
Introduction to Windows and Linux

The student will be given an overview of the Windows and Linux operating systems in preparation for the tools used in the SANS Security Essentials Labs.

SANS Security Essentials – © 2011 SANS

Introduction to Operating Systems

It is important that you familiarize yourself with Windows and Linux in preparation for this course. The exercises in this book assume a basic knowledge of both of these operating systems. This chapter provides an overview of both operating systems. It is not intended as a comprehensive guide to Windows and Linux; it is intended to help prepare you for this course.

Windows (1)

- Understand the cmd prompt and critical commands including:
 - cmd
 - ipconfig
 - regedit
 - netstat
 - cls
 - dir
 - mkdir
 - Task Manager

SANS Security Essentials – © 2011 SANS

Windows (1)

The Windows operating system is a dynamic and continually changing operating system with new security patches and hot fixes being released often. In a normal production environment, it is highly recommended that you maintain a patching schedule to keep your systems up-to-date.

This "Introduction to Windows" guide teaches you about the basic commands and actions you need to know for the Security Essentials Labs. This document introduces you to the following: cmd, ipconfig, regedit, netstat, cls, dir, mkdir, and the Task Manager.

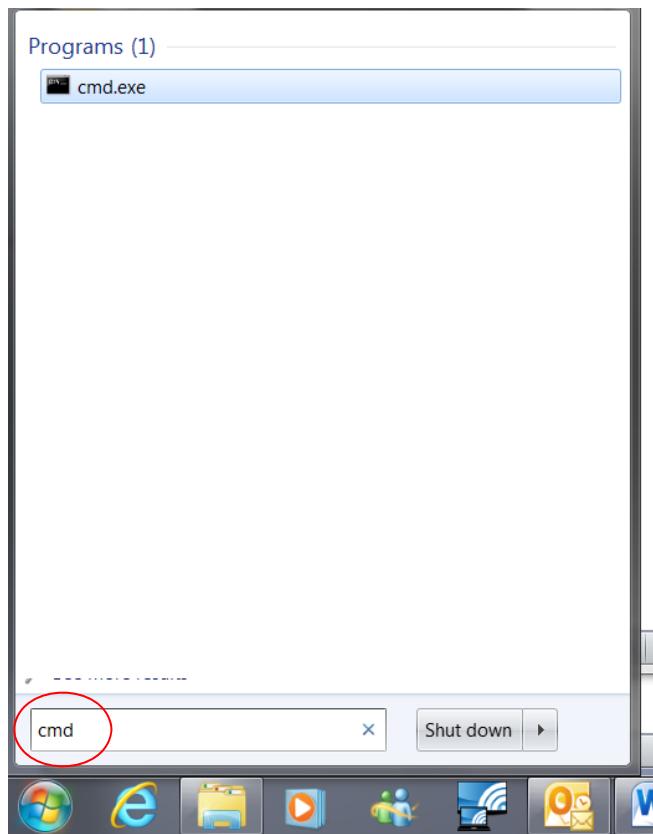
The Cmd Prompt

Since the release of Windows 2000 Professional, the old 16-bit command.com program has been replaced with the cmd.exe program. There are many benefits of using cmd including the following:

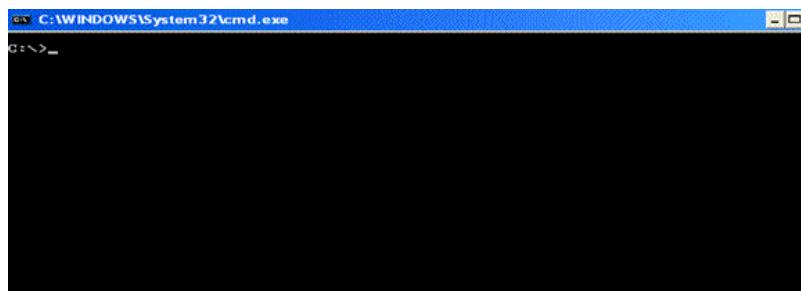
- The capability to run scripts in the CMD language
- WMIC (Windows Management Instrumentation Console)
- There are no 8.3 filename limitations
- The capability of running multiple commands on the same command line
- Support for command pipelines
- Help functionality with /?

The following list of tasks shows you how to use the command prompt to obtain help or information about your system:

1. To display the command prompt, select the Start icon and type cmd.



2. The following window appears...



2. If you need help with a command while using cmd, type `/?` after the command in question. For example, to get NIC TCP/IP information, type `ipconfig`. To get a list of the available `ipconfig` options, type `ipconfig /?` after the command prompt, as shown in the following screen.

```

C:\>ipconfig /?

USAGE:
  ipconfig [/? | /all | /renew [adapter] | /release [adapter] |
            /flushdns | /displaydns | /registerdns |
            /showclassid adapter |
            /setclassid adapter [classid] ]

where
  adapter      Connection name
              <wildcard characters * and ? allowed, see examples>

Options:
  /?           Display this help message
  /all         Display full configuration information.
  /release    Release the IP address for the specified adapter.
  /renew     Renew the IP address for the specified adapter.
  /flushdns  Purges the DNS Resolver cache.
  /registerdns Refreshes all DHCP leases and re-registers DNS names
  /displaydns Display the contents of the DNS Resolver Cache.
  /showclassid Displays all the dhcp class IDs allowed for adapter.
  /setclassid  Modifies the dhcp class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid, if no ClassId is specified, then the ClassId is removed.

Examples:
  > ipconfig           ... Show information.
  > ipconfig /all       ... Show detailed information
  > ipconfig /renew
  > ipconfig /renew EL* ... renew any connection that has its
                         ... name starting with EL
  > ipconfig /release *Con* ... release all matching connections,
                                eg. "Local Area Connection 1" or
                                "Local Area Connection 2"

```

3. To get the IP address information for your system, type ipconfig /all. This also displays your MAC address, as shown in the following screen. If you have a virtual machine application installed, you will receive other interfaces in addition to the below.

```

C:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : whoami
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . . . . . : AMD PCNET Family PCI Ethernet Adapter
  Physical Address. . . . . : 00-50-56-40-82-5B
  Dhcp Enabled. . . . . : No
  IP Address . . . . . : 192.168.1.2
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1

```

Windows (2)

- Understand the registry and how to edit it using
 - regedit
- Learn how to change IP addresses through network properties
- Learn how to connect to shares
- Use Task Manager
- Setup directories

SANS Security Essentials – © 2011 SANS

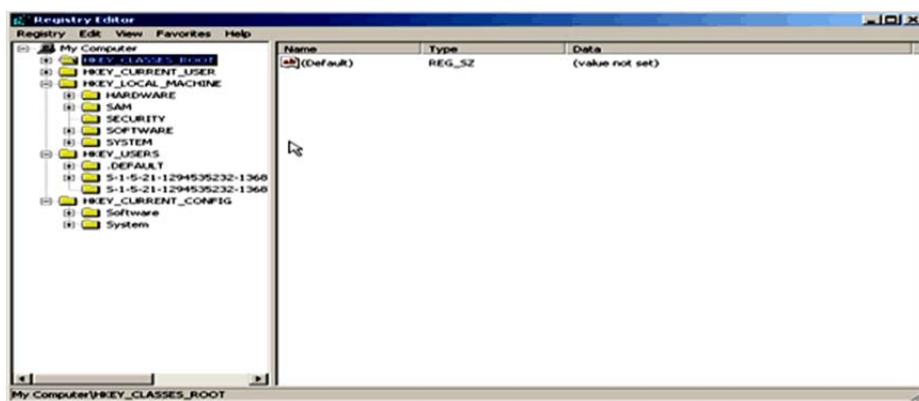
Windows (2)

To edit the registry in a Windows environment you can use the regedit command at the Run prompt. One of the nice features of using regedit is that you can search every hive for specific keys, values, and data.

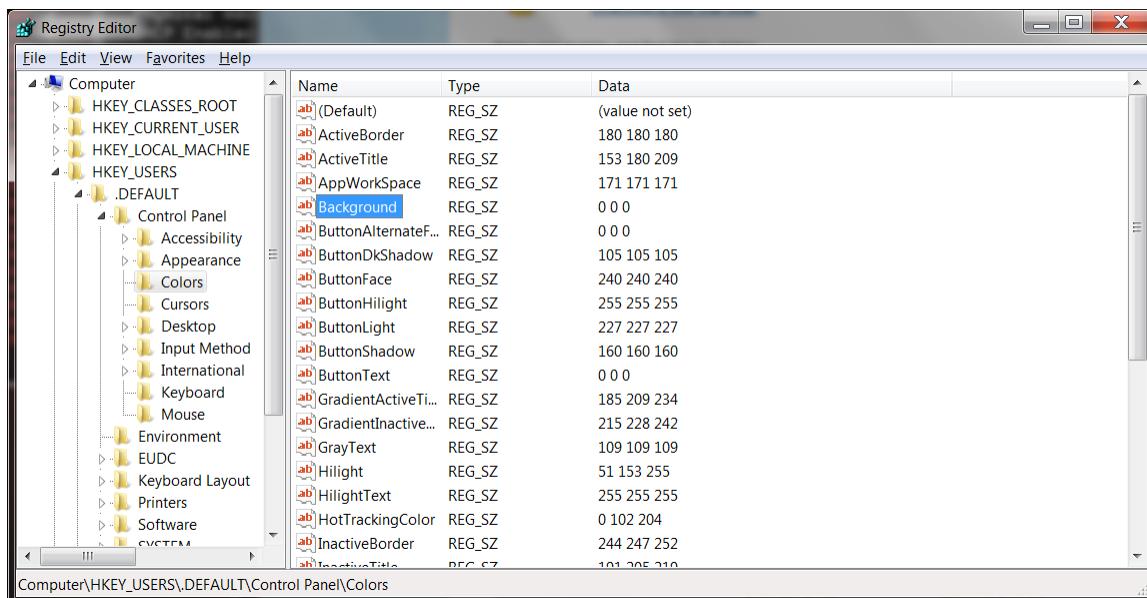
Warning: When using regedit, exercise extreme caution because any change you make is permanent and could potentially render your system unusable.

The following list of tasks explains how to edit the registry and how to use regedit:

1. To start regedit, choose Start, Run. Then, type regedit and press Enter. The following is a screen shot of regedit.



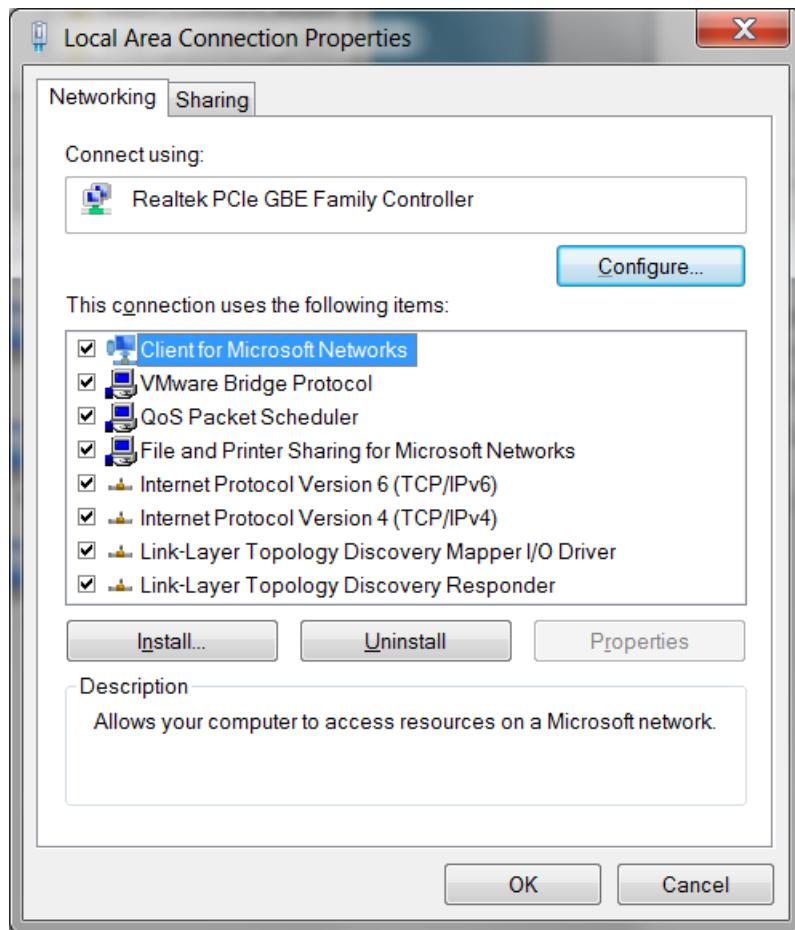
2. To ensure you can recover from making detrimental mistakes when editing the registry, you should always save a copy of the keys you change. To do this, right click on a registry key and select export from the menu.
3. There are a lot of powerful things you can do with the registry. To minimize any impact on your system, let's look at a relatively save example. To change the logon screen background color you would edit HKEY_USERS -> DEFAULT -> Control Panel -> Colors. You would change the color using RGB settings. For example 0 0 0 is black and 255 255 255 is white. If you do change the color, you would have to reboot the system for the change to apply. This was meant as an example, but it is not recommended that you change the color at this time.



