CREATING VISCERAL CYBERSECURITY LEARNING LABS

Brett J. L. Landry
College of Business, University of Dallas
1845 East Northgate Drive, Irving, TX 75062
blandry@udallas.edu 972-636-8633

ABSTRACT

This paper examines a highly successful and easy to support visceral learning environment for teaching cybersecurity and technology classes. The Minerals Lab experience at the University of Dallas, has been successful mainly because it relies on sound and time tested cybersecurity principles while including secure remote access. This paper outlines the need for visceral learning environments, the transition to mobile learning labs, and the Minerals approach. While we run a number of classes and scenarios in the labs, the focus here will be on the use of insider threats to illustrate the concepts in the risk mitigation class.

INTRODUCTION

In working with computing labs over the last 20 years in both commercial and university environments, I have tried a variety of lab scenarios and setups to provide students a robust visceral learning environment that is secure and reliable. Over the years this has included boot prom PCs, locked down labs, mobile laptop carts, reimaging solutions, Citrix, and now VMware solutions. Until now there have been always been caveats with these approaches, because they did not allow student to run multiple Operating Systems (OS), be remote users, or experiment. This paper outlines a solution that supports local and remote users, multiple platforms, and various levels of control. However in discussing virtual lab environments with colleagues at other schools and conferences such as DSI, it is clear that a number of schools have launched VMware initiatives that have not fit the need of the class. They have in many cases resorted to still mailing out DVDs with hacking tools, having limited computing platforms, or somehow missed how to put it all together. It is hard to discuss university security labs today without mentioning virtualization. Over the last few years, server virtualization has led to consolidation using less resources and greater flexibility and administration. However, this is not the only type of virtualization currently in use, Virtual Machines (VM) can run on top of a server or guest operating system or virtual desktops can be deployed as thin clients. The most common virtualization scheme today is using hypervisors such as ESX or ESXi from VMware that allow the greatest flexibility and scalability of all the VM options.

This paper will outline the results at the University of Dallasô (UD) efforts to build an easy to maintain, scalable, and inexpensive virtual lab environment that supports distance learners and teams to actually scan, enumerate and attack a network in order to understand how to defend a network. The reason for this is simple, if students have never seen an internal attack, they cannot protect and defend an attack.

PC Lab Background

To understand the design behind the Minerals lab, it is important to understand the last 20 years of computing labs. The early 1990's, it was possible to build a bulletproof PC. A boot prom was installed on the Network Interface Card (NIC) that enabled the PC to boot from a read only boot image across the network. The network server contained the image and stored all user files. This environment worked for both DOS and Windows 3.X clients. Basically, the methodology was simple. A PC was powered on, and sent a request across the network requesting an image. A network file server responded with the corresponding image file and the machine booted. Since the image file was read only, a pristine, virus free client was provided each time the machine was restarted. If the machine had a hard drive for temporary storage, it was quick formatted at the next boot.

For Windows 3.X Operating Systems (OS) this meant that different drivers had to be enabled for different video cards and sounds cards. Because this was before the time of plug and play OSs, it was necessary through the use of common UNIX tools such as SED and AWK that were ported to DOS to dynamically rewrite the system.ini and win.ini files at boot up to the appropriate configurations based on the MAC address for that station. The hard drive also allowed students some flexibility to make changes to their local configuration, complete assignments, and experiment with the PC. The good news was that any changes made by the user were temporary and a reboot reset all configuration changes. This gave students the ability to truly experiment and learn by doing, knowing that if they screwed up, one reboot and all was fixed again.

Although hardware was not as dependable in the early 1990s as it is today, maintaining hardware in this timeframe was much easier. The reason was simple; if a PC had a problem, the lab operator would reboot the PC. If the PC received network boot prom issues, it was the NIC or the network media. If the image loaded and there was a problem, it was a hardware issue, because the software was common to all PCs, and could not be changed by the end user. When the PC needed to be replaced, a tech would disconnect the old PC, add the new one to the corresponding tables, plug a new one in and everything worked. Literally a five minute fix and the hardware problem could be repaired off site offering minimum downtime to the end user. It is this kind of support environment that I wanted to return to with our Minerals lab at UD.

