Teaching Tip
The Development of a Red Teaming Service-Learning Course

Jacob A. Young
Entrepreneurship, Technology & Law
Bradley University
Peoria, IL 61625, USA
jayoung@fsmail.bradley.edu

ABSTRACT

Despite advancements in pedagogy and technology, students often yearn for more applied opportunities in information security education. Further, small businesses are likely to have inadequate information security postures due to limited budgets and expertise. To address both issues, an advanced course in ethical hacking was developed which allows students to perform security assessments for local businesses through red team engagements. This paper will allow academics to implement similar courses, improving security education for students and increasing opportunities for local businesses to receive affordable security assessments.

Keywords: Security education, Ethical hacking, Red team, Penetration testing, Security assessment, Social engineering

1. INTRODUCTION

Verizon (2018) reports that 58 percent of data breach victims are small businesses. Even with an increased awareness of security threats (Pritchard, 2010), small to medium enterprises (SMEs) are still likely to suffer from inadequate information security postures due to limited budgets and expertise (Pritchard, 2010; Renaud and Weir, 2016). Although some small business leaders might view their organizations as insignificant and unlikely targets, attackers regularly attempt to leverage footholds in vendor networks to access larger organizations (PwC, 2014), as was demonstrated in the Target breach (Plachkinova and Maurer, 2018). Further, the Ponemon Institute (2018) estimated a $41.55 per record cost for a data breach involving 1 million compromised records. However, since the estimated cost per record flattens from $15.64 for 10 million records to $7.63 for 50 million records, large organizations can better absorb the expenses associated with a mega breach than small businesses can from small breaches.

To address these issues, we created an innovative service-learning course in ethical hacking which allows undergraduate students to perform penetration tests for local businesses as members of a red team engagement. In its most basic form, a penetration test is "an analysis of some aspect of a system" to identify potential security weaknesses (Bishop, 2007, p. 84). Red teaming is a specialized approach to conducting penetration tests that assesses security from an adversary's perspective. Ultimately, allowing students to engage in red teaming activities aids the development of the adversarial mindset necessary to defend against contemporary threats. Many external security assessments are limited engagements lasting one to two weeks, whereas this course allows students to conduct an extended assessment over an entire semester. While such a class certainly introduces its own risks and challenges, the ability to perform an assessment over a longer period results in a deeper engagement, which might provide clients with a different perspective than those conducted by professional security firms.

Therefore, the purpose of this paper is to assist academics in the implementation of similar courses to enhance security education for students and increase opportunities for local businesses to receive low-cost security assessments through red teaming engagements. We followed the recommendations of Lending and Vician (2012) for this teaching tip. In section two, we provide a review of the limited pedagogical research on penetration testing and red teaming. The next two sections cover the course development process and the steps for course preparation. We then describe our experiences with the course implementation and how student learning is evaluated. In section seven, we provide student feedback and course outcomes. Finally, we share some of the challenges we faced, offer additional recommendations for instructors to consider, and outline our future course development plans.

2. LITERATURE REVIEW

Educators have made substantial progress with respect to information security curriculum and pedagogy in recent years by allowing students to attack and defend networks using isolated lab environments (Hill et al., 2004; Wagner and Wudi, 2004; O'Leary, 2006; Aman, Conway, and Harr, 2010) and through the use of teaching cases (Hackney, McMaster, and Harris, 2007). Despite advancements in pedagogy and instructional technology, students often yearn for more realistic

opportunities and employers often find it challenging to hire enough college graduates who already possess the skills they seek (Fulton et al., 2013). Therefore, educators must find ways to incorporate more experiential learning opportunities to better prepare graduates to meet industry demands (Sauls and Gudigantala, 2013).

One such learning opportunity is having students conduct security assessments. Some courses have attempted to address this need by allowing students to perform penetration tests to assess the security of their institution (Shen, 2018), whereas others have students conduct a passive risk assessment of an organization's operations (Spears, 2018). While these courses provide students with valuable hands-on experience, they do not involve active attacks against external clients. Further, despite social engineering being the oldest form of compromise (Ceraolo, 1996), it has not been a major focus of the security curriculum (Twitchell, 2006). Thus, students are rarely afforded the opportunity to personally experience how effective social engineering attacks can be.

This course builds upon such efforts by allowing students to gain hands-on, ethical hacking experience through red teaming by actively employing offensive techniques against an external client. Not only does conducting an assessment aid in learning and improve client security, exposing students to ethical hacking and white hat principles is expected to help them resist the temptation to engage in black hat hacking activities (Pike, 2013). Dimkov, Pieters, & Hartel (2010) outlined five requirements that must be considered for any penetration test to be considered successful for the client organization, especially when engaging in social engineering. The five requirements, provided in Table 1, consist of realistic, respectful, reliable, repeatable, and reportable.

Requirement	Explanation
Realistic	Employees should act normally, as they would in everyday life.
Respectful	The test is done ethically, by respecting the employees and the mutual trust between employees.
Reliable	The penetration test does not result in productivity loss by employees.
Repeatable	The same test can be performed several times and, if the environment does not change, the results should be the same.
Reportable	All actions during the test should be logged and the outcome of the test should be in a form that permits meaningful and actionable documentation of findings and recommendations.

Table 1. Dimkov, Pieter, and Hartel's (2010) R* Requirements for Penetration Tests

Realistic refers to ensuring employees are not aware of the assessment to preserve the validity of the tests being conducted. *Respectful* involves careful planning to avoid causing unnecessary issues for employees. *Reliable* requires being mindful of productivity for the client organization and its employees. *Repeatable* tasks help team members assess results over multiple test attempts. *Reportable* stresses the importance of documenting all assessment activities to aid in remediation. Since these requirements can oftentimes conflict with each other, the goal is to strike a balance among all and limit the potential for negative outcomes as much as possible. With respect to the red teaming course, we discuss the measures in place to ensure adherence to the first three requirements in the pre-engagement interaction section (4.2) and the other two throughout the course implementation section (5).

3. COURSE DEVELOPMENT

In this section, we begin by outlining the development timeline. Next, we discuss our pedagogical approach and explain the adopted assessment methodologies. Then, we report student demographics and discuss how the course satisfies standards outlined in modern security curriculum frameworks. Lastly, we briefly discuss the value of relationships with industry partners.

3.1 Development Timeline

We discuss three full iterations of the course in this paper. We piloted the course in the spring semester of 2017 and offered a second iteration in the spring semester of 2018. The latest offering was in the fall semester of 2018. The 3-hour course is taught over 15-week semesters with 28 class meetings and a 2-hour final exam period. Due to scheduling limitations, the pilot of the course consisted of one scheduled weekly meeting of two and a half hours. Subsequent offerings have been scheduled for two weekly meetings of one hour and fifteen minutes each.

3.2 Pedagogical Approach

For this course, we employ a service-learning (Furco, 1996) approach to security education (Hall and Johnson, 2011; Lee, 2012). As shown in Figure 1, service-learning equally balances academic objectives with the service being provided to the client. This requires the service project to be fully integrated into the course. Doing so allows students to provide a valuable service while simultaneously learning how to perform security assessments. Aside from client recruitment, which is conducted by faculty and staff, the students are responsible for conducting every step of the security assessment. This results in a classroom environment where the students are expected to immerse themselves into the project to identify opportunities for exploration on behalf of the client. Due to the flexible, student-driven nature of the course, the instructor must facilitate assessment activities by supervising and offering guidance to the students as they discover and test potential risks to the client.

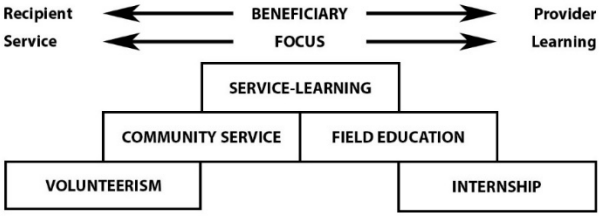

Figure 1. Service Programs (Furco, 1996)

The terms and definitions for Anderson, Krathwohl, & Bloom's (2001) revision of Bloom et al.'s (1956) original taxonomy have been reproduced in Table 2. The taxonomy consists of remembering, understanding, applying, analyzing, evaluating, and creating. While students must remember and understand the material taught in prior courses, this course also requires students to effectively engage in higher order thinking

Term	Definition
Remembering	Retrieving, recognizing, and recalling relevant knowledge from long-term memory.
Understanding	Constructing meaning from oral, written, and graphic messages through interpreting, exemplifying, classifying, summarizing, inferring, comparing, and explaining.
Applying	Carrying out or using a procedure through executing or implementing.
Analyzing	Breaking material into constituent parts and determining how the parts relate to one another and to an overall structure or purpose through differentiating, organizing, and attributing.
Evaluating	Making judgements based on criteria and standards through checking and critiquing.
Creating	Putting elements together to form a coherent or functional whole; reorganizing elements into a new pattern or structure through generating, planning, or producing.

