

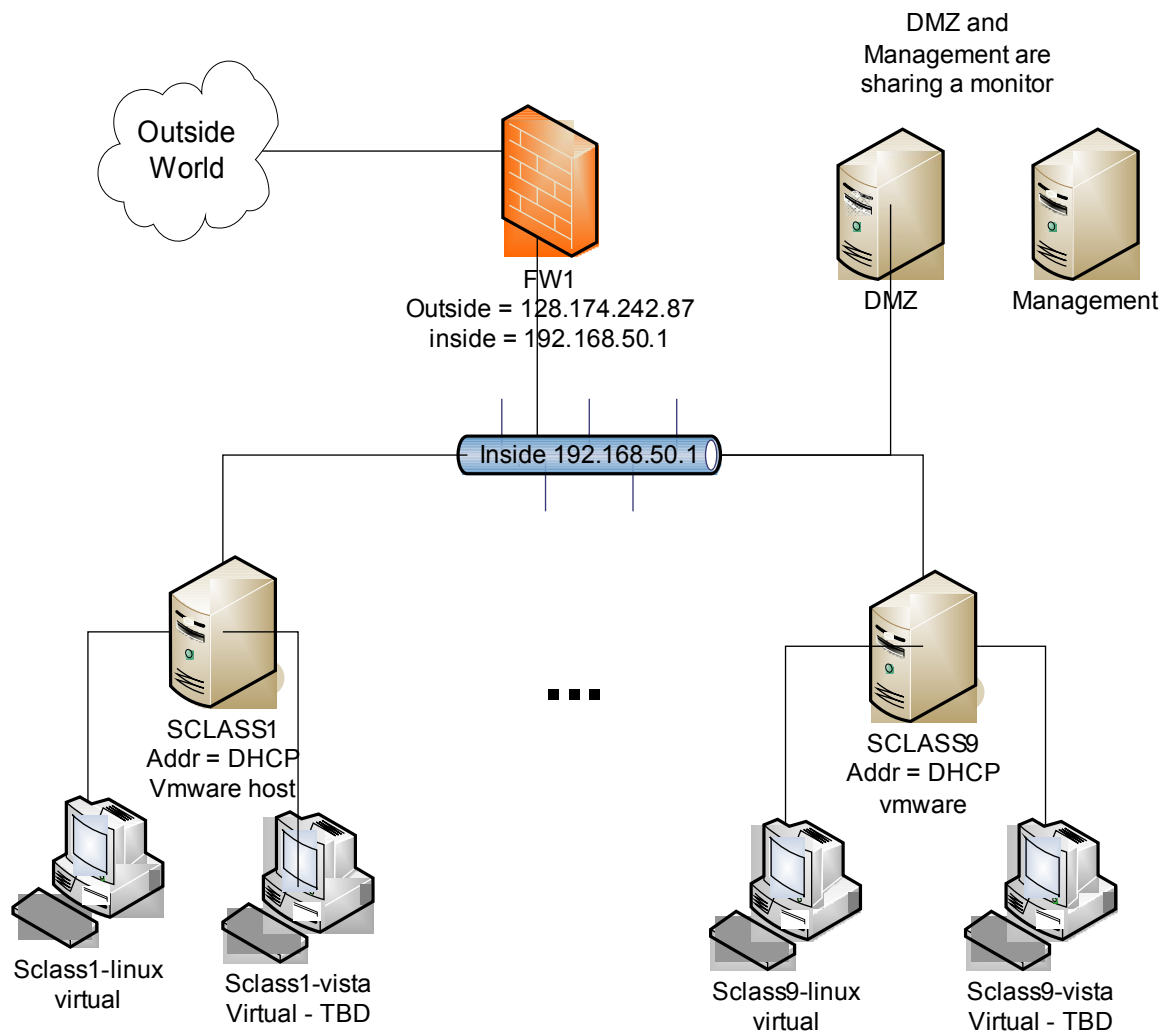
# Overview of Cyber Security Laboratory

cs498sh  
Spring 2008

The laboratory for the Cyber Security course is in 0222 Siebel Center. This room is shared with several other classes. The machines associated with the security class are on the right rear quarter as you enter the room.

