Journal of Information Technology Education: Innovations in Practice Volume 14, 2015

Cite as: Li, C. (2015). Penetration testing curriculum development in practice. *Journal of Information Technology Education: Innovations in Practice, 14,* 85-99. Retrieved from http://www.jite.org/documents/Vol14/JITEv14IIPp085-099Li1014.pdf

Penetration Testing Curriculum Development in Practice

Chengcheng Li
University of Cincinnati, Cincinnati, Ohio, USA

Chengcheng.li@uc.edu

Abstract

As both the frequency and the severity of network breaches have increased in recent years, it is essential that cybersecurity is incorporated into the core of business operations. Evidence from the U.S. Bureau of Labor Statistics (Bureau of Labor Statistics, 2012) indicates that there is, and will continue to be, a severe shortage of cybersecurity professionals nationwide throughout the next decade. To fill this job shortage we need a workforce with strong hands-on experience in the latest technologies and software tools to catch up with the rapid evolution of network technologies. It is vital that the IT professionals possess up-to-date technical skills and think and act one step ahead of the cyber criminals who are constantly probing and exploring system vulnerabilities. There is no perfect security mechanism that can defeat all the cyber-attacks; the traditional defensive security mechanism will eventually fail to the pervasive zero-day attacks. However, there are steps to follow to reduce an organization's vulnerability to cyber-attacks and to mitigate damages.

Active security tests of the network from a cyber-criminal's perspective can identify system vulnerabilities that may lead to future breaches. "If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. But if you know the enemy and know yourself, you need not fear the result of hundred battles" (Sun, 2013). Penetration testing is a discipline within cybersecurity that focuses on identifying and exploiting the vulnerabilities of a network, eventually obtaining access to the critical business information. The pentesters, the security professionals who perform penetration testing, or ethical hackers, break the triad of information security - Confidentiality, Integrity, and Accountability (CIA) - as if they were a cyber-criminal. The purpose of ethical hacking or penetration testing is to know what the "enemy" can do and then generate a report for the management team to aid in strengthening the system, never to cause any real damages. This paper introduces the development of a penetration testing curriculum as a core class in an undergraduate cybersecurity track in Information Technology. The teaching modules are developed based on the professional penetration testing life cycle. The concepts taught in the class are enforced by hands-on lab exercises. This paper also shares the resources that are available to institutions looking for teaching materials and grant opportunities to support efforts when creating a similar curriculum in cybersecurity.

Keywords: Cybersecurity, Curriculum Development, Penetration Testing, Ethical Hacking, Computer Networking.

Editor: Peter Blakey
Submitted December 9, 2014; Revised March 2, 11, and 13, 2015; Accepted March 15, 2015

Introduction

There has been a significant increase in the number of computer-related crimes over the past years. This is due to the pervasive availability of software tools designed for hacking into computer systems and penetrating data networks. Seventy-nine percent of the crimes that the FBI investigates are white-collar crimes in which computers are either the target of a crime or the means of committing a crime (Barnett, 2013). Cyberwarfare and cyberterrorism, considered myths a decade ago, are the hot topics of debate in political and military circles. Cybersecurity has become a core business function that plays a critical role throughout business processes. Yet there is a substantial number of unfilled jobs in networking and cybersecurity, both locally and nationwide. In early 2014, the National Institute of Standards and Technology (NIST) released the cybersecurity framework for private companies and infrastructure networks (NIST, 2014). The framework guides companies to defend their networked assets from hackers and cyber threats. "Cybersecurity" has been the dominant term, replacing "computer security", "digital security", "information security", "information assurance", and "online privacy", among government agencies and education and research communities.

The cybersecurity job is booming in many regions of the country. Holding a degree in cybersecurity can secure an IT graduate a job with a relatively higher salary than other IT entry jobs (Corbin, 2013; Dave, 2013). In addition, it is projected that there will be a 37% increase in the job market for cybersecurity analysts for the next decade, the highest job increase rate among all the IT jobs (Bureau of Labor Statistics, 2012). However, US higher institutions of learning are not preparing a sufficient number of students to build a workforce with the skills needed to fight future cybercrimes. In recent years comprehensive cybersecurity curricula have been proposed by individual institutions (Kessler & Ramsay, 2014; Luallen & Labruyere, 2013; Mishra, Romanowski, Raj, Howles, & Schneider, 2013) while the National Science Foundation (NSF) and the National Security Agency (NSA) work diligently promoting cybersecurity education by creating standards and assessment frameworks that regulate the cybersecurity curriculum development. An organization newly established for this purpose is the National Initiative for Cybersecurity Education (NICE). It developed the National Cybersecurity Workforce Framework that provides a common understanding of, and lexicon for, cybersecurity tasks (National Initiative for Cybersecurity Careers and Studies [NICCS], 2013). The NICE annual conferences are dedicated to gathering institutions with cybersecurity curricula to collaborate, learn, and promote K-16education, share available resources, and create innovative resources in various disciplines of cybersecurity.

In the meantime, the NSA and the Department of Homeland Security (DHS) redesigned the 2013 Center Academic Excellence in Information Assurance and Cyber Defense (CAE IA/CD) Program which provides a guideline for institutions to prepare a workforce to defend the Nation's networks (NSA, 2013). This program regulates higher education institutions, including 2-year colleges and 4-year universities that offer cybersecurity curricula, and designates these programs as the CAEs for improved collaboration and grant opportunities. NSA defined a set of Knowledge Units (KUs) as the criteria to evaluate the CAEs. These KUs are seamlessly mapped to the NICE Framework.