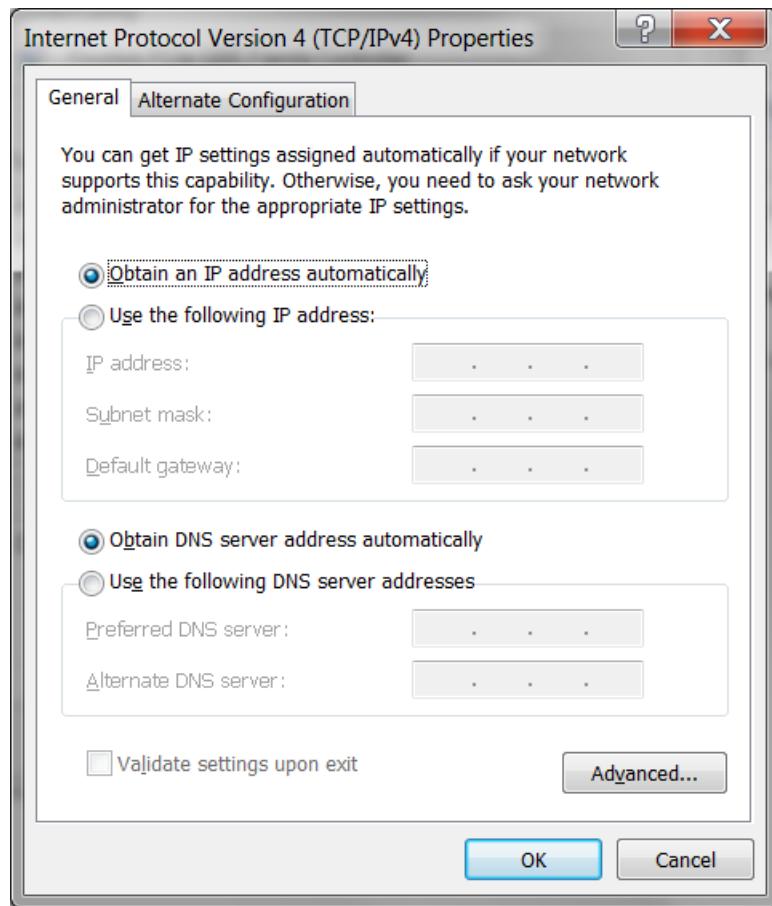
IP Changes

The following steps are necessary for making IP changes on your Windows system:

1. To make IP address changes to your local machine, open the NIC properties. Open up your Control Panel by choosing Start, Control Panel, select Network and Internet, then select View network status and tasks and finally select change adapter settings. Highlight the local area connection. Right-click the Local Area Connection, and click Properties. The following screen appears.



3. Highlight Internet Protocol (TCP/IP) and click the Properties button.
Most systems use DHCP but this is where you would change an address.
This could also be used as a basic way to spoof an IP address for certain types of attacks.



Viewing Ports

To see what ports are open on your box, you can use the netstat command, as shown in the following screen. Since you are not connected to a network, you might receive limited information.

```
C:\>netstat -an
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135           0.0.0.0:0             LISTENING
  TCP    0.0.0.0:445           0.0.0.0:0             LISTENING
  TCP    0.0.0.0:1025          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:5000          0.0.0.0:0             LISTENING
  TCP    192.168.1.2:139       0.0.0.0:0             LISTENING
  UDP   0.0.0.0:135           *:*                  *
  UDP   0.0.0.0:445           *:*                  *
  UDP   0.0.0.0:500           *:*                  *
  UDP   0.0.0.0:1026          *:*                  *
  UDP   0.0.0.0:1027          *:*                  *
  UDP   127.0.0.1:123         *:*                  *
  UDP   127.0.0.1:1900         *:*                  *
  UDP   192.168.1.2:123       *:*                  *
  UDP   192.168.1.2:137       *:*                  *
  UDP   192.168.1.2:138       *:*                  *
  UDP   192.168.1.2:1900      *:*                  *
```

You can see every open port and the state of each port. States include listening, waiting, or connected. The netstat command also shows you TCP and UDP connections.

While netstat will show you which ports are open, by default it does not show you which service is causing a given port to be open. Attackers connect to systems via ports. The more ports that are open, the more avenues of attack. Therefore it is important to shut down unneeded ports. In order to close a port you need to know which service is causing a given port to be open. By typing the following command: netstat -o will show which service is causing a given port to be open. It is important to note that if you do not have an active network connection, you might receive limited information.

```
C:\>netstat -o
Active Connections

  Proto  Local Address          Foreign Address        State      PID
  TCP    117CC360A849459:1036  205.188.9.244:5190  ESTABLISHED  1624
  TCP    117CC360A849459:1051  oam-d13c.blue.aol.com:5190  ESTABLISHED  1624
  TCP    117CC360A849459:1054  client-207-159-90-20.seccomputing.com:22  ESTABLISHED  2576
  ISHED  2576
  TCP    117CC360A849459:1079  mse6fe1.mse6.exchange.ms:https  ESTABLISHED
  2548
  TCP    117CC360A849459:1081  mse6fe1.mse6.exchange.ms:https  ESTABLISHED
  2548
  TCP    117CC360A849459:1088  mse6fe1.mse6.exchange.ms:https  ESTABLISHED
  2548
  TCP    117CC360A849459:1089  mse6fe1.mse6.exchange.ms:https  ESTABLISHED
  2548
  TCP    117CC360A849459:1094  ads.web.aol.com:http    ESTABLISHED  1624

C:\>
```

Other Useful Commands

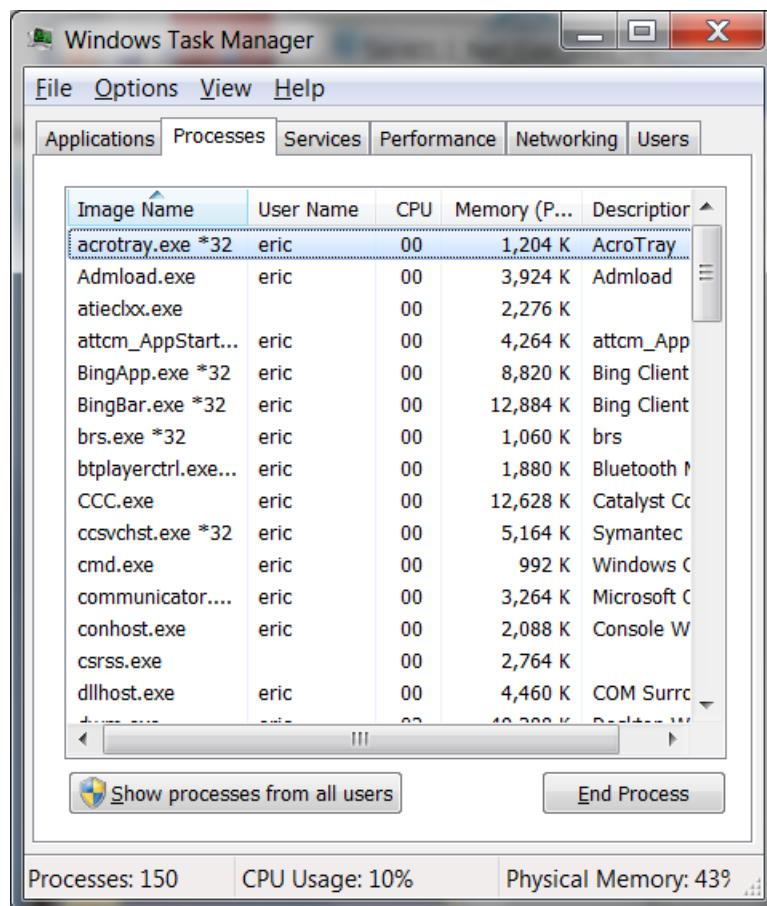
Some other commands to use at the cmd prompt are:

- **cls**-Clears everything on the screen and returns you to the top of the cmd window
- **dir**-Displays a directory listing
- **cd **-Returns you to c:\ from whatever directory you are in

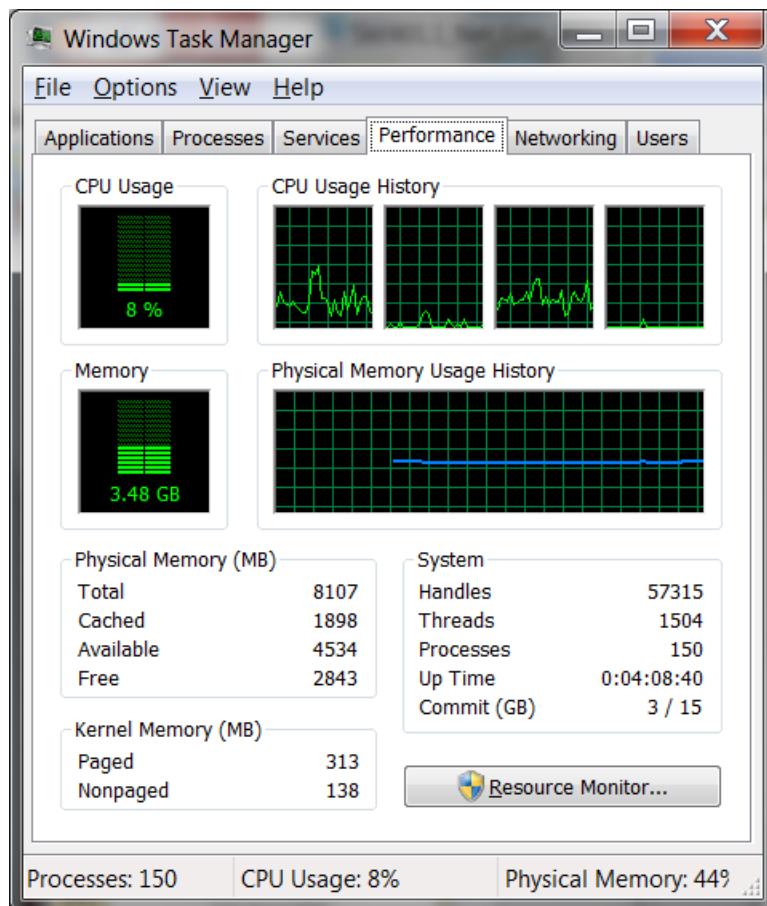
Task Manager

Another great built-in tool in Windows is the Task Manager. The following list shows you how to open and use the Task Manager:

1. To open hold down CTRL-ALT-DEL at the same time and select Task Manager. The default screen that opens shows which applications are running on the system.