Table 2. Revised Bloom's Taxonomy (Anderson, Krathwohl, and Bloom, 2001)

for the security assessment to be successful. For example, students must (1) apply appropriate assessment methodologies and penetration testing techniques, (2) analyze information about the organization's operations, people, and systems, (3) evaluate the organization's resilience to tested threats, and (4) create a practical report and presentation for the client that outlines recommended steps for remediation.

3.3 Methodologies

The assessment we conducted in the pilot course was based upon the National Security Agency's INFOSEC Evaluation Methodology (IEM) (Rogers et al., 2005) and INFOSEC Assessment Methodology (IAM) (Rogers et al., 2004). Subsequent iterations have followed the Penetration Testing Execution Standard (PTES) which organizes activities into seven stages: Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation, and Reporting. A mind map of the PTES methodology is provided in Figure 2 (Amit, n.d.). We supplement the PTES with the Open Source Security Testing Methodology Manual (OSSTMM) (Herzog, 2010). Depending on client needs, instructors might find that following the OWASP Testing Guide (Meucci and Muller, 2014) would also be appropriate.

3.4 Student Background

Student demographics are provided in Table 3. We invited 11 high performing undergraduates majoring in management information systems (8), computer information systems (2), and computer science (1) to participate in the pilot course. The course roster included two juniors and nine seniors, with seven males and four females. The second offering of the course consisted of seven management information systems majors, three computer information systems majors, and one computer science major. All 11 were seniors, with one female. The third instance of the course included eight management information systems majors, two computer science majors, and one accounting major. The latest iteration of the course is currently underway with nearly double the enrollment of prior sections.

		Spring 2017	Spring 2018	Fall 2018	Fall 2019
Major	Management Information Systems	8	7	8	8
	Computer Information Systems	2	3	0	3
	Computer Science	1	1	2	7
	Other	0	0	1	3
Class	Senior	9	11	9	18
	Junior	2	0	2	3
Gender	Male	7	10	8	17
	Female	4	1	3	4

Table 3. Student Demographics

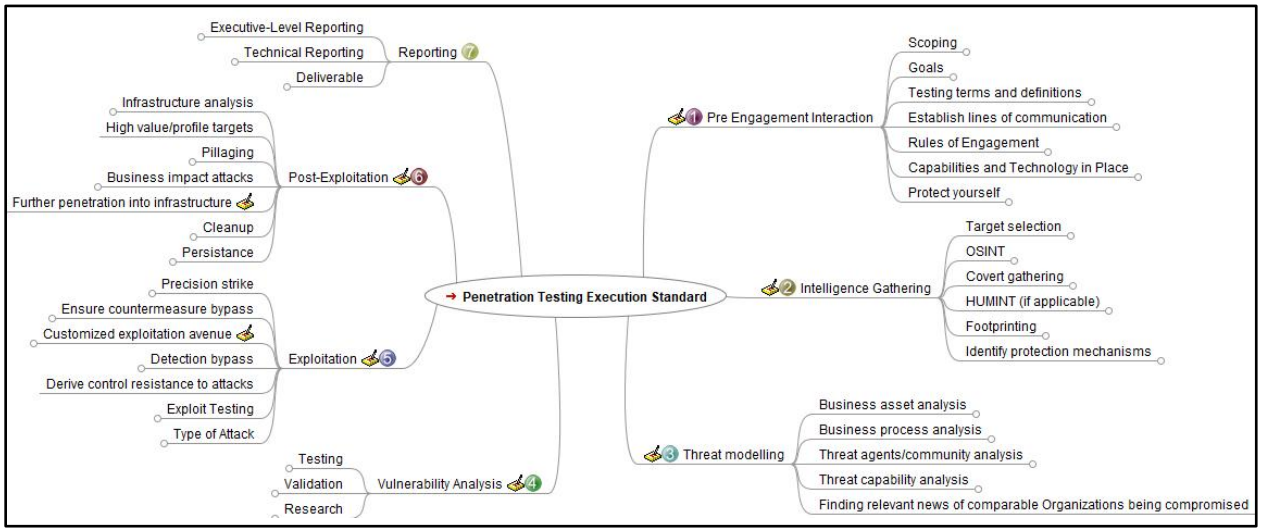

Figure 2. Penetration Testing Execution Standard (PTES) Mind Map (Amit, n.d.)

The mix of majors provides a diverse pool of skills that allows students to apply their talents to specialized tasks best-suited to their backgrounds and interests. Each student was either concurrently enrolled in or had already completed the requisite coursework in networking and information security offered within their discipline. Program degree plans and course offerings have since been altered to reduce the need for concurrent enrollment in the prerequisites.

In addition to encouraging more females to pursue careers in technology, a high level of female involvement has many benefits for this course. For example, due to the stereotypical image of black-hat hackers being primarily male, our observations lead me to believe that the involvement of female students significantly contributed to the success of the social engineering tasks as it appeared our targets were less likely to suspect attacks from females.

3.5 Curriculum Frameworks

Based upon the success of the pilot, the course now serves as the capstone of the cybersecurity concentration within the management information systems major and is also available to computer science and computer information systems majors as an elective. The cybersecurity concentration in the management information systems major is aligned with the 2019 standards for the National Security Agency's (NSA) Centers for Academic Excellence in Cyber Defense (CAE-CD) Network Security Administration Specialization (National Information Assurance Education & Training Programs, n.d.). The knowledge units for the Network Security Administration specialization are distributed among a four-course sequence with the Penetration Testing (PTT) and Vulnerability Analysis (VLA) knowledge units being covered in this course. The course is also structured in alignment with the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse et al., 2017) by focusing on the Vulnerability Assessment and Management specialty area of the Protect and Defend (PR) category and All Source Intelligence, Exploitation Analysis, Targets, and Threat Analysis specialty areas of the Analyze (AN) category.

3.6 Industry Partners

Throughout the development process, we engaged with several professionals to gather feedback and guidance (von Konsky, Miller, and Jones, 2016). These industry partners aided with operational logistics, helped address legal challenges, and shared security assessment expertise. We encourage those who wish to offer a similar course at their institution to develop relationships and seek assistance from industry partners, such as information security firms, Internet service providers (ISPs), law enforcement agencies, and attorneys. As a courtesy, we often refer clients to these partners for follow-up services.

4. COURSE PREPARATION

As with any new course, preparation can be the most time-consuming aspect. These suggestions should enable instructors to prepare for a successful security assessment.

4.1 Instructor Background

We recommend that instructors have at least a background in teaching introductory networking and security courses. While holding a professional certification in ethical hacking or penetration testing (e.g., Certified Ethical Hacker or PenTest+) is certainly desirable, it is not necessary if the instructor is willing to obtain the knowledge through self-study or with the assistance of industry partners. The depth and breadth of approved assessment activities can grow as the instructor gains more experience in managing assessments over time. The instructor will serve primarily as project manager by facilitating the course, keeping the team on schedule, and ensuring that assessment activities abide by the rules of engagement.

Ultimately, the prerequisite knowledge and experience necessary for an instructor to manage this course is dependent on the activities students can pursue. Some teams might focus entirely on assessing social engineering whereas others might employ technical attacks against client networks. Since the instructor has complete control over the scope of activities, the assessment can be tailored to his or her expertise. If a proposed test is beyond the instructor's expertise and the students cannot demonstrate how it can be conducted safely and at minimal risk to the client, the instructor can always reject it.

4.2 Pre-Engagement Interaction

All pre-engagement interactions with the client and course preparation steps are to be performed by the instructor and must be completed prior to the start of the course. First, a willing client must be identified. Second, legal issues must be addressed. Third, all necessary course resources must be secured. After the pre-engagement interactions have been completed, the remaining stages of the PTES methodology are conducted entirely by students during the course.

4.2.1 Client recruitment. The target client for this course consists of small to medium, community-based organizations (CBOs). Client recruitment was aided by a strong institutional reputation developed over decades of experience with managing student consulting projects. Due to the risks associated with performing live security assessments, we initially limited client recruitment for this course to CBOs with established student-consulting relationships. Future client recruitment will extend to new CBOs now that the course has been refined and proven success can be demonstrated. However, given the nature of the course, instructors might elect to test their processes against the institution's security posture and work towards providing assessments for outside clients.

When first discussing the course with a potential client, we ask them to limit knowledge of the assessment to as few employees as possible until after it has concluded. While we always provide the client organization with the list of students, we do not provide any other details to minimize the likelihood of employees recognizing them during on site activities. These steps ensure that our findings are valid and reflect true employee reactions to potential attacks to satisfy Dimkov, Pieter, and Hartel's (2010) realistic requirement. Second, we ensure management understands the purpose of security assessments. Every organization is vulnerable to some degree. We stress that a security assessment should be viewed as part of a continuous improvement process; our findings are opportunities to strengthen the defenses of the organization. Therefore, we do not encourage our clients to take disciplinary action against any employee. Instead, we recommend our clients increase their security education training awareness

(SETA) to address any deficiencies in employee performance. This aids in meeting Dimkov, Pieter, and Hartel's (2010) respectful requirement. Of course, the client is well within their right to dismiss any employee who does not exhibit improvement after reasonable efforts have been made to retrain.

