NYU-Poly VLAB Introduction
LAB 0

1. Overview

The purpose of this lab is to familiarize yourself with the operations and access to the NYU-Poly Virtual Information Technology and Assurance Lab (VITAL). VITAL makes use of Virtual Machines (VMs) within a closed networking environment that provides hands-on access to a diverse blend of operating systems (OS) and IT/IA tools. The VMs provide an isolated instance of separate OS running on shared hardware platform. You can find more information about the virtualization technology used in VITAL at http://www.xen.org.

All access to VITAL is done via a web browser. VITAL is designed to work with a wide range of browsers **(Firefox 3+, IE8, Safari 4)** under a variety of OS (BSD, Linux, Windows, Macintosh). You must have an updated version of the Java Plugin for your browser installed and Enable Java Applets to allow access from https://vital.poly.edu. Nowadays web browsers come with recent java plugin enabled with them. If not please download the latest version of the Java Plugin and have it installed for your browser. In most standard configuration, you will be prompted to allow access upon first visit to the website. If you are not prompted, consult your browser's manual for help.

If at any time you have questions, or problems, feel free to email vital@isis.poly.edu.

1.1. Registration

In order to access VITAL you need the course number and registration code provided by your instructor. Once you have been given the registration code, you can register to get VITAL login ID at the following URL:

https://vital.poly.edu/interim/registration.php

When you have finished submitting your information, you will be emailed your login and password information.

1.2. Login

The URL to login is:

https://vital.poly.edu/interim/

Once you are logged in with the UID/PWD emailed to you from the registration process, you will see the main page that displays all the systems assigned to you, and basic network information. The main page will look as below:

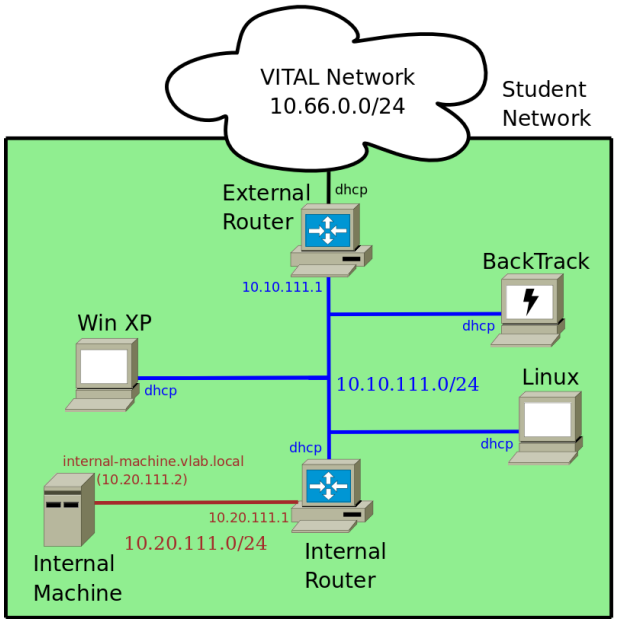
2. Using the VM

Using the VM is similar to a regular desktop or laptop computer with a few important differences. First, since your VM is run in a shared environment, you should be mindful of doing things that hog the CPU or saturate the network. Second, you do not have direct access to your VM. Access to your VM is managed through a remote keyboard/video/mouse sharing protocol called VNC. This allows the VM to run on a remote system, but provides the functionality of being connected directly to the machine. The VNC connection is handled by a Java Applet which is loaded automatically when you log into the VITAL website. You can find out more information about VNC from:

http://en.wikipedia.org/wiki/Virtual_Network_Computing.

2.1. VM and Network Description

Each student is assigned six VMs and two dedicated network segments. This configuration will be used throughout the class, although not all VMs will be used for all labs. Below is the network map of the various systems and how they are connected:



Here is a brief description of the VMs and their functions:

- External Router (rtr##) – uid/pwd: root/badpasswordExternal router needed to access network resources not on the student network (ie, other VITAL servers). This machine also provides DHCP and DNS for the student network and should be started first if networking is needed on the student network.

