Whatcom CC Cybercamp

[4/1/2014]

Table of Contents

LAB 3

Required Tools

PC running Windows XP or higher

Session 3

LAB 4

Required Tools

VMWare Player Version 4.0.2

Ubuntu Version 10.10

LAB 5

Required Tools

VMWare Player Version 4.0.2

Customized Windows Server 2000 (Instructions will be provided)

Netcat

LAB 6

Required Tools

VMWare Player Version 4.0.2

Windows Server 2008

Session 4

LAB 7

Required Tools

VMWare Player Version 4.0.2

Ubuntu Version 10.10

LAB 8

Note: Only Exercises 3 through 8 are used

Required Tools

VMWare Player Version 4.0.2

Ubuntu Version 10.10

Session 5

LAB 9

Required Tools

VMWare Player Version 4.0.2

Windows Server 2008

Install Ubuntu 10.10 using VMware player

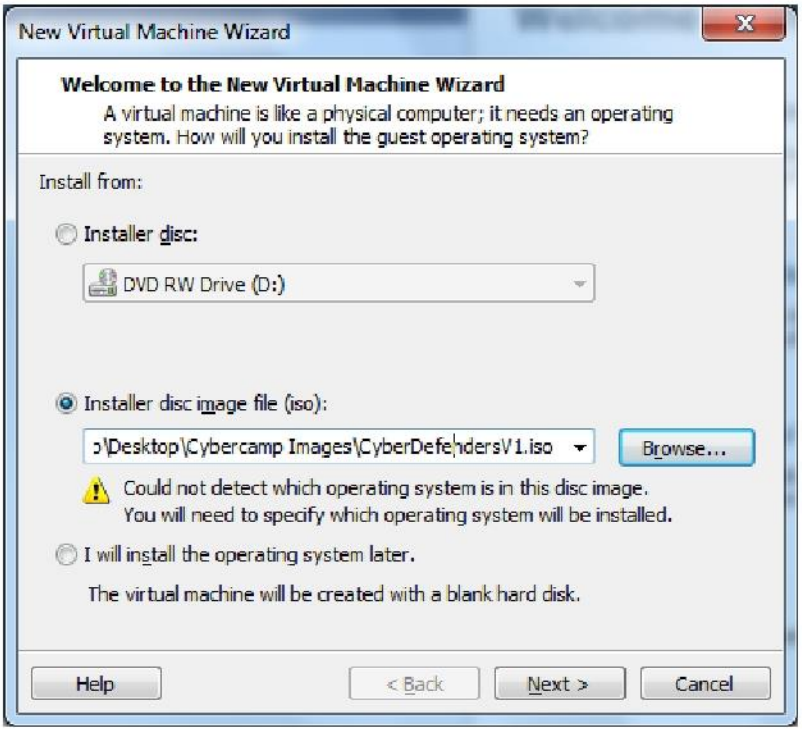
VMware player is a free application available from vmware.com. It allows you to try out multiple operating systems on your computer. In order to run it you need the following minimum requirements:

1 GHz or faster processor (2GHz recommended)
1GB RAM minimum (2GB RAM recommended)
Enough memory to run the host operating system and the guest operating system
VMware Player requires approximately 150MB of disk space to install the application

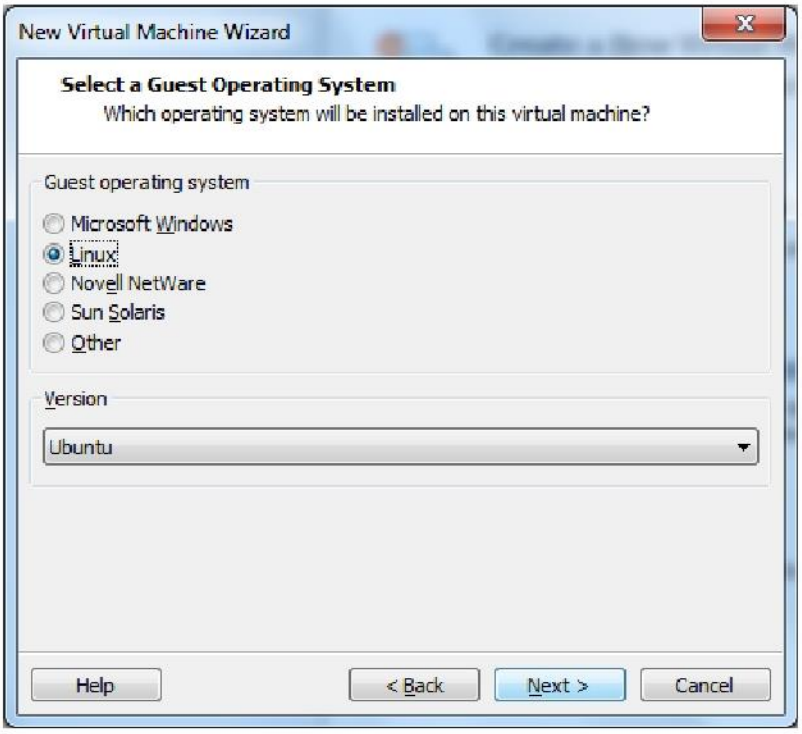
Today we will be trying out Ubuntu 10.10 with VMware player. Ubuntu is a user friendly linux operating system that is widely used by individuals and industry. More information about ubuntu can be found here: www.ubuntu.com

If you have any questions during this install, please ask a mentor or instructor for assistance.

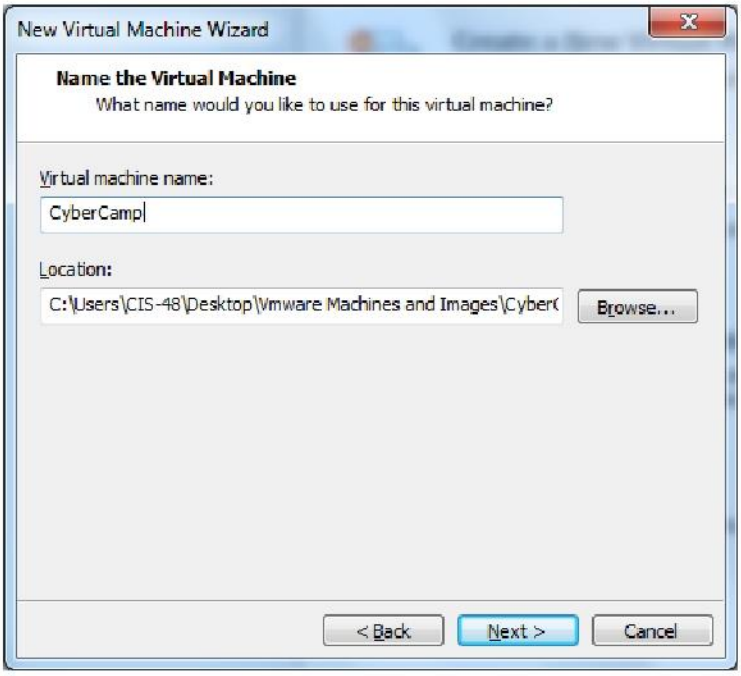
Start VMware Player by going to all programs, VMware, VMware Player. When the VMware Player
console opens select "Create new Virtual Machine".



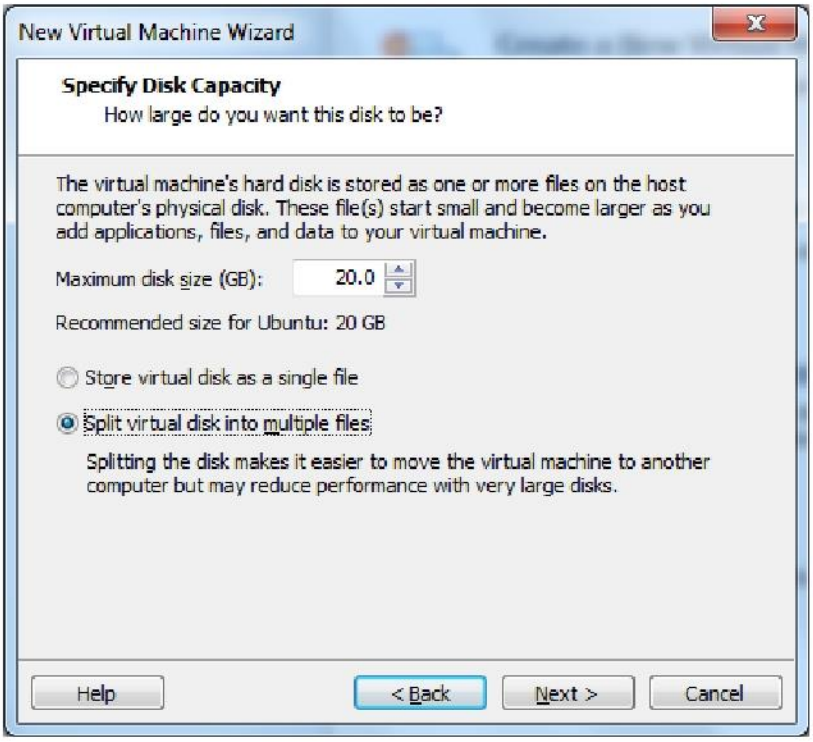
-We will be using a disc image for our installer. Click Installer disc image file, and browse to the following location: C:\Users\Cybercamp\Desktop\Cybercamp Images\CyberDefendersV1.iso



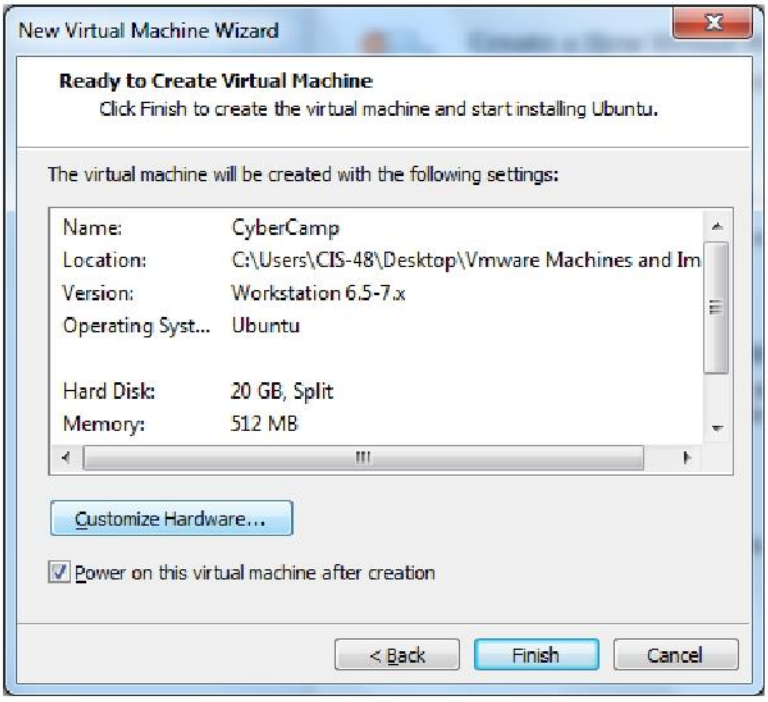
-We will be installing Ubuntu Linux, please make the following selections to reflect this.



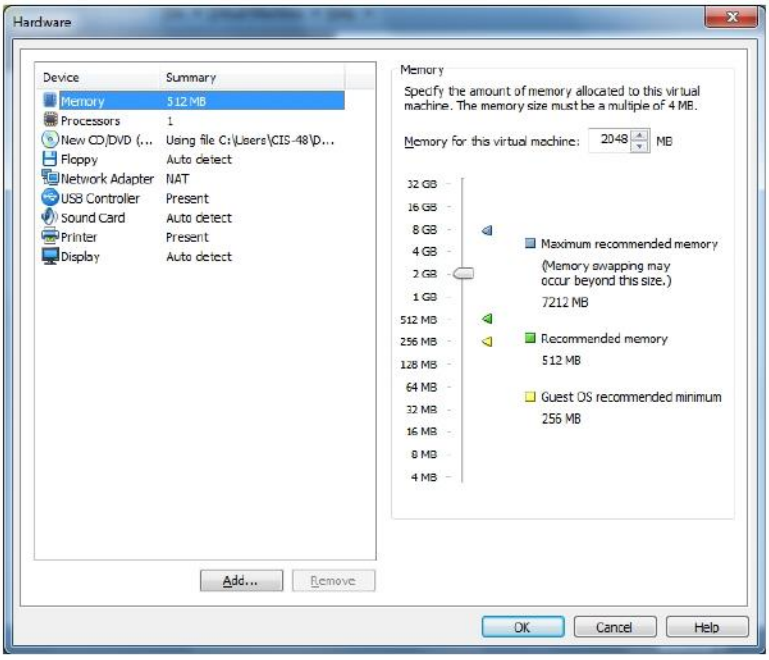
-Here we will give our new Virtual Machine a name, in this case we will give our VM the name 'CyberCamp'



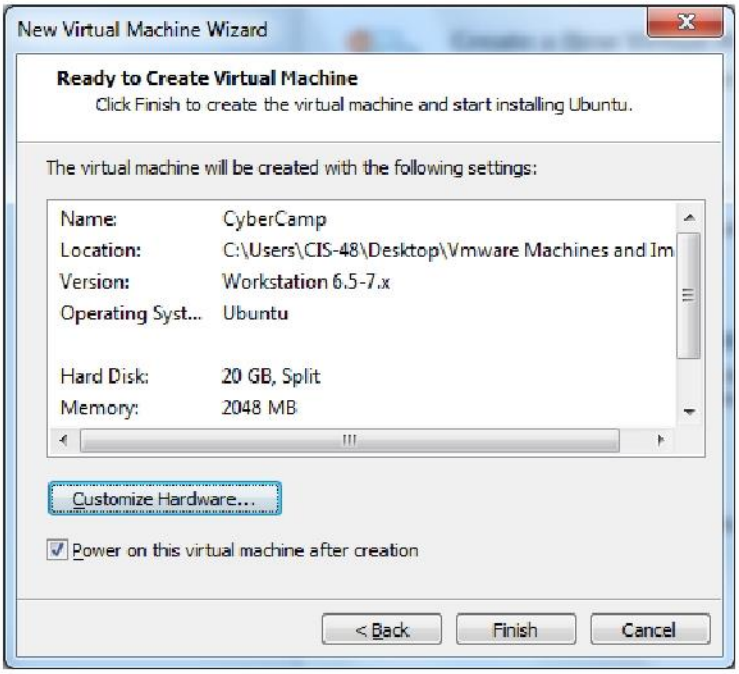
-We will leave the default size of 20 GB for our VM's hard disk, and click "Split virtual disk into multiple files." For most uses this selection will be fine and will shorten the length of our install time.



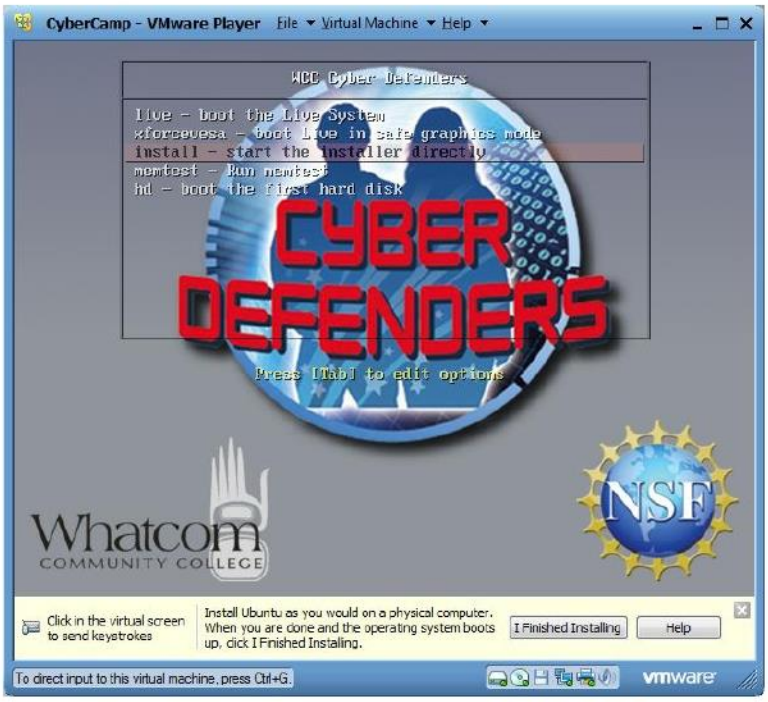
-After clicking next, you will see a screen to review your hardware settings before completing the install. Click "Customize Hardware" , and proceed to the following step.



-Next we will increase the amount of Memory available to the Virtual Machine . This will make our install faster and increase overall performance. There are two methods to accomplish this, you can either click "2 GB" in the slide selector or enter 2048 (remember 1 GB = 1024 MB) inside the momory dialog box. Click ok and we'll move on to the next step.



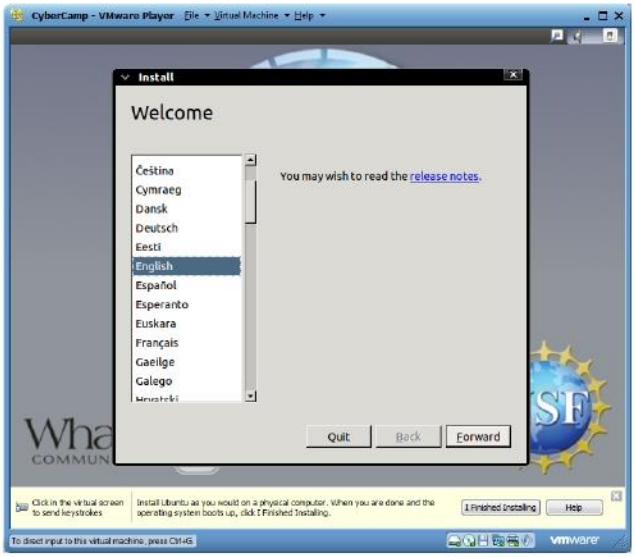
-Review your new settings and click Finish. This will reboot the Virtual Machine and begin the installer.



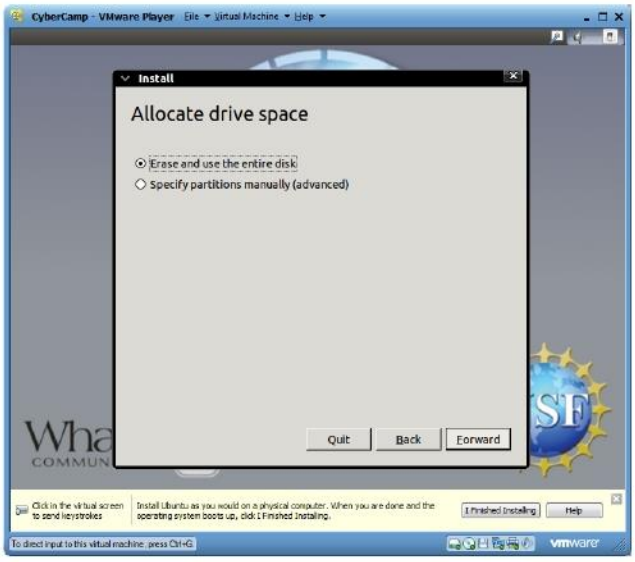
-After reboot, you will be greeted with a boot splash screen. Press an arrow key to stop the boot splash screen's timer and take some time to read and review these options. If you have questions about what a specific option does please ask your mentor or an instructor. Using the arrow keys, and enter to select, choose the "install - start the installer directly" option.

-Ubuntu will start the Ubiquity application, and begin the installation process.

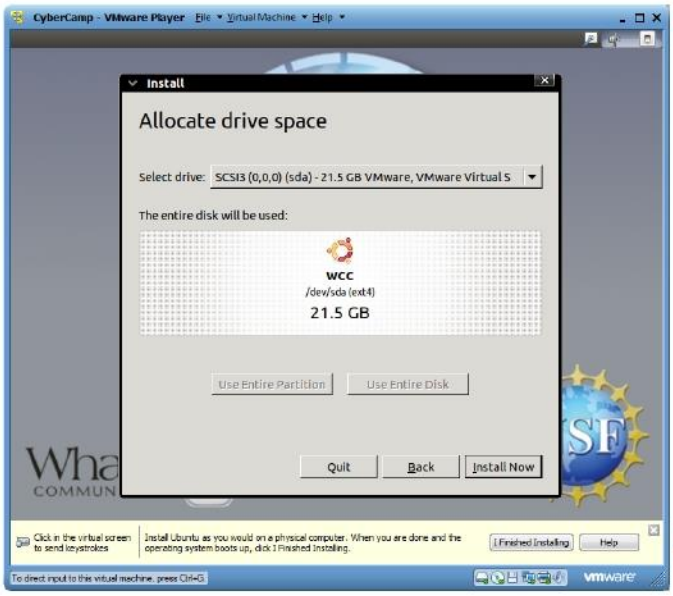
-Ubuntu will check for some requirements. For this installation we do not need to install any third party drivers or install any update. Click Forward.

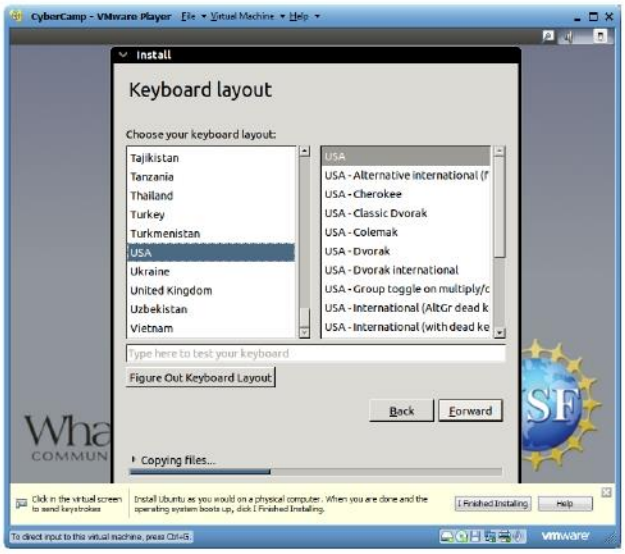


-Choose the default laguage for this installation.



-Click "Erase and use entire disk". Click Forward.



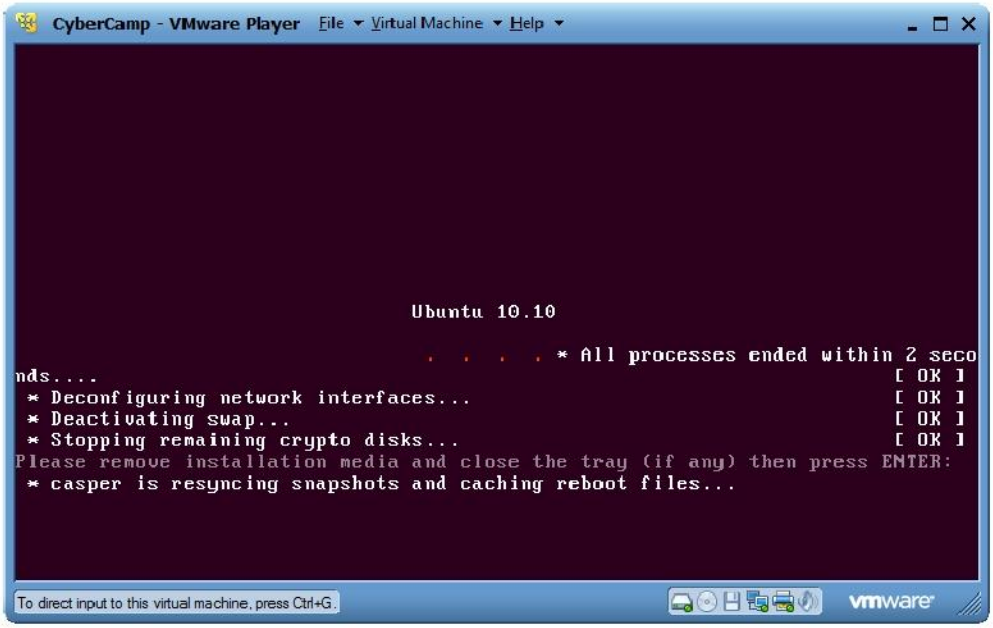


-Verify the disk location and click Install Now.