4.2.2 Legal considerations. Due to the sensitive nature of such work, it is imperative that all legal issues are properly considered. In this section, we will discuss key legal issues to address prior to engaging in red teaming activities: establishing a protected relationship aided by attorney-client privilege, establishing the scope of the assessment, finalizing a letter of engagement, obtaining a letter of authorization, and having students sign white hat and non-disclosure agreements.

4.2.2.1 Attorney-client privilege. It would be wise for CBOs interested in commissioning security assessments to have the client's attorney hire the red team. This makes it possible for the final work-product to be protected by attorney/client privilege – should the client ever be the subject of a lawsuit due to a data breach, not only is the client protected from divulging the vulnerabilities uncovered by the assessment, but it also helps protect members of the red team (faculty and students) from being forced to testify about their involvement in the security assessment.

4.2.2.2 Scoping and letter of engagement. After agreeing to proceed with a client, a letter of engagement should be carefully crafted to outline the scope and limitations of the assessment (Appendix A). Although our first three clients have not limited the assessment activities that we could conduct against their organizations, we have placed limited restrictions on attacking certain systems, data, or people. We encourage instructors to discuss these limitations with clients as soon as possible to ensure that a mutually beneficial scope can be achieved to facilitate student learning. Team members must adhere to the scope of work and rules of engagement when planning and executing their assessment tasks. All proposals must be reviewed by the faculty member to ensure that all potential risks to the client have been identified. No active attacks against any client assets are permitted until instructor approval has been granted for the task. These steps reduce the likelihood of our actions causing a reduction in client productivity, in accordance with Dimkov, Pieter, and Hartel's (2010) reliable requirement.

4.2.2.3 Letter of authorization. Once the scope has been finalized, instructors should obtain a signed letter of authorization (Appendix B) that contains contact information for the client and specifically outlines the names of the individuals involved in performing the security assessment. This provides the red team with the colloquially named "get out of jail free card" to prove their activities have been sanctioned by the client should they ever be challenged by employees or law enforcement. Students are only provided a copy of their initialed version of the letter of engagement prior to the commencement of active attacks against the client.

While a letter of authorization does grant students permission to perform otherwise illegal activity against a client's assets, it does not allow for a carte blanche disregard for the law. For example, it is always illegal to pose as a representative of any local, state, or federal government. Further, state laws vary with respect to the legality of audio and video recording, especially for phone conversations. Although the letter of authorization clearly outlines the details of the engagement, we do not recommend relying solely upon this document, especially if the assessment will consist of any activities conducted on the client's premises. For example, if a student rightly produces their letter of authorization after being challenged, it does not prevent an overzealous employee from immediately shredding or burning it. Therefore, we suggest that students carry two copies of their letter of authorization on their person to ensure a backup copy is always readily available. We also strongly encourage faculty members to inform the relevant law enforcement agencies that proper authorization has been obtained prior to initiating any on-site assessment activities.

4.2.2.4 Student agreements. There are several risks and ethical issues to consider when teaching penetration testing and red teaming skills (Logan and Clarkson, 2005), especially when employing social engineering (Mouton et al., 2015). Thus, students should be required to sign both a white hat agreement (Appendix C) and a non-disclosure agreement (Appendix D) prior to knowing the client organization. To maintain client confidentiality, engagement-related communication among team members is handled through end-to-end encryption channels. We also recommend that faculty prohibit students from referring to the client organization by name to reduce the likelihood of accidental disclosures outside of class meetings. Instead, the target organization should simply be referred to as "the client" to form a habit that will carry on outside of the walls of the classroom. Students are also warned that they will receive a failing grade for the course if they violate the terms of the non-disclosure agreement. This extends to protecting their initialed letter of engagement since they are collected at the conclusion of our assessment period. These steps further satisfy Dimkov, Pieter, and Hartel's (2010) requirement to respect the client organization and its employees.

4.2.3 Course resources. Due to the wide variety of tasks that students might want to pursue, the instructor will often need to point students to task-specific resources. Some course activities require access to specialized equipment, tools, and information to perform the security assessment in an organized and efficient manner. While not everything outlined in this section is necessary, the variety of assessment tasks will be limited if some cannot be provided to students.

4.2.3.1 Equipment. A new $12,000 server was implemented to support this course. The server was purchased with the support of an internal teaching development grant and funding from the college and department. The server was virtualized using VMware's ESXihyperviser, vSphere, and vCenter. Virtualization not only provides excellent efficiency benefits in terms of system resources, but it also affords instructors greater control over the team activities. VMware licensing was obtained through a departmental subscription to the VMware Academic Partner (VMAP) program (https://kivuto.com/solutions/institutions/vmware-academic-program-vmap/). Subscriptions allow for unlimited licensing for academic purposes for $250 per year per department, and campus subscriptions can be obtained for $1,250 per year.

Students were granted virtual private network (VPN) access to the server to utilize the tools off-campus.

4.2.3.2 Team management. Team communication is facilitated through the Wire (https://wire.com) messaging application. Each member creates a unique username and joins a private group created by the instructor dedicated to the security assessment. This increases real-time collaboration and prevents students from discussing client-sensitive information through standard text messaging.

The Dradis Framework (https://dradisframework.com) was implemented beginning with the third iteration of the course to streamline the collaboration and reporting aspects of the security assessment. Dradis is an open-source reporting and collaboration system, primarily used by security teams to store, organize, and report assessment information and findings. Dradis has significantly improved the efficiency of our engagements due to increased visibility and the ability to export information using report templates. The technical guidelines outlined in the PTES can also be added to Dradis by installing the PTES compliance package. Students can then check off completed tasks as they add their findings to Dradis. It is important to note that since many of the assessment tasks must be performed outside of the scheduled meeting times for the course, the faculty member must be willing and available to supervise these activities.

4.2.3.3 Network tools. We provide each student with remote access to their own Buscador (https://inteltechniques.com/buscador) and Kali Linux (https://kali.org) virtual machine (VM). Buscador is a Linux-based operating system for open-source intelligence gathering. Kali is a powerful, Linux-based penetration-testing platform that provides students with easy access to an extensive library of tools, such as Maltego (https://paterva.com/web7), Metasploit Framework (https://metasploit.com), Armitage (http://fastandeasyhacking.com), Nmap (https://nmap.org), and Wireshark (https://wireshark.org).

4.2.3.4 Phishing. Phishing is a social engineering attack method that leverages email communication to compromise users. Multiple second-level domains have been purchased to provide students with look-alike domains to employ in phishing campaigns. Client-specific look-alike domains are only purchased and controlled through the end of the security assessment and are transferred to the client to prevent others from employing them against the organization's interests.

We initially used Phishing Frenzy (https://phishingfrenzy.com) for the pilot course, but we have subsequently adopted GoPhish as our phishing platform. GoPhish offers a simplified installation process and quickly clones most emails and landing pages. We are considering employing the new Modlishka (https://github.com/drk1wi/Modlishka) phishing tool in future engagements. Modlishka serves as a reverse proxy that can support the interception of two-factor authentication tokens.

We use Postfix as the SMTP email server for phishing emails. Students can test the "spammyness" of their emails by sending them to Mail-Tester.com (https://mail-tester.com/). Ensuring that each domain has properly configured MX records will reduce the likelihood of phishing emails not reaching the intended target. For example, authorizing the email server to send email on behalf of each domain using the Sender Policy Framework (SPF), signing emails through DomainKeys Identified Mail (DKIM), and employing Domain-based Message Authentication, Reporting, and Conformance (DMARC) will greatly enhance the success of phishing campaigns.

4.2.3.5 Vishing. Vishing consists of obtaining useful information about the target organization over the phone. Since students shouldn't reveal their phone number to the target organization, alternate numbers can be easily obtained for any area code by using Google Voice or the MySudo app (https://mysudo.com), which is currently limited to Apple devices. These numbers are fully functional and can be included with various social engineering attacks. True caller ID spoofing can also be achieved using Viproy (http://viproy.com) through Metasploit's SIP Invite Spoof module.

4.2.3.6 Site visit tools. Most of our site visits have only required the use of standard smartphones and flash drives. For example, students can easily record the client facility during a "facility tour" supposedly needed to complete a class assignment. Or, students can drop relatively cheap flash drives containing seemingly important information with a script disguised as an "open if found" text file. Depending on student creativity, site visits can require a wide variety of tools and resources. For example, students posing as technicians could use a car magnet that says "Contractor" to increase the believability of their pretext. If students develop a task that calls for more specialized equipment, we can provide them with many of Hak5's penetration testing products, such as the WifiPineapple, Rubberducky, Bash Bunny, LAN Turtle, or Packet Squirrel. Students have also successfully used the KeyMe app (https://www.key.me) to quickly order a duplicate key without removing it from the facility.

4.2.3.7 Textbooks. As suggested by Knapp, Maurer, and Plachkinova (2017), several courses in our curriculum are designed to prepare students to obtain professional certifications, such as CompTIA's Network+ and Security+. Following the pilot, we adopted the study guide (Walker, 2017) for the EC-Council's Certified Ethical Hacker (CEH) certification. However, since the exam requires two years of work experience and prevents most of our students from obtaining the certification prior to graduation, we now intend to use the study guide for CompTIA's new PenTest+ certification (Nutting, 2018) as the required textbook beginning in Fall 2019.

