Virtual Learning Tools in Cyber Security Education

Dr. Sherly Abraham
Faculty Program Director IT and Cybersecurity

Dr. Lifang Shih
Associate Dean

School of Business & Technology,
Excelsior College
Overview

- Importance of electronic training for Cyber security education
- How technology can be used to enhance the learning process
- Interactive tools that can be used for identifying security threats
- Application of practical labs in mastering core technical competencies in Cyber Security
Cyber Security Online Education

- Professional Workforce
- Shortage of Workforce in Cyber Security
- Overcome the limitations of time and distance
- Evolving landscape of Cyber Security threats
- Bachelor’s degree is a common requirement for most cyber security related positions
Cybersecurity Jobs Report

- Maryland Cybersecurity Job Breakdown

Entry-level to mid-level positions requiring a Bachelor’s degree dominate cyber security job openings. However, there are plenty of opportunities for high school graduates to engage.

Figure 4: Education and Experience Breakdown

Background

- Excelsior College founded in 1971 (previously Regents College)
- 1998 Private, independent
- Large student body (approximately 33,000 students)
- Distance education, flexible learning format

**Philosophy:**

“What you know is more important that where or how you learned it”
Background

- A student centered adult learning model
- Cybersecurity Accreditation
  - CNSS (Committee on National Security Systems)
  - CAE/IA (Center for Academic Excellence in Information Assurance Education) – Pending Approval
  - Middle States (all programs)
  - ABET (specialized accreditation - Technology)
  - IACBE (specialized accreditation – Business)
Degrees Offered in Cyber Security

- Bachelor of Science in IT with Cybersecurity concentration
- Bachelor of Science in IT with Information Security concentration
- Master of Science in Cybersecurity
- Masters of Business Administration with a concentration in Cyber Security Management
- Undergraduate Certificate in Cyber Security
- Graduate Certificate in Cyber Security Management.

The programs offers an assortment of courses that focuses on technical, managerial, communicative and soft skills in developing an effective workforce to meet the challenge of next generation cyber security professionals.
Educational Methods Employed

Interdisciplinary Approach

- Discussion Questions
- Group Projects
- Case Studies
- Interactive activities
- Virtual Labs
Interactive Activities

- Provides learners with feedback
- Repetitive Learning
- Interesting
- Thought Provoking
Introduction:

Cryptography focuses on the many techniques that can be used to implement secure and trustworthy communication between two communicating parties. The concepts and implementation of cryptography is complicated and requires a large amount of complex programming. In this course you will learn about some of the basic definitions of cryptographic methods. You will now engage in learning some of the basic definitions of concepts in cryptography. It is important to ensure that you clearly understand the concepts highlighted in this activity as it will provide you with a foundation on further learning the concepts of cryptography.

Basic Scenario for Cryptography

Figure 8.1: The basic scenario for cryptography. Alice and Bob encrypt their communications so that the eavesdropper Eve, can’t understand the content of their messages.

Figure: Goodrich and Tamassia (2011)
Cross Word Puzzle

To complete the crossword puzzle, choose from the following list:

- Cryptography
- Cipher Text
- Encryption
- Decryption
- Cryptographic Key
- Symmetric Cryptography
- Asymmetric Cryptography

Solve the crossword puzzle:

Across:
1. Enables two communicating parties to communicate securely even if their messages are accessed by an eavesdropper
2. The process of changing the cipher text back to readable format
3. The unreadable format of text created as a result of the cryptography process
4. Two keys are used, one for encrypting and one for decrypting

Down:
1. Two keys are used, one for encrypting and one for decrypting
2. The process of changing the cipher text back to readable format
3. The unreadable format of text created as a result of the cryptography process
4. Two keys are used, one for encrypting and one for decrypting
CYS 526
Cyber Attacks and Defenses

- Methodologies, project management tools for penetration testing
- Assess target Systems and networks for vulnerabilities
- Detect security threats
- Recommend and implement defensive, corrective, and preventative measures based on penetration test results.
A person stumbled upon a distributed denial of service (DDoS) application from a peer-to-peer file-sharing source. He/she downloaded the application and decided to launch it against his or her bank’s website to see what it did.

Q What type of hacking is this?

- Black hat
- White hat
- Gray hat
Penetration Testing Guidelines

Pen Test Guidelines

You are an experienced pen tester who has been hired to conduct a security audit of a web server with a backend SQL database.

Q Which guidelines will you choose to complete the audit?

Enter your answer and click Submit to compare it with expert feedback.
Identifying Type of Attack Based on Characteristics

Vulnerability Identification

In this activity, you will identify the type of attack based on the information and image provided in the scenarios.

Enter your answer and click Submit to compare it with expert feedback.

Q2 A program was forced to attempt to execute more data in a buffer than it holds

Microsoft Visual C++ Runtime Library

Buffer overrun detected!
Program: C:\WINDOWS\explorer.exe

A buffer overrun has been detected which has corrupted the program’s internal state. The program cannot safely continue execution and must now be terminated.

