Why You Should Start with the Offense: How to Best Teach Cybersecurity's Core Concepts

Michael Kranch
*United States Military Academy**
www.mjkranch.com

Abstract

This paper uses a comprehensive approach to demonstrate why offensive (hacking) techniques are the best method for teaching cybersecurity's core competencies, even when the purpose of the program is to build defensive cybersecurity professionals. I analyze the concepts taught by both offensive and defensive techniques and evaluate these through several established curricular frameworks. These results demonstrate that both techniques teach the same core cybersecurity competencies. I then discuss the importance of the security mindset and lifelong learning in building successful cybersecurity practitioners, particularly due to the rapid evolution of the field, and analyze the psychological impacts of both teaching techniques. Ultimately, this analysis shows that offensive techniques, which teach the same core concepts as defensive techniques, are the best for developing the security mindset and lifelong learners - crucial outcomes from any effective cybersecurity education program.*

1 Introduction

Over the past decade, the growing shortage of cybersecurity professionals [23, 41, 49] has caused an increase in cybersecurity education programs in universities, through bootcamps, and even with programs for high school students [9, 35]. Cybersecurity education is a broad field with a large body of previous research. This research includes papers on the teaching method with a focus on gamification [17, 20, 63], frameworks for evaluating these teaching methods [11, 54, 66], and even the required skills from a cybersecurity program [25, 53]; however, no previous research as evaluated the difference between offensive and defensive education techniques, nor has a prior paper tied these three focus areas together to identify a unified best approach for cybersecurity education.

This paper demonstrates why offensive (hacking) techniques are the best method for teaching any cybersecurity program, even when the purpose of the program is to build defensive cybersecurity professionals. I start in section 2 by discussing the evolution of cybersecurity education to establish the current state of formalized cybersecurity curricula. In section 3, I assess offensive and defensive education methods utilizing several cybersecurity evaluation frameworks and show that both techniques teach the same core concepts. I then detail the physiological impacts of these two techniques in section 4. Through this discussion, I demonstrate why offensive techniques are the best method of teaching cybersecurity's core concepts and developing resilient security professionals that are lifelong learners.

2 Background

Cybersecurity is a broad field comprised of several other disciplines, encompassing elements of computer science, engineering, information systems, mathematics, and policy. Although computer security education dates back to the 1970s [6], the work of Schneider as well as McGettrick et al. first moved towards formalizing cybersecurity education in the early 2010s [47, 60], and the Cybersecurity Curricula finally established guidelines for post-secondary degree programs in cybersecurity in 2017 [11]. In this section, I will provide some relevant background information, including discussions on the rapid evolution of cybersecurity, the gamification methods used in cybersecurity education, and the importance of developing lifelong learners within any cybersecurity education program.

*The views expressed herein are those of the author and do not reflect the position of the United States Military Academy, the Department of the Army, or the Department of Defense. This paper is authored by employees of the United States Government and is in the public domain. Non-exclusive copying or redistribution is allowed, provided that the article citation is given and the authors and agency are clearly identified as its source.
The 23rd Colloquium for Information System Security Education (CISSE 23), June 10-12, 2019, Las Vegas, NV, USA

2.1 The Rapid Evolution of Cybersecurity

The rapid advancement of the cybersecurity industry will make the tools, techniques, and best practices taught today obsolete in just a few years [22]. Dodge et al. referenced the industry's rapid evolution when they established the need for core competencies in the future cyber workforce, stating, "employers and employees have struggled to keep pace with change... Because specific job roles will shift with the advent of new threats and new technologies, participants agreed competency in core skills is essential [25]." Parekh et al. also referenced this evolution when they established timelessness as a primary criteria for cybersecurity's core concepts [53].

A recent Economist report on earnings in technology jobs listed "the ability to keep learning" as a core skill because "technology is changing in unpredictable ways [29]." This report then referenced several technology companies' new recruitment policies, such as Google's, which focuses on recruiting *learning animals*. Cybersecurity expertise requires a diverse set of dynamic skills. Training a specific tool or technique will not suffice; instead, cybersecurity education should focus on a broad set of core competencies.

2.2 Cybersecurity Gamification

Gamification pedagogy is an extension of the experiential learning theory, a theory that focuses on active, student-centered learning [3]. Specifically, gamification techniques combine game mechanics, like scoreboards, challenges, and achievements, with learning objectives in an effort to motivate and engage the students. Several previous studies have addressed the positive effects of gamification on student learning, including the work of Juho Hamari, one of the most cited gamification education researchers [62].

Hamari et al. conducted a literature review of 24 peer-reviewed empirical studies on gamification across a breadth of fields [36]. In this research, they found that each of the reviewed studies determined gamification had a positive impact on engagement, and their research concluded that gamification has positive benefits and effects on education. In a follow-on paper, Hamari et al. showed that the increased engagement caused by the use of gamification "has a clear positive effect on learning and [this positive effect] is best achieved in challenging games [37]," and Banfield et al. demonstrated that gamification pedagogy increases students' intrinsic motivation [3]. Below, I will discuss the methods of gamification specifically used in cybersecurity education.

2.2.1 Cyber Defense Exercises

Cyber Defense Exercises (CDXs) date to the early 2000s [59] and were the first gamification method specifically used to teach cybersecurity [20]. In a CDX, each blue team receives a similar computer network with common running services that they must secure using a set of resources available to every team. Each blue team then defends its network against a team of attackers called the red team. These networks have emulated or real gray-team players that replicate the problems or clueless actions taken by network users. A white team (cell) serves as the exercise referees, and the blue teams are not allowed to take offensive actions against other teams.[1]

2.2.2 Capture-the-Flag Competitions

Capture-the-Flag Competitions (CTFs) are the oldest form of cybersecurity competition, with the DEF CON CTF dating back to 1996 [24]. A CTF is a generic type of competition where the players (teams) must solve challenges to recover secret information (flags) that they can submit for points. Although the CTF format can be used for many challenge types, this format most commonly features challenges utilizing offensive techniques.[2]

In 2011, Cheung et al. formally introduced teaching cybersecurity with CTFs [17]. Chapman et al. and Burns et al. discuss using CTFs to engage cybersecurity novices [12, 16], and Carlisle et al. as well as Schreuders and Butterfield introduce using CTFs to teach formal cybersecurity education [15, 63]. Finally, Gonzalez et al. establish a classification taxonomy for gamified cybersecurity resources [34].

