AC 2009-1316: INNOVATIVE NETWORK SECURITY COURSE DEVELOPMENT

Hetal Jasani, Northern Kentucky University

Dr. Hetal Jasani is an assistant professor in the Department of Computer Science at Northern Kentucky University. His research interests include mobile and wireless networks, distributed systems and network security. He has published many publications in refereed journals and conference proceedings and given presentations at a variety of conferences. He is a professional member of various technical organizations such as ACM, IEEE and ASEE.

Dr. Jasani received the Ph.D. from Florida International University in 2006. He also worked as assistant professor at Michigan Technological University before joining NKU. At NKU, he teaches graduate and undergraduate classes in the area of computer networks and network security. He has chosen academic career since he believes that by teaching he can contribute towards community development.

Wei Hao, Northern Kentucky University

Dr. Hao came to NKU in August 2008 from Cisco Systems in San Jose, California, where he worked as a software engineer. He earned his PhD in Computer Science from the University of Texas at Dallas in 2007. He brings both academic and industrial expertise, having also worked for Motorola and Alcatel. His research interests include Web Technologies (such as web caching, web services, and web-based systems), Computer Networks, and Operating Systems.

Innovative Network Security Course Development

Abstract

Network security courses become increasingly popular in colleges (including community colleges) and universities. This paper discusses about developing the novel course of network security using laboratory activities. It elaborates innovative projects that are suitable for laboratory work in network security curriculum. It explores both hardware and software components that are now being used for practical exercises in network security courses. Most often these laboratory exercises include many hands-on activities.

In learning the concepts of network security via hands-on labs, students have ample opportunities to understand the underlying security technologies that prepare the engineers and technologists of the next generation. This paper discusses the hands-on labs for network security technologies, especially configuring the firewall (Access Control List - ACL), VPNs (Virtual Private Networks), IPS (Intrusion Prevention Systems) on various devices such as Cisco routers and Adaptive Security Appliances (ASA). In addition, this paper also discusses the wireless network security which is also very important part of the course due the growth of wireless LAN.

Introduction

The field of network security is dynamically changing due to the advances in the technologies. It becomes more and more vital as people spend more and more time connected to the Internet. Intruding into networked resources is often much easier than compromising physical or local security. Many areas of network security demand highly trained personnel to solve the new challenges such as firewall, VPN, IDS (intrusion detection system), IPS, wireless LAN security, etc. There is a great demand of technicians and engineers who can maintain and secure the networked environment.

While theory oriented electrical and computer engineering and computer science curriculums offer students few network security courses, this may not be enough to train network engineers with the proper background on the newer security technologies. Although many courses on computer and network security have been developed in these programs, they are primarily focused on in-depth mathematics, algorithms, and theory. Most of these courses are not focused on hands-on experiments that are very useful to gain the understanding of fundamental concepts. Since computer information technology (CIT) program emphasizes the hands-on learning, the previous approach taken by computer engineering programs is not suitable for CIT program. As mentioned earlier, due to the high demand and need of network security education, our CIT program curriculum includes few courses related to the network and computer security.

The goal of the network security (CIT484) course at our university is to familiarize students with several different network security technologies through a series of laboratory experiments using small-scale test beds although the network devices for performing laboratory experiments with the newest technologies are expensive and change constantly. Consequently, it is very difficult to upgrade and continuously enhance these laboratories. However, hands-on experiments are the best way to enhance the students' learning.

Many universities have used different network security protocols and devices for hands-on labs in network security courses. The CIT program[1] in the Department of Computer Science[2] at Northern Kentucky University[3] offers several courses in network, system and database administrations. In newly designed network security course (CIT484) with enhanced laboratory experiments have demonstrated effectiveness in teaching the concepts of different network security technologies[4]. This course has been proposed to provide a practical view of network security using real equipment configurations. The course assumes that students have the knowledge of networking (i.e., students had taken the first course of network administration/troubleshooting). It includes lectures covering the relevant concepts needed to understand the different security technologies including VPN, IDS, IPS, etc. and their applications. We acquired Cisco equipments to enhance these laboratories experiments. This paper discusses some of lab experiments belong to network security course. This course is a three credit-hour course consisting of two 75-minutes lectures/labs per week. The evaluation and feedback from students show that they understand many of the topics in the network security field, and gain hands-on experience and skills to defend the networked systems.

In the rest of the paper, we discuss the general course development approach. We illustrate some sample hands-on labs. This paper also discusses the assessment from the network security course in computer information technology program. Finally, it concludes our discussion on developing the network security course.

