FTP Enumeration

The File Transfer Protocol (FTP) is a widely used protocol for transferring files between computers over a network. FTP servers often contain sensitive information and can be vulnerable to various attacks if not properly configured.

Version Detection

Lets start with the first technique in which we will enumerate the version of the FTP server.

This can be done very easily with the help of Nmap.

```
sudo nmap -p 21 -sV -sC 192.168.29.141
```

Now that we know the version of our FTP server, we can look for potential exploits related to it.

Another way to find the version of the running FTP server is using Metasploit.

```
use auxiliary/scanner/ftp/ftp_version
set RHOSTS <TARGET IP>
run
```

FTP Anonymous login

Now this one is one of the most important thing you have to check while performing FTP enumeration as this can create potential entry on to the server.

Anonymous FTP is a misconfiguration on the server where it allows us to access public files on an FTP server without needing a special username and password. It's like a public library where anyone can walk in and borrow books.

To check it we can use the nmap default scripts but to interact with it, we can do it manually.

```
ftp IP
```

For the username type anonymous and on password just hit enter. Now we are in, we can list the files on the server.

Lets understand why this is a jackpot for us. If we find any server with FTP anonymous login enabled and if we can put on the server using this, then we can eventually also upload our payload on the server and execute it.

Also, if we are in the user's home directory after logging in, then we can use our SSH keys to create a backdoor on the machine.

Lets first check if we can put a file on the server.

```
put test.txt
```

On thing to note here is that, Binary and ASCII files have to be uploaded using the `binary` or `ascii` mode respectively, otherwise, the file will become corrupted. Use the corresponding command to switch between modes.

Here binary files are the executable files and if you are uploading any text file then it is a ASCII file.

Recursive Download

Suppose there are folders in the FTP server that you want to download. You can do that recursively using a single command.

```
wget -m ftp://user:pass@10.0.0.3/
```

```
wget -m --no-passive ftp://anonymous:anonymous@10.10.10.98
```

Guessing potential usernames

We can guess potential FTP usernames using the ftp-userenum perl script. It uses

```
ftp-user-enum.pl -U users.txt -t IP
```

Beware of this, as the script sometimes also shows false positives.

After we have the potential username list, we can perform a bruteforce attack to get its password using hydra. I will not go into the detail of that in this section as it will be covered thoroughly in the exploitation module

---

Configuration Files

If we land on a server, then there are some sensitive FTP configuration that we should look into.

```
ftpusers
ftp.conf
proftpd.conf
vsftpd.conf
```