There are two primary types of CTFs [21]. Jeopardy-style CTFs include challenges of increasing difficulty that are divided into categories like web exploitation, forensics, reverse engineering, or cryptography. In the Attack-Defense[3] format, each team starts with a similar host and network running several vulnerable services. Each team must identify these vulnerabilities and then patch their services to prevent other teams from stealing their flags. These teams must also create exploits to steal flags from other teams, and the scoring takes place in timed rounds. The DEF CON CTF is the most famous Attack-Defense CTF, with PicoCTF and DEF CON Quals being well-known Jeopardy-style CTFs [16, 24].

2.3 Lifelong Learning

Lifelong learning has been frequently identified as a required skill in the computing and technology fields due to their rapid evolution. Both the Computer Science and Information Technology Undergraduate Curricula specifically identify lifelong learning as a required outcome in graduating students as well as in their teaching faculty [2, 42], and this concept is referenced in the ACM, IEEE, Software Engineering Joint Task Force, and Association of Information Technology Professionals Code of Ethics [2, 19, 39, 40].

[1] These rules are a composite from the three most popular CDXs - the NSA's CDX [55], NCCDC [74], and CyberPatriot [72].

[2] See Section 3.2 for details on offensive techniques.

[3] *Attack and Defend* is a synonymous name for this format.

The term *lifelong learning* dates to the early 1990s, when it was defined as the "independent pursuit of learning without formal institutional support or affiliation [14]." Adding to this definition, Bentley said that successful education programs should be judged by "how well students can apply what they learn in situations beyond the bounds of their formal educational experience, and how well prepared they are to continue learning and solving problems throughout the rest of their lives [4]." More recently, lifelong learner has been associated with the concept of a *growth mindset*, which encourages effort and resilience through failure instead of focusing on achievement, is a key component of developing long-term learning [28].

Lifelong learning is also a requirement in the commercial industry. An IBM Institute for Business Value paper specifically addresses the need for lifelong learners to fill the current cybersecurity gap, listing *enjoys challenges and constantly learning* as a core attributes of successful cybersecurity professionals [75]. An Economist report showed a direct relationship between continued learning and increased earning stating, "technology firms are encouraging a growth mindset" since "training someone early to do one thing is not the solution" with the rapid evolution of technology [29].

Finally, research has identified several key factors for developing lifelong learning in students. The Oxford Handbook on Lifelong Learning lists *technical curiosity and interest*, *learning that includes feedback*, *encountering novel problems*, and *a positive feeling about learning* as attributes that all contribute to developing lifelong learners [46]. Dunlap explains that intrinsic motivation is another primary contributor to lifelong learning and that "students will expend more effort on tasks and activities they find inherently enjoyable and interesting, even when there are no extrinsic incentives [27]," and numerous studies show being challenged and persevering through this challenge is an important part of lifelong learning [3, 28, 36, 37].

3 Cybersecurity's Core Concepts Assessment

In this section, I assess the skills taught by both offensive and defensive cybersecurity techniques to demonstrate that both methods teach the same core concepts. First, I discuss several established circular frameworks to generate a comprehensive list of cybersecurity's core competencies. I then explain the difference between defensive and offensive cybersecurity techniques. Finally, I classify and analyze the skills taught by several popular cybersecurity resources to determine which core concepts are taught using these two techniques, and I conclude with a discussion of the results.

3.1 Cybersecurity's Core Concepts

To evaluate the effectiveness of both techniques in teaching future cybersecurity professionals, I first needed to identify the core concepts - the subjects that create a unifying foundation of knowledge from which our students can later build [1].[4] Due to the rapid evolution of cybersecurity, these core concepts should be timeless and not tied to current technology as well as those concepts that provide the greatest barrier to mastery of future topics [33, 53]. These concepts should be introduced early, reinforced throughout, and comprise the minimum required content for any cybersecurity program [11].

There have been several significant projects to assess and classify cybersecurity's skills and concepts. I will present three of the most complete frameworks below and discuss their ability to assess cybersecurity's core concepts.

3.1.1 National Initiative for Cybersecurity Education

The most well-known cybersecurity framework is the National Initiative for Cybersecurity Education Workforce Framework (NICE Framework). NICE started in 2010 to "help protect the nation from cyber threats by improving the cyber behavior, skills, and knowledge of the nation as a whole," and included a framework to establish consistency with regards to how cybersecurity work is defined [54]. An updated NICE Framework was published in 2017 and includes both cybersecurity work roles as well as the requisite skills for those roles [50].[5]

CyberSeek is a collaborative effort between NICE, Comptia, and Burning Glass that provides data about cybersecurity's workforce and categorizes entry, mid, and advanced-level cybersecurity positions [23]; however, these roles do not correspond to the work force roles defined in the NICE Framework. Unfortunately, the NICE Framework does not identify introductory work roles nor does it define essential skills for all work roles. Conversely, the framework's work roles are intentionally broad to allow entry, intermediate, and advanced-level capability classification within each role, and the current work role classification matrices do not differentiate KSAs between these skill levels [68]. Instead, these matrices rely primarily on previous education and certifications to differentiate between levels, making the NICE Framework not suitable for evaluation in this study.