Course Development

In our CIT program, many courses (securing computer systems, advance system administration, network security, etc.) deal with computer and network security technologies. However, network security course primarily focus on securing the network using real networking devices. The objectives of network security course in our CIT program at Northern Kentucky University are that students should be able to:

- Use the security appliances to configure firewalls, intrusion prevention, VPNs
- Harden Cisco routers
- Understand and implement wireless network security
- Configure and debug network security appliances using the IOS (Internetwork Operating System) command line
- Design network security architecture

For the hands-on network security labs, students configure several networking devices such as Cisco routers, Cisco switches, Cisco adaptive security appliances (ASA), Cisco wirelesses access points, etc. to provide various security features of the networks.

Course outline

The course is scheduled for a 15-week semester with laboratory assignments that students perform during regular/assigned lecture/lab time. To accomplish the above mentioned objective, the following topics are included[4,5]:

- Network security fundamentals

- Firewalls
- Access control lists
- Network address translations
- Wireless network security
- Hardening the routers
- Security protocols and virtual private networks
- Intrusion detection systems
- Intrusion protection systems

It was difficult to find the ideal textbook for this course due to the coverage of many security technologies with emphasis on networking. We adopt following textbooks for this course:

- Title: Inside Network Perimeter Security, 2nd Edition, Sams publication, Authors: Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, Ronald W. Ritchey, ISBN: 0672327376
- Title: Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance, Authors: Omar Santos, Jazib Frahim., Published by Cisco Press, ISBN: 1587052091

