HackerFrogs Afterschool Network Hacking – Session 3

Class:
Network Hacking

Workshop Number:
AS-NET-03

Document Version:
1.75

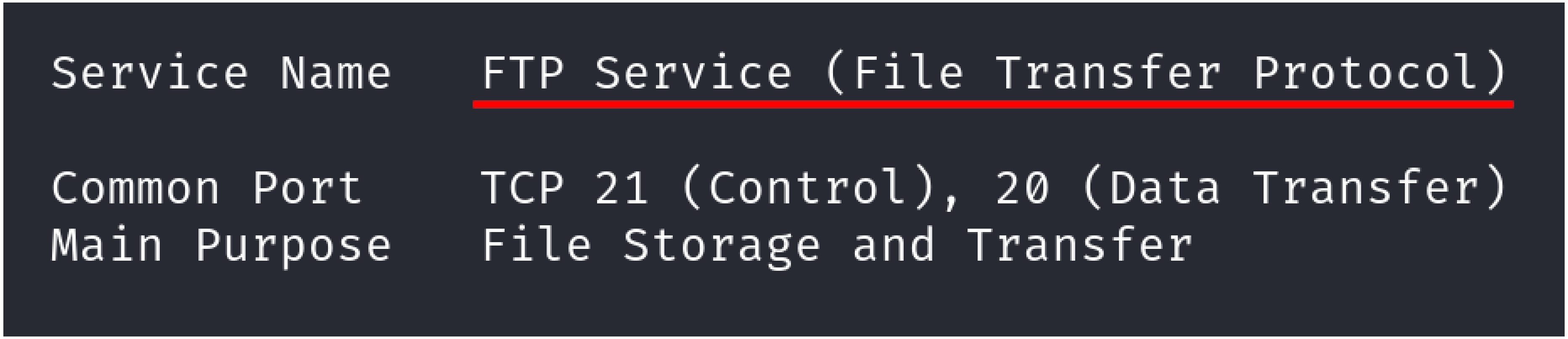
Special Requirements:
Registered account
at tryhackme.com

Welcome to HackerFrogs Afterschool!

This is the third session for network hacking!

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

FTP Service (File Transfer Protocol)

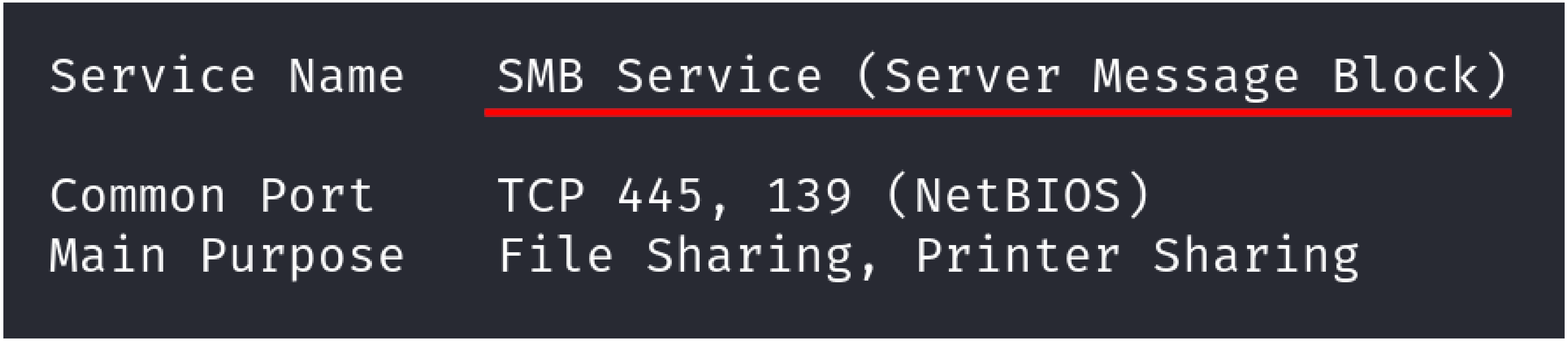


```
Service Name    FTP Service (File Transfer Protocol)

Common Port     TCP 21 (Control), 20 (Data Transfer)
Main Purpose    File Storage and Transfer
```

The FTP service is a common networking service which allows users to upload and download files

