HackerFrogs Afterschool
Network Hacking – Session 6

Class:
Network Hacking

Workshop Number:
AS-NET-06

Document Version:
1.75

Special Requirements:
Registered account
at tryhackme.com

Welcome to HackerFrogs Afterschool!

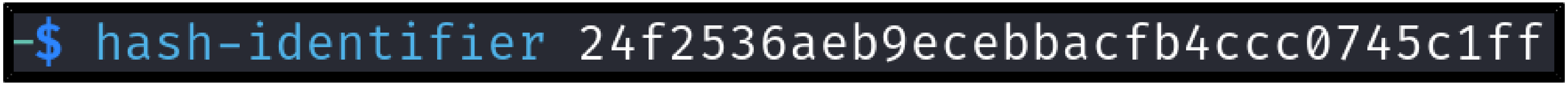
This is the sixth session for network hacking!

Let's go over the concepts we covered in the previous session!

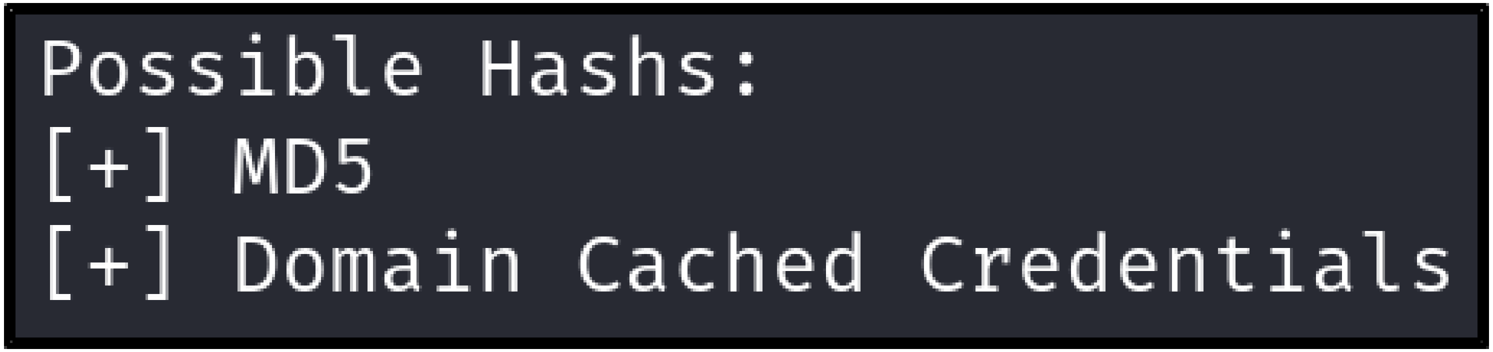
What is Password Cracking?

Password cracking is the act of determining the plaintext of a password hash by hashing a string and comparing it to the password hash

Identifying Hash Types



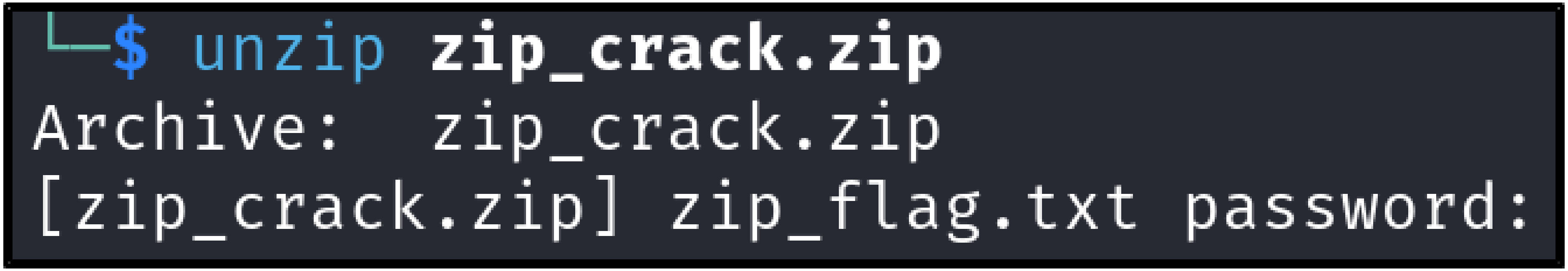
```
-$ hash-identifier 24f2536aeb9ecebbacfb4ccc0745c1ff
```



```
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials
```