Environmental Changes

However, this environment changed in 1995 with the advent of Windows 95, the rapid adoption of the World Wide Web as well as increased home Internet Access. Windows 95 and all subsequent versions of Windows required a full install and did not work in a boot prom environment. Having a full install of Windows locally pushed administrators to centralized lab management strategies such as SMS and Zenworks and imaging strategies such as Ghost and Powerquest. However these were labor intensive and reimaging a PC meant revisiting it or determining a scheduled downtime for scripted reimaging. Reimaging is the process of taking a saved copy of the hard drive and restoring the continents. It can be considered a point in time backup of the OS, applications, registry, and files. The problem is that reimaging is often not granular enough because people to do not create images often enough because both the creation time and the restore times take too long. However reimaging or a complete reinstall is the only

way for a physical machine to be restored to a truly clean and known state. Working in commercial labs during the late 1990ôs, I often spent more time waiting on reimaging and restores then actual testing.

However, moving to a restricted environment meant that students no longer had a true experimental environment; they now had a productions locked scenario, where they could make very few changes, if any at all. The support for locked down labs came to a head in 2003 when university networks around the country were inoperable due to attacks from a new breed of viruses and worms. The fact that universities were attacked was not new; it was the speed and ferociousness with which it happened that was amazing. On infected networks, an unprotected PC could be attacked and compromised in as little as 30-45 seconds. The reason for the mass infection was that the majority of workstations on campuses were un-patched, did not have adequate passwords, and did not run local virus protection with current pattern files.

At the same time, users were becoming accustomed to web based accessed to resources over the Internet and did not want university labs to be any different. A solution for remote access was Citrix. Although Citrix was very limited by todayôs standards, it provided a secure place for students to run their applications 24x7, however it also did not provide experimentation.

Creating Visceral Learning Environments

However, this move to locked down production environments does not allow students the opportunity to truly experiment. To accomplish, I created the Minerals lab at UD to provide any time / anywhere access to students, have the opportunity for students to experiment, be secure from external malicious attacks as well as student led attacks coming from the inside, and be easy to maintain. The first of these, any time / anywhere computing environment is important for distance learners and local students as well. Why would local on campus students need any time access? Because those moments of ñahaò do not always occur between 7:30 A.M. and 9:00 P.M. during lab hours. If you want students to get the most of your classes, then allow them the most time to access the class labs.

Start with the End in Mind

Decide early what is needed in your lab and what roles you need to accomplish. Too often in most industry and academics, virtual servers are deployed without any real rhyme or reason. VMs are rolled out and additional VMs installed without a clear understanding to the purpose and functions needed. With this in mind, the first recommendation is to start with the end in mind. Simply put, go to the whiteboard and outline all of the functions, business needs, and security needed for the environment instead of deploying VMs and then finding out they do not fit. This concept of virtual sprawl is not limited to the academic space. When discussing virtualization at ISSA, ISACA, and IEEE meetings, a common response I hear is that VMs are not secure because servers with different security needs are on the same physical network. When one of these servers was compromised it was used as a staging ground to other servers. Another common complaint is that VMs are slow due to network contention. This vulnerability and slow performance is not due to virtualization, but sloppy network design. Not everything should be on the same network and no one single NIC can handle your entire server load.

In our lab environment, we want to support a number of functions and classes that have different needs. We support a digital forensics lab running FTK, a database class running Oracle, SQLServer and ER-Studio, student sandboxes, faculty sandboxes, and a risk mitigation class. The risk mitigation class has multiple needs with a class lab component and 4 team penetration exercises. Additionally, all of these environments must be accessed and supported fully online. To accomplish this and keep student teams doing penetration testing from disturbing the other team and other classes, each team is given its own network. This environment also supports secure not changeable production environments as well as experimental ones.