In the regulated cybersecurity curricula, strong analytical skills, mastery of fundamental operating systems and network operations are emphasized. On top of these skills, the students are exposed to a large number of open-source and commercial security tools that are used by both security professionals and the "black hat" hackers. More companies have come to realize that the traditional defensive security will eventually fail. Hackers can explore and exploit network and application vulnerabilities that have not been detected by the users, called "zero-day" attacks. It is estimated that the typical zero-day attack is detected an average of 180 days after the attack was launched. This means the current defensive mechanism will not detect the intrusion until after a great degree of damage has been done-- days, weeks, or even months before. In the recent Target

and Home Depot security breach cases, hackers accessed their targets' databases and retrieved millions of valuable user accounts more than six months before the problems were identified and fixed (Pritchard, 2014). A recent hacking on Sony Pictures Entertainment is suspected, not simply for financial gains, but as an act of cyberwar that promotes political agenda and possibly is led by an organized military intelligence team from an enemy country (Reisinger, 2014). We have to arm our workforce with the same techniques and tools that are used by the hackers and to fully test our system and fix problems before the hackers discover the vulnerabilities. A class that focuses on teaching ethical hacking concepts and techniques should be incorporated into the core of the cybersecurity curriculum in order to prepare the future professional pentesters. Perfect security does not exist; if it did, the security defense system would be extremely over-budgeted. This offensive security, combined with the traditional defensive mechanisms, is the ultimate and realistic solution to fighting cybercrimes.

In recent years, penetration testing (pentest) began appearing in the cybersecurity curricula at higher education institutions (Bechtsoudis & Sklavos, 2012; Falkenberg, Mainka, Somorovsky, & Schwenk, 2013; Hudic et al., 2012; Mainka, Somorovsky, & Schwenk, 2012). There are currently eighty institutions designated by the NSA as the CAE IA/CD. These institutions, including three levels of designations for two-year education, four-year education, and four-year research, are the leading institutions in the nation for teaching cybersecurity. However, fewer than twenty percent of these institutions offer a complete course on pentest (https://www.iad.gov/NIETP/). The main pentest curriculum development efforts came from professional training companies such as SANS, InfoSec, and EC-Council. For example, SANS created a pentest curriculum that consists of fourteen courses (SANS, 2015), and EC-Council has a popular certificate exam and training curriculum for ethical hacking. These curricula have excellent content with updated technologies and lab exercises; however, they were created for short-term intensive training for the field professionals, usually in a one-week boot camp format. Although EC-Council has a version of their ethical hacking curriculum that can be adopted by academia, the course content is outdated. There are insufficient efforts on creating, reporting, and sharing a pentest curriculum among higher institutions. It is now a good time to share the experience and resources of preparing and teaching a pentest curriculum.

The following sections introduce a pentest curriculum we developed as an upper-level undergraduate course. It is one of the four core courses in our cybersecurity track. Students have already taken system administration and network security courses before beginning this class. We developed effective learning modules, including fifteen pentest topics that train students with practical hands-on skills while helping prepare them for industry pentest certificates. There also is a large amount of open source software tools, a guideline of setting up a pentest lab environment, and the public learning resources this paper shares with the academic community.

The Pentest Curriculum Development

The Learning Modules

The prerequisites of the pentest class are system administration and network security courses, and it is one of four core classes in the cybersecurity track. This class is offered once a year, in parallel with the system/network forensics class and followed by an intrusion prevention and network monitoring class. This pentest course provides students ethical hacking tools to develop skills and techniques to identify host and network vulnerabilities. Course objectives are for each student to understand the scope of pentest and the responsibilities of performing these tests by following a strict code of ethics. Through hands-on lab exercises students learn to use a set of modern software tools to perform various pentest tasks on computer hosts and enterprise networks. Students,

therefore, are able to implement appropriate defense mechanisms to mitigate and remediate the identified issues. The designed learning outcomes are:

- Plan, organize, and perform penetration testing on a simple network
- Understand the ethical implications of penetration testing and the necessary organization-defined scope of engagement
- Understand the potential negative technical implications of penetration testing on existing network and systems infrastructure
- Understand the impact of, and defense against, social engineering attacks
- Understand families of attacks and flaws that lead to vulnerabilities
- Identify and properly utilize modern-day penetration testing tools such as NMAP, Nessus, Metasploit, and Social Engineer Toolkit (SET)
- Perform ethical hacking to identify host and network vulnerabilities

The learning modules are designed to follow a four-phase pentest life cycle as illustrated in Figure 1. There are nine learning modules taught in a typical 15-week semester. Additional skills and knowledge in legality, social engineering, programming, using pentest frameworks, and writing professional reports also are incorporated.