A couple of different ways to identify the type of hash being used, including the CLI program, **hash-identifier**, and the **hashes.com** website

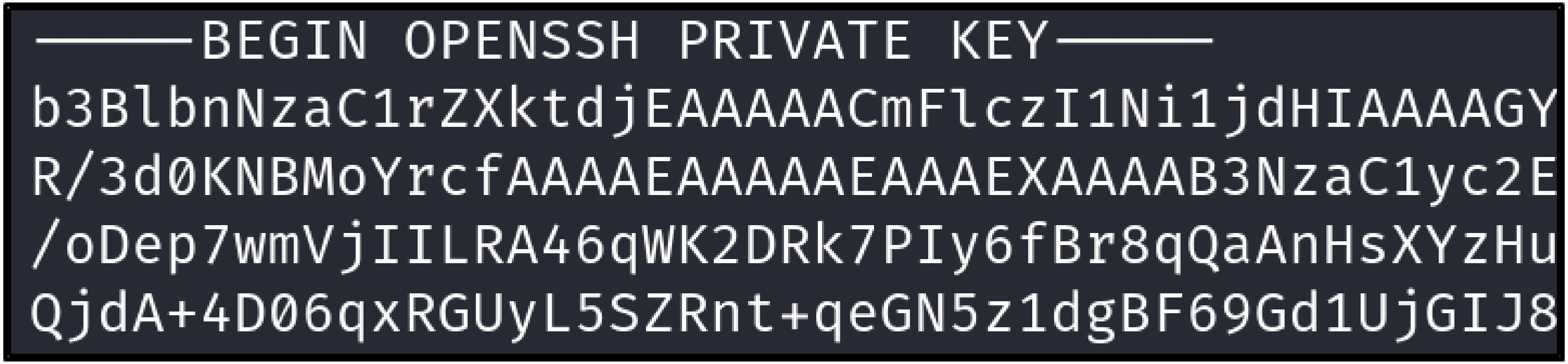
Cracking Zip File Password Hashes



```
└─$ unzip zip_crack.zip
Archive:  zip_crack.zip
[zip_crack.zip] zip_flag.txt password:
```

Zip files are a common file type that can be password protected, and we can extract the hash, then crack the password using a tool like John the Ripper

Cracking SSH Private Key Hashes



```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGY
R/3d0KNBMoYrcfAAAAEAAAAAEAAAEXAAAAB3NzaC1yc2E
/oDep7wmVjIILRA46qWK2DRk7PIy6fBr8qQaAnHsXYzHu
QjdA+4D06qxRGUyL5SZRnt+qeGN5z1dgBF69Gd1UjGIJ8
```

Another common file that can be cracked are the passphrases for SSH private keys, which allow users to login

This Session's Topics

- What are Brute Force Attacks?

- Brute Force Attacking a Login Page

- Brute Forcing Attacking SSH Login

What are Brute Force Attacks?

Brute force attacks are attempts to determine legitimate usernames and passwords on online services