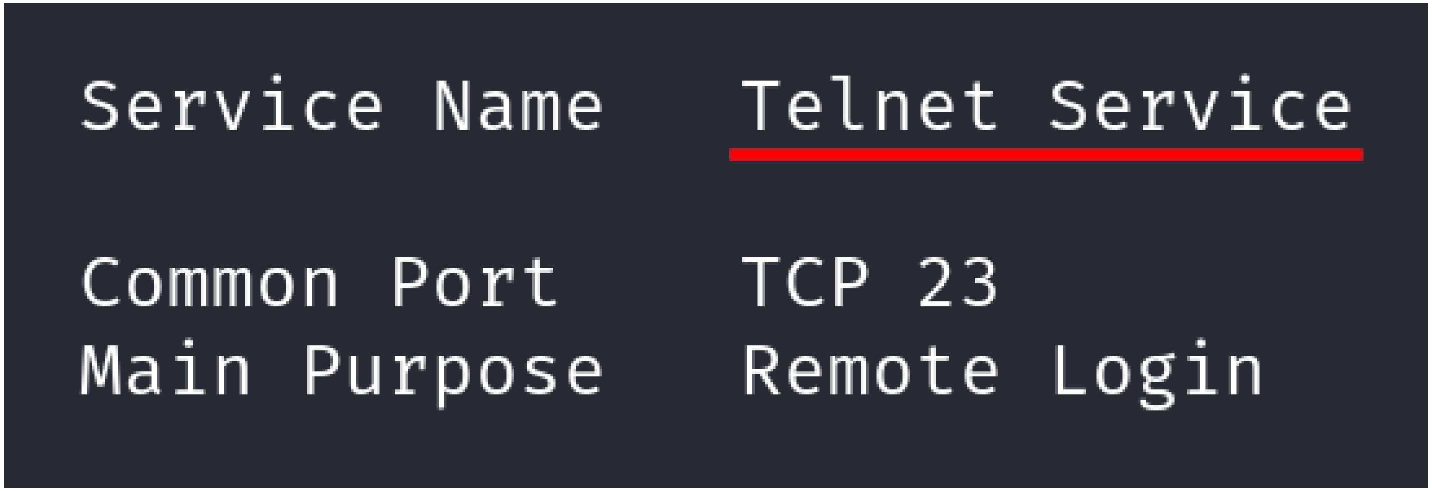
SMB Service (Server Message Block)



Service Name	SMB Service (Server Message Block)
Common Port	TCP 445, 139 (NetBIOS)
Main Purpose	File Sharing, Printer Sharing

The SMB service is a file and printer sharing service that is most commonly associated with the Windows OS

Telnet (Telecommunications Network)



```
Service Name    Telnet Service

Common Port     TCP 23
Main Purpose    Remote Login
```

Telnet is a service that allows remote terminal login, and it is the predecessor to the SSH service