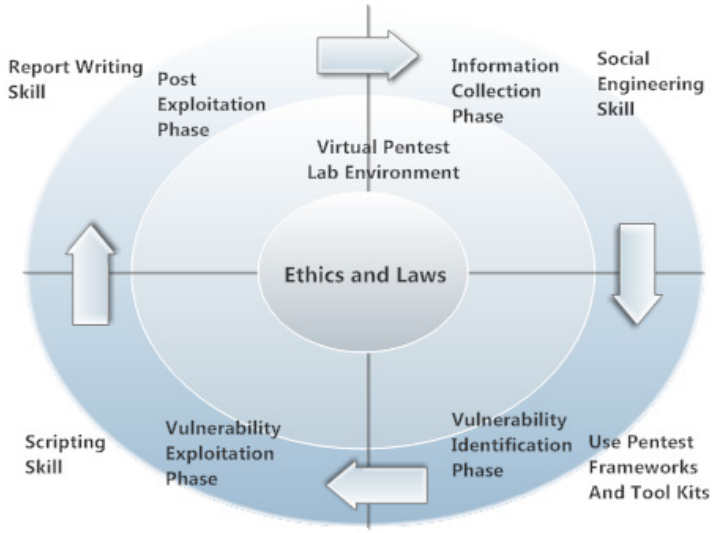


Figure 1. Penetration Testing Life Cycle, Knowledge Units, and Core Learning Components

Module 1. Ethics and Laws (Week 1): Ethics and legality are stressed as the main supporting element of pentest. Authorization and compliance with related laws distinguish pentest from criminal hacking. A code of ethics in IT is developed during the week to guide pentest tasks in the security lab and in the classroom. This week also includes studies of the laws, discussions, and writing essays.

Module 2. Get Familiar with a Pentest Lab (Week 2): The second module guides students to install a pentest lab environment on their personal laptops. A more comprehensive lab is installed on a "Sandbox" system which is a cloud-based VMware vSphere lab. There are eleven virtual machines (VM) preinstalled for each student in the Sandbox. The system is persistent, meaning students can use the VMs remotely any time during the semester and activities on the VMs can be saved permanently. In this week, students learn the interfaces of remote lab, launch the VMs in browsers, and test the connectivity of the virtual networks. Some of the VMs in the lab are pur-

posely unpatched or left with security hole and are used as the targets of pentest. To avoid security breaches of the Sandbox system, the lab VMs are connected in the local area network and are without Internet access. Therefore, all needed software is preinstalled in the Sandbox. The Sandbox system enables teamwork, collaboration, and in-class demonstration using real-time systems. The Sandbox also isolates the lab network from the university production network so the hacking tools and unpatched VMs do not impose security concerns nor leave vulnerabilities for hackers to exploit from the Internet. Students access the Sandbox using secure VPNs off-campus. A simplified version of a pentest lab is installed on student personal laptops, which consists of only two VMs, a Kali Linux, and a Victim VM for basic pentest tasks. All of our IT students are required to have a personal laptop with a minimum configuration of 4G system memory and 160G storage space. With these minimum requirements, students should have no problems hosting the 2-VM lab topology on their laptops.

Module 3. Collecting Information (Weeks 3-4): Hackers increasingly probe networks both actively and passively to evaluate the target systems. The information collection phase is arguably the most time and resource consuming phase of pentest.

Topic 1: Reconnaissance: In this topic students use various foot-printing techniques to collect information passively, such as the location, company profile, web presence archives, DNS services, and other information leading to the blueprint of the target network.

Topic 2: Network Scan: More passive and active scans are performed primarily through NMAP to reveal the target's network resources, operating system, and applications, leading to the discovery of the system vulnerabilities.

Module 4. Vulnerability Identification and Exploitation (Weeks 5-7): This module teaches students how to identify system vulnerabilities and then obtain access to the system.

Topic 1: Identify Vulnerabilities: The open ports and their associated applications, OS signatures, and shared network resources all can lead to the vulnerabilities already identified at the national database (Zhang, Caragea, & Ou, 2011), antivirus vendor websites, and hacker community public portals such as the Open Source Vulnerability Database (Kuo, Ruan, Chen, & Lei, 2012). Students learn how to identify these vulnerabilities using online information and special tools and frameworks such as Metasploit (Remirez-Silv & Dacier, 2007).

Topic 2: System Hacking: Successful exploiting the identified vulnerabilities lead to system breach. In this topic, students learn how to use the tools to sniff, dump, and crack passwords and to obtain the privileges of the system account. They also will manipulate the system files and cover their tracks to hide the hacking processes from being recorded by the system logs.

Topic 3: Spreading the Viruses: In this week students identify several strains of viruses, Trojans, and worms that easily invade a system through system hacking and social engineering techniques, launch denial of service and other attacks, and leave backdoors for future reentry.

Module 5. Post-exploitation (Week 8-10). This module teaches the techniques hackers use to cover their tracks, leave backdoors for reentry, and create pivot points to go deeper into the network for retrieving sensitive information from the databases and web applications.

Topic 1: Masquerade: Students investigate how different types of Intrusion Detection Systems (IDS) and firewalls are installed and configured so they can apply tools or try their hacking methods to evade the system defense systems. We used Snort IDS and iptables with basic configurations as the defense systems to test pentest evasion skills.

Topic 2: MITM and Session Hijacking: This topic teaches the methods to break, inject spoofed packets, and therefore hijack the existing communication between a victim machine and

a server. Through the lab exercises, the importance of data encryption is emphasized as an effective countermeasure.

Topic 3: SQL Injection and Cross Site Scripting: Web penetration testing is taught this week to attack poorly configured and programmed network services and applications. A selection of projects under the Open Web Application Security Project (OWASP) is used to teach and demonstrate the concepts and practices of web pentest (Wichers, 2013).

Module 6. **Framework and Tool Sets (Week 11)**: Pentest frameworks are developed to perform automated tasks and routines using the libraries of community contributed scripts, payloads, exploits, and encoders. Advanced and specialized pentest tasks can be easily and quickly launched by using the frameworks. This week exposes students to open source pentest frameworks such as Metasploit and special pentest Linux distributions such as Kali and Backbox. Rapid7, the company that makes Metaspoilt, has provided the professional versions of their commercial products to teach this module.