Brute forcing is similar to, but not the the same as password cracking

Accessing TryHackMe

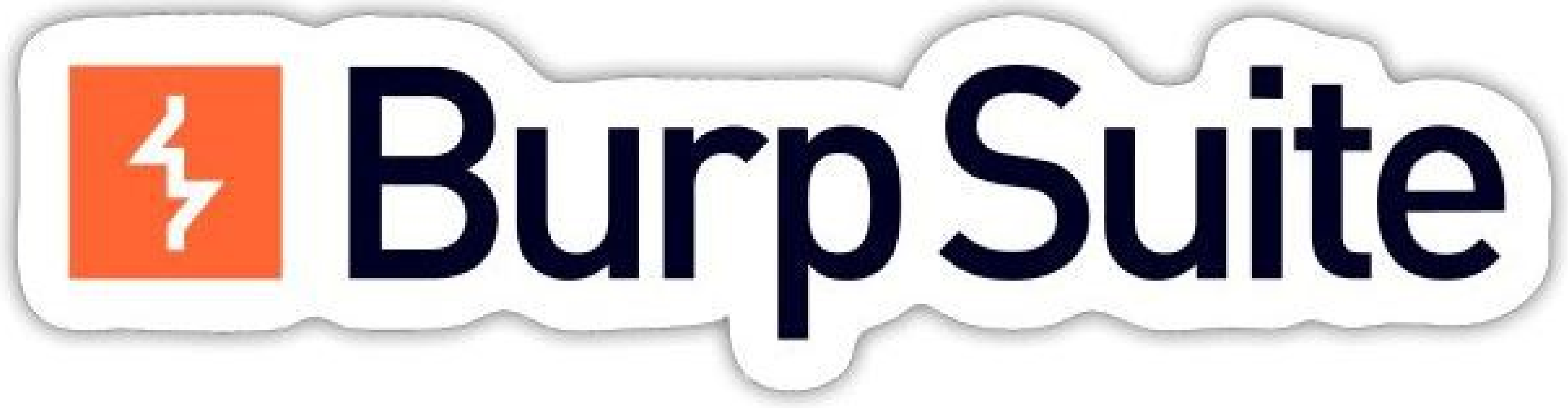
Let's access this TryHackMe room to learn about cracking passwords access:

https://tryhackme.com/room/hydra

Brute Force Attacking a Login Page

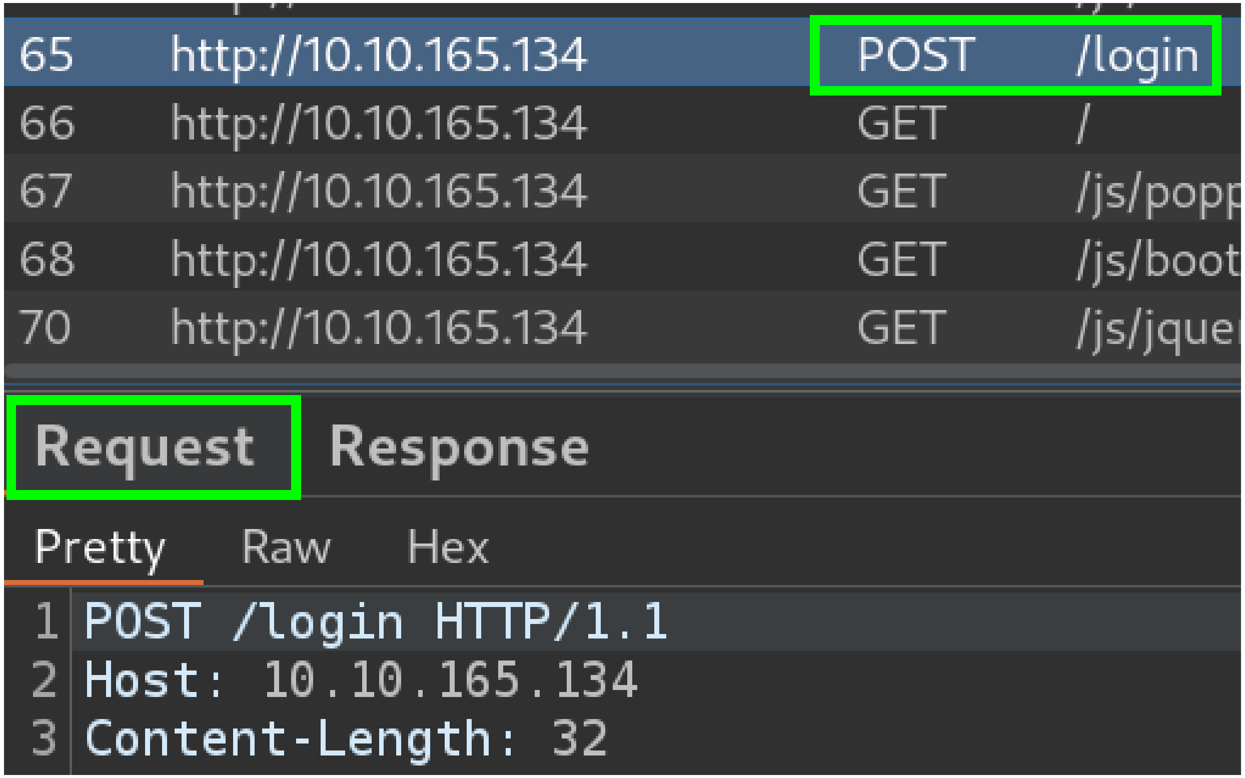
A very common target for brute forcing attacks are web app login pages, so let's learn how to do login page brute forcing attacks with the FFuF program!