Sample Hands-on Labs

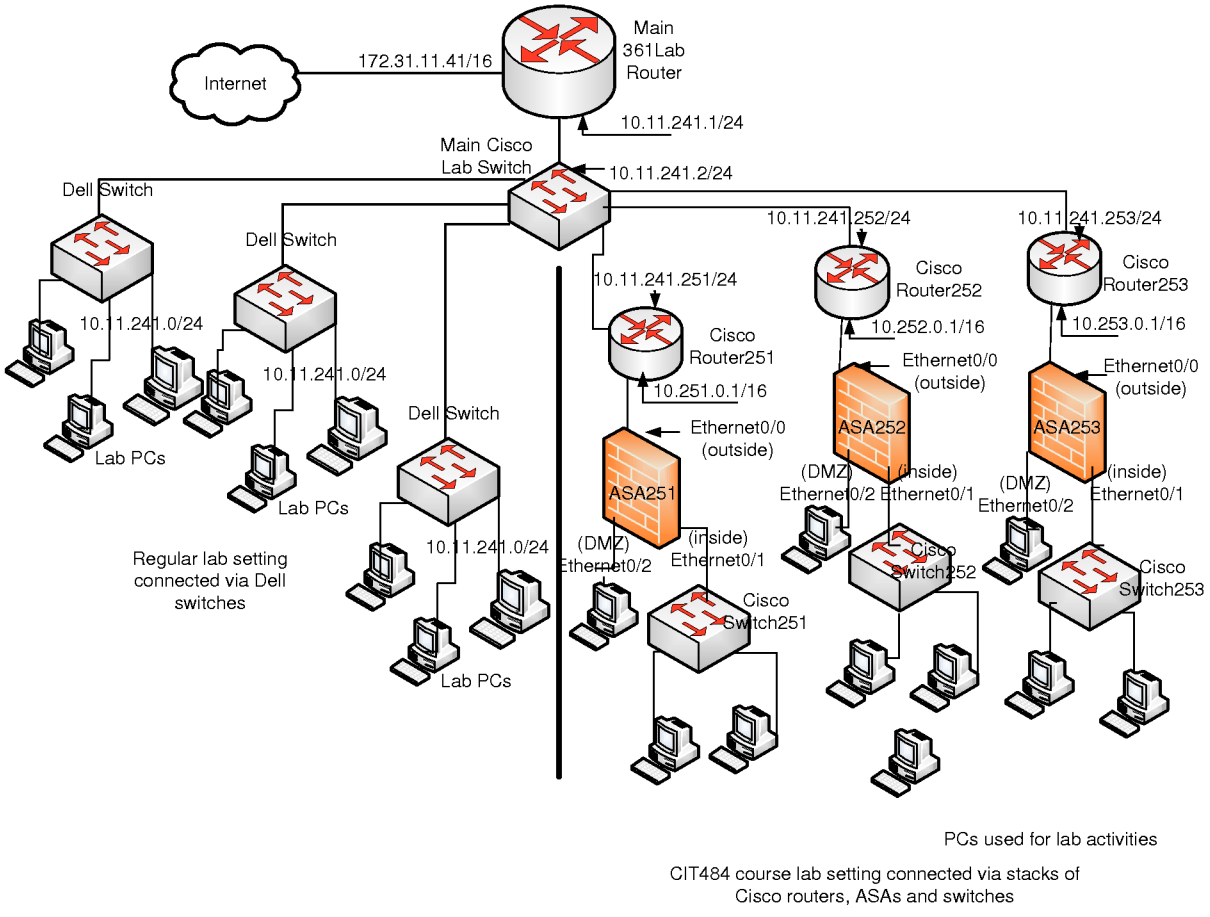

Figure 1 General Lab/Classroom Network Diagram

Some sample labs including theoretical background are discussed below to demonstrate the major areas of this course. Students perform hands-on labs using command line interface to configure the access control lists (ACL) on the Cisco routers. Students configure standard and extended control list to filter the various networking traffic. Students also configure the Cisco Access Point (AP) to enhance the wireless security[12]. Students configure Cisco ASA (adaptive security appliances) to create site-to-site VPN, remote-access VPN, IPS. Due to the limitation of space, only few sample labs are described in this paper.

Figure 1 shows the classroom network that students use for various courses. In other words, the security lab is set up in the regular classroom, in which many classes are being taught. On left side, regular lab network setting is shown and connectivity to Internet can be identified via Dell switch, Cisco switch and Internet router. However, on the right side, network connections for networking and security lab are shown using additional Cisco switches, routers, and ASAs that could be configured in various networking/security lab exercises.

Sample Lab#1: Firewall Technologies or Access Control List (ACL) on Cisco routers

The perimeter security is very important in today's networking world. It could be provided by the network-based firewalls. Detailed understanding of how firewalls and their related technologies work is extremely important for all network security professionals and students. The knowledge of firewall helps them to configure and manage the security of their networks precisely and efficiently. Students are taught two types of firewall: network firewall and personal firewall. The network firewall could be systems or devices that are placed between an outside and an inside network. Numerous network firewall solutions that students learn in this course offer user and application policy enforcement that provide attack protection for different types of security threats. Students also learn the logging capabilities of these firewall devices that allow them to identify, investigate, validate, and mitigate such threats that could be carried out in the real world. The personal firewall could be software applications that can run on a system to protect only that host. In this network security course, the focus was the network firewall. The primary duty of a network firewall is to deny or permit traffic that tries to enter the network based on explicit preconfigured policies and rules. The filtering techniques that are used to allow or block traffic may include the following:

- Simple packet-filtering techniques
- Multifaceted application proxies
- Stateful inspection systems

Students configure simple packet-filtering techniques in this lab. This experiment aims to create and apply the standard and extended ACL[14] to filter specific network traffic that pass through the router.

As shown in Figure 2, students connect PCs to Cisco switch that has already been configured for normal connectivity. Students configure a standard IP access list on the Cisco router using console/rollover cable, which filters traffic based on source IP addresses. This process is carried out in two steps. First, the list is created using a console terminal connection and configured in global configuration mode. Second, the list is applied to the appropriate interface as either an

inbound or an outbound direction in interface configuration mode. Students create standard access list and apply in order to deny traffic from particular host IP. Finally, student monitor and test the list. In the second part of the lab, students create an extended list. The process of creating extended list is the same as creating the standard access list. An extended list will allow students to filter traffic based on source address, destination address, source port and destination port. In this case, students block the ICMP (Internet Control Message Protocol) traffic to specific destination host from the specific source host using ping utilities.

