Hacking The Matrix

1 Day

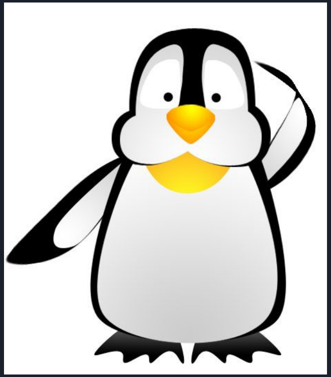
Lead - Friday
Co Lead - Issac

^ Join the discord if you haven’t

General Agenda

1. Diving deeper into recon phase of penetration testing methodology
2. Introducing more common recon tools, revisiting an old one (:
3. Introduction to interacting with & exploiting an FTP server
4. Introduction to Google Dorking
5. Google dorking to find open FTP servers
    - google dork & filter for domains ending in .edu to avoid issues

Recon Whaaaat?



- Who remembers what recon is?
- Exploring a target in order to map out their attack surface and get a lay of the land
- We’ll dive deeper into the **nmap**’s scripting engine!

File Transfer Protocol (FTP)

- FTP is exactly what it sounds like!
- A protocol meant to perform file transfers
- FTP itself -> insecure
  - Transfers data over cleartext
  - FTPS (FTP over TLS)
  - SFTP (FTP using SSH)
- Most FTP servers allow for **anonymous** login!
  - **anonymous:anonymous**

Useful FTP Commands

- Scenario: You’re performing a penetration test and you find an FTP server that you can anonymously login to! How do you navigate it?
- FTP Cheatsheet:
  - ? -> list available FTP commands
  - dir or ls -> list directories
  - get -> download a file from FTP server
  - put -> upload a file to the FTP server
  - pwd -> print current directory
  - quit -> exit