2. From this window, you can check the running processes on the device, the performance trends, and the applications that are currently running. It is a great tool to open if you have an application that stops responding. You can open Task Manager, highlight the application, and then choose to close the offending application. By clicking on the performance tab, you can see CPU and memory usage.



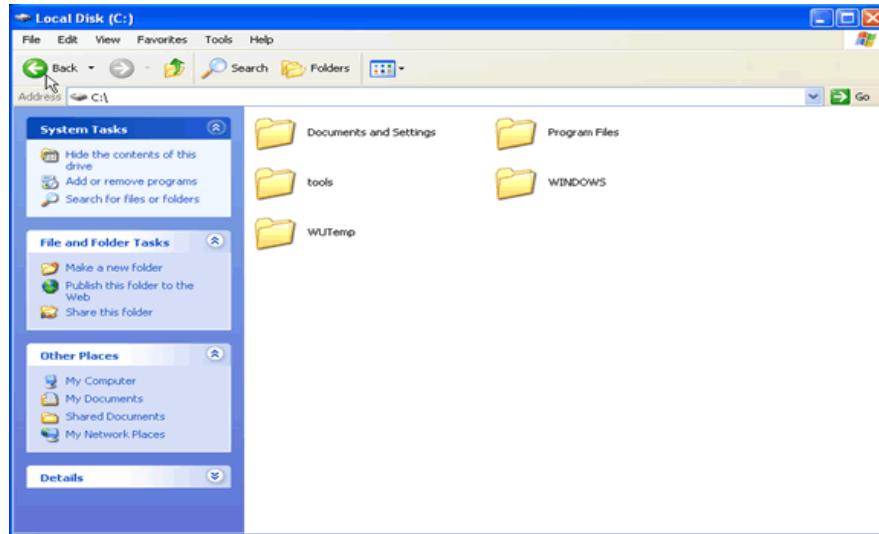
There are many other Windows functions that are not covered in this book. Our goal is to give you the basics, so that you can quickly install and run the tools covered throughout the following chapters.

Setting Up the Directory Structure

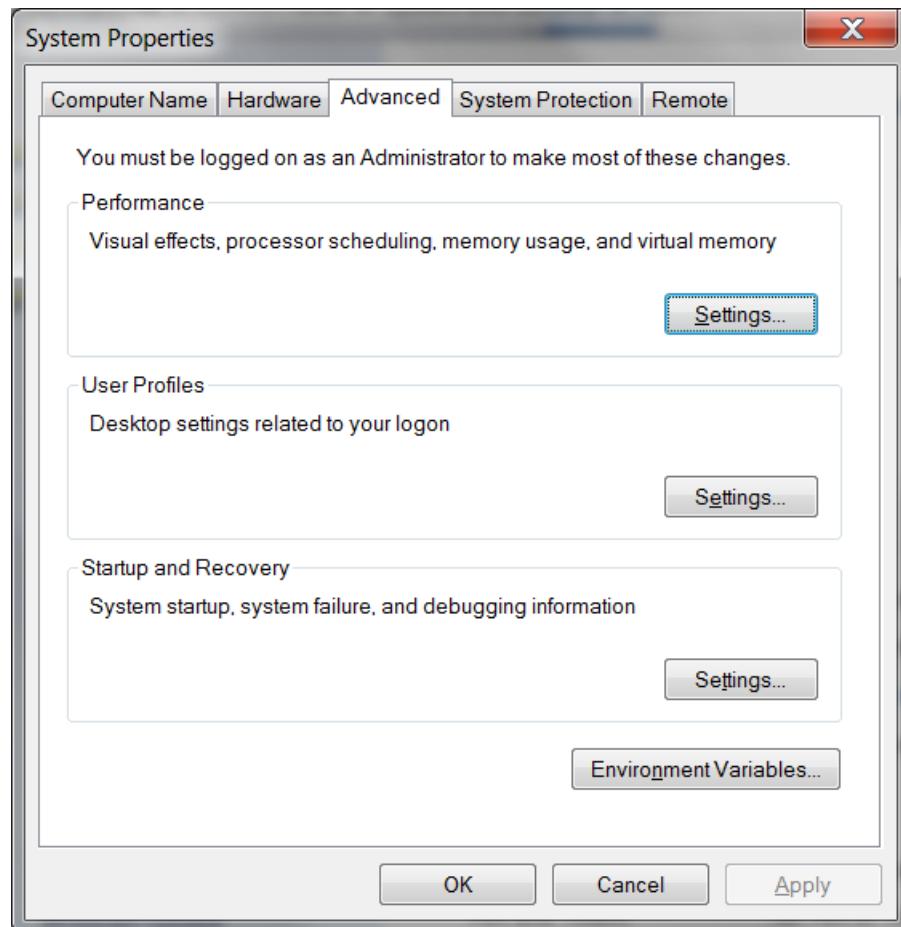
Now that you have installed the operating system and seen some of the tools that are built into it, you need to set up your directory structure, so that it's consistent with the directory structure used for installing and storing the tools discussed in this book. Follow these steps to setup the directory structure:

1. First click on Start, My Computer and then double-click Local Disk (c:). The window that appears lists the structure of the C:\ drive. Right-click a spot in the window that is blank. Move your mouse down the menu that appears and left-click New and choose

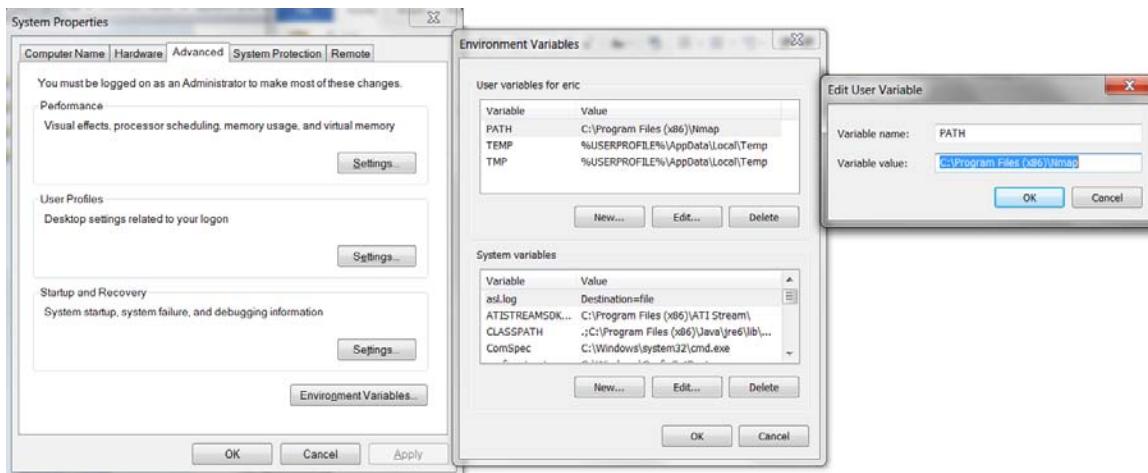
Folder. Name the folder tools. The following screen shows a directory structure with the new tools folder.



2. The exercises in this book require you to run several tools from the command line. Thus, you need to add the new folder we created, c:\tools, to PATH. If you do this, you won't have to navigate to the tools folder each time you want to run an application. To add the folder to PATH, Click on Start, right-click on My Computer, and choose Properties from the pop-up menu. Click the Advanced system settings option, as shown in the following screen.



3. Click the Environment Variables button. In the System Variables section, highlight the line labeled Path and click Edit.



4. In the Variable Value field, move your cursor to the end of the line and add the following exactly as it is shown here:

;c:\tools

Click OK on each of the Edit System Variable, Environment Variables and System Properties windows.

The executables located in c:\tools can now be run from any directory in your file structure. This saves a lot of time when you are using the command prompt and want to run an application from it.

Linux

- Learn how to login
- Create accounts
- Understand file and directory manipulation and the associated commands, which include:
 - ls
 - ls -al
 - mkdir
- Learn how to use the power of man
- Changing directories using the following:
 - cd
 - pwd

SANS Security Essentials – © 2011 SANS

Linux

Linux is an open source operating system that runs on a wide range of hardware platforms. So what is open source? As an open source system, Linux is protected under the GNU General Public License, which guarantees the freedom to use and change the software it covers. Numerous Linux distributions are available from many companies, and each distribution has its own advantages and disadvantages. With these characteristics comes a faithful user following who think that their preferred distribution is the best. Some of the Linux distributions that are currently available include Red Hat, SUSE, Debian, and Mandrake.

As Linux became popular, various versions have been created. The version we will use in class is BackTrack.

At the heart of each distribution is the kernel, which interacts directly with the hardware. The kernel handles such functions as memory management, security, and resource allocation. The kernel also provides features such as true multitasking, threading, and TCP/IP networking. Contrary to popular belief, the kernel is, in fact, Linux. All other applications and programs are part of a particular distribution.

The Linux shell is another name for the command shell, which is similar in function to a DOS shell. It is the program that gives you an interface to type commands, and it accepts the commands you type. During the examples that follow, remember that nearly everything in Linux is case sensitive.

Starting up BackTrack

Once the system boots up, you will be required to log on to the system. Logon with a userID of root and a password of toor (remember the password is just root backwards) and hit enter.

BT5R2-GNOME-VM-32 - VMware Player File ▾ Virtual Machine ▾ Help ▾



<< back | track 5 >>

```
[ 2.685612] scsi12 : ioc0: LSI153C1030 B0, FwRev=01032920h, Ports=1, MaxQ=128, IRQ=17
[ 2.790289] hub 2-2:1.0: USB hub found
[ 2.801393] scsi 2:0:0:0: Direct-Access     VMware, VMware Virtual S 1.0 PQ: 0 ANSI: 2
[ 2.805889] scsi target2:0:0: Beginning Domain Validation
[ 2.806048] hub 2-2:1.0: 7 ports detected
[ 2.807293] scsi target2:0:0: Domain Validation skipping write tests
[ 2.809923] scsi target2:0:0: Ending Domain Validation
[ 2.810130] scsi target2:0:0: FAST-40 WIDE SCSI 80.0 MB/s ST (25 ns, offset 127)
[ 2.814190] sd 2:0:0:0: [sda] 62914560 512-byte logical blocks: (32.2 GB/30.0 GiB)
[ 2.814346] sd 2:0:0:0: [sda] Write Protect is off
[ 2.814545] sd 2:0:0:0: [sda] Cache data unavailable
[ 2.814623] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 2.815181] sd 2:0:0:0: [sda] Cache data unavailable
[ 2.815196] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 2.816101] sda: sda1 sda2 < sda5 >
[ 2.819735] sd 2:0:0:0: [sda] Cache data unavailable
[ 2.819813] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 2.819891] sd 2:0:0:0: [sda] Attached SCSI disk
[ 2.821333] sd 2:0:0:0: Attached scsi generic sg1 type 0
[ 2.829309] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2
/2-1/2-1:1.0/input/input2
[ 2.829938] generic-usb 0003:0EOF:0003.0001: input,hidraw0: USB HID v1.10 Mouse [VMware VMware Virtual U
SB Mouse] on usb-0000:02:00.0-1/input0
[ 2.831853] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2
/2-1/2-1:1.1/input/input3
[ 2.834626] generic-usb 0003:0EOF:0003.0002: input,hidraw1: USB HID v1.10 Mouse [VMware VMware Virtual U
SB Mouse] on usb-0000:02:00.0-1/input1
[ 2.834842] usbcore: registered new interface driver usbhid
[ 2.834921] usbhid: USB HID core driver
[ 3.085309] usb 2-2:1: new full-speed USB device number 4 using uhci_hcd
```

