SANS 502 Perimeter Security Hardware and Software Requirements

1) Windows laptop with a live Linux CD file system

This is the preferred option and probably the easiest method for anyone who is unfamiliar with Linux or Unix. You can configure a Windows based laptop using the guidelines specified below. When you wish to work with Linux, simply load in one of the live Linux file system CD's and reboot the system. Linux will then boot directly from the CD. While the system runs a bit slower than usual (CD-ROM access times are slower than hard drives), this setup permits you to run Linux while making no modifications to the hard drive. When you wish to return to Windows, simply remove the CD and reboot the system.

2) Dual boot

It is possible to load both Windows and Linux from the same hard drive. The process typically involves installing Windows but partitioning the hard drive to leave half of it unused. You then install Linux onto the remaining portion of the disk. The Linux install will usually automatically detect the Windows partition and add it to the boot loader menu. When you start the system, you simply select from the menu which operating system you wish to boot.

More information on running a dual boot system can be found here:
http://www.linux.org/

3) User mode virtual operating systems

Tools such as VMWare permit you to run an additional operating system as if it was an application. So for example you could boot your Windows based laptop and use VMWare to run Linux as an application on the system. Virtual images can be a bit tricky to get going initially but typically work quite nicely once they are up and running.

More information can be found here:
http://www.vmware.com/

4) Two laptops, one with Windows and the other with Linux

Finally, the student can simply choose to bring two separate laptops to class. One would be configured to run Windows while the other is configured with Linux.

Configuring Windows for the Security 502 Labs

Perform the following in order to configure your system for running the Security 502 labs:

1) Create a C:\Tools directory

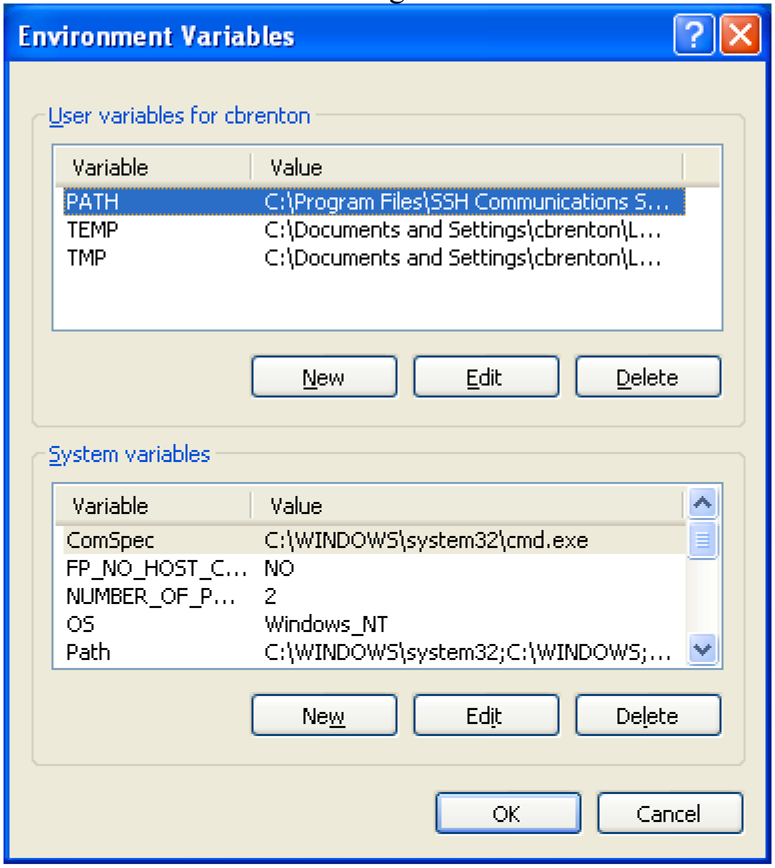
This will be the install location for most of the tools we will use in the labs. If you want to give it another name that is fine, but this document will assume the above path for all instructions. We will be working at the command line quite a bit so creating this directory as close to the root level as possible (right off of C:\ or D:\) will be a real time saver.

2) Place C:\Tools in your path

If you are unsure how to do this, perform the following steps:

A) Right click on “My Computer”
B) Left click on “Properties”
C) Click on the “Advanced” tab
D) Click on the “Environment Variables” button

You should now see something similar to this:



Variable	Value
PATH	C:\Program Files\SSH Communications S...
TEMP	C:\Documents and Settings\cbrenton\L...
TMP	C:\Documents and Settings\cbrenton\L...

Variable	Value
ComSpec	C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_C...	NO
NUMBER_OF_P...	2
OS	Windows_NT
Path	C:\WINDOWS\system32;C:\WINDOWS;...