Module 7. Scripting (Week 12-13): Pentesters cannot rely on the open source and commercial tools to perform all the tasks. Specialized tests sometimes need tailored scripts for improved efficiency. In addition, pentest tasks can be highly automated through simple scripting. Scripting is a crucial skill for the security professionals.

Topic 1. Bash Scripting: Bash scripting also known as the shell programming is the critical skill that a pentester must master for proficiently maneuvering the target system once it is breached. This week students review and create basic bash scripts for system task automation.

Topic 2. Python: Students learn how to program Python scripts to accomplish basic tasks such as password cracking and network scanning. The most important objective of this week is not to teach the programming language but to teach the use of the available rich Python libraries and add-on packages for penetration testing and hacking activities.

Topic 3. Other scripting tasks: There are other scripting skills that are critical for pentest such as scripting the Metasploit payloads, automating a fuzzer to obtain abnormal system responses, and crafting a buffer-overflow attack. Demonstrations in these areas are conducted during this week. Students will conduct a hands-on practice to create their own scripts during the lab session.

Module 8. Writing Professional Pentest Report (Week 14): At this point students have already written more than 20 assignments and in-class group exercise reports. This topic focuses on how to prepare a professional pentest report, document the findings, and present them to the non-technical customers. Therefore, the customers can understand the business impact of the findings, justify spending to harden the network and meet the overall security objectives for business continuity.

Module 9. **Capture the Flag (Week 15):** A capture the flag (CTF) lab is created based on Metasploit and OWASP for students to practice and experience real-world pentest challenges. The CTF lab will be used to assess students' learning outcomes, specifically the hands-on skills of the pentester.

Lab Exercises

Hands-on exercises are a critical component of cybersecurity curricula. Many renowned pentesters and hackers did not have formal education in cybersecurity while at school because pentest only became a distinct IT discipline not many years ago. Pentest skills were learned and software tools collected or crafted through years of hands-on practices and problem solving. The lab exer-

cises created for this course cover every phase of pentesting and give the students an average of fifty hours of hands-on practice. There are twenty labs hosted on the Sandbox system using eleven VMs to simulate a variety of enterprise network topologies for individual hands-on lab assignments. Another portion of the hands-on practice is conducted in class as group projects. These exercises immediately reinforce the topics learned during the class and allow students to have a discussion while solutions to pentest tasks are provided.

There are two pods of VMs preinstalled for each student on the sandbox system and twenty lab exercises developed based on these VMs. Lab manuals with detailed step-by-step instructions are provided for the students to complete each lab. Students are required to write a report of each lab by completing the required tasks and answering an average of twelve questions per lab. One pod of VMs is adopted from the labs designed by the Center for Systems Security and Information Assurance (CSSIA). The CSSIA is a national center of excellence in cybersecurity education that provides excellent teaching material for a large number of Information and Communication Technology (ICT) courses (Twichell, 2006). Thanks to an NSF Advanced Technological Education grant, the CSSIA developed these high-quality pentest labs. The VMs used in these labs do not require Internet access because all the required software is pre-installed. After performing each lab exercise students restore the VMs to the stored initial states called "snapshots" for the subsequent labs.

A second pod consists of three VMs that include one pentest system and two target systems. This pod is more flexible in design; students can change the target systems between the standard OS and a collection of pre-configured vulnerable systems or pentest tools, such as Metasploitable 2, DE-ICE, OWASP VM, Kali, Backbox, and Security Onion, for both offensive and defensive security testing.

The in-class group exercises are conducted by groups of three students. Unlike the lab assignments, there are no step-by-step instructions except for lab requirements and limited hints. The students need to conduct research and discussion, work assuming different roles and responsibilities, complete the tasks as a group, and report their findings within the specified time limits. This is reportedly the most enjoyable class component voted by the students. The group exercise commonly starts after a one-hour lecture. The contents of the lab are directly tied to the lecture to reinforce the concepts covered. After the initial research and discussion, one student volunteers as the "researcher" who searches for the relevant information from online or in-class resources. A second student works as the "operator" who executes the commands and performs pentest tasks on the VMs. The third student works as the "auditor" who assists the operator, writes down the findings, and summarizes the tasks performed for drafting the report. Upon the completion of the tasks, they will have a team discussion and complete the report after the class.

The twenty individual lab assignments are from twelve CSSIA labs and eight in-house developed labs. Most of these labs employ open source tools and systems collected from the security communities. We use additional commercial tools provided by security vendors free-of-charge for educational purposes. A sample group exercise, developed in-house and used in week 10 on the topic of Session Hijacking, is shown below:

Lab Scenario: Students using the given VMs perform a man-in-the-middle (MITM) and session hijacking attack on a victim. The goal is to capture the user name and password on the victim machine that is used by the victim to access a secure web service, such as an online bank or an email service. The physical and logical lab topologies are shown in Figure 2.

