INTEGRATE INFORMATION SECURITY WITH INTERNETWORKING

Cheer-sun D. Yang[1]

***Abstract* ¾** *This paper presents a nontraditional approach to incorporate the concept of information security with the course entitled 'internetworking with TCP/IP'. Traditionally, the internetworking course mainly concentrated on the interconnection of homogeneous and heterogeneous machines. Very little attention was focused on information security issues. After the terrorist attack on September 11, 2001, information security suddenly came under the spotlight. To raise the awareness of students on information security, the internetworking course was modified. For example, a Cyber Defense/Attack Lab was established; the pedagogical approach was modified to add a Cyber War as part of the course activities. In this paper, the general concept of an integrated curriculum is introduced first. Then the course content is described in detail followed by the hands-on labs. The layout of the Cyber Lab and some tools used by students to hack computer systems are discussed. Finally, the experiences learned are described.*

Index Terms ¾ *information security, internetworking, integrated curriculum, non-traditional curriculum*

INTRODUCTION

Since September 11, 2001, security in general has become the top priority issue in many organizations. With a goal to raise the awareness of students on information security, we begin to integrate information security with internetworking. To achieve this goal, several efforts have been initiated to support the major change. First, a Cyber Defense/Attack Lab is established for teaching the course *Internetworking with TCP/IP*. Second, this course material is revised to integrate information security issues and concepts. Traditionally, this course only focused on the techniques and issues involved in the interconnection of various networks using repeaters, bridges, routers, and gateways [1]. The revised material also includes information security as part of the themes [2, 3, 4]. Third, lab assignments will include Cyber Defense/Attack as part of the major tasks students are involved. Currently, the course is offered under the course title '*Internetworking with TCP/IP*'. In the future, it is recommended that the course be renamed to 'Internetworking *and Security* with TCP/IP".

In the remaining of this paper, the course content, some hands-on labs, tools used in the cyber war, and experienced learned are discussed in detail. Finally, the summary section describes the future work.

COURSE CONTENT

The internetworking course consists of three major phases: (1) communications and networking fundamentals, (2) internetworking techniques, and (3) cyber war. Since the internetworking course is offered to students with minimum networking experiences, it is essential to provide enough background information. Thus, some fundamental topics are presented in phase I. In the following sections, the first and the second phases will only be described briefly; the major focus of this paper is on the third phase, i.e., the cyber war, since this is the major deviation comparing with a traditional internetworking course.

Phase I – Communication Fundamentals

During the first phase, the fundamental concepts include (1) the layered architecture, (2) OSI seven-layer reference model, (3) TCP/IP five-layer model, and (4) standards and protocols. As mentioned previously, it is essential to introduce these fundamental concepts in a 'whirlwind fashion' without spending a tremendous amount of time so that students in all experience spectrums are considered. After this phase completes, students are expected to understand the concepts such as TCP ports and IP addresses.

Phase II –Internetworking

When two hosts attempt to communicate with each other, some intermediate nodes are usually involved. Networking and internetworking of many LANs are the main topics in this phase. Only the major goal is to lay the groundwork for the third phase. Hence, we started with the introduction of internetworking with hubs, bridges, and routers; we soon focus on the password used for an administrator to change the configuration of a router. While security becomes the focus, the course then enters the final stage.

Phase III – Cyber War

In the third phase of this course, information security issues are discussed. To unveil the mystery, some hacking tools such as a Trojan horse (a server and a client) and a port scan tool [6] are discussed to demonstration how a hacker can

[1] Cheer-sun D. Yang, West Chester University of Pennsylvania, Anderson Hall 324, West Chester, PA 19383 cyang@wcupa.edu

www.manaraa.com

attack a computer and steal users' passwords. To end this course at a high note, students are separated into two teams. One team performs hacking activities, while the other team performs defense. Before the Cyber War period begins, students submit a Cyber War Strategic Plan to describe how they are going to conduct attack and/or defense. This war plan will only be distributed to the instructor and their teammates. At the end of the Cyber War, students will submit a Summary Report discussing issues, concerns, and techniques that they have learned during the Cyber War. The topics discussed in the class include the following:

