Developing a Social-Engineering Course

1st Ida Ngambeki
Computer and Information Technology
Purdue University
West Lafayette, USA
ingambek@purdue.edu

2nd Grusha Ahluwalia
Computer and Information Technology
Purdue University
West Lafayette, Country
gahluwal@purdue.edu

3rd Subia Ansari
Computer and Information Technology
Purdue University
West Lafayette, USA
ansari0@purdue.edu

4th Minglu Li
Computer and Information Technology
Purdue University
West Lafayette, USA
li3603@purdue.edu

5th Glaris Lancia Raja Arul
Computer and Information Technology
Purdue University
West Lafayette, USA
grajaaru@purdue.edu

***Abstract*—This Innovative Practice Full Paper describes an implementation of a Social Engineering course. Social Engineering (SE), which is the process of obtaining unauthorized access to systems by exploiting humans, has been flagged by the FBI and US Banking Industry as a threat to national security. According to a report by McAfee, the global cost of cybercrime has exceeded $1 trillion since 2018, and an additional $145 billion was spent on cybersecurity in 2020. Research has shown that 97% of cybersecurity attacks employ some element of social engineering. This Innovative Practice paper will present an effective and hands-on course designed to introduce students to social engineering penetration testing. The course is based on a social constructivism approach to learning, where students first develop an understanding of the individual and social context of social engineering. It uniquely combines the psychology of human behavior, legal precepts, and computer science to identify how psychological principles are applied in cyberspace to exploit individuals and how the same principles can be applied during SE penetration testing to detect vulnerabilities.**

***Index Terms*—Computer education, social engineering, psychology, principles of persuasion,**

I. Introduction

In information security, Social Engineering (SE) is the process of obtaining unauthorized access to computer systems, and/or committing fraud by exploiting flaws in human decision-making. Malicious entities achieve this by using psychological tactics to influence an individual or group into revealing information that is not public or providing access that should remain restricted. PhishMe reported that social engineering scams alone stole about $5 billion worldwide from2013-2016 [1]. Social engineering is largely interdisciplinary in nature, comprising of principles from sociology, political science, psychology, management, and arts. The applications of social engineering were initially found in areas like urban planning and awareness campaigns, but recent applicationsof the discipline are now prevalent in the computing sector, specifically within the field of cybersecurity. From the information security perspective, social engineering is the art of manipulating or deceiving an individual into intentionally providing sensitive information that can then be used against them for malicious intent. Attackers who use social engineering techniques take advantage of the psychological deception of individuals because humans have been consistently found to be the weakest link in the information security chain [2][3]. The most sophisticated security systems would not hold up againsteven a novice attacker if the attacker can trick the people manning these systems into giving up sensitive information. Scenarios like this are not new, and attackers are coming up with increasingly creative methods of manipulating people, professionals and regular technology users alike, into giving them what they want. As in the past, and in the present with theevolution of cyberattacks that now leverage social engineering techniques, the discipline historically has had negative con- notations attached to it because of the deceptive tactics that are used. Particularly from the cybersecurity perspective, it is important to understand how attackers use social engineering tactics to be able to protect oneself against such attacks, and to take preventative measures against attacks instead of solely investing in mitigation efforts later.

However, due to the novelty of this knowledge domain in cybersecurity, there are a limited number of courses that train students in ethical SE penetration testing practices. Currently, graduate-level courses on SE are limited because the topic finds itself between an intersection of sociology, psychology, technology, computer science, and criminology. The few courses that do exist, take a computing approach and focus less on the underlying psychology and more on technicalities and tools of SE along with its defenses. There is less understanding of why humans make the decision to expose the technical vulnerabilities or violate security policies (knowingly or unknowingly). This highlights the need for an effective course that introduces students to social engineering

fundamentals. In this paper, the researchers present a course that comprehensively explains how cybercriminals exploit human decision-making process using psychology while incorporating the technical aspects of penetration testing and reporting procedure. Throughout the course, students identify and describe techniques of SE, explain the underlying psychological principles, plan and execute a simple social engineering attack and design strategies to prevent or mitigate SE attacks. Since the course was designed based on the theory of social constructivism of learning, students were encouraged to develop knowledge through collaborative learning activities. More specifically, students were required to practice SE attacks on individuals and organizations, keeping in mind the social engineering code of ethics.

Understanding how this course was designed will aid those preparing for social engineering instruction and other aspects of cybersecurity education to better understand the defense and mitigation techniques necessary to conduct effective SE penetration testing and design appropriate security policies and procedures.