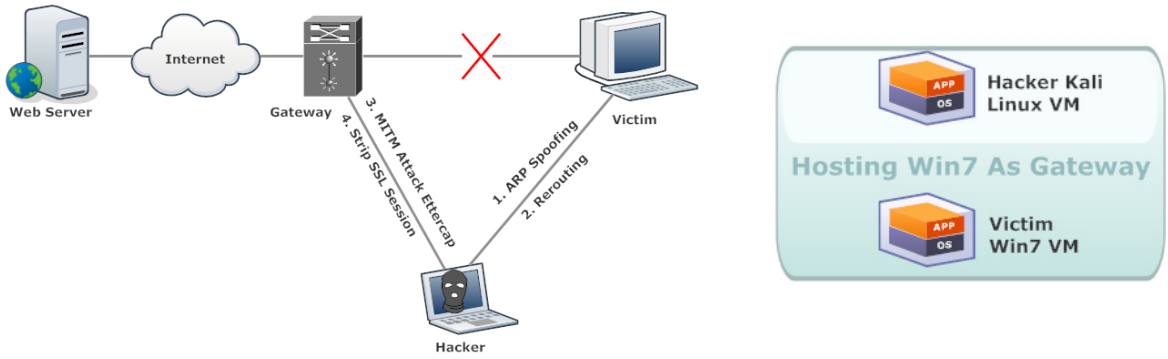


Figure 2. Logical and Physical Lab Design for the MITM and Session Hijacking Group Exercise

Requirements:

1. Create a MITM attack using ARPspoof from the Kali Linux. The Kali VM will masquerade itself as the gateway and take the traffic from Win7 to the Internet. Make sure the Win7 machine can explore the Internet through Kali. Show the captured traffic using Wireshark. (20 minutes)
2. Capture the SSL sessions of Win7's login information to a secure website such as ebay.com or gmail.com. You can create a temporary account for this exercise. (15 minutes)
3. Combine the functions of SSLstrip, Ettercap, and iptables to capture the login credentials. (15 minutes)
4. Write a report on the hacking process, lessons learned, recommended fixes, and screenshots of accomplished tasks. (30 minutes)

Topics covered: MITM, Session Hijacking, Routing, Linux Firewall

Tools used: Kali Linux, vi Text Editor, iptables, Ettercap, SSLstrip

Feedback

A student survey was conducted at the end of the semester. A list of selected questions is shown in Table 1. The standard Likert scales, ranging from strongly disagree to strongly agree, are used to provide the qualitative measures of student opinions. The result shows that almost all the student answers are in the "strongly agree" category. The class was offered as an upper level course in a newly established cybersecurity track where only three students had the needed prerequisites and were able to enroll in the class. Due to the small size of the class, the result may not be statistically significant enough to evaluate the course, but the results still show that students expressed appreciation of the pedagogical design and the rich learning contents of the class. They particularly enjoyed the hands-on portion of the class because they were able to systematically penetrate a target network after taking the class, a very marketable skill sought by employers. The class increased their interests in pursuing a career in cybersecurity, especially in pentest and ethical hacking. It is projected that there will be a big jump of enrollment in this class next year; there are already close to forty students in the cybersecurity track entering their junior year. The statistical data will be collected, analyzed, and published in a future work.

Table 1. Student Survey Questions

Questions	Strongly Agree
1. **I feel confident describing the phases and requirements of penetration testing life cycle.**	100%
2. **The lab assignments are sufficient for me to practice hands-on skills.**	100%
3. **The in-class group exercises are a necessary component of learning.**	100%
4. **The lectures help me understand the concepts of the penetration testing.**	67%
5. **The online virtual lab is easy to connect and configure.**	100%
6. **The lab manuals are either easy to follow or the tasks are intuitive enough for me to complete by myself.**	100%
7. **I may choose a career as a penetration tester because of class.**	67%
8. **This class meets my learning objectives.**	100%
9. **I will recommend this class to other students.**	100%
10. **The overall quality of the class is high.**	100%

Lessons Learned

A code of ethics must be developed in the first week and enforced throughout the semester. It is vitally important for each student to understand that the key difference between pentest and criminal hacking is that pentest must be officially authorized by the customer and compliant with laws, regulations, contracts, and policies. A "class use policy" needs to be defined to prohibit students from applying the hacking methods learned in class to the public and campus networks. Most institutions cannot afford a dedicated network that is completely separated from the campus production network for the security lab. The Internet connection of all VMs in the online lab must be turned off because these VMs may have exploitable vulnerabilities or contain malicious software. Student access to these VMs must be limited through the Sandbox online interface only.

When designing the learning modules, national frameworks and subject areas of industry certificates can be adopted as guidelines. The NICE framework and EC-Council's Certified Ethical Hacker (CEH) certificate were referenced for the design of our curriculum. Mapping the learning modules to the NSA's KUs also aided in the application for government designations and grants. In addition, there are a large number of free resources already available as described in the next section. Knowledge of resources location can significantly reduce the workload of the instructor.

The VMware vSphere and other virtualization technologies can be conveniently deployed, managed, and maintained to provide students a persistent networked teaching environment. A successful approach was allowing all the students to work on eleven VMs simultaneously, which is difficult for the students to implement individually due to limited computing power on their personal computers.

The software used in the class is not limited to open source tools developed by the community contributors. In the real-world pentest tasks, open source tools are supplemental with multiple professional security products. Knowing how to configure and deploy these professional products is another skill sought by the employers. Contacting the security product vendors may result in surprising outcomes. Many of them would provide academic license and partnership at no cost when the software licenses are used for education purposes only. We used Rapid7's Metasploit

and Nexpose professional versions for free in our class. Juniper also allowed us remote access to their security appliance training system for free.

Resources

Through the development of the pentest curriculum, a collection of teaching resources previously developed by the security community and the government funded projects were discovered. They are summarized below to share with the institutions that are developing a similar course.

