DESIDOC Bulletin of Information Technology , Vol. 25, No. 5, September & November 2005, pp. 11-16

A Model Curriculum for Security Aspects in IT Education

Ashwani Kush & Sawtantar Singh

Abstract

Security has become a primary concern in order to provide protected data transfer in all networking environments. An internetwork security-teaching laboratory course, which includes both defensive and offensive security laboratory experimentation, is proposed here. This proposed laboratory will be oriented towards an introductory internetworking security class and is intended to complement more theoretical network security classes while motivating student interests and industry needs. The laboratory will be unique in that it uses an isolated laboratory network that attempts to represent the internet as closely as possible to typical educational laboratories which use only a few physical computers with virtual machines. It is also suggested that all of the laboratory assignments should be made available on internet for general community use and modification. General community expects solution from trained IT-professionals with respect to planning, configuration, implementation and maintenance of secure system for data transmission. Proposed study is an attempt in that direction.

1. INTRODUCTION

In the modern era of interconnected world, secured communications are needed for business (e-commerce activities), government (e-government activities) organisations and customers or citizens (e-services) to benefit from the advancements that the internet (networking) is empowering. The information security is important as the Government and business are now increasingly becoming dependent on information technology (IT). Secured information and protected infrastructure from malicious interventions is need of the hour. The organisations have access to sensitive and sometimes even secret business/government information. One of the first things to do is to build an organisation security policy to ensure that safe transactions are conducted in routine business[1]. Information assurance and infrastructure protection is a national priority as well as a complex and critical challenge.

The possibility of having organisation's data exposed to a malicious attacker is increasing exponentially. The main reason for this is the high number of `security illiterate' users. Many of the end users are not even aware of what is the meaning of network-security. Even qualified IT professionals from universities, engineering colleges and technical institutes are paying little attention to information security. The educational institutions should start security awareness programme[2] to define and outline the specific role of each of the employees in an effort to secure critical organisation assets, as well as covering each of the core elements pointed in a good security policy. In order to complement the highly theoretical security courses in various disciplines that exist in professional computer diploma, degree and postgraduate courses, a new scheme has been proposed for a laboratory based class. The proposed scheme allows student to be exposed to the real world challenges of network security. The academic institutes have conducted several seminars on information security but there have not been concrete suggestions to implement information security course in academic institutions. There is need to setup laboratories and develop associated laboratory materials, where the students could learn penetration testing techniques, hardening networks against attacks, and logging/audit controls for the purpose of convicting hackers. In international scenario many groups have explored methods of teaching information security. The pedagogical issues related to designing and implementing a cyber warfare laboratory for a computer security course have already been put into exercise[3] on virtual machines. [4, 5]

In this paper the proposed teaching laboratory model builds on the previously discussed methods of teaching and also adds unique elements that help build a teaching environment that approaches a real world laboratory that is both fun and inspiring students. In order to strengthen laboratory design, it is important to understand the industry's best practices and latest developments. There are several organisations that are making important contributions to the network security community and are useful resources in identifying network security laboratory components and teaching.[6,7,8] These organisations contribute to the community in various ways from informing security professionals of the latest alerts to offering free material on information security related topics.

2. NEED FOR COMPUTER SECURITY COURSE

In universities and technical institutes around India, most of the computer science/application graduates go directly to workplace after completion of their degrees/diploma courses. The academic syndicates of the educational bodies try their best to include practical topics to supplement the traditional computer science curriculum. But in these professional courses maximum stress is laid on general education and the practical approach is less used. As the demand for qualified IT security personnel (having certified trainings) is growing, most of the time, these IT professionals need to enroll for certified security training courses or the organisations hiring these professionals need to train them which involve efforts, time and money. With increasing trend in use of e-resources, this trend is getting upwards day by day.

3. PROPOSED SCHEME

In this article a scheme has been proposed to take care of security needs of the industry in general and student curriculum in particular. The scheme is a blend of theoretical and practical course work and tries to achieve the goal of supplying trained security professionals in IT. The proposed scheme intends to prepare certified trained security professional for network solutions. Proposed scheme has been divided into 4 layer structure as shown in Table 1.

Table 1. 4 Layered Structure

Hardware support requirements
Software support requirements
Testing and certification
Application in market

3.1 Hardware Requirements

A general hardware setup is required for lab set up. High powered server and 15 to 20 nodes should suffice the purpose for a group of 20 students. Server needs to support all platforms in terms of operating system and all protocols to connect it via LAN or internet.