- Internal Router (int-rtr##) – uid/pwd: root/badpassword
  Internal router needed to access the Internal Machine to/from the student network.

- Internal Machine (int-lin##) – uid/pwd: root/badpassword
  Internal machine running SSH, HTTP, and Telnet services. This machine is behind the Internal Router (int-rtrXX) and cannot access the network unless that machine is also started.

- BackTrack (bt5_##) – uid/pwd: root/toor
  BackTrack is a Linux-based penetration testing platform that aids security professionals in the ability to perform assessments in a purely native environment dedicated to hacking. For more information, visit http://www.backtrack-linux.org.

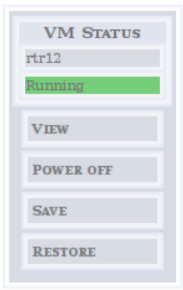
- Linux (lin##) – uid/pwd: student/badpassword
  Basic Linux machine with compiler (gcc) and other tools installed for class. The root password is also badpassword

- Win XP (xp##) – uid/pwd: poly/[BLANK PASSWORD]
  Basic Windows XP machine with various applications installed for class.

2.2. Controlling the VM

Control is broken down into two pages: The main page, and the individual VM control page. The main page displays the entire student VMs, and indicates that power-on status of all the VM.

VM Powered Off



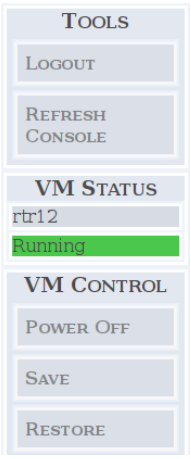
VM Powered On

For any of the VMs displayed on the main page, clicking on one of the four label buttons (View, Power On/Off, Save, Restore) will open a new separate browser tab with the individual control page for that VM. The purpose of the four label buttons is as follows:

- View – Open individual control page. If the VM is in a Powered-on, this will also launch the VNC applet from the control page.
- Power On/Off – Toggle the power-on status.

- **Save** – One of the key virtualization features is the able to save the state of the running machine. This is similar to suspending a laptop, but instead of shutting down, the machine continues to run. Then, at any point in the future you can choose to restore to that previous saved state. Any changes the to system (files, running processing, memory state, etc.) done after that save will be reverted to the previous state.
- **Restore** – This will restore the running state of your VM to the last Saved state if one exists. Please note that this will completely revert everything on the VM (files, running processes, memory state, etc.) and ALL CHANGES SINCE THE LAST VM SAVE WILL BE LOST.

The individual VM control pages differ only slightly from the main page aside from only listing one VM:



Individual VM Control Page

The Refresh Console label button under the "Tools" section allows you to refresh the VNC session if the window was closed, or is not responsive.

The other label buttons (Power On/Off, Save, Restore) behave the same as described above for the main page.

2.2.1. Starting Up a VM

In order to start up a VM click on the Power on label for the VM from either the main page, or the individual VM control page.

Please note, if your machine is left idle for more than 2 hours, it will be automatically shutdown. Automatic shutdown does not check for open files or saved work. An automatic shutdown may corrupt open files and/or system configuration settings that could result in lost work and/or a non-functioning VM. Make sure you manually shutdown your systems when not in use to avoid possible lost work.

2.2.2. Stopping a VM

Stopping your VM is a little different from a regular application because of the VNC session you use to control your machine. It is important to note that closing the web browser, or VNC console, will NOT shutdown the VM. This will only close the VNC session, while the VM continues to run on the remote server. This can be a helpful feature if you are moving your work

to a different computer, or your network connection gets dropped for some reason. However, it is not same as shutting down a VM.

Properly shutting down your VM requires two steps: 1) Stop the VM from the OS 2) Stop the VM from the VM control page.