Government Guidelines and Grants

The 2014 NSA's NICE framework and the CAE IA/CD programs provide the detailed guidelines for creating cybersecurity curricula and degree programs. Each year, the NSF issues multiple educational grants that facilitate the creation of cybersecurity teaching contents and dissemination of the outcomes. Rich teaching resources can be obtained from past and active NSF projects. The current grants that support pentest curriculum development is primarily under the division of undergraduate education (DUE). The relevant DUE grants are listed below.

1. Advanced Technological Education (ATE, 2014) grant promotes technical education in the 2-year community colleges. Some labs used in my teaching are adopted from CSSIA, a national ATE Center for IT education development. The CyberWatch (Tobey, Pusey, & Burley, 2014) is another very active ATE center specializing in cybersecurity curriculum development and support.

2. Innovative Technology Experiences for Students and Teachers (ITEST, 2014) grant seeks the creation of innovative models to teach K-12 students and train the teachers' STEM experiences. K-12 Information and Communication Technology (ICT) is one of the core themes that this grant funds.

3. Improving Undergraduate STEM Education (IUSE, 2014) grant consolidates several past STEM education grants. It addresses immediate challenges and opportunities that are facing undergraduate STEM education and supports teaching and curriculum development efforts.

4. CyberCorps: Scholarship for Service (SFS, 2014) grant provides student scholarships and capacity building activities for academic excellence in cybersecurity. Free cybersecurity workshops and conferences for ICT educators are supported by this grant.

In addition to the above NSF education grants that directly support the development of cybersecurity curricula, there are numerous research grants funded by NSF, DoD, DHS, NSA, DoEd, and DoL to support fundamental research of security algorithms, create new tools and appliances, and collaboration between industry and academia for research and hands-on experiences of faculty and students in cybersecurity. The grant agency official websites and grants.gov have request for proposals (RFP) posted for the latest grant opportunities.

Cyber Competitions and Industry Certifications

Teaching pentest skills is decidedly hands-on. Students learn from repeated trials and failures, even on simple lab tasks. The hacking process can be time consuming and tedious. Students usually need to conduct research after class on a set of special purpose tools and hacking methods. It is a good practice to tie student extracurricular activities to pentest learning in order to stimulate innovation and interest. Participation in cybersecurity competitions and studying industry certificates can foster student interest in pentest and facilitate in-class learning. There are a number of

well-organized regional and national cyber competitions. The National Collegiate Cyber Defense Competition (CCDC, 2014) is the largest security competition in the nation. It provides tiered and regional based competition and training supplementing the college education tracks and programs. In the meantime, it controls and assures that the college education prepares students with sufficient hands-on skills.

The CyberPatriot competition sponsored by the Air Force Association is the nation's largest youth cyber defense competition (CyberPatriot, 2014). The competition provides excellent training content that can be smoothly adopted by K-12 science classes and after-class IT clubs. The competition is organized fully online, lowering the participation cost to the minimum. We are hosting the after-school IT clubs at the local public schools. We plan to train the students with IT and security skills and prepare them for the CyberPatriot competition. These club teams also will participate in our local IT competitions, such as TechOlympics (TechOlympics, 2014) and IT Expo hosted by the university and industry partners. The winner teams receive a college scholarship and credits when team members are admitted to our cybersecurity track.

CyberAces, created by SANS, the leading security professional training and standardization organization (CyberAces, 2014), provides free online courses and completion services. There are excellent training videos and courses developed for K-12 cybersecurity outreach programs. Some videos can be adopted by the pentest class for students to review key security concepts.

Students are encouraged to obtain the industry IT certifications while taking the course, although it is not required by the curriculum. Compared to other graduates without work experience, students with professional pentest certifications have higher probabilities to obtain better jobs. The pentest certificates recommended for students to earn along with their coursework are:

1. Certified Ethical Hacker, by EC-Council. This is a vendor neutral certification and covers a broad range of pentest topics. The certification exam contents are frequently updated to reflect the skills for the latest operating systems and software tools. EC-Council launched an academic program to facilitate higher education institutions to adopt their teaching materials (CEH, 2014).

2. GIAC Certified Penetration Tester, by Global Information Assurance Certification, is another vendor neutral pentest certification that targets IT professionals with years of field experience (GPEN, 2014).

3. There are several other vender specific and general cybersecurity certifications that students can study. These certificates include $(ISC)^2$, Cisco, Juniper, and Check Point's security certification.

Collaboration with the Leading Security Product Vendors

The stringent budget in academia usually encourages the use of open source software and simulation technologies to avoid expensive licensing fees for vendor specific appliances. However, mastery of the leading commercial security products is a crucial skill that employers are seeking from the college graduates. We have worked successfully with the following leading industry vendors for research collaboration and low-cost software and hardware products.

Rapid7 (http://www.rapid7.com/) makes two software packages that are ranked at the top of professional pentest tools. The company provided free licenses on Metasploit Pro, the No.1 pentest framework used by the professionals, and Nexpose Pro, the No.1 vulnerability scanner (Rapid7, 2014).

Juniper provided support through the Academic Alliance Program, a free training program for IT in higher education. Juniper provided remote access to their advanced cybersecurity lab, allowing our students the opportunity for hands-on experience on expensive Juniper security appliances in addition to collaborative research opportunities with the Juniper security practitioners (JNAA, 2014).