OK
Identifying Type of Attack Based on Characteristics

Is Someone Watching You?
Individuals or companies can monitor what you do on your computer using "spyware" programs that they secretly install on your computer. How can you tell if your computer is being affected by spyware?

A. Look for signs of tampering, such as a missing back panel on your computer, or miniature microphones or cameras hidden nearby.

B. Watch for odd computer behavior - such as a barrage of pop-up ads, a browser that takes you to sites other than those you type in, changes in your home page or toolbars, non-working keys, or slow performance.

C. Look on your computer for any file whose name contains the word "spyware." It may have an icon that looks very similar to others.
Virtual Lab Activities

- ToolWire
- EC Virtual Environment
  - Experimental learning environment
  - Hands on learning
- Simulates practical environments
EC Virtual Environment

- VMWare Version 5 ESXi hypervisors
  - Hewlett Packard Server Blades
- Dedicated to courses in Cybersecurity
- System
  - 12 Fedora Core 14 64-bit Linux systems
  - 12 Windows Server 2008 R2 64-bit systems
  - 12 Windows 7 Professional 64-bit systems
CYS 501
Communications Security

- Network security fundamentals
- Security policies, networking threats, and technologies
- Design and implementation of secure communications networks
- Network Management and Scanning
- Device hardening, encryption, proxies, firewalls, VPN and remote access design, NAT, DHCP, VoIP
- Honeypots, intrusion detection systems (IDS), and other network defenses are examined.
Network Vulnerability Assessment

• Tools
  • NMAP
  • Nessus

• Analysis
  • Operating systems and service packs
  • Ports and Services
  • Compare the security level of the different systems
  • Compare the functionality and features of NMAP and Nessus
Securing Network Devices

- Firewall
  - Location of firewall on the network
  - Configure to defend
  - Permit and deny traffic
  - Set rules
### Firewall: Rules

<table>
<thead>
<tr>
<th>Lan</th>
<th>Way</th>
<th>Proto</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Gateway</th>
<th>Schedule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Allow All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pass</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>block</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>reject</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>pass (disabled)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>block (disabled)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>reject (disabled)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>log (disabled)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Firewall Configuration
Honeypot

- Honeynet Project
  - https://honeynet.org/project

- HoneyBOT

- Valhala Honeypot
  - http://sourceforge.net/projects/valhalahoneypot/
Virtual Lab Design

Configure as honeypot
Configure Honeypot as a Web Server
Web Server
Activities

- Connect to the honeypot from the landing VM
- Conduct an NMAP scan
- Review logs and analyze the details effectiveness in detecting malware activity
- Assess the effectiveness of honeypots
CYS 526 Cyber Attacks and Defenses

- Students will learn to assess target systems and networks for vulnerabilities and exploits, detect security threats, and recommend and implement defensive, corrective, and preventative measures based on penetration test results.
VMs used

- Windows 2003- Landing VM
- Security Onion- Intrusion Detection
- Windows XP Pro- Target System
- WebGoat- Web Application Hacking Lab
- BackTrack 5- Attack System
Active and Passive Info Gathering

- Web Recon
- Identify live hosts using ICMP ping command
- Identify open ports
  - Telnet, NetCat, NetDiscoverer
- Identify ports running services
  - Ports, running services, MAC address, OS
- Advanced NMAP operations
  - NULL Scan
  - XMAS Scan
  - SYC scan, OS scan, probe open ports
Exploiting a Windows target with Metasploit

- Establish Connectivity
- Armitage
- Discover attacks against target
- Research the Hail Mary attack
- Launch the Hail Mary attack
- Meterpreter
  - Getuid, getprivs, getsystem, hashdump
Hail Mary Vulnerability Attacks
Maintaining Access

- Netcat/CryptCat for File Transfer and Backdoor
  - Setup communication between systems
  - Use NetCat/CryptCat to setup communication
  - Wireshark act as network sniffer
  - Use NetCat to setup a backdoor with root access to access BT5 from Security Onion
Virtual Lab Setup

Figure 1: The lab setup with Wireshark

BT5 sends content of FILE.TXT to SO

WireShark sniffs all traffic between BT5 and SO
Lessons Learned

- Use of NetCat, Wireshark
- Maintaining access to a target during pen test
- Importance of encryption
- Functionality of backdoor
De-Ice Disk 1.100 Ethical Hacking Challenge
Rootkits and Defenses

- Hacker Defender rootkit
- Install rootkit
- Hxdef100.2INI
- Analyze and report on
  - Hidden services
  - Hidden Regkeys
  - Password to access the victim with infected rootkit
Execution of the Hacker-Defender rootkit:
Rootkit countermeasures: Black-Light
Conclusion

- Online Education
  - Overcome the limitations of distance and time
- Cyber Security field requires technical and soft skills
- Learning environments to implement technician skills
  - Interactive tutorials
  - Virtual tools
  - Discussions
  - Case Studies and Group Projects
Questions

Dr. Sherly Abraham
Faculty Program Director IT and Cybersecurity
Sabraham@excelsior.edu

Dr. Lifang Shih
Associate Dean
Ishih@excelsior.edu

School of Business and Technology
Excelsior College
7 Columbia Circle, Albany, NY 12203-515