This Session's Topics

- web service enumeration

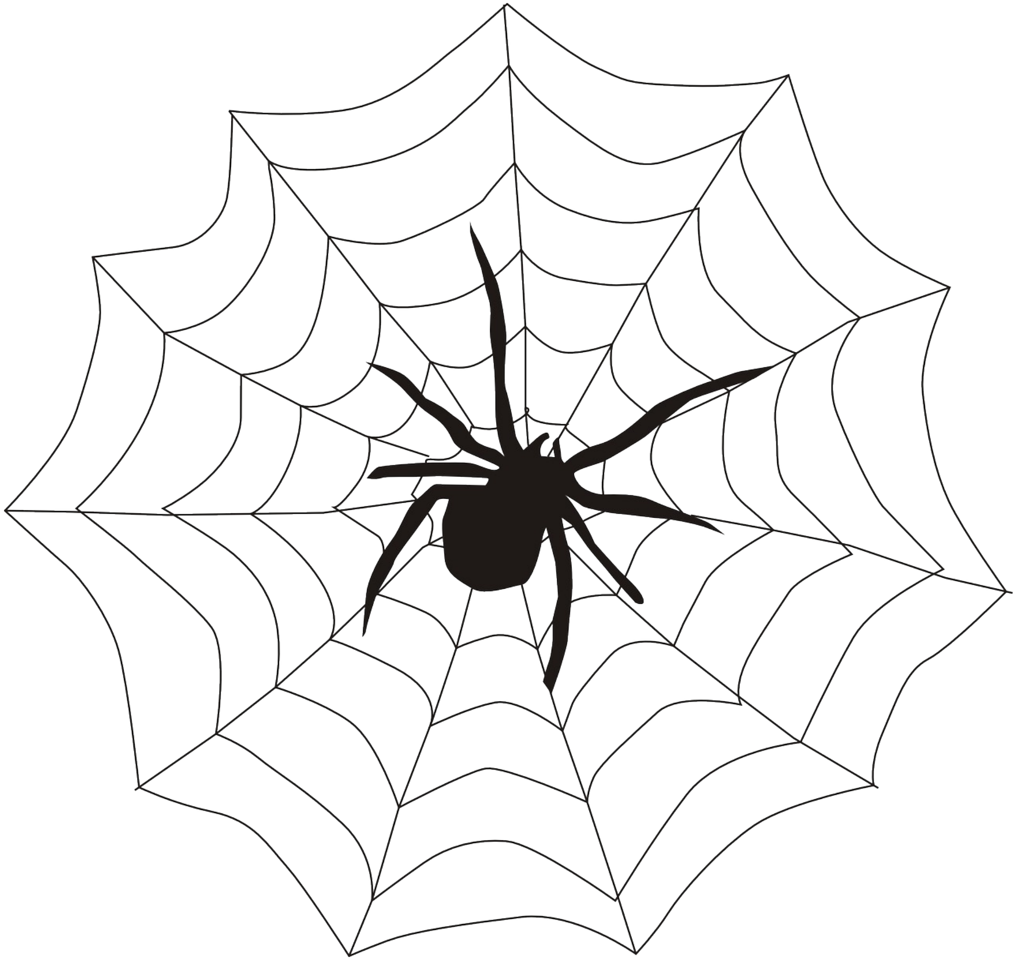
- Dirb tool

- Nikto tool

- Gobuster tool

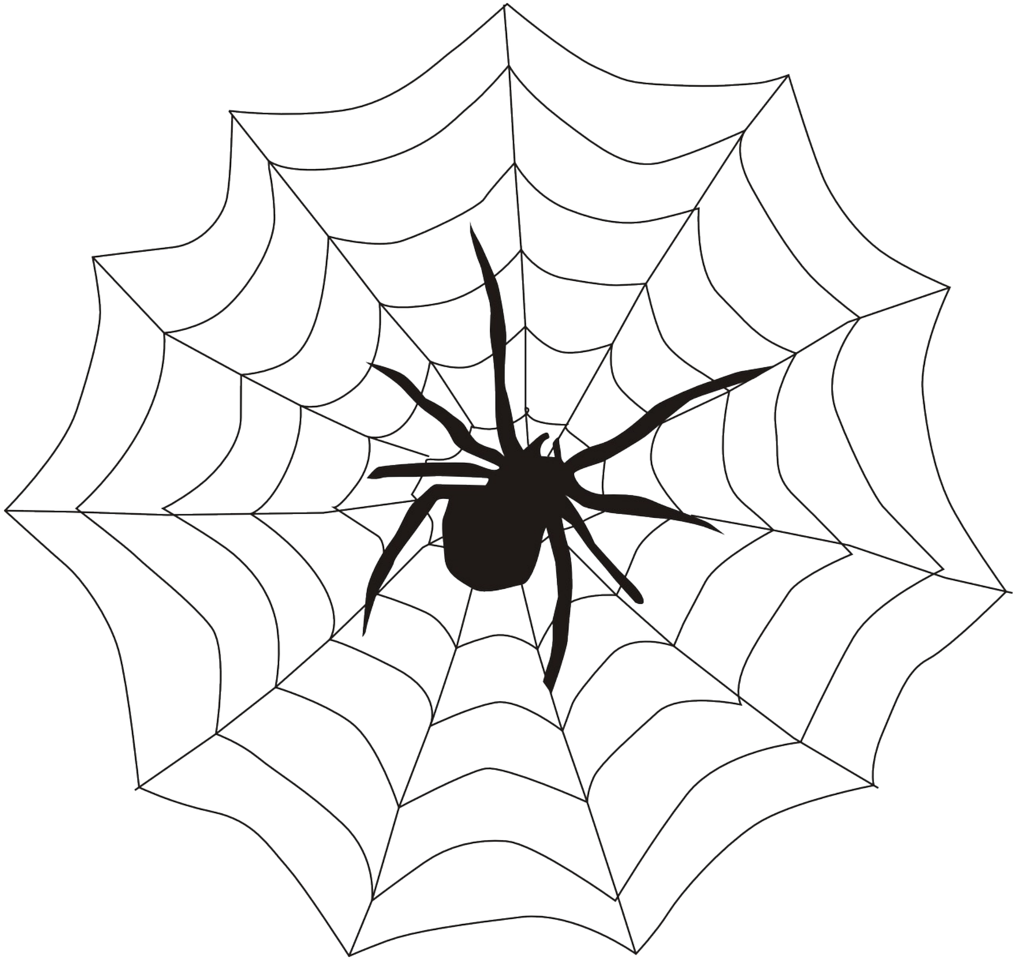
Why are we Learning Web Stuff?

This is a network hacking course, so why are we learning how to enumerate web servers?



Why are we Learning Web Stuff?

That's because web services are network services! In fact, web services are among the most popular networking services!



Accessing TryHackMe

Let's access this TryHackMe room to learn about enumerating web services:

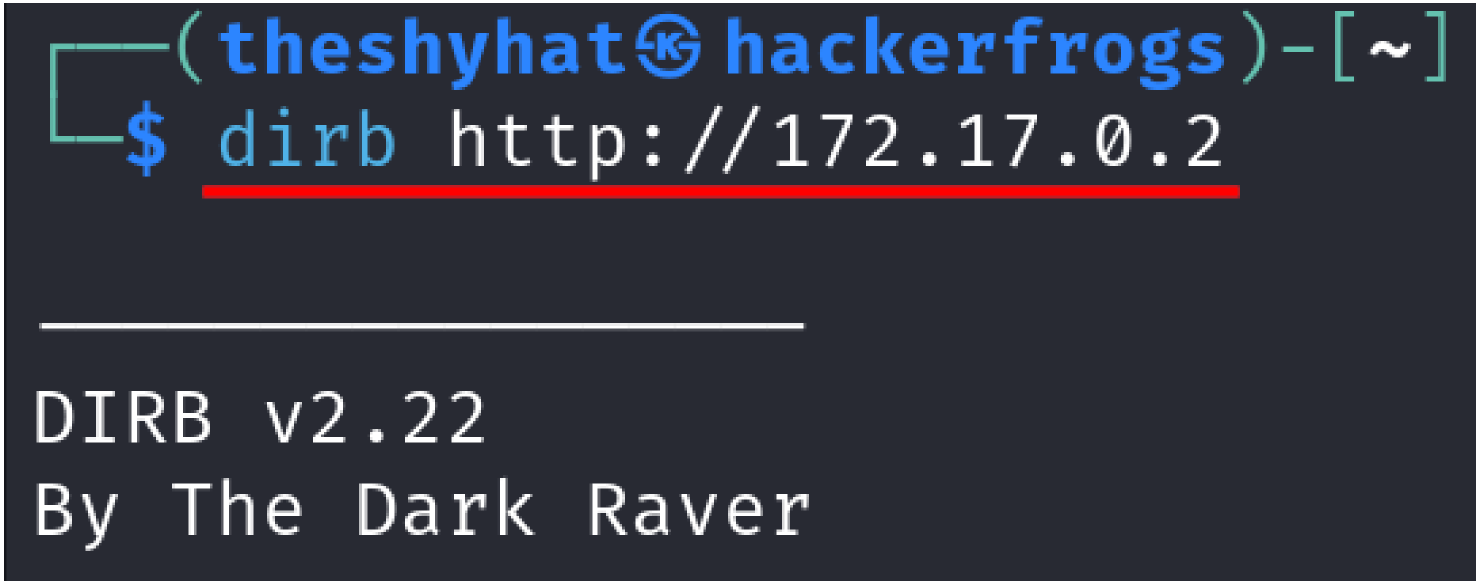
https://tryhackme.com/room/dvwa

The first part of this session is in Task 11 on this webpage

What is Dirbusting?

Directory busting (dirbusting) is the act of determining what endpoints (files and directories) exist on a web app, by trying to access those endpoints. It is a type of brute force attack

Dirb Tool



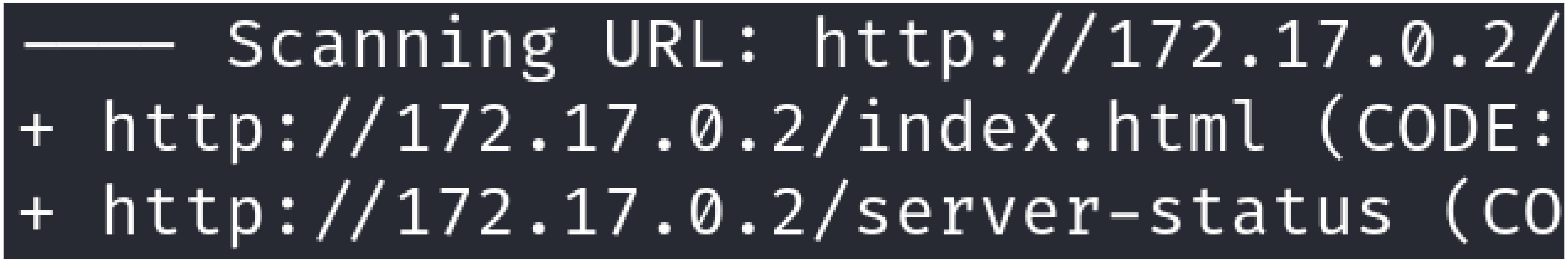
```
┌──(theshyhat㉿hackerfrogs)-[~]
└─$ dirb http://172.17.0.2

-----------------

DIRB v2.22
By The Dark Raver
```

The Dirb tool is an older directory busting tool, and but it's a good first program to run on web servers--

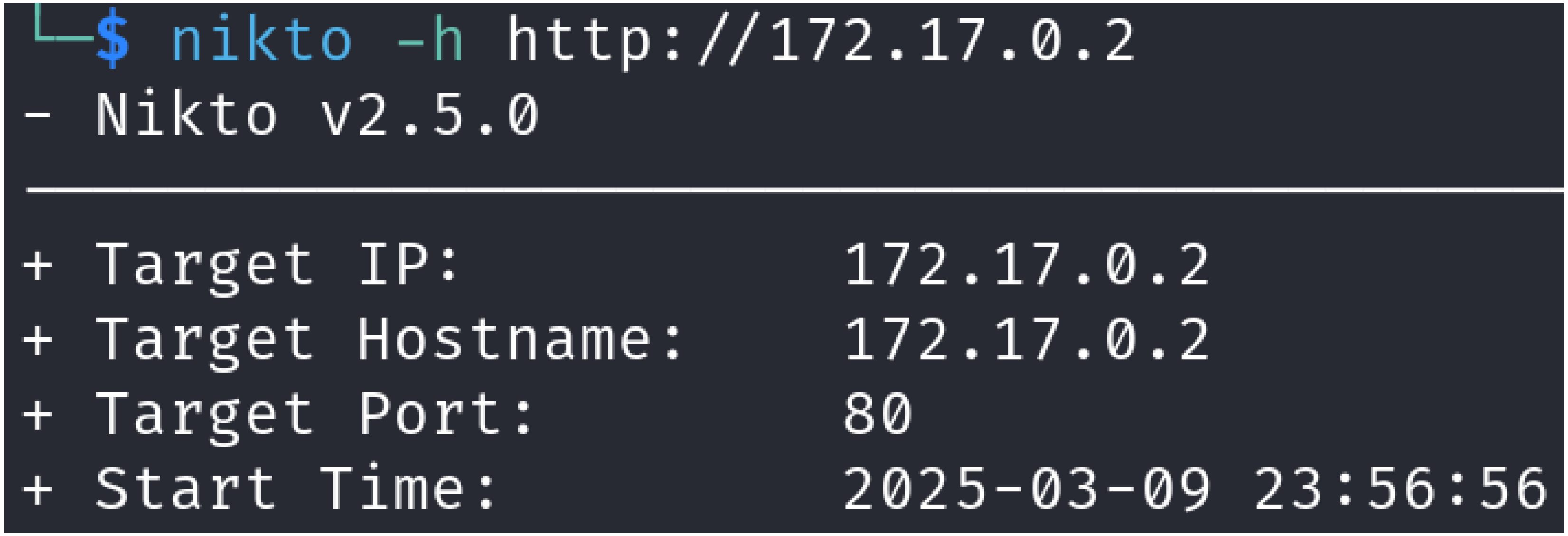
Dirb Tool



```
———— Scanning URL: http://172.17.0.2/
+ http://172.17.0.2/index.html (CODE:
+ http://172.17.0.2/server-status (CO
```