II. Literature Review

A. History of Social Engineering

Social engineering, in the scope of political science where it was first determined as a discipline, broadly refers to efforts undertaken by entities to influence popular social attitudes and behaviors. The term (*sociale ingenieurs*) was first coined by Dutch industrialist J.C. Van Marken in 1894 [4]. At the time, the premise of social engineering was to understand and handle problems of the human nature, instead of only focusing on improvements to machines and their processes. The goal of social engineering then was to analyze, influence and understand social systems to such an extent that decisions could be made effectively in a scientific manner. These decisions were generally made to exact social control and promote specific narratives over large urban areas.

The principles of social engineering were not necessarily restricted to public policy initiatives, and motivations began to expand from exacting social control to understanding human nature to the extent of exploiting certain aspects of inherent human dispositions. The advent of basic computing and communication technologies in the 1960s and 1970s gave rise to new social engineering tactics that were still based on the original psychological standards and principles, but with added intentions for self-serving purposes. One of the earliest examples of this in the technology space was phone phreaking, in which computer hackers studied phone systems extensively in order to manipulate the system to make free phone calls [5]. Social engineering tactics have evolved since then, in part to keep up with advances in technology and complexities associated with exploring newer systems. Modern-day social engineering attacks leverage characteristics associated with newer technologies, but also rely heavily on existing information about non-verbal behavior, psychological traits, decision making and mannerisms of people in order to be successful [6].

B. Types of Social Engineering Attacks

In the age of technology and widespread use of the internet, attackers need not interact with people face-to-face to carry out social engineering attacks. There are different kinds of social engineering attacks and tactics that exploit commonly held notions and attitudes that people have. Attacks that leverage social engineering techniques can be roughly classified depending on whether it is conventionally technical or non-technical in nature. Most times, the non-technical tactics are used prior to or in conjunction with technical attacks [7]. Irrespective of the medium used, all SE attacks are largely based on the widely researched theories of persuasion. Dr. Robert Cialdini's Principles of Persuasion, Message Learning Theory, Impression Management Theory, Social Judgement Theory, and the Elaboration Likelihood Model are some exemplars of theories that explain persuasion in the context of SE, that is, why people can be persuaded into divulging information or performing actions that may not be in their best interest.[8] Types of attacks that leverage these psychological principles along with other technical attack vectors include phishing, smishing, vishing, pretexting, tailgating, dumpster diving[9][10]. The most popular type of social engineering attack that has become increasingly prevalent in cyberspace is phishing. In phishing attacks, attackers impersonate an entity or use a previously compromised account to solicit sensitive information from unsuspecting individuals via emails. Phishing attacks are effective because the content of the emailsor messages are phrased in a manner meant to evoke a response from the target in the form of clicking on a malicious link, downloading malicious files or replying with sensitive information. Pretexting is another type of social engineering attack where attackers assume a fictitious background in order to build relationship based on trust with their target [11]. Attackers build their background to appear credible to their target. This is achieved by conducting extensive information gathering on their target, including searches on social media or other publicly available information sites. Tailgating is a social engineering technique where the attacker gains access into unauthorized areas by entering the premises alongside those with authorized access to the areas. To successfully execute the tailgating technique, attackers must be able to blend in with their surroundings and be prepared to look the part and account for unexpected situations that might act as barriers to entering the premises. Vishing attacks are similar to phishing attacks, with the difference being that attackers solicit information from their targets over phone calls. Attacks like Business Email Compromise (BEC), watering holes and quid pro quo techniques are sub-categories of above mentioned attacks. These are largely technical in nature, but still prey on attitudes of innate curiosity and greed to get individuals to partake unintentionally in certain activities like clicking on links, downloading malware or leaking sensitive information.

C. Impact of Social Engineering

Social engineering has largely become relevant in cybersecurity due to the prolific nature of social engineering attacks,

the ease with which attackers can incorporate relevant social engineering techniques into traditional modes of cyber-attacks, and the characteristic of taking advantage of basic human nature to execute malicious actions. These attacks cost millions of dollars in financial losses, wreak havoc on hardware and software systems, compromise data privacy and integrity, and disrupt regular business services, among other negative consequences. The 2019 Internet Crime Report released by the Internet Crime Compliant Center of the FBI stated that one of the most prevalent crime types reported was phishing/vishing. Crimes such as fraud schemes that targeted the elderly reported some of the highest losses, with adjusted losses in excess of $ 835 million. Compromised email accounts or business accounts cost over $ 1.7 billion in financial damages [12]. Unsurprisingly, these kinds of attacks have also been steadily increasing over the past years. More than 80% of security incidents that are reported tend to be phishing attacks [13], and 94% of malware is sent by email [14]. As more and more entities attempt to implement technical countermeasures, attackers are getting more creative with the way they use social engineering tactics to trick people into falling for these attacks. Therefore, it is important to understand social engineering tactics so that people can be educated about the dangers of such attacks and have the right training and support to respond to, or at the very least mitigate the effects of, these attacks. Having some knowledge about the basic tenets of social engineering techniques can enable individuals to be vigilant in both online environments and the physical world. With worldwide cybercrime financial losses slated to cost about $ 6 trillion annually by this year [14], it is important now more than ever that all individuals, and not just companies or large entities alone, know how to detect and avoid social engineering-based attacks and tactics.