- System level attack - The attacks initiated from within a LAN or an Intranet is considered a system level attack. The major topic includes various password attacks and viruses. We assume that hackers are insiders and own a valid user id; the targets are other users. For example, using NAT (NetBIOS Audition Tool) [11], a hacker can check if any user uses 'simple' passwords. The hacker can enter a range of IP addresses and simply hit the ENTER key, NAT will display a list of user names and the password for each user id. At this level, a hacker usually attacks the Intranet within a company or campus networks. Using the compromised user id, a hacker can attack other systems without exposing the hacker's own identity. Hence it is why important to raise the awareness of all users in a company. In many situations, naive users use the password the same as the user id, easy-to-remember numerical digits, birthday, telephone number, etc. These are among the passwords that are easily obtained by hackers. Unfortunately, some computer users including college students tend to use some of these schemes to assign their passwords.
- Network level attack - The intrusion initiated from outside of a LAN via network connections is considered a network level attack. This class of attacks usually target at other systems and server machines. For example, IP scanning, port scanning, and information interception [3, 4] are considered network level attacks. IP scanning software can be used to collect information about file names on a system [12]. Port scanning software [13] allows you to find out what services (daemons) are waiting for external connections. They are 'double-swords' that can be used to hack a system or detect intrusions.
- Denial-of-service attack - Any attack preventing network or service providers from providing services is considered a denial-of-service attack [6]. For example, a router could be under attack and forced to reconfigure. Students will benefit from learning in an isolated environment how denial-of-service can be realized.
- Cyber defense - With the awareness of all kinds of cyber attack, students should now be ready for learning tactics to defend a system or network systems against hackers' attacks. Many techniques have become available on the Internet for defending a system or a network system against various attacks. Mostly they belong to the following categories: anti-virus [5], system checking [7, 8, 9], intrusion detection, firewall [6]. Anti-virus software usually prevents a system from being contaminated. System checking software usually operates prior to hackers' attacks and must be executed regularly. It is considered an attack prevention technique. Intrusion detection is an approach to detect that a system has been compromised. This is a difficult job without the help of intrusion detection software. One of the reasons is that, after a Trojan horse attack, a Trojan horse server program could be stored on a system folder with a system-related name. It is difficult to judge whether or not it could be deleted without hurting the system. A firewall can be used to shield the system from being connected to an outsider via certain specific port numbers.

HANDS-ON LABS

It is generally believed that hands-on experience can reflect what an instructor covers in a lecture and further enhance the impression. Therefore, some hands-on lab experiments areassigned to supplement the lectures throughout the whole semester. Some of the examples are listed as follows:

- Configuration PCs for internetworking purposes - Configuring an Operating System is not as trivial as students might think. This lab includes the installation of the Linux operating system to coexist with Windows 98. The hard drive must be partitioned first prior to the configuration of the Linux. Currently, the Linux Operating System used is Redhat 7.0 although the upgrade to the latest version, i.e., Redhat 7.2, has been planned. Also, on one of the PCs, a Windows® 2000 Server is installed.
- Configuring PCs to form a peer-to-peer network - When internetworking techniques are introduced, it is instructive to teach students how to configure PCs running various operating systems to form a peer-to-peer network. With this configuration, a PC can share files and printers with others via an Ethernet link. This can be achieved via switches or hubs. In our lab, we provided hubs to connect PCs running Windows 98 operating system. Linux can also be the choice. Since the target Cyber War will target the systems running Windows operating systems, we chose Windows as the operating system for this lab experiment.
- Configuring Cisco® routers - A minimum lab environment for a Cyber War requires two LANs to be connected together. There are several alternatives. Currently, we are using hubs and Cisco 2621® routers to achieve the simplest function. In the future, we plan to replace the hubs with Ethernet switches. This lab experiment involves the configuration of Cisco® routers

المنارة للاستشارات
www.manaraa.com

to form an isolated network with two LANs in it. Figure 1 illustrates the configuration of the Cyber Security Lab. In this Lab configuration, two LANs are formed. For simplicity, only two hosts are included in each LAN in the figure. In fact, four PCs are connected to each hub. The reason to use hubs for connecting hosts together is due to the constraint that a Cisco® 2621 router only supports two FastEthernet interfaces. Each interface only allows one RJ-45 connector to be connected to the router. Sharing one FastEthernet port using a hub then becomes the most economical and natural approach. For a real world, a layer-2 switch can replace the position where hubs are used. In addition to the hosts and internetworking devices, a Windows® 2000 Server is also connected to the Cisco1538_2 Hub. The server provides the necessary services such as Domain Name Service (DNS), Windows Internet Naming Service (WINS), and file transfer service. In the future, it will be enhanced to support the function of routing for connecting to the campus network.