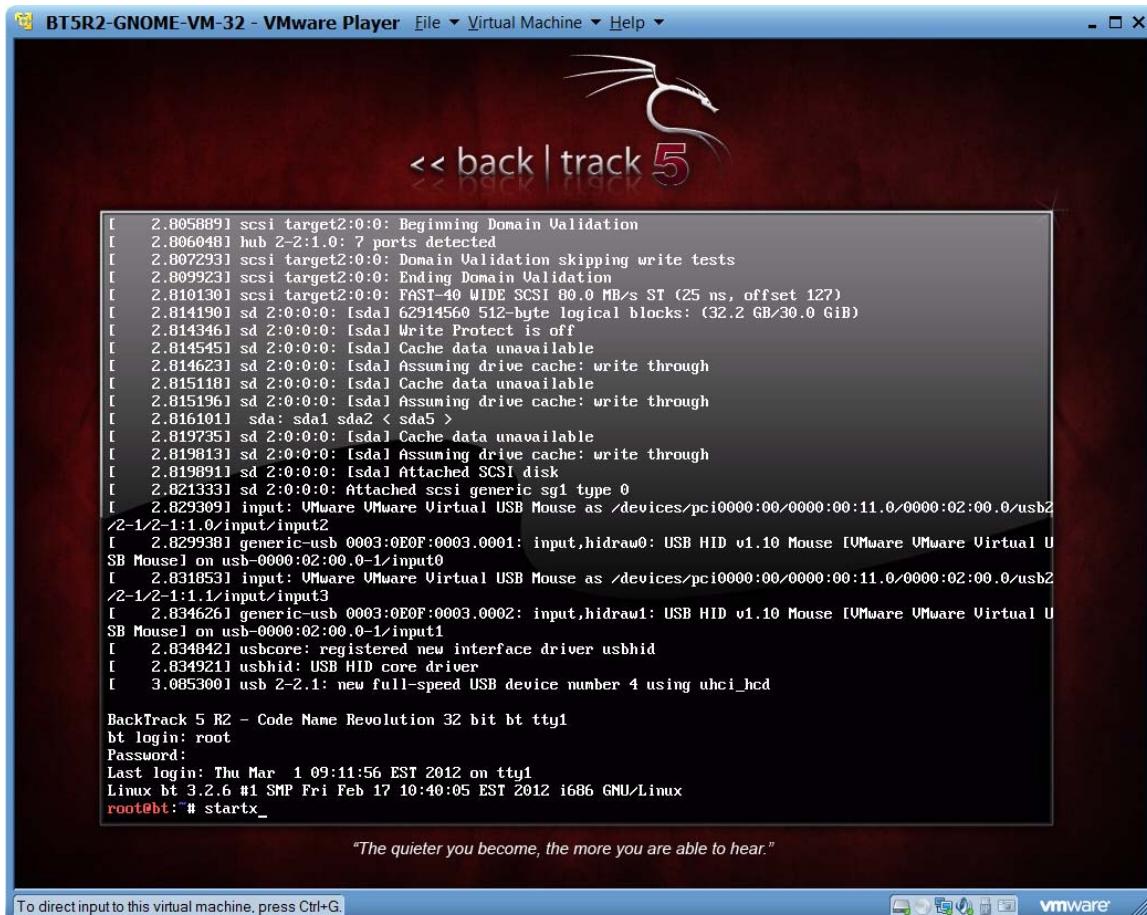
BackTrack 5 R2 - Code Name Revolution 32 bit bt tty1
bt login: root
Password:

"The quieter you become, the more you are able to hear."

To direct input to this virtual machine, press Ctrl+G.



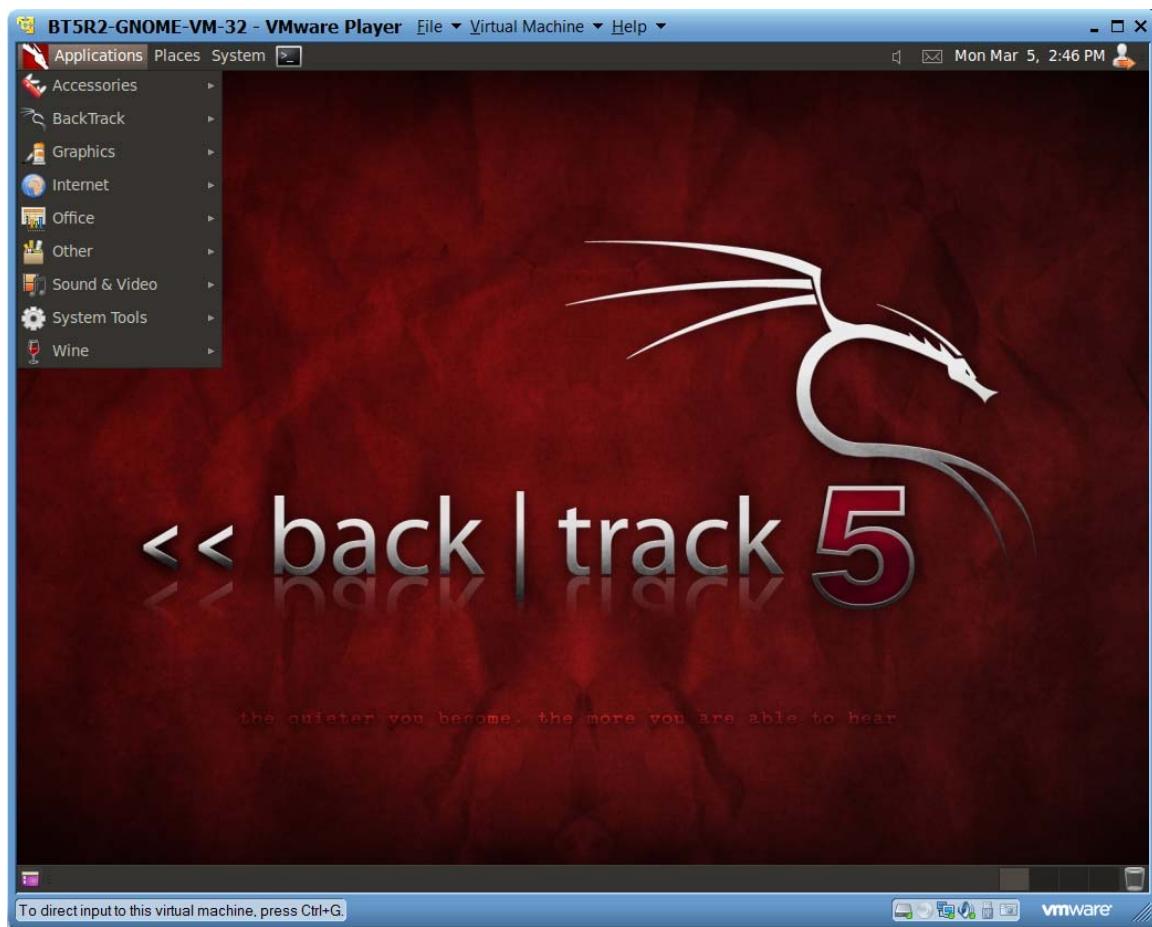
At the root prompt, type **startx** to start up the GUI.



To direct input to this virtual machine, press Ctrl+G.

vmware

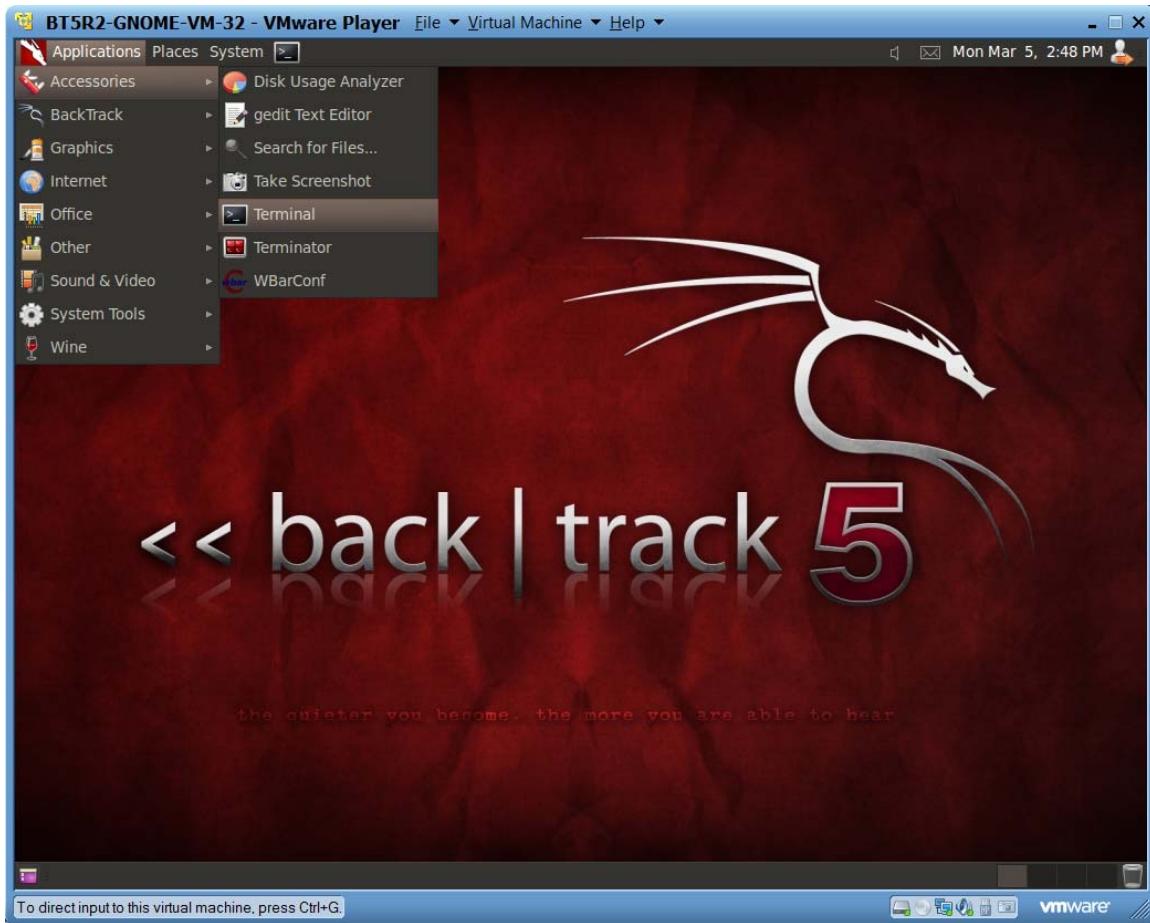
The BackTrack GUI will start. You would click on the Application menu in the upper left hand corner to run programs on the system.