D. Penetration Testing

"Penetration testing is the exploitation of vulnerabilities present in an organization's network" [15]. It is a part of security evaluation process where an ethical hacker (a pen-tester) simulates an attack on the entity in a controlled and organized manner in the face of realistic threats to identify weaknesses in the security systems that protect a set of identified important assets. Penetration testing is typically performed by a licensed pen-tester after obtaining a signed contract from an organization or entity, and the results of the test are provided in a report which also discusses potential measures or solutions that can be implemented to narrow the identified vulnerabilities.

In social engineering, penetration testing plays a pivotal role when it comes to identifying potential vulnerabilities in the network and security threats to an organization. Since social engineering involves the exploitation of humans, the weakest component in a network, the process of penetration testing involves determining what extent an organizations employee can exploit their knowledge of the organization's secrets, and to ascertain the organization's vulnerability to the exploit. The process tests employees' adherence to security policies defined by the organization, while simultaneously determining the level of security awareness amongst employees' and the success of the security training provided by the organization. For example, one of the most common social engineering methods is the phishing email exploit where pen-testers fake the identity of an individual in upper management and require the target to download an attachment, visit an unauthorized website or provide sensitive information. Another common method is vishing, where the pen-tester makes a voice call pretending to be an individual the target would trust and ask them to provide sensitive information.

Penetration testers must typically go through three common phases which form the baseline of each test; 1. Reconnaissance, 2. Execution, 3. Delivery [16]. There can be more phases in the test corresponding to the needs of the organization and terms of the contract. In the reconnaissance phase, information about the target network is gathered, this process can be automated using OSINT tools such as the Social Engineering Toolkit (SET) [17]; in the execution phase, the attack is carried out based on the information gathered in the reconnaissance phase; and in the third phase, documentation must be performed to point out weaknesses identified in the network, the threats they pose and mitigation recommendations [16].

Shebli et. al. [18] defined the three phases in pen-testing; in the first step, which is the test preparation phase, documents are collected and finalized, scope and objective of the test are specified, and contracts are signed. In the second step, test implementation, information gathering is performed to identify what information is required to perform vulnerability required and collect that information using automated tools if needed, in this phase the tester also performs vulnerability analysis and exploits. Finally, in the test analysis phase, the tester provides a document reporting and summarizing the process, technical details, assessment findings, risk level indication overview, budget estimate and recommended steps to avoid the exploitation of vulnerabilities.

This process resembles the process of hacking or scamming, but what makes it different is the fact that testing in this case is carried out legally with the permission of the owner of system, who employ penetration testers to identify all possible vulnerabilities to prevent such attacks from occurring. It is imperative that all parties involved sign a contract of mutual agreement before performing the test. Social engineering pen-testing is different due to the human factors involved because to evaluate security awareness amongst employees' and the success of the security training provided to them, an understanding of human psychology and behavior is important.

E. Social constructivism

Social constructivism is a learning theory that explains how humans learn knowledge and considers learning as a social process based on the socio-cultural context. It also underlines that learning depends on interacting with teachers, colleges, parents, and so on [19][20][21]. To be more specific, during the process of learning, students exploit the information they

already know to fit new knowledge [22]. Social constructivismalso states that communication within the group of peers can evolve understanding during learning [23]. Social constructivism as a framework might reveal the way people interact with others and illustrate how people's ideas are generated from experience [24][25]. In practice, four things are essential for constructing a social constructivism learning environment: teachers will share information with students, both teacher andstudent have authority, the teacher's job is to serve as a guide during learning, and maintaining a small number of learning groups [24]. It has become an increasingly popular frameworkin the area of computer science education [26][27].

According to social constructivism, it is essential to acknowledge the students' current knowledge system and then guide them to the accepted theory. There is no absolute wrong with students' cognition of concepts. Even though there are many misconceptions in computer science education, these should not be treated as fatal mistakes but opportunities for inquiry to correct and advance learning. Misconceptions can happen a lot, but it is a way to construct 'correct' knowledge [26]. For example, business students and computer science students might have different perspectives when it comes to the same concept. Social constructivism can help students adjust their knowledge models if they miss the vital concept [27]. In [28], the author illustrates one way to apply social constructivism to practice: "(a) learners construct their own knowledge, participating in authentic activities and internalizing the tools of practices, (b) learners are reflective beings, they can think and reflect on their lived experiences, (c) socialinteraction/ dialogue plays a crucial role in learning". The differences between a constructivism classroom and a traditional classroom are as follows: "(a) Curriculum emphasizes big concepts, beginning with the whole and expanding to include the parts. (b) The pursuit of student questions and interests is valued. (c) Materials include primary sources of material and manipulative materials. (d) Learning is interactive, building on what the student already knows. (e) Teachers have a dialogue with students, helping students construct their knowledge. (f) The teacher's role is interactive, rooted in negotiation. (g) Assessment includes student works, observations, and points of view, as well as tests. The process is as important as the product. (h) Knowledge is seen as dynamic, ever-changing with our experiences. (i) Students work primarily in groups." [22]