Purely because the command syntax is so simple, and because the wordlist it uses is good for enumerating older webservers and web apps

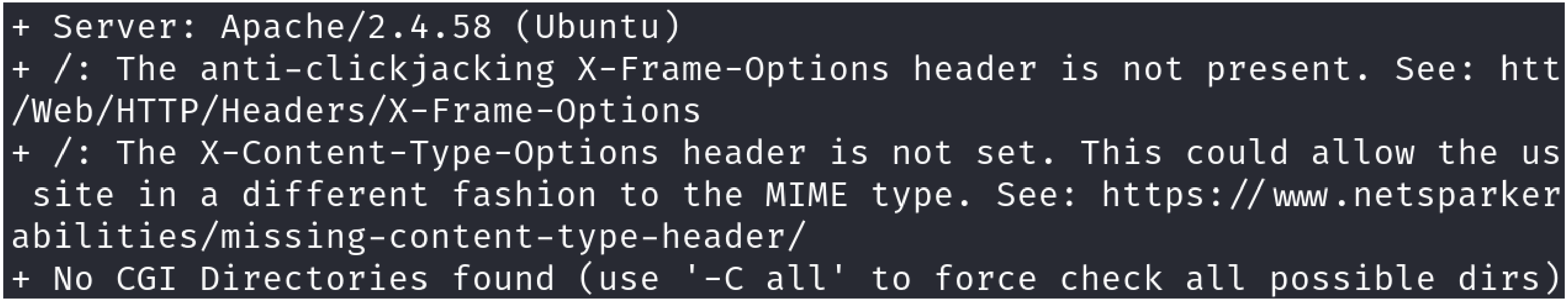
Nikto Tool



```
└─$ nikto -h http://172.17.0.2
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          172.17.0.2
+ Target Hostname:    172.17.0.2
+ Target Port:        80
+ Start Time:         2025-03-09 23:56:56
```

The Nikto tool is not a directory busting tool, but rather a web app vulnerability scanner, which attempts to ID insecure configurations and general web app settings

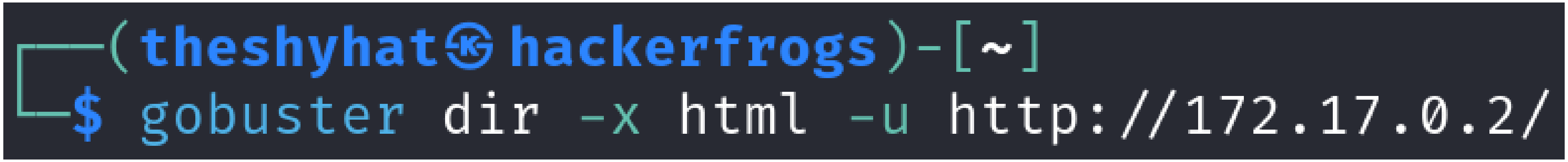
Nikto Tool



```
+ Server: Apache/2.4.58 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: htt
/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the us
 site in a different fashion to the MIME type. See: https://www.netsparker
abilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Like Dirb, Nikto is also an older tool that is better suited to finding vulnerabilities on older webservers and web apps, and it also have a very easy-to-remember command syntax

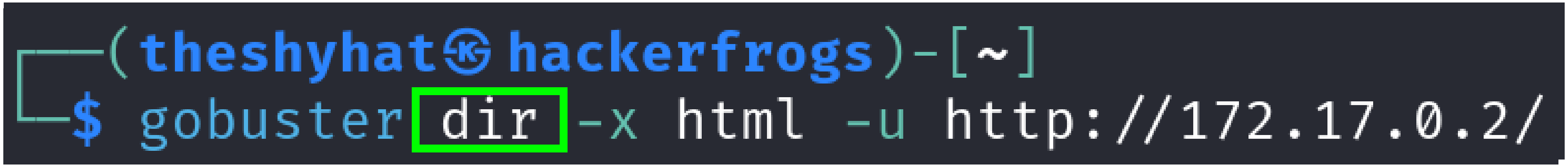
Gobuster Tool