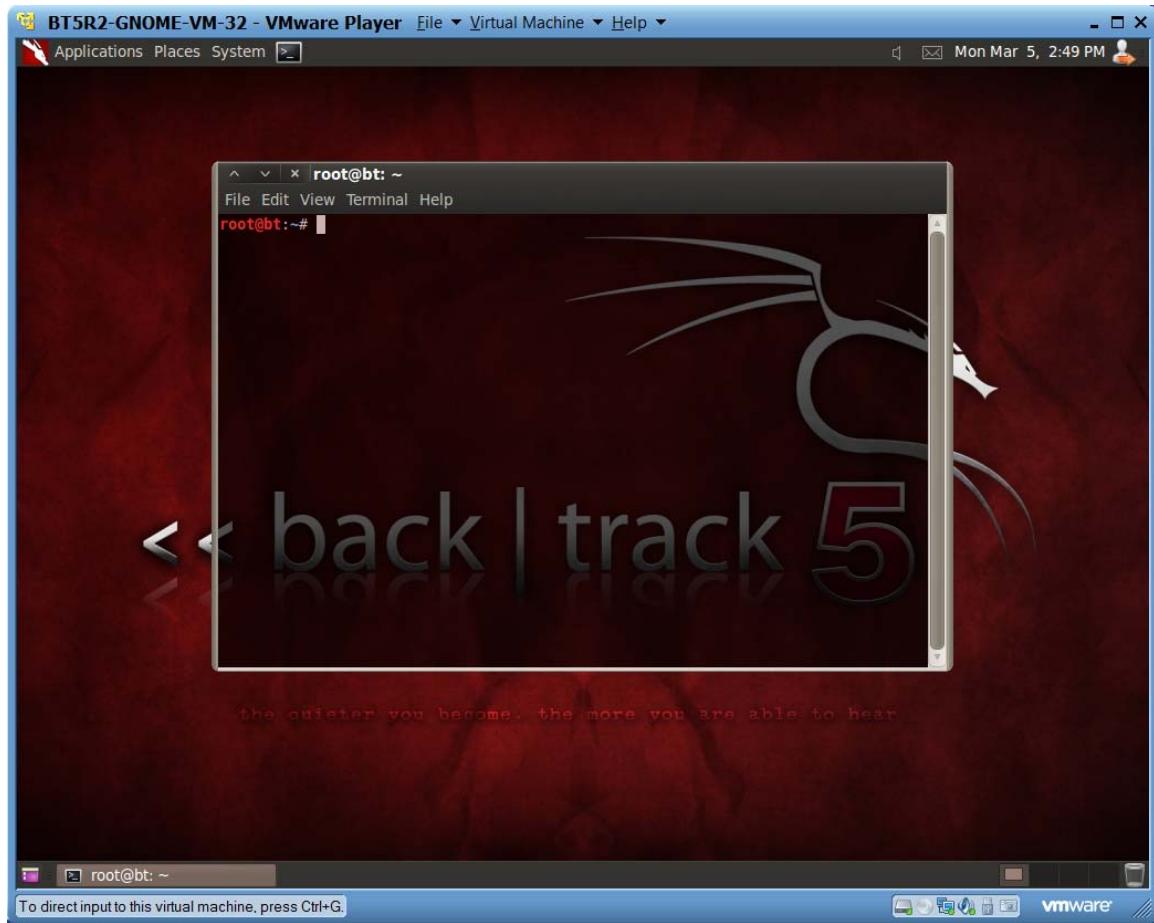
Click on BackTrack from the Applications menu to see all of the security tools you already have installed.



Many of the tools will be run from a root terminal shell. While there are many ways to open a root terminal shell, the easiest is to go to the Application menu, select Accessories and select Terminal.



A root terminal shell will open. You can tell you are at a root shell because the prompt is the # symbol. If the prompt was a \$ that would mean you are logged in as a normal user. In a normal production environment you would always login as a normal user. In order to run many of the labs in this course we will have you log in as root.



To learn about the tools and ensure that everything works correctly, most of what we will be doing in the labs will be from a root shell.

Linux (2)

- File viewing/manipulation
 - ls
 - less
- Accounts
 - su
 - whoami
- System Configuration
 - ping
 - netstat
 - ps

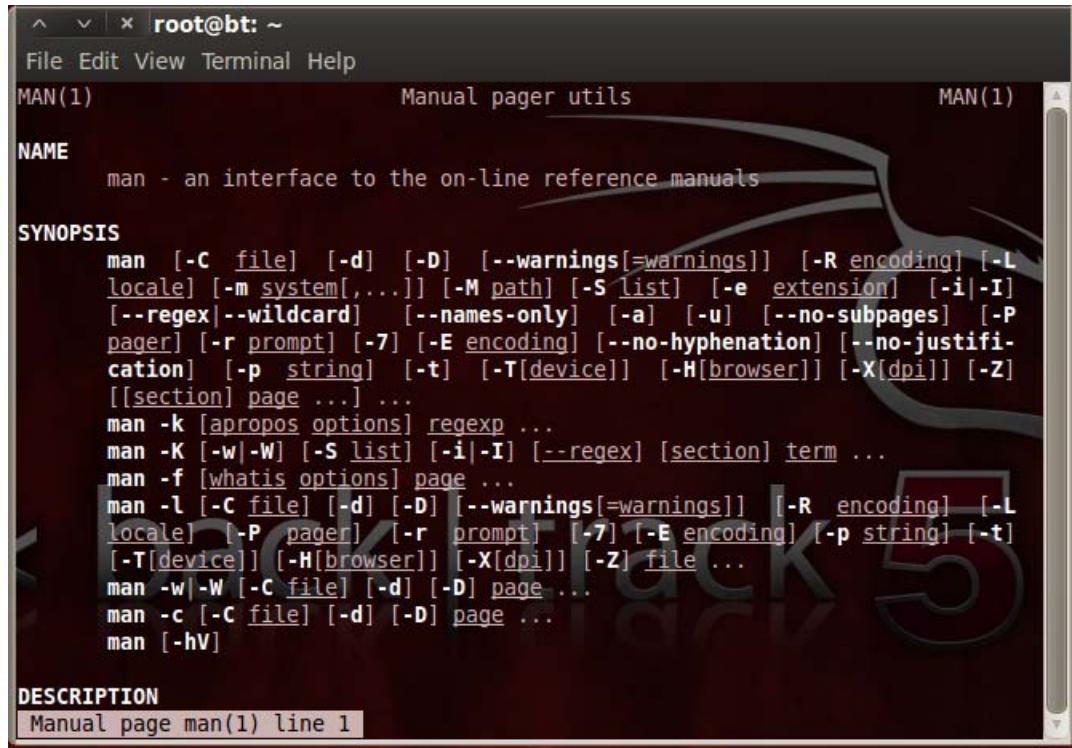
SANS Security Essentials – © 2011 SANS

Linux (2)

This section introduces you to the basics of Linux by covering some of the most common commands, files, and directories used in Linux. Each topic includes a brief description and an example of how the topic is used. You can find more information on each topic by typing man. For example, issue the following command at a shell prompt:

man man

This command displays a manual that describes the man command and also demonstrates how man pages are formatted.



```
^ ~ | x | root@bt: ~
File Edit View Terminal Help
MAN(1)                               Manual pager utils                         MAN(1)
NAME
    man - an interface to the on-line reference manuals
SYNOPSIS
    man [-C file] [-d] [-D] [--warnings[=warnings]] [-R encoding] [-L
    locale] [-m system[,...]] [-M path] [-S list] [-e extension] [-i|-I]
    [--regex|--wildcard] [--names-only] [-a] [-u] [--no-subpages] [-P
    pager] [-r prompt] [-7] [-E encoding] [--no-hyphenation] [--no-justifi-
    cation] [-p string] [-t] [-T[device]] [-H[browser]] [-X[dpi]] [-Z]
    [[section] page ...] ...
    man -k [apropos options] regexp ...
    man -K [-w|-W] [-S list] [-i|-I] [--regex] [section] term ...
    man -f [whatis options] page ...
    man -l [-C file] [-d] [-D] [--warnings[=warnings]] [-R encoding] [-L
    locale] [-P pager] [-r prompt] [-7] [-E encoding] [-p string] [-t]
    [-T[device]] [-H[browser]] [-X[dpi]] [-Z] file ...
    man -w|-W [-C file] [-d] [-D] page ...
    man -c [-C file] [-d] [-D] page ...
    man [-hV]

DESCRIPTION
    Manual page man(1) line 1
```

The ls Command

One of the most basic commands in Linux is ls. Just as you use dir in DOS, type ls to output a listing of the directories and files that are contained within the current directory. Open a root shell as described above. Now, in the command shell, type ls, as shown in the following screen. Trying typing a few commands to get comfortable with the directory structure.

```
^ ~ x root@bt: /  
File Edit View Terminal Help  
root@bt:~# ls  
Desktop  
root@bt:~# pwd  
/root  
root@bt:~# cd ..  
root@bt:/# pwd  
/  
root@bt:/# ls  
bin dev initrd.img media pentest sbin srv usr  
boot etc lib mnt proc selinux sys var  
cdrom home lost+found opt root share tmp vmlinuz  
root@bt:/# ls -l  
total 112  
drwxr-xr-x 2 root root 4096 2012-03-01 08:11 bin  
drwxr-xr-x 3 root root 4096 2012-03-01 08:46 boot  
drwxr-xr-x 2 root root 4096 2011-03-05 11:41 cdrom  
drwxr-xr-x 15 root root 4600 2012-03-05 14:45 dev  
drwxr-xr-x 141 root root 12288 2012-03-05 14:44 etc  
drwxr-xr-x 2 root root 4096 2011-03-05 15:40 home  
lrwxrwxrwx 1 root root 21 2012-03-01 08:11 initrd.img -> boot/initrd.img-3.  
2:6  
drwxr-xr-x 26 root root 12288 2012-03-01 08:11 lib  
drwx----- 2 root root 16384 2011-03-05 11:40 lost+found  
drwxr-xr-x 4 root root 4096 2012-03-01 08:38 media  
drwxr-xr-x 3 root root 4096 2012-03-01 08:38 mnt  
drwxr-xr-x 12 root root 4096 2012-02-28 09:12 opt  
drwxr-xr-x 26 root root 4096 2012-02-23 23:37 pentest  
dr-xr-xr-x 121 root root 0 2012-03-05 14:43 proc  
drwx----- 20 root root 4096 2012-03-05 14:45 root  
drwxr-xr-x 2 root root 12288 2012-03-01 08:37 sbin  
drwxr-xr-x 2 root root 4096 2009-12-05 16:55 selinux  
drwxr-xr-x 4 root root 4096 2011-05-10 03:42 share  
drwxr-xr-x 3 root root 4096 2011-07-12 06:59 srv  
drwxr-xr-x 12 root root 0 2012-03-05 14:43 sys  
drwxrwxrwt 10 root root 4096 2012-03-05 14:53 tmp  
drwxr-xr-x 12 root root 4096 2011-05-10 03:41 usr  
drwxr-xr-x 16 root root 4096 2011-06-08 09:16 var
```

As with most commands in Linux, you can specify options to change the result of the command's execution. For example, enter ls -al in the command shell, as shown in the following screen.

```
^ v x | root@bt: /  
File Edit View Terminal Help  
root@bt:/# ls -al  
total 120  
drwxr-xr-x 24 root root 4096 2012-03-01 08:11 .  
drwxr-xr-x 24 root root 4096 2012-03-01 08:11 ..  
drwxr-xr-x 2 root root 4096 2012-03-01 08:11 bin  
drwxr-xr-x 3 root root 4096 2012-03-01 08:46 boot  
drwxr-xr-x 2 root root 4096 2011-03-05 11:41 cdrom  
drwxr-xr-x 15 root root 4600 2012-03-05 14:45 dev  
drwxr-xr-x 141 root root 12288 2012-03-05 14:44 etc  
drwxr-xr-x 2 root root 4096 2011-03-05 15:40 home  
lrwxrwxrwx 1 root root 21 2012-03-01 08:11 initrd.img -> boot/initrd.img-3.2.6  
drwxr-xr-x 26 root root 12288 2012-03-01 08:11 lib  
drwx----- 2 root root 16384 2011-03-05 11:40 lost+found  
drwxr-xr-x 4 root root 4096 2012-03-01 08:38 media  
drwxr-xr-x 3 root root 4096 2012-03-01 08:38 mnt  
drwxr-xr-x 12 root root 4096 2012-02-28 09:12 opt  
drwxr-xr-x 26 root root 4096 2012-02-23 23:37 pentest  
dr-xr-xr-x 121 root root 0 2012-03-05 14:43 proc  
drwx----- 20 root root 4096 2012-03-05 14:45 root  
drwxr-xr-x 2 root root 12288 2012-03-01 08:37 sbin  
drwxr-xr-x 2 root root 4096 2009-12-05 16:55 selinux  
drwxr-xr-x 4 root root 4096 2011-05-10 03:42 share  
drwxr-xr-x 3 root root 4096 2011-07-12 06:59 srv  
drwxr-xr-x 12 root root 0 2012-03-05 14:43 sys  
drwxrwxrwt 10 root root 4096 2012-03-05 14:54 tmp  
drwxr-xr-x 12 root root 4096 2011-05-10 03:41 usr  
drwxr-xr-x 16 root root 4096 2011-06-08 09:16 var  
lrwxrwxrwx 1 root root 18 2012-03-01 08:11 vmlinuz -> boot/vmlinuz-3.2.6  
root@bt:/#  
root@bt:/#  
root@bt:/# I think you become the root, you are able to do  
root@bt:/#  
root@bt:/#  
root@bt:/#  
root@bt:/#  
root@bt:/#  
root@bt:/#
```

The -a option tells the command interpreter to show all files, and -l tells it to use the long listing format. These are two of the many options that can be used with ls.