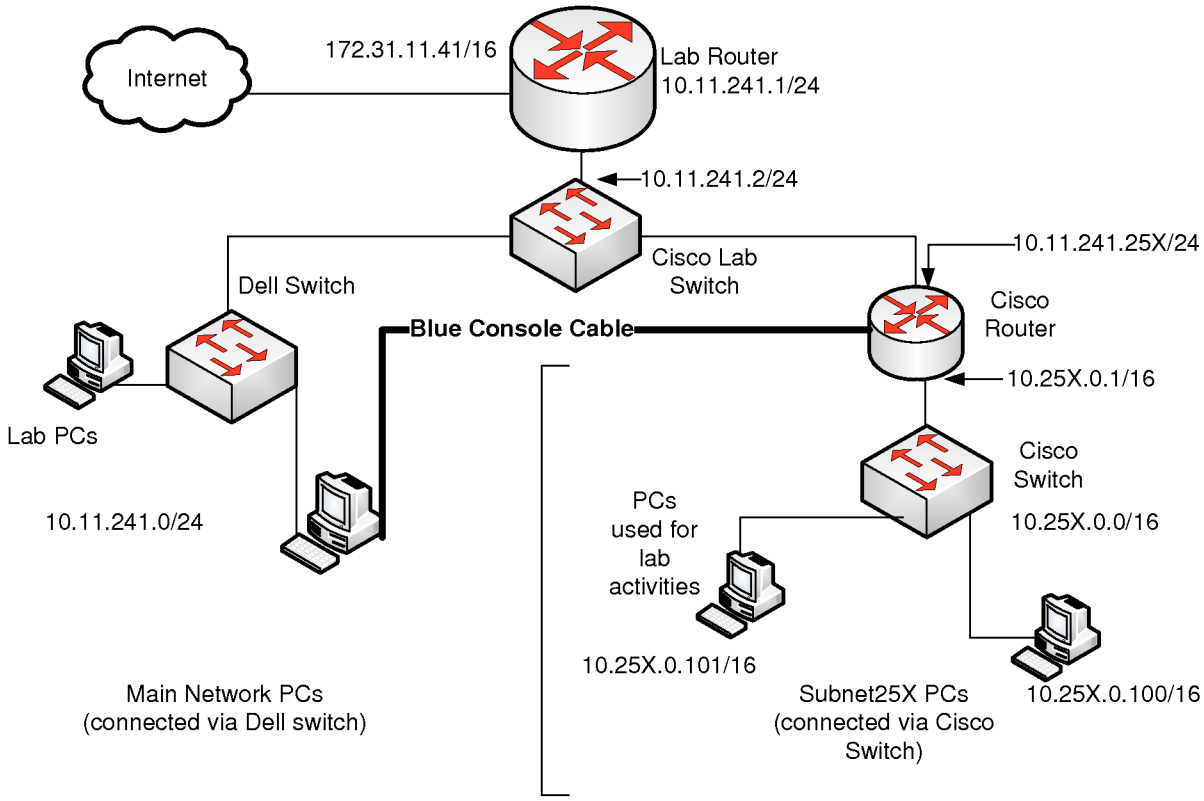

Figure 2 Network Diagram for ACL Lab Network Diagram

After creating standard and extended list, students are asked to create more advanced features such as named list, reflexive list, use of object grouping, etc. Students are also asked to submit a lab report discussing their learning experience based on this lab.

Sample Lab#2: Site-to-Site VPN using Cisco ASA

The virtual private networks (VPNs) are useful to provide the low-cost, widespread medium to transport data while providing data integrity and confidentiality to protect the information within the data packets. Students are introduced to the following examples of VPN protocols[5]: Point-to-Point Tunneling Protocol (PPTP)[6], Layer 2 Forwarding (L2F)[7] Protocol, Layer 2 Tunneling Protocol (L2TP)[8], Generic Routing Encapsulation (GRE)[9] protocol, Multiprotocol Label Switching (MPLS)[10] VPN, and Internet Protocol Security (IPSec)[11].

Two or more offices of a corporation can establish a VPN connection using the site-to-site protocols so that they can send traffic back and forth using a shared medium such as the Internet. This is cost effective solution since it eliminates the need to have dedicated leased lines to connect the remote offices to the corporate network. The high maintenance cost of point-to-point WAN links can be reduced by using the IPSec VPN tunnel in site-to-site mode. The network administrators can use broadband connections, including DSL (digital subscriber line) or cable modem, to achieve Internet connectivity at a considerably cheaper rate, and they can deploy IPSec VPN on top of that to connect the remote locations to the central site in a secure way.

