ABSTRACT

One of the difficult things in teaching Information Technology classes online is transforming physical lab classrooms into online labs that offer equivalent learning environments. This is even more difficult in presenting wireless labs that students can use via distance. This paper outlines a reliable and relatively inexpensive means for providing remote access to a virtual wireless lab.

STUDENT LAB SOLUTIONS

There are a variety of technologies that can be used for student lab configurations ranging from network boot prom PCs in the early 1990s to fully locked down machines in Active Directory. With all of these solutions, there are two problems, experimentation and remote access. The first problem is due to the fact that almost all student computing labs are not laboratories. They are production environments that are locked down. They are locked down because students will go in there and mess things up. To create a true student learning environment, students need to admin access to change things. Sometimes these changes makes the workstation unusable. While this is bad for a lab, it is needed for a true visceral learning experience.

The second problem is that the lab is only available for limited hours. For non-traditional students that are on campus just for class and distant learners, the idea of coming to the lab is not feasible. A remote solution that was used a lot in the late 1990’s and into the early part of this decade was Citrix. Citrix remote desktop allowed the use of application publishing and remote mapping of printers. The downside was that there was usually one or two servers that had to run all applications and application compatibility and setup were often issues, not to mention costs.

Wireless Laptop Labs

In 2002, the Department of Management at University of New Orleans purchased 40 wireless laptops for use in IT classes. One of the requirements for the project was that students have full control of the laptops and be able to install applications and make changes to complete IT assignments. This requirement arose because it was found that locked down Windows PCs were so restrictive that students could not complete in class assignments. To support these goals, Powerquest was used to reimage the PCs from the local hard drive. This meant that if anyone had a problem with a PC, they could choose the second option in the boot menu and in 15 minutes the PC was restored. Any changes, deletions, viruses, worms, new applications, or P2P sharing applications and media files were not restored. While this provided a means for
experiential learning and wireless labs, it was very limited to a time when laptops could be checked in and out while on campus.

**Virtual Machines**

In the last five years, Virtualization and virtual servers have revolutionized the data center. Virtual Machines have really gained acceptance in the data center as well as desktop replacements. This lead to the idea of a truly multi-platform remote and local access lab environment.

In 2007, I began building our virtual laboratory at the University of Dallas called Minerals. Minerals is a collection of workstations and servers running VMware products to host a variety of scenarios and solutions. They also serve as a controlled test facility for experimentation with new and emerging technologies. As part of the visceral learning environments we have moved from static simulations on DVDs to engaging live scenarios that students can collaborate on and be part of a real investigation. An example of this is our Information Security Risk Mitigation class where students are divided into 3 person teams and asked to examine an environment. Whether the class meets on campus or online, the entire lab is provided online and over the Internet via an SSL VPN gateway. Each team has its own tools server along with routed private networks where the fictitious case’s servers and personal computers reside and can work on the lab all hours of the day and night.

The whole environment is firewalled from the campus network and subneted from the other teams. Realizing that giving students admin rights on the servers, they have the ability to mess things up. This is not a problem as each server is a VMware server instance with snapshots. In the event of a problem, the server or workstation is rolled back to a known good state.

**Hypervisor**

In 2008, VMware made their ESXi hypervisor free. Before this, the only VMware hypervisor (ESX) was a paid product. A hypervisor runs directly on the hardware without the use of an operating system. The advantages to a hypervisor is that is allows for more resources to be devoted to the guest OS and reduced the attack profile of the host. Management of the ESXi environment can be done on an individual server basis through the VMware Infrastructure client or over a group of hosts using VMware’s Vsphere. The advantages of managing in a group are that guest OSs can be moved from one host to another.

**Virtual Networks**

It is important to realize that Virtualization is more than just virtual servers. It can also be virtual networks. In the Risk Mitigation example earlier, each team has a variety of networks to investigate. Some of these networks are physical with network cabling and switches and some are virtual. The virtual networks provide and easy a free means to subnet student teams, separate production and test systems and enforce security without the problems of cabling and switches. In the class example, each team has a virtual network for all of their penetration testing and foot
printing. The network can be setup anywhere from 10Mb to 1Gb. Having separate subnets for each group to work on also sets the scopes and boundary for the exercise. The campus DNS servers should not be a target for port scanning. By giving group 1 the 172.29.1.0 /24 network for example makes it very clear what is and is not part of the exercise.