Changing Directories and Creating Directories

Now that you can tell what files and directories the root directory contains, let's move back to the / directory. In order to change directories, you use the cd command; here, you would use the command cd /, as shown in the following screen.



The screenshot shows a terminal window titled "root@bt: /". The window has a dark background with a faint "back | track 5" watermark. The terminal menu bar includes "File", "Edit", "View", "Terminal", and "Help". The command history shows:

```
root@bt:~# pwd
/root
root@bt:~# cd /
root@bt:/# pwd
/
root@bt:/#
```

You can use the mkdir command to create a directory. The format of the mkdir command is mkdir <new directory name>. For example, type mkdir downloads to create a location where we save files that have been downloaded from the Internet.

A screenshot of a terminal window titled "root@bt: ~". The window shows the following command-line session:

```
root@bt:~# ls
Desktop
root@bt:~# mkdir downloads
root@bt:~# ls
Desktop  downloads
root@bt:~# ls -l
total 8
drwxr-xr-x 2 root root 4096 2012-03-01 08:44 Desktop
drwxr-xr-x 2 root root 4096 2012-03-05 14:58 downloads
root@bt:~#
```

The terminal is running on the BackTrack 5 desktop environment, which features a dark background with the "back|track 5" logo.

Issuing ls after the mkdir shows the newly created download directory, as shown in blue in the previous screen.

Determining Directory Placement

After using cd and ls to learn about the Linux structure of changing directories, you may not remember which directory you are currently in. You can determine where you are in the directory structure by typing pwd (print working directory).

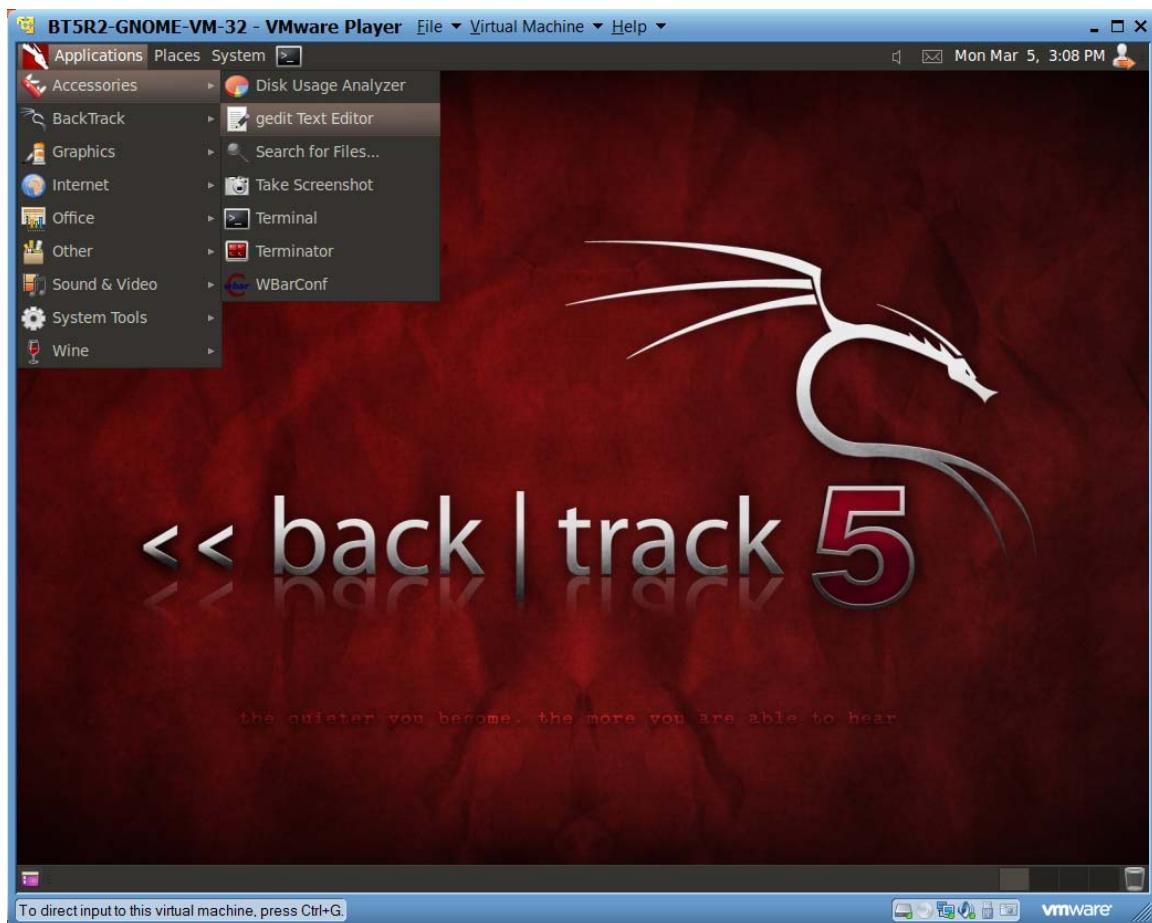
The screenshot shows a terminal window titled 'root@bt: /bin'. The terminal displays the following command-line session:

```
root@bt:~# pwd
/root
root@bt:~# cd /
root@bt:/# pwd
/
root@bt:/# ls
bin dev initrd.img media pentest sbin srv usr
boot etc lib mnt proc selinux sys var
cdrom home lost+found opt root share tmp vmlinuz
root@bt:/# cd bin
root@bt:/bin# pwd
/bin
root@bt:/bin#
```

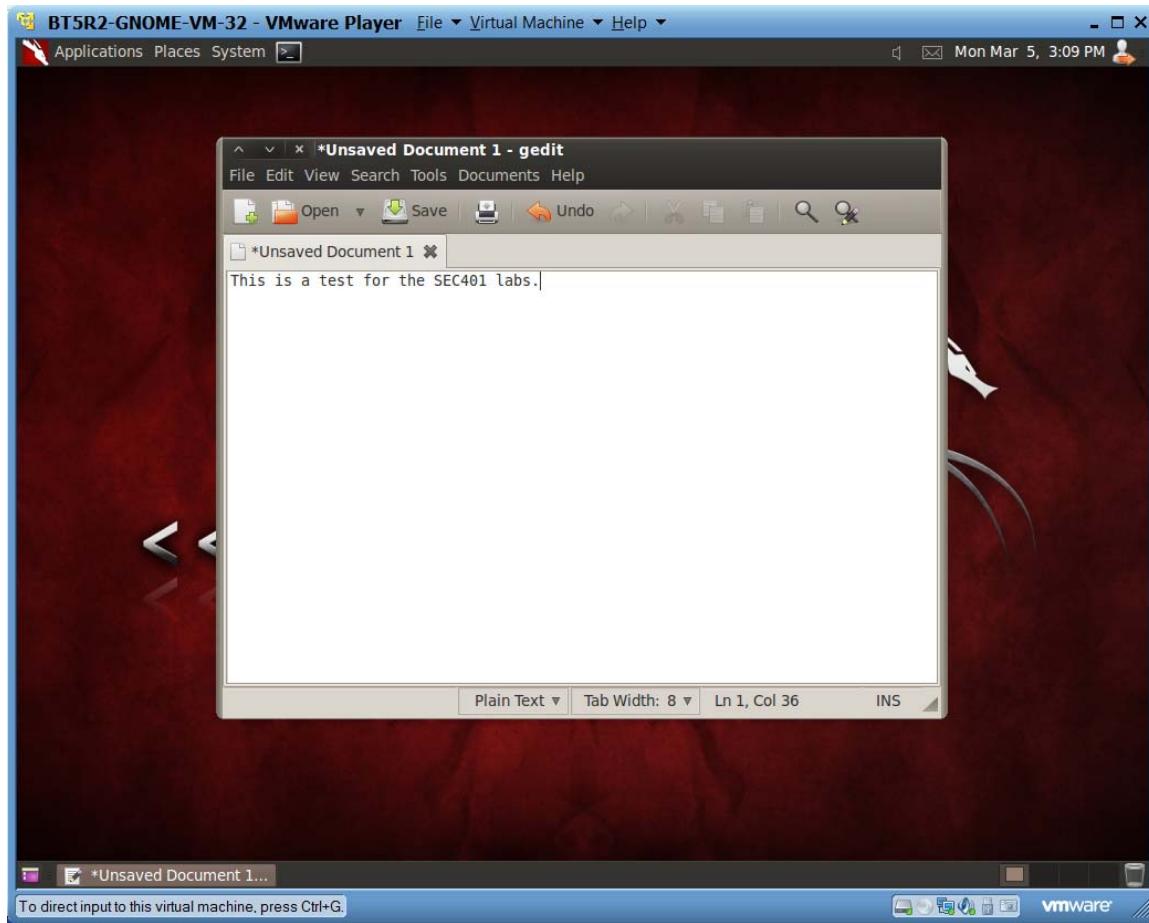
The background of the terminal window features the 'back | track 5' logo.

Creating Files

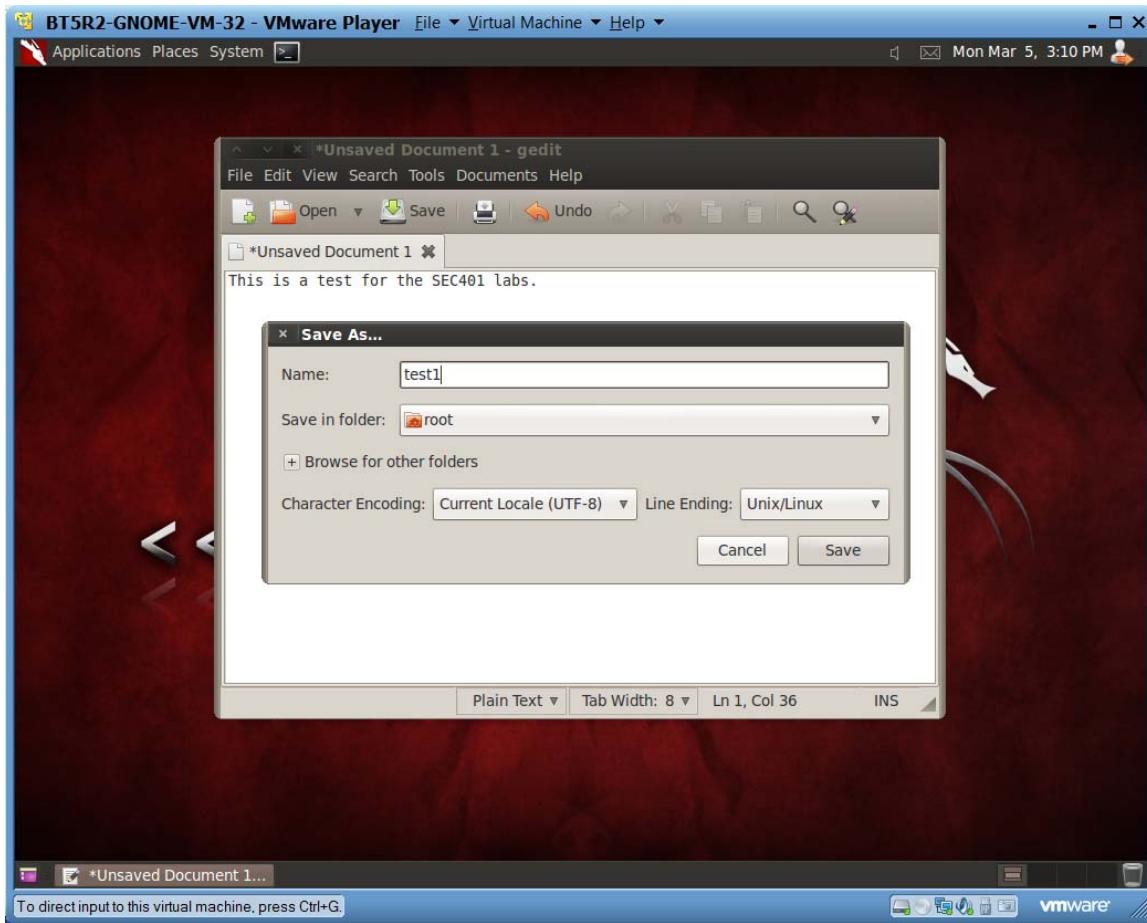
To create a file you can use gedit. To run gedit from the Applications menu select Accessories and gedit Text Editor.