nmap Scripts Practical Use

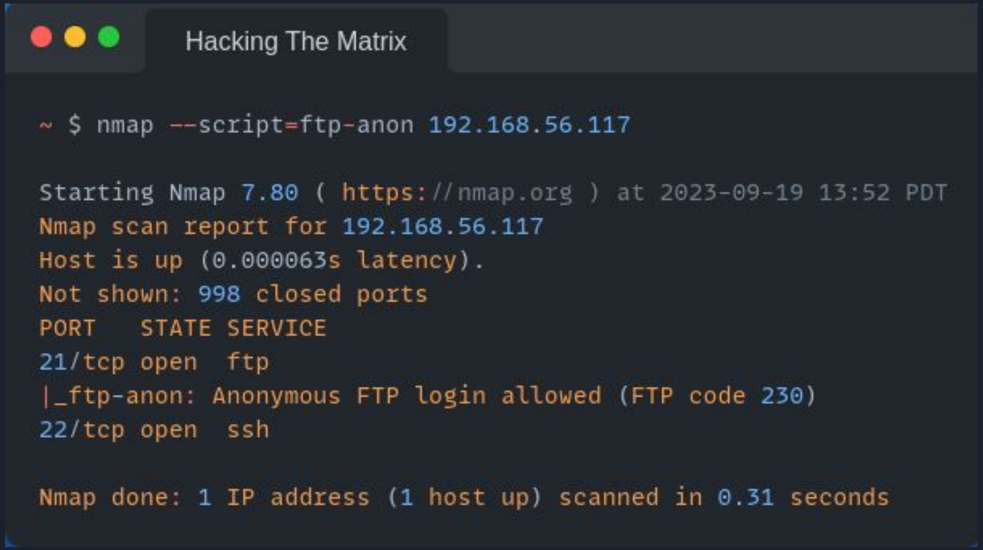
- We can use nmap scripts to perform various attacks and enhance our recon!
  - List of scripts here: https://nmap.org/nsedoc/scripts/
- To run scripts, you would run:

  -
    ```
    nmap –script=<script name> –script-args <insert script args here> 192.168.1.18
    ```
- Scripts have various uses, like brute-forcing or performing more intrusive scans which help gain more info!
  - EX: ftp-anon script tells us whether FTP anonymous login is enabled

Time to get some mud on our hands

- Scenario: There’s an FTP Server running on <INSERT IP ADDR HERE>. Use nmap’s scripting engine to see if anonymous login is enabled…
  - Are there any interesting files you can read?

FTP-Anon Script Usage



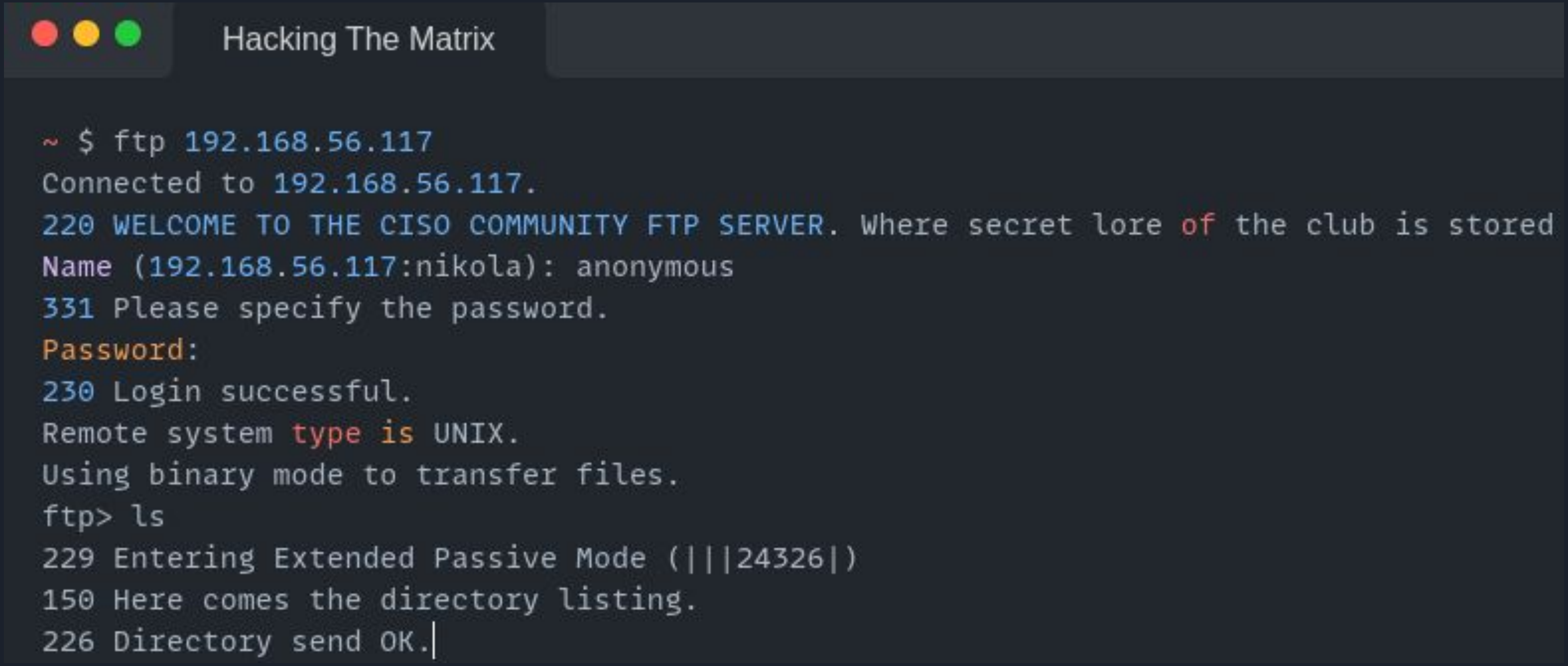
```
~ $ nmap --script=ftp-anon 192.168.56.117

Starting Nmap 7.80 ( https://nmap.org ) at 2023-09-19 13:52 PDT
Nmap scan report for 192.168.56.117
Host is up (0.000063s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

- –script=ftp-anon will run the anonymous login test script
- As you can see, anonymous login is indeed enabled!

Anonymous Login FTP

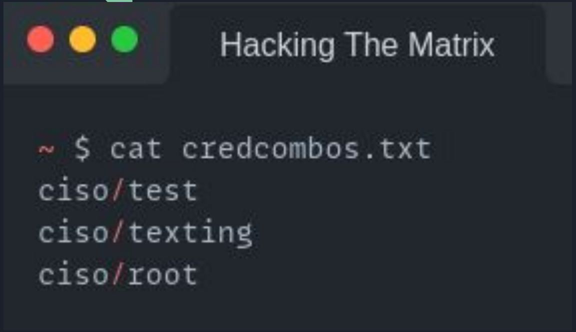


```
~ $ ftp 192.168.56.117
Connected to 192.168.56.117.
220 WELCOME TO THE CISO COMMUNITY FTP SERVER. Where secret lore of the club is stored
Name (192.168.56.117:nikola): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||24326|)
150 Here comes the directory listing.
226 Directory send OK.
```

Time For Some More Mud!