3.1.2 Cybersecurity Curricula 2017

The Joint Task Force Cybersecurity Curricula 2017 (CSEC2017) provides curriculum guidance for academic institutions that match current cybersecurity industry

[4]The terms *fundamental knowledge*, and *essential skills* are equivocally the same as the term *core concepts*, and I use core concepts interchangeably with these terms.

[5]The new version establishes 7 Categories (a high-level grouping of common cybersecurity functions), 33 Specialty Areas (distinct areas of cybersecurity work), and 52 Work Roles (the most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities [KSAs] required to perform the tasks in a work role)

needs [11].[6] This guidance defines 8 knowledge areas (KAs) that are made up of critical concepts of broad importance within and across multiple computing-based disciplines which, collectively, represent the full body of knowledge within the field of cybersecurity.[7] For each KA, the curricula explicitly identifies which concepts are the core competencies that should be taught in every cybersecurity program. This framework is the most rigorously developed framework for assessing core concepts.

3.1.3 Cybersecurity Assessment Tools

The Cybersecurity Assessment Tools (CATS) Project provides rigorous evidence-based instruments for assessing and evaluating cybersecurity practices [66].[8] The first tool is a Cybersecurity Concept Inventory (CCI) that measures how well students understand basic concepts equivalent to the knowledge gained by a student in their first cybersecurity course. The second tool is a Cybersecurity Curriculum Assessment (CCA) that measures how well students understand core concepts equivalent to the knowledge learned after graduating from a college-level cybersecurity program. These two tools where developed through a two Delphi process in which cybersecurity experts rated topics based on importance, difficulty, and timelessness to identify the basic and core cybersecurity concepts [53].

3.2 Classification & Assessment Methodology

To compare offensive and defensive cybersecurity education techniques, I must first classify a cybersecurity education resource as offensive or defensive. I then need to assess the skills taught by that resource to determine the underlying concepts, and then evaluate those concepts with regards to the core competencies specified in the CSEC2017 and CATS circular frameworks. In assessing these skills, I focused solely on direct measures for assessing the learning outcomes from the various resources, specifically observations of students performing various cybersecurity tasks.

The first step is differentiating between offensive and defensive techniques. Defensive techniques are the traditional cybersecurity education methods which teach security concepts from a defender's perspective. Defensive cybersecurity education methods focus on learning establish security principles, implementing those principles through a set of guided procedures, and then verifying the implementation by following checklists. More recently, defensive training focuses on Security Operation Center (SOC) tactics by teaching tools, such as implementing a Security Information and Event Management (SIEM) systems [5], evaluation methods like MITRE's ATT&CK [69], and attack remediation with response playbooks [44].

Offensive cybersecurity education is the use of offensive (hacking) techniques to teach cybersecurity concepts. These techniques encompass the concepts of ethical hacking, penetration testing, or red teaming where the student utilizes an attacker's perspective to assess the security of system, focusing on the identification and exploitation of vulnerabilities [30]. Offensive techniques are used in commercial cybersecurity certifications [52, 58] and are the primary skills reinforced in CTFs like PicoCTF and Plaid [16, 51].

While there are many cybersecurity education resources, I focused on those with an explicit offensive or defensive classification. For example, I assessed the well-established traditional computer security textbook "Computer Security: Principles and Practice" by Stallings and Brown [67], but I did not use the more modern "Computer Security: A Hands-on Approach" by Du [26] since this book's labs utilize both techniques.

Commercial vendors often categorize cybersecurity training as red team (offensive) or blue team (defensive). I leveraged this established classification to differentiate between offensive and defensive skills. Specifically, I assessed several popular cybersecurity training courses offered by the SANS Institute and Offensive Security by examining the course websites, syllabuses, and lab manuals to identify the skills and underlining concepts taught within these courses [52, 58].

Finally, I leveraged the classification taxonomy presented by Gonzalez et al. to analyze and identify the core concepts taught by several popular gamification resources that feature attack-oriented content [34].

3.3 Results

Table 1 shows the combined results of the assessment with Tables 2, 3,and 4 listing the results of the CSEC2017, CCI, and CCA assessments, respectively. The core competencies provided by these frameworks contain several concepts external to the specific method of instruction. For example, instructors can incorporate *communication skills* and *legal aspects* from the CCA or *documentation* and *governance and policy* from CSEC2017 into any education program using either teaching technique. These concepts are not specifically inherent to the education technique; therefore, I excluded them from the comparison.

In total, I assessed 116 (86%) of the total 135 core concepts within this study. Of these 116 concepts, both teaching techniques covered 97 (84%) of the concepts. Offensive techniques covered 7 fewer concepts than defensive tech-

[6] This is a Joint Task Force between the Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)

[7] The areas are Data, Software, Component, Connection, System, Human, Organizational, and Societal.

[8] Not to be confused with the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool (CAT)[31].

Table 1: CCI, CCA, and CSEC2017 Core Competencies by Teaching Technique

	CCI		CCA		CSEC2017		Total	
	#	%	#	%	#	%	#	%
Core Concepts	38	-	53	-	44	-	135	-
External to Technique	0	0%	9	17%	10	23%	19	14%
Assessed Concepts	38	100%	44	83%	34	77%	116	86%
Taught by Both	30	79%	36	82%	31	91%	97	84%
Offensive Only	5	13%	1	2%	0	0%	6	5%
Defensive Only	3	8%	7	16%	3	9%	13	11%
Offensive Total	35	92%	37	84%	31	91%	103	89%
Defensive Total	33	87%	43	98%	34	100%	110	95%
Primarily Offensive	16	42%	6	14%	10	29%	32	28%
Primarily Defensive	6	16%	2	5%	5	15%	13	11%
Offensive not including Primarily Defensive	29	76%	35	80%	26	77%	90	78%
Defensive not including Primarily Offensive	17	45%	37	84%	24	71%	78	67%

niques, with the offense covering 103 (89%) of the concepts compared to 110 (95%) of the concepts being covered by the defense; however, offensive techniques primarily covered 17% more of the concepts taught by both techniques, with 32 concepts being primarily offensive compared to only 13 concepts being primarily defensive. These primarily offensive concepts included topics like *assess vulnerabilities*, *explain how to exploit traffic analysis*, and *reverse engineering* as opposed to primarily defensive concepts like *monitoring*, *ability to identify and apply best practices*, or *given a breach, explain how to recover from it*. Both types of training cover these concepts; however, they are covered in considerably more depth by one of the techniques.