TOOLS USED IN THE CYBER WAR

The Cyber War marks the beginning of the third phase. The cyber war involves the defense and attack from an insider as well as from an outsider. Several rules have to be enforced such as: no physical installation of a Trojan horse on others' machines, no 'stealing' of the root password with other means without going through the Internet. No one is allowed to perform a 'trivial defense', i.e., shutting down the machines. As part of the rules, students are required to conduct normal activities as well as security-related activities when the Cyber War takes place. The total length of the Cyber War lasts three weeks and the following tools and 'tricks' are involved:

- Trojan horse [20, 21] - A Trojan horse is usually implemented as a server in a client/server system. A Trojan horse server must be executed prior to a client. When the victim accidentally invokes the Trojan horse server program, a client program can be executed at any remote host to communicate with the server. As a result, even the victim's screen can be displayed on the hacker's monitor. In the specific version used in the class, the password file also becomes accessible. In Figure 2, a client program is looking for a Trojan Horse by scanning a range of IP addresses specified by a user, i.e., the hacker. As you may notice, this Trojan Horse client program with a Chinese user interface was downloaded from a Chinese web site that is kept anonymous in this paper. When a Trojan horse client program searches the IP addresses between *144.26.71.1* and *144.26.71.255*, the port number 7626 is found that it is currently used by a Trojan horse server running on the PC with the IP address *144.26.71.246*.

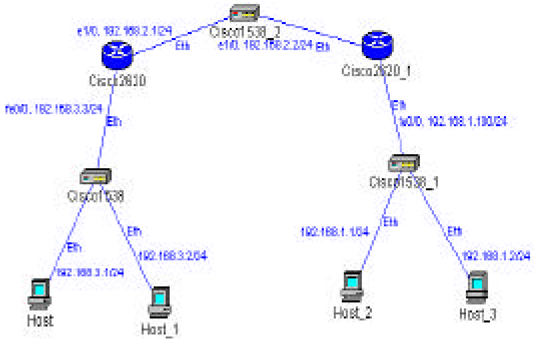
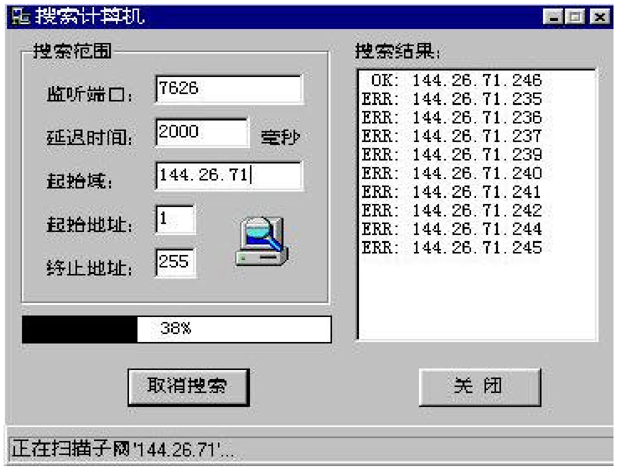


FIGURE 1
The Configuration of the Cyber Security Lab



搜索范围

监听端口: 7626

延迟时间: 2000 毫秒

起始域: 144.26.71

起始地址: 1

终止地址: 255

38%

搜索结果:

```
 OK: 144.26.71.246
ERR: 144.26.71.235
ERR: 144.26.71.236
ERR: 144.26.71.237
ERR: 144.26.71.239
ERR: 144.26.71.240
ERR: 144.26.71.241
ERR: 144.26.71.242
ERR: 144.26.71.244
ERR: 144.26.71.245
```

正在扫描子网'144.26.71'...