Saving an HTTP Request with Burp



Burp Suite can be used to record HTTP request data, and it's convenient to pair this with CLI program like FFuF and SQLmap

Saving an HTTP Request with Burp

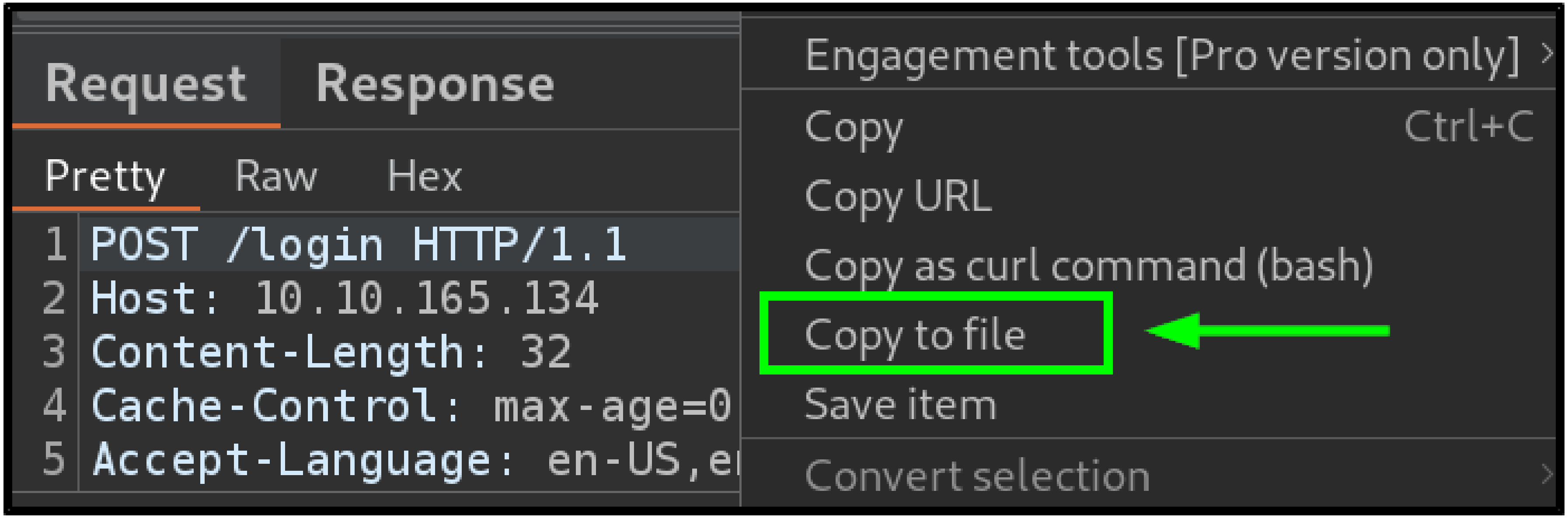


65	http://10.10.165.134	POST	/login
66	http://10.10.165.134	GET	/
67	http://10.10.165.134	GET	/js/popp
68	http://10.10.165.134	GET	/js/boot
70	http://10.10.165.134	GET	/js/jque

```
POST /login HTTP/1.1
Host: 10.10.165.134
Content-Length: 32
```