It has been proven that social constructivism is one promising framework to learn computer science concepts, also can adapt to other approaches very well [8]-[12]. According to [28], "Students had developed ways of communicating, reasoning, and providing arguments to defend their ideas as they participate in and contribute to the norms and practices of their learning communities." It is believed that the model of social constructivism can help students construct knowledge, and the principles can be applied to computer science education with better outcomes [26]. The model also has been verified that it has valuable properties for learning computer science concepts and suitable for adapting to other non-cognitive approaches [27]. It also can improve student's ability to solve problems, as well as the understanding of software engineering issues [29]. Social constructivism can also have a significant result in a virtual environment [30].

The Social Engineering course described here takes this social constructionist approach to learning. Students work together in pairs or small groups over a range of activities. Students are encouraged to draw on their experiences with cybersecurity from prior courses, internship and other work experiences, and having been the target of cybersecurity attacks. Students are also required to engage in peer education wherein they learn from each other.

III. Existing Courses

The following section is a brief overview of existing social engineering courses, offered in different formats. It constitutes, four online courses, one professional in-person course and one undergraduate course taught at University of Arizona.

A. Social Engineering attack and defenses (UA South)

This advanced upper division Junior/Senior level course in Social Engineering is a part of the curriculum for Cyber Operations Bachelor of Applied Science (BAS) degree at University of Arizona. The course is offered in Face-to-Face, Hybrid, and Fully Online formats as an elective in the Defense and Forensic Track. The track *requires* students to have knowledge of Algebra, networking and security principles, and python programming. The course intends to teach how the principles of influence and manipulation are used to "trick a user into violating a security policy", different types of delivery methods, embedded file analysis, using browsers for malware infection, mitigation strategies to defend the human, endpoint and network from a SE using Ethical Hacking and Social Engineering tests to develop policies and procedures for enhancing any organization's security posture [31].

B. Advanced Social Engineering Training (Social-Engineer, LLC)

Designed and written by Christopher Hadnagy, this four day long professional course is typically taught in-person (now virtual) and costs $2800. It is supposedly the only performance-based SE training course that combines lectures, discussions, hands-on exercises along with demonstrations to prepare the students for Social Engineering Pen-test Profession (SEPP) certification. This course focuses on self-analysis through DISC assessment, research-based learning, learning "Social and psychological skills of the trade" like Influence, Rapport building and tactics of elicitation. It also dives into understanding human decision process, reading and using non-verbal behavior. As this course provides guidance on how to include SE in penetration testing, the instructions include documentation and reporting of findings along with debrief and feedback from professional pen-testers. Interestingly, this course is not only targeted towards security professionals, but also psychologists, social scientists, and sales professionals [32].

C. Social Engineering (Cybrary)

Social Engineer by Ken Underhill is a 2 hour 14 min, beginner's course targeted towards students prepping for EC-Council Certified Ethical Hacker (CEH) or Comp-Tia Pentest+. This short-course is part of the Career Path: Become a Penetration Tester and recommends students who take this class should be security professionals who have a basic knowledge of penetration testing and security policy principles, and who have worked in the IT industry for at least two years. It intends to educate students on how SE plays a vital role in ethical hacking, understand different types of SE attacks, behavioral and technical controls, communicate basic security awareness and perform SE attacks step by step, from imitation through exploitation. The course revolves around methods used by criminals to exploit humans, execute SE methods and how to use methods ethically to gather intelligence. It mainly covers topics like targeting, exploitation life-cycle, digital profile reduction, digital information gathering, psychology of social engineering, cold calling, elicitation, pretexting, post exploitation among others [33].

D. Social Engineering for Penetration Testers (SANS)

This two-day SANS course that fulfills 12 Continuing Professional Education (CPE) credits is targeted towards penetration testers and other security professionals. Overall, the first day of the course focuses on social engineering fundamentals, reconnaissance, and Phishing. The second day focuses on payloads (malware), pretexting, physical pen-testing and reporting. The course specifically focuses on principles of per- suasion and psychology foundations that help craft SE attacks, tools and labs that provide technical skills to create malware and track phishing campaigns, tailgating, and physical access. The course ends with a capture the flag (CTF) for students to practically apply the learned skills [34].