The text editor will open. Type a phrase in the editor.



When you are done typing your phrase, from the File menu, select Save As and type a name for your file and hit save. When done, select Quit from the File menu to exit the program.



Viewing Files

There are many ways to view the contents of a file in Linux. One command you can use for this function is less. To view the contents of the `linux_lab` file that we just created, follow these steps:

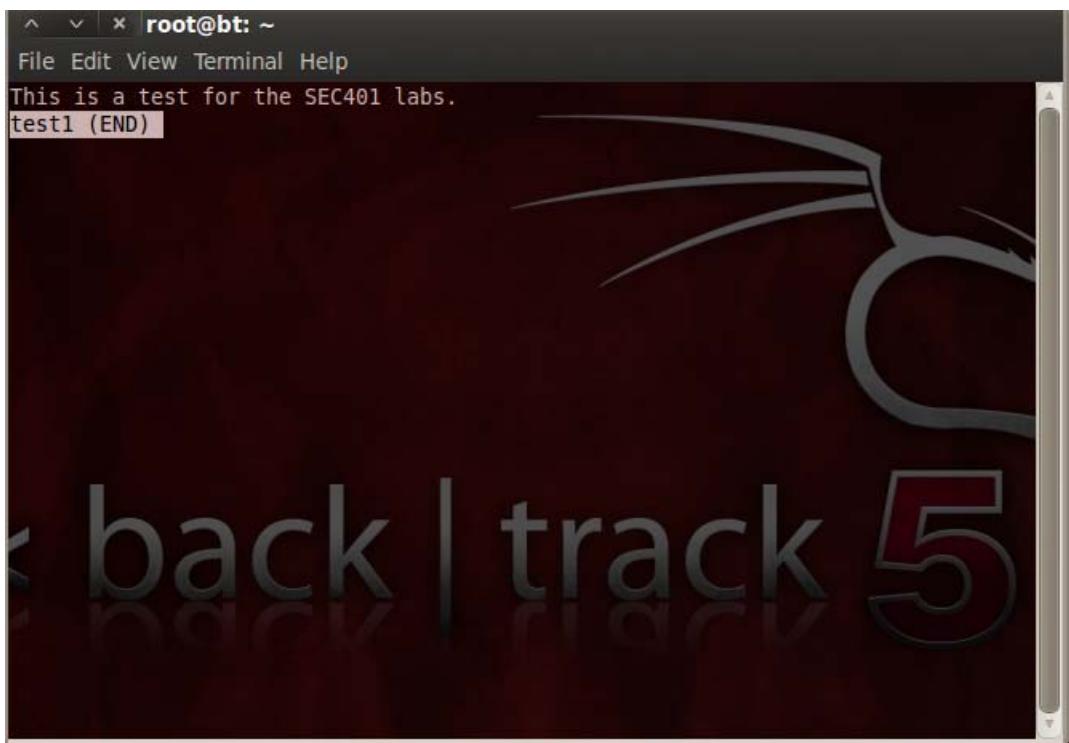
1. Open up a root terminal window.
2. Issue the command `cd /root` to change to the root directory.
3. Type `ls` to confirm that your file is listed

A screenshot of a terminal window on a BackTrack 5 desktop. The terminal title is 'root@bt: ~'. The menu bar includes 'File', 'Edit', 'View', 'Terminal', and 'Help'. The command history shows:

```
root@bt:~# cd /root
root@bt:~# ls
Desktop  downloads  test1
root@bt:~# less test1
```

The background of the desktop is the BackTrack 5 logo, which features a stylized cat head and the text 'back | track 5'.

4. Type **less test1** to view the content of the file.

A screenshot of a terminal window on a BackTrack 5 desktop. The terminal title is 'root@bt: ~'. The menu bar includes 'File', 'Edit', 'View', 'Terminal', and 'Help'. The command history shows:

```
This is a test for the SEC401 labs.
test1 (END)
```

The background of the desktop is the BackTrack 5 logo, which features a stylized cat head and the text 'back | track 5'.

5. The arrow keys allow you to navigate through the contents of the file. When you have finished, type q to exit and return back to the command shell.

Determining Account Types

As you gain more Linux experience, you will find yourself telnetting or ssh-ing to other systems on your network, or on the Internet. Knowing which account you are currently logged in as is vital; to determine this, type whoami.

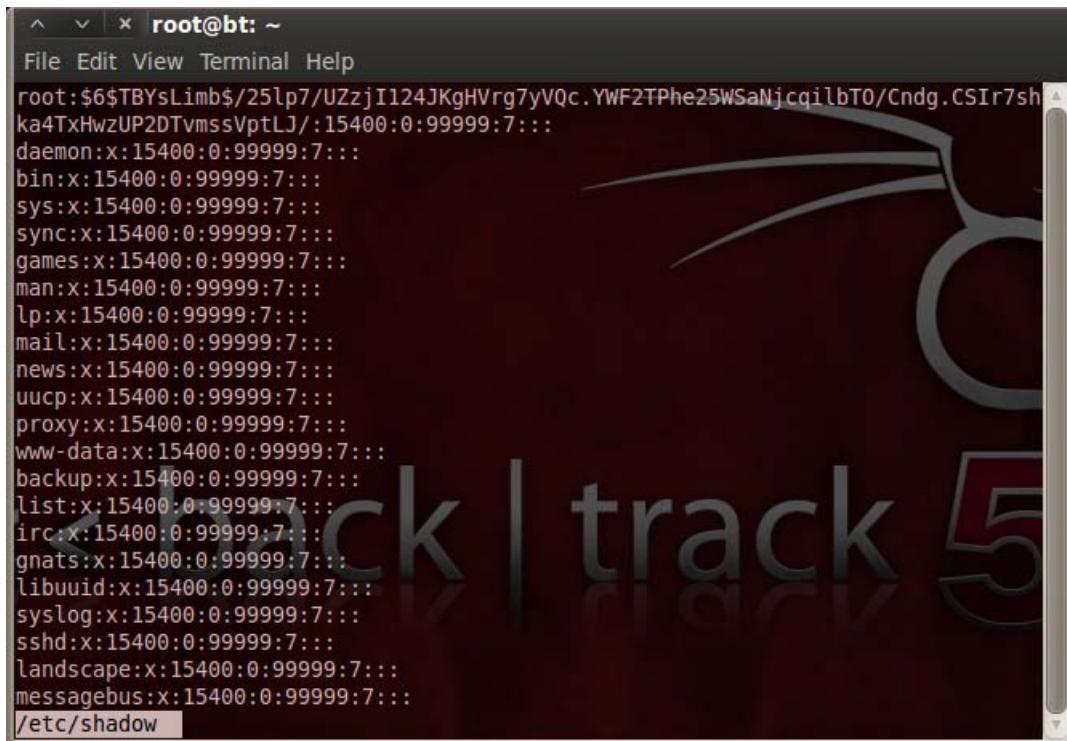


Common Files and Directories

Some user information is stored in a file called **passwd**, which is located in the **/etc** directory. This file also contains the path to the user's home directory, as well as to the current shell. Issue the command **less /etc/passwd** to view the contents of **passwd**. Press **q** to exit less.

```
^ v x root@bt: ~
File Edit View Terminal Help
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:::6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
landscape:x:103:108::/var/lib/landscape:/bin/false
messagebus:x:104:112::/var/run/dbus:/bin/false
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
/etc/passwd
```

Notice that since the Linux default is to use a shadow file, the password for all accounts is listed as x. The shadow file contains an encrypted version of the actual password, and is used to enhance security. The permissions on the shadow file are generally more restrictive than the passwd file. To view the contents of the shadow file, issue the command less /etc/shadow. Press q to exit less.



The screenshot shows a terminal window titled "root@bt: ~" with the following text displayed:

```
File Edit View Terminal Help
root:$6$TBYsLimb$/25lp7/UZzjI124JKgHVrg7yVQc.YWF2TPhe25WSaNjcqilbT0/Cndg.CSIr7sh
ka4TxHwzUP2DTvmsVptLJ/:15400:0:99999:7:::
daemon:x:15400:0:99999:7:::
bin:x:15400:0:99999:7:::
sys:x:15400:0:99999:7:::
sync:x:15400:0:99999:7:::
games:x:15400:0:99999:7:::
man:x:15400:0:99999:7:::
lp:x:15400:0:99999:7:::
mail:x:15400:0:99999:7:::
news:x:15400:0:99999:7:::
uucp:x:15400:0:99999:7:::
proxy:x:15400:0:99999:7:::
www-data:x:15400:0:99999:7:::
backup:x:15400:0:99999:7:::
list:x:15400:0:99999:7:::
irc:x:15400:0:99999:7:::
gnats:x:15400:0:99999:7:::
libuuid:x:15400:0:99999:7:::
syslog:x:15400:0:99999:7:::
sshd:x:15400:0:99999:7:::
landscape:x:15400:0:99999:7:::
messagebus:x:15400:0:99999:7:::
/etc/shadow
```

Note, that the shadow file is only accessible by root, so if you were not logged in as root you would not be able to see the contents of the file.

Like Windows, Linux uses a hosts file that contains the IP address and associated hostname for a particular device. In a default install of Linux, the hosts file contains only one entry for localhost. The location of the hosts file in Linux is /etc/hosts.

A screenshot of a terminal window titled "root@bt: ~". The window shows the contents of the /etc/hosts file. The file contains several entries, including the loopback address (127.0.0.1) and a local host entry (127.0.1.1). It also includes IPv6 entries and a comment about IPv6 capable hosts. The file ends with a line indicating it is the end of the hosts file. The terminal has a dark background with a logo of a cat's head and ears.

```
^ v x root@bt: ~
File Edit View Terminal Help
127.0.0.1      localhost
127.0.1.1      bt.foo.org      bt

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
/etc/hosts (END)
```