For a small annual support fee, Cisco Academy is another good option to provide students hands-on experience using the Cisco networking and security appliances. With more than 10,000 academies worldwide, Cisco Network Academy is creating the largest "classroom" for teaching essential networking knowledge (https://www.netacad.com). A physical Cisco networking lab and security appliances such as firewalls, ASA, IDS can be incorporated into the pentest classes.

Community Contribution

In the era of Web 3.0, a tremendous amount of free teaching materials is available online for learning from anywhere at any time. Excellent, up-to-date pentest learning contents are created by the community contributors and posted on social media. Some of this content is created by the top pentesters and security associations. We recommend the following materials for the pentest class.

SecurityTube.net (http://www.securitytube.net/) provides a comprehensive video-based training course on the community version of Metaspliot. There are more than 30 videos illustrating step-by-step tutorials of various pentest topics under the Metasploit framework.

Offensive-Security.com (http://www.offensive-security.com/) is created by the community team that made the No.1 pentest Linux distribution, Kali Linux. They designed many realistic pentest scenarios that were implemented into a set of VMs. Students have the opportunity to practice pentest skills on the lab scenarios created by others, generating an element of uncertainty to advance facilitated learning (Wilhelm, 2014).

YouTube.com has several channels on the topic of pentest. The ones we recommend for students to watch are the "CBTNuggets Mini" and "Security Onion" channels.

Conclusions

The increasing number of security breaches and the rapid development of cybersecurity technologies need a larger workforce to fight digital crimes. Pentest, as a new IT discipline, has emerged to train cybersecurity professionals. Employers seek graduates with hands-on skills in using up-to-date cyber defense technologies. Based on the demands from the industry and the guidelines of the national cybersecurity frameworks, we developed a new pentest curriculum as an upper level undergraduate course in the cybersecurity track. In this curriculum, the teaching modules are designed to fit in a 15-week academic semester. The distribution of the lectures, in-class group exercises, and after-class assignments and projects expose students to the complete pentest cycle. A large collection of open source and commercial software tools are selected to facilitate teaching. Both a distributed lab installed on the student personal computing devices and a secure online lab were developed. These labs enabled students to practice hands-on skills at any time with or without Internet access. Through the labs students also are able to conduct research, leading to self-motivated deep learning that is beyond the requirements of the assignments. Student feedback shows that the students enjoyed the class and believed that they learned the essential skills necessary to get their feet into the door as a professional pentester. The paper also summarizes valuable resources for developing a pentest curriculum. These resources include government frameworks, guidelines, grant opportunities, existing teaching materials created by the national ATE centers and community contributors, cybersecurity competitions, industry certifications, and vendors that can be contacted for academic collaboration.

Future Improvement

Along with the rapid evolvement of pentest technologies, the curriculum has enormous potential for future improvement. We plan to add a significant amount of content in mobile pentest since mobile devices have taken the place of personal PCs and laptops as the largest target for collecting personal information by hackers. However, a wireless network is difficult to implement on our remote Sandbox systems. We will start by setting up a small in-class lab to teach how to break WAP and WPA2 encryption when the class is next offered. An additional course may be developed to extend the topics of web application and service pentest. This class will dive into the more extensive knowledge of web programming, reverse engineering, database management and development. We will also develop or adopt more in-class group exercises in the CTF format; students tend to be particularly motivated toward accumulating points and tokens while competing against other groups in a game-like learning environment.

References

ATE. (2014). *Advanced technological education grant*. National Science Foundation. Retrieved from http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5464&org=DUE&from=home

Barnett, C. (2013). *The measurement of white-collar crime using uniform crime reporting (UCR) data*. Uniform Crime Reports, U.S. Department of Justice Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Division. Retrieved from http://www.fbi.gov/stats-services/about-us/cjis/ucr/nibrs/nibrs_wcc.pdf

Bechtsoudis, A., & Sklavos, N. (2012). Aiming at higher network security through extensive penetration tests. *Latin America Transactions, IEEE (Revista IEEE America Latina)*, *10*(3), 1752, 1756.

Bureau of Labor Statistics. (2012). *Occupational outlook handbook*. United States Departments of Labor. Retrieved from http://www.bls.gov/ooh/computer-and-information-technology/home.htm

CCDC. (2014). *National Collegiate Cyber Defense Competition*. Retrieved from http://www.nationalccdc.org/

CEH. (2014). *Certified Ethical Hacker Version 8*. EC-Council. Retrieved from http://www.eccouncil.org/Certification/exam-information/ceh-exam-312-50

Corbin, K. (2013, August 8). Cybersecurity pros in high demand, highly paid and highly selective. *cio.com*. Retrieved from http://www.cio.com/article/2383451/careers-staffing/cybersecurity-pros-in-high-demand--highly-paid-and-highly-selective.html

CyberAces. (2014). *Your gateway to cybersecurity skills and careers*. Cyber Aces Foundation. Retrieved from http://www.cyberaces.org/

CyberPatriot. (2014). *The CyberPatriot national youth cyber education program*. Air Force Association. Retrieved from http://www.uscyberpatriot.org/

Dave, P. (2013, August 6). Cybersecurity salaries average $116,000; D.C. seen as center. *Los Angeles Times*. Retrieved from http://www.latimes.com/business/technology/la-fi-tn-cybersecurity-jobs-salaries-dc-20130806-story.html

Falkenberg, A., Mainka, C., Somorovsky, J., & Schwenk, J. (2013). A new approach towards DoS penetration testing on web services. *2013 IEEE 20th International Conference on Web Services (ICWS),* pp.491, 498, June 28 2013-July 3 2013