E. Learn Social Engineering from Scratch (Udemy)

Developed by Zaid Sabih and zSecurity, this course dives deep into SE to teach beginners with no previous hacking experience, the 'practical side' of SE, along with 24/7 support for Q&A. This three-to-four week-long course is divided into sections, typically based on various steps of a SE attack. The first section on information gathering covers how to pick a target, discover target's information and build an attack strategy. The second section on Generating Malware covers creating custom malware (backdoor, keylogger, embedded MS docs) based on the chosen attack strategy. SE techniques like pharming, phishing, fake updates, etc. that can be used to deliver the custom malware to target, are covered in the third section. The fourth section on post-exploitation teaches techniques to interact with the hacked system (Win, Linux, Mac OS X, Android) by accessing file systems, maintaining access, escalating privileges and also using compromised systems to hack other systems. The course then ends with learning "how to protect yourself and your systems" from SE. Currently, it costs $139.99 [35].

F. The Complete Social Engineering: Phishing & Malware (Udemy)

This course is developed for beginners, by Muharren AYDIN. The course description claims to teach, "how to ethically apply social engineering." Covering the main terminology of SE, creation and distribution of malware, OSINT to gather information, phishing mails, vishing techniques and tools like Epire Project, MSFvenom, veil and TheFatRat, makes this course quite similar to the one discussed before, however the duration of this course is estimated to be 4-5 hours and costs $89.99 [36].

G. Tools

A social engineer's toolbox will have everything from lock picking tools to sophisticated software technologies to carry out successful attacks. Some of the most common tools are:

- The Social Engineer Toolkit(SET) -[37][38] SET was written by David Kennedy, founder and CEO of TrustedSec. It is a well-supported, open-source pen-testing tool driven by python that is used to perform advanced SE attacks. SET can be downloaded from a github repository. The user can choose different attacks from this menu driven attack system, for instance, Spear-Phishing, SMS Spoofing, Infectious Media Generator, and Wireless Access Point attacks.
- Maltego is another OSINT and forensic tool that allows user to automatically fetch data about a person-of-interest and puts it in a visual format that can help find links between pieces of information using data correlation, graphical-link analysis, mindmaps, etc. The gathered data like social media information, emails, websites, apps used, domain information, etc. could be very useful for a social engineer for reconnaissance. [39]
- Burner Phones are inexpensive, prepaid mobile phones. They are popularly used for malicious activities as they can be disposed of after quick use and prevent tracking [40].
- Lock Picking Tools help social engineer pen-testers for testing the physical security of an organization by trying to gain access to buildings, file cabinets or other areas where sensitive information can be found [41].
- Spy gadgets like Cameras, glasses, GPS Trackers, recorders, voice changers, etc.
- Card readers and card printers to decipher and create ID cards.

IV. The Social Engineering Course

A. Course Structure

The Social Engineering course is structured into four major areas. Each of these is made up of 2-6 modules taught over a 16-week period. The course uses elements of social constructivism such as small group work, peer instruction, active learning, and the use of authentic activities to support learning. Assignments are distributed across the entire 16-week period culminating in a course project.

B. History, Ethics and Law of Social Engineering

The first part of the course is intended to introduce the students to the context of social engineering. Students are taken trough the history of social engineering so they can understand the origin of the term, how it evolved over the centuries, and how is it has particularly been applied variously in cybersecurity. This historical view helps them understand the complexity of the social engineering landscape. It also prepares them for the ongoing evolution of social engineering tactics and effects.

Students then use a case study approach to identify and examine some of the ethical issues in social engineering. As a requirement of being a social engineering penetration tester, they will regularly engage in deceptive and manipulative behavior. It is important that they have a strong grounding in ethics so they do not cause damage to individuals and to the reputation of the field in pursuit of security. They are also introduced to what little law does exist governing social engineering. This includes laws regarding fraud, impersonation, harassment, defamation, recording and the use of other SE tools, privacy, and the Computer Fraud and Abuse Act.

C. The Psychology of Social Engineering

This section forms the core of the course. It is designed to be the most important section for three reasons. 1) An ability to manipulate and therefore a deep understanding of human behavior is the basis of social engineering. The primary task of the social engineer is to get the target to compromise their own security - hence the term "human hacking". If a student masters the psychology, they have a strong foundation for social engineering that they can build other skills around. 2) The majority of the students in this course are majoring in cybersecurity and so are competent in most of the technical skills required for social engineering from their other courses. They simply need to learn to apply these skills in a social engineering setting. 3) No other course available to professionals that we have found provides students with this deep grounding in psychology. Unlike many other skills of social engineering, this is knowledge that is not readily available to them in any other social engineering training.

The section on psychology begins with an introduction to what is considered the core element of an individual's psychology - personality. Students explore the question of what personality is and the different ways in which personality is measured. Students then learn the major theories of personality across the six domains and five traditions viz. dispositional, biological, intra-psychic, cognitive experiential, socio-cultural, and adjustment across the psychoanalytic theories, the humanistic theories, the social cognitive theories, the trait theories, and the bio-evolutionary theories. They then learn how this understanding of personality works in action. They take tests to measure their own personalities and engage in simple activities to identify how various elements of different personalities would affect social engineering scenarios.