```
┌──(theshyhat㉿hackerfrogs)-[~]
└─$ gobuster dir -x html -u http://172.17.0.2/
```

The Gobuster tool is a much more powerful directory busting tool than Dirb, however its command syntax is much more complex

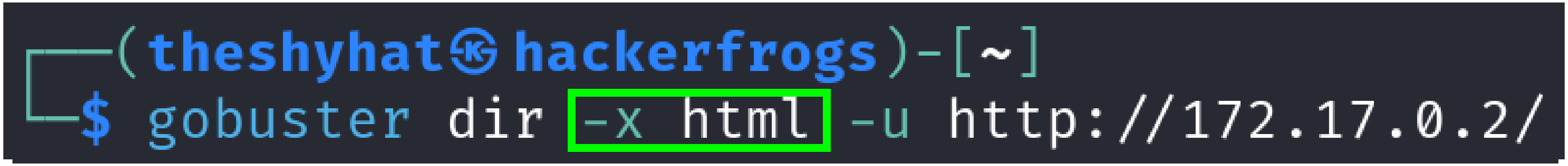
Gobuster Tool



```
┌──(theshyhat㉿hackerfrogs)-[~]
└─$ gobuster dir -x html -u http://172.17.0.2/
```

The first thing we need to give to the gobuster command is the `dir` parameter, which instructs Gobuster to work in directory busting mode

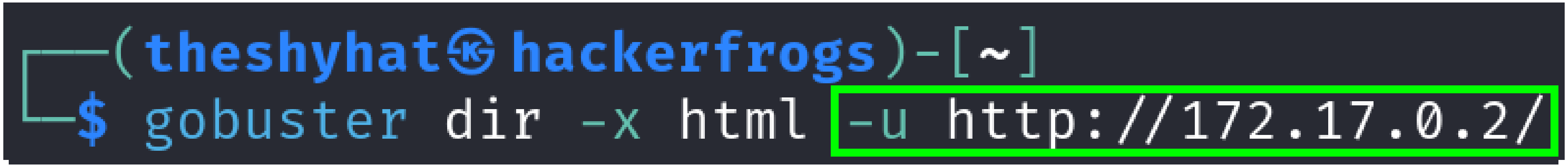
Gobuster Tool



```
┌──(theshyhat㉿hackerfrogs)-[~]
└─$ gobuster dir -x html -u http://172.17.0.2/
```

Then we specify which file extensions to look for with the `-x` parameter, then provide a number of extensions to search for. Here, we're searching for `html` files

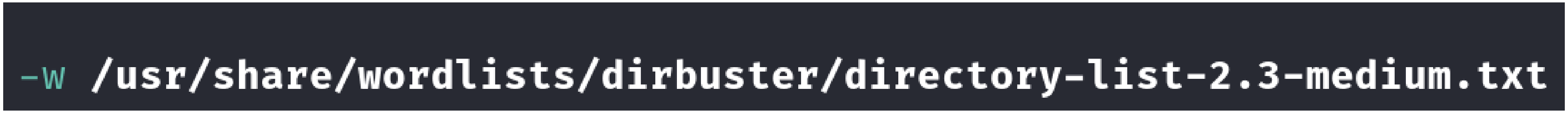
Gobuster Tool



