Developing an Efficient Remote Lab Environment for Online IDS Courses[1]

Xin Tang, Kai Li

Department of Technology Systems, East Carolina University

Abstract - *In this project, a remote lab network environment was developed to support our online IDS (Intrusion Detection Systems) courses. We created the lab network with the criteria of availability, flexibility, reliability, and economy in mind. The designed lab network is shown to be a reliable working environment, and has proven to be flexible for conducting various individual as well as collaborative IDS experiments. By minimizing the hardware/software requirement on the remote side, our approach offers students great freedom in supporting various remote environment and experiment designs.*

1. Introduction

Nowadays, information security plays a critical role in computer-based information systems. According to a 2004 CSI/FBI Computer Crime and Security Survey, all investigated organizations experienced security incidents at different levels over the last year. Among countermeasures to be considered, network security training was rated as very important by seventy percent of the organizations investigated.

Widely accepted to be of paramount importance within the network security field, intrusion detection systems (IDS) look for suspicious behavior by constantly monitoring what is taking place on a system. However, IDS itself cannot ensure a secure environment. Reliable network security depends on well-educated professionals who can adapt IDS to practical network settings.

Typically, information security technology education is delivered to students through classroom learning and hands-on laboratory experiments. However, with the steady increase in Internet use in recent years, we have witnessed a rapid maturation in remote technology education. The trend toward online information security technology education is inevitable, and shows a likelihood of becoming essential.

In online technology education, significant efforts have been made to design and develop user-friendly Web-based learning environments, such as Blackboard and the virtual learning community, which mainly provide asynchronous learning activities for geographically distributed virtual classrooms.

[1] This work is supported by the online education grant from UNC system.

According to Kolb's experiential learning model, in addition to the necessary theoretical lectures and written material, effective learning should integrate hands-on experience in a laboratory environment. In [1], Crowley created a need for security-focused lab modules by incorporating Kolb's experiential learning model to assure an optimum learning experience. He stated that, in the absence of the laboratory, learning, including distance learning, of information security technology is incomplete. As a result, online experimental sessions play a critical role for students involving into distance technology programs, including those having to do with information security technology.

Many efforts have been made to develop remote lab solutions. A mobile laboratory was used in [2] for distance engineering courses. It was actually not an online laboratory solution. In their pioneering work [3], the authors propose a remotely shared laboratory, which enables sharing of laboratory data between universities using networked workstations. It aimed at developing specific control system laboratory experiments.

A Java-based interactive online laboratory was developed in [4]. The Java applet running on a student's computer collects commands and forwards them to the server in the lab to be executed. The results are sent back to student side and displayed. Students can only execute the commands that are predefined and understood by the server.

An interactive remote laboratory based on Microsoft ConferenceXP Learning Infrastructure was discussed in [5]. Authors also suggested a Web enabled remote lab in [6] that can offer students real-time collaboration during experiments. Since this system requires high bandwidth Internet access, its application is restricted to small groups of users.

Because IDS technology has a short history, IDS education, particularly its distance program, has not matured to the extent that other information security courses have. There are few IDS training classes available online, and they in general do not offer students a solution based on online hands-on experiments because of the difficulty of implementing them. Remote students are therefore required to attend on-site lab sessions. Moreover, those online IDS trainings are product-specified, which means that they are costly and very closely linked to particular system configurations. Altogether, they do not present a viable approach for general information security education.

In this project, we developed an efficient lab network to support our online IDS courses. Four major concerns were addressed with regard to the design of an efficient remote lab environment: availability, flexibility, reliability, and economy. Our approach offers remote students great flexibility in laboratory activities. Students can design and perform their own IDS experiments with a minimum of hardware/software restrictions on their computer systems.

2. IDS Lab Environment

IDS systems come with various implementation approaches that were developed for different network configurations. Host-based IDS (HIDS) resides on an individual computer and monitors computer activities for suspicious events. A typical network-based IDS (NIDS) is an

isolated distributed system. A number of sensors are located around the whole network, and they monitor the traffic of local network segments. Suspicious traffic will be forwarded to some dedicated hosts for further processing and storing. Command consoles are used to manage the whole IDS hardware and software systems. All NIDS elements function in a collaborative manner.