Notice the “Path” variable in the top pane. Left click on this variable and then click the “Edit…” button. At the end of the line, add in:

;C:\Tools

Note the semi-colon as the first character. Once complete, simply continue to click “OK” till you are back at your desktop. Depending on your version of Windows, you may need to logoff and logon for your changes to take effect. You can check to see if you have set the path statement correctly by opening a command prompt and typing in the command “path” (without the quotes).

3) View all file extensions

Windows likes to hide the extensions of known file types. Doing so will make performing the software installation as well as the labs a bit more difficult, so we are going to disable this functionality. Note that the exact steps vary slightly between Windows versions. The steps below assume Windows XP.

A) Run Windows Explorer (Not Internet Explorer, Windows Explorer (previously File Manager)
B) Select Tools → Folder Options → View
C) Select "Show Hidden Files and Folders"
D) De-select "Hide file extensions for known types" and "Hide protected operating system files"
E) Click "OK" to exit

You Windows environment is now properly configured and you are ready to install the software required for performing the labs.

Required Windows Software for Security 502 Labs
The following is a list of tools you will need to have installed on your Windows system. Unless specified otherwise, you should install them in the C:\Tools directory created earlier in this document.

WinDump and WinPcap
http://www.winpcap.org/windump/install/

Follow the installation instructions on the Web site. To test your installation, open a command prompt and type:
windump –D
This should produce a list of network interfaces on your system.

nmap
http://www.insecure.org/nmap/
Download the latest version and follow the directions specified on the Web site. To test the install, type:
nmap –V

p0f
http://lcamtuf.coredump.cx/p0f-win32.zip

To test your install, type:
p0f –h

Note the second character is a zero, not an "oh".

Netcat
http://www.vulnwatch.org/netcat/

To test your install, simply type:
nc –h

Ethereal
http://www.ethereal.com/

This is a graphical interface tool. It should create a desktop icon that you can click on to verify the installation.

grep
http://gnuwin32.sourceforge.net/packages/grep.htm

To test your install, type:
grep –h

ngrep
http://ngrep.sourceforge.net/

Download and install per the instructions on the Web site. Make sure you install the "release" version of the binary rather than the "debug" version.

Snort
http://www.snort.org/

Download the latest version of the Snort system files. Note that you now must download a copy of the Snort rules separately. Once you have downloaded the Snort package, follow the "Download Rules" link off of the download page. Grab the latest copy listed.

To test your installation, type "snort –V" without the quotes. You may need to do this from the C:\Snort\Bin directory.

Note that the Windows version of Snort has a lot of trouble finding its default files. If you try to do anything more than check the version Snort will most likely fail to run. When you come to class you will be given a configuration file that will fix all of these problems.

md5sum
http://theopencd.sunsite.dk/md5sum.exe

Copy the file to your C:\Tools directory. To test it, simply type in:
md5sum *

PSTools
http://www.sysinternals.com/Utilities/PsTools.html

Download the tools from the above link and extract them to your C:\Tools directory.

John The Ripper
http://www.openwall.com/john/

Download the Windows version of the tool and install it to your C:\Tools directory.

pwdump6
http://www.foofus.net/fizzgig/pwdump/

Download the latest ZIP file and extract the contents to the C:\Tools directory.

Putty
http://netmirror.org/mirror/putty/download.html

Putty is an SSH client for Windows. Go to the above page and download “putty.zip” which includes all required files. Extract each of these files to the C:\Tools directory.

Required Linux Software For Security 502 Labs

With Linux, you have two options. You can either install a regular distribution on your hard drive (such as SUSE, Fedora, Red Hat, Slackware, etc.) or you can install one of the recommended live Linux CD file systems. The live CD file systems are the easiest method as you simply download the CD ISO image, burn it to a CD, and pop it in your CD-ROM drive whenever you wish to run Linux.

Live Linux File System CD’s

The following is the list of recommended live Linux file systems you can run in order to perform the Security 502 labs.

Auditor
http://www.remote-exploit.org/index.php/Auditor
Auditor is a stable collection of security tools based on the Knoppix Linux distribution. It has a great selection of tools and supports many different hardware configurations.

BackTrack
http://www.remote-exploit.org/index.php/BackTrack
BackTrack is a combination of Auditor as well as another Linux distribution called Whax. At the time of this writing it is still beta code, but relatively stable. While it does not include as many tools as Auditor, the tools that are there are more up to date.