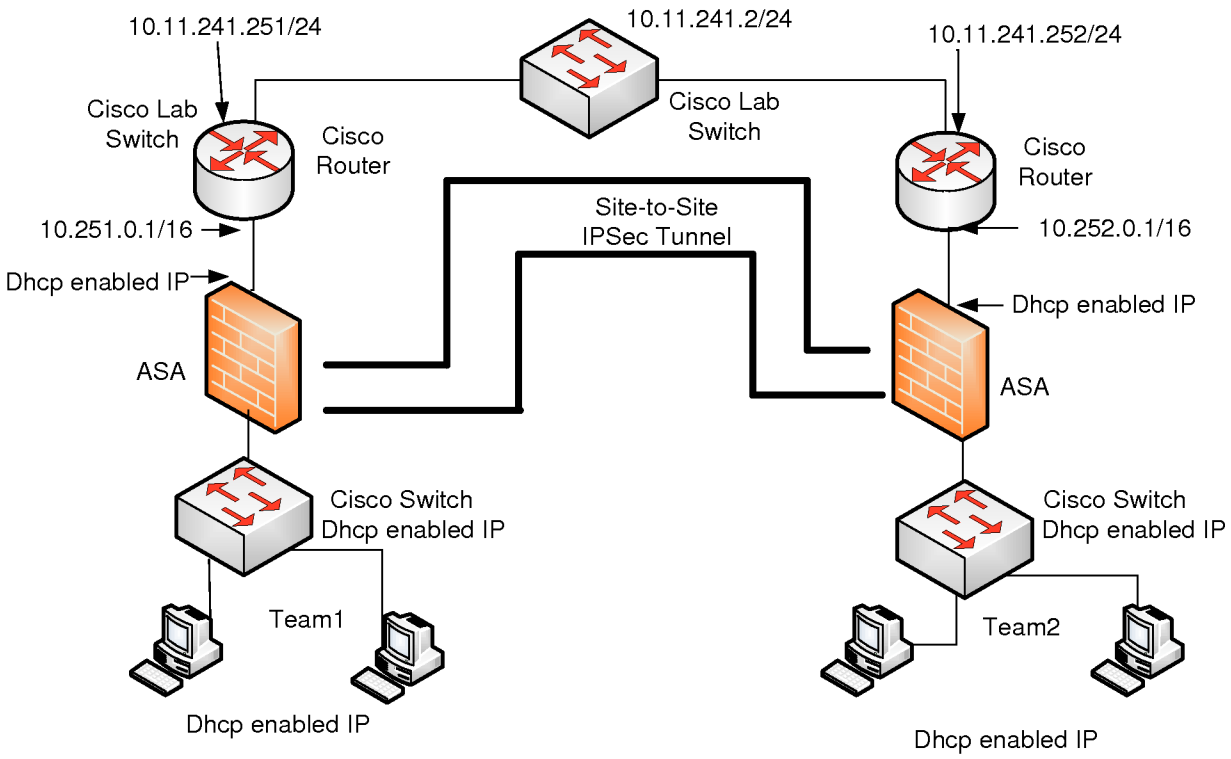

Figure 3 Site-to-Site VPN Lab Network Diagram

In this lab, students configure a site-to-site IPSec tunnel between two ASAs, as shown in Figure 3, using Cisco IOS commands. Here are some steps involved in order to create site-to-site VPN[5]:

1. Enable ISAKMP.
2. Create ISAKMP policy.
3. Set the tunnel type.
4. Configure preshared keys.
5. Define the IPSec policy.
6. Specify interesting traffic.
7. Configure the crypto map.
8. Apply the crypto map to the interface.
9. Configure traffic filtering.

This lab provided a challenging real world experience to the students since students have an unique opportunity to create site-to-site VPN using Cisco ASA. Students were very happy to learn this exciting technology.

Sample Lab#3: Remote access VPN using Cisco ASA

As mentioned earlier, the remote-access VPN is another kind of VPN connection. It could be beneficial to an organization by allowing mobile users to work from remote locations such as home, hotels, and Internet cafes. Previously, the only way to provide this kind of connection was through dialup connections using analog modems. To accommodate remote users, corporations had to maintain a huge pool of modems and access servers. Moreover, it was quite expensive due to the use of toll-free and long-distance phone service charges. More and more dialup mobile users are migrating to broadband DSL and cable-modem connections due to the rapid growth of the Internet technologies. Consequently, corporations are in the process of moving these dialup users to remote-access VPNs for faster and secure communication. Therefore, it is very important for students to know this technology and how to configure it.