Because they lack necessary network components, remote students' computers are usually incapable of running experiments such as NIDS. Therefore, it is far from sufficient to ask students to practice on their own computers. Online IDS lab courses should be introduced to provide students with the experience of both individual and collaborative IDS experiments.

Designing such an IDS lab network is challenging, since remote students are not physically present in the lab. Asking instructors to adjust network hardware configurations before and/or during each lab exercise is not a solution. An efficient lab design should be capable of providing students with remotely re-configuring ability.

2.1 Design Criteria

Offering students an online laboratory that accommodates different IDS approaches and collaborative experiments is the basic goal of our approach. For remote education purposes, our design rule has been to keep restrictions on remote side to the minimum. We focus our attention on the following characteristics:

Availability: The designed online lab is accessible for remote users anytime, anywhere, and requires minimum hardware and software.

Today, many students own a laptop or desktop and have access to the Internet from home, office, campus, classroom or dormitory. This access provides all the equipment the student needs to be able to achieve a remote laboratory experience. From the other side, this might be the only opportunity students have to take courses and labs remotely. Consequently, an effective remote lab network designed for distance education should avoid any equipment beyond these basics.

In our lab, a student computer running Internet Explorer is sufficient for accessing the lab network resource and performing lab activities. Also, the Internet access method can be of any type: dial-up, DSL, etc.

Flexibility: Online, students can easily configure the designed lab network to various IDS approaches with no hardware configuration change required or instructors involved.

Reliability: There are two concerns. One is the reliable communication between remote users and the lab network. The other involves the reliable lab environment provided to students to execute lab activities successfully. Here, we used the minimum-maximum criteria to offer a reliable lab system. To simplify, it means to reduce the resources available to remote students to minimum while still enough to fulfill their lab activities. The instructors, on the other hand, have maximum privilege on resource management.

Economy: No redundant systems are adopted in the lab network in order to support various system configurations.

2.2 Lab Internal Network

Our developed lab network is an internal LAN (Local Area Network) network with student segment extension through VPN (Virtual Private Network) connection. The core of the lab network is a group of local hosts, which consist of the internal LAN network. Each local host has a second NIC (Network Interface Card) connected to the SPAN port of the switch and operated in promiscuous mode. The span port enables every local host to monitor all traffic transmitted over the LAN segment. In other words, any local host can capture malicious traffic occurring over the network; every local host within the LAN is, therefore, capable of acting as a sensor of the IDS system.

Since all local hosts can communicate with each other within the internal LAN, students have the freedom to select an arbitrary local host to receive alert messages from sensors and send management information. This means that each local host is ready to be configured as any function of the IDS system, such as a detection database or command console. It is the instructor's responsibility to assign specific local resources to each individual student based on the demand of experiments.

2.3 VPN Connection

To perform IDS experiments, remote students join the internal LAN and access the local hosts. This is achieved through the VPN connection. We used Cisco's VPN concentrator to establish a VPN tunnel with students' computers. Cisco VPN solution provides secure communication between remote computers and the internal lab network. Another advantage of using Cisco VPN concentrator is that it enables instructors to control and manage remote users' activities, such as remote student accounts management, access privilege management, and scheduling management, etc. On the remote side, students install VPN client software on their own computers. VPN client software functions the same way as other application software. A minimum configuration, such as VPN gateway IP address, student's account information, is required.

2.4 Remote Desktop Web Connection

Once they have been accepted as members of the internal lab network, remote students are authorized to access and use local hosts because all experiments are performed on local hosts. The control of local hosts by remote students is obtained through Remote Desktop Web Connection (RDWC).

To support RDWC, all lab local hosts are configured as the web servers. This means that the operating system running on local hosts must be Windows XP Professional. With the help of RDWC, remote students can work on any assigned local host through a virtual interface

running on their own Internet Explorer browser. From this point on, remote students can perform lab experiments the same way as they work on the lab's local hosts directly.