-Choose you correct timezone.

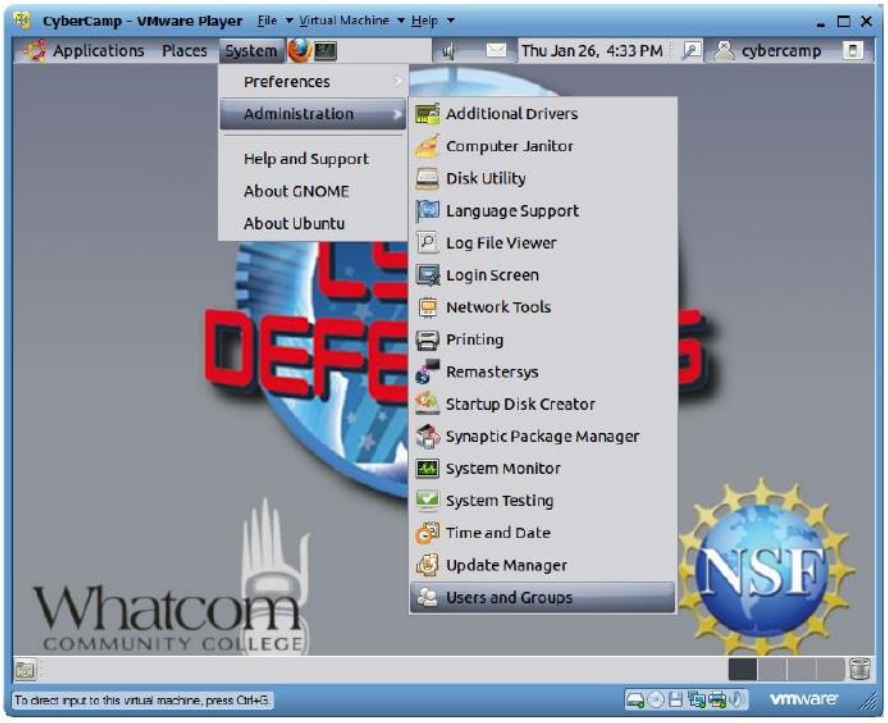
-Ubuntu will now copy and install it's files.

-Once ubuntu has completed it's installation successfully you will be prompted to restart. Click Restart Now and observe Ubuntu's behavior during the shutdown process.

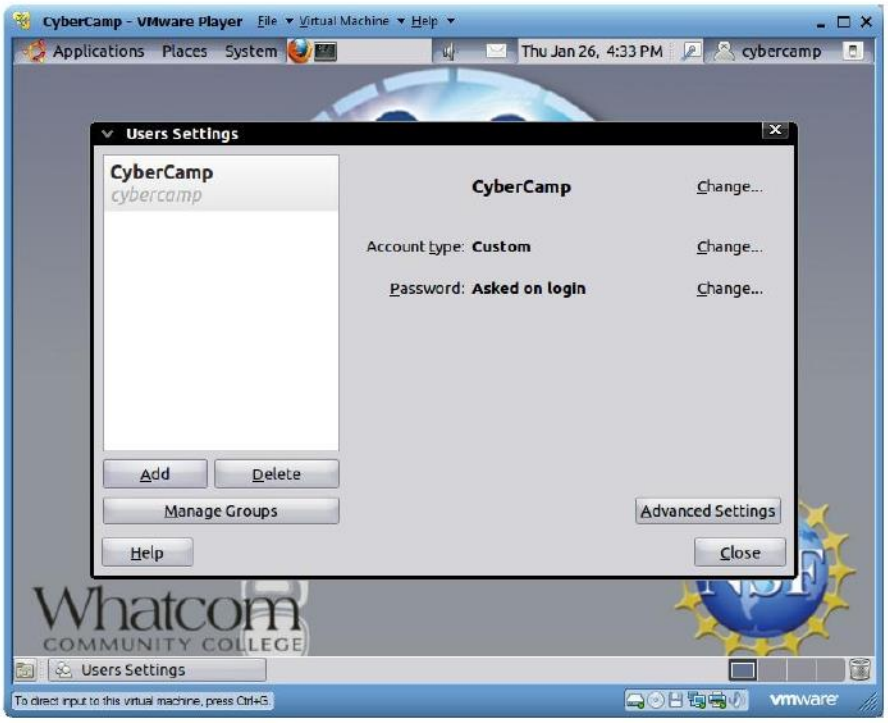


-At this screen, press Enter. The installer disc will automatically unmount and the system will reboot.

-Log in to the CyberCamp account and the GNOME you will be greeted with the GNOME desktop environment.



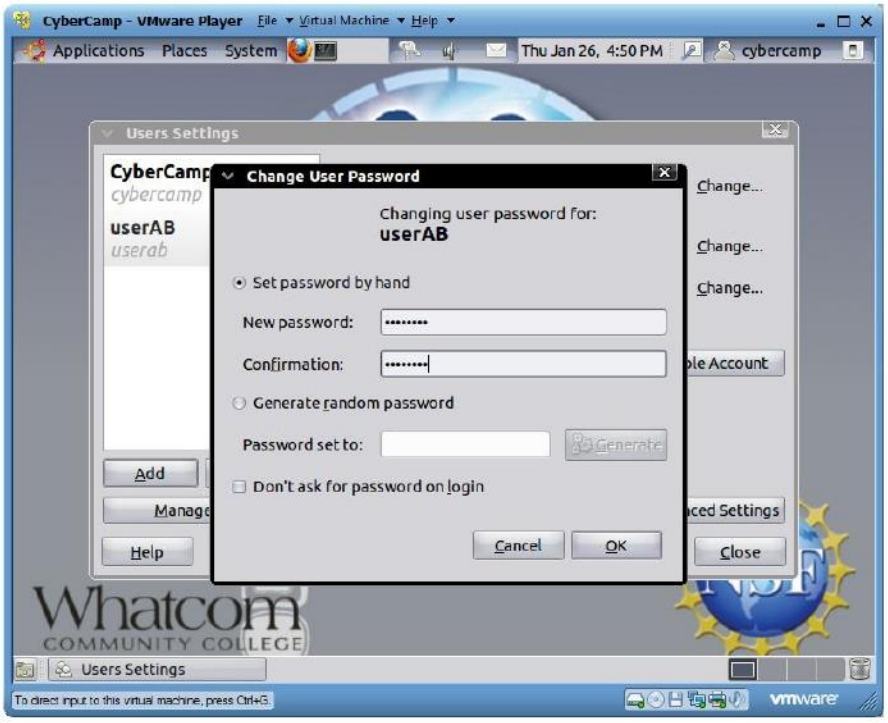
-From the Main Menu, select System, Administration and then Users and Groups



-Click Add to add your new user account. Ubuntu will then prompt you to authenticate to make any system changes.

-Enter the CyberCamp user password and then click Authenticate.

-Enter your new username, this will consist of your Angel username.



-Choose a new password for your account and click OK.

-After your account has been created, click Close.

-Click the button in the top right corner of your desktop and select the Restart option. When the system restarts, log in with your new account.

Congratulations you have just installed Ubuntu Linux.

Partial support for this work was provided by the National Science Foundation's Advanced Technological Education (ATE) program under Award No. 1104192. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Set up a simple network

In this activity, each group will connect their machines together and then establish connectivity.

Components needed:

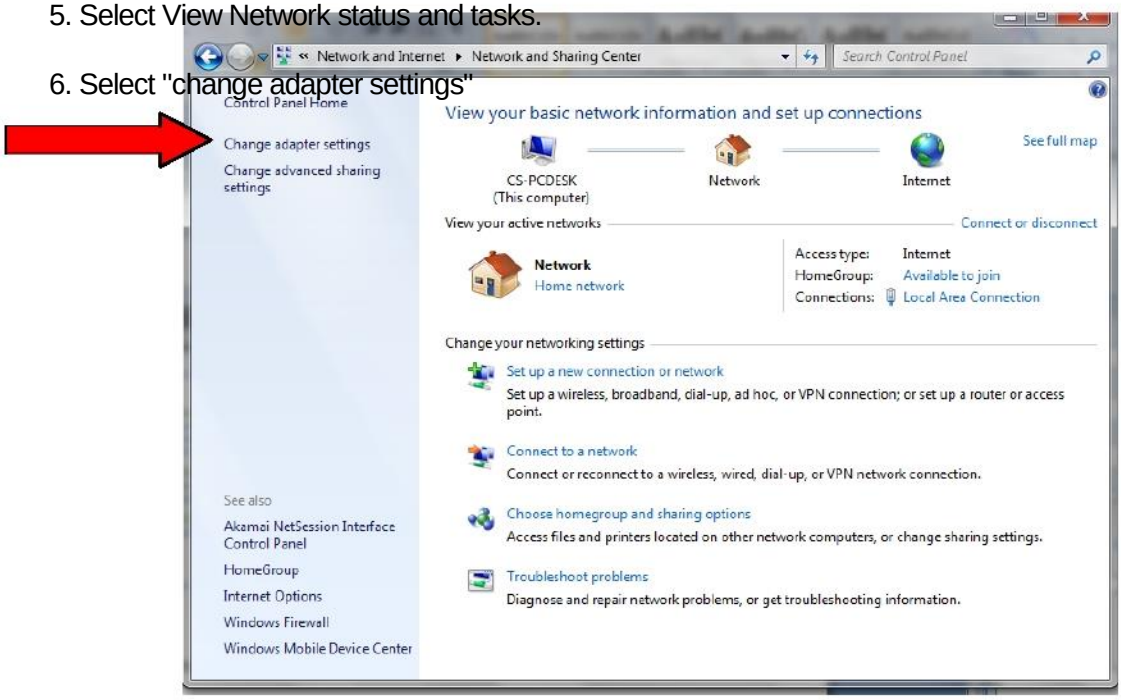
- Cables: to connect a pc to a switch, you need a *straight through* cat 5 cable.
- Switch
- Pcs
- Ip addresses : we will use *private* ip addresses.

1. Use the cable provided to connect your pc to the switch. One end of the cable should go to your pc and the other end into a port on the switch:

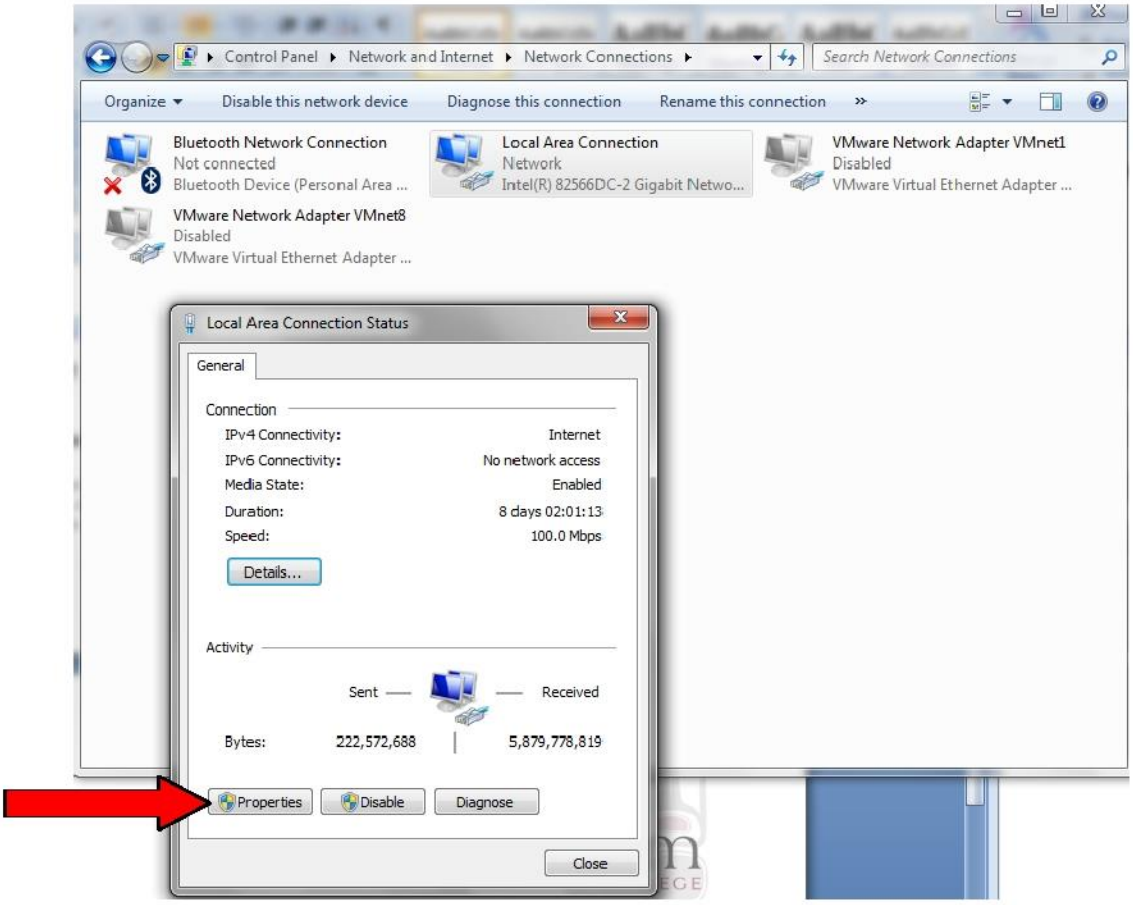
2. After you connect the cable, the light for your port on the switch should turn green.
3. Now we have to configure the ip address for our computer.
4. Click on the windows 7 start button (located in the lower left hand corner) and select control panel.

5. Select View Network status and tasks.

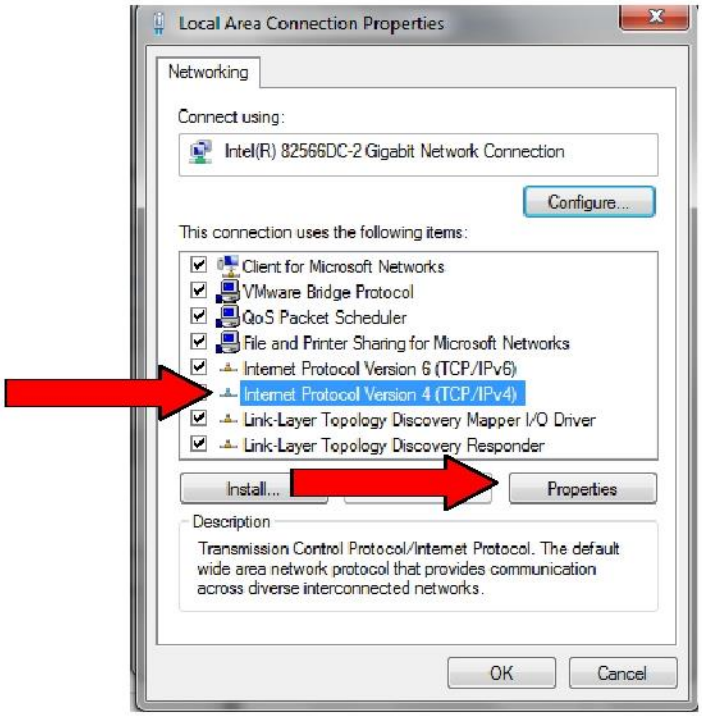
6. Select "change adapter settings"



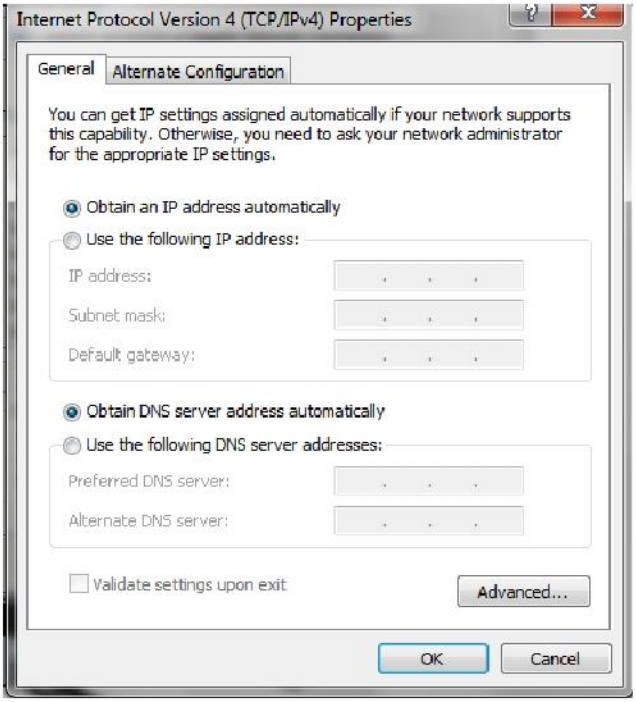
7. Click on local area network and the properties box should be displayed:



Click on properties, select Internet Protocol Version 4, and click on properties again.:

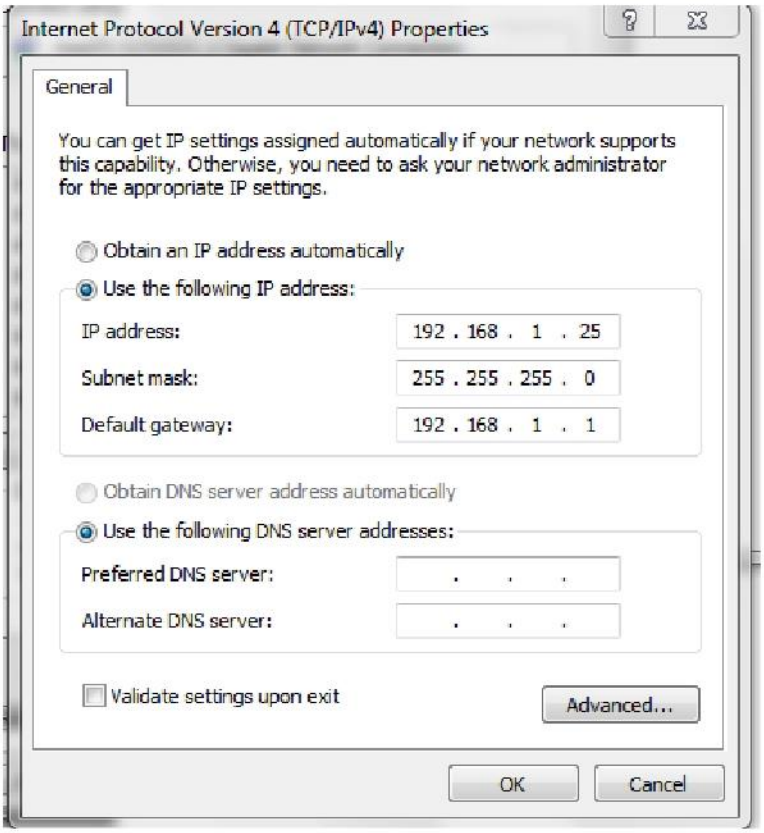


Notice how your computer is receiving its ip address. We need to change this so that you can manually assign an ip address.



Click on "Use the following ip address" and enter the ip address, subnet mask, and default gateway for your pc (check the whiteboard for your assignment). For this lab we will be leaving the dns server setting blank.

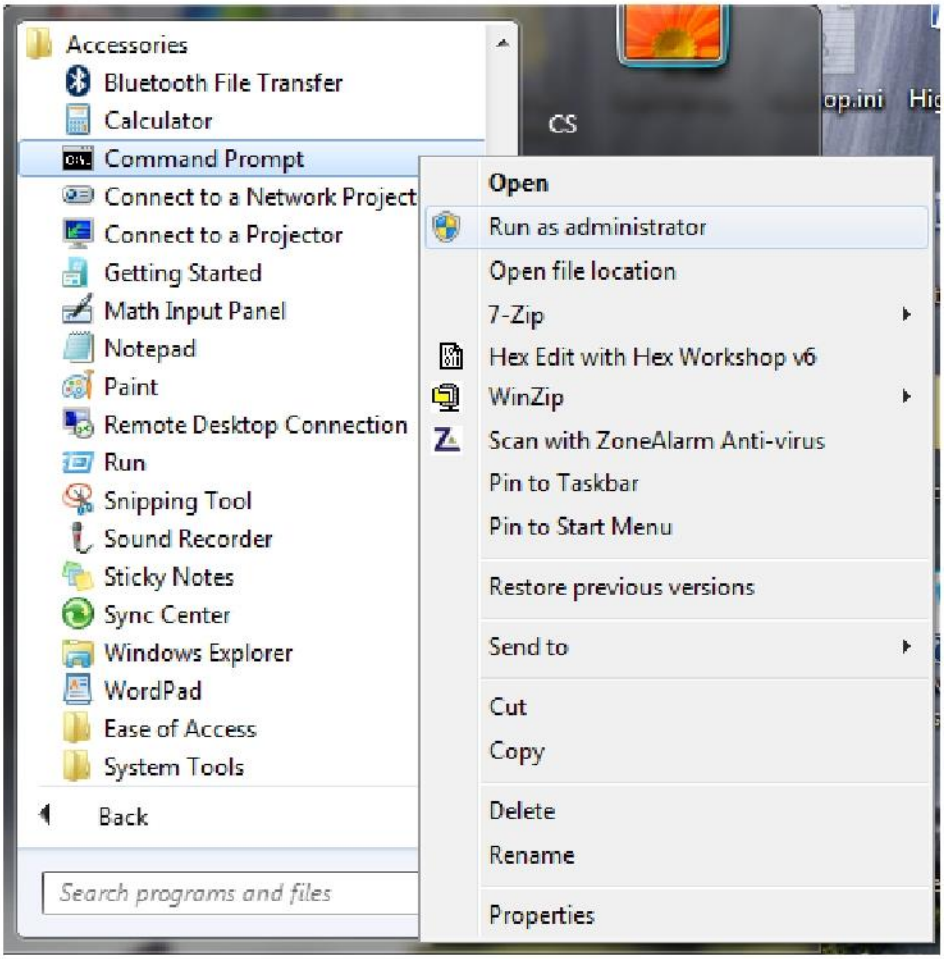
Here is an example



When everyone in your group has completed their setup, we will test to make sure we have connectivity to all machines by using the ping command. A few things to note: **Windows firewall by default will not respond to pings. If you have difficulty the most likely reason is windows firewall or other security applications not responding to your ping. Other things to check: wrong cable, port on switch not lit up, wrong ip address.**

Open up a command line and ping your fellow students machines. Here is how to do that:

1. Go to the windows start button, all programs, accessories, command prompt.

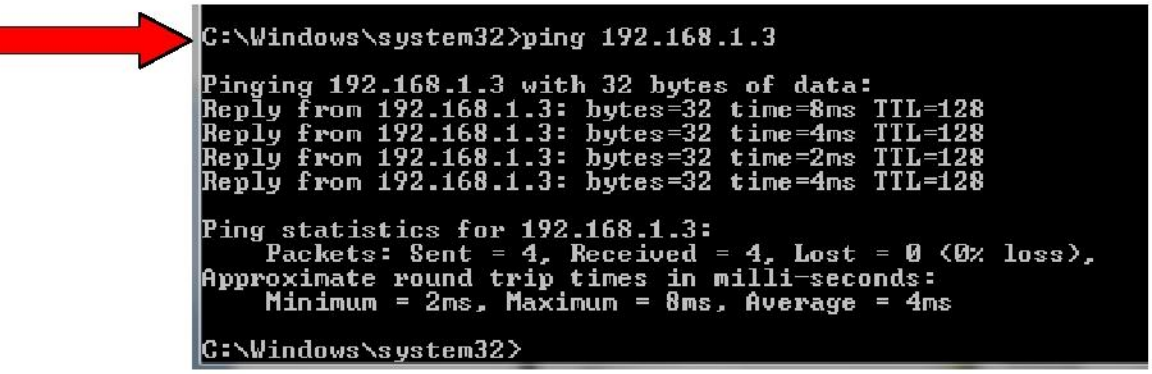
2 

3. Click on Run as an administrator and the command line box should open. At the command line, type the following:

ping 192.168.1.YOUR NEIGHBORS ADDRESS.