## Initial machine configuration

The diagram below shows the initial logical configuration of the machines.



The lab has 10 new dell systems. Each dell computer has Fedora Core 8 (FC8) and vmware server installed. The host machine is named sclassX (where X is a value between 1 and 10). There is currently one FC8 guest OS installed on each system with the name sclassX-linux. There will eventually be vista guest OS's with the name sclassX-vista. Currently the host and the guest OS's are using DHCP to dynamically get addresses.

This is the first year, we're using vmware. In previous years we have dual booted the machines. Hopefully, Vmware gives us more options and a friendlier environment, but it will be a learning curve for me anyway. Vmware should also make it easier to set up the lab with consistent images, and perhaps give you personalized images for your assignments.

The machines use DHCP to retrieve their IP addresses and DNS information from FW 1, a PIX firewall. The firewall enables connections initiated from the lab to the outside world, but no connections initiated from the outside world in. The connections between the machines, the firewall, and the outside world are made through two VLAN's implemented on the 24 port switch.

**Note:** The firewall is not configured to allow ping replies to return. Therefore, you cannot use ping to test for connectivity to the outside world. Instead try accessing a web page through a browser or wget, or try to access a machine using ssh/putty.

There are two older machines on a desk next to the network rack (DMZ and management). The Management machine is used to display the console to access the networking equipment (more on that later). DMZ may be used in later experiments for shared web server or tftp server space.

## Users

On all systems, the password for the root or the administrative user is *class-test*. The following set of users will be installed on all guest OS.

- Alice (also installed on the host OS)
- Bob
- Carol
- Dave
- Ellen
- Gus

The password for each user is <username>-test, e.g. alice-test for alice.

## Determining Addresses on Windows

If you bring up a command window (i.e. run the “cmd” command), you can invoke “ipconfig” which will show the IP address currently assigned to your machine’s interface. “ipconfig /renew” will try the dhcp request again. “ipconfig /all” will show additional address details like DNS addresses.

## Determining Addresses on Linux

From a terminal window, you can use the “ifconfig” command to see all the addresses associated with the interfaces. This is in the /sbin directory (in case it is not on your path). You can call “ifdown eth0” and “ifup eth0” to retrigger the DHCP request. Or you can call “dhclient” to restart the address negotiation.

## Linux Installed Software

The developer environment and vi are installed. Standard network client applications like firefox and ssh are also installed. Feel free to use yum to install other application on the systems. Contact me if there are other applications you would like installed on the guest OS's.

## Vmware

Each of the Dells is running vmware server 1.0.4. From the host operating system, invoke “vmware” to start the vmware management console. From here you can start and stop guest operating systems.

Each guest operating system can be run at full screen size. Hit ctl-alt to bring the cursor back from the guest OS to the host OS. If the guest OS is running at full screen, it can be easy to assume it is the host OS. Look at the machine name. If the name is of the form sclass<x>-<os>, it is a guest OS. Hit ctl-alt to return to the host OS.

## Turning off security

In general, the machines in the lab are not configured for security as they would be in the real work, e.g., you really shouldn't share the same simple administrative password everywhere. For much of our work, we will disabling two other FC8 security features: host firewall and SELinux.

The host firewall may complicate our network experiments. To turn off the FC8 firwall:

- “/sbin/chkconfig iptables off” - This causes the firewall to not start on next reboot.
- “/sbin/service iptables stop” - This turns off the firewall immediately.

Vmware doesn't play nice with SELinux, so it is turned off on the host systems. It may also impede some of our experiments on the guest OS. SELinux can run in enforcing (checks and prevents access), permissive (checks but does not prevent access) and disabled (does nothing) modes. I have been setting systems into permissive mode. To make SELinux permissive.

- “setenforce 0” - This immediately stops SELinux from enforcing.
- Edit /etc/selinux/config and change the enforcing to permissive so SELinux operates in permissive mode on reboot.