The next section on psychology deals with authority and empathy. Research has demonstrated that empathy is the most essential skill for any social engineer. It is more important than the ability to improvise, than technical skills, and the ability to act. In this module students explore the difference between sympathy and empathy, the components and empathy, the empathetic process, and various models of empathy. Students then examine how empathy is related to helping behavior. They then learn how to evoke empathy and harness helping behavior in social engineering situations. In the section on authority, students learn the different forms of authority, why and how authority works, and how to encourage obedience.

The following section deals with persuasion. This is arguably the core of the social engineering enterprise, the ability to persuade individuals to engage in behavior that compromises their security. Here students learn about attitudes and attitude change and how that is linked to behavior. They also learn the major theories of persuasion: conditioning and modeling theories, message learning, judgmental, motivational, attributional, self-persuasion, social influence, and combinatory approaches. For each of these they examine real world examples an discuss how these can be harnessed in social engineering settings. Special attention is paid to the Cialdini model of persuasion since this is most useful from a practical social engineering perspective [42].

The last module in the psychology section focuses on non-verbal behavior. It is essential for social engineers to understand this since over 70% of communication is non-verbal. Here students learn about communication pathways and non-verbal cues. Students are introduced to kinesics, paralinguistics, proxemics, and olfactics. Students spend time observing non-verbal behavior in various mediums, practice expressing themselves non-verbally, and learn to read other students' non-verbal cues.

All of these discussions of psychology are taught using a range of materials including lectures, readings, audio recordings, videos, case studies, and in-class activities. The conclusion of each section is also followed by a short quiz.

D. The Tools of Social Engineering

This section of the course deals with the practical skills necessary for social engineering. These range from interpersonal skills such as the ability to gain information from talkingto people and being able to impersonate others, to technical/practical skills like picking locks and setting up phishing campaigns. These include elicitation, pretexting, information gathering and organization, open-source intelligence, threat modeling, attack vectors, physical security, report writing, and SE tools. In this section the activities center around applying these skills including lock picking practice, pick pocketing, acting and improvisation, charming and disarming, and eliciting information. This is accompanied by technical cybersecurity skills.

E. The Prevention and Mitigation of Social Engineering

This section of the course is important to round out the students' education in social engineering. They not only need to know how to perform social engineering, they must also be

be able to defend against social engineering and teach others to do so. Many cybersecurity penetration testers, in addition to testing security, are also asked to help companies prepare for security threats by training their employees and improving their security policies. Students therefore need to know how to create effective training programs to teach individuals about social engineering. In this section we emphasize skills that move training beyond raising awareness to actually being able to recognize and act when targeted by social engineering. Students also learn how to write effective policy that encompasses the difficult to identify, often nebulous, rapidly evolving threats from social engineering.

F. Course Activities

Students explore these issues through a variety of activities and assignments. Each course period starts with peer instruction. Each student is required to identify a real- life case of social engineering. The student then has to describe the major elements of the case including the target of the attack, the attack vector, the primary and secondary social engineering attacks used, the psychological factors that are exploited, the aftermath of the attack, and how such attacks could be mitigated. This peer instruction process has several advantages:

- Students are able to learn from each other. Peer instruction gives students the opportunity to learn from other students. This helps the instructing student to develop presentation skills, to think deeply about topics, organize their knowledge and plan the transmission of that knowledge. [29]
- It encourages engagement. All the students in the class have an opportunity to participate with peer instruction and are therefore more present. It also requires those who may be hesitant to speak up and interact. [43]
- Authentic learning. Students have the opportunity to apply the knowledge that they have learned in class to a real-world analysis. This allows them to see that the knowledge they are gaining in class is relevant to real life situations. This helps give the knowledge value. It also requires them to apply their knowledge in new contexts which promotes transfer [43].

Students engage in at least one short activities in every course period throughout the semester. These are specific to the topic being discussed that day. They range from short 5 minute to longer 30-minute activities. They are usually completed in groups of 2 or 3. These short activities are intended to break up the lecture and allow students to apply some principle or practice knowledge. These include active listening exercises during discussions of elicitation, improvisation activities during sessions on pretexting and impersonation, face reading exercises during discussions of non-verbal behavior, and lock picking exercises during lessons on physical security.