For instance, your ip address is 192.168.1.2. Your neighbors ip address is 192.168.1.3. At the command prompt, type

ping 192.168.1.3



You should receive a reply from your neighbor. If you do not receive a reply, then you must troubleshoot using the ideas mentioned above. Ping all of your neighbors to ensure you have connectivity
throughout your network.

Partial support for this work was provided by the National Science Foundation's Advanced Technological Education (ATE) program under Award No. 1104192. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

NETSTAT LAB

In this lab you will learn to use the command line utility Netstat to identify open ports on a computer. You will also learn how to identify what applications are using those ports.

The Internet Assigned Numbers Authority (IANA) is responsible for assigning port numbers to applications. Services can use either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). There are times when both TCP and
UDP might use the same port number.

There are three types of port numbers:

- Well-known ports (numbers 0 through 1023)
- Registered ports (numbers 1024 through 49151)
- Dynamic or private ports (numbers 49152 through 65535)

Some examples of ports, the application that uses them, and the protocol used:

WELL-KNOWN PORTS

Port	Application	Protocol
20	File Transfer Protocol (FTP) Data	TCP
21	File Transfer Protocol (FTP) Control	TCP
25	Simple Mail Transfer Protocol (SMTP)	TCP
80	Hypertext Transfer Protocol (HTTP)	TCP
443	Secure Hypertext Transfer Protocol(HTTPS)	TCP

REGISTERED PORTS

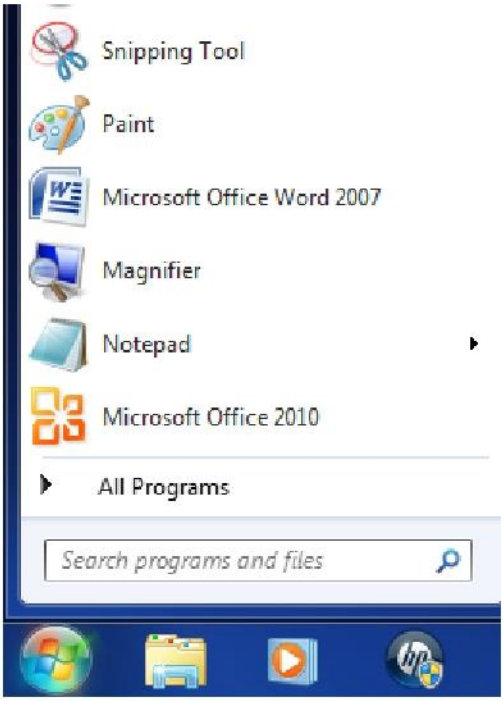
Port	Application	Protocol
1863	MSN Messenger	TCP
5004	Real-Time Transport Protocol	UDP
8008	Alternate HTTP	TCP

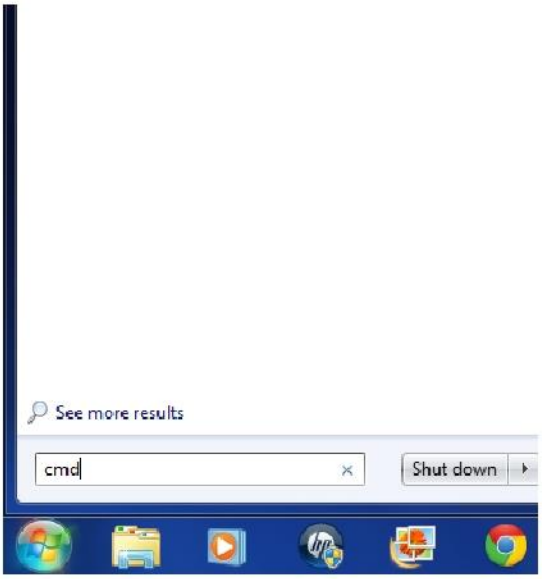
8080	Alternate HTTP	TCP

Dynamic or private ports are usually assigned dynamically to client applications when a connection is initiated.

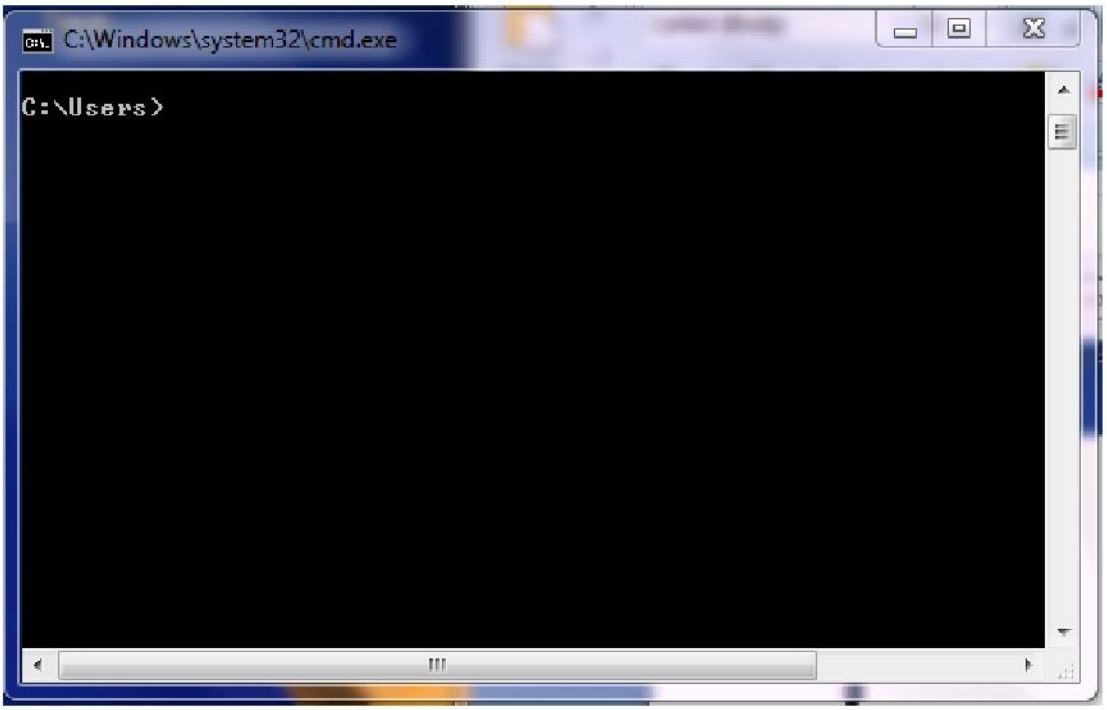
GETTING STARTED:

To access the command line, click on the start button in the lower left. Then type "cmd" into the Search programs and files box and hit enter.

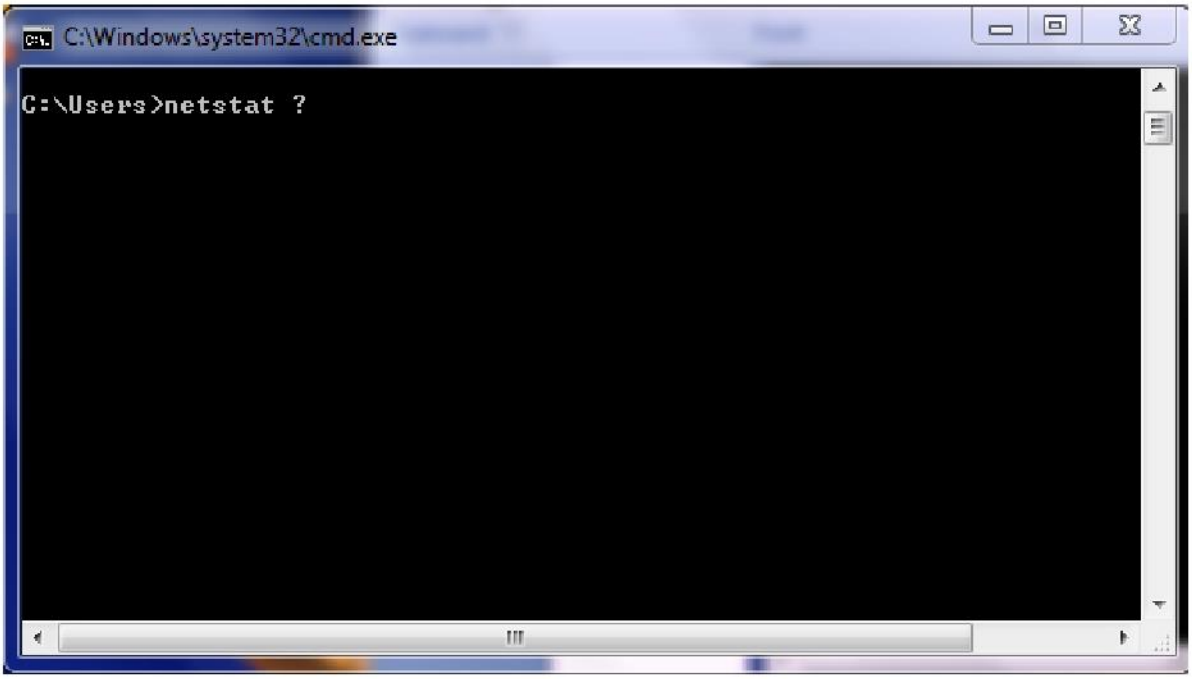




This will open up a command line window.



The Netstat utility has a number of options that can be set to modify the output you get. In the command line type "netstat ?" and hit enter. This will bring up a list of the options and what they are used for. Please note that more than one option can be used in one netstat command.



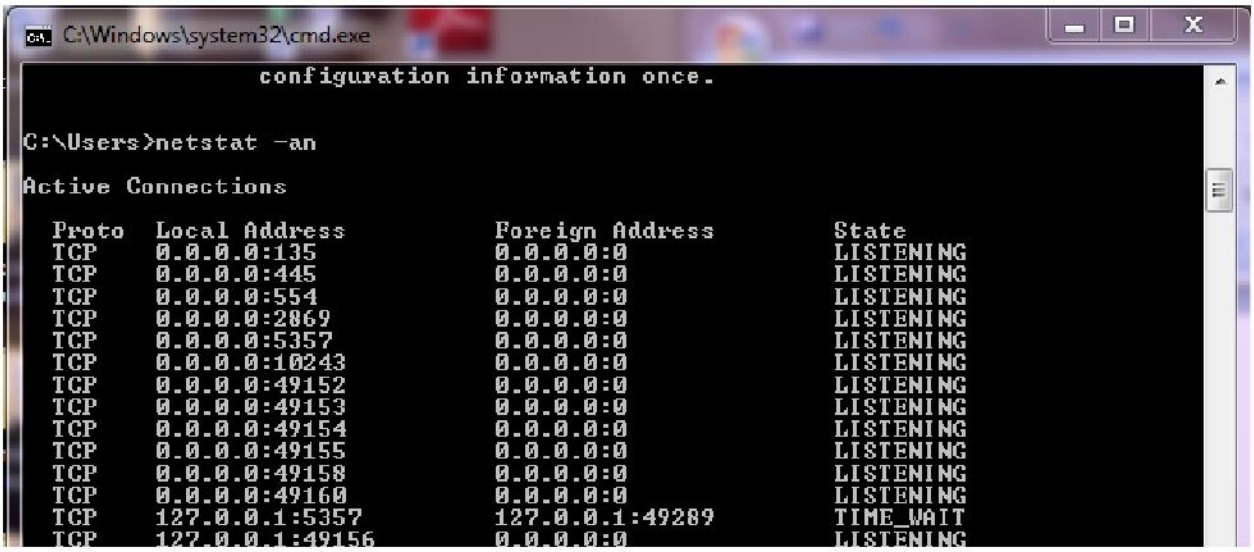
Observing the results of the "netstat ?" command, fill out the following table:

OPTION	DESCRIPTION
	Displays addresses and port numbers in numerical form
	Displays the routing table.
	Displays all connections and listening ports.
	Displays Ethernet statistics every 10 seconds. Pressing CTRL+C will end this.
	Displays Fully Qualified Domain Names (FQDN) for foreign addresses.

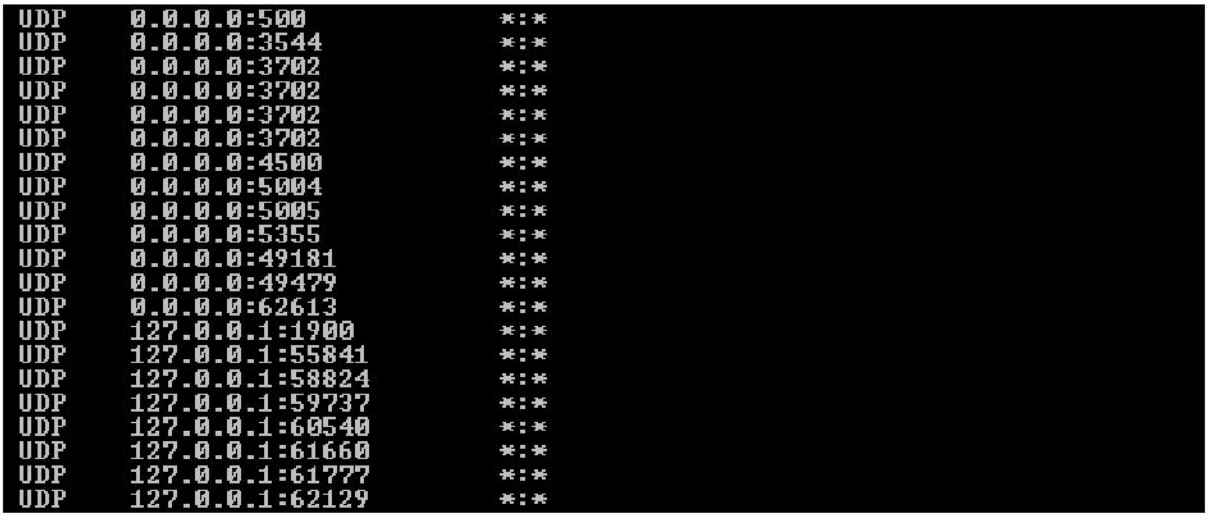
In this exercise, we will use two controls:

- -a displays all connections and listening ports
- -n displays addresses and port numbers in numerical form

Type in the command "netstat -an" and hit enter. You will get a readout similar to the following:



This is a sample of the UDP output from the same command:



As can be seen the UDP protocols don't have a state listed, but they are open.

The Proto column tells what protocol is being used, be it TCP or UDP.

The Local Address column lists what address is being used to listen with and what port number is separated by a colon. An address of 0.0.0.0 means it is listening on all available addresses. The address 127.0.0.1 means it is listening on the
loopback address. An address like 192.168.1.1 would mean that it is listening on the computer's IP address.

The Foreign Address column lists the address it is listening to and the port from that address separated by a colon. A result of 0.0.0.0:0 means that it isn't connected to anything but waiting to listen to something. 127.0.0.1 is again a loopback address. A different IP address would indicate the address of the other computer/server that the session has been established with.

This covers the entries that have address:port format of x.x.x.x:x. These are using IPv4 addresses. Later in the output from the netstat command there will be addresses in the form of [::] and [::1]. These represent the same entries as the earlier ones but in IPv6 form instead of IPv4.

The State column has a number of different possibilities. Listening means that the port is open and ready to accept a connection. Established means that a session is in progress. Time_wait is the state where a session has been actively closed. There are others, but these are the primary ones that will be seen.

With your results from the netstat command in front of you, open up a web browser and use www.google.com to find out what some of the ports in the list are for. Fill in the following table with the information you gather. Pick at least four TCP and four UDP.

PROTOCOL	LOCAL ADDRESS	PORT	WHAT USES THE PORT	FOREIGN ADDRESS	STATUS

Partial support for this work was provided by the National Science Foundation's Advanced Technological Education (ATE) program under Award No. 1104192. Any opinions, findings, and conclusions or recommendations expressed in this material are ~~those of the author(s) and do not~~ necessarily reflect the views of the National Science Foundation.

1.1 Starting the terminal

To open the Linux Terminal click on the toolbar shortcut or click Applications -> Accessories -> Terminal.

A Linux Terminal should open.

1.2 Listing Files and Directories

When you first login, your current working directory is your home directory.

To find out what is in your home directory, type: **# ls**

The ls command (lowercase L and lowercase S) lists the contents of your current working directory.

ls does not, in fact, cause all the files in your home directory to be listed, but only those ones whose name does not begin with a dot (.) Files beginning with a dot (.) are known as hidden files and usually contain important program configuration information. They are hidden because you should not change them unless you are very familiar with Linux!!!

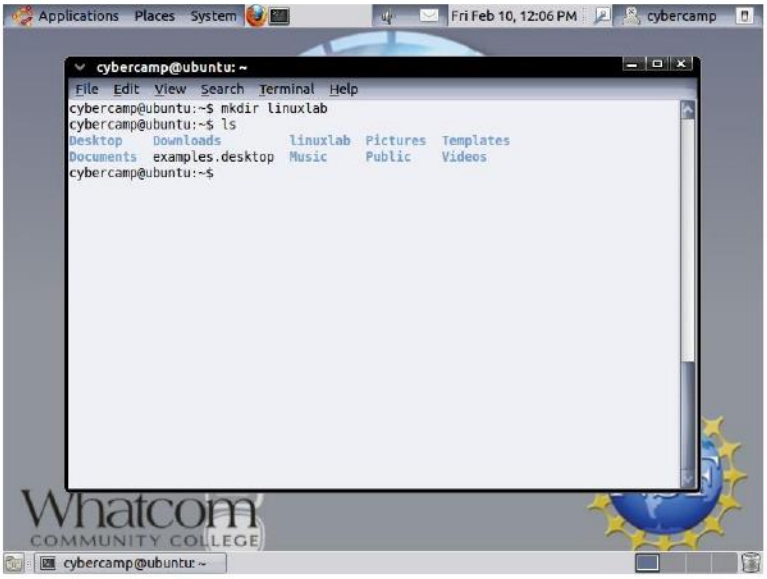
To list all files in your home directory including those whose names begin with a period, type: **# ls -a**

As you can see, ls -a lists files that are normally hidden.

ls is an example of a command which can take options: -a is an example of an option. The options change the behaviour of the command.

1.3 Making Directories

We will now make a subdirectory in your home directory to hold the files you will be creating and using in the course of this lab clear. To make a subdirectory called linuxlab in your current working directory type: **# mkdir linuxlab**

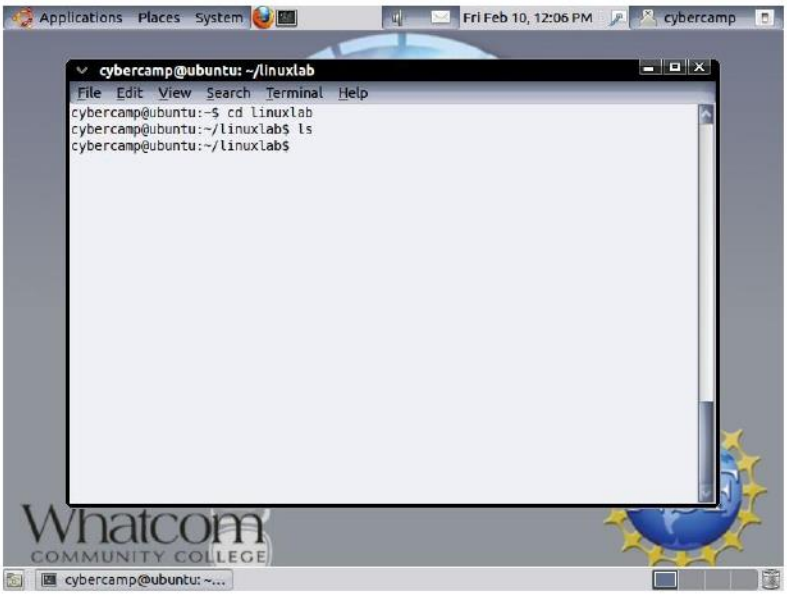


To see the directory you have just created, type: **# ls**

1.4 Changing into a different directory

The command cd directory means change the current working directory to 'directory'. The current working directory may be thought of as the directory you are in, i.e. your current position in the file-system tree. To change to the directory you have just made, type: **# cd linuxlab**

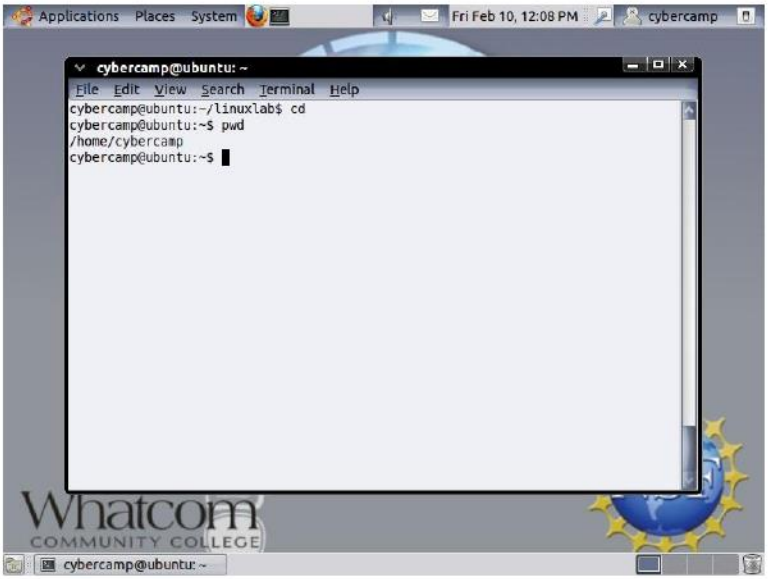
Type ls to see the contents (it should be empty).



Make 2 new directories inside the linuxlab directory called cyber and camp. Then type ls view the new directories.

1.5 Understanding the working directory

Pathnames enable you to work out where you are in relation to the whole file-system. For example, to find out the absolute pathname of your home-directory, type cd to get back to your home-directory and then type: # **pwd**



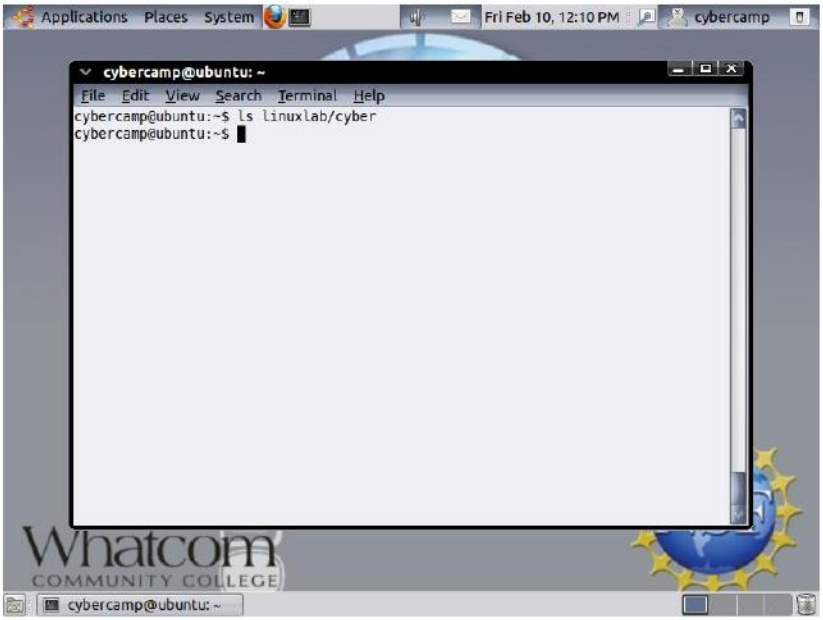
1.6 Learning about pathnames

To list the contents of the directory linuxlab, type: # **ls linuxlab**

Now type: # **ls cyber**

You should receive an error message.

