2.1.2 - pyFTP

Overview

Python is capable of hosting both `read-only` and `read-write` FTP servers. These are an easy to use alternative to installing a product like `VSFTPd`.

pyFTP

How is it used

pyFTB makes use of the Python module `pyftpdlib`. Once installed, you call it using the `-m` switch for `Python3`.

```
        -m module-name
                Searches sys.path for the named module and runs the
corresponding .py file as a script.
```

> The `pyftblib` allows you to serve a folder so that it is available over the FTP protocol

Why is this important

Some target machines may not be able to use all protocols. Using Python to host FTP allows another avenue for infill and ex-fill of data.

Real-word applications

Consider the scenario below.

> You have gained an unprivileged shell on a machine and located sensitive files which you need to analyse with tools not available on the target. The only command available to you is `ftp`. You may easily host an `ftp` server on your attacking machine and copy the files over using the `FTP` protocol.

Exercise

Installation

First, make sure that your list of packages are up-to-date.

```
sudo apt update
```

Next, ensure `pip` for `Python3` is installed.

```
sudo apt install python3-pip
```

Finally, install the `pyftpdlib` module using `pip`.

```
pip3 install pyftpdlib
```

Usage

You can read more about the command-line usage of the `pyftpdlib` module by reading the documentation at the link below.

https://pyftpdlib.readthedocs.io/en/latest/tutorial.html#command-line-usage

Manual

With it the module successfully installed, the command below will run an FTP server with the root of the FTP server as the current folder

> The root of the FTP server is what will appear when some is connected. For example, if I ran the command within `/opt/ftp`, the contents of `/opt/ftp` will be visible when a connection is made.

This command will set the port to `21` and the `-w` flag enables write permissions.

```
sudo python3 -m pyftpdlib -p 21 -w
```

Once running, it may be connected to using `anonymous:anonymous` as the login credentials.

> Removing the `-w` flag will make the FTP server read-only.

Script

I have written the script below. If you paste the block into `Kali`, it will create a file called `pyftd`

You'll need to run this as root, so `sudo su` before it. Just paste the entire block as per the screenshot.

```
cat <<EOF > /usr/bin/pyftp
#/bin/bash

if [ -z "\$1" ]
  then
    echo "Missing argument: pyftp <port>"
    exit
fi

echo "Starting Read-Write FTP Server"
```

```
echo "PORT: \$1"
echo "LOCAL WORKING PATH: $(pwd)"
# use the first argument to run a ro ftp server on \$1 port
python3 -m pyftpdlib -p \$1 -w
EOF

sudo chmod 755 /usr/bin/pyftp
```

```
┌──(root💀kali02)-[/usr/bin]
└─# cat <<EOF > /usr/bin/pyftp
#/bin/bash

if [ -z "\$1" ]
  then
    echo "Missing argument: pyftp <port>"
    exit
fi

echo "Starting Read-Write FTP Server"
echo "PORT: \$1"
echo "LOCAL WORKING PATH: $(pwd)"
# use the first argument to run a ro ftp server on \$1 port
python3 -m pyftpdlib -p \$1 -w
EOF

sudo chmod 755 /usr/bin/pyftp

┌──(root💀kali02)-[/usr/bin]
└─# ls -lha /usr/bin/pyftp
-rwxr-xr-x 1 root root 268 Jan 31 11:54 /usr/bin/pyftp

┌──(root💀kali02)-[/usr/bin]
└─#
```

With that, you will be able to run it. If you do not define a port, you will see the message below.

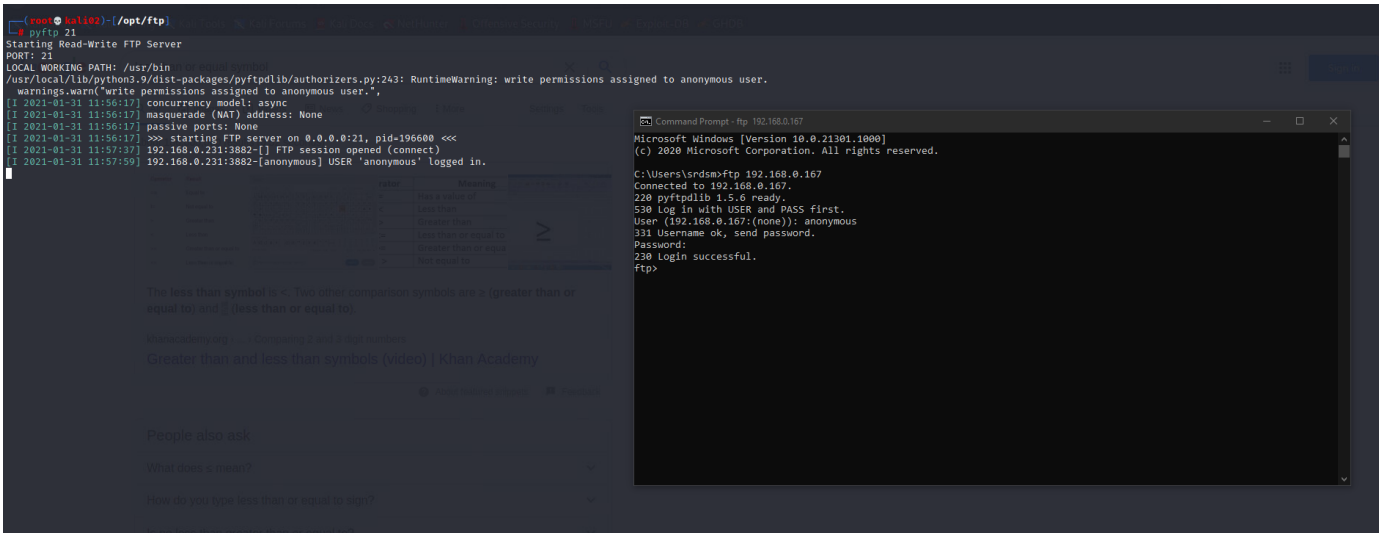
```
┌──(root💀kali02)-[/usr/bin]
└─# pyftp
Missing argument: pyftp <port>

┌──(root💀kali02)-[/usr/bin]
└─#
```

Once you set a port, it will start the FTP server.

```
┌──(root💀kali02)-[/opt/ftp]
└─# pyftp 21
Starting Read-Write FTP Server
PORT: 21
LOCAL WORKING PATH: /usr/bin
/usr/local/lib/python3.9/dist-packages/pyftpdlib/authorizers.py:243: RuntimeWarning: write permissions assigned to anonymous user.
  warnings.warn("write permissions assigned to anonymous user.",
[I 2021-01-31 11:56:17] concurrency model: async
[I 2021-01-31 11:56:17] masquerade (NAT) address: None
[I 2021-01-31 11:56:17] passive ports: None
[I 2021-01-31 11:56:17] >>> starting FTP server on 0.0.0.0:21, pid=196600 <<<
```

Finally, you will be able to connect with it and use it.



Assessment

Nil.