To stop the VM from the OS, you must manually shutdown the VM using the appropriate method for whichever OS you wish to stop. Briefly, for the two OS used in VITAL, you can shutdown the VM as follows:

- Windows XP – From the Start menu, click "Turn Off Computer". A window will pop up, select "Turn Off". Once the mouse stop responding, the OS is shutdown.
- Linux – This method applies to all the other machine in VITAL (BackTrack, Internal and External Routers, as well as the machine labeled Linux). From the console, or command- line, type "halt". When the message "Will now halt." Is displayed, the OS is shutdown.

3. Common Problems

3.1. VNC console is frozen or non-responsive

If your VNC console is non-responsive, close the windows, and click "Refresh Console" from the VM control page. If the problem persists, you may need to Power-off and Power-on the VM from the VM control page. If this happens frequently, please contact the administrator (vital@isis.poly.edu)

3.2. VNC console reports a network error

Power-off and Power-on the VM from the VM control page. If this happens frequently, please contact the administrator (vital@isis.poly.edu)

3.3. Browser Crashes when opening VMs

Upgrade to the latest version of Java 1.6 Plugin for your browser.

EXERCISE 1: Start and Stop a Linux and Windows Machine

Start and stop the Linux and Windows XP machine. Make sure you understand the difference between closing the VNC session and shutting down the machine.

Windows

Start up the Windows XP machine and begin a game of Minesweeper. Note your time and close the browser completely. Then, relogin to VITAL and re-establish your VNC session. Verify your time has increased (and finish your game using this hint: http://www.tunexp.com/tips/ work_with_multimedia/how_to_cheat_at_minesweeper/). You may now shutdown the VM properly.

Linux

Start up your Linux machine. Login (uid/pwd: root/badpassword), and type "time cat" at the command line. Close the browser completely. Then, relogin to VITAL and re-establish your VNC session. Now, press the CTRL and 'c' keys at the same time to stop the process. The "real" time should display the amount of time it took you to relogin. You may now shutdown the VM properly.

EXERCISE 2: Learn Basic OS Commands

If you are unfamiliar with Linux, here are a few tutorials to review:

http://www.ee.surrey.ac.uk/Teaching/Unix/
http://www.linux.org/lessons/beginner/toc.html
http://tldp.org/LDP/gs/node5.html

You can also find out about a specific command by typing, "man COMMAND NAME" from the command prompt.

You will also have to be comfortable with Windows XP including networking. If you are not already, review the following:

http://www.baycongroup.com/windows_xp/index.htm
http://www.computerhope.com/overview.htm
http://www.networktutorials.info/windows_networking.html

EXERCISE 3: Text Editor

For Windows, I will assume everyone already knows how to use Notepad and/or Wordpad. If not, now is the time to figure them out.

For Linux, if you are already familiar with the vi, or nano, text editors, you can skip this exercise. If not, I recommend nano and reading this tutorial: http://www.debianadmin.com/nano-editor-tutorials.html.

EXERCISE 4: Upload/Download File to/from VM

Since VITAL is a closed network environment, you will not be able to upload/download files to/from your VM. In order to transfer files, you must first transfer the file to the SFTP server. Your SFTP account information is identical to your student account that was provided in the registration email.

For this exercise, power up your External Router, login and create a small text file. Now use the 'sftp' command to transfer the file up to the SFTP server. Next, download the file from the SFTP server to the Windows XP machine using the PUTTY SFTP client on the desktop. Note, the External Router will need to be powered on for the Windows XP machine to access the network properly. Once the file has been downloaded to the Windows XP machine, modify the file in some small way. Afterwards, upload the file back to the SFTP, and download the file to your PC. If you do not already have a SFTP client, I recommend Filezilla (http://filezilla-project.org/).

EXERCISE 5: Screenshots

Your assignments will often require you to submit some screen output from your VM. For this assignment, simply show that you can take a screen shot from your PC to include two VMs that have been started.