The reason for this error message is because cyber is not in your current working directory. To use a command on a file (or directory) not in the current working directory (the directory you are currently in), you must either cd to the correct directory, or specify its full pathname. To list the contents of your linuxlab directory, you must type: # **ls linuxlab/cyber**



1.7 The Home Directory

Home directories can also be referred to by the tilde ~ character. It can be used to specify paths starting at your home directory. So typing: # **ls ~/linuxlab** will list the contents of your linuxlab directory, no matter where you currently are in the file system.

What do you think# ls ~would list?

2.1 Copying Files

What we are going to do now, is to take a file stored in a different portion of the file system, and use the cp command to copy it to your linuxlab directory.

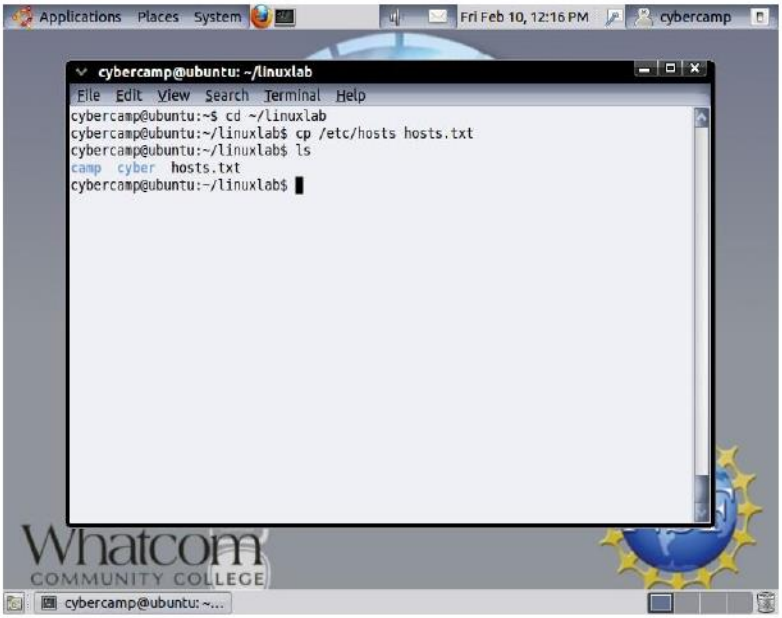
First, cd to your linuxlab directory.

Type: **# cd ~/linuxlab**

Then at the Linux prompt, type**: cp /etc/hosts hosts.txt**

The above command means copy the file hosts to the current directory, with the new name hosts.txt. Type: **# ls**

To verify that the copy of the /etc/hosts file was made.



2.2 Moving Files

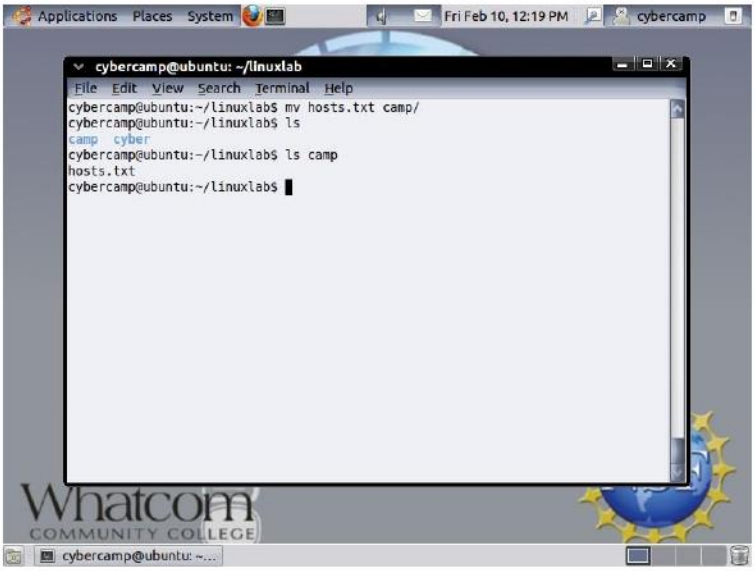
To move a file from one place to another, use the mv command. This has the effect of moving rather than copying the file, so you end up with only one file rather than two. It can also be used to rename a file, by moving the file to the same directory, but giving it a different name.

We are now going to move the file hosts.txt to your camp directory. First, change directories to your linuxlab directory (if you are not currently there). Then, inside the linuxlab directory,

type: **# mv hosts.txt camp/**

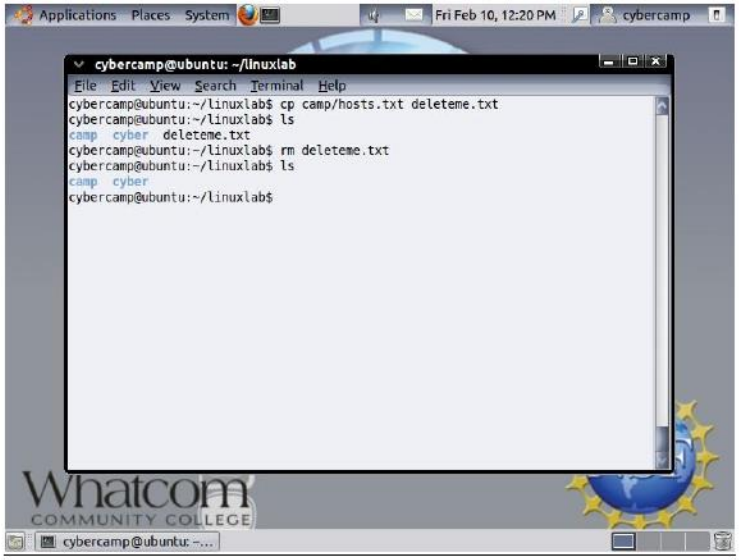
Now type: **# ls**; Then type: **# ls camp**

This is to verify that the file was moved into the camp directory.

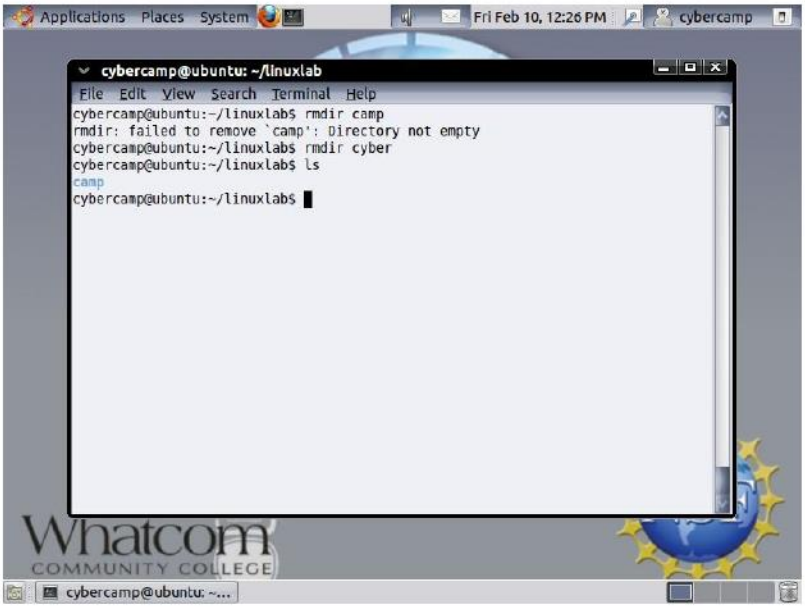


2.3 Removing Files

To delete (remove) a file, use the rm command. As an example, we are going to create a copy of the hosts.txt file then delete it. Inside your linuxlab directory, type these commands: # **cp camp/hosts.txt deleteme.txt** ; # **ls** ; # **rm deleteme.txt** ; # **ls**



You can use the rmdir command to remove a directory (make sure it is empty first). Try to remove the camp directory. You will not be able to since linux will not let you remove a non-empty directory. Now type: # **rmdir camp** ; # **rmdir cyber**

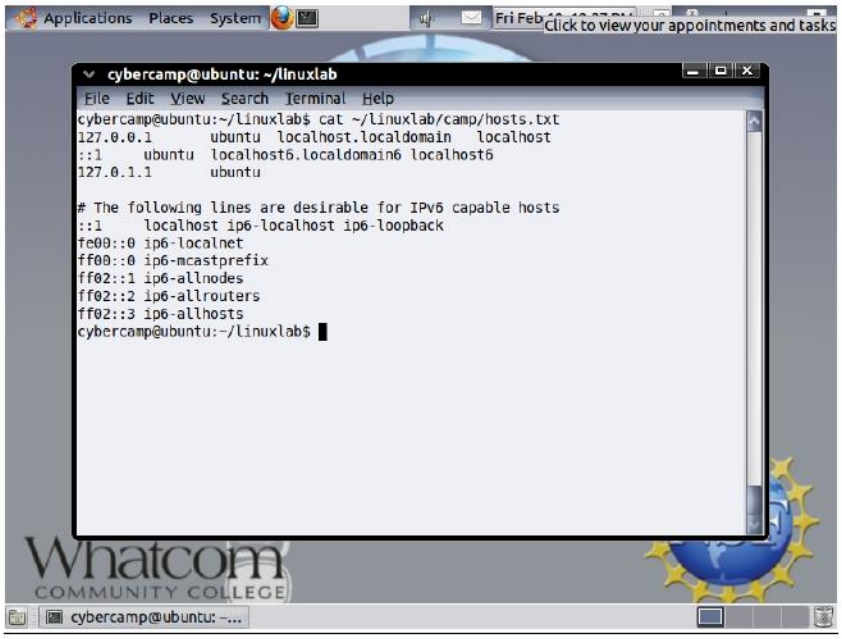


Were you able to remove the directory cyber without any error messages?

2.4 Displaying File Contents

The command cat can be used to display the contents of a file on the screen. Trying displaying the contents of the file hosts.txt by typing:

 # cat ~/linuxlab/camp/hosts.txt



3.0 Challenge Activity [OPTIONAL]

Using the commands discussed in this lab, navigate and explore the linux filesystem.

To change direcotory to the root folder, type: **# cd /**

Then view the contents with ls. Type: **# ls**

Displayed on the screen should be the linux file-system mount points.

Explore the contents here using **cd, pwd, ls, and cat**.

4.0 Independant Linux Research Resources: [ADDITIONAL INFO]

An Introduction to the Linux Command Shell for Beginners

|---http://vic.gedris.org/Manual-ShellIntro/1.2/ShellIntro.pdf

A-Z Index of the Bash command line for Linux

|---http://ss64.com/bash/

The Linux Documentation Project

|---http://tldp.org/index.html

YoLinux - Unix for DOS Users Comparison Table

|---http://www.yolinux.com/TUTORIALS/unix_for_dos_users.html

DistroWatch.com - Distribution and Package Monitoring

|---http://distrowatch.com/

Partial support for this work was provided by the National Science Foundation's Advanced Technological Education (ATE) program under Award No. 1104192. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

About process explorer:

Process Explorer is an advanced process management utility that picks up where Task Manager leaves off. It will show you detailed information about a process including its icon, command line, full image path, memory statistics, user account, security attributes, and more. When you zoom in on a particular process you can list the DLLs it has loaded or the operating system resource handles it has open. A search capability enables you to track down a process that has a resource opened, such as a file, directory or Registry key, or to view the list of processes that have a DLL loaded. The Process Explorer display consists of two sub-windows. The top always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window, which you can close, depends on the mode that. Process Explorer is in: if it is in handle mode you will see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you will see the DLLs and memory-mapped files that the process has loaded.

Lab Scenario:

You are a computer forensics worker who has come in to analyze the same backdoor you found last week in the Windows 2000 machine. The company wants to know more about what infected the computer, simply killing the process is not your job. You have made a snapshot of the Windows 2000 computer and have taken it to the lab to analyze. You need to write a report about what you have found. Luckily you have some steps listed below.

1. Open VMWARE Player.

2. Click 'Open existing VM or Team'

3. Go to C:\Users\Cybercamp\Desktop\CyberCamp Images\BreakIn-lab and select the Windows 2000 Server VMX file.

4. There is no password, just press enter at the login screen.

5. Open process explorer

6. Open task manager and go to the process tab

7. Compare task manager and process explorer output.

8. What is different and which program would you prefer?

9. Locate the BACKDOOR on process explorer

10. What kind of file is BACKDOOR?

11. What parent program is BACKDOOR running under?

12. Click the binoculars at the top of process explorer.

13. Search for BACKDOOR.exe

14. How many DLL substrings show?

15. Right click BACKDOOR and select properties

16. Select the Image tab

17. When was this program started? Can you correlate any similarities between when the program started?

18. What is the BACKDOOR PID number?

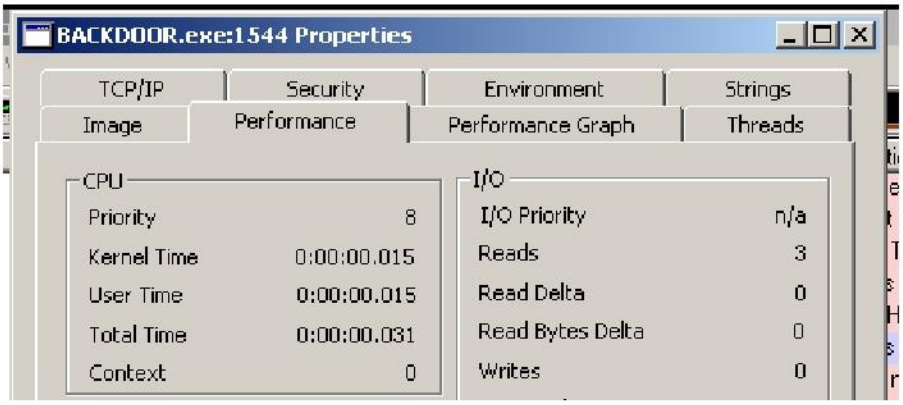
PID: The PID is the process identifier---the number that identifies the order in which processes are spawned from the Windows kernel, with one being the primary process and higher numbers being the latest or more recent processes.

About the image tab:

This page shows version information extracted from the process' image file, the full path of the image file and the command-line that launched the process. It also shows the current directory of the process, the user account in which the process is running, the name of the process' parent process, and the time at which the process started execution

19. Now select the Performance Graph tab.

20. How much of the CPU is used by BACKDOOR?



About the Performance Graph:

A history of a process' CPU usage and its private bytes allocation shows as in Task Manager like graphs on this page

21. Now select the TCP/IP tab

22. What is the protocol the program is using?

23. What port is the program listening on?

About the TCP/IP tab:

Any active TCP and UDP endpoints owned by the process are shown on this page.

24. Select the Security Tab

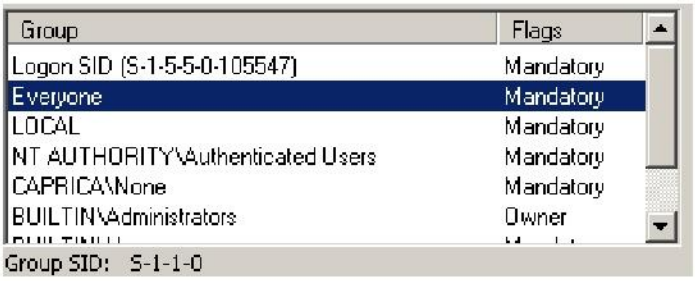
25. What user is the program running under?

26. Would it be more harmful for the program to have access to the administrator account? Why?

27. Make note of the Logon SID of the current user.

28. Click on different users in the Group table, notice how the Group SID changes.

29. Select user EVERYONE

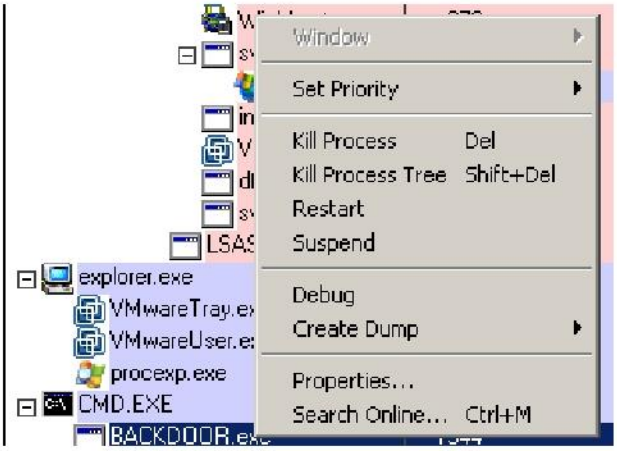


30. What permissions does user EVERYONE have?

SID: The SID (Security Identifier) is a unique ID number that a computer or domain controller uses to identify you.

31. Exit the properties window.

32. Right click BACKDOOR.exe and notice the kill process, and kill process tree options.



33. If you were to kill the process of BACKDOOR.exe would you want to kill the process or the process tree? Why?

34. Right click BACKDOOR and select "Search online".

35. How might you use this if you are unsure of a process?

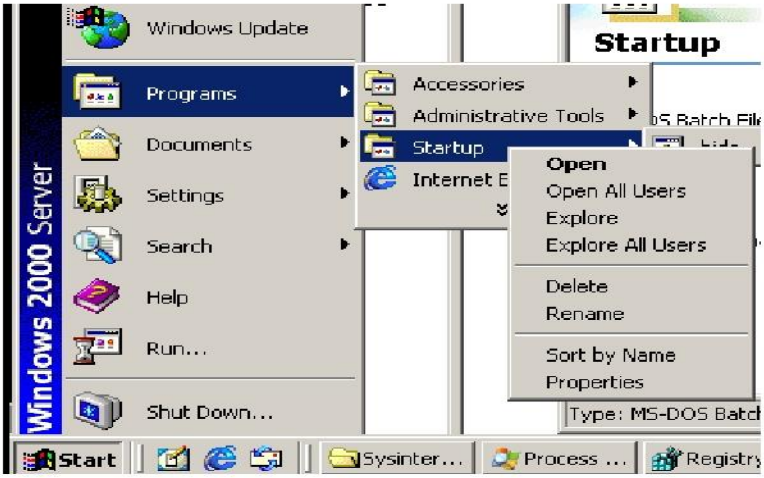
Additional questions:

Where is BACKDOOR.exe located?

1. Click start

2. Go to Programs

3. Right click startup and click on open.



4. You should see a batch file entitled "hide".

5. The programs in the startup folder, start when windows boots up.

6. If you were to delete this file, the BACKDOOR would not run on startup.

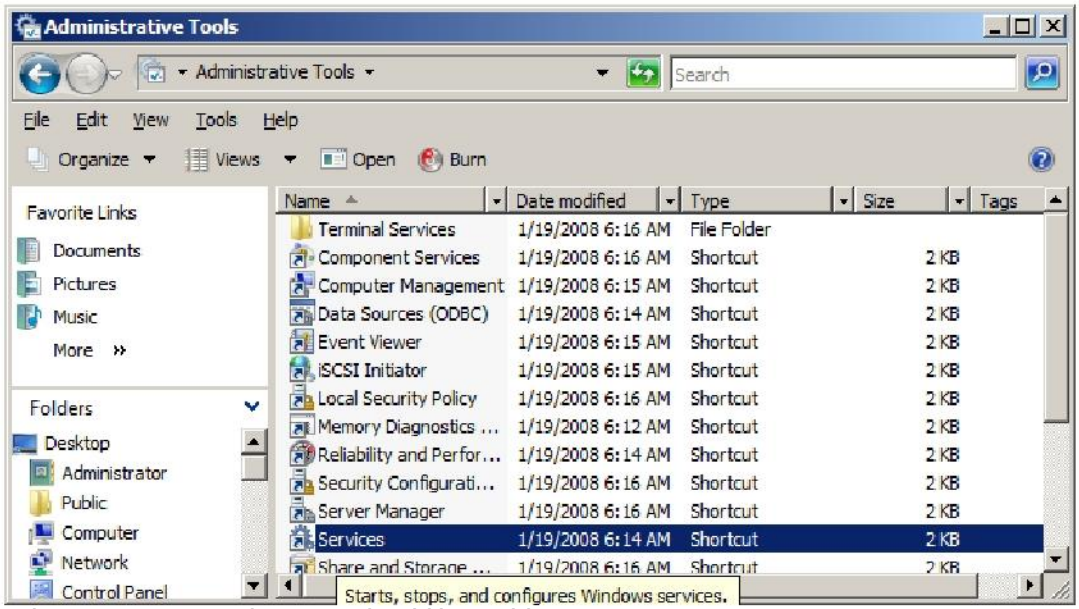
7. Would a malicious user want the BACKDOOR to run on startup?

Partial support for this work was provided by the National Science Foundation's Advanced Technological Education (ATE) program under Award No. 1104192. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

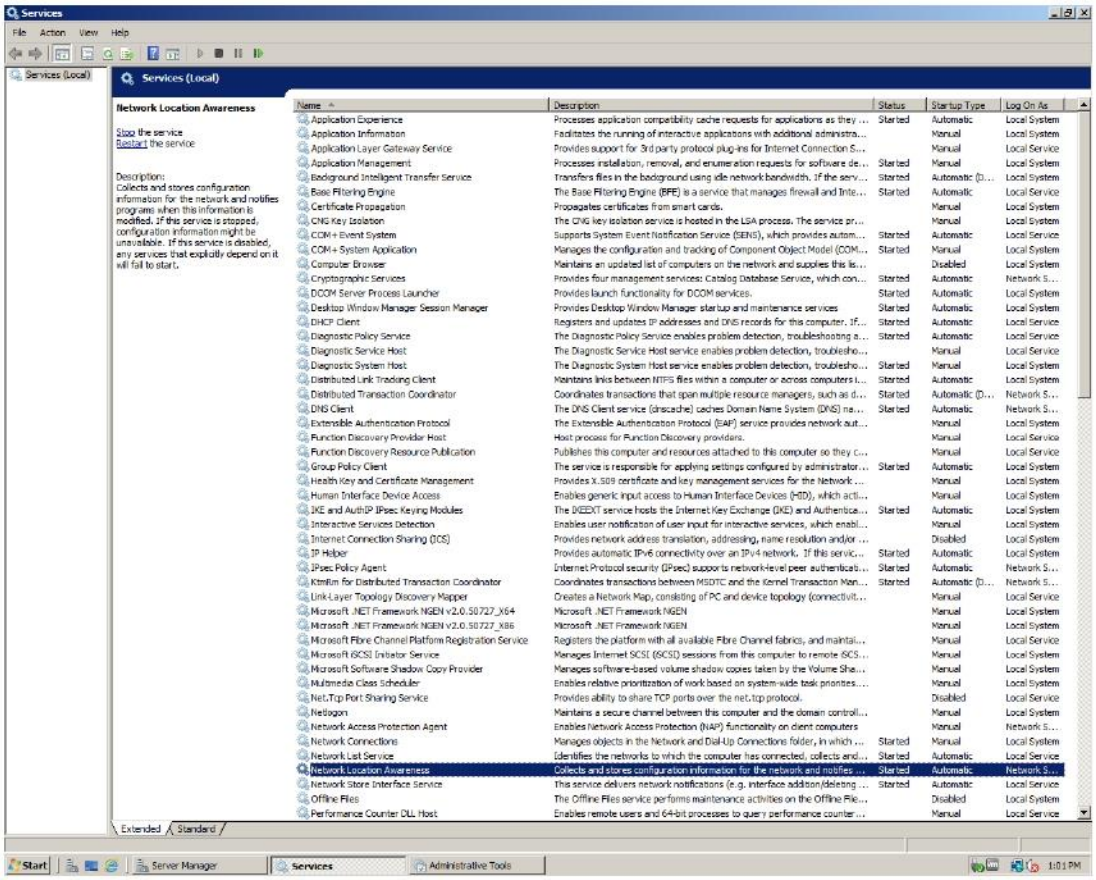
Disabling Unnecessary Services & Tasklist / Taskkill

Allowing unneeded services to run on a machine leaves vulnerabilities that can exploited; the best way to remove these vulnerabilities is to simply shut down these unnecessary services. Also letting these services run can lead to performance issues on older machines.