Students also have longer assignments due approximately every two weeks. These assignments are designed to bring together multiple elements of a portion of the class and give the students practice in a skill that will be necessary for their final course project. These larger assignments include a recon report that requires them to use their skills learned in information gathering, information organization, target identification, and open- source intelligence techniques to compile a detailed report on an individual and describe how that information could be used to target the individual. Another example is the development of an attack plan which requires them to use skills learned in information gathering, threat modeling, attack vectors, and identifying vulnerabilities to create a comprehensive plan for a single penetration test. Each of these assignments is completed individually. This ensures that all students have mastered the skills they will need to successfully complete that large course project which is undertaken as a group.

The major course assignment is a group project. Each group of 3-4 students is given a real-world client. They are then required to undertake the entire social engineering penetration test process. They must make initial contact with their client and determine their needs, they draft the contract with the client (based on a template provided), they secure the Get Out of Jail Free letter, they undertake initial reconnaissance, complete a threat analysis, plan their attacks, execute their attacks, prepare a report for the client, complete a debriefing with the client, and potentially provide training materials or update policy to address any security shortcomings. This is usually carried out over the last month of the semester. This final project gives the students the opportunity to apply all the skills covered during the course in a real-world setting. During this process, the instructor functions only as a guide for the students as recommended by the tenets of social constructivism.

V. Conclusion

This paper describes the implementation of a social engineering course. This course is designed on the principles of social constructivism. Students engage in peer instruction, active learning, and authentic learning to learn and practice the principles of social engineering penetration testing.

References

[1] “NIST SP 800-63 Digital Identity Guidelines.” / (accessed May 01, 2021).

[2] Lineberry, S. (2007). The human element: The weakest link in information security. Journal of Accountancy, 204(5), 44.

[3] Aloul, F. A. (2012). The need for effective information security awareness. Journal of advances in information technology, 3(3), 176-183.

[4] “Social engineering (political science),” Social engineering (political science) — Project Gutenberg Self-Publishing - eBooks — Read eBooks online. [Online].

[5] J. M. Hatfield, “Social engineering in cybersecurity: The evolution of a concept,” Computers Security, vol. 73, pp. 102–113, 2018.

[6] C. Hadnagy, P. Ekman, and P. F. Kelly, Unmasking the social engineer: the human element of security. Indianapolis, IN: Wiley, 2014.

[7] Hinson, G. (2008). Social engineering techniques, risks, and controls. EDPAC: The EDP Audit, Control, and Security Newsletter, 37(4-5), 32-46.

[8] M. Dainton and M. Dainton, “Applying communication theory for professional life,” in Applying communication theory for professional life: a practical introduction, Los Angeles: SAGE, 2004, pp. 103–131.

[9] “Attack Vectors,” Security Through Education. https://www.social-engineer.org/framework/attack-vectors/ [accessed May 01, 2021].