Since students are only required to purchase the certification study guide, students are also provided access to additional resources to assist them in performing specialized tasks as needed. For example, students involved in performing reconnaissance and open source information gathering followed the guidance of (Bazzell, 2018). Social engineering methodology is primarily obtained from Hadnagy (2011) and Talamantes (2014). Advanced instruction for performing specific tasks using Kali is obtained from Weidman (2014), Kim (2015), and Dieterle (2016). A full list of recommended textbook resources is provided in Appendix E.

5. COURSE IMPLEMENTATION

We have organized assessment activities and each of the steps in the PTES into one of three phases of the course: planning, execution, and reporting. Since instructors are expected to familiarize themselves with their chosen penetration testing and red teaming methodologies in detail, we will only provide a brief discussion of the activities conducted in each phase. A suggested course schedule is provided in Appendix F.

5.1 Planning

The planning phase consists of the intelligence gathering, threat modeling, and vulnerability analysis stages of the PTES methodology. Once enough intelligence has been gathered, several assessment activities are identified and assigned to small task teams for threat modeling and vulnerability analysis. For example, task teams might be responsible for planning activities to assess physical security, network security, susceptibility to social engineering, and organizational policies. While students do gravitate to the tasks that best fit their existing skillset, the excitement of certain types of activities does draw some to explore new skills.

Prior to commencing intelligence gathering activities, the instructor should devote the first class meeting to providing an overview of the course, outlining the PTES, allowing for student introductions, and having students sign the white hat and non-disclosure agreements. If possible, having members of prior red teams share their experiences and recommendations can be extremely beneficial. Otherwise, the instructor can simply relay comments from former students collected through assessment debrief surveys. The second class meeting is typically spent demonstrating how to access the various virtual machines used throughout the course. The remaining class sessions in the planning phase begin with a short lecture highlighting the key points of each chapter of the required textbook followed by assessment updates from each task team. Since the success of the assessment is dependent upon the team working together, class attendance is critical.

5.1.1 Intelligence gathering. Prior to actively engaging the target client with any task, it is critical to spend a significant amount of time researching the organization. This intelligence gathering process consists of several categories of information collection: open-source intelligence (OSINT), covert gathering, footprinting, and the identification of protection mechanisms. All students participate in the collection of public information. More technically savvy students will likely gravitate to network scanning, while others might create an organizational chart based on employee social media profiles or performing on-site reconnaissance. Once intelligence gathering responsibilities are distributed across the team, students are directed to the relevant resources needed to complete their task. As information is gathered, students store it in Dradis to increase team awareness.

The level of detail for intelligence gathering is determined by the scope of a penetration test and the amount of time and effort that can be committed. Since this course involves performing red teaming engagements, the most intensive level must be conducted, otherwise the execution phase will struggle to yield results due to poor planning. During the planning stages, OSINT should begin in a passive manner, with an eventual transition to semi-passive. For example, the use of Google Hacking and Shodan queries allows for the collection of tremendous amounts of information without being noticed by the client since students are not interacting directly with client-owned resources. Whereas active methods, such as full port scans of the client network, are likely to be detected by the client and raise suspicion. Therefore, students should take advantage of the semester-long engagement period by performing these tasks slowly to avoid jeopardizing other assessment activities. Hayes and Cappa (2018) provide an excellent demonstration of the power of OSINT activities.

Covert gathering primarily consists of direct reconnaissance of the client's premises. These activities can involve passive activities, such as inspecting the physical security of client facilities, scanning for wireless signals, observing employee behavior, scouting for accessible areas adjacent to target buildings, dumpster diving, and making note of any visible equipment. Active covert gathering is directed more towards gathering human intelligence (HUMINT) through interaction with employees under assumed identities, as our students have done by requesting facility tours.

In a true red teaming engagement, footprinting will always begin with external methods since the team is simulating an outside threat. The more targets that can be identified through banner grabbing, the more likely students will be able to infiltrate the network remotely. If the team can successfully gain access to the internal network in the exploitation phase, internal footprinting methods can reveal the internal network range and allow for the sniffing of network traffic.

Identifying protection mechanisms is also critical to the success of any penetration test. With protection mechanisms accounted for, students will be better able to apply exploitation techniques and minimize detection. Therefore, students should identify protections for network, host, application, storage, and user resources during their intelligence gathering activities.

5.1.2 Threat modeling. Threat modeling involves applying models to identify security risks for a given target, such as a system, individual, or organization (Shostack, 2014). This process involves identifying the most desirable assets, determining the internal and external threat actors most interested in acquiring the assets (Table 4), and assessing the likely attack vectors they might pursue. The threat modeling process helps students develop realistic attack strategies, especially when planning social engineering attacks.

Internal	External
Employees	Business Partners
Management (executive, middle)	Competitors
Administrators (network, system, server)	Contractors
Developers	Suppliers
Engineers	Nation States
Technicians	Organized Crime
Contractors (with their external users)	Hacktivists
General user community	Script Kiddies (recreational/random hacking)
Remote Support	

Table 4. Potential Internal and External Threat Agents ("Threat Modeling," 2015)

For example, once students put themselves into the role of a threat actor, it is easier for them to identify attack methods that they otherwise might not recognize. The threat models should leverage the intelligence gathered about the client in the previous step and focus on threats to the client's business assets and processes. There are several tools available designed specifically for threat modeling, such as OWASP's Threat Dragon (https://threatdragon.org) and IriusRisk (https://iriusrisk.com/threat-modeling-tool/).

5.1.3 Vulnerability analysis. Once enough information has been obtained and threat models are taking shape, students should begin drafting their initial task proposals to assess suspected vulnerabilities. These activities are considered vulnerability analysis. This step involves careful planning and considerable research, so instructors should help students nurture early ideas into well formulated proposals by the end of the planning phase. For example, students should consult Offensive Security's Exploit Database (https://exploit-db.com) and research specific Common Vulnerabilities and Exposures (CVEs) as early as possible to ensure that enough time can be spent learning how to execute a given exploit (https://cve.mitre.org). Before planning a specific attack, it is always important to determine whether pursuing a suspected vulnerability is within scope. If it is not, students must still document the CVE in their report so that the client is made aware of the potential issue. Even still, instructors should never approve the execution of any exploit that falls within the scope of the assessment if students cannot successfully demonstrate they understand and have accounted for any potential risks to a client. Regular proposal review on at least a weekly basis will help students progress through their planning and research more efficiently.

5.2 Execution

The Execution phase consists of the exploitation and post-exploitation steps of the PTES. To meet the repeatability requirement outlined by Dimkov, Pieter, and Hartel (2010), we execute multiple attempts of our assessment activities whenever possible. For example, we will often target multiple employees with the same phishing email. However, some of our activities cannot be repeated without jeopardizing subsequent assessment tasks. Instead, we recommend that these activities be re-attempted during the client's next assessment. Subsequent red teams can refer to the detailed explanations provided in our report.

5.2.1 Exploitation. During the exploitation step, students conduct more refined social engineering attacks and attempt to exploit systems with suspected weaknesses identified in the vulnerability analysis step. For example, rather than rely on broad phishing campaigns, spear phishing is used to target specific employees and vishing helps establish a pretext for site visits. Although the amount of time spent on various attack methods has varied from client to client, all three engagements have included both technical and social engineering attacks. Many assume that hacking into a business would mostly consist of highly technical attacks, but social engineering has proven to be far more effective for us. In addition to the textbook resources, Mouton, Leenen, and Venter (2016) also provide several examples of social engineering attacks. Regardless of the outcome or the methods employed, students are required to immediately record the results of their exploitation attempts to ensure that all relevant details are captured. Obvious recommendations should also be noted, but most are left for the reporting phase. Since the intent behind any security assessment is to help the client, students must understand that reporting positive findings is equally important.

5.2.2 Post-exploitation. Successful exploitation of client assets will inevitably lead to additional opportunities. Any new information gained should be quickly incorporated into subsequent activities, effectively returning the team to the planning phase for that task. Given the time constraints of a red teaming engagement, it is helpful if students have already anticipated and planned for post-exploitation activities so that the assessment can continue with as little delay as possible.

One of the safest ways to demonstrate successful exploitation of an asset is to plant a flag that can be verified by the client after the engagement has concluded. For example, if students gain physical access to a client facility, they could hide a small token, take a picture or video, and detail it in the report. Prior to moving to the reporting phase, instructors should always collect letters of engagement from students and make it clear that all ongoing activities are to cease.

5.3 Reporting

The final phase of the course consists of condensing the hundreds of pages of information and results into an easily digestible report for the client. Results should be organized by category. The report narrative should adequately describe the findings, and supporting documentation should be included to provide detailed explanations. The report should also include suggestions for resolving each negative outcome, as well as a recommended mitigation plan that begins with addressing the most critical issues. Identified risks should be quantified by accounting for the event probability, threat actor capability, existing controls, and estimated loss per successful event.