To save a request to a file, first open Burp Suite, then the Burp Suite browser, then record a test login on the desired web page

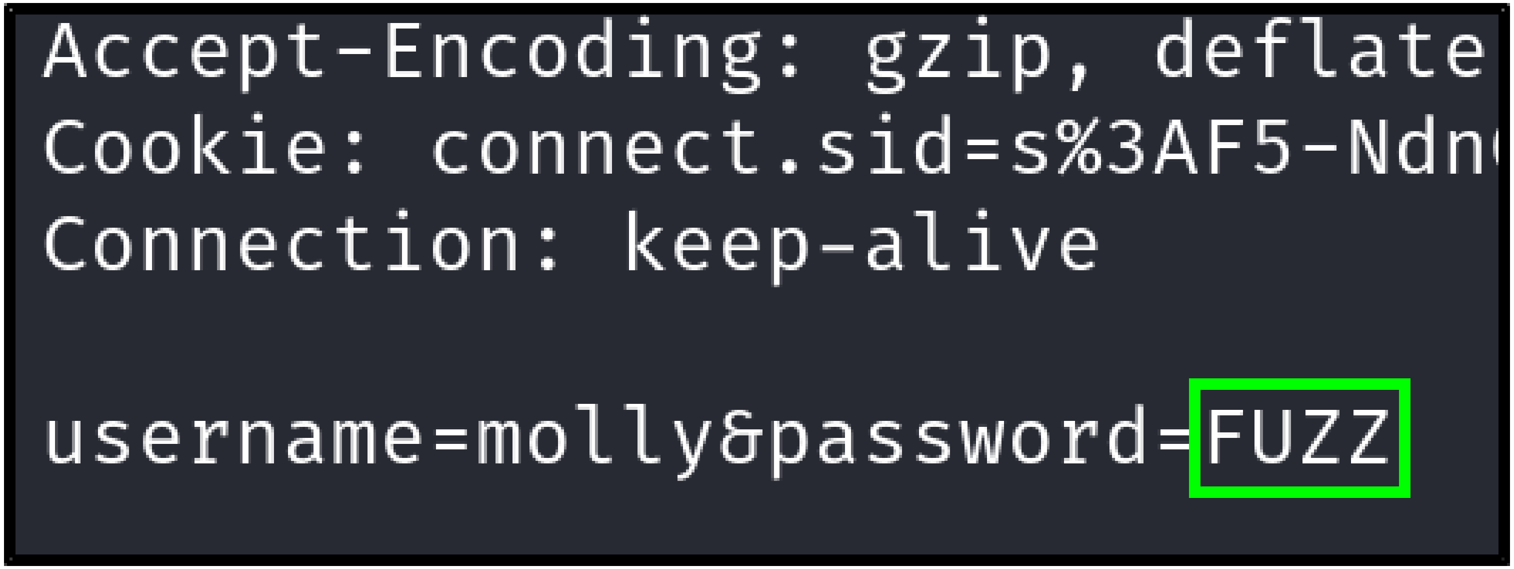
Saving an HTTP Request with Burp



```
POST /login HTTP/1.1
Host: 10.10.165.134
Content-Length: 32
Cache-Control: max-age=0
Accept-Language: en-US,e
```

From there, locate the login request, select it, then right-click on the Request portion and select **Copy to file**

