NYU-Poly VLAB Introduction

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 uses HTML5 and WebSockets so it will work with all the latest browsers. 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 a VITAL login ID at the following URL:

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

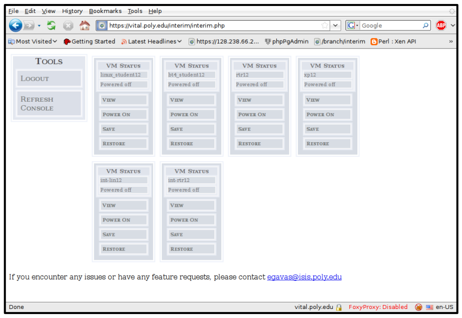
When you have finished submitting your information, you will be emailed your login and password information.

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:



VM Status
linux_student12
Powered off

VM Status
bt4_student12
Powered off

VM Status
rtr12
Powered off

VM Status
xp12
Powered off

VM Status
int-lin12
Powered off

VM Status
int-rtr12
Powered off

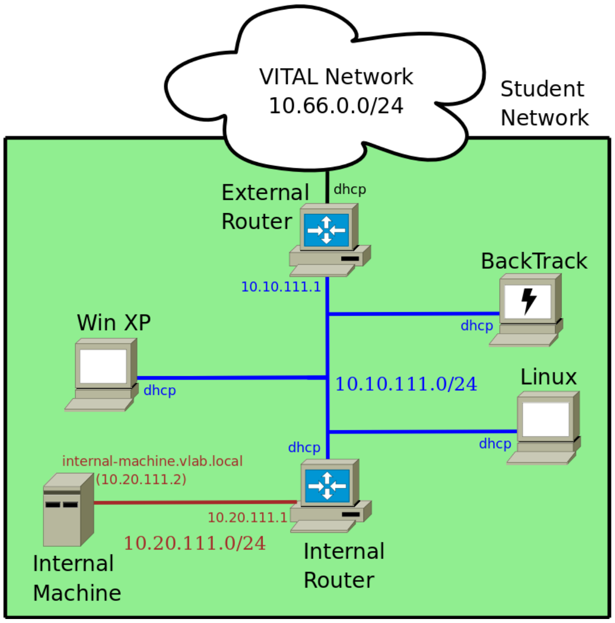
If you encounter any issues or have any feature requests, please contact egavas@isis.poly.edu

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 the VLAB web interface. This allows the VM to run on a remote system, but provides the functionality of being connected directly to the machine.

2.1 VM and Network Description

Each student is assigned seven 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:

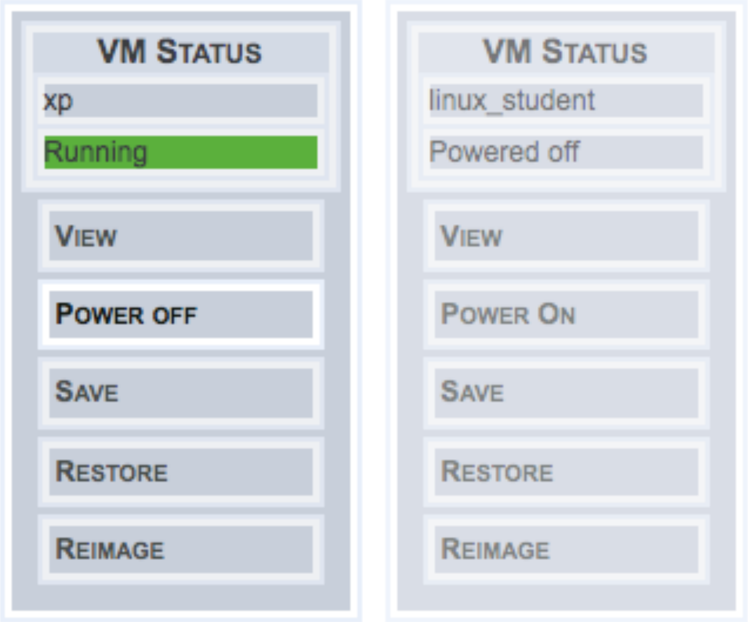
- External Router (rtr) – uid/pwd: root/badpassword
  External router needed to access network resources not on the student network (ie, other VITAL servers). This machine also provides DHCP and DNS for the student network and should be started first if networking is needed on the student network.
- 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-rtr) 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 (linux_student) – 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.
- Damn Vulnerable Linux (dvl) – uid/pwd: root/toor
  DVL is a linux distro that was intentionally made to have many exploitable vulnerabilities. The distro includes exercises, tutorials, and tools preinstalled.

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.



Left VM is Powered On, while Right VM is Powered Off

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.
- 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.
- Reimage – This will bring the VM back to the original state. This feature allows you freely experiment within VLAB without concern for breaking the machine. This is especially useful on the WindowsXP machine after an exploit which usually makes it somewhat unstable. ALL CHANGES WILL BE LOST.

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 session you use to control your machine. It is important to note that closing the web browser will NOT shutdown the VM. The VM will continue 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.

2.3 VM Startup Order

Since the routers provide routing and DHCP services in VLAB, the VMs should be started in the following order:

1. External Router (rtr) – to provide routing to 10.10.111.0/24 network
2. Internal Router (int-rtr) – to provide routing to the 10.20.111.0/24 network
3. Any other VM

3 Common Problems

3.1 Networking issues such as unable to ping

Check to see if the two routers (rtr and int-rtr) are running. They may have been automatically shut off due to being idle. For any other issues, please contact the administrator (vital@isis.poly.edu)

4 Exercises

The following exercises will help to familiarize yourself with VLAB.

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 web page 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 connection to the Windows XP machine. 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: student/badpassword), and type ”time cat” at the command line. Close the browser completely. Then, relogin to VITAL and re-establish your connection. 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, You should know (or learn) how to use Notepad and/or Wordpad.

For Linux, You should know (or learn) nano or vim. If not read 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. The SFTP server has the same IP address that's accessible from both VLAB and from the Internet. Your SFTP account information is identical to your VLAB student account that was provided in the registration email.

1. Create a small text file on your local PC.
2. From your local PC, login into the SFTP server using putty/Window or sftp/Linux and transfer the file up to the SFTP server.
3. Login to VLAB and power up your External Router.
4. From your VLAB Windows XP VM, download the file from the SFTP server using the PUTTY SFTP client on the desktop.
5. Once the file has been downloaded modify the file in some small way. Upload the file back to the SFTP, and download the file to your local PC.

EXERCISE 5: Screenshots

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