[10] "The Most Common Social Engineering Attacks [Updated 2020]," Infosec Resources, 06-Aug-2020. [Online]. Available: https://resources.infosecinstitute.com/topic/common-social-engineering-attacks/. [Accessed: 01-May-2021]
[11] C. M. University, "Social Engineering: Pretexting and Impersonation - Information Security Office - Computing Services - Carnegie Mellon University," 20-Feb-2020. [Online]. Available: http://www.cmu.edu/iso/news/2020/pretexting.html. [Accessed: 01-May-2021]
[12] "FBI Releases IC3 2019 Internet Crime Report — CISA." [Online]. Available: https://us-cert.cisa.gov/ncas/current-activity/2020/02/12/fbi-releases-ic3-2019-internet-crime-report (accessed May 01, 2021).
[13] "Top cybersecurity facts, figures and statistics — CSO Online."[Online]. Available: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html (accessed May 01, 2021).
[14] R. S. Updated: 3/16/2021, "134 Cybersecurity Statistics and Trends for 2021 — Varonis," Inside Out Security, Jan. 13, 2020.[Online]. Available: https://www.varonis.com/blog/cybersecurity-statistics/ (accessed May 01, 2021).
[15] S. Bavisi, "Chapter 22 - Penetration Testing," in Computer and Information Security Handbook, J. R. Vacca, Ed. Boston: Morgan Kaufmann, 2009, pp. 369–382.
[16] I. Yaqoob, S. Hussain, S. Mamoon, N. Naseer, and J. Akram, "Penetration Testing and Vulnerability Assessment," Aug. 2017.
[17] M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, "Panning for gold: Automatically analyzing online social engineering attack surfaces," Computers Security, vol. 69, pp. 18–34, Aug. 2017.
[18] H. M. Z. A. Shebli and B. D. Beheshti, "A study on penetration testing process and tools," in 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), May 2018, pp. 1–7, doi: 10.1109/LISAT.2018.8378035.
[19] L. S. VYGOTSKY, "Mind in Society: Development of Higher Psychological Processes," Edited by Michael Cole et al., Harvard University Press, 1978. [Online]. Available: www.jstor.org/stable/j.ctvjf9vz4. Accessed 2 May 2021.
[20] "CERE12-13: Combined student wikis."[Online]. Available: https://www.psy.gla.ac.uk/ steve/courses/archive/CERE12-13-safari-archive/topic3/webarchive-index.html (accessed May 01, 2021).
[21] D. Schunk, , "Learning theories: An educational Perspective (6th Ed)," Pearson Education, 2012.
[22] Bada and S. Olusegun, "Constructivism Learning Theory : A Paradigm for Teaching and Learning," 2015. /paper/Constructivism-Learning-Theory-3A-A-Paradigm-for-and-Bada-Olusegun/1c75083a05630a663371136310a30060a2afe4b1 (accessed May 01, 2021).
[23] J. Brophy, "Social Constructivist Teaching: Affordances and Constraints (Advances in Research on Teaching, Volume 9)." https://ur.zlibcdn2.com/book/893886/83e264 (accessed May 01, 2021).
[24] Creswell, J.W., "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches," SAGE Publications Inc, Apr. 14, 2021. https://us.sagepub.com/en-us/nam/research-design/book255675 (accessed May 01, 2021).
[25] J. McKinley, "Critical Argument and Writer Identity: Social Constructivism as a Theoretical Framework for EFL Academic Writing," Critical Inquiry in Language Studies, vol. 12, no. 3, pp. 184–207, Jul. 2015, doi: 10.1080/15427587.2015.1060558.
[26] M. Ben-Ari, "Constructivism in computer science education," SIGCSE Bull., vol. 30, no. 1, pp. 257–261, Mar. 1998, doi: 10.1145/274790.274308.
[27] P. Machanick, "A social construction approach to computer science education," Computer Science Education, vol. 17, no. 1, pp. 1–20, Mar. 2007, doi: 10.1080/08993400600971067.
[28] R. K. Mishra, "Social Constructivism and Teaching of Social Science," Journal of Social Studies Education Research, vol. 5, Dec. 2014, doi: 10.17499/jsser.22283.
[29] S. Hadjerrouit, "Constructivism as guiding philosophy for software engineering education," SIGCSE Bull., vol. 37, no. 4, pp. 45–49, Dec. 2005, doi: 10.1145/1113847.1113875.
[30] N. Henze and W. Nejdl, "Constructivism in Computer Science Education: Evaluating a Teleteaching Environment for Project Orie," 1998. /paper/Constructivism-in-Computer-Science-Education (accessed May 01, 2021).
[31] University of Arizona, "CYBV481 Social Engineering Attacks Defenses — Cyber Operations — CAST," Center of Academic Excellence Cyber Operations. [Online]. Available: https://cyber-operations.azcast.arizona.edu/content/cybv481-social-engineering-attacks-defenses. [Accessed: 20-Apr-2021]
[32] Social-Engineer, LLC, "Advanced Practical Social Engineering Training," Social-Engineer, LLC., 2020. [Online]. Available: https://www.social-engineer.com/training-courses/advanced-practical-social-engineering-training/. [Accessed: 15-Apr-2021]
[33] K. Underhill, "Social Engineering Course, Online Training," Cybrary, 26-Jun-2020. [Online]. Available: https://www.cybrary.it/course/social-engineering/. [Accessed: 21-Apr-2021]
[34] SANS.org, SEC567 Social Engineering for Penetration Testers. [Online]. Available: https://www.sans.org/brochure/course/social-engineering-for-penetration-testers/2022
[35] Z. Sabih and ZSecurity, "Learn Social Engineering From Scratch Course Online," Udemy, 2021. [Online]. Available: https://www.udemy.com/course/learn-social-engineering-from-scratch/. [Accessed: 24-Apr-2021]
[36] M. AYDIN, "The Complete Social Engineering, Phishing, OSINT Malware," Udemy, 2021. [Online]. Available: https://www.udemy.com/course/learn-malware-social-engineering-and-osint-for-hacking/. [Accessed: 25-Apr-2021]
[37] "Meet the Consulting, Technical Advisory Experts," TrustedSec. https://www.trustedsec.com/team/ (accessed May 01, 2021).
[38] "Experience Our Open Source Security Tools," TrustedSec. https://www.trustedsec.com/tools/ (accessed May 01, 2021).
[39] "Homepage." https://www.maltego.com/ (accessed May 01, 2021).
[40] "Social Engineering, Part 1: Scoring a Free Cell Phone," Wonder- How To. https://null-byte.wonderhowto.com/how-to/social-engineering- part-1-scoring-free-cell-phone-0130180/ (accessed May 01, 2021).
[41] C. Hadnagy, "Social Engineering: The Art of Human Hacking," 2010.
[42] R. B. Cialdini, The psychology of persuasion. New York. 1993.
[43] C.H. Crouch E. Mazur, E. "Peer instruction: Ten years of experience and results", American Journal of Physics, vol. 69, no. 9, pp. 970-977. 2001.