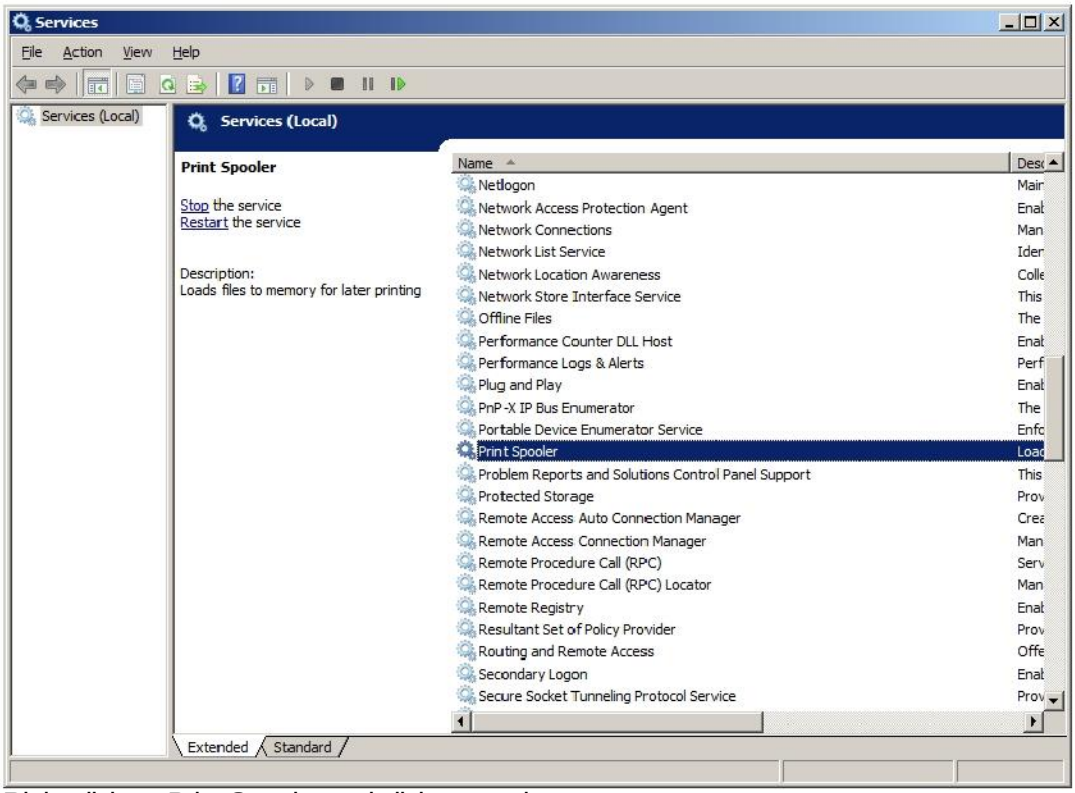
Go to start menu and click on control panel Administrator Tools services.



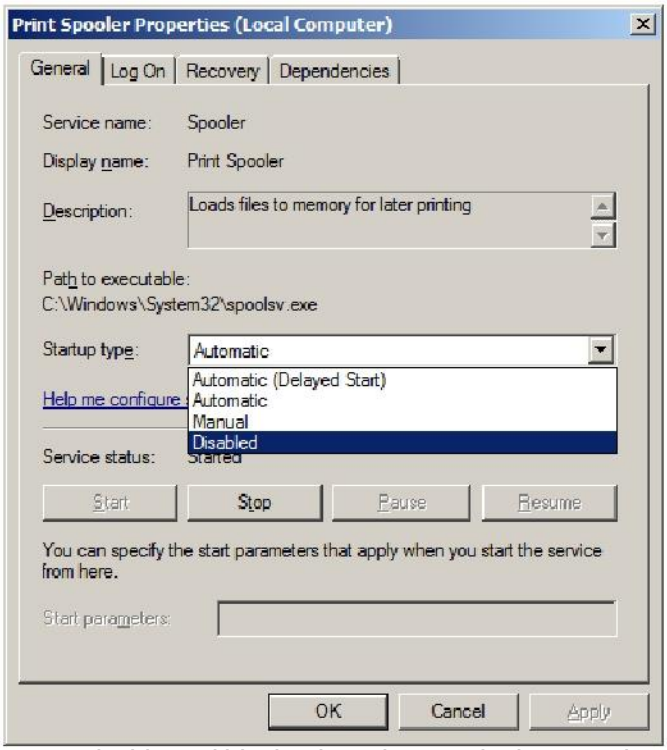
When you open services you should have this screen.



Next we want to disable unnecessary ports. Windows server 2008 does a farily good job of not starting up with to many unnecessary services but there are stil a few that should be disabled.

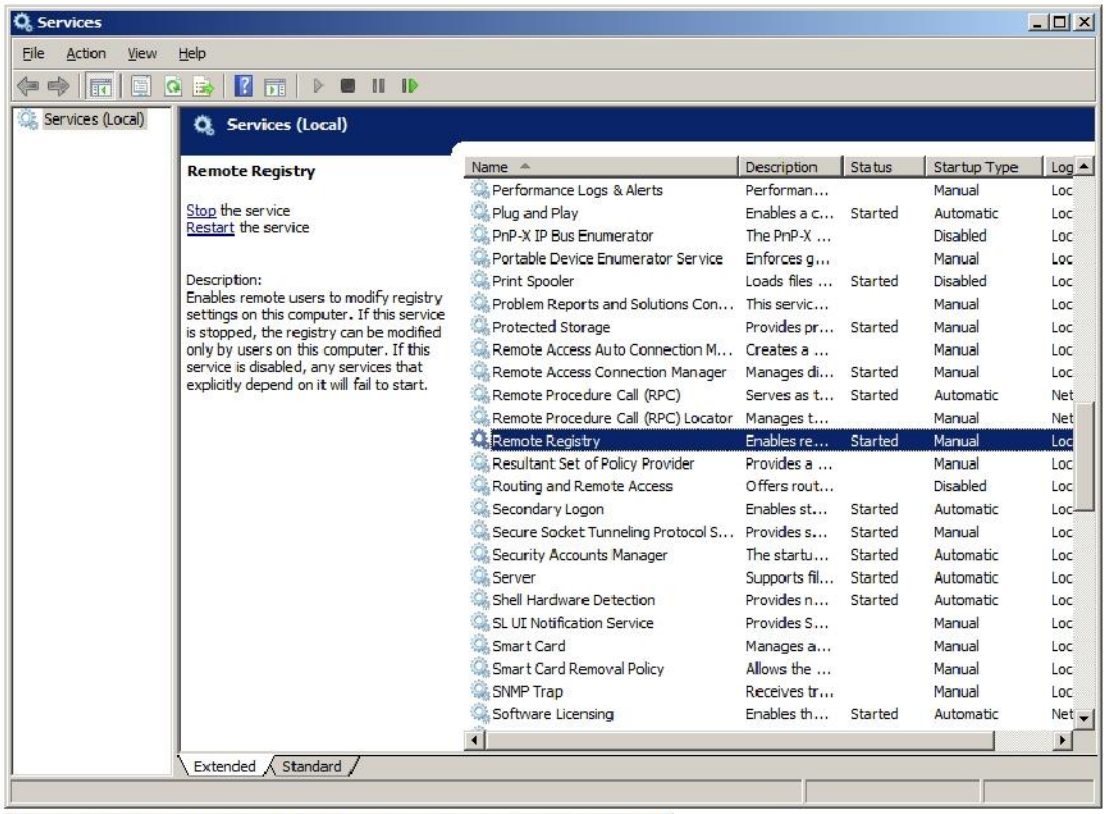


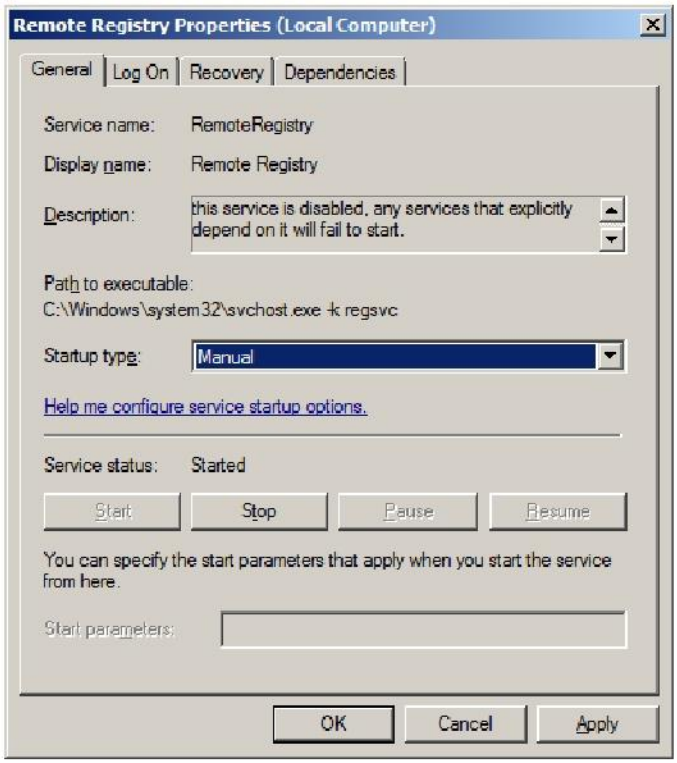
Right click on Print Spooler and click properties.



Go to Disable and hit ok. The Print Spooler has now been disabled.

Next click on remote registry





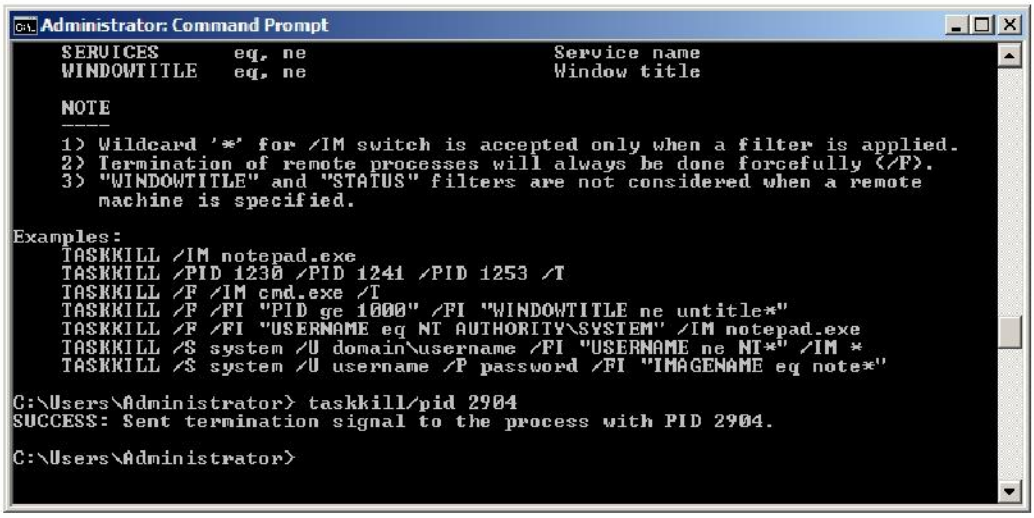
Lets set this to manual, this means it can be truned on by a program that needs it but will not run automatically. Click ok.

Next we are going to see what processes and services are running and how to kill these task. 1st open Internet Explorer. Next click Start, then in the search box type in **cmd** and press enter.

Once your command line is open type **tasklist /?** This command will give you an overview of the tasklist command.

Now lets do **tasklist /svc** and see whats running.

We can see that iexplore.exe is running (that's internet explorer) so now lets kill this process using the taskkill command type **taskkill /?** To see an overview of the commands.



Type **taskkill /pid ###** (the ### is the PID number that is deplayed for iexplore.exe in my example it is 2904. We can see that the termination signal was sent successfully and internet explorer closed.

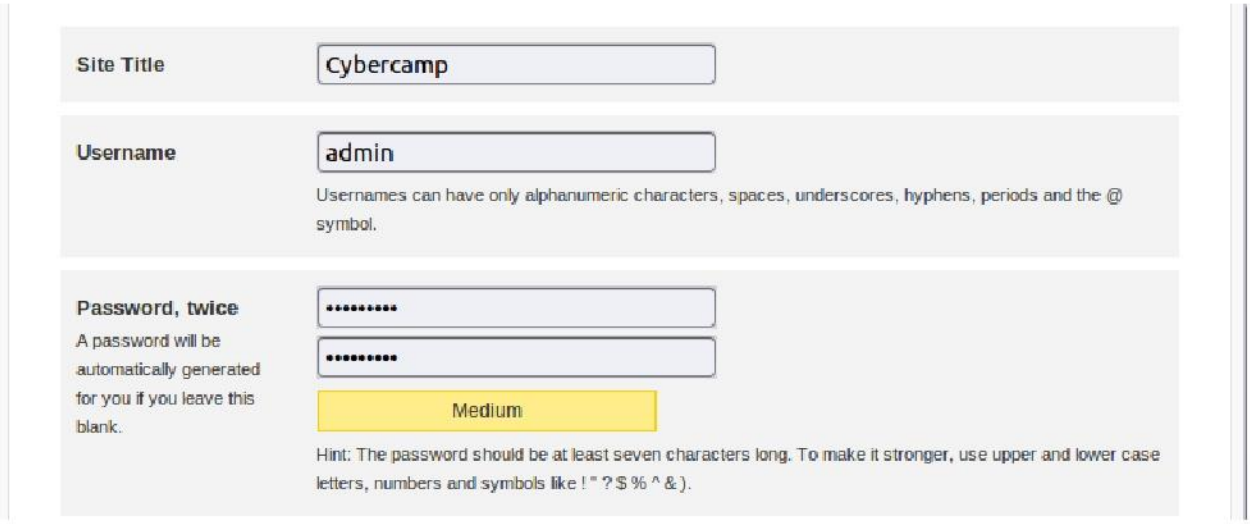
Partial support for this work was provided by the National Science Foundation's Advanced Technological Education (ATE) program under Award No. 1104192. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Word Press and Zencart Lab

Login into the Cyber Defenders Word.Zen image, Password is cybercamp all lowercase

Wordpress Install

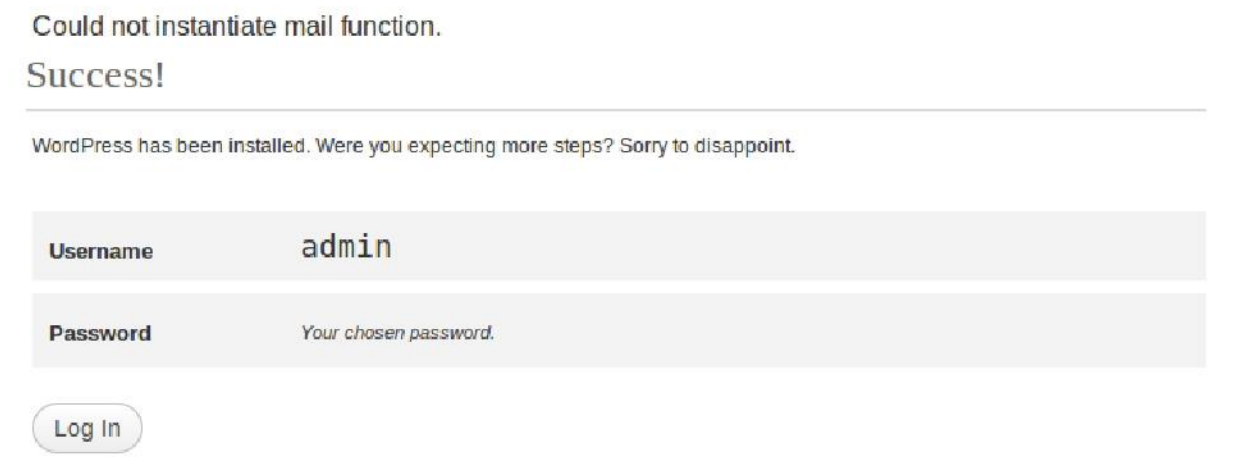
Open Firefox Web Browser and go to bookmarks
Look for Wordpress Install and open the link



Fill in cybercamp for the site title and passwords and use admin for the username
For lab purposes we will be using a made up email cybercamp@cybercampwcc.net
Be sure to uncheck the box near the bottom before continueing

Then push continue onto the next page

If everything went ok you will get a screen looking something like this below



After the success screen shows, we will click on the log in button to navigate to the admin controls

Next we will log into the control panel using the username admin and password cybercamp

Once logged into the control panel, we will be setting up a default theme for the wordpress
Navigate the left control panel and click on appearance

After clicking on appearance you'll get a screen with a few options for themes,

You can change the theme by clicking the Activate button to change the theme or you can preview it before changing it.

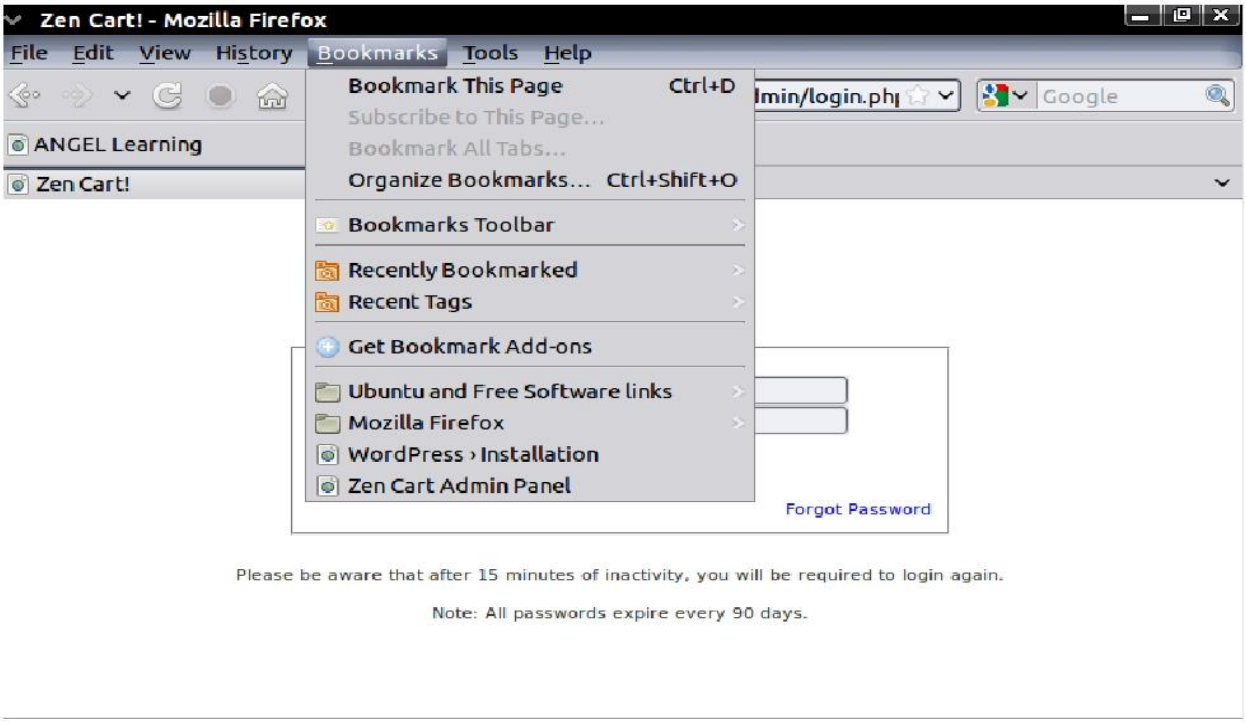
You can now navigate to the webpage by typing into the browser "http://localhost/wordpress/" into the url bar

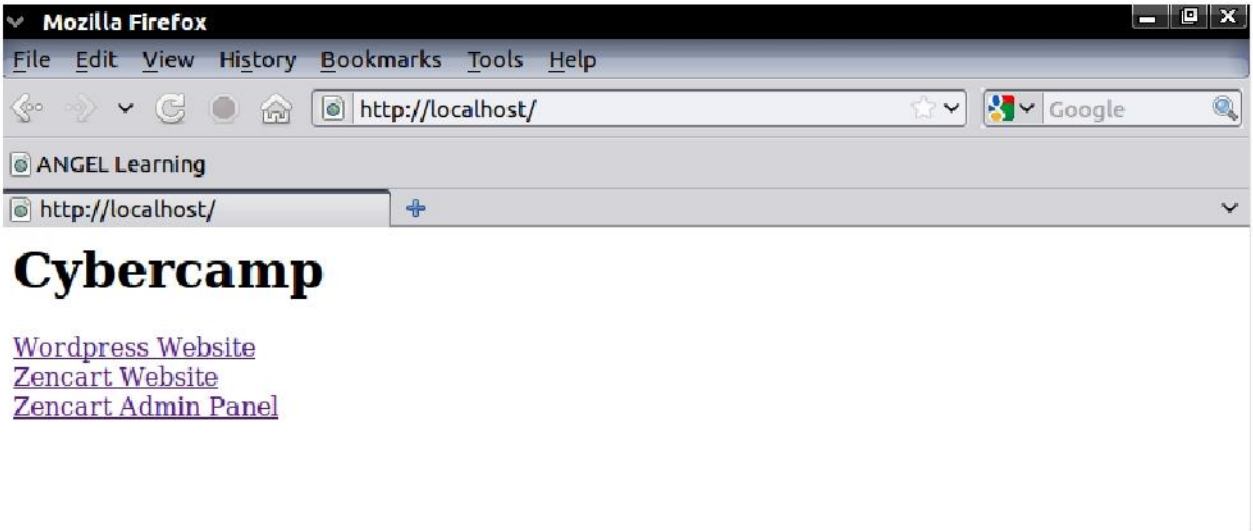
You should end up with the theme you selected.
You can also now navigate back to the admin panel on the front page near the bottom right by clicking login if needed to go back and test other items on the admin control panel to change the blog.