3.2 Software Requirements

Table 2 shows the goals, and tools used in some example laboratory assignments. The laboratory exercises should be made available online which can be taken after modification.

3.3 Testing and Certification

The course curriculum for internet work security course includes almost all relevant topics. Some background in system administration and computer network is necessary. A basic knowledge of computer security features like firewall, intrusion detection, Trojan horse, Denial of service, Authenticity, Cryptography[9,10,11] should be prerequisite requirement for entry level to such a course.

The trainees can use the Computer Oracle and Password System (COPS), Netcracker and Network Security Scanner (NESSUS) tools[12] to locate opportunities for mischief on other people's systems, it is important that they understand why breaking into computers and disrupting computer operation is both illegal and unethical. The laboratory exercises will be developed where students work in teams to secure a computer system and then try to gain access to other systems present in the network, including the systems used by

Table 2. Goals and objectives and the tools used in some example laboratory assignments

Laboratory Exercises	Goals (including detection and countermeasures)	Software (used to support these goals)
1	Operating system installation, network reconnaissance, network mapping, and vulnerability assessment	VmWare, CheopsNG, nmap, nessus, SuperScan, Sam Spade
2	Password cracking, sniff network connection between computers, Man-in-Middle attacks	L0phtCrack, John the Ripper, ethereal, nmap, hunt
3	Falsifying identity on a network, Denial of service, detection spoofing	DNSspoof and dsniff, arpwatch, datapool
4	Buffer overflows vulnerabilities in software	Programs in C/C++ language
5	Rootkit methodologies for regaining access to systems once compromised and methods of detecting rootkits	Irk4, Knark, Kern_check, chkrootkit, sterace, rootkit Hunter, Hacker Defender
6	Back doors and Trojans for compromising systems	Netcat, icmp-backdoor, Virtual Network Computing, Back Office
7	Honeynets and forensics	AIDE, Scan of the month Challenge, FIRE, Coroner's Toolkit, Autopsy, Sleuth Kit
8	Firewalls	Linux firewall iptables, Zone Alarm, Cisco PIX Firewall
9	Worm fundamentals, proliferation techniques, and spreading rates	Self written worm, annakurikova
10	Wireless security, cracking WEP keys	Kismet, airsnort
11	Virtual private network security	SSH VPN in Linux, IPSec VPN using a Cisco VPN Concentrator
12	World wide web vulnerabilities	WGET, Nikto
13	Capture flag network security exercise	Attack & defend using all tools & techniques

other teams. In the first part of the course, the students should be able to handle exercises to demonstrate cumulative understanding of various security issues, strategies and tools.

Some of the tools to be used are: General information gathering (ping, traceroute, finger, whois, nslookup/dig, arp, netstat, etc.), Packet sniffing (tcpdump, ethereal), Password cracking (johntheripper, 10phtcrack), Cryptography (PGP), Port scanning (nmap), Vulnerability assessment (nessus, chkrootkit) and Intrusion detection (snort), etc. It is expected that by the end of the course students will be fairly well aware of the issues and representative tools used in security scenario. The main reason for realistic network architecture is to provide the infrastructure for challenging complex security issues. Though it is possible to accomplish the laboratory assignments with few (less than 10) machines but studies show that using more complex network enables many more possibilities and interesting exercises.

The purpose of the course, the lab exercises during the course, and the cyber war exercises at end of the course is for the better understanding of defence and design of computer systems and networks through the study of both attack and defence strategies. It is also ethically important to stress that attack strategies are important to understand from a defensive standpoint. The goal of the cyber war lab exercise is to give students further experience with the major issues, strategies and tools involved in computer security and to see how they synthesized the information presented earlier in the course.

Figure 1 represents existing course work based on four major scales in four areas as shown on right side panel. Figure 2 shows the proposed theme which is more practical oriented.

Specifically achievements should cater to the following:

- ❑ Real-world team based experience with system defence in a live environment
- ❑ Exposure to attack in order to better understand the strategies, tactics and mindset of the attacker, and to be able to respond defensively in a real time environment
- ❑ Experience with technological, physical and social engineering security.