GPEN. (2014). *GIAC penetration tester exam*. Global Information Assurance Certification. Retrieved from http://www.giac.org/certification/penetration-tester-gpen

Hudic, A., Zechner, L., Islam, S., Krieg, C., Weippl, E. R., Winkler, S. & Hable, R. (2012). Towards a unified penetration testing taxonomy. *Privacy, Security, Risk and Trust (PASSAT), 2012 International*

Conference on and 2012 International Conference on Social Computing (SocialCom), pp.811-812, Sept. 2012

ITEST. (2014). *Innovative Technology Experiences for Students and Teachers Grant*. National Science Foundation. Retrieved from http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5467

IUSE. (2014). *Improving Undergraduate STEM Education Grant*. National Science Foundation. Retrieved from http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505082&org=DUE&from=home

JNAA. (2014). *Juniper Networks Academic Alliance*. Juniper Networks. Retrieved from http://www.juniper.net/us/en/training/academicalliance/

Kessler, G. C., & Ramsay, J. D. (2014). A proposed curriculum in cybersecurity education targeting homeland security students. *2014 47th Hawaii International Conference on System Sciences (HICSS)*, pp.4932, 4937, 6-9 Jan. 2014.

Kuo, C., Ruan, H., Chen, S., & Lei, C. (2012). An analysis of security patch lifecycle using Google Trend Tool. *Information Security (Asia JCIS), 2012 Seventh Asia Joint Conference on. IEEE*, 2012.

Luallen, M. E., & Labruyere, J. (2013). Developing a critical infrastructure and control systems cybersecurity curriculum. *2013 46th Hawaii International Conference System Sciences (HICSS),* pp.1782, 1791, 7-10 Jan. 2013

Mainka, C., Somorovsky, J., & Schwenk, J. (2012). Penetration testing tool for web services security. *2012 IEEE Eighth World Congress on Services (SERVICES),* pp.163-170, June 2012

Mishra, S., Romanowski, C.J., Raj, R.K., Howles, T. & Schneider, J. (2013). A curricular framework for critical infrastructure protection education for engineering, technology and computing majors. *Frontiers in Education Conference, 2013 IEEE*, pp.1779, 1781, 23-26 Oct. 2013

National Initiative for Cybersecurity Careers and Studies [NICCS]. (2013). *National Cybersecurity Workforce Framework*. Retrieved from http://niccs.us-cert.gov/

NIST. (2014). *Framework for improving critical infrastructure cybersecurity Version 1.0*. National Institute of Standards and Technology. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

NSA. (2013). *National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD).* National Security Agency & Central Security Service. Retrieved from https://www.nsa.gov/ia/academic_outreach/nat_cae/

Pritchard, R. (2014). Cyber wars. *ITNOW, 56*(4), 40-41.

Ramirez-Silva, E., & Dacier, M. (2007). Empirical study of the impact of Metasploit related attacks in 4 years of attack traces. *Advances in Computer Science–ASIAN 2007.* Computer and Network Security. Springer Berlin Heidelberg, Pp. 198-211, 2007

Reisinger, D. (2014). Why the Sony hack is a serious cyber-war escalation. *Eweek.com*. Retrieved from http://www.eweek.com/security/slideshows/why-the-sony-hack-is-a-serious-cyber-war-escalation.html

SANS. (2015). *Penetration testing curricula*. Retrieved from http://www.sans.org/curricula/penetration-testing

SFS. (2014). *CyberCorps: Scholarship for Service Grant.* National Science Foundation. Retrieved from http://www.nsf.gov/pubs/2014/nsf14586/nsf14586.htm

Sun, T. (2013). *The art of war*. CreateSpace Independent Publishing Platform.

TechOlympics. (2014). *Cincinnati's premiere high school technology competition and expo*. InterAlliance of Greater Cincinnati. Retrieved from https://www.techolympics.org/

Tobey, D., Pusey, P., & Burley, D. (2014). Engaging learners in cybersecurity careers: Lessons from the launch of the National Cyber League. *ACM Inroads, 5*(1), 53-56.

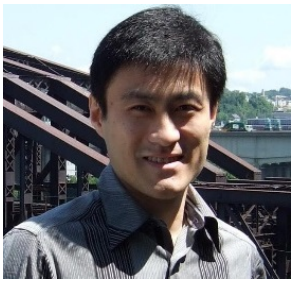
Twitchell, D. P. (2006). Social engineering in information assurance curricula. *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 191-193). ACM.

Wichers, D. (2013). *The 2013 OWASP Top 10*. AppSec USA 2013 Conference. Owasp, 2013, https://owasp.org

Wilhelm, T. (2013). *Professional penetration testing, Creating and learning in a hacking lab* (2nd ed.). Syngress.

Zhang, S., Caragea, D. & Ou, X. (2011). An empirical study on using the national vulnerability database to predict software vulnerabilities. In A. Hameurlain, S. W. Liddle, K.-D. Schewe, & X. Zhou (Eds.), *Database and Expert Systems Applications, 22nd International Conference, DEXA 2011*, Toulouse, France, August 29 - September 2, 2011, Proceedings, Part I (pp. 217-231). Springer Berlin Heidelberg.

Biography



Dr. Chengcheng Li received his Ph.D. in Computer Science from Texas Tech University. He is the graduate director of the School of Information Technology at the University of Cincinnati. His teaching and research interests are in cybersecurity. He's also engaged in promoting IT education to the K-12 students and teachers in the region.