During the pilot, students were unable to fully complete the written report because not enough time was allocated. To address this issue and better satisfy Dimkov, Pieter, and Hartel's (2010) reportability requirement, modifications were made to ensure that all assessment activities are logged, and task specific reporting is completed immediately following execution. The use of the Dradis Framework has significantly improved the report quality and efficiency. By organizing report content within Dradis through the PTES template, much of the reporting phase can be spent researching mitigation steps and cleaning up the exported report file, which is available in both Microsoft Word or HTML formats.

In lieu of a final exam, the students present their findings to the executive team of the client organization during their regularly scheduled final exam period. Once the assessment report has been completed, students must then identify the key findings to discuss during the client presentation. Each team member is expected to add their content to the presentation but speaking responsibilities are often handled by a representative from each task team. Client questions are directed to the member most responsible for planning or executing that aspect of the assessment. Following the presentation, all property, such as a copied key, is returned to the client and look-alike domains used to phish the client are scheduled for transfer.

After making any necessary edits identified in the client discussion portion of the presentation, the finalized report contents are encrypted and delivered to the client. Clients are also provided with each student's activity report and other supplementary material to help them understand the full breadth of our engagements.

5.4 Course Reset

Once all engagement activities have concluded, instructors must immediately revoke student access to all assessment resources. Instructors can then revert to a snapshot of the Dradis database. If you want to retain certain phishing templates and landing pages to repurpose in future sections of the course, you can assign ownership to the instructor's account by changing the userid to the instructor account by modifying the records in the GoPhish database. Once these changes have been made and all client information has been deleted from the database, a new snapshot should be created.

6. STUDENT EVALUATION

Student evaluation was originally difficult due to the unique nature of this course. Since we were not sure what to expect for the pilot, we included alternate activities in case the assessment had to be terminated prematurely. For example, we asked students to draft a chapter for a best practices handbook and had them present their recommendations to university faculty and staff. Fortunately, our pilot was highly successful due to the hard work of the high-achieving students we invited to participate. After adjusting the required components of the course, we have settled on a point distribution that we believe fairly balances student workload with assessment goals (Table 5). Course activities will now be evaluated based upon performance on quizzes, information shared through activity reports and team updates, completion of reflection papers, and the overall quality of their portions of the assessment report and client presentation. However, assessment activities are still primarily evaluated subjectively based upon demonstrated effort and creativity.

6.1 Quizzes

Given the amount of work students must conduct outside of class, quizzes simply serve to ensure students read the assigned chapters of the required textbook to prepare for the PenTest+ certification exam. This is reflected in the point total, as quizzes only account for just 10 percent of the course grade, and the fact that we also drop their lowest quiz score. All 11 quizzes are to be completed during the planning phase so that students familiarize themselves with the penetration test process at the beginning of the course. This allows them to focus entirely on the client during the execution and reporting phases. Note that Chapter 5, Mobile Device and Application Testing, is not covered since we are unlikely to have the opportunity to test client-owned mobile devices during our engagements and we never intentionally interact with employee-owned devices.

6.2 Activity Reports

To ensure that assessment tasks and other class activities are completed on schedule, all students must briefly summarize their progress and plans in their activity report from week 2 through week 11. With the addition of Dradis, students now continuously log activities in their own Dradis note. Task-specific information is stored in separate nodes, so students simply include a reference to the appropriate node when updating their activity reports. In addition, each task group is required to share their progress on assigned activities to the class on a weekly basis.

6.3 Reflection Papers

Although students have responded to a reflection survey at the conclusion of the course, we intend to adopt Spears' (2018) approach by incorporating reflection papers prior to the start of the course and after each assessment phase. This will allow me to better evaluate learning expectations and course outcomes at various stages of the assessment process.

6.4 Assessment Report

The assessment report is the most critical component of the course and represents 25 percent of a student's course grade. For the most part, grading the assessment report should be straightforward. For example, when all students put forth consistent effort and address the issues you share with them from week to week, applying an overall team grade to each student is certainly appropriate. However, there might be instances where some students do not carry their weight. For those cases, determining the grade for the report should then be tied to the execution and reporting of their assigned tasks throughout the assessment.

6.5 Client Presentation

Evaluating the client presentation has been the most rewarding aspect of the course. Students are excited to finally discuss their hard work outside of the red team and help the client improve their security posture. We use a standard presentation rubric to evaluate the team's practice presentation to help them improve. Then, we and the client provide additional feedback following the final presentation. Just as with the report writing, there might be rare cases where a student would not deserve to receive the same grade as the rest of the team, but these issues usually manifest themselves far sooner than the presentation.

Component	Points Per Item	Total Points	Percentage
Quizzes (10)	10	100	10%
Activity Reports (10)	10	100	10%
Team Updates (10)	30	300	30%
Reflection Papers (4)	25	100	10%
Assessment Report	250	250	25%
Client Presentation	150	150	15%
	TOTAL	1000	100%

Table 5. Point Distribution

7. COURSE OUTCOMES

This course has generated several beneficial outcomes. First, our clients have benefited from the performance of low-cost, but effective, security assessments. While our teams have not had much, if any, prior experience with penetration testing, their success in identifying and exploiting vulnerabilities has clearly demonstrated that if amateur security professionals can compromise your business, experienced hackers with malicious intent are likely to have little difficulty. This helps our clients recognize the urgent need to plan and budget for regular security assessments.

Second, the students benefited by gaining practical experience by conducting a real-world security assessment. Many students have shared that simply listing the course on their résumé led to the course being the primary topic of interview conversations. This has resulted in a large majority of our students securing internships and full-time employment in information security roles, with some offered to immediately join penetration teams as entry-level employees. Third, some students elected to extend their course experience by participating in the academic research process, including authoring research papers and presenting at conferences. These outcomes are reflected in the comments from standard student evaluations of teaching. Select comments are included in Appendix G. We also have students conclude the term by offering suggestions and sharing lessons learned from which students in future sections of the course will benefit. Select student responses to this survey are provided in Appendix H.

Fourth, we benefited by discovering new opportunities for pedagogical and security research. For example, we plan to publish additional pedagogical research describing our approach to specific assessment activities. We also intend to publish client-approved articles discussing the results and recommendations from our engagements so other organizations can better protect against the threats we have identified and exploited. Lastly, the institution benefited from positive public response and increased external engagement, which has led to increased interest in our security programs and will likely result in the generation of additional service-learning opportunities.

8. CHALLENGES FACED

The course was first offered a year earlier than originally planned to make it available to the group of students recruited to participate in the pilot since a large majority of these students were on schedule to graduate within the next three semesters. While we were fortunate to successfully implement this course in a condensed timeframe, we highly recommend ensuring that adequate time is allotted to develop the necessary infrastructure and complete all pre-assessment steps.

Even though students are excited to explore new techniques, participating in the course can sometimes be overwhelming due to the scale and open-ended nature of the project. Instructors should guide students through the planning and execution of each task but should not be afraid to let the students fail. However, some students might not admit that they are having trouble out of a fear of doing something wrong or being labeled a failure. In most cases, simply providing reassurance that you are there to protect them from doing anything that could get them into trouble and to guide them whenever they struggle is all that is needed to keep them moving forward. Therefore, we highly recommend that instructors speak with each student individually at least once a week to ensure that all students have a clear understanding of how to complete their tasks to keep any members of the team from falling behind.

Instructors should do their best to resist mission creep by sticking to the course schedule. Once students gain momentum, it can be tempting to allow them to extend task execution into the reporting phase. Doing so will only create an unnecessarily stressful final month and result in weakened client deliverables. To ensure that this deadline remains firm, we recommend that the letter of engagement only authorize assessment activities from the class start date to the end of the execution phase, not the end of the semester. Upon reaching the deadline, instructors must rescind approval for any outstanding assessment activities.

9. FUTURE DEVELOPMENT

Past offerings have focused our efforts on a single client; however, a planned seat increase could potentially allow for up to three clients to be assessed simultaneously. Students from other disciplines will also be invited to participate in future iterations of the course. For example, theater majors with extensive experience with improvisational theater will be able to assist with social engineering engagements, and nursing students could assist in the assessment of clients in the medical field.

Experiences from this course will now be introduced to students earlier in anticipation of the students' matriculation to the advanced course. For example, additional training on social engineering methods, as well as the assessment tools employed, such as Buscador, Kali Linux, and GoPhish, will be provided during the existing prerequisite information security courses, which will reduce the learning curve. An additional prerequisite course is also planned to provide students with practice exercises tailored to further develop penetration testing skills.

10. CONCLUSION

While the course requires careful planning and oversight, it has provided students with valuable, real-life experience that is already being well-received by prospective employers. Further development and evolution of this course will only strengthen the curriculum at our institution and further enhance the security of local organizations. Therefore, we strongly encourage faculty at other institutions to implement similar courses.

11. ACKNOWLEDGEMENTS

The course described in this article would not have been possible without the hard work of the first Bradley Red Team: Alex Alicea, Justin Burkhart, Kerstyn Campbell, Angelica Fanti, Steven Kellerhals, Maggie Musquez, Samantha Roseman, Zachary Sells, Ethan Supler, Alex Sutter, and Matt Weiss. We must also give a special thanks to David Scuffham for his guidance and support. This research was supported by Bradley University's Center for Cybersecurity.