**Wireless Remote Lab Access Solution**

To give a true wireless experience to students, they need to connect to a machine that has wireless capabilities. One solution would be to use the previous laptop example and setup laptops for students to remote into. The problem here is maintaining the physical laptops in terms of space, security, and management. If a student messes up the configuration, locks it up, or make it unreachable, someone must physically go visit the PC.

VMware on a server, workstation, and/or hypervisor would be an easy way to extend the lab. The problem is that VMware server, workstation and the ESXi hypervisor virtualizes NICs including wireless devices which make it very stable for the guest OS, but does not allow the user to run wireless tools such as Netstumbler. However, there is a work around that can be employed. VMware workstation allows the administrator to “give” USB devices such as printers, and jump drives to the guest OS. It also allows you to give USB Wireless 802.11 variety NICs to the guest OS natively. This allows Windows to see the device as hardware and install the appropriate drivers.

**Steps for Creating Virtualized Wireless**

In this particular lab, I began with a Pentium 4 PC with 4 GB of RAM and installed Windows XP SP3 along with patches and antivirus. VMware workstation was then installed and configured. Once VMware was running, a VMware guest install of Windows XP SP3 was installed and patches along with AV. The next step is to plug in the three Linksys USB WIFI NICs. The default action for the Windows host to want to discover these devices and install drivers. When this occurs, tell windows to ignore these devices and not to install drivers. Once you give the USB NIC to the guest OS Windows will auto discover these devices and ask for drivers. Install the drivers and configure for whatever default WIFI network you want to connect to. Once this configuration was complete, the workstation was shutdown and cloned three times, leaving the original image unaltered.

The wireless guests are then able to connect to a WIFI AP to run their scans. Without the ability to shield wireless, the groups see each others WLANs as well as any other APs in range. To keep the model simple, the physical PC had 3 NICs in it. One for the lab network, and one for each private network to the AP. Because students are encouraged to reconfigure the subnet on the router, DHCP is configured for these interfaces. Virtual NICs connected to the lab network allow students to terminal serve in and remote the XPSP3 guests. This topology is shown in figure 1.
Figure 1: WIFI LAN Topology

Equipment and Software Needed

To implement this lab, the following hardware, software and solutions were used. SSL-VPN gateways allowed remote access from off campus. Computer hardware included 1 PC with 3 physical NICs, 2 wireless USB NICs, 2 SOHO FW, SOHO router / AP, and some cabling. Software included VMware workstation, Windows XP, and the WIFI USB NIC drivers.
LESSONS LEARNED

Although 3 identical WLAN USB NICs were purchased at a local electronics supplier at the same time and were the same model, two different hardware versions meant that a standard image could not be used across all three Windows XP SP3 guests. So insuring that having the same hardware will make administration easier. The second lesson was that the PCs needed to have two networks, a wired connection to terminal serve into and a WIFI network to probe. It is possible to have one network connection on WIFI, however if the student connects to another WIFI network, they inadvertently sever their connection.

If you don’t break it then you did not do it right…

If students are really trying new things and running hack tools, they are going to knock things down. An advantage to a virtual environment is snapshotting and cloning. VM in all three platforms, workstation, server and hypervisor allow for the snapshotting of the guest. Snapshots are point in time restores that rollback changes in minutes. Cloning allows you to make a copy of the guest for future deployment. Telling students that if they don’t break something, they are not trying hard enough changes the learning paradigm. It gives permission to challenge, try, explore and learn.

CONCLUSION

Creating virtual labs is an incredibly efficient way to manage your environment and provide students a means to really have a true visceral learning experience. With a little experimentation and imagination, the virtualization tools from the server rooms can be leveraged into the online classroom to provide true anywhere anytime learning environments.