2.5 File Server

To perform IDS experiments successfully, remote students should be granted the full privileges of local hosts. One obvious disadvantage is the unreliability of the lab network. Local hosts may be corrupted and out of service as a result of inappropriate operation and/or unnecessary software installed by the students. Strict resource control can reduce the occurrence of system failures. This is achieved in our lab design with the file server.

All experiment-related software resources reside on the file server, from which students download the necessary software to the local hosts during each experiment. These resources have been pre-examined to ensure their reliability. Only instructors are authorized to manage these resources.

3. IDS Experiments

When students work on their experiments, the real lab activities are implemented on local hosts. Only the necessary display information is delivered to the remote sites and shown on students' computers. Remote students operate the lab hosts and perform experiments exactly the same way they do in on-site laboratory exercises.

3.1 HIDS Experiments

In HIDS, all IDS components are located together on the same host from which IDS monitors suspicious events. To engage in HIDS experiments, each student is assigned one local host, and all experimental activities are limited to this local host. Such experiments are typically done individually.

3.2 NIDS Experiments

In NIDS, IDS components are distributed over the whole network, so that NIDS experiments are basically collaborative ones. In a typical NIDS experiment, some local hosts are used to launch attacks and a selected number are configured as IDS sensors to detect these potential attacks. Other local hosts are used as alert databases or command consoles. During the experiment, students can rotate their roles to go through each part of NIDS system.

4. Evaluations and Conclusions

All local hosts are grouped within the internal network as a monitored LAN network during experiments. Remote students can configure any or all of them to establish either distributed or centralized IDS systems. Therefore, our lab approach combines both monitored and experimental networks together. It improves efficiency and reduces the cost of lab equipment. An entire lab network environment is exhibited in Figure 1.

In our IDS remote lab network, there are a total of 18 Dell computers working as internal hosts. Our IDS course is designed for a maximum enrollment of 24 for each semester. Considering every student must be assign to at least one internal host, the 24 students should break into two groups. Each group then accesses the lab network on a shift schedule. The instructor is responsible to schedule each group's lab hours on the VPN concentrator.

We tested in various user environments. Students can easily access the lab network and perform lab exercises with the help of Internet Explorer, a standard component of Windows OS. The lab network shows itself to be a reliable working environment and is flexible, allowing remote users to conduct both network-based and host-based IDS system experiments.

Figure 2 is a screen snapshot of a remote student's experiment. In this experiment, students deployed the Snort IDS system on some internal hosts. A number of other internal hosts are used to launch attacks, such as DoS (Denial of Services) attacks, against the internal network. The malicious traffic will pass through the internal network and be captured and displayed by Snort IDS systems. Using RDWC, remote students can easily deploy, configure, and manage Snort IDS applications on their own computers, and perform the entire experiment.

To participate in the developed online lab, remote students are required to provide their own computers with an Internet connection. The only additional step necessary is to install Cisco VPN client software on their computers. Our approach avoids putting an extra burden on students who are pursuing degrees through distance education program.

Using the Cisco VPN concentrator, instructors are able to control lab resources remotely, as shown in Figure 3. Through the VPN connection, instructors can remotely manage students' accounts, schedule lab sessions, and monitor VPN traffic.

Our testing also revealed some problems using the designed system. The network speed is still the primary bottleneck in our remote labs. If a student uses dial-up Internet access, remote lab access delay during the experiment may become intolerable. Using a wideband Internet connection such as DSL can improve lab performance significantly.

When more than one group exists in the class, each group must finish their own experiment before the next group starts, to avoid experimental configuration conflict. If the first group can't finish in time, the next group may not have enough time to work on their own job. One obvious solution is to expand the internal network -- but this may not be possible because of cost restrictions and network size. Running a remote lab more efficiently with limited resources is an interesting and important topic to consider, particularly when the class size is large.