LAB COMPONENTS

While Minerals is a very robust environment, allowing remote administration and isolated sandbox and production environments, it is not very complicated. It relies on proven technology such as statically routed isolated subnets firewalled from each other and multiple NICs. The lab components will be discussed here to illustrate what is necessary to build a lab environment that supports Cybersecurity education. Minerals is composed of only four physical servers today that run dozens of VMs concurrently.

Networks, Remote Access, and Firewalls

The reality is that your campus administrators are not going to want to support an environment where hacking and students breaking things are encouraged. We originally stood up the Minerals lab firewalled from campus and then this year air gapped it from campus on its own Internet connection. Being that it is separate from campus, administration is important. With this in mind Minerals is composed of ten distinct physical subnets and multiple virtual networks. The first network you should create is your management subnet to include all of the managed devices; ILO, managed ports for the firewalls, VPN Servers, VMWare servers, and other management agents. This subnet needs to be distinct and separate from all devices so that students or other intruders cannot sabotage the lab. This allowed remote management of every device securely away from student access. We standardized on HP Proliant DL380s that support built-in standard Integrated Light Out (ILO) connectivity. ILO allows you to connect to the server even if it is off and turn it on or off as well as health checks. The second network is dedicated for iSCSI access from the servers to the SAN.

Remote access is provided by a Sonicwall SSL VPN server that allows bookmarks for lab resources and can be tailored based on Active Directory groups. In the three years, that we have utilized the Sonicwall solution, it has performed extremely well, is easy to support and works because of its clientless nature. The Sonicwall VPN is a definite recommendation for any IA lab being deployed. In fact, all users whether on campus or off utilize this connection ensuring that no direct access to the servers is possible unless explicitly defined on the firewalls.

All connections inside of the VPN are then firewalled to one of a pair of SSG5 firewalls. Two 6 port firewalls were deployed, as opposed one 12 port FW, to allow granularity of administration and flexibility. The clear text config files of the Juniper firewalls also make configuration easier than other FW solutions that do not allow editing such as the Sonicwall FW. In most modern routing environments, static routing is considered to be archaic and cumbersome. However, it

ensures that secure networks cannot find routes to unsecure networks and ensures isolation. Static routing can be a difficult process, but if you design your networks with routing in mind it can be easy. Two static route rules can support hundreds of subnets by designating a higher level subnet. For example, firewall one has a static route for 172.30.0.0 /16 which means that there can be 255 class C subnets or any combination of supernets behind that FW. Likewise, creating a rule of 172.31.0.0 /16 on firewall 2 allows access for all of those subnets. Each server has multiple NICs installed to give access to each specialized network that is connected to one of the SSG5 FWs via an unmanaged switch.

Hypervisors

In 2008, VMware made their ESXi hypervisor a free product. Before this, the ESX hypervisor 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 vsphere utilities and can be done as a VM that resides on ESXi. All four servers run ESXI version 4.1 and are connected to a NETAPP SAN from an internal flash drive.

Guest Operating Systems

One of the easiest first steps is to create a Windows Server running terminal services and allow students to connect to the server. In fact this is the first required lab exercise and starts a week before students actually need access to the lab. This allows students to make sure that their PC, browsers, and firewall restrictions allow them to connect and login and reset an AD password. For those migrating from Citrix environments this is a similar experience; there is one server that students utilize for remote access to run applications. Once this has been established, other guest OSs can be made available, knowing that basic connectivity has been established.

Snapshotting and Cloning

If students are really trying new things and running hack tools, they are going to knock things down. One of the things I tell students is that if they are not knocking things down than they are not trying hard enough. 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 OS. Snapshots are point in time restores that rollback changes in minutes. Cloning happens within vSphere and allows the administrator to make copies of an image for reuse or for backup. So if an administrator needed 5 Linux servers, they could create one server, patch, and configure it, and then clone it 5 more times leaving the original server as a master to clone from. Cloning allows you to make a copy of the guest for future deployment. Tools within the NETAPP SAN greatly accelerate the cloning process and allow one to many clones instead of the one to one native in VMware.