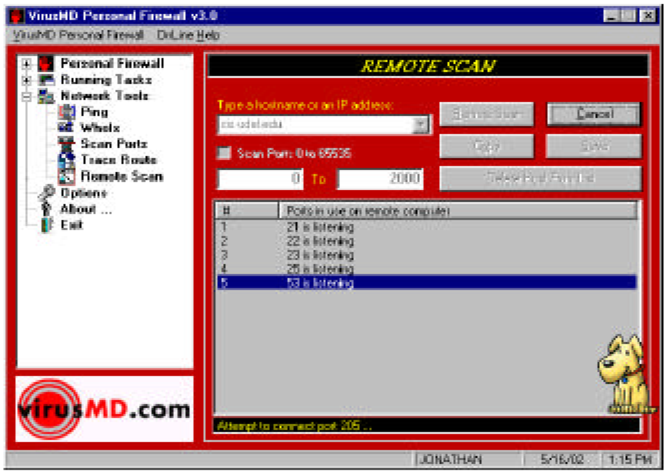
FIGURE 2
A Trojan Horse Client Program

- Web account password cracking tool - A program obtained from the Internet is used in the class to 'steal' the password from a *yahoo* e-mail user. As a user of this e-mail system, one needs to enter the user id and a password. It seems to be fairly secure to enter a password. But there is a way to go around the system. Usually, a web server provides a supplemental procedure just in case a user forgets the password. The normal procedure that *yahoo.com* provides requires one to enter a user id and then the birthday, and a secret sentence. All these seemingly secure procedures turn out to be surprising. A tool students downloaded from a web site can be used to guess the birthday and even the answer to secret sentences. After a user's id and the password are stolen, the hacker can use some remote executable commands to logon to the accunt remotely using a ‘net use’ command, copy a Trojan horse server program onto the machine using ‘copy’ command, and then assign the scheduled execution time using ‘at’ command. All these commands can be executed

المنارة للاستشارات
www.manaraa.com

remotely. The victimized user may not even be aware of the fact that this account has beeb intruded.

- Sniffer [10] - Usually, a sniffer is used as a software tool for monitoring the network traffic on a network system. However, a sniffer can also be used as a tool for hacking Intranets connected by hubs. Some sniffer provides connection information such as TCP connection packets and byte counts, interface statistics; others monitors TCP/IP traffic and filters out information in various format.
- Service level network protection tool [14, 15, 17, 19] - A firewall is considered one way to defend a LAN from outsider's hacking. During the Cyber War, students experience the actual operations and effects of installing a firewall. However, it is not a 'silver bullet'. Some well-known ports must be kept opened to the outside world and are subject to hackers' attack. Blocking some ports also prevents a user from accessing a system remotely using these ports. As an example of a personal firewall, VirusMD [19] provides features such as: port scan, application status report, etc. It can be downloaded for free from the Internet. Figure 3 shows a window when VirusMD is running a port scan under Windows 98. It is remotely scanning ports specified by a user and reporting the status of each port.
- Vulnerability analyzing tools - Some tools can provide information about the vulnerability of a system. *CyberCop* by Network Associates [8] provides this kind of information. It can be used to proactively detect the 'holes' in a system that can be vulnerable to hackers' attacks.
- Trojan horse prevention tool [16, 18] - On a college campus network, all users are allowed to use any computer as long as a valid user id and a password are available. This makes it difficult to prevent from Trojan horse attacks. However, one conservative solution is to delete all non-standard software from any PC after a user logs out of the account. A software tool that does this is called Deep Freeze [16]. However, this approach is still not flawless. For example, a system is still vulnerable if a user leaves a computer unattended, the user clicks on an icon while accessing a web site, or a user clicks on an attached file without knowing what may occur.



Type a hostname or an IP address:

□ Scan Ports 0 to 65535

0 To 2000

#	Ports in use on remote computer
1	21 is listening
2	22 is listening
3	23 is listening
4	25 is listening
5	53 is listening

Attempt to connect port 205 ...

FIGURE 3
A port scan operation in progress

EXPERIENCES LEARNED

This course was offered the first time in Spring 2001 without discussing information security issues. It was offered in Spring 2002 with an emphasis on information security issues. Some experiences have been learned. They are listed as follows:

1. The approach to integrate information security with internetworking is demonstrated to be a feasible approach for teaching information security especially when it is offered at its early stage. Later, the internetworking component in this course can be flexibly reduced after more security-related material becomes available.
2. In terms of evaluation, students are required to submit a Cyber War Plan prior to the beginning of the cyber war. Hence, students can have clear ideas on how to proceed during the cyber war. The cyber war plan must include, but is not limited to, the objectives of the software (either defense or attack), the location where the software is obtained, detailed steps on how to perform the defense or attack, and expected results. At the end of the cyber war, students amend their war plan with results, explanations, and limitations of the software.
3. Once the cyber war begins, students physically experience the phenomena that they have very little experience on. For example, screens on another PC are displayed on a hacker's PC, an invisible password suddenly become visible, etc. The computer lab can become a zoo without proper supervision and control. It is essential that an instructor still has a complete control of the whole lab. In particular, the instructor must keep track of the activities and remind students

المنارة للاستشارات
www.manaraa.com

to clear all Trojan horses, for example, after the Cyber War is over.