- Scenario: You’ve tested for anonymous login, you know that it’s enabled but you haven’t found any juicy data through the anonymous user. You’ve got some super secret confidential intel that tells you that the username **ciso** exists on the server. Perhaps you can brute force your way into the **ciso** user?
    - Hint: Use the ftp-brute nmap script
        - **–script=ftp-brute**
        - Create custom credential file using **brute.credfile** format
        - Target: 192.168.1.18
        - Remember to check https://nmap.org/nsedoc/scripts/ to see the argos necessary
        - Don’t be afraid to ask AI

FTP Brute Forcing With nmap



```
~ $ cat credcombos.txt
ciso/test
ciso/texting
ciso/root
```

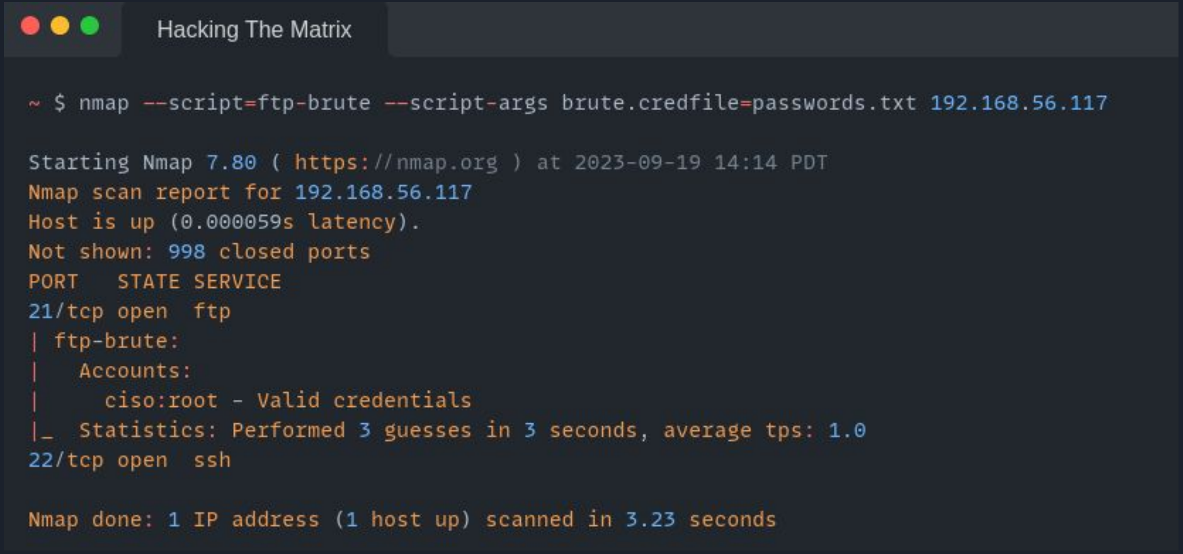
← First, we'll create a credential file

The format is username\password

Then we can perform the brute force using nmap & the ftp-brute script →

Now brute force!

The correct username & password combo is ciso:root



```
~ $ nmap --script=ftp-brute --script-args brute.credfile=passwords.txt 192.168.56.117

Starting Nmap 7.80 ( https://nmap.org ) at 2023-09-19 14:14 PDT
Nmap scan report for 192.168.56.117
Host is up (0.000059s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts:
|     ciso:root - Valid credentials
|_  Statistics: Performed 3 guesses in 3 seconds, average tps: 1.0
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 3.23 seconds
```

Now that you have the FTP creds…

Login to the FTP server and try to find that juicy CISO lore!

Dorks Are Cool

- *Dorks* are advanced search operators we can use & specific search queries that can be used with search engines to find info that’s not indexed or easily accessible through normal searches
- Say you wanted to find FTP servers on the Internet.
    - How to do?
    - Shodan? Sure. But why not Google?
- We can use Google dorks to find info about specific targets!

Dork Operators

- There's a ton of Google Dork operators, too many to cover in an hour!
  - https://hackr.io/blog/google-dorks-cheat-sheet ← Cheatsheet for them here!
- Some cool ones are:
  - **Inurl:** ← Will find all indexed websites that contain some keyword in the URL
  - **Intitle**: ← Will find all indexed websites that contain some keyword in the title
  - **Fileext:** ← Will find all indexed websites that allow downloading of a specified file
    - **site:csusb.edu fileext:pdf** will show all PDFs on the csusb website
- **Your task**:
  - Find FTP servers on domains that end in .edu!
    - FTP servers typically have the keyword **index of** within the title!

Join the Discord!