3.4 Application in Market

The computer security course itself is a combination of lecture and laboratory exercises developed to build exercises in both security concepts and particular tools. The benefits of a laboratory component for a computer security course have been noted repeatedly from SIGCSE bulletins (vol nos. 32, 33, 34 and 35). The benefits of this certifications course will include: expertise and competency recognised by the industry, government and academia if adopted by the university, engineering colleges along with benefit to profession, organisational gain and personal gain. In the society where networking is increasing in an exponential phase, the need for security professionals will rise in abundance. The only trained professionals can suffice the need of the networking solutions. So the proposed

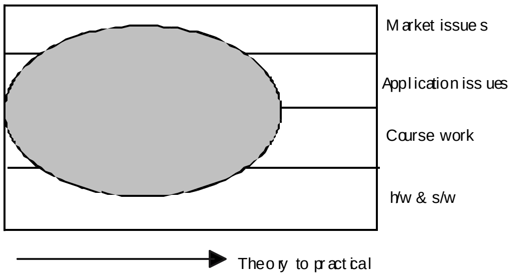

Figure 1. Existing course work

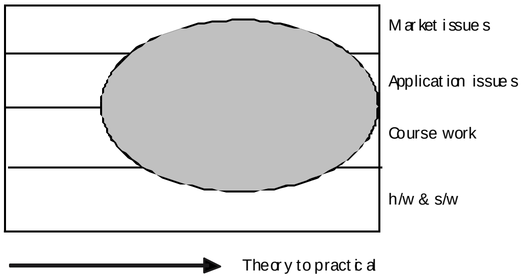

Figure 2. Proposed course work

scheme is going to have tremendous potential in the market of IT. Department of Telecommunication aims to achieve the target of internet subscribers from current 3-4 million to around 90-100 million by 2020. Table 3 shows the targets in years to come.[14,15]

This much growth will lead to more and more security problems and need for trained security professionals.

CONCLUSION

Having a totally isolated information security laboratory where students are allowed to launch attacks and attempt to defend against them is highly educational and motivating. Students hardening their machines and network and then seeing them compromised will be better prepared to understand how to prevent similar compromises in the future and in the real life scenario. The laboratory gives exposure to realistic network background traffic, access control lists, firewall rules, network address translation, etc. In a network of the complexity presented here, system teaches valuable operational issues that theoretical and simpler laboratory implementations never encounter. This should prepare to make the IT professionals face the challenges in information security. The universities, engineering colleges, and polytechnic colleges should take initiative to start network security courses with more than 80% of the course stress on practical exposure as being suggested in this proposal. The training curriculum for computer security course should include awareness, education, training and certification. This course can be a part of the other professional degree/diploma course and can be started side by side as vocational training programme.

REFERENCES

1. Singh, A. Girdhar. Building and implementing a successful information security policy. *In* Proceedings of National Seminar on e-Security at Guru Teg Bahadur Khalsa Institute of Engg & Technology, Malout, India, 26-27 May 2004.
2. Singh, S. & Singla, S. Building a security awareness program. *In* Proceedings of National Seminar on e-Security at Guru Teg Bahadur Khalsa Institute of Engg & Technology, Malout, India, 26-27 May 2004.
3. Wagner, P.; & Wudi, J. Designing and implementing a cyberwar laboratory exercise for a computer security course. *In* Proceedings of 35th SIGCSE Technical Symposium on Computer Science Education, Norfolk, Virginia, 2004, pp. 402-06.
4. Ragsdale, D.; & Dodge, R. A virtual environment in IA education. *In* Proceedings of 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY, June 2003, pp. 17-23.
5. Hill, J.; Carver, C.; Humphires, J.; & Pooch, U. Using an isolated network laboratory to teach advanced networks and security. *In* Proceedings of 32nd SIGCSE Technical Symposium on Computer Science Education, Charlotte, North Carolina, 2001, pp 35-40.
6. SANS
   www.sans.org
7. CERT Coordination Centre
   www.cert.org
8. Insecure.org
   www.insecure.org

Table 3. Internet and broadband users' targets

Year ending	Broadband subscribers target	Penetration	Internet subscribers target	Penetration
2005	3 million	0.3 %	6 million	0.6%
2010	20 million	1.7 %	40 million	3.4%
2020	32-40 million	4-5%	90 million	10.0%

215-28.

9. Stephen, N. Network intrusion detection: An analyst's handbook. New Riders, 1999.

10. Dieter, G. Computer security. John Wiley & Sons, 1999.

11. Dennis, G. & Hal, C. A firewall configuration strategy for the protection of computer networked labs in a college setting. *Journal of Computing in Small Colleges*, 2001, **17**(1), 181-87.

12. Frank, C. & Wells, G. Laboratory exercise for a computer security course. *Journal of Computing in Small Colleges*, 2002, **17**(4), 51-54.

Contributors: **Sh. Ashwani Kush,** Department of Computer science, Kurukshetra University, Kurukshetra.

Sh. Sawtantar Singh, Punjabi University, Guru Kashi Campus, Talwandi Sabo, Bathinda.