INTRODUCTORY:BREAKING HOLLYWOOD BY Monhal

MEDIUM

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.

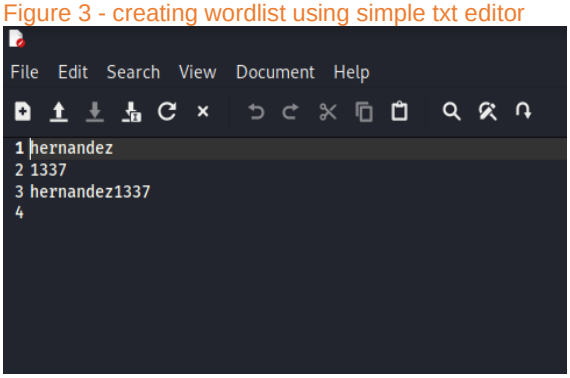
```
                          # User
                          # Passwords
                          # Profiler
                          [ Muris Kurgas | j0rgan@remote-exploit.org ]
                          [ Mebus | https://github.com/Mebus/]

[+] 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.

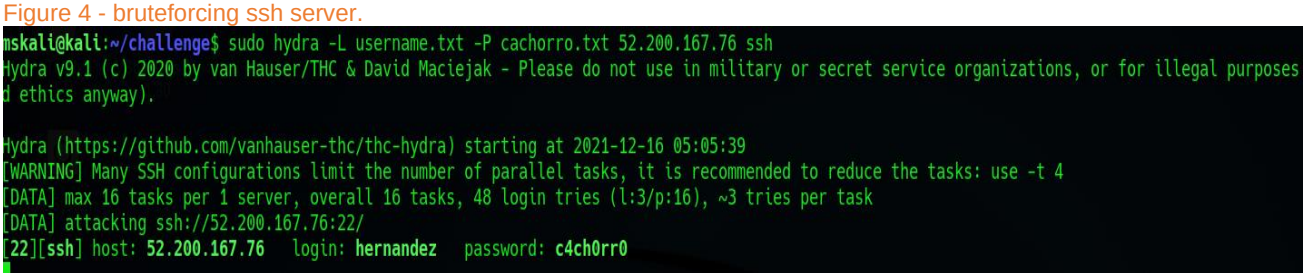
Creating a userlist according to the provided user information:

Figure 3 - creating wordlist using simple txt editor



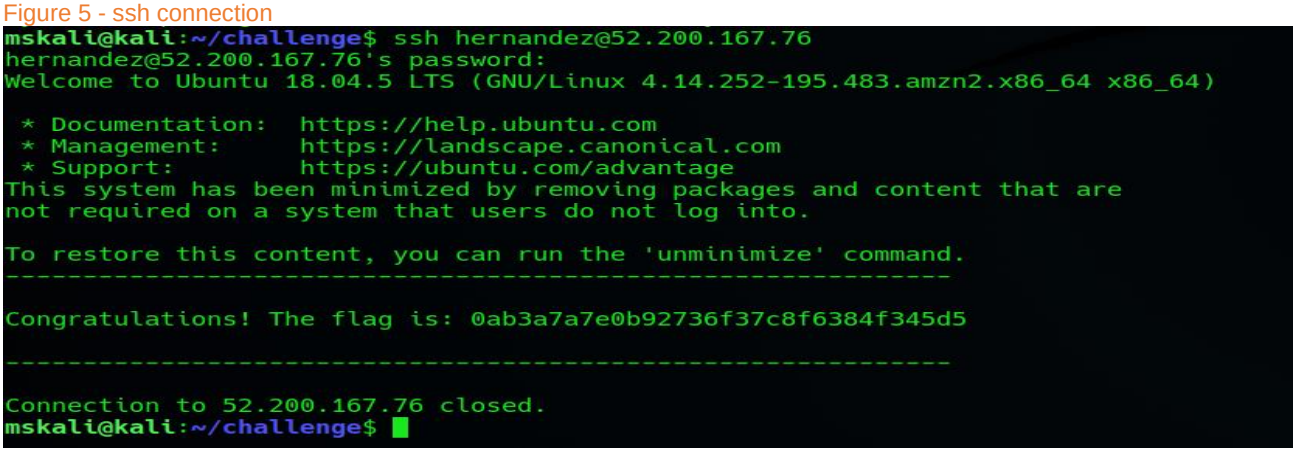
Now, we have two wordlists, one for the username and the second for the password.
Making an SSH connection Brute-Force using Hydra.

Figure 4 - bruteforcing ssh server.



We have a credentials; hernandez:c4ch0rr0
Using the supplied credentials in order to remotely login to the server using SSH

Figure 5 - ssh connection



CHALLENGE PWNED!

Please feel free to contact me on: **Monhalsarbouch@gmail.com**