Zencart Lab

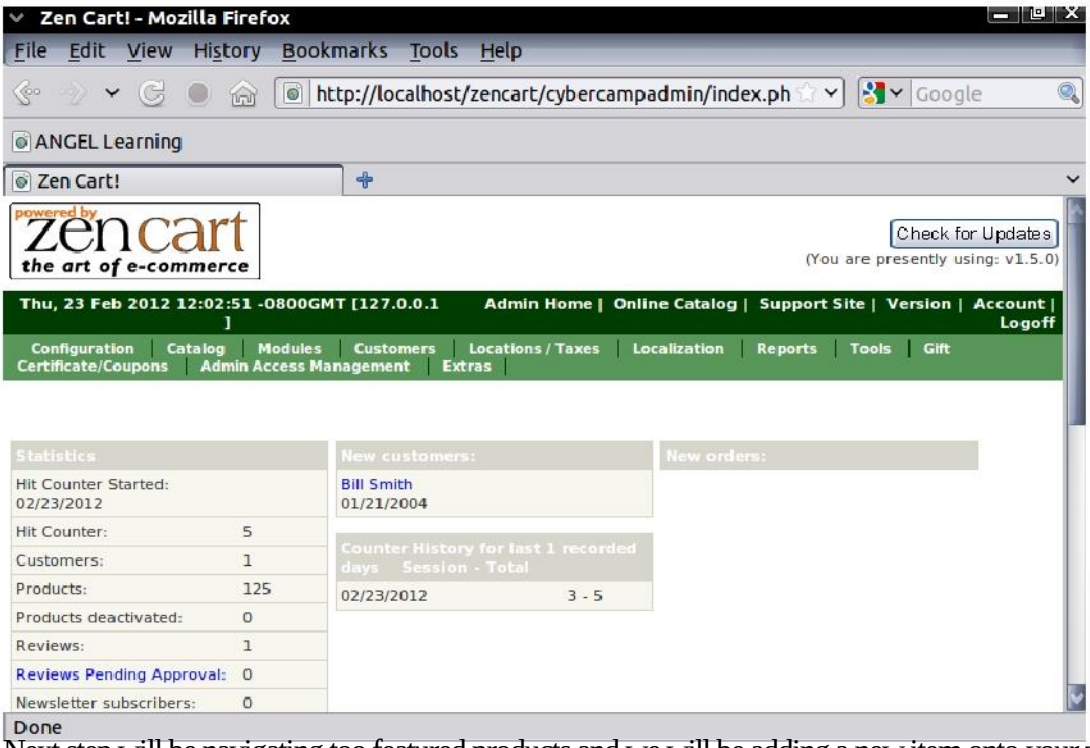
In this lab we will add an item to purchase into your Zencart website.

First we will navigate to the admin control panel via bookmark, or by going to localhost in a web browser



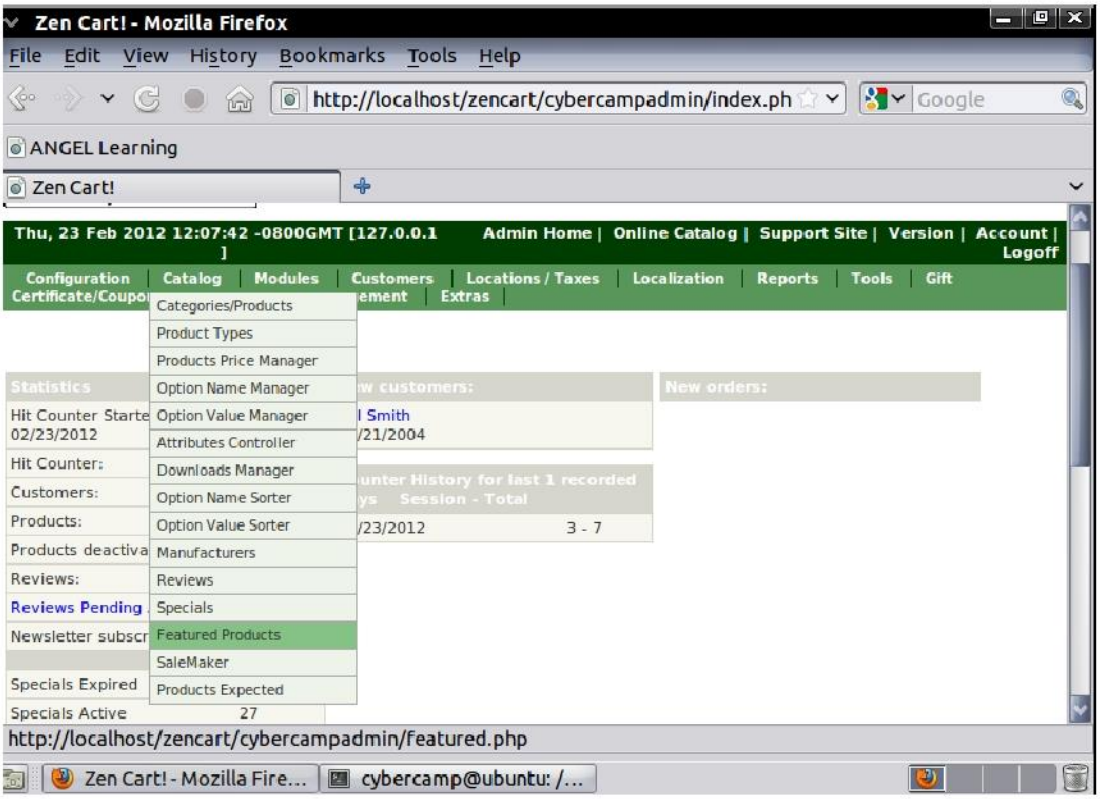


After getting to the zencart login screen we will be loggin into the control panel with the credentails listed here.
Username: admin
Password: cyber5amp
Once your in, you'll reach a screen looking like something below



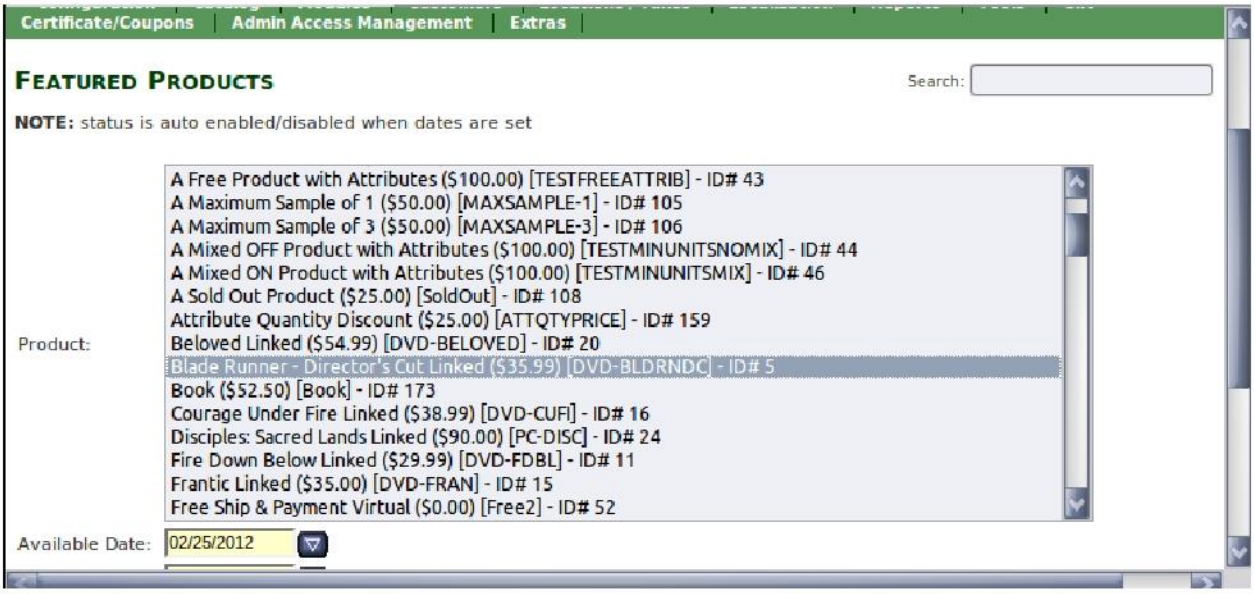
Next step will be navigating too featured products and we will be adding a new item onto your zencart website.

To do that you will move your mouse over catalog located near the top left on the navigation bar, and down to featured items like shown below.



Once there you then click on the new product button shown below.

Next select one of the products from the list of your choice and set the date for when it's available.
Go ahead and set it for today and for it to end a week later and continue after you select your product.



After you have selected your product it will be added to the list and showing its status, make sure the color to the right of the product is lit green.

If it is red, recheck the date you set to be sure it's available for today by clicking on the E icon next to the X.

You can navigate to your zencart website via typing http://localhost/ into firefox and navigate using the links shown, to get to zencart.

Or type in http://localhost/zencart/ into your url bar on firefox.

If done correctly you will have your item you added, shown in the featured item list on the main page.

Congratulations you have finished the lab
Now use the knowledge you gained today to attempt to further change the websites we have used in the lab.

Example: Add more products, Add products in other categories, Edit the blog website, add a post.

Partial support for this work was provided by the National Science Foundation's Advanced Technological Education (ATE) program under Award No. 1104192. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Whatcom
COMMUNITY COLLEGE

PACE UNIVERSITY
Hands-on Teaching Modules for Secure Web Application Development

ACM SIGCSE 2011 Workshop 27

Li-Chiou Chen and Lixin Tao

March 12, 2011

 The authors would like to acknowledge the support from the National Science Foundation's Course Curriculum, and Laboratory Improvement (CCLI) program under Grant No. 0837549. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Introduction

This workshop will discuss security issues in web application development and demonstrate a set of teaching modules in this area through hands-on exercises, developed by a NSF-funded project called SWEET (Secure WEb dEvelopment Teaching). The workshop will guide the participants to run through a couple of web security hands-on exercises, including web server threat assessment, security testing, and secure web transactions. All exercises are pre-configured in Linux virtual machines. The workshop will also discuss examples of incorporating SWEET in computing curriculum.

SWEET features virtualized web servers and a development platform that allows instructors to teach the security issues in web application development using regular computer laboratories. It includes teaching modules that are composed of the lecture materials and hands-on exercises.

The workshop DVD includes the laboratory exercises for the workshop, the presentation slides and the following sub-directories:

- Modules: All SWEET teaching modules including labs
- Solutions: Sample solutions for lab questions
- Tools: VMware Player[1]
- VM: SWEET virtual machines
- Tutorial: Linux & HTML tutorials

The exercises in this document are excerpted from SWEET teaching modules, which are included in the workshop DVD. For updates of SWEET teaching materials, you should visit the project website at **http://csis.pace.edu/~lchen/sweet/.** Below is the agenda of this workshop.

- Introduction to the SWEET project (10 minutes)
- Virtualization technology (30 minutes)
    - Exercise 1-3: Starting Linux virtual machine
- Security issues in web application development (40 minutes)
    - Exercises 4-8: Web server threat assessment
- Web application security testing (40 minutes)
    - Exercises 9-10: Web server scanning
- Digital certificate, HTTPS & SSL (40 minutes)
    - Exercises 11-13: Secure web transactions
- Wrap up & discussions (20 minutes)
    - Exercise 14: Turn off Linux virtual machine
    - Course integration, support, and others

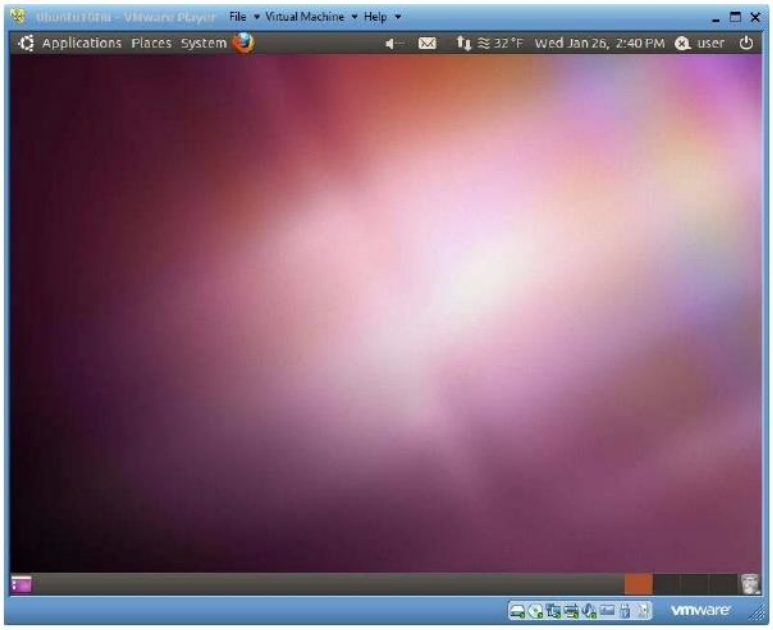
[1]VMware player (for Windows) is free for downloading and VMware Fusion (for MacOS X) is free for 30-day evaluation at www.vmware.com.

Exercise 1: Virtual Machine Installation

1. Copy all DVD materials to your computer where you will run the exercises.
2. On your computer, under the folder Tools, double click on VMware-player-xxxx.exe to install VMware player on your Windows machine or install VMware-Fusion-3.1.2-332101-light.dmg on your MacOS.
3. On your computer, under the folder VM, extract unbuntu10tm.zip to obtain the virtual machine.

Exercise 2: Boot up Linux Virtual Machine

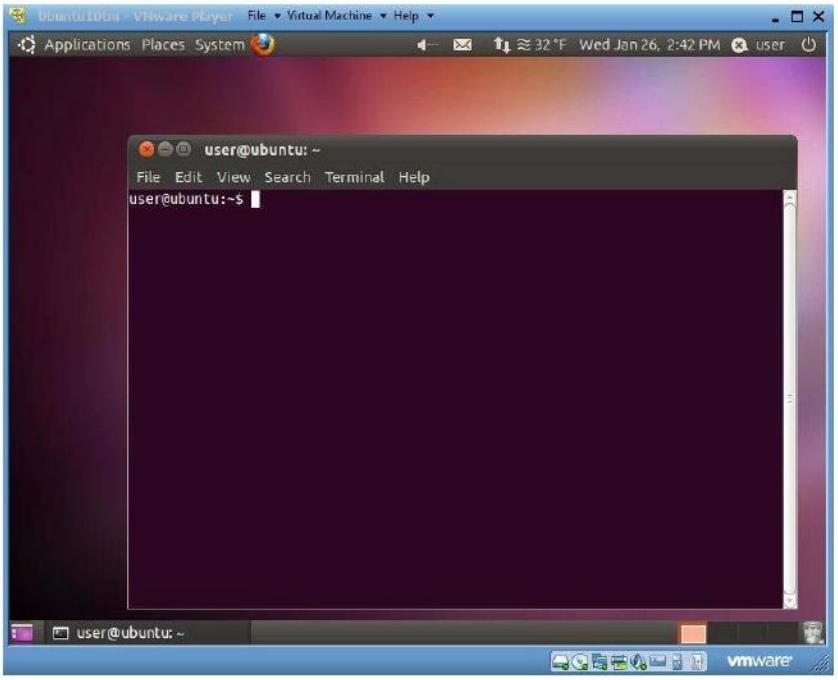
1. After VMware Player (or VMware Fusion) is installed, run the software and you should see a blue VMware Player Window pops up. Click on "Open a Virtual Machine" and select "Ubuntu10tm.vmx" from the "ubuntu10tm" folder under the ubuntu10tm folder.
2. Click on "play virtual machine". When being asked "Did you move this virtual machine, or did you copy it?" check "copy it".
3. When being asked "Would you like an attempt to be made to connect this virtual device every time you power on the virtual machine?", press "No" to avoid connecting to a virtual floppy.
4. When being asked if you would like to download VMware tools for Linux, answer "remind me later." Linux will boot up in about 2-3 minutes.
5. Login Linux using username "ubuntu10tm" and password "123456". After logging in, you will see Ubuntu 10 GNOME interface. The virtual machine runs Linux as if it is an independent computer. Actually, the Linux is run in the memory of the computer and simulate another physical machine that the virtual machine (VM) was created.
6. Once you logging in the system, you will see the Linux desktop, which looks like the screen below.



7. Below are some basic skills to use a virtual machine
   - To start directing mouse and keyboard input to a running virtual machine, type Ctr+g or click anywhere in the virtual machine window.
   - To start directing mouse and keyboard input to the host PC, type Ctr+Alt.
   - To get the logon window for Windows, use Ctr+Alt+Insert, instead of Ctr+Alt+Delete.
   - Scroll the bar on the right and at the bottom of the virtual machine window to see a wider screen.
   - To transfer files between the host and a running Windows virtual machine, just drag-and-drop the files.
   - USB disk is also a convenient way for transferring files between the host PC and a virtual machine. Inserting a USB disk to your PC when the virtual machine is active will attach the USB disk to the virtual machine.
8. Check out the menu bar for Linux GUI on the top panel of the window. The menu bar includes Applications (similar to Windows Start Panel), Places (all devices and storages), and System (Linux system functions).

Exercise 3: Basic Linux Commands

1. Click on Applications, Accessories and Terminal (You may need to scroll the window down to see Terminal if your screen is not big enough).
2. It opens up a Linux command prompt like the screen below.



3. Try Linux commands under the command prompt "user@ubuntu~$" (we will use $ referring the command prompt for all the instructions below). We will practice several basic Linux commands. For more Linux commands, please read the Linux Tutorial.
4. Try the following to see the files in this directory.

    $ls -al

Question 1: What are your results from "ls -al"? Copy and past the last three lines below.

Question 2: What does each line above mean? Please explain it. (**Hint**: In Linux, if you do not what a command mean, simply type "man command-name" to figure it out. For example, in this case, you can type "man ls")

Exercise 4: Observing HTTP Communications with *Paros*

In this exercise, you will use the *Paros* proxy server on your *Ubuntu virtual machine*, and use *Paros* to observer HTTP communications. The *Paros* proxy server will run at port 8088. You will set up the *Firefox* web browser so that when you use the browser to visit any web site, the HTTP request will be first forwarded to the *Paros* proxy server running at port 8088, which displays the HTTP request information in its graphic user interface, lets the user to have a chance to review and modify the request, sends the request to its destination server, and forwards the HTTP response from the web server back to the *Firefox* web browser. In this exercise you mainly use *Paros* to intercept HTTP GET/POST requests.

1. To start Paros, you need another Linux terminal window. Select Applications > Accessories > Terminal. Run these commands in the terminal window:

   cd ~/tools/paros

   sh startserver.sh &

   The Java-based Paros will execute and you will be greeted with its interface.

2. Open a Firefox browser. Now, you will need to change the proxy server settings in Firefox to redirect the web traffic to the proxy server. The proxy server is run under localhost and port 8088.

   - Go back to your browser. Select Edit > Preferences > Advanced > Network Tab > Settings.
   - Select the Manual Proxy Configuration radio button.
   - Enter these values into the fields: HTTP: 127.0.0.1 Port: 8088
   - If there are any values in the No Proxy For: text field, delete them. This is important to make the proxy work successfully.

3. Test the Paros proxy server by visiting http://localhost with your Firefox web browser. Once the browser contacts your web server, Paros starts to display HTTP request information in its graphic user interface.
4. You have just enabled all HTTP traffic generated by Firefox to be sent to the running Paros proxy server which can analyze HTTP traffic before it is sent off to its final destination.
5. Reload http://localhost. Go back to Paros, click on Sites to reveal "http://localhost", and select it.

Question 3: What HTTP request was used in the step above? _____

Question 4: Copy and paste below the Paros window with the HTTP request information.

6. Click on the HTTP request and the Response tab. You will see the HTTP response sent from the local Apache web server that Paros reads while being transmitted.

Question 5: What is the server version? _____

Question6: Copy and paste below the Paros window with the HTTP response information.

Exercise 5: Starting WebGoat

1. The web server has already been pre-installed and all you need to do is run the program.

2. From the menu bar on the top of the VM, select Applications > Accessories > Terminal. This will open up a Linux shell command terminal.

3. Run the following commands to start the web server.

```
cd ~/tools/tomcat/bin

sh startup.sh
```

4. Go to the Apache server homepage on your VM by entering http://localhost:8080/ into the Firefox address bar.

   (Tip: When running a program on port 80, you do not have to specify the port number as it is the default HTTP port used by most web applications and servers.)

Question7: Take a screenshot of the Apache Tomcat welcome page and paste it below.

Exercise 6: Web Goat Login

1. Go back to the browser in Ubuntu. Browse to http://localhost:8080/WebGoat/attack.

2. When prompted for login information, the user name is guest and the password is guest. On the WebGoat home page, click Start WebGoat.

3. Go back to Paros. You should see Paros logs of the connection between the browser and WebGoat.

Question 8: What is the first HTTP request in these transactions? _____

4. Go back to your browser. The left side of the screen is a list of WebGoat exercises you can try. We will try the first lesson, click on "General" and underneath it choose "HTTP Basics".

5. This WebGoat exercise will accept a value in the text box that you enter and reverse it. In the "Enter your name" textbox, type your name and click on Go.

6. You can see the parameters sent between your browser and WebGoat with Paros.

   - In Paros, look under Sites > http://localhost > WebGoat > POST:Attack(Screen,menu).
   - Change the view from Raw View to Tabular View.

7. You can see the session ID by looking under the Request tab in Paros next to the Cookie: reference.

Question9: There are two parameters in the transactions using POST: person and SUBMIT. The value for person is _____ and the value for submit is _____.

Question 10: Explain the function of the POST command with the two parameters.

8. When you see a green check on the exercise name in the left pane, you have successfully finished the exercise. You can also see the solution for the exercise by clicking on Show Solution in WebGoat. For all the exercises below, you can either read instructions from this manual or read the instructions from Show Solution (We use Paros instead of WebScarab in our lab).

Exercise 7: Injection Flaws - String SQL Injection

SQL injection is used to gain access, extract data or compromise secured databases. The methods behind an attack are simple and the damage dealt can range from inconvenience to system compromise.

1. On WebGoat, click on Injection Flaws and underneath select String SQL Injection in the left pane in WebGoat.

2. The exercise first prompts you to enter the last name Smith (SQL is case sensitive). A simple SQL query to a database would looks like this

SELECT * FROM user_data WHERE last_name = 'Smith'

3. In this case, Smith is the value you enter in the "Enter your name" textbox. The SQL will select all information about the user 'Smith' from the database.

Question 11: How many entries have you obtained? _____

Are they all information regarding the user "Smith"? _____

4. Let us look at the following SQL command

SELECT * FROM user_data WHERE name = '**Smith' OR '1'='1**'

5. This SQL command will ask the database to show all user information since '1'='1' is always true. String SQL injection exploit the vulnerability that a database that does not conduct checks on constraints so that attackers can inject SQL commands through the regular user interface.

6. Now, enter **Smith' OR '1'='1** in the "Enter your last name" textbox.

Question 12: Paste a screen shot of your results below.

Question 13: What is the security implication of your results?

Question 14: Describe a method to fix the vulnerability in this exercise.

Exercise 8: Cross Site Scripting (XSS) - Stored XSS attack

Stored XSS attacks allow users to create message content that could cause another user to load an undesirable page or undesirable content when the message is viewed or accessed. In this exercise you will create such a message.

1. On WebGoat, click on Cross-Site Scripting (XSS) and underneath select Stored XSS Attacks in the left pane in WebGoat.

2. In the title text box, type "XSS example"

3. In the message text box, type in the following HTML content.

```
<script language="javascript" type="text/javascript">alert("you are hacked");</script>
```

4. Click on Submit and click on the message you have just posted under message list.

Question 14: What will happen if someone clicks on the message you have just posted?

Question 15: Paste a screenshot of the results below.

Question 16: What is the security implication of your results?

5. Logout WebGoat and close the browser.

Exercise 9: Crawling Web Pages and Hidden Web Directories

We will investigate the web traffic between your browser and a pre-configured vulnerable website, the BadStore.net, using a web proxy called Paros on a same virtual machine. All web communication between the browser and the Web server will be sent to Paros (the proxy server) first before it reaches the appropriate destination. We will be browsing BadStore.net or investigate its vulnerabilities.

In order for an attacker to successfully plan and execute an attack, the attacker must know the website's layout and all the pages that might be available for exploitation. While manual web crawling is an option, it is a very time consuming process. An automated web crawler application will speed up the mapping process significantly.