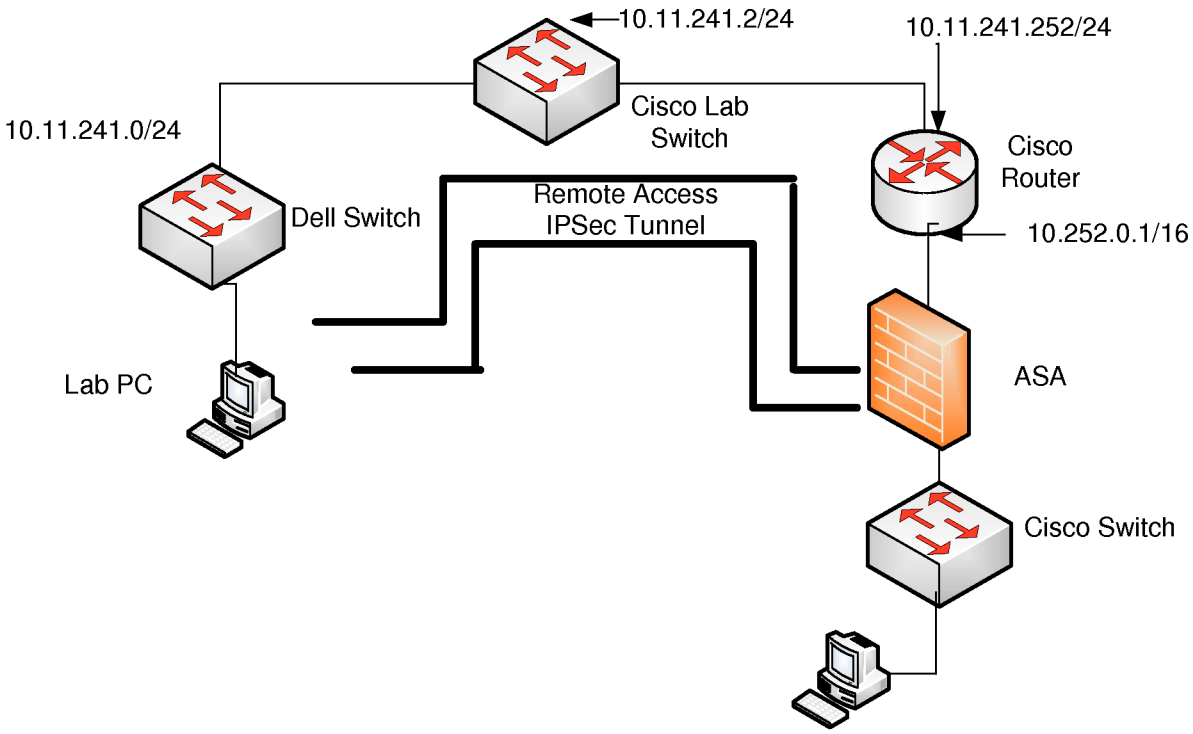

Figure 4 Remote-Access VPN with local authentication Lab Network Diagram

Students are taught that there are many remote-access VPN protocols as in the case of site-to-site VPN such as Point-to-Point Tunneling Protocol (PPTP)[6], Layer 2 Forwarding (L2F)[7] Protocol, Layer 2 Tunneling Protocol (L2TP)[8], and Internet Protocol Security (IPSec)[11]. Those protocols could be used to provide the secure network access. Figure 4 shows the network set up which students create in order to perform this lab. This is the first part in which students use the local authentication on Cisco ASA (without using any external devices such as RADIUS server).

In this lab, students follow the following steps in order to configure the remote-access VPN on Cisco ASA using Cisco IOS commands:

1. Enable ISAKMP.
2. Create the ISAKMP policy.
3. Configure remote-access attributes.
4. Define the tunnel type.
5. Configure preshared keys.
6. Configure user authentication.
7. Assign an IP address.
8. Define the IPSec policy.
9. Set up a dynamic crypto map.
10. Configure the crypto map.
11. Apply the crypto map on the interface.