Network Configuration

Current network configurations can be viewed by issuing the ifconfig command. With Linux (if you are not connected to a network) you should only receive an entry for 127.0.0.1 which is the loopback address.

```
^ ~ x root@bt: ~
File Edit View Terminal Help
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~# ifconfig
eth1      Link encap:Ethernet HWaddr 00:0c:29:5c:7b:60
          inet addr:192.168.163.128 Bcast:192.168.163.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe5c:7b60/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3612 (3.6 KB) TX bytes:2344 (2.3 KB)
          Interrupt:19 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4161 (4.1 KB) TX bytes:4161 (4.1 KB)

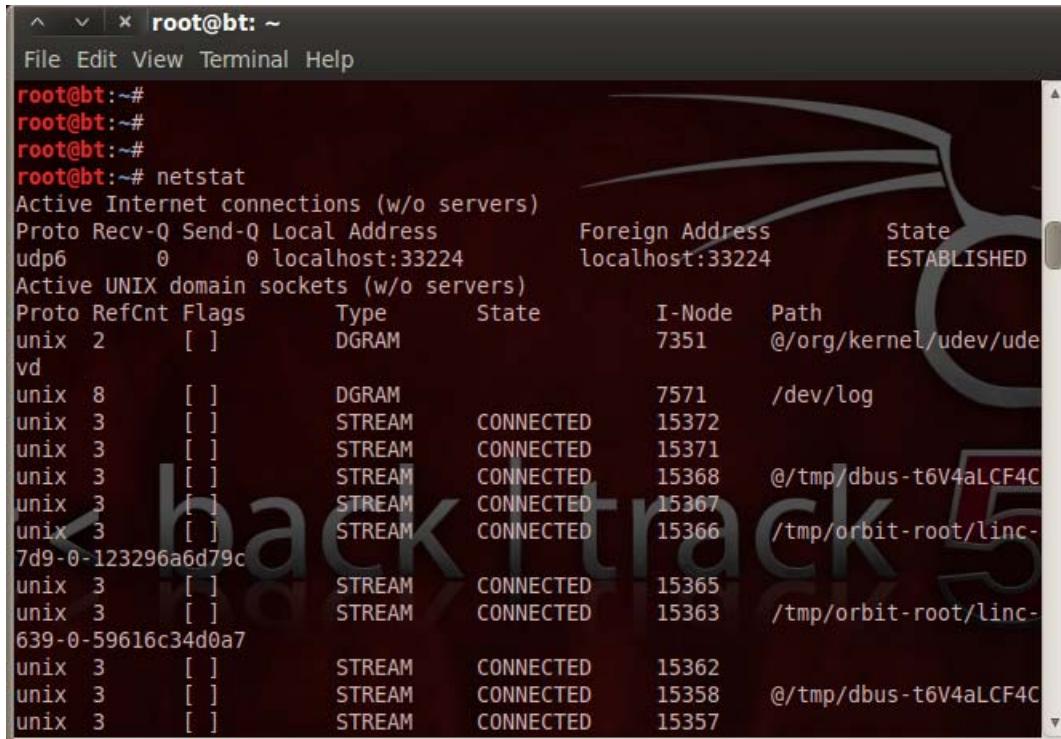
root@bt:~#
```

To verify that TCP/IP is setup correctly, simply ping 127.0.0.1. This will validate that the loopback is properly working. Pinging the loopback will be used for many of the exercises. To stop ping, type CTRL-C.

```
^ ~ x root@bt: ~
File Edit View Terminal Help
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.101 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.074 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.076 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.070 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.068 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.078 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.076 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.082 ms
64 bytes from 127.0.0.1: icmp_seq=11 ttl=64 time=0.080 ms
64 bytes from 127.0.0.1: icmp_seq=12 ttl=64 time=0.075 ms
^C
--- 127.0.0.1 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11003ms
rtt min/avg/max/mdev = 0.043/0.072/0.101/0.016 ms
root@bt:~#
```

Listening Services and Network Connections

It is always important to know what services are listening on your system, as well as what connections have been made. Examples of listening services are sendmail, rpc and sshd; each of these listen on a specific port or a number of ports. To display the active network connections on your system, issue the netstat command. Depending on how your system is configured, you might receive different results.



```
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~# netstat -an
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
udp6       0      0 localhost:33224          localhost:33224      ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags      Type      State         I-Node      Path
unix    2      [ ]      DGRAM          7351      @/org/kernel/udev/udev
vd
unix    8      [ ]      DGRAM          7571      /dev/log
unix    3      [ ]      STREAM     CONNECTED    15372
unix    3      [ ]      STREAM     CONNECTED    15371
unix    3      [ ]      STREAM     CONNECTED    15368      @/tmp/dbus-t6V4aLCF4C
unix    3      [ ]      STREAM     CONNECTED    15367
unix    3      [ ]      STREAM     CONNECTED    15366      /tmp/orbit-root/linc-
7d9-0-123296a6d79c
unix    3      [ ]      STREAM     CONNECTED    15365
unix    3      [ ]      STREAM     CONNECTED    15363      /tmp/orbit-root/linc-
639-0-59616c34d0a7
unix    3      [ ]      STREAM     CONNECTED    15362
unix    3      [ ]      STREAM     CONNECTED    15358      @/tmp/dbus-t6V4aLCF4C
unix    3      [ ]      STREAM     CONNECTED    15357
```

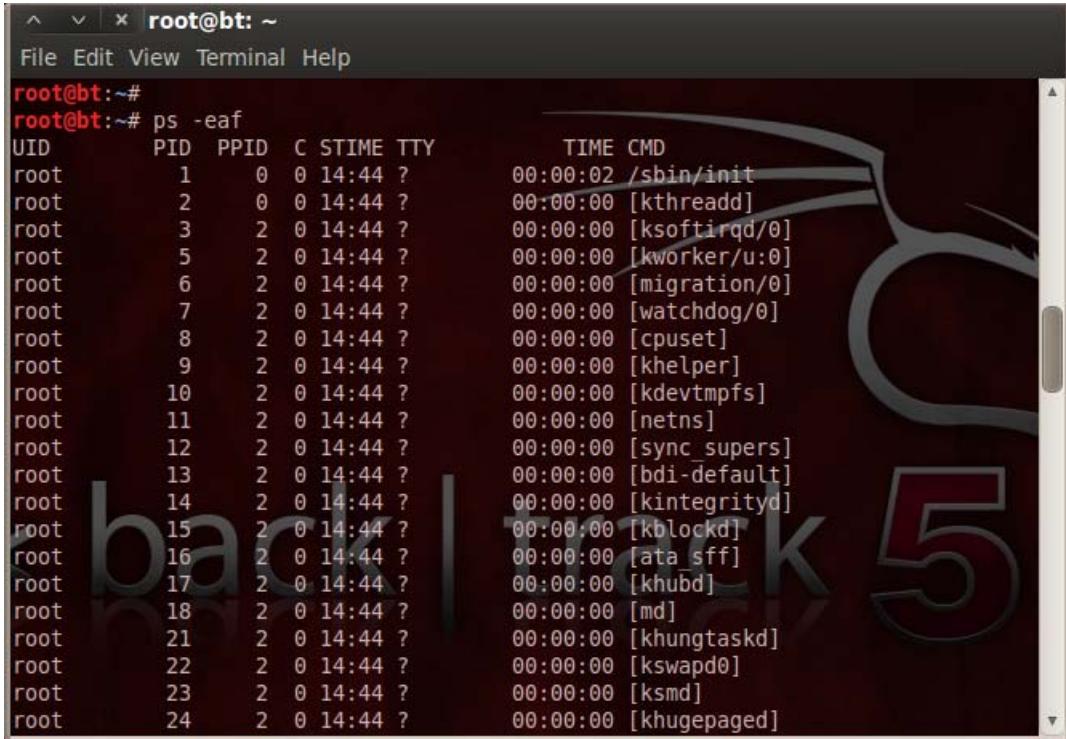
The **-an** option that was added to netstat specifies to list all connections (**-a**) and does not try to resolve hostnames (**-n**).

Depending on the applications you are running, the output may not fit onto one screen. This is a great time to pipe the output of one command through another. You can issue the command **netstat -an | more** to show one screen of information at a time, or you can use grep to search the output for specific requirements. The following screen shows that the command **netstat -an | grep LISTEN** outputs all of the servers that are listening on your system. Some of the other possible states besides LISTEN are ESTABLISHED and TIME_WAIT.

```
^ ~ x root@bt: ~
File Edit View Terminal Help
root@bt:~# netstat -an | grep LISTEN
tcp      0      0 127.0.0.1:7337          0.0.0.0:*
tcp6     0      0 ::1:7337              ::*:*
unix    2      [ ACC ]      STREAM      LISTENING    10171  @/tmp/.ICE-unix/1586
unix    2      [ ACC ]      STREAM      LISTENING    9964   /tmp/X11-unix/X0
unix    2      [ ACC ]      STREAM      LISTENING    10032  /tmp/ssh-bgUwCI1539/a
gent.1539
unix    2      [ ACC ]      STREAM      LISTENING    10172  /tmp/.ICE-unix/1586
unix    2      [ ACC ]      STREAM      LISTENING    10187  /tmp/orbit-root/linc-
639-0-59616c34d0a7
unix    2      [ ACC ]      STREAM      LISTENING    10322  /tmp/orbit-root/linc-
632-0-418c1114f8a8
unix    2      [ ACC ]      STREAM      LISTENING    10439  /tmp/keyring-ZBEjEG/c
ontrol
unix    2      [ ACC ]      STREAM      LISTENING    10440  /tmp/keyring-ZBEjEG/s
sh
unix    2      [ ACC ]      STREAM      LISTENING    10456  /tmp/keyring-ZBEjEG/p
kcs11
unix    2      [ ACC ]      STREAM      LISTENING    10469  /tmp/orbit-root/linc-
642-0-263241dc76f8c
unix    2      [ ACC ]      STREAM      LISTENING    10866  /tmp/orbit-root/linc-
648-0-f8d2b442e7b7
unix    2      [ ACC ]      STREAM      LISTENING    7264   @/com/ubuntu/upstart
unix    2      [ ACC ]      STREAM      LISTENING    10969  /tmp/orbit-root/linc-
```

The ps Command

Linux gives the user the ability to run a command in the background by adding a blank space, and then & to the end of the command. To obtain a listing of currently running processes, including those that are running in the background, Linux provides the ps command. This command is invaluable for troubleshooting and for determining the current state of the system. Many options can be given to ps to control what it outputs to the command shell. For example, type ps -eaf into a command shell and press Enter, as in the following screen.



```
root@bt:~# ps -eaf
UID      PID  PPID  C STIME TTY          TIME CMD
root      1    0  0 14:44 ?        00:00:02 /sbin/init
root      2    0  0 14:44 ?        00:00:00 [kthreadd]
root      3    2  0 14:44 ?        00:00:00 [ksoftirqd/0]
root      5    2  0 14:44 ?        00:00:00 [kworker/u:0]
root      6    2  0 14:44 ?        00:00:00 [migration/0]
root      7    2  0 14:44 ?        00:00:00 [watchdog/0]
root      8    2  0 14:44 ?        00:00:00 [cpuset]
root      9    2  0 14:44 ?        00:00:00 [khelper]
root     10   2  0 14:44 ?        00:00:00 [kdevtmpfs]
root     11   2  0 14:44 ?        00:00:00 [netns]
root     12   2  0 14:44 ?        00:00:00 [sync_supers]
root     13   2  0 14:44 ?        00:00:00 [bdi-default]
root     14   2  0 14:44 ?        00:00:00 [kintegrityd]
root     15   2  0 14:44 ?        00:00:00 [kblockd]
root     16   2  0 14:44 ?        00:00:00 [ata_sff]
root     17   2  0 14:44 ?        00:00:00 [khubd]
root     18   2  0 14:44 ?        00:00:00 [md]
root     21   2  0 14:44 ?        00:00:00 [khungtaskd]
root     22   2  0 14:44 ?        00:00:00 [kswapd0]
root     23   2  0 14:44 ?        00:00:00 [ksmd]
root     24   2  0 14:44 ?        00:00:00 [khugepaged]
```

As you can see there is a lot of information. To practice searching for information, what command would you type if you wanted to see if any crypto process is running?

If you said type **ps -eaf | grep crypto**, you were correct.

A screenshot of a terminal window titled "root@bt: ~". The window shows a root shell with multiple "#" prompts. The user then runs the command "ps -eaf | grep crypto", which outputs two processes:

PID	User	TTY	Time	Command
27	root	2	0 14:44 ?	00:00:00 [crypto]
2123	root	2081	0 15:49 pts/0	00:00:00 grep --color=auto crypto

In the event that a program becomes unresponsive, you can forcibly end it. In order to do so, you first need to know what process id (PID) it is using. To determine this, issue the `ps -eaf` command and find the entry for the unresponsive program. The second column from the left contains the PID. Issue the command `kill` to kill the program.

You should now have a basic understanding of Linux. As is the case with anything in life, the best way to understand a topic is to practice. The information contained in this section should provide you with a basic knowledge to navigate the file system, perform basic configuration changes, and install applications. There are many security tools written for Linux. Taking the time to learn the tools will provide a powerful, yet free toolbox for assessing the security of your network.