```
┌──(theshyhat㉿hackerfrogs)-[~]
└─$ gobuster dir -x html -u http://172.17.0.2/
```

Then we can provide a mandatory parameter, `-u`, which lets us provide the URL of the web app we want to scan, which in this case is `http://172.17.0.2/`

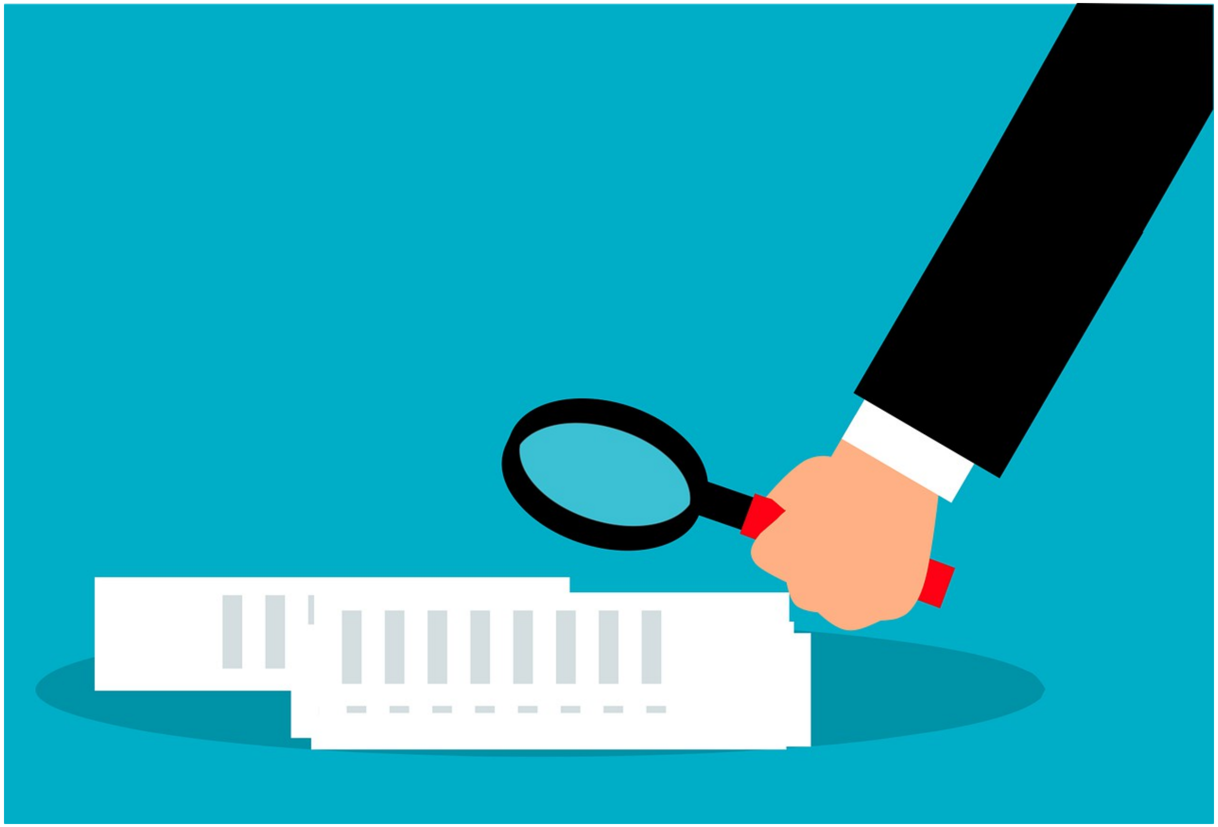
Gobuster Tool



```
-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

Lastly, we have to supply another mandatory parameter, `-w`, which is the word list to use for the dirbusting attack. A common list to use is the `directory-list-2.3-medium.txt` list

Summary

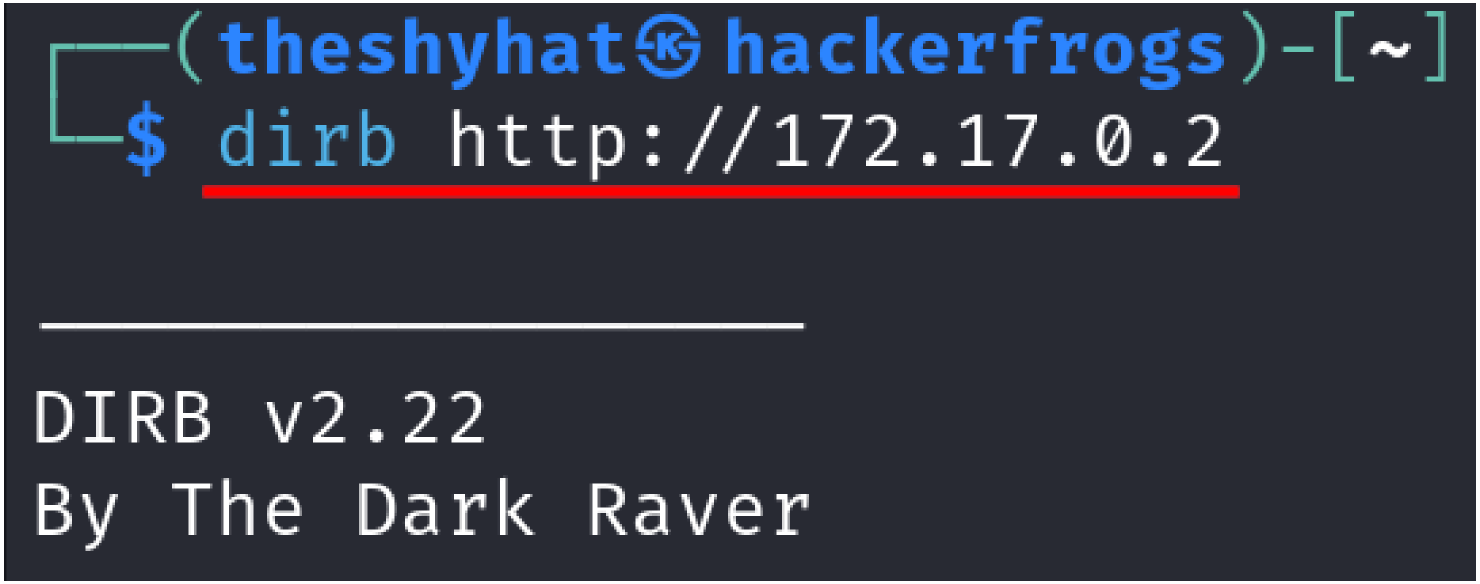


Let's review the network hacking concepts we learned in this workshop:

What is Dirbusting?