Running FFuF with Request File

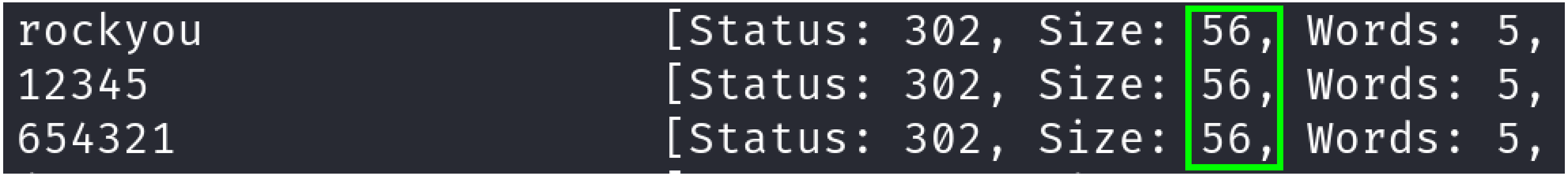


```
Accept-Encoding: gzip, deflate
Cookie: connect.sid=s%3AF5-Ndn
Connection: keep-alive

username=molly&password=FUZZ
```

The last step before running FFuF is to edit the request file and specify a fuzzing point inside the request. In this case, it'll be the password parameter

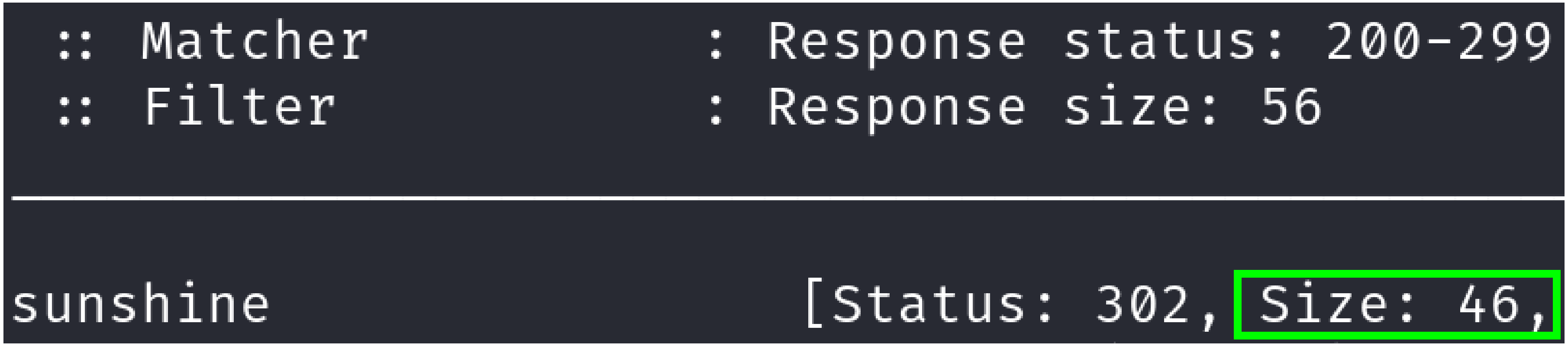
Running FFuF



```
rockyou                 [Status: 302, Size: 56, Words: 5,
12345                   [Status: 302, Size: 56, Words: 5,
654321                  [Status: 302, Size: 56, Words: 5,
```

Now that we're set up, we can run FFuF and get a sense for what failed responses look like. It looks like the failed responses are all size 56, so we can filter out all responses with size 56

Running FFuF



```
 :: Matcher          : Response status: 200-299
 :: Filter           : Response size: 56
________________________________________________

sunshine                [Status: 302, Size: 46,
```

The next time we run FFuF, we discover one response that has a different response size, so that's probably the correct password

Brute Forcing SSH Passwords

Another common service for brute force attacks is SSH, especially in easy-level CTF challenges