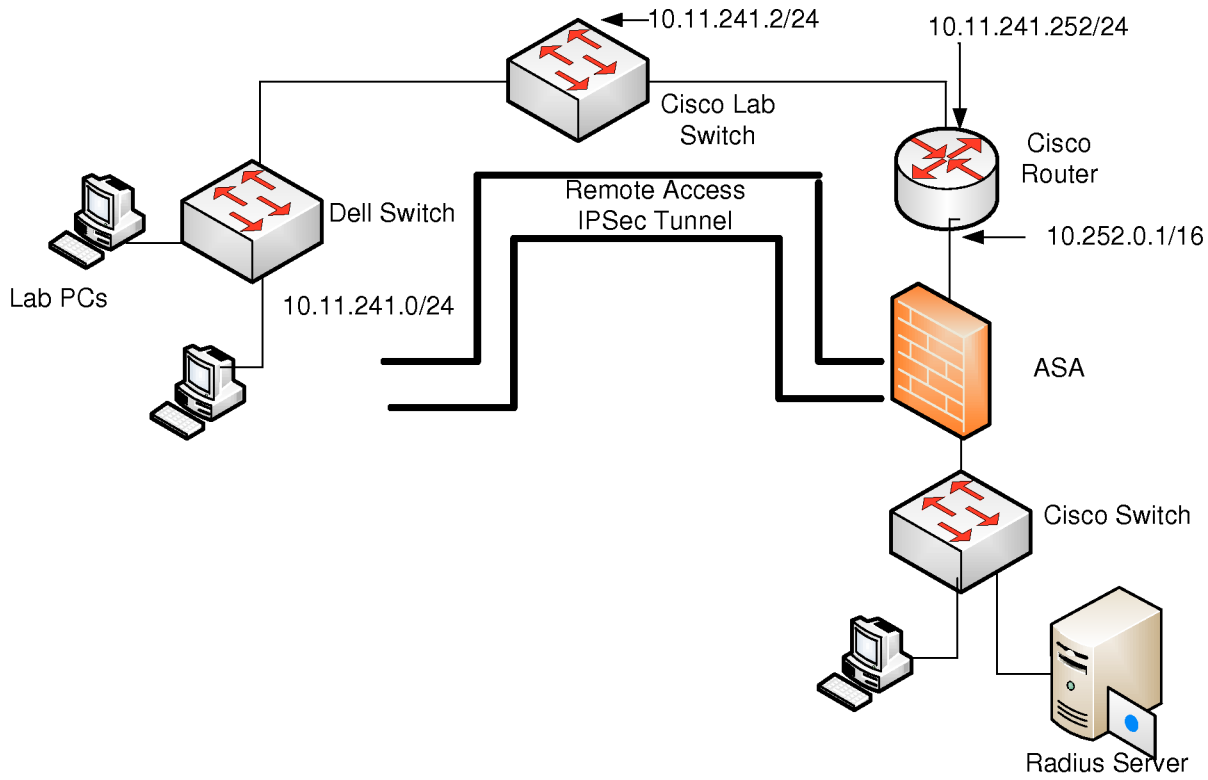

Figure 5 Remote-Access VPN with Radius Server Authentication Lab Network Diagram

Students are made aware of two types of modes that could be used for creating IPSec. It is recommended to use main mode for IKE authentication using RSA signatures because of the known vulnerabilities in aggressive mode[5]. There are two different types of authentications (step 6 above) that could set up for this lab. Figure 4 shows the local authentication while Figure 5 shows the remote authentication using RADIUS (Remote Authentication Dial-in User Service) server. Configured RADIUS server has been provided to the students to accommodate lab completion time.

This lab is very important as mentioned earlier due to the importance of technology for providing secure connection for employees to the corporate data networks. Students get chance to play with very expensive Cisco ASA that is the latest appliance from Cisco which supports many security technology including VPN, IDS, IPS, firewall, etc.

Sample Lab#4: IPS (Intrusion Prevention System) using Cisco ASA

Students can effectively detect and react to security threats using the Cisco Intrusion Prevention Software that is integral part of Cisco ASA. This device could detect attempts from malicious users to steal information or to gain unauthorized access to a network or a host to create performance degradation such DDoS (Distributed Denial of Service). In this lab, students learn about the Cisco IPS software architecture. In addition, they also learn how to configure and monitor the AIP-SSM (Adaptive Inspection and Prevention Security Services Module), and several troubleshooting techniques. By performing this lab, students achieve the efficient network intrusion protection skill which is vital to maintaining a high level of protection. Students learn that the cautious protection ensures business continuity and minimizes the effects of costly interruption of services.

The CIPS 5.x CLI on Cisco ASA provides a user interface for all direct connections to the AIP-SSM (e.g., Telnet, SSH, and session from the ASA). Students achieve the following skills by performing this lab:

- How to log in to the AIP-SSM via the CLI
- CLI command modes
- Initial AIP-SSM configuration

In addition, students also configure the different types of users in the AIP-SSM with different roles associated to them. Each AIP-SSM user account has a role associated to it. There are a total of four roles that can be assigned to a specific account: administrator account, operator account, viewer account, and service account. Students also learn about the advanced features and configuration of the AIP-SSM CIPS software, such as IPS tuning, custom signatures, IP logging, and shunning.