4. One of the most astonishing facts is that hacking tools are so inundated that anyone can easily obtain a hacking tool from the Internet and use it to attack others. It seems so hopeless when one attempts to secure an 'open network' (such as those in many school campuses). However, there are ad hoc techniques for defending against any known problems if the problems are detected. A possible dilemma is that one can become aware of a hacker's attack only after the system has been compromised.
5. We claim without a proof that there is no single solution for defending a computer against all hacking schemes. One can only hope that a series of policies, tools, procedures, etc., collectively can scare hackers away. For example, a simple logging history for every host in an open computer lab can be used to trace back who may have been a culprit for a Trojan horse attack.
6. Either the top-down or the bottom-up approach is not flawless when teaching the internetworking with TCP/IP. A 'tunnel drilling' approach is attempted. It serves the purpose of teaching internetworking with the emphasis on security in a more natural fashion.
7. Students appreciate some hands-on labs as well as lectures. The lab experiments not only reflect the theories, but also provide some invaluable experience. For example, some may not truly understand the purposes and the difficulty to configure two PCs running either Linux or Windows to form a LAN until actual connecting two PCs and using the services, i.e., file sharing and printer sharing.
8. Finding a textbook that incorporates security into internetworking is not an easy task. Many textbook authors usually cover the concepts of TCP/IP suite and the internetworking devices. As the major goal is to design and interconnect various LANs in a secure fashion, it requires supplemental teaching material to cover information security issues.
9. In each lab experiment, students form a team of two to four students (no more than 5 students). A direction is provided to students to specify what needs to be done and how each step must be performed. During the lab experiments, students interact with each other. Some students who have some experience on some of the lab experiments can volunteer to provide help to others. Although the teaching/learning style deviates from the traditional or classic style of teaching, students and teachers alike all appreciate the learning and teaching experiences.

SUMMARY

In this paper, the revisions on the 'Internetworking with TCP/IP' course are discussed to incorporate information security issues as the major goal of the course. The course content and the lab experiments including a cyber war are described. The major changes underline the importance of information security and teach students to become sensitive about these issues. Also, students experience a cyber warfare first-hand without causing real damage on systems using an isolated Cyber Lab. In the future, this lab facility will be enhanced to connect to the campus network and install a firewall on one LAN and not on another for testing the effectiveness of a firewall. In the future, the percentages of internetworking and information security can be flexibly adjusted depending on students' reactions.

ACKNOWLEDGEMENT

The author would like to thank all students enrolling in the internetworking and security course for participating in the cyber war with a malice-free attitude. They are Yuhong He, Lakshmi Mallaiah, Shru Medisetti, Brahim Medjbevr, Jatinder Singh, Suresh Venkannagari, Shubhra Vedanti, and Yuchen Zhou. The author is also indebt to the anonymous referees for reviewing this paper and providing constructive comments.

REFERENCES

[1] Comer, Douglas E. , "Internetworking with TCP/IP," Vol. 1, Prentice Hall, 2000.
[2] Anonymous, "Maximum Linux Security," Sams, 2000.
[3] Chirillo, John, "Hacker Attacks Revealed," John Wiley & Sons, Inc., 2001.
[4] Hatch, B., Lee, J., and Kurtz, G., "Hacking Linux Exposed: Linux Security Secrets and Solutions," McGraw-Hill, 2001.
[5] McAfee Anti-Virus, Network Associates, www.networkassociates.com (5/13/2002).
[6] Peter Davis+Associates, http://www.pdaconsulting.com/Audit.htm (5/13/2002).
[7] System Scanner, available at http://www.iss.net (5/13/2002).
[8] SFProtect-Mobile, available at http://www.agilent.com (5/13/2002).
[9] AdvancedChecker, available at http://www.trustedsystems.com (5/13/2002).
[10] Sniffer Technologies, available at http://www.nai.com (5/13/2002).
[11] NAT, available at ftp://ftp.technotronic.com (5/13/2002).
[12] IP Network Browser, available at http://www.solarwinds.net/Tools/ (5/13/2002).
[13] Port scanner, http://www.sdesign.com/securitytest/index.html (5/13/2002).
[14] Firewall, available at http://www.arrowtop.com/home.asp (5/13/2002).
[15] HackerShield, available at http://www.bindview.com (5/13/2002).
[16] Deep Freeze, available at http://www.deepfreezeusa.com (5/13/2002).
[17] ZoneAlarm Pro, available at http://www.zonelabs.com (5/13/2002).
[18] TrojanTrap3.exe, available at http://www.tinysoftware.com (5/13/2002).
[19] VirusMD Personal Firewall, available at http://www.virusmd.com (5/13/2002).

www.manaraa.com