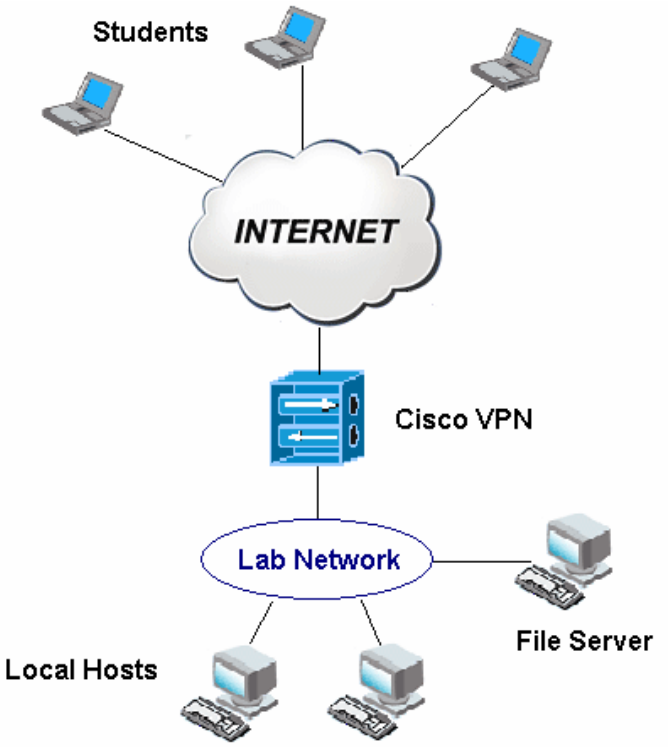

Figure 1: IDS Lab Network

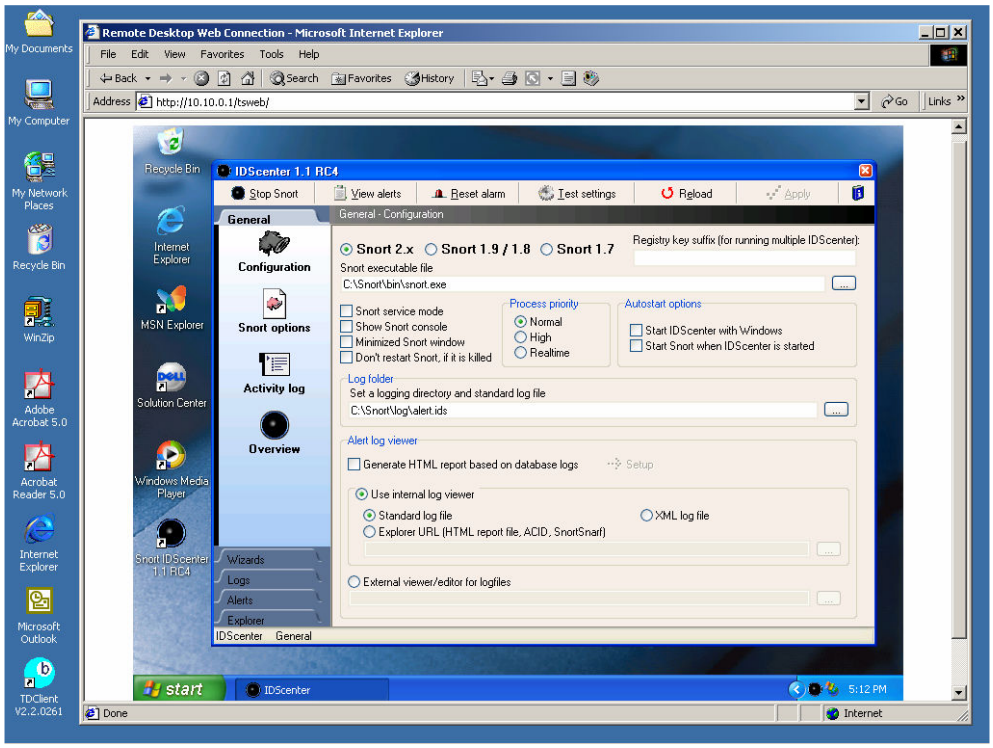

Figure 2: Screen Snapshot of IDS Experiments with Snort

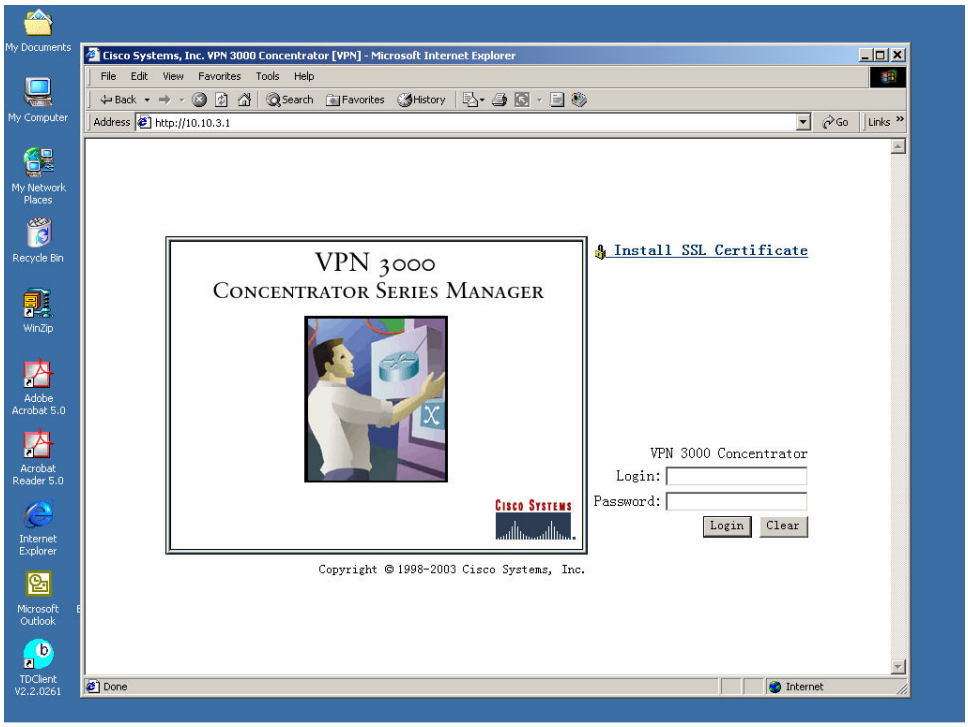

Figure 3: Student Accounts and Usage Management with Cisco VPN

References

[1] Crowley, Ed "*Experiential Learning and Security Lab Design*", Proceedings of the 5th Conference On Information Technology Education, Session: Security III. 2004, Pages: 169 – 176

[2] Taylor, K.D.; Honchell, J.W.; DeWitt, W.E.; "*Distance learning in courses with a laboratory*", Frontiers in Education Conference, 1996. FIE '96. 26th Annual Conference, Proceedings of, Volume: 1, 6-9 Nov. 1996, Pages: 44 - 46

[3] Aburdene, M. F., Mastascusa, E. J. and Massengale, R. "*A proposal for a remotely shared control systems laboratory*", Proceedings of theASEE 1991 Frontiers in Education Conference, Session 24A3, 1991, Pages: 589-592

[4] Hong Shen, et al. "*Conducting laboratory experiments over the Internet*", Education, IEEE Transactions on, Volume: 42, Issue: 3, Aug. 1999, Pages: 180 – 185

[5] Hua, Ji and Ganz, Aura "*A New Model For Remote Laboratory Education Based On Next Generation Interactive Technologies*", *Microsoft ConferenceXP Resource Library.* http://www.conferencexp.net/community/Library/Papers/aseeivlab.pdf

[6] Hua, Ji and Ganz, Aura "Web Enabled Remote Laboratory (R-Lab) Framework", The 33th ASEE/IEEE Frontiers in Education Conference, Session T2C, 2003, Pages: 8 – 13

Xin Tang received his Ph.D. from New Jersey Institute of Technology in major of electrical engineering. Currently, he is an assistant professor in Department of Technology Systems, East Carolina University. His research interests include digital communications, signals detection and estimation, CDMA multi-user detection, wireless communication system development, information system security.

Kai Li is an Assistant Professor in the Department of Technology Systems at East Carolina University. He received his M.S. degree in Computer Science and a Ph.D. in Electrical and Computer Engineering, both from the University of North Carolina at Charlotte.