12. REFERENCES

Aman, J. R., Conway, J. E., & Harr, C. (2010). A Capstone Exercise for a Cybersecrity Course. *Journal of Computing Sciences in Colleges*, 25(5), 207–212.

Amit, I. I. (n.d.). Penetration Testing Execution Standard Mind Map. Retrieved August 6, 2020, from http://www.iamit.org/docs/Penetration_Testing_Execution_Standard.mm.

Anderson, L. W., Krathwohl, D. R., & Bloom, B. S. (2001). *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*. White Plains, New York: Longman.

Bazzell, M. (2018). *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information* (6th ed.). North Charleston, South Carolina: CreateSpace Independent Publishing Platform.

Bishop, M. (2007). About Penetration Testing. *IEEE Security & Privacy Magazine*, 5(6), 84–87.

Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (1956). *Taxonomy of Educational Objectives: Handbook I: Cognitive Domain*. New York, New York: David McKay Company.

Ceraolo, J. P. (1996). Penetration Testing through Social Engineering. *Information Systems Security*, 4(4), 37–48.

Dieterle, D. W. (2016). *Basic Security Testing with Kali Linux 2*. North Charleston, South Carolina: CreateSpace Independent Publishing Platform.

Dimkov, T., Pieters, W., & Hartel, P. (2010). Two Methodologies for Physical Penetration Testing using Social Engineering. In *Proceedings of the 26th Annual Computer Security Applications Conference on - ACSAC '10* (pp. 399–408). New York, New York: ACM Press.

Fulton, E., Road, O. R., Lawrence, C., & Clouse, S. (2013). White Hats Chasing Black Hats: Careers in IT and the Skills Required To Get There. *Journal of Information Systems Education*, 24(1), 75–80.

Furco, A. (1996). Service-learning: A Balanced Approach to Experiential Education. *Expanding Boundaries: Serving and Learning*. Washington, D.C.: Corporation for National Service.

Hackney, R. A., McMaster, T., & Harris, A. (2007). Using Cases as a Teaching Tool in IS Education. *Journal of Information Systems Education*, 14(3), 229–234.

Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking*. Indianapolis, Indiana: Wiley.

Hall, L. L. & Johnson, R. D. (2011). Preparing IS Students for Real-World Interaction with End Users Through Service Learning. *Journal of Organizational and End User Computing*, 23(3), 67–80.

Hayes, D. R. & Cappa, F. (2018). Open-Source Intelligence for Risk Assessment. *Business Horizons*, 61(5), 689–697.

Herzog, P. (2010). *Open Source Security Testing Methodology Manual* (3rd ed.). Barcelona, Spain: ISECOM. Retrieved August 6, 2020, from https://www.isecom.org/OSSTMM.3.pdf.

Hill, J. M. D., Carver, C. A., Humphries, J. W., & Pooch, U. W. (2004). Using an Isolated Network Laboratory to Teach Advanced Networks and Security. *ACM SIGCSE Bulletin*, 33(1), 36–40.

Kim, P. (2015). *The Hacker Playbook 2: Practical Guide to Penetration Testing*. North Charleston, South Carolina: CreateSpace Independent Publishing Platform.

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education*, 28(2), 101–114.

Lee, R. L. (2012). Experience is a Good Teacher: Integrating Service and Learning in Information Systems Education. *Journal of Information Systems Education*, 23(2), 165–177.

Lending, D. & Vician, C. (2012). Writing IS Teaching Tips: Guidelines for "JISE" Submission. *Journal of Information Systems Education*, 23(1), 11–18.

Logan, P. Y. & Clarkson, A. (2005). Teaching Students to Hack: Curriculum Issues in Information Security. *ACM SIGCSE Bulletin*, 37(1), 157.

Meucci, M. & Muller, A. (Eds.). (2014). *OWASP Testing Guide* (4th ed.). Bel Air, Maryland: OWASP Foundation. Retrieved August 6, 2020, from https://www.owasp.org/images/1/19/OTGv4.pdf.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social Engineering Attack Examples, Templates and Scenarios. *Computers & Security*, 59(June), 186–209.

Mouton, F., Malan, M. M., Kimppa, K. K., & Venter, H. S. (2015). Necessity for Ethics in Social Engineering Research. *Computers & Security*, 55, 114–127.

National Information Assurance Education & Training Programs. (n.d.). CAE Requirements and Resources. Retrieved March 31, 2019, from https://www.iad.gov/nietp/CAERequirements.cfm.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)*. Gaithersburg, Maryland.

Nutting, R. (2018). *CompTIA PenTest+ Certification All-in-One Exam Guide (Exam PT0-001)* (1st ed.). McGraw-Hill Education.

O'Leary, M. (2006). A Laboratory-Based Capstone Course in Computer Security for Undergraduates. In *Proceedings of the 37th SIGCSE technical symposium on Computer science education* (Vol. 38, pp. 2–6). Houston, Texas.

Pike, R. (2013). The "Ethics" of Teaching Ethical Hacking. *Journal of International Technology and Information Management*, 22(4), 67–75.

Plachkinova, M. & Maurer, C. (2018). Security Breach at Target. *Journal of Information Systems Education*, 29(1), 11–20.

Ponemon Institute. (2018). *2018 Cost of a Data Breach Study: Global Overview*. Retrieved August 6, 2020, from https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf.

Pritchard, S. (2010). Navigating the Black Hole of Small Business Security. *Infosecurity*, 7(5), 18–21.

PwC. (2014). *Managing Cyber Risks in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015*. Retrieved August 24, 2020, from https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

Renaud, K. & Weir, G. R. S. (2016). Cybersecurity and the Unbearability of Uncertainty. In *Proceedings - 2016 Cybersecurity and Cyberforensics Conference, CCC 2016* (pp. 137–143).

Rogers, R., Fuller, E., Miles, G., & Cunningham, B. (2005). *Network Security Evaluation Using the NSA IEM*. Rockland, MA: Syngress.

Rogers, R., Miles, G., Fuller, E., Hoagberg, M. P., & Dykstra, T. (2004). *Security Assessment: Case Studies for Implementing the NSA IAM* (1st ed.). Rockland, MA: Syngress.

Sauls, J. & Gudigantala, N. (2013). Preparing Information Systems (IS) Graduates to Meet the Challenges of Global IT Security: Some Suggestions. *Journal of Information Systems Education*, 24(1), 71–73.

Shen, A. (2018). NDSU Students Legally Hack Into University's Network. *KVRR*. Retrieved August 6, 2020, from https://www.kvrr.com/2019/03/13/ndsu-students-legally-hack-into-university-network/.

Shostack, A. (2014). *Threat Modeling: Designing for Security*. (C. Long, Ed.) (1st ed.). Indianapolis, Indiana: Wiley.

Spears, J. L. (2018). Gaining Real-World Experience in Information Security: A Roadmap for a Service-Learning Course. *Journal of Information Systems Education*, 29(4), 183–202.

Talamantes, J. (2014). *The Social Engineer's Playbook: A Practical Guide to Pretexting*. Woodbury, Minnesota: Hexcode Publishing.

Threat Modeling. (2015). Retrieved August 6, 2020, from http://www.pentest-standard.org/index.php/Threat_Modeling.

Twitchell, D. P. (2006). Social Engineering in Information Assurance Curricula. In *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development - InfoSecCD '06*, 191.

Verizon. (2018). *2018 Data Breach Investigations Report*. New York, New York. Retrieved August 6, 2020, from https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.

von Konsky, B. R., Miller, C., & Jones, A. (2016). The Skills Framework for the Information Age: Engaging Stakeholders in Curriculum Design. *Journal of Information Systems Education*, 27(1), 37–50.

Wagner, P. J. & Wudi, J. M. (2004). Designing and Implementing a Cyberwar Laboratory Exercise for a Computer Security Course. *ACM SIGSCE Bulletin*, 36(1), 402–406.

Walker, M. (2017). *CEH Certified Ethical Hacker Bundle*. (B. Horton, Ed.) (3rd ed.). New York, New York: McGraw-Hill Education.

Weidman, G. (2014). *Penetration Testing*. San Francisco, CA: No Starch Press.

AUTHOR BIOGRAPHY

Jacob A. Young is an assistant professor of management information systems and director of the Center for Cybersecurity at Bradley University. He earned his doctorate from Louisiana Tech University. He focuses his research on privacy, security, and anonymity issues related to information systems with a specific focus on whistleblowing. He serves as the Senior Advisor on Cybersecurity at the National Whistleblower Center in Washington, D.C. His research has been presented at several regional and national conferences, as well as published in journals, such as *AIS Transactions on Human-Computer Interaction*, *Journal of the Midwest Association for Information Systems*, and *DePaul Business & Commercial Law Journal*.

APPENDIX A: LETTER OF ENGAGEMENT

_____ ("Client") hereby authorizes the following individuals of _____ ("Assessment Team") to conduct security assessment activities.

[Insert List of Faculty and Students]

Statement/Scope of Work: Client authorizes Assessment Team to conduct security assessment activities pertaining to the applications, systems, networks, and facilities owned by Client as described below.