1. From the menu bar on the top of the VM, select Applications > Accessories >
2. Terminal. This will open up a Linux shell command terminal, execute the command

   ifconfig
3. You will receive several lines of output. You are going to look for the Ethernet interface **(i.g. eth0)**. Find the **inet addr**: field and write down the IP address in the space below.
4. Make sure Tomcat server is not running, otherwise go to Select Applications > Accessories > Terminal. Run following command in the terminal window to shut down tomcat

   tomcat-stop
5. Open a Firefox browser to browse BadStore.net by typing the IP address of your VM in the URL e.g **http:// IP ADDRESS/badstore** (DO NOT browse www.badstore.net directly since it will redirect you to original website if you have an Internet connection).
6. Switch to the Paros application and click **File > New Session** and click **OK** to have Paros start a new session and purge itself from any logged content.
7. In the Paros menu toolbar, navigate to **Tools > Options** and select the **Spider** option. You will change the **Maximum Depth to Crawl** from its default value to the

maximum value of **9**. This will allow Paros to crawl web pages that may be deeply nested in BadStore.net Click **OK** to confirm and return to the main screen.

8. In the **Sites** panel on the left will be all the websites that Paros is logging. It is currently blank, change to the Firefox application and refresh BadStore web page (You may have to clear recent browsing history first to reload the page. **Tools > Clear Recent History**)
9. Switch back to Paros and you will see an arrow next to **Sites** that is point to the right. Click the arrow to un-collapse the logged websites. You will see the IP address of BadStore website.
10. Select the IP address for BadStore under **Sites** in Paros. The IP address will be highlighted in brown and go to **Analyze > Spider** in the Paros toolbar menu.
11. A Spider window will open. In the **URL crawling:** field should be the IP address of BadStore.net. If all checks out, click **Start**.
12. Once crawling has begun, the main Paros window will begin to populate with web pages and images that are hosted within BadStore.net.
13. In the bottom pane of the main screen, you will see a **URL found during crawl:** panel. Notice that it is located under the **Spider** tab near the bottom.
14. Looking through the entries, you will notice that most of the web cgi pages are located in the **/cgi-bin/** directory but some are not. List one other directory that Paros had crawled and one file under this directory

Directory name: _____

File name: _____

Question 17: Briefly explain what information one might obtain by crawling a web site.

Question 18: What is the potential risk for a web site being crawled?

Exercise 10: Scanning For Known Vulnerabilities

In the previous exercise, you have mapped BadStore.net; in this exercise you will execute a vulnerability scan on BadStore.net.

1. In the Paros Sites panel, Click on the IP address of BadStore, highlighted in brown.
2. In the Paros toolbar menu, navigate to **Analyze > Scan**. The vulnerability scan will begin. Give it a minute to complete the scan.
3. Once the scan is finished, the results can be viewed on the bottom panel of the Paros application under the **Alerts** tab. If you would like to have an actual report, click on **Report** > **Last Scan Report**. The report will be generated in the **/user/paros/session** folder and it is called **LatestScannedReport.html.** Open it in a browser. (Click on the menu bar on the top, click on **Places** to access **Home Folder**)
4. The vulnerabilities are called alerts and are classified as High, Low, and Medium. List two vulnerabilities from the report and discuss the countermeasures to fix them.

Question 19: Vulnerability 1: _____

Countermeasure 1: _____

Question 20: Vulnerability 2: _____

Countermeasure 2: _____

5. Not all web crawlers and web vulnerability scanners are as robust. Commercial web crawlers and vulnerability scanners may perform a much more complete crawl and may list more potential vulnerabilities.
6. Click on **File** > **Exit** to close Paros.
7. Close all the command prompt terminals on your VM.
8. Open a Firefox browser. Now, you will need to change the proxy server settings back. Go back to your browser. Select Edit > Preferences > Advanced > Network Tab > Settings. Select No Proxy radio button and hit OK.

Exercise 11: Creating SSL Certificates Using OpenSSL

In the following exercises, you will learn how to install your very own secure web server which utilizes SSL/TLS for secure communications. To install an open-source secure web server, web developers usually need to install two software packages from different sources. For simplicity, they have already been installed on your Ubuntu virtual machine.

- **Apache 2.2.11**: Apache2 is an open-source web server. You can find more information about Apache2 at *http://httpd.apache.org/*.
- **OpenSSL 0.9.8k**: OpenSSL is a set of open-source toolkits that implement the Secure Socket Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a general purpose cryptography library. You can find more information at *http://www.openssl.org/*.
- **Mod_SSL 2.2.11**: Mod_SSL is an add-on module for older versions of Apache that had to be compiled. With Apache2, mod_SSL is built into the server which provides the interface between Apache and OpenSSL. You can find more information about mod_ssl from *http://www.mod_ssl.org*.

We will need to create a SSL certificate for the web server before we can run the server securely with HTTPS. This exercise creates a public/private key pair, a SSL certificate, a certificate signing request (CSR) and we will also become a Certificate Authority (CA). Usually a commercial server would ask a trusted third party to sign their certificate. For example, VeriSign is one of the most well-known companies that signs certificates for commercial servers.

You must have a public/private key pair before you can create a certificate request. You will also need a FQDN (Fully Qualified Domain Name) for the certificate you want to create. Since we are hosting the website locally, you are able to choose any FQDN that you like. For this lab exercise we will use **www.BadStore.net** as a domain name. You will also be creating a certificate for www.BadStore.net which is actually hosted on the local virtual machine

1. Access the Terminal window by navigating to *Applications* > *Accessories* > *Terminal.*

2. Point the terminal shell to the ***/etc/apache2/ssl*** directory by running command:

cd /etc/apache2/ssl

3. The ***ssl*** directory is where you will store all your private keys, certificate signing request and certificates.

4. There are existing keys and certificates under this directory (you can see them using ***ls*** command). We will start this exercise by a new set of keys. So, please delete the files under this directory before we start.

sudo rm *

When prompted for the [sudo] password, it is the same password (***123456***) that was used to login.

5. To generate the Certificate Signing Request (CSR), you will need to create your own private/public key first. You will create a key by the name of **server.key**. Run the following command from terminal to create the key:

sudo openssl genrsa -des3 -out server.key 1024

genrsa indicates to OpenSSL that you want to generate a key pair.

des3 indicates that the private key should be encrypted and protected by a passphrase.

out indicates the file name in which to store the results.

1024 indicates the number of bits of the generated key.

The result is going to look something like this:

Generating RSA private key, 1024 bit long modulus

.....++++++

..++++++

e is 65537 (0x10001)

Enter pass phrase for server.key:

Verifying - Enter pass phrase for server.key:

You will be prompted for a pass phrase, once you type in your initial pass phrase, you will be asked to verify this pass phrase. **Write down your passphrase below:**

_____

If you execute command ***ls*** in terminal you will see a file called **server.key** in the *ssl* directory**.**

6. You will store your passphrase in a password script, so that Apache2 will not prompt you for the pass phrase whenever Apache2 is started or restarted.

   Run command: **sudo gedit /etc/apache2/ssl_passphrase**

   The **ssl-passphrase** script will be opened in a text editor. Enter your private key pass phrase in-between the pink quotes replacing ***123456***. Click *File > Save*.

   If the pass phrase does not match the pass phrase that you had submitted to Apache2 when you created your private key, the private key will not be decrypted when Apache2 starts resulting in non accessible hosted websites.

7. Next you will create a certificate signing request with the private/public key you have just created. This command will prompt for a series of things: When prompted enter the values as follows:

   Country Name: US
   State or Province Name: New York
   Locality Name: New York

Organization Name: Pace University

Organizational Unit Name: CSIS-IT300

Common Name: **www.BadStore.net**

Email: Your email address

A challenge password: enter another password that you can remember.

An Optional Company Name: CSIS

A very important step to keep in mind is when filling out the **Common Name (CN)** field. The Common Name should match the web address, DNS name or the IP address you will specify in your Apache configuration. For this lab example the Common Name that we will be using is www.BadStore.net

Otherwise to create the Certificate Signing Request, run the following command at the terminal prompt, making sure you are still in the ***/etc/apache2/ssl*** directory.

sudo openssl req -new -key server.key -out server.csr

You will be prompted to enter your private key passphrase. You will also be prompted to enter the values which were addressed above.

You may run command **ls** in the *ssl* directory to see a file called ***server.csr*** when you are finished. This is your certificate signing request.

8. Now you will create your self-signed certificate. Make sure you are still in the ***/etc/apache2/ssl*** directory.

   The certificate signing request (CSR) has to be signed by a Certificate Authority (CA). For testing purpose, we will not ask a commercial CA (such as Verisign) to sign our certificate but sign the CSR by ourselves, which is called self-signing. In this case, we are our own CA.

   The following command will create a self signed certificate that will last for 365 days.

sudo openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

The command will prompt you to enter your private key passphrase. Once you enter the correct passphrase, your certificate will be created and it will be stored in the `server.crt` file.

The above command, took the certificate signing request, plus your private key in order to make your self-signed certificate.

9. Run command **ls** in the ***/etc/apache2/ssl*** directory and you will see ***server.crt,*** ***server.csr***, and ***server.key***.
10. You have just created your very own self-signed certificate.

Exercise 12: Configuring Apache2 with BadStore.net

1. In the **ssl** folder under the Apache2 directory, there should exist three files, server.crt, server.csr and **server.key**. Make sure these files reside in this directory for the next steps to be successful.
2. Enable the SSL module for Apache2

   sudo a2enmod ssl

** To disable the SSL module for Apache2, the command is **sudo a2dismod ssl ****

3. A restart of Apache2 is required for the SSL module to be effective.

   sudo /etc/init.d/apache2 restart

   Apache should restart with no errors.

4. Creation of a virtual host for the secured BadStore.net website is necessary so that when the FQDM is entered into a web browser, the secured BadStore.net website will be available at that address. Start by copying the default template which will be modified in the following steps.

   sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/www.badstore.net

   The template copy is now named www.badstore.net and is located in the /etc/apache2/sites-available/ directory.

5. Edit the content of the template copy. This is a very important step. Make sure it is modified correctly.

   sudo gedit /etc/apache2/sites-available/www.badstore.net

   Change the VirtualHost port from 80 to 443. The first line of the file will look like the following:

<VirtualHost *:443>

Next declare the server name and the fully qualified domain name plus the HTTPS port number after the **ServerAdmin** line.

ServerName www.badstore.net:443

Change the **DocumentRoot** to point to the badstore web directory (setup of the badstore directory will be explained later in this document).

DocumentRoot /var/www/badstore

Also change the **<Directory /var/www/>** to reflect the badstore web directory.

<Directory /var/www/badstore>

In the line before ErrorLog /var/log/apache2/error.log, you will enter these values

SSLEngine On
SSLCertificateFile /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key

These entries tell the virtual host where the SSL certificate and key are located and to turn on SSL.

6. Save the file.
7. Enable the website.

sudo a2ensite www.badstore.net

8. Edit the **/etc/hosts** file to resolve the www.badstore.net website to 127.0.0.1 since the website is hosted locally.

sudo gedit /etc/hosts

Find the line that begins with 127.0.0.1, replace localhost text at the end and in its place enter www.badstore.net.

9. Save the file and exit gedit. You have just configured SSL on www.badstore.net, a local Apache web server.

Exercise 13: Running a Secure Web Server

1. All the web server settings are contained in the Apache2 server configuration files. For simplicity, the configuration files have already been modified for you. If you have correctly followed the directions for generating SSL certificates, everything will work correctly.

2. You need to restart Apaceh2 for the SSL certificate settings to take effect. Run command:

   sudo /etc/init.d/apache2 restart

   If everything is correct, Apache2 will restart and give you an [OK] message.

3. Open Firefox and visit *http://localhost* you should be greeted with a message that states "It Works!"

4. In your browser, visit the following URL https://www.badstore.net

5. **VERY IMPORTANT**: The beginning of the URL is **HTTPS** not **HTTP**

   Firefox will display a message stating ***This Connection is Untrusted*** due to the certificate that is used. In Firefox, The certificate is not trusted because it is self-signed. We will accept the certificate anyway and add an exception.

   - Click the ***I Understand the Risks*** link.
   - Click the ***Add Exception*** button.
   - Click the ***Get Certificate*** button.

   You can click the ***View*** button to see the self-signed certificate that you have created.

   Make sure the ***Permanently store this exception*** checkbox is selected and click the ***Confirm Security Exception*** button.

6. Take a screenshot of the secured web page and paste it below.

7. Do you see a silver lock on the lower right corner of the browser window? _____

Question 21: Double-click on the silver lock. Click on the ***View Certificate*** button. What is the validation period of this certificate? _____.

Question 22: Click on the ***Details*** tab. Who is the issuer of this certificate?

Question 23: What is the functionality of the certificate during web communication between the browser and your web server?

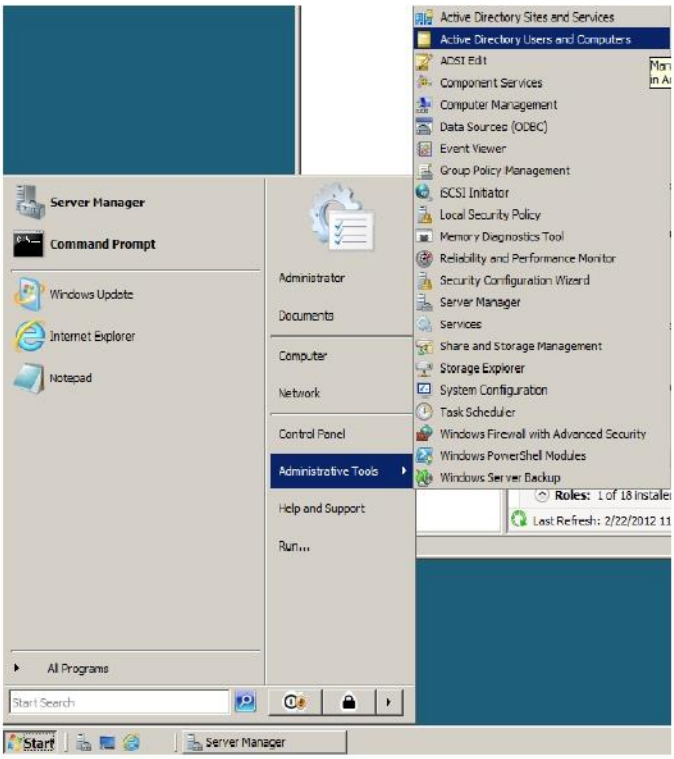
[**Note**: You will see the same silver lock when you check out your purchase on Amazon.com or other secure web servers. Double-click on the silver lock next time when you shop online and take a look at their certificates]

Exercise 14: Turn off Linux VM

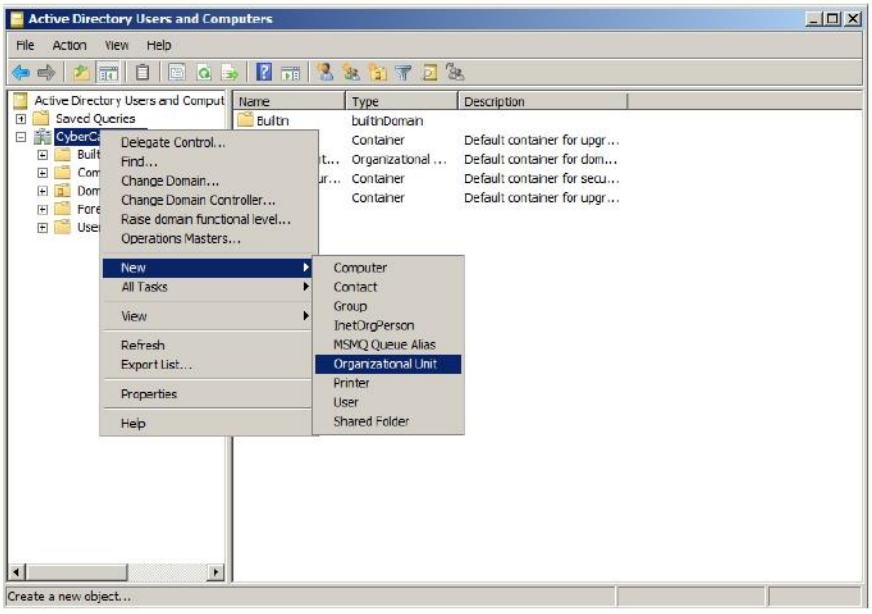
1. Close all the browsers and terminal windows on the VM.
2. Turn off the Linux VM by clicking on the power button on the upper-right corner.
3. This VM is used by all exercises in the SWEET teaching modules. Please keep it on your computer for all the exercises.

Windows 2008 Server and Active Directory

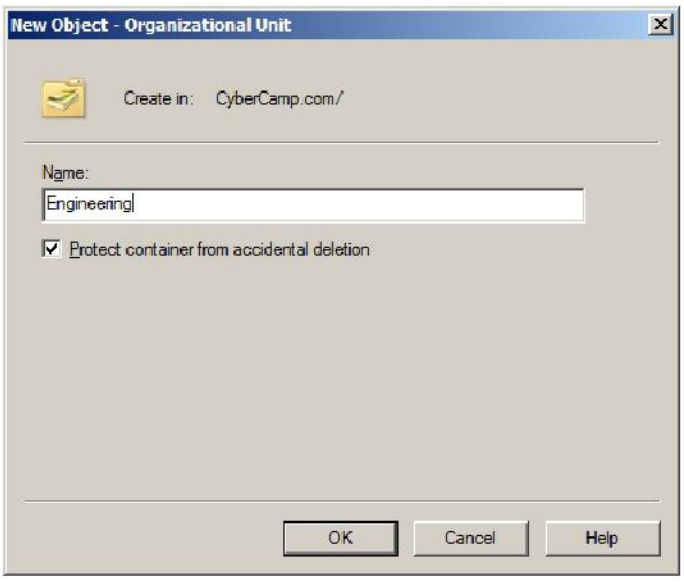
1. First we are going to add some OU's (organizational units) for Engineering, Marketing, Programing, Management and Sales. Go to VM at the top of your screen and send CTRL ALT DEL to log in, Username = Administrator Password = Password02 (it is case sensitive) Go to Start □ Administration Tools □ Active Directory Users and Computers



Next we want to expand the CyberCamp.com Domain and a new OU



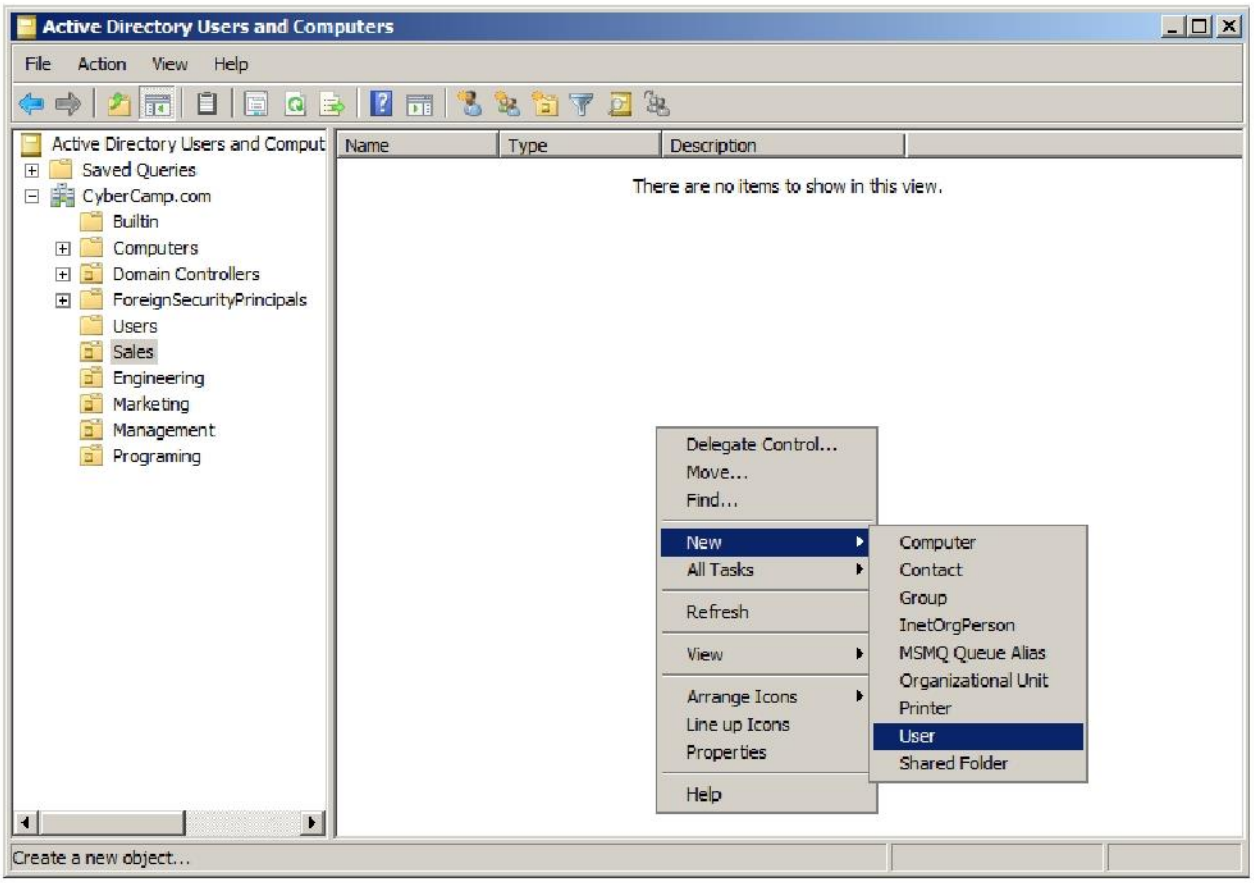
Type in the OU's name and click OK.



Do this for all OU's Engineering, Marketing, Programming, Management and Sales.

Next we need to add users to these OU's.

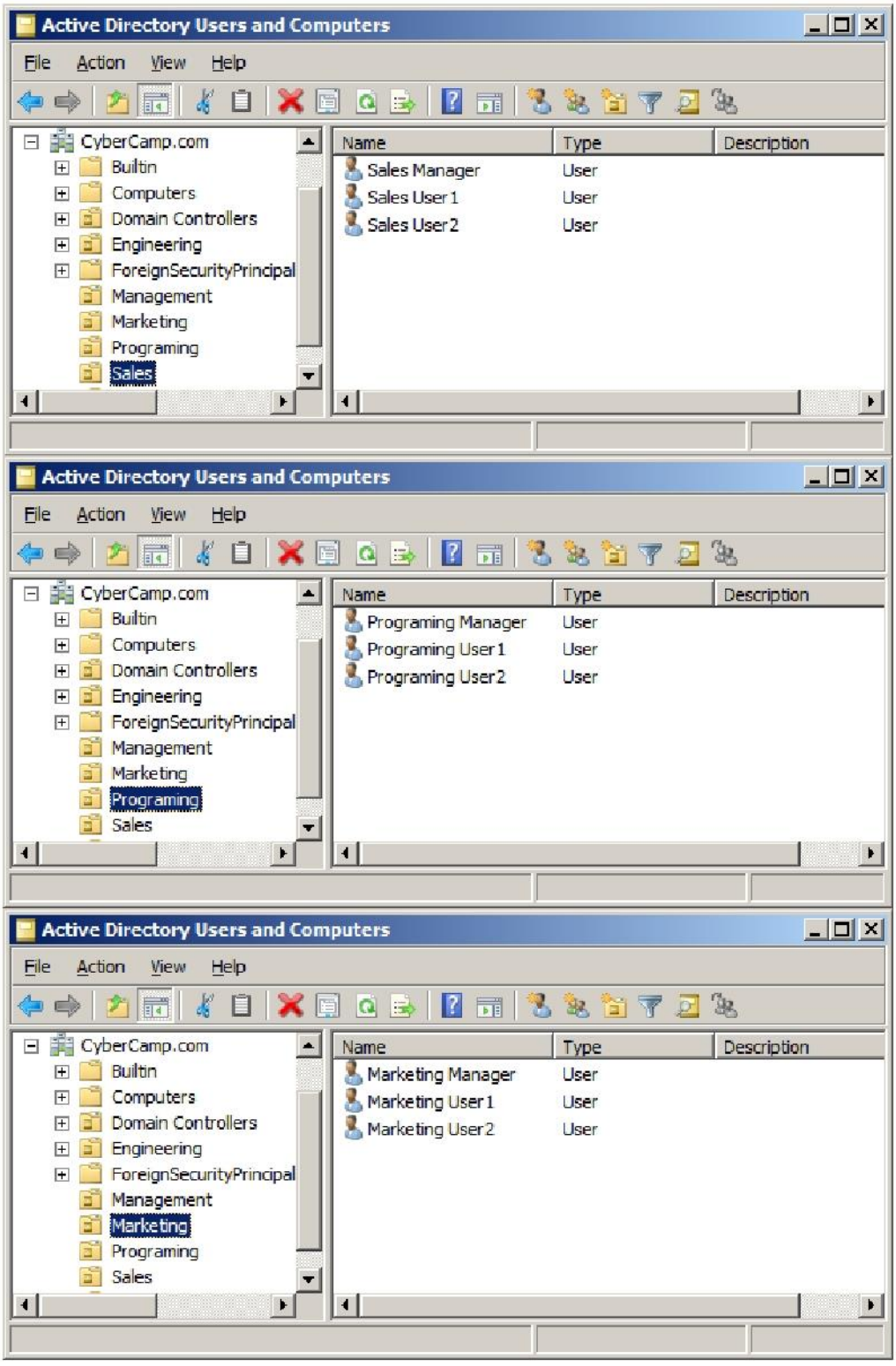
Right click in the right window and go to new □ user



We will use a simple naming scheme SalesUser1, SalesUser2 and SalesManager do this for all
OUs (Engineering, Programing, etc.)