Sample Lab#5: Wireless LAN Security

Without including the wireless network security, course objectives could not be fully fulfilled as wireless network security is very important topic. Students are asked to perform lab to setup the various security on Cisco Access Point. Students perform the following lab activities:

- Set a MAC address filter on Cisco AP (access point)
- Configure open authentication with WEP on Cisco AP
- Set dynamic WEP keys on Cisco AP
- Setting up WPA (Pre-shared Key) on the Cisco AP
- Setting up WPA2 on the Cisco AP

By performing the above activities, students could understand the weakness of WEP, and dynamic WEP. Students also understand the WEP could be cracked easily with tools available for free. Students also configure the WPA and WPA2 which are more secure ways of providing the wireless access to the users. Students learn that the corporation should use WPA2 in order to provide confidentiality and privacy of data communication over the wireless link.

Assessment, Students Feedback and Teaching Reflection

Various methods were used to formally assess the effectiveness of this course, including tests, the evaluation of student work, and the instructor's assessment. At the end of the semester, an anonymous survey was conducted to evaluate the content and effectiveness of the course. The overall response from students regarding whether the course met their expectations was very positive. Here is a summary of student comments and results of the survey:

- This course presents interesting topics and helps them to learn various technologies to secure the networks.
- They have a better understanding of network security issues.
- The hands-on labs were excellent and effective.
- The lab helped them in understanding the lecture topics.
- Few students considered that some labs were very long in term of completion time.
- It is rewarding to see the result although some of the labs are complex.

The future improvement for this course is to add more hands-on labs involving network security tools such as Argus, Snort, NMAP (security/port scanner), etc. Moreover, simulation experiments using OPNET[13] will be designed to enhance learning of the network security concepts.

Conclusions

Network security courses become increasingly popular in colleges (including community colleges) and universities. In learning the concepts of network security via hands-on labs, students have ample opportunities to understand the underlying security technologies that prepare the engineers and technologists of the next generation. The development of the network security course using laboratory experiments was the main theme of this paper. We presented few hands-on experiments. Students performed experiments using Cisco networking devices such as switches, routers and ASAs, submit lab reports, and completed evaluation forms to give a feedback in order to improve and update the assignments for coming semesters. Students found this course along with lab assignments helpful to them in understanding the theory of network security, and gaining practical experience. In the future, more lab assignments would be developed involving more advanced security tools. Moreover, simulation experiments using OPNET will be designed to enhance the learning of the network security concepts.

Bibliography

1. CIT Program at NKU, http://informatics.nku.edu/csc/undergraduate/cit/index.php, last accessed January 29, 2009.
2. Department of Computer Science at NKU http://informatics.nku.edu/csc/programs/index.php, last accessed January 29, 2009.
3. Northern Kentucky University (NKU), http://www.nku.edu/, last accessed January 29, 2009.
4. Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, Ronald W. Ritchey, "Inside Network Perimeter Security", 2nd Edition, Sams publication, ISBN: 0672327376, 2005
5. Omar Santos, Jazib Frahim., "Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance", Cisco Press, ISBN: 1587052091, 2005
6. RFC 2637 - Point-to-Point Tunneling Protocol (PPTP), http://www.faqs.org/rfcs/rfc2637.html, last accessed January 29, 2009.
7. RFC2341 - Cisco Layer Two Forwarding (L2F) Protocol, http://www.faqs.org/rfcs/rfc2341.html, last accessed January 29, 2009.
8. RFC2661 - Layer Two Tunneling Protocol (L2TP), http://www.faqs.org/rfcs/rfc2661.html, , last accessed January 29, 2009.
9. RFC2784 - Generic Routing Encapsulation (GRE), http://www.faqs.org/rfcs/rfc2784.html, last accessed January 29, 2009.
10. RFC3031 - Multiprotocol Label Switching (MPLS) Architecture, http://www.ietf.org/rfc/rfc3031.txt, last accessed January 29, 2009.
11. RFC - Security Architecture for the Internet Protocol (IPSec), http://www.ietf.org/rfc/rfc2401.txt, last accessed January 29, 2009.
12. Cisco Systems, "A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite", Cisco Systems, Inc., 2002.
13. Online Documentation, "OPNET Modeler," http://www.opnet.com/, Date visited: March 2007.
14. Wendell Odom, CCNA Official Exam Certification Library (CCNA Exam 640-802), 3rd edition, Cisco Press, ISBN: 1587201836, 2008