Hydra Brute Forcing Program

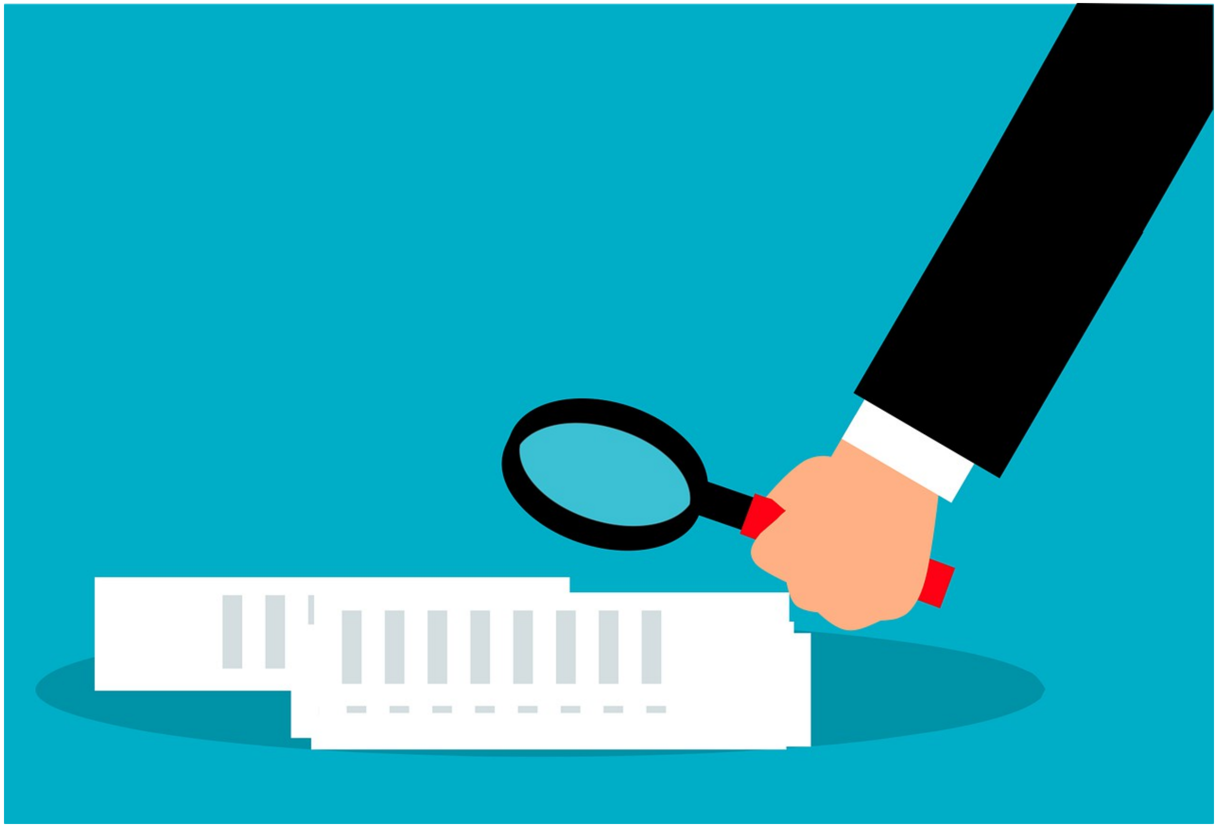
There are a number of programs that can brute force SSH, but a popular option is the Hydra program

Hydra Brute Forcing Program

```
hydra -l <username> -P
<password_list> <IP_address> ssh
```

Compared to login page brute forcing, SSH brute forcing is much easier: all we need to provide to Hydra is a username or list, a password or list, an IP address, and the protocol name, SSH

Summary



Let's review the network hacking concepts we learned in this workshop:

What are Brute Force Attacks?

Brute force attacks are attempts to determine legitimate usernames and passwords on online services

Brute forcing is similar to, but not the the same as password cracking

Brute Force Attacking a Login Page

We learned how to brute force a web app login page with the FFuF program!

Hydra Brute Forcing Program

And we learned how to brute force the SSH service using the Hydra program

What's Next?

In the next HackerFrogs Afterschool Network Hacking workshop, we'll be learning how to transfer files from one device to another