- Application security of websites, e-mail clients, operating systems, and software are in scope. Systems hosted by third parties are NOT in scope.
- System security of Client-owned workstations, mobile devices, access controls, and equipment are in scope. Information Security and Systems Administration computers are in scope. Employee-owned computing devices are NOT in scope.
- Network and physical security of routers, firewalls, servers, switches, access points, printers, and Internet of Things (IoT - embedded devices) are in scope.
- Operational security of policies, procedures, and employee practices, to include social engineering and garbage/recycling disposal are in scope.

Rules of Engagement: The following restrictions shall apply to this authorization:

- This authorization shall be in effect from _____ until _____.
- Members of the Assessment Team must not willfully damage any application, system, facility, or piece of property belonging to Client while conducting the assessment.
- If Client asset(s) are damaged, Assessment Team agrees to notify Client immediately.
- It is understood that Assessment Team will execute all tests according to the best practices in the industry and that all measures will be taken to avoid disrupting usability and performance, damaging Client's networks and systems as well as the data contained within such networks or systems. Denial of Service (DoS) is NOT allowed.
- If Assessment Team discovers a security breach or a vulnerability deemed critical enough that it should be remediated immediately in Client networks, Assessment Team will interrupt all tests immediately, document the breach or vulnerability, and notify Client. Assessment Team shall suspend all further testing unless and until Client authorizes Assessment Team to proceed with the testing as planned.

Pursuant to granting this authorization, Client declares that:

- Client owns the systems to be tested, and the undersigned has the proper authority to allow Assessment Team to perform security verification activities.
- Client has created a full backup of all systems to be tested and has verified that the backup procedure will enable Client to restore systems to their pretest state.
- Client understands that the assessment necessarily involves the use of network tools and techniques designed to detect security vulnerabilities, that it is impossible to guarantee that no unexpected reactions to testing will occur, and that it is impossible to identify and eliminate all the risks involved with the use of these tools and techniques.

_____	_____	_____	_____
Client	Date	Student/Faculty	Date

APPENDIX B: LETTER OF AUTHORIZATION ("GET OUT OF JAIL FREE CARD")

[Date]

To Whom It May Concern:

This letter is to confirm that I authorize the following individuals to perform tests on our networks from both internal and external locations. Additionally, I authorize the following individuals to perform on-site social engineering to glean information to assist in the penetration test.

1) From _____ until _____, the following individuals have permission to scan the organization's computer equipment to find vulnerabilities and assess the physical security of network equipment owned by _____, generally located at _____.

2) I, _____, have the authority to grant this permission to assess the security of the computer assets owned by _____.

3) Should any individual or member of law enforcement need to confirm the authorization granted in this letter, he or she may contact me via the following.

Office: (____) ____ - _____
Mobile: (____) ____ - _____
Email: _____

APPENDIX C: STUDENT WHITE HAT AGREEMENT

As part of this course, you will be exposed to systems, tools, and techniques related to information security. Used properly, these tools allow a security or network administrator to better understand vulnerabilities and security precautions. Misused (either intentionally or unintentionally), these tools can result in breaches of security, damage to data, or other undesirable results.

You must agree to the following before you can participate. If you are unwilling to sign this form, then you cannot participate in this course.

I agree to:

- Examine only the areas outlined within the scope stated in the letter of engagement.
- Report any security vulnerabilities discovered to the course instructors immediately, and not disclose them to anyone else.
- Maintain the confidentiality of any client information learned through the course.
- Hold harmless the course instructors and _____ for any consequences of this course.
- Abide by the computing policies of _____ and by all laws governing use of computer resources on campus.

I agree to NOT:

- Attempt to gain administrator access to any server, network hardware or other network device in order to increase in privilege on any _____ workstation.
- Disclose any private information that I discover as a direct or indirect result of this course.
- Take actions that will modify or deny access to any data or service not owned by me.
- Attempt to perform any actions or use utilities in the course outside the confines and structure of authorized security assessment activities.
- Exploit any security vulnerabilities beyond the client scope or beyond the duration authorized by the client.
- Pursue any legal action against the course instructors or _____ for consequences related to this course.

Executed as of the date and year below:

_____ _____

Student Date

APPENDIX D: NON-DISCLOSURE AGREEMENT

This Agreement is made and entered into by and between _____ and the undersigned [student/faculty] at _____ ("[Student/Faculty]") for the purpose of receiving certain confidential information of _____ ("Company") to enable the class to undertake the Project described at the end of this Agreement ("Project").

Company and [Student/Faculty] hereby agree as follows:

1. "Confidential Information" means proprietary and confidential information of Company.
2. No information will be Confidential Information that: (i) is already known to [Student/Faculty], or
3. (ii) is or becomes publicly known through no wrongful act of [Student/Faculty], or (iii) is received by [Student/Faculty] from a third party without similar restrictions and without breach of this Agreement.
4. Except as provided herein, [Student/Faculty] will not disclose any Confidential Information to any other person. [Student/Faculty] will not use any Confidential Information other than in connection with the Project.
5. [Student/Faculty] may disclose Confidential Information (i) to other students or faculty who have executed non-disclosure agreements with Company.
6. Company understands that to complete the requirements of the course in which [Student is enrolled/Faculty teaches], he or she must give a presentation concerning the Project to an audience that might not have signed non-disclosure agreements. Accordingly, such presentation may contain information about the Company, but will not contain Confidential Information about the Company. In such settings, Company shall only be identified as a "business in [state]."
7. All Confidential Information delivered by Company to [Student/Faculty] will be and remain property of Company. All Confidential Information, and any copies thereof, will be promptly returned to Company at the end of the Project.
8. The obligations of [Student/Faculty] under this Agreement shall continue for five years following the conclusion of the Project.
9. This Agreement may not be modified except by written instrument signed on behalf of each party. This Agreement embodies the entire agreement and understanding of the parties and terminates and supersedes all prior independent agreements and undertakings between the parties. The provisions of this Agreement shall be construed in accordance with the laws of the state of [state]. All notices, requests or consents given in connection with this Agreement shall be given in writing and sent by first class mail, postage prepaid to the addresses listed at the end of this Agreement, unless either party notifies the other party of a different address.

Description of Project:

The primary purpose of this project is to provide students with an opportunity to plan and perform a security assessment for a local client. The assessment will attempt to discover vulnerabilities in various aspects of the client organization, which may include, but is not limited to, physical security, network security, and social engineering. Upon completion of the assessment, the project team will present Company with a report detailing the vulnerabilities discovered and suggested remedies for each.

Executed as of the date and year below:

_____	_____	_____	_____
Client	Date	Student/Faculty	Date

APPENDIX E: TEXTBOOK RESOURCES

Red Teaming

Title	Author(s)	Year
Red Team Field Manual (RTFM)	White, Alan J	2017
Red Team: How to Succeed by Thinking Like the Enemy	Zenko, Micah	2015

Methodologies

Title	Author(s)	Year
CompTIA PenTest+ Certification All-in-One Exam Guide (Exam PT0-001)	Nutting, Raymond	2018
Network Security Evaluation Using the NSA IEM	Russ Rogers	2005
Security Assessment: Case Studies for Implementing the NSA IAM	Russ Rogers	2004
Threat Modeling: Designing for Security	Shostack, Adam	2014
CEH Certified Ethical Hacker Bundle, Third Edition (All-In-One)	Walker, Matt	2017

Open Source Intelligence Gathering

Title	Author(s)	Year
Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information	Bazzell, Michael	2018
Nmap: Network Exploration and Security Auditing Cookbook	Calderon, Paulino	2017
Google Hacking for Penetration Testers, Third Edition	Long, Johnny	
Complete Guide to Shodan	Matherly, John	2016
Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks	Zalewski, Michal	2005

Social Engineering

Title	Author(s)	Year
Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails	Hadnagy, Christopher	2015
Social Engineering: The Art of Human Hacking	Hadnagy, Christopher	2011
Unmasking the Social Engineer: The Human Element of Security	Hadnagy, Christopher	2014
No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing	Long, Johnny	2008
Ghost in the Wires: My Adventures as the World's Most Wanted Hacker	Mitnick, Kevin D.; Simon, William L.	2012
The Art of Deception: Controlling the Human Element of Security	Mitnick, Kevin D.; Simon, William L.	2003
The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers	Mitnick, Kevin D.; Simon, William L.	2005
The Social Engineer's Playbook: A Practical Guide to Pretexting	Talamantes, Jeremiah	2014