One notable area of difference between the techniques was within the CCI. In this framework, offensive techniques outperformed defensive techniques in every category. This result is not surprising, as the CCI focused on the basic cybersecurity concepts and follows previous research that shows offensive techniques are the best for introducing new students to cybersecurity [12, 16].

Overall, the results of the assessment show that both offensive and the more traditional defensive techniques cover most of cybersecurity's core competencies and are rather comparable. Defensive techniques cover 6% more of the concepts, while offensive techniques cover 9% more of the concepts covered by both techniques in greater detail. These results show that either technique can be used to teach the majority of cybersecurity's core competencies. While both techniques cover the core concepts, offensive techniques are better for developing intrinsic motivation and resilience in cybersecurity students, two key components of lifelong learners.

4 The Psychological Impact of Offensive and Defensive Cybersecurity Techniques

While both offensive and defensive techniques cover the same core concepts, there is a distinct difference in the psychological impact of the two education techniques. I start this section by introducing the security mindset, a crucial component of an effective defender. I then discuss the negative impacts of defensive education methods on intrinsic motivation. I finish by explaining the positive effects of offensive education methods which, ultimately, demonstrate why offensive techniques are the best for developing future cybersecurity professionals.[9]

4.1 The [Offensive] Security Mindset

Potter and McGraw first circulated the concept of the security mindset with the idea that software testers need to use approaches grounded in *an attacker's mindset* to adequately gauge software security [56]. Kohno introduces the term security mindset [43] which was later refined by Schneier, who states, "this kind of thinking [the security mindset] is not natural for most people. It's not natural for engineers. Good engineering involves thinking about how things can be made to work; the security mindset involves thinking about how things can be made to fail. It involves thinking like an attacker, an adversary or a criminal. You don't have to exploit the vulnerabilities you find, but if you don't see the world

[9]The discussion on the psychological effects of offensive compared to defensive cybersecurity techniques often devolves into a comparison between the value of CDXs compared to CTFs, such as with Week's post on CCDC and CTFs [71] and Nighswander's response [51]. While the following discussion will include a comparison of these two important education methods, the focus is on the impact of offensive and defensive techniques in teaching cybersecurity's core concepts, particularly with regards to best developing cybersecurity professionals with a lifelong interest in the field.

Table 2: CSEC2017 Topics by Category with Technique Type (T) [O: Offensive, D: Defensive, B: Both, or -: Not Assessed]

	Skill	T	Category		Skill	T	Category
1	Basic cryptography concepts	B	Data	23	Holistic approach	B	System
2	End-to-end secure communications	B	Data	24	Security policy	B	System
3	Digital forensics	B	Data	25	Authentication	B	System
4	Data integrity and authentication	B	Data	26	Access control	B	System
5	Data erasure	B	Data	27	Monitoring	B	System
6	Fundamental design principles; least privilege, open design, and abstraction	B	Software	28	Recovery	D	System
7	Security requirements and the roles they play in design	B	Software	29	Testing	B	System
8	Implementation issues	B	Software	30	Documentation	-	System
9	Static, dynamic analysis	B	Software	31	Identity management	B	Human
10	Configuring, patching	B	Software	32	Social engineering	B	Human
11	Ethics, especially in development, testing, and vulnerability disclosure	B	Software	33	Awareness and understanding	B	Human
12	Vulnerabilities of system components	B	Component	34	Social behavioral privacy and security	B	Human
13	Component lifecycle	D	Component	35	Personal data privacy and security	B	Human
14	Secure component design principles	B	Component	36	Risk management	-	Org.
15	Supply chain management	B	Component	37	Governance and policy	-	Org.
16	Security testing	B	Component	38	Laws, ethics, and compliance	-	Org.
17	Reverse engineering	B	Component	39	Strategy and planning	-	Org.
18	Systems, architecture, models, and standards	D	Connection	40	Cybercrime	-	Societal
19	Physical component interfaces	B	Connection	41	Cyber law	-	Societal
20	Software component interfaces	B	Connection	42	Cyber ethics	-	Societal
21	Connection attacks	B	Connection	43	Cyber policy	-	Societal
22	Transmission attacks	B	Connection	44	Privacy	-	Societal

that way, you'll never notice most security problems [61]." Felten adds to this concept with his discussion of *harmless failures* - innocuous-seeming features or bugs that an attacker can chain together to accomplish something harmful [32].

This security mindset is not new. The recent Cybersecurity Curricula even addressed the importance of this adversarial security mindset, stating, "due to the adversarial nature of cybersecurity, the study of offensive or hacking techniques is often a good way to develop stronger defensive cyber skills [11]." This mindset takes time to establish and can only be developed by repeatedly thinking like an adversary about how to circumvent the security features of a system. Frequently practicing offensively oriented techniques is the best way to develop this important mindset, a mindset required by cybersecurity professionals to build and adequately test truly secure systems.

4.2 The Negative Effects of the Defense

Students who learn through traditional, defensive-oriented cybersecurity education do not develop the security mindset because they do not practice thinking like an attacker; however, this missing mindset is not the only negative psychological effect of defensive training. Defensive techniques also focus on assets, whereas offensive techniques focus on security relationships, resulting in a fundamental difference in how attackers and defenders view system infrastructure.