Directory busting (dirbusting) is the act of determining what endpoints (files and directories) exist on a web app, by trying to access those endpoints. It is a type of brute force attack

Dirb Tool



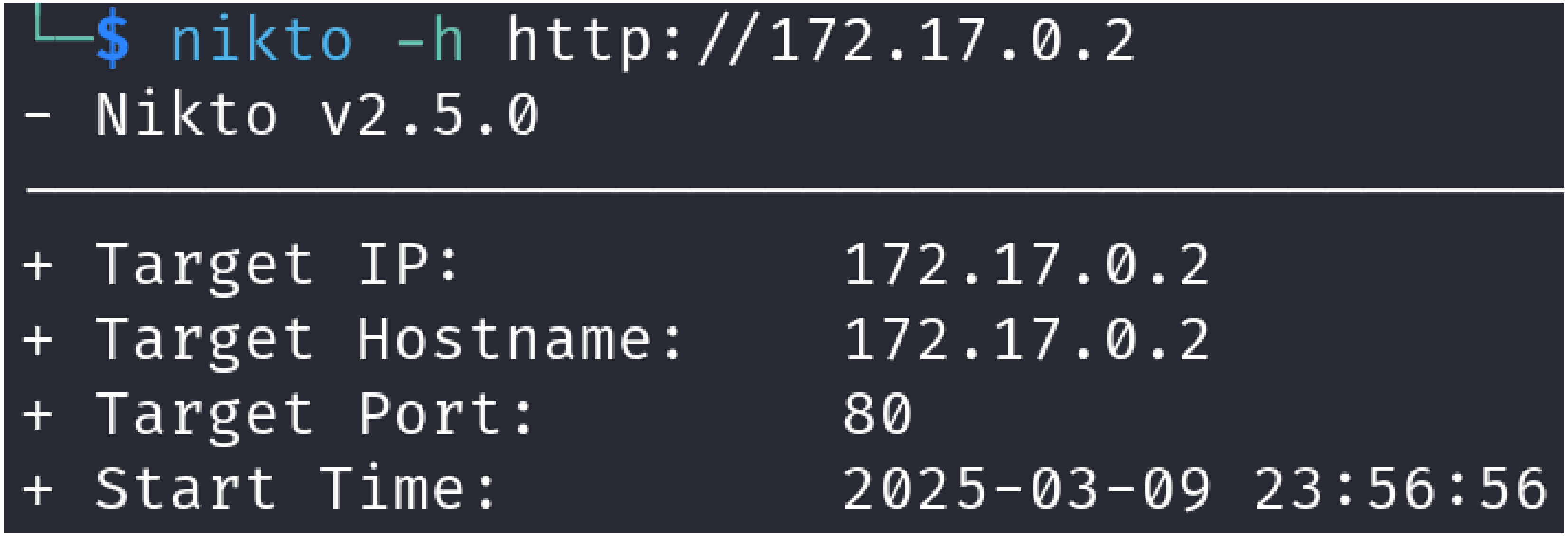
```
┌──(theshyhat㉿hackerfrogs)-[~]
└─$ dirb http://172.17.0.2

-----------------

DIRB v2.22
By The Dark Raver
```

The Dirb tool is an older directory busting tool, and but it's a good first program to run on web servers--

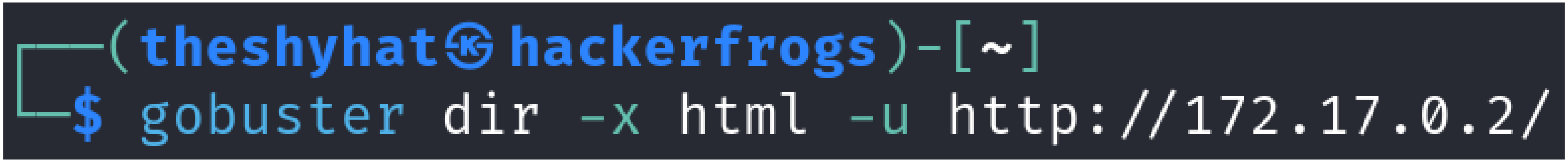
Nikto Tool



```
└─$ nikto -h http://172.17.0.2
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          172.17.0.2
+ Target Hostname:    172.17.0.2
+ Target Port:        80
+ Start Time:         2025-03-09 23:56:56
```

The Nikto tool is a web app vulnerability scanner, which attempts to ID insecure configurations and general web app settings

Gobuster Tool



```
┌──(theshyhat㉿hackerfrogs)-[~]
└─$ gobuster dir -x html -u http://172.17.0.2/
```

The Gobuster tool is a much more powerful directory busting tool than Dirb, however its command syntax is much more complex

What's Next?

In the next HackerFrogs Afterschool Network Hacking workshop, we'll be learning about how to create reverse shell and bind shell connections between networked computers!