Penetration Testing

Title	Author(s)	Year
The Browser Hacker's Handbook	Alcorn, Wade	2014
Advanced Penetration Testing: Hacking the World's Most Secure Networks	Allsopp, Wil	2017
Ethical Hacking and Penetration Testing Guide	Baloch, Rafay	2015
Hands-On Penetration Testing on Windows	Bramwell, Phil	2018
Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework	Bullock, Jessey	2017
Wireshark (R) 101: Essential Skills for Network Analysis (Wireshark Solutions)	Chappell, Laura	2017
Security Data Visualization: Graphical Techniques for Network Analysis	Conti, Greg	2007
Basic Security Testing with Kali Linux 2	Dieterle, Daniel W.	2018
Hacking: The Art of Exploitation	Erickson, Jon	2008
Penetration Tester's Open Source Toolkit	Faircloth, Jeremy	2016
Kali Linux Revealed: Mastering the Penetration Testing Distribution	Hertzog, Raphael	2017
Metasploit: The Penetration Tester's Guide	Kennedy, David	2011
The Hacker Playbook 3: Practical Guide to Penetration Testing	Kim, Peter	2018
Basic Hash Cracking	Mad76e	2016
Network Security Assessment: Know Your Network	McNab, Chris	2016
Network Analysis Using Wireshark 2 Cookbook	Nainar, Nagendra Kumar; Ramdoss, Yogesh; Orzach, Yoram	2018

Web Penetration Testing with Kali Linux	Najera-Gutierrez, Gilberto; Ansari, Juned Ahmed	2018
Gray Hat C#	Perry, Brandon	2017
Metasploit for Beginners	Rahalkar, Sagar	2017
Kali Linux: Wireless Penetration Testing Beginner's Guide	Ramachandran, Vivek; Cameron Buchanan	2015
Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems	Sanders, Chris	2017
Black Hat Python: Python Programming for Hackers and Pentesters	Seitz, Justin	2014
Black Hat Python	Seitz, Justin	2015
Kali Linux – An Ethical Hacker's Cookbook	Sharma, Himanshu	2017
Metasploit Penetration Testing Cookbook	Teixeira, Daniel; Singh, Abhinav; Agarwal, Monkia	2018
Mastering Kali Linux for Advanced Penetration Testing	Velu, Vijay Kumar	2017
Penetration Testing: A Hands-On Introduction to Hacking	Weidman, Georgia	2014

Reporting

Title	**Author(s)**	**Year**
Complete Guide to Internet Privacy, Anonymity & Security	Bailey, Matthew	2015
Practical Cyber Intelligence	Bautista Jr., Wilson	2018
Hiding from the Internet: Eliminating Personal Online Information	Bazzell, Michael	2018
The Complete Privacy & Security Desk Reference: Volume I: Digital (Volume 1)	Bazzell, Michael; Carroll, Justin	2016
CISO Desk Reference Guide: A Practical Guide for CISOs	Bonney, Bill; Hayslip, Gary; Stamper, Matt	2018
Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft	Cole, Eric; Ring, Sandra	2005
Escape the Wolf: A Security Handbook for Traveling Professionals	Emerson, Clinton	2009
Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats	Gardner, Bill	2014
How to Measure Anything in Cybersecurity Risk	Hubbard, Douglas W.; Seiersen, Richard	2016
Blue Team Field Manual (BTFM)	White, Alan J.; Clark, Ben	2017

APPENDIX F: SUGGESTED COURSE SCHEDULE

Phase	Week	Class	Team Activity	Ch.	Lecture/Quiz Topic
Planning	1	1	Sign Legal Documents	1	Pre-engagement Activities
		2	Lab Tutorial / OSINT	12	Reporting and Communication
	2	3	OSINT Update	2	Getting to Know Your Targets
		4	OSINT Update	3	Network Scanning and Enumeration
	3	5	OSINT Update	4	Vulnerability Scanning and Analysis
		6	OSINT Update	6	Social Engineering
	4	7	Team Forming		
		8	Planning Update	7	Network-Based Attacks
	5	9	Planning Update	8	Wireless and RF Attacks
		10	Planning Update	9	Web and Database Attacks
	6	11	Planning Update	10	Attacking Local Host Vulnerabilities
		12	Planning Update	11	Physical Penetration Testing
Execution	7	13	Execution Update		
		14	Execution Update		
	8	15	Execution Update		
		16	Execution Update		
	9	17	Execution Update		
		18	Execution Update		
	10	19	Execution Update		
		20	Execution Update		
	11	21	Execution Update		
		22	Execution Update		
Reporting	12	23	Report Generation		
		24	Report Generation		
	13	25	Report Generation		
		26	Report Generation		
	14	27	Report Generation		
		28	Practice Presentation		
	15	29	Client Presentation		

APPENDIX G: SELECT STUDENT COMMENTS FROM TEACHING EVALUATIONS

What were the strengths of the course? Why?
New course gave us the opportunity to set systems up and do research.
Enjoyed going to class each week because we got to pick what we wanted to be involved in, learning this information in his other classes then actually doing it here.
We got the opportunity to focus on aspects we were most interested in while still learning something new.
It was a pilot class so everything we were doing was brand new and exciting.
I learned more than any other MIS course and it helped me get an internship.
It's awesome to get the real-life experience to work with a client. This course has helped me learn a lot.
The course gave hands on experience with a Red v. Blue team. This is valuable knowledge and resume material.
I really liked all the security assessment tasks we did. I learned a lot about hacking and security concepts. It was a really cool and unique class.
This class does a great job of giving students real world experience of ethical hacking and improving teamwork and presentation skills.
I appreciated [the instructor's] excitement when we succeeded. He understood where we were coming from, like each of our educational backgrounds were different and he let us each shine doing what were we interested in.

APPENDIX H: STUDENT REFLECTION RESPONSES

What was the most enjoyable aspect of this project?
Getting to brainstorm and try all the interesting attack vectors we came up with and getting the opportunity to present in front of the CIO.
Doing the info gathering. Finding out and using Google hacking/open Intel tools.
The most enjoyable aspect of this project was the freedom of designing and implementing our own assessment tasks. As well as being able to use professional tools pen testers would also use against clients.
Learning the different approaches used in a Pen Test, it was interesting seeing us adapt after getting reported.
Being able to come up with ideas on how to get information from the client. Also, being broken up into teams and working on specific attacks.
I think that being able to do penetration testing on a real-life client, and a client that we knew very well was very fun. Also, being able to see the different types of penetration we could do was very interesting.
I really enjoyed using Kali and experimenting with the things on that. I also really enjoyed creating the Phishing email and sending that out to the employees in order to possibly trick them.
Overall, I really enjoyed performing all the assessment activities that I participated in for the class.
I really enjoyed the hands-on experience of the class. I think it was fun seeing what other people were working on as well. I liked that it wasn't a structured environment that didn't allow you to explore.

What recommendations do you have for future members of the red team?
Always brainstorm by staying aware of our surroundings. You never know what new details will appear, or new ideas you get just from walking around.
Get as much info as possible at the start of the project. Plan a lot of attacks and do as many as you can. Plan more attacks with the info you get from the previous ones. Don't be afraid to do tasks and research outside of class.
My recommendation for future members would be to take on as many tasks as possible and learn what it takes to be a pen tester from all angles.
There is so much to learn from this class, but you must be able to want to learn it. Make sure you are trying to learn new things and different programs to not only get more from the client but to get more from the class.
Just go for it, but get permission first.
Make sure that you read the material and check out the books, because those two things helped a lot. Also, don't be discouraged when you don't get results right away, because if you keep trying and have patience, you may get results eventually. It's important to stick with what you're doing and be willing to try something new.
I would make sure the students know that this takes a lot of time outside of the class room.

If you could go back to the beginning of the semester, what would you tell yourself that would have helped you be more successful?
Doing the network scanning was the most challenging aspect of the project, because the client has very good network protection set in place. We were able to get several results from the Nmap scans, but when we tried to examine further using OpenVAS, we were largely unsuccessful. Also, the time constraint was a little difficult for the Phishing email, because it took a little while to figure out the technical issues.
Most challenging aspect was first starting out. Not having much of a direction to go in. It was difficult to know where to go and what to do.
Keep working, and don't get demoralized because nothing seems to be happening.
Just because something hasn't happened yet, doesn't mean that your project won't be the one to start it.
Do your tasks on time, do more independent research, and think more about how to use the info gathered.
I would have requested more tasks to take on with my chosen assessment.
Use time to your advantage, nothing needs to happen in short periods, but as long as you set a safe plan, you can get results.
Learn more about different aspects of pen testing. I was more focused on the phishing and social engineering side of things, but I would have also liked to learn more about programs in Kali. Don't be afraid to ask for help if you didn't know what you were doing.
I would tell myself to do more research early in the semester so that I could try to perform more scans over the course of time. I feel like we waited too long to start scanning the network to find vulnerabilities, and that is why we didn't produce many results through those activities.
If I could go back, I think I would have liked to play around more with Kali. I would like to be able to experience all the different aspects to understand it better.
What was the most challenging aspect of this project?
Actually performing the assessment tasks we came up with. We were all unsure if they would work, but once one group was successful, the rest of us got a jumpstart on the projects.
Staying on task and putting in the effort outside of class.

The most challenging aspect was executing social engineering.
Mostly it was to find a direction to head in and how to go about this. 379 did help, but honestly it would've been better if I took it beforehand and learned all the concepts before coming into this course.
The hardest part was figuring out what to do with the information we got. Knowing what information is useful and what vulnerabilities can come of that information was the hardest.
I think that getting started on actually attacking the client was a little challenging, mainly because we didn't have the tools necessary to perform the type of test we wanted to do at the time.