Migrating Existing Workstations and Servers to VMs

One of the biggest stumbling blocks to moving to VMs, is the existing servers, desktops, and laptops are in place and working. This was the case when I started the minerals lab three years ago. There were physical servers that were migrated to VMs running on VMWare server and then when VMware ESXi became a free product they were migrated to the hypervisor. VMWare provides a tool called converter that allows you to migrate a physical server or desktop to a virtual machine or from one VMware platform to another. Literally in a matter of a few hours, the whole lab was migrated from physical machines to VMs. While VMware is the market leader, they are not the only virtual environment solution. It was decided early on that the lab needed to be cross platform and support not only Windows, but Linux and other applications provided as VMware appliances. An example of this are Backtrack and SAINT that areboth provided as VMware images ready to be deployed.

Creating Student Team Networks

In creating the Minerals environment, one of the requirements was to support the risk mitigation class where students work in collaborative teams to perform enumeration and pen testing exercises against a fictional company, ACME. To do this, there are four teams assigned each to a separate network of servers, workstations, print servers, wireless access points and networks. In creating, the separate networks there are a number of ways to accomplish this. One way would be through the use of virtual networks in the VMware environment, but this would not allow for other physical devices such as WIFI and print servers. VLANs would be another way however, it could be possible that the students could in their test perform an ARP poison cache against the switch and corrupt the environment for their team and the others as well.

The solution employed for Minerals was to create 4 distinct IP subnets that are firewalled from each other with explicit ñAny / Any / Denyò rules to each other to ensure that they cannot compromise another team. To accomplish this, a Juniper SSG5 was deployed to route and firewall each subnet. Each subnet was then placed on an unmanaged 8 port 10/100 Switch again to ensure that students could not disrupt their environment. Server connectivity was accomplished with a 4 port 1GE NIC and to further isolate traffic the student VM guests were only connected to that one subnet. The solution here works well in the virtual classroom as well as in class or red / blue team exercises.

Developing Virtual Networks

It is important to realize that virtualization is more than just virtual severs. It can also be virtual networks. In the risk mitigation class 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 an easy 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 172.22.22.0 /23 network for example makes it very clear what is and is not part of the exercise.

Simple things

There are other simple things that you can do to change your environment and make it easier for you and your users in accessing multiple servers. A simple one is to set a different color desktop for each server, export that registry color key and enforce it simply in a usersô registry by importing that key in their login bat.

```
@Echo Off
Regedit /s e:\userconf\colors.reg
```

This makes it a lot easier for students to remember what system they are on as well as supporting them. This is not to say this is the only thing to do, but small support changes such as this will make it easier on a daily basis.

Things Beyond ESXi

While ESXi has provided a great environment for most things in the Minerals labs, there are some things that it cannot provide such as USB direct connectivity. Direct USB connectivity is required for license dongles for both Encase and FTK, however ESXi does not support direct USB connectivity. The solution for this was one additional stand alone server for running the license managers and connecting the dongles.

Wireless Remote Lab Access Solution

To give a true wireless experience to students, they need to connect to a machine that has wireless capabilities. VMWare on server, workstation, and ESXi, virtualizes wireless devices which make it very stable for the guest OS, but do not allow the user to run wireless tools such as Netstumbler and other tools. However, there is a work around that can be employed. VMWare ESXi now allows the administrator to ñgiveò 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 the guest OS to see the device as hardware and install the appropriate drivers.