Lambert has written extensively on this difference between how attackers and defenders view the system. Defensively taught students focus on established procedures, security principles, and checklists that they use to defend assets [45]. Whittaker and Ford also discuss the defender's over-reliance on checklists when they said, "security checklists are important, and all developers and system administrators should use them, [but] ... checklists are not enough and, worse, they make us focus on single-point solutions and treat security as a series of bandages on top of working systems. [73]."

Conversely, attackers do not think in terms of assets but rather in terms of security relationships [45]. They leverage these relationships to build a graph of the security dependencies within the network graph and determine multiple paths to the high value assets, like the domain controller. Ultimately, attackers then use this graph to navigate through vulnerable systems and compromise the high value assets. "As long as this is true," says Lambert, "attackers win [45]."

The psychological difference is even more than the assets verses graph mentality or not having the security mindset. Fundamentally, the issue is that defensive cybersecurity ed-

Table 3: CCI Topics by Importance (I*) Including Technique Type (T) [O: Offensive, D: Defensive, or B: Both]

	Topic	T	I		Topic	T	I
1	Identify vulnerabilities and failures	B	9	20	Technology vs Policy	B	7
2	Identify attacks against CIA triad and authentication	B	9	21	Assess the risk of acting and of not acting	B	7
3	Devise a defense	D	9	22	Given a policy, devise a way to evade it	B	7
4	Identify the security goals	D	9	23	Assess the difficulty of various attacks	B	7
5	Identify potential targets and attackers	B	9	24	Rank a set of possible corrective actions	B	7
6	Devise an attack	O	8	25	Assess the risks for two different types of users	B	7
7	Given a breach, explain how to recover from it	B	8	26	Rank a set of vulnerabilities	B	7
8	Explain why a failure happened	B	8	27	Devise attacks that exploit the role of actors and information outside of the system	O	7
9	Identify risky behaviors	B	8	28	Identify and classify vulnerabilities by categories	B	7
10	Identify vulnerabilities based on usability issues	B	8	29	Identify a vulnerability	B	6
11	Identify which assumptions of a system are most likely to be exploitable	B	8	30	Identify a vulnerability in software	B	6
12	Given two security solutions, compare their pros and cons	B	8	31	Explain how to exploit a software vulnerability	O	6
13	Devise a social engineering attack	O	8	32	Solve a puzzle requiring "out-of-the-box" thinking	B	6
14	Identify new vulnerabilities caused by a change	B	7	33	Explain how to exploit traffic analysis	B	6
15	Identify vulnerabilities based on gaps between theory and practice	B	7	34	Identify ways to influence people	B	6
16	List assumptions that a system makes implicitly	B	7	35	Identify possible phishing emails from a set of samples	B	6
17	Devise a security plan	D	7	36	Devise an attack that analysts can't identify	O	5
18	Identify vulnerabilities caused by a faulty functionality or incorrect assumption	B	7	37	Given a multi-party protocol, identify vulnerabilities based on people cheating	B	5
19	Rank the relative risks of certain possible actions	B	7	38	Given a malware example, characterize its behavior	B	5

*: Importance as determined by the CATS project [66].

ucation, particularly at the introductory level, focuses on implementing procedures to prevent a compromise. Not being compromised is unrealistic both during hands-on defensive exercises as well as outside the education environment were a compromise is essentially inevitable [13]. As such, defenders feel that they have failed when they are compromised. They also miss the dopamine release that usually accompanies success since not being compromised is the expectation and not seen as a significant achievement [8]. Ultimately, these combine to have a negative effect on building intrinsic motivation.

Let us consider the student experience in the biggest defensive competitions (CDXs). First, most CDXs use professional red teams. The NSA CDX's red team features professional operators including operators from the NSA's Tailored Access Operations and the lead developer of Cobalt Strike [64]. CCDC also uses security professionals [7]. The purpose for expert red teams is to provide a standardized experience across all teams [72], but this large-skill discrepancy causes an almost insurmountable challenge that leads to frustration, particularly for younger students [57].

In addition, all CDXs contain some gamified rules, which generally favor the offense, in an attempt to simulate the conditions of a real-world network enterprise, such as the virtually unlimited time a red team would have normally, in a time-constrained competition [48]. These rules, along with the skill discrepancy, create a situation where even the top defensive teams often spectacularly fail. In the 2017 national CCDC, every team was red[10] on at least two of the twelve services, and one team was red on every service [7]. This was at the highest level of CCDC competition.

A similar experience occurs in defensive course capstones where the expert teacher attacks the students' networks and even in Attack-Defense CTFs like iCTF [70]. In Attack-Defense CTFs, teams need to identify the vulnerabilities in their provided services (challenges) to both craft exploits to launch at the other teams as well as patch these issues in their own services. These vulnerabilities range from easy to extremely difficult to identify with the best teams often unable to find all the vulnerabilities. The top teams generally start exploiting the other teams very early on. A middle team will eventually discover a vulnerability and patch a service, but other teams, particularly the top teams, are still exploiting them on their other services. Even worse, the challenges

[10]Red means the service was repeatedly not functioning as designed. All services generally start as green (i.e. functioning as designed) so a red service means the blue team broke the service with a miss-configured update or, more commonly, the service was compromised and intentionally broken by the red team.