Knoppix-STD
http://s-t-d.org/
This live file system has not been updated in quite some time but has a very large number of tools. It also has better support for older hardware platforms. If your laptop is a few years old and you cannot get Auditor or BackTrack to run, Knoppix-STD may do the trick. The only caveat is that two of the binaries used in the labs are missing from the distribution, which means you could have problems with three of the labs.

Standard Linux Install

If you have installed a standard Linux distribution, here are the tools you will need:

tcpdump and libpcap

Most distributions include a copy of tcpdump and libpcap by default. If yours does not, you can grab the latest version from here:
http://www.tcpdump.org/

To test your installation, logon as root and type the following:

```
tcpdump –V
```

nmap

http://www.insecure.org/nmap/
Download the latest version and follow the directions specified on the Web site. To test the install, type:

```
nmap –V
```

Netcat

Some distros include Netcat by default, but some do not. You can grab a copy of it here:
http://netcat.sourceforge.net/download.php

To test the install, simply type:

```
nc –h
```

p0f

http://lcamtuf.coredump.cx/p0f.tgz

To test your install, type:

```
p0f –h
```

Note the second character is a zero, not an "oh".

Ethereal

http://www.ethereal.com/

This is a graphical interface tool that is included with some distros, so you may already have a copy. Typing "ethereal" (without the quotes) within a terminal window should launch the GUI.

hping

http://www.hping.org/

Download and install per the instructions on the Web site. To test the installation, type:

```
hping –help
```

Etherape
http://etherape.sourceforge.net/

This is a graphical interface tool. Typing “etherape” (without the quotes) within a terminal window should launch the GUI.

iptraf
http://iptraf.seul.org/

This is a command line utility. Open a terminal window and type “iptraf” without the quotes. This should launch the Curses interface.

ngrep
http://ngrep.sourceforge.net/

Download and install per the instructions on the Web site.

Snort
http://www.snort.org/

Download the latest version of the Snort system files. Note that you now must download a copy of the Snort rules separately. Once you have downloaded the Snort package, follow the “Download Rules” link off of the download page. Grab the latest copy listed.

To test your installation, type “snort –V” without the quotes.

John The Ripper
http://www.openwall.com/john/

Download the latest tar ball and build as required.

ssldump
http://www.rtfm.com/ssldump/

Download the latest tar ball and build as required.

Secure Shell (SSH)
http://www.openssh.com/

Most likely your Linux distribution includes a copy of SSH, usually OpenSSH. If you do not have a copy, you can download the latest version from the above link.

Dsniff
This can be a difficult package to get running. If you have problems, use Google and search on your distribution name and version along with the key words “dsniff” and “2.4” (without the quotes).

A copy of the software can be found here:
http://www.monkey.org/~dugsong/dsniff/beta/dsniff-2.4b1.tar.gz

Dependencies for Dsniff can be downloaded here:
http://www.packetfactory.net/projects/libnids/dist/libnids-1.16.tar.gz
http://www.packetfactory.net/libnet/dist/deprecated/libnet-1.0.2a.tar.gz

If you are running Fedora, there is an excellent site with all the required fixes to get Dsniff up and running:
http://www.enzotech.net/dsniff.html

If all goes well, you can verify your install with the following commands:

```
sshow –h
sshmitm –h
```

Fragrouter
http://packetstormsecurity.org/UNIX/IDS/fragrouter-1.6.tar.gz

Download the above tar ball and install.

Live Linux File System Help

To produce the application menu in Knoppix-STD, right click anywhere on the screen.

To start the graphical interface with BackTrack, type in the command “startx”.

To assign an IP address in all three distros, use the ifconfig command:

```
ifconfig eth0 192.168.1.1
```

Some of the distros include a graphical tool for doing this, but they do not always work that well and can cause connectivity problems.

BackTrack will automatically mount any hard drive partitions it finds to the /mnt directory. Auditor and Knoppix-STD require you to manually mount drive partitions. To find out what partitions are on your system, type the command:

```
fdisk /dev/hda
```

and then press “p” followed by the Enter key. This will list all the partitions as well as the file system type. To quit fdisk, press “q” followed by the Enter key. To mount a partition, type the command:

```
mount /dev/hda1 /mnt/hda1
```

Replacing “hda1” with the device name reported by fdisk. Note that the directory /mnt/hda1 must already exist. If it does not, create it using the “mkdir” command before running the mount command.

To mount a USB flash drive, type the following commands:

```
mkdir /mnt/usbdrive
mount /dev/sda1 /mnt/usbdrive
```

Note that the live distros can sometimes be a bit finicky. For example Auditor seems happier if the USB flash drive is already connected to the system prior to booting, while BackTrack works better if you let the system boot and then plug in the flash drive. Try it both ways.