Advantages to Virtual Labs

So in practice, solutions based on restrictive user policies alone have not eliminated the infection of individual computers with malicious code. Increasingly, viruses and worms are exploiting system level privileges to install their malware, requiring a defense in depth approach to desktop security. There is no particular way to ensure that infected PCs are really cleaned, as remnants can still exist even after the most through inspection by an experienced technician. The most that can reasonably be expected is that no obvious additions or deletions have taken place. The technician can look for unfamiliar applications, newly added local user accounts, or unusual services running in the background for example. Without an enterprise wide standard desktop

environment and a current method to authenticate that the contents of the hard drive have not been altered there is no real way to ensure that any dropped files or ñtool kitsò havenôt been left behind, leaving the system vulnerable to future attacks. With the unique requirements of academic computing environments, a standard desktop environment is unlikely at best, and with the constant stream of updates to individual software products and new virus template files constantly being delivered to anti-virus clients via the web, as well as patches and security updates for operating systems, an accurate listing of what should be on a given hard drive would be impractical if not impossible to maintain. The only way to really know that the machine has been cleaned is to wipe it clean, reimage it, snapshot it or clone it from a known good master image. In the lab scenario, here we have seen a restoring from a snaphot or a clone works every time and is fast and efficient.

Resetting for the Next Semester

One of the big challenges in any lab environment is resetting it for the following semester. In the Minerals lab, this is an easy task. The original master server is updated with the latest OS and application patches and is then snapshotted and cloned to its needed function. IP Addresses are assigned and user accounts are created, and everything is ready.

RUNNING AN INSIDER THREAT LAB

I use the example in the risk mitigation threat that you cannot be a fireman if you have never seen a fire. Fire is tricky and it does not always behave the same. It is influenced by it environment, fuel, and yes even motive. Insider threats are no different. Attackers on the inside of a network have a great advantage; they know the systems, subnets and have connectivity speeds of 100MB to 1GB. They also often today have remote access from machines that may or not may not be clean. To illustrate the concept of insider threats, in the risk mitigation class we examine and have students use a variety of tools to footprint, scan and enumerate lab systems that compromise the Acme Corporation. Acme is a fictional company that produced a unique widget that is a guarded intellectual property that competitors would like to have. Working in 3-4 person teams, students VPN to Acme and examine what is in place. The first exercise is simple run SAINT to discover devices on the local network. The purpose here is to illustrate the issues of having devices on a flat network that is not segregated by VLANs or subnets. Next, students run the tools found on the Backtrack Image to see the types of tools available in the hackers tool bag. Students are also given windows password hashes that have been gathered from computer hard drives that Acme has discarded. Using LCP, students are required to break the password that still reside on the hard drives to understand the issues with both unsalted passwords and discarded equipment.

There is a common misconception that hiding the SSID on wireless actually secures from attackers finding it and connecting to it. In the wireless labs, students connect to a virtual laptop and scan the network using Netstumbler. Netstumbler is a simple windows program that shows all the APs in the clear whether it is being broadcast or not. To further illustrate the exercise, students have to report on all APs that are found for Acme. A rogue AP is connected to an electrical timer that is operational only between the hours of 2:00 A.M. and 6:00 A.M. to illustrate that scanning must occur at all hours and not just between 8:00 A.M. and 5:00 P.M.

Now that students have found rogue APs, a flat network and a Linux machine run Backtrack 4.1 they have a secure sandbox area to use more intrusive tools such as hyrdra, nmap, and metaploit. Because each team is firewalled from each other, they cannot attack each other and their penetration attempts are limited to their subnet. When a team does break something or would like run a scenario again it easy to recreate the environment via the created snapshots.

Lessons Learned

After running Minerals for the last three years, there are some definite prescriptions and lessons learned to pass on. The first is allow adequate time for testing by the users and by yourself using a student equivalent account. This will ensure that students will not be left behind when the actual lab deliverables open. Enable through ESXi and VMware server the startup order for all VM guests. Although three 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 XPSP3 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 severed their connection.

Conclusions

This paper outlined some of the successes of the UD Minerals Lab in developing a secure environment that students can work either in a locked down mode or in an experimental basis. 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.

Creating and maintaining the lab does not have to be an involved process, but it does require a great deal of planning and forethought in terms of what your lab should and should not be. It should be noted that the Minerals lab at UD has been supported through U. S. Department of Defense Annex II grants, and partnerships with Microsoftôs MSDNAA, SAINT, and VMwareôs Academic Alliance programs.