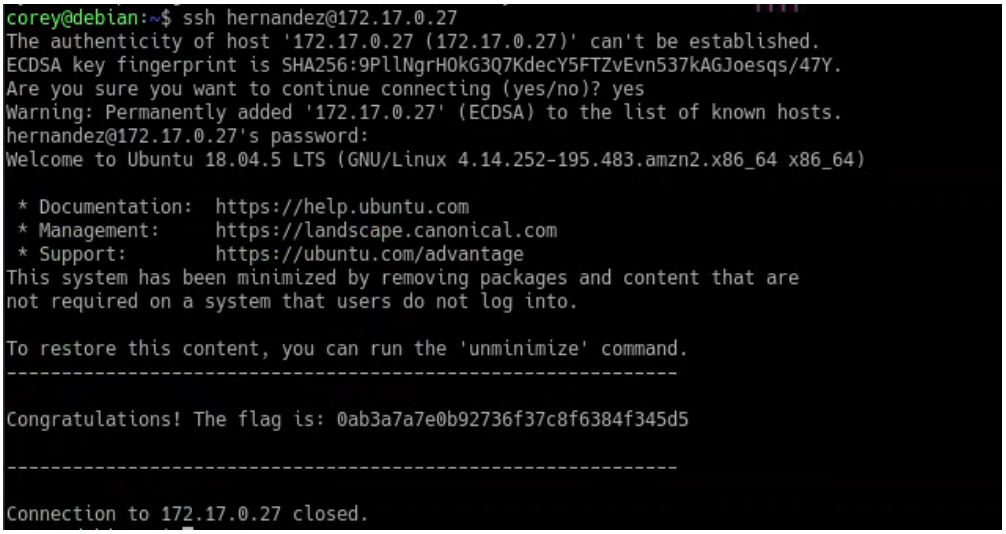
  ```
  ssh hernandez@172.17.0.27
  ```

  - Successfully logged into the server using the discovered credentials.

Successfully retrieved and noted the flag.

4 Solution

4.0.1 The Flag



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.