Table 4: CCA Topics by Importance (I*) Including Type (T) [O: Offensive, D: Defensive, B: Both, or -: Not Assessed]

	Topic	T	I		Topic	T	I
1	Privacy	B	10	28	Well-known attacks, such as man-in-the-middle	B	8
2	Ethics	B	10	29	Apply symmetric and asymmetric encryption	B	8
3	Authentication	B	10	30	Operational security	-	8
4	Integrity	B	10	31	Legal aspects	-	8
5	Confidentiality	B	10	32	Economic aspects of cybersecurity	-	8
6	Secure coding	B	9	33	Countermeasures	B	8
7	Assess vulnerabilities	B	9	34	Collaboration skills	-	8
8	Analyze threats	D	9	35	Design secure protocols	D	7
9	Manage risks	-	9	36	Malware analysis	B	7
10	Operating system security	B	9	37	Perform security assessments	B	7
11	Assured operations	B	9	38	Select and apply appropriate cryptographic primitives	B	7
12	Trust, including rooting trust in hardware	B	9	39	Wireless security	B	7
13	Communication skills	-	9	40	Penetration testing	O	7
14	Ability and desire to keep up-to-date	B	9	41	Virtualization and cloud security	B	7
15	Social engineering	B	9	42	Scripting languages, systems programming, low-level programming	B	7
16	Insider threat	D	9	43	Incident analysis	D	7
17	Access control	B	9	44	Design & analyze secure web applications	B	7
18	Forensics	B	8	45	Response & recovery	D	7
19	Design & analyze secure networks	B	8	46	Formulate and evaluate security policies	B	7
20	Adversarial modeling	B	8	47	International aspects of cybersecurity	-	7
21	Attention to detail	B	8	48	Secure development lifecycle	D	7
22	Manage keys	B	8	49	Auditing	D	7
23	Cyberphysical systems	B	8	50	Ability to identify and apply best practices	B	7
24	Software vulnerability analysis	B	8	51	Ability to identify and use modern tools	B	7
25	Usable security	-	8	52	Applications of homomorphic encryption and private information retrieval	B	5
26	Balance competing objectives	-	8	53	Zero-knowledge protocols	B	4
27	Healthy skepticism and paranoia	B	8				

*: Importance as determined by the CATS project [66].

often include multiple vulnerabilities, and this middle team might later realize that the patch they implemented is not stopping all exploits.

The above experience can lead to even a middle team feeling defeated and, at a minimum, is not a positively reinforcing event for all but the top teams. Carlisle et al. specifically addresses this issue stating, "defense-only exercises can be very demotivational, as students feel like they've been bullied by the red team and that they aren't capable [15]." Defense competitions provide excellent hands-on experience and educational value, but they are not the ideal experience for building intrinsic motivation.

In traditional defensive cybersecurity education, the defender also does not often face an adversary prior to the culminating competition. As such, the defender not often experiencing meaningful failure and, therefore, does not experience the positive self-reflection that comes from simple failures nor do they develop successful coping methods to handle future failures [28, 65]. In addition, when the defender experiences failure, the adversary is not often appropriated scaled to their ability level, such as when competing against a professional red team in a CDX. Conversely, a defender's limited failures are often spectacular, such as with the thorough compromise in the final event of a CDX even after months of preparation, and can have a negative long-term impact on instinct motivation [3, 37]. Instead of being a positively reinforcing event, this type of failure decreases motivation and has harmful consequences towards developing lifelong cybersecurity professionals [57].

Traditional cybersecurity defensive techniques are proven to be better than a hands-off and not gamified method of teaching [20], and they are particularly useful for experienced cybersecurity students to learn and practice in-depth defensive techniques; however, they are not the ideal training method for teaching cybersecurity core competencies with the goal of a foundation of lifelong learning in our students.

4.3 The Positive Impact of the Offense

Offense being more exciting than defense is a fairly accepted social paradigm, and it is supported by research that shows offensive output has a significantly greater positive correla-

tion to attendance numbers than defensive output at sporting events [38]. Offense being more exciting than defensive is no different in cybersecurity, as is evident by the quirky hacker included in so many popular shows [18]. Even though defensive operations are the primary focus for most cybersecurity programs, educators should leverage the popularity of offensive operations to engage cybersecurity student, an important aspect in inculcating the necessary intrinsic motivation that will sustain continued learning in the field. As shown in section 2.3, interesting and enjoyable challenges are a key component to developing lifelong learners. Offensive challenges are inherently more enjoyable and interesting than defensive challenges, and they are also better for building resiliency.

Offensive techniques build a more resilient mindset since the inherent expectation is to fail often and repeatedly. These techniques also have an establishing problem-focused troubleshooting methodology which helps develop better coping methods [65]. This mindset is epitomized in the mantra for Offensive Security's Introductory Ethical Hacking Course, "Try Harder [52]." In addition to providing a technical foundation for offensive techniques, this course visibly and repeatedly reinforces the expectation of failure, and the need for increased effort in order to succeed in the course.[11] This cycle of repeatedly failing helps develops better problem-focused coping methods, and the eventual success provides both a chemically induced increase in motivation as well as positive self-reflection which helps tackle future, more difficult challenges [65].

Offensive cybersecurity training and competitions use a series of scaled challenges to teach concepts which increases student resilience and motivation [37]. Consider the previous example of iCTF. My undergraduate students competed in this competition in 2017. As an undergraduate team, my students were able to find vulnerabilities for two of the services over the competition. By the time they created these exploits, the top teams had already patched their services, but there were numerous teams in the bottom half of the competition that the team could still exploit to extract flags. Even though my students did not come close to winning, simply exploiting another team and submitting a flag was victory.

This small victory was a positively reinforcing and enjoyable experience for the team, and it increased the students' resilience towards facing future, bigger challenges. Previous research shows that having fun through enjoyable, interesting, and challenging resources best develops intrinsic motivation in students [27, 46]. As such, offensive techniques are the best for developing this intrinsic motivation that will continue to move cybersecurity students to learn long after their initial education program has ended.

[11] Offensive Security wants their students to internalize this motto so much they put it on stickers, made it a song, and prominently display it on the inside of their certificate folder.