Next for the password we will be using the password you should NEVER use in a non-lab environment, Password01.

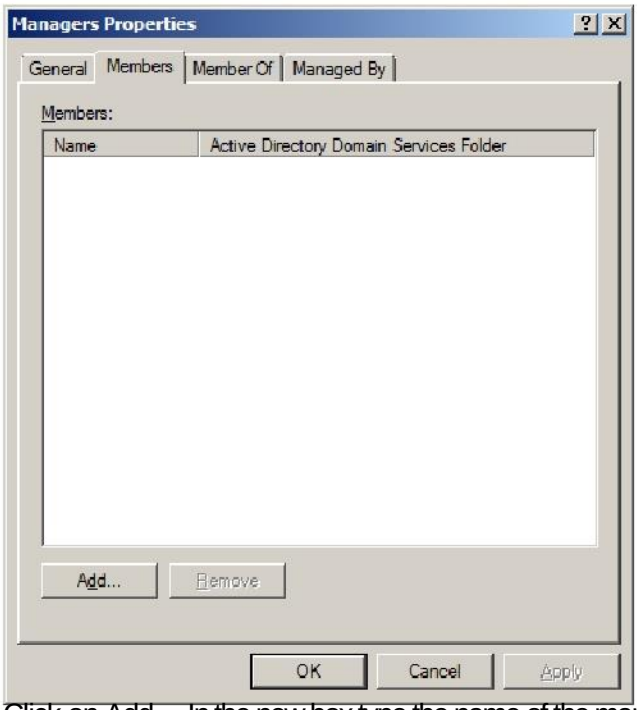
Create a Sales User 2 and Sales Manager, now do the same for the Marketing Engineering and Programing OU's. Afterwards your AD should look like this.



Next we are going to set up 2 groups to add our users to. Groups are a great way of setting permissions for many users at once instead of setting permissions for each user individually.

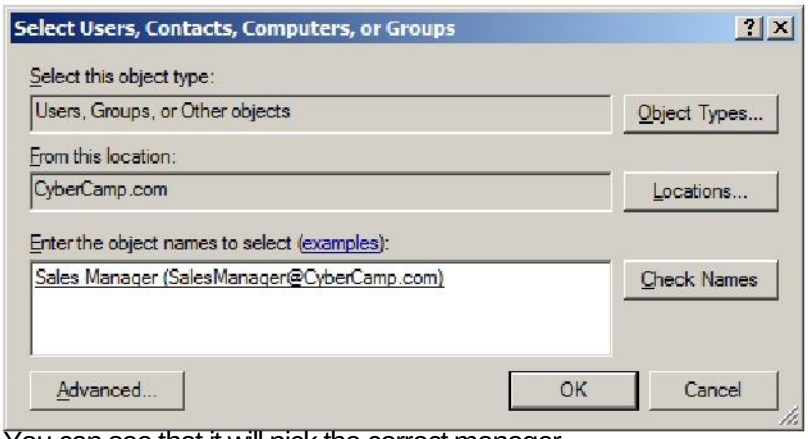
Let's start by going to our manager OU and adding a Manager group. For now we can leave the group as a global security group.

After we have created our new group we need to add our managers to this group. Right click on the new group and click properties, then move to the Members tab.

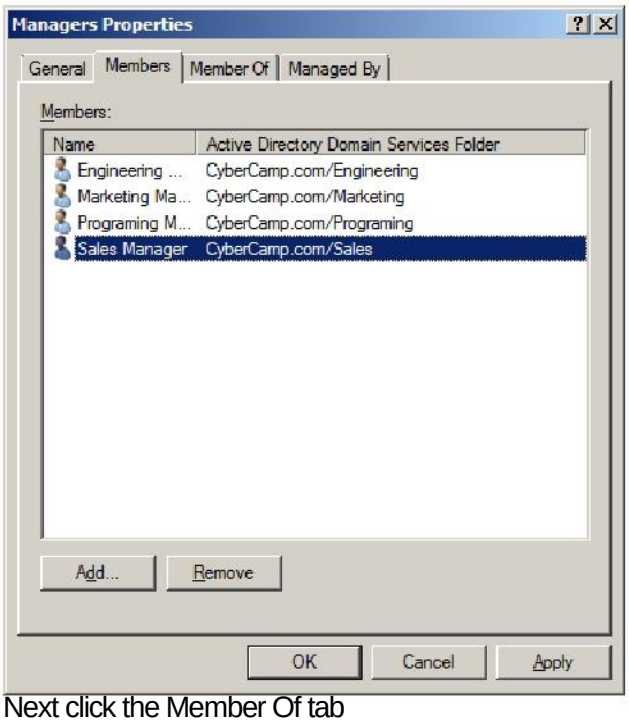


Click on Add… In the new box type the name of the manager you want to add, we will do this for Managers, Programming, Engineering, Marketing and Sales.

Type Sales Manager and click check Names



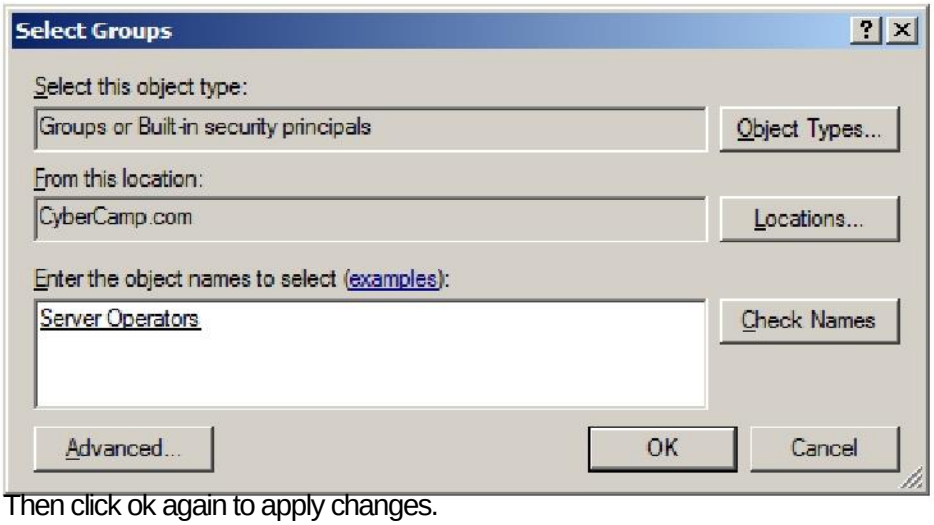
You can see that it will pick the correct manager



Next click the Member Of tab

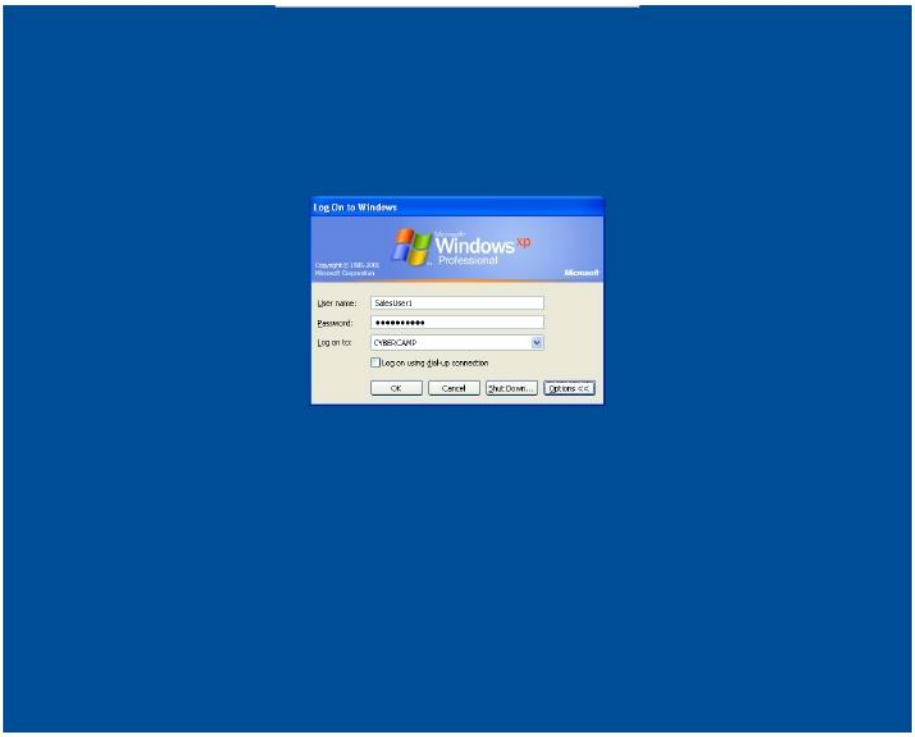
We want our managers to have the permissions needed to manage their users so lets go ahead and set them to be Server Operators.

Click Add… then they in Server operators check name and click ok

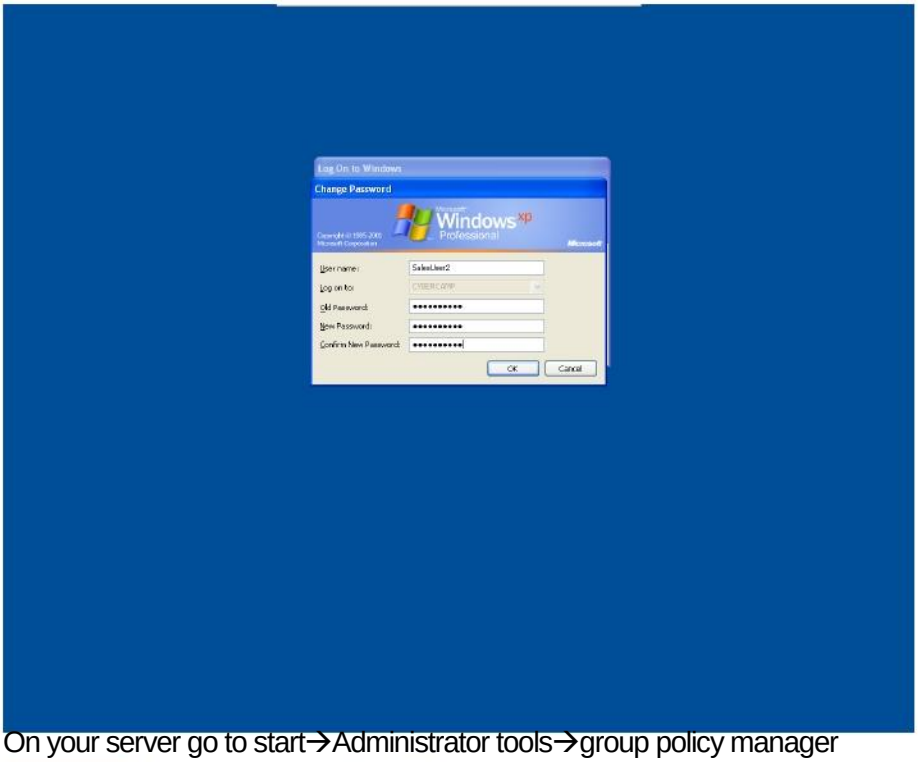


Then click ok again to apply changes.

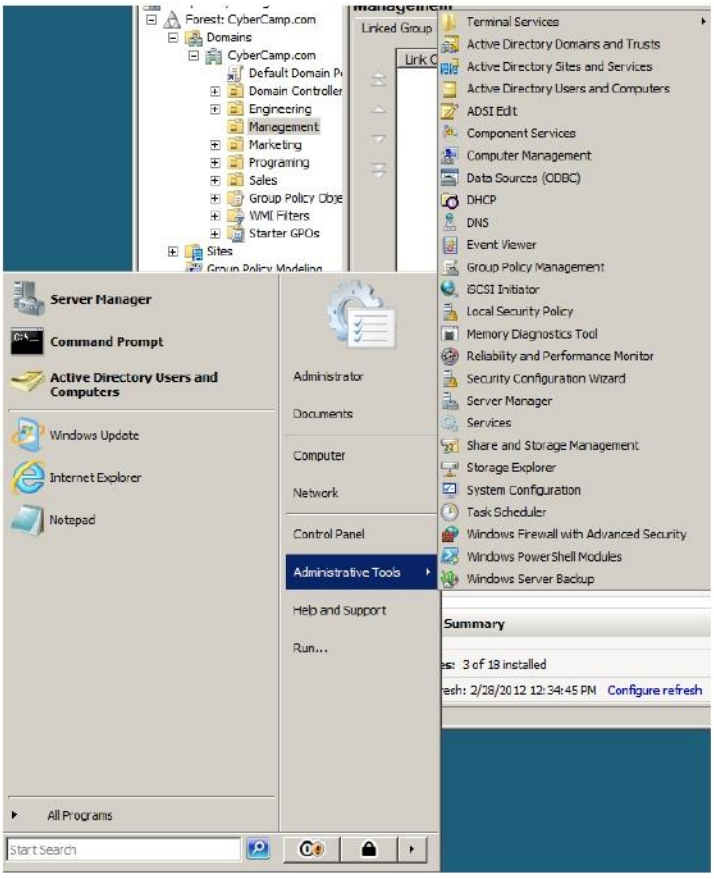
2. We have already set up a XP machine on the domain. Boot up and log into the SalesUser1 account on the xp machine through the domain to test some GPO's.



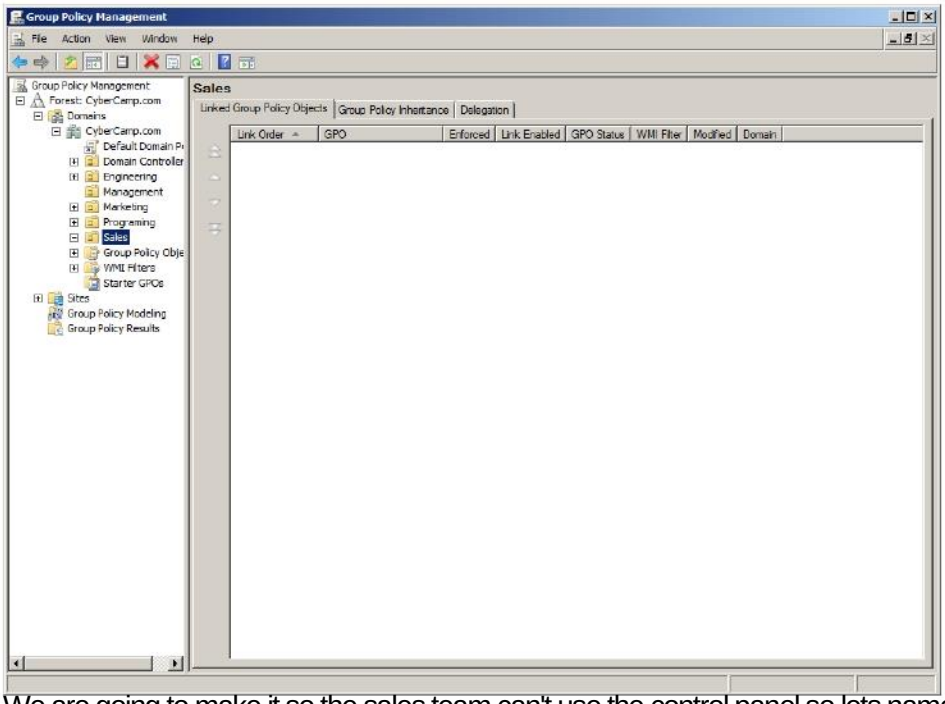
You will be prompted to change the password, let's use Password02



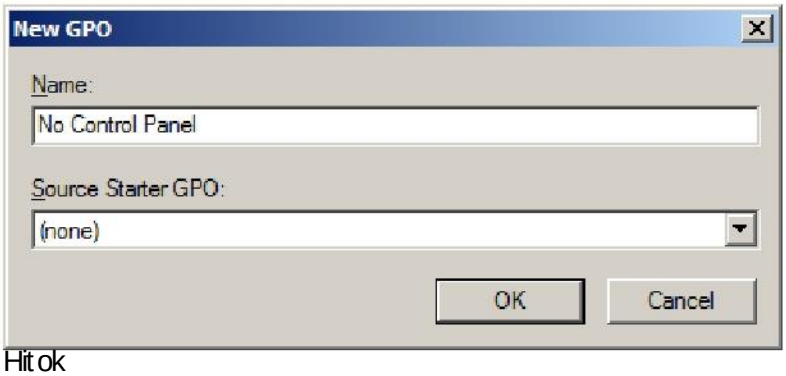
On your server go to start→Administrator tools→group policy manager



Right click on Sales and choose to create a new GPO under this domain.

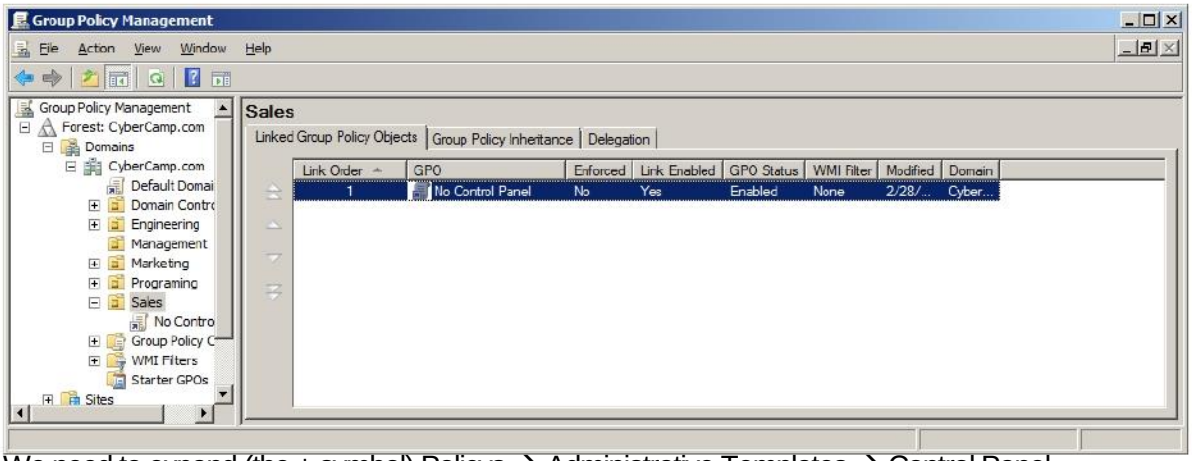


We are going to make it so the sales team can't use the control panel so lets name it No Control Panel.

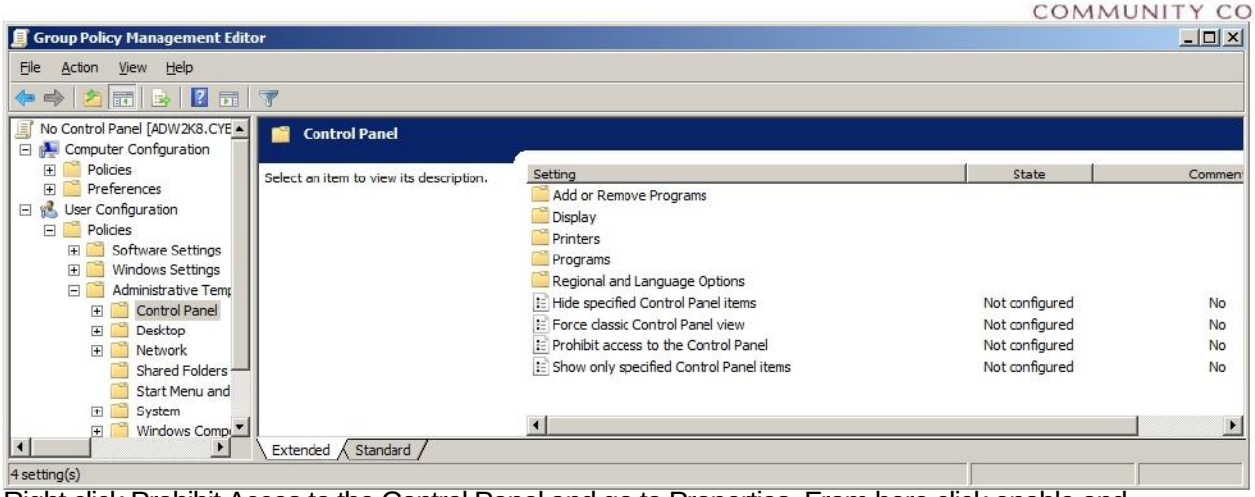


Hit ok

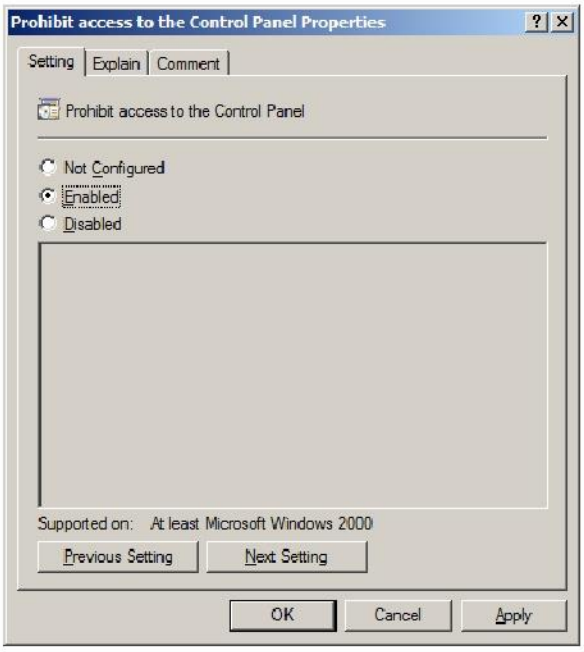
Now that the GPO has been created we can edit it to block Control Panel, right click → edit



We need to expand (the + symbol) Policys → Administrative Templates → Control Panel



Right click Prohibit Acces to the Control Panel and go to Properties. From here click enable and ok.



Now go back to our xp machine and you can see Control panel in the start menu, should be able to use it. This is because your group policies need updated so go to start run and type cmd. When the command prompt opens type cd c:\ gpupdate /force.
This updates the group policies so the control panel is restricted when you click on it.

Partial support for this work was provided by the National Science Foundation's Advanced Technological Education (ATE) program under Award No. 1104192. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.