5 Conclusion

This paper demonstrates why offensive techniques are the best for teaching any cybersecurity program, even when the primarily purpose is to train defensive specialists. Most significantly, this paper demonstrates that offensive and defensive techniques are equivalent in terms of teaching the core cybersecurity competencies. I then build on the previous research to show that only offensive techniques develop the security mindset in cybersecurity students; a mindset required to defend our computing and information systems. In addition, offensive techniques are notably more engaging and exciting, and, as such, they inculcate resiliency within cybersecurity students and increase their intrinsic motivation. These attributes are the foundation for producing lifelong learners - a characteristic cybersecurity professionals desperately need due to the rapid advancement of the technology to learn new tools, new techniques, and, most importantly, new identify new vulnerabilities.

The true end-state of any cybersecurity training program is to build better defenders since the vast majority (85%) of cybersecurity positions are defensive [10]. This paper discuss why offensive techniques are the best for teaching these defenders and, hopefully, will lead to improving how we educate defensive cybersecurity professionals in the future.

6 Acknowledgments

I want to thank William (Clay) Moody for his advice and inspiration on this topic, and Roy Ragsdale for his pessimistic feedback as to the value of this research which forced me to better develop the study. I also want to thank my amazing cybersecurity students (lab rats) because their experiences were truly the foundation for this research.

7 Availability

For more information on this work, please visit *https://www.mjkranch.com/publish/*.

References

[1] AMBROSE, S. A., BRIDGES, M. W., DIPIETRO, M., LOVETT, M. C., AND NORMAN, M. K. *How learning works: Seven research-based principles for smart teaching*. John Wiley & Sons, 2010.

[2] ASSOCIATION FOR COMPUTING MACHINERY'S COMMITTEE ON PROFESSIONAL ETHICS. ACM Code of Ethics and Professional Conduct, 2018.

[3] BANFIELD, J., AND WILKERSON, B. Increasing student intrinsic motivation and self-efficacy through gam-

ification pedagogy. *Contemporary Issues in Education Research 7*, 4 (2014), 291–298.

[4] BENTLEY, T. *Learning beyond the classroom: Education for a changing world*. Routledge, 2012.

[5] BHATT, S., MANADHATA, P. K., AND ZOMLOT, L. The operational role of security information and event management systems. *IEEE security & Privacy 12*, 5 (2014), 35–41.

[6] BISHOP, M. *Early computer security papers, part 1*. 1998.

[7] BORGES, D., LEVINSON, A., AND MARCOS, J. Adventures in Red Teaming: Collegiate Cyber Defense Competition, Apr. 2017.

[8] BROMBERG-MARTIN, E. S., MATSUMOTO, M., AND HIKOSAKA, O. Dopamine in Motivational Control: Rewarding, Aversive, and Alerting. *Neuron 68*, 5 (2010), 815 – 834.

[9] BRYAN, W. Shaping the Next Generation Cybersecurity Workforce Today, Oct. 2017.

[10] BUREAU OF LABOR STATISTICS, U.S. DEPARTMENT OF LABOR. Information Security Analysts: Occupational Outlook Handbook, May 2017.

[11] BURLEY, D. L., BISHOP, M., BUCK, S., EKSTROM, J. J., FUTCHER, L., GIBSON, D., HAWTHORNE, E., KAZA, S., LEVY, Y., MATTORD, H., AND OTHERS. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. *A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education Version 1.0 Report* (Dec. 2017).

[12] BURNS, T. J., RIOS, S. C., JORDAN, T. K., GU, Q., AND UNDERWOOD, T. Analysis and Exercises for Engaging Beginners in Online CTF Competitions for Security Education. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)* (Vancouver, BC, 2017), USENIX Association.

[13] CALVERT, S., AND KAMP, J. More U.S. Cities Brace for Inevitable Hackers. *Wall Street Journal* (Sept. 2018).

[14] CANDY, P. C. *Self-Direction for Lifelong Learning*. Jossey-Bass, 1991.

[15] CARLISLE, M., CHIARAMONTE, M., AND CASWELL, D. Using CTFs for an Undergraduate Cyber Education. In *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)* (Washington, D.C., 2015), USENIX Association.

[16] CHAPMAN, P., BURKET, J., AND BRUMLEY, D. PicoCTF: A Game-Based Computer Security Competition for High School Students. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)* (San Diego, CA, 2014), USENIX Association.

[17] CHEUNG, R. S., COHEN, J. P., LO, H. Z., AND ELIA, F. Challenge based learning in cybersecurity education. In *Proceedings of the International Conference on Security and Management (SAM)* (2011), The Steering Committee of The World Congress in Computer Science, Computer , p. 1.

[18] COLLINS, S. 13 Memorable Computer Hackers on TV Shows, From '24' to 'Mr. Robot', 2016.

[19] COMPTIA ASSOCIATION OF INFORMATION TECHNOLOGY PROFESSIONALS (AITP). AITP Code of Ethics and Standards of Conduct, 2018.

[20] CONKLIN, A. Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (Jan. 2006), vol. 9, pp. 220b–220b.

[21] CTFTIME.ORG. All about CTF (Capture The Flag), 2015.

[22] CURRAN, K. The Need for Life Long Learning in Cyber Security, July 2018.

[23] CYBERSEEK. Cybersecurity Career Pathway, 2019.

[24] DEF CON HACKING CONFERENCE. CTF History, 2019.

[25] DODGE, R., TOREGAS, C., AND HOFFMAN, L. J. Cybersecurity Workforce Development Directions. In *HAISA* (2012), pp. 1–12.

[26] DU, W. *Computer Security: A Hands-on Approach*. CreateSpace Independent Publishing Platform, Oct. 2017.

[27] DUNLAP, J. C. Preparing Students for Lifelong Learning: A Review of Instructional Methodologies. *Procedings of Selected Research and Development Presentations at the 1997 National Convention of the Asociation for Educational Comunications and Technology* (1997), 14.

[28] DWECK, C. S., WALTON, G. M., AND COHEN, G. L. Academic Tenacity: Mindsets and Skills that Promote Long-Term Learning. *Bill & Melinda Gates Foundation* (2014).

[29] ECONOMIST. Lifelong Education: Earning and Learning, 2017.

[30] ENGEBRETSON, P. *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier, 2013.

[31] FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (FFIEC). Cybersecurity Assessment Tool, 2017.

[32] FELTEN, E. The Security Mindset and "Harmless Failures", 2008.

[33] GOLDMAN, K., GROSS, P., HEEREN, C., HERMAN, G. L., KACZMARCZYK, L., LOUI, M. C., AND ZILLES, C. Setting the scope of concept inventories for introductory computing subjects. *ACM Transactions on Computing Education (TOCE) 10*, 2 (2010), 5.

[34] GONZALEZ, H., LLAMAS, R., AND ORDAZ, F. Cybersecurity Teaching through Gamification: Aligning Training Resources to our Syllabus. *Research in Computing Science 146* (2017), 35–43.

[35] GORKA, S., AND MILLER, J. Kinder Garten Security: Teaching the Pre-college Crowd, 2019.

[36] HAMARI, J., KOIVISTO, J., AND SARSA, H. Does gamification work? A literature review of empirical studies on gamification. In *2014 47th Hawaii international conference on system sciences (HICSS)* (2014), IEEE, pp. 3025–3034.

[37] HAMARI, J., SHERNOFF, D. J., ROWE, E., COLLER, B., ASBELL-CLARKE, J., AND EDWARDS, T. Challenging Games Help Students Learn. *Comput. Hum. Behav. 54*, C (Jan. 2016), 170–179.

[38] HANSEN, H., AND GAUTHIER, R. Factors affecting attendance at professional sport events. *Journal of sport management 3*, 1 (1989), 15–32.

[39] IEEE-CS/ACM JOINT TASK FORCE ON SOFTWARE ENGINEERING ETHICS AND PROFESSIONAL PRACTICES. Software Engineering Code of Ethics and Professional Practices, 1999.

[40] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE). IEEE Code of Ethics, 2019.

[41] (ISC)2. Report Finds Cybersecurity Workforce Gap Has Increased to More Than 2.9 Million Globally, 2019.

[42] JOINT TASK FORCE ON COMPUTING CURRICULA, A. F. C. M. A., AND SOCIETY, I. C. *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. ACM, New York, NY, USA, 2013.

[43] KOHNO, T. How to think like a security professional, 2007.

[44] KRISHNAN, B. Open Source Playbooks, Mar. 2018.

[45] LAMBERT, J. Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win., 2016.

[46] LONDON, M. *Lifelong Learning: Introduction*. The Oxford Handbook of Lifelong Learning. Oxford University Press, Mar. 2011.

[47] MCGETTRICK, A., CASSEL, L. N., DARK, M., HAWTHORNE, E. K., AND IMPAGLIAZZO, J. Toward Curricular Guidelines for Cybersecurity. In *Proceedings of the 45th ACM Technical Symposium on Computer Science Education* (New York, NY, USA, 2014), SIGCSE '14, ACM, pp. 81–82. event-place: Atlanta, Georgia, USA.

[48] NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION. CCDC Rules, 2019.

[49] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Demand, 2019.

[50] NEWHOUSE, W., KEITH, S., SCRIBNER, B., AND WITTE, G. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. *NIST Special Publication 800* (2017), 181.

[51] NIGHSWANDER, T. Why CTF (Plaid 2014), 2014.

[52] OFFENSIVE SECURITY. Penetration Testing Training with Kali Linux, 2019.

[53] PAREKH, G., DELATTE, D., HERMAN, G. L., OLIVA, L., PHATAK, D., SCHEPONIK, T., AND SHERMAN, A. T. Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. *IEEE Transactions on Education 61*, 1 (Feb. 2018), 11–20.

[54] PAULSEN, C., MCDUFFIE, E., NEWHOUSE, W., AND TOTH, P. NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy 10*, 3 (2012), 76–79.

[55] PETULLO, W. M., MOSES, K., KLIMKOWSKI, B., HAND, R., AND OLSON, K. The use of cyber-defense exercises in undergraduate computing education. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)* (2016).

[56] POTTER, B., AND MCGRAW, G. Software security testing. *IEEE Security & Privacy 2*, 5 (2004), 81–85.

[57] PUSEY, P., DAVID TOBEY, S., AND SOULE, R. An Argument for Game Balance: Improving Student Engagement by Matching Difficulty Level with Learner Readiness. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)* (San Diego, CA, 2014), USENIX Association.

[58] SANS INSTITUTE. Cyber Security Skills Roadmap, 2019.

[59] SCHEPENS, W. J., AND JAMES, J. R. Architecture of a cyber defense competition. In *SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme - System Security and Assurance (Cat. No.03CH37483)* (Oct. 2003), vol. 5, pp. 4300–4305 vol.5.

[60] SCHNEIDER, F. B. Cybersecurity education in universities. *IEEE Security & Privacy 11*, 4 (2013), 3–4.

[61] SCHNEIER, B. Inside the Twisted Mind of the Security Professional. *Wired* (Mar. 2008).

[62] SCHOLAR, G. Most Cited Gamification Publications, 2019.

[63] SCHREUDERS, Z. C., AND BUTTERFIELD, E. Gamification for Teaching and Learning Computer Security in Higher Education. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)* (Austin, TX, 2016), USENIX Association.

[64] SHALAL-ESA, A. U.S. Air Force cadets win cyber war game with NSA hackers. *Reuters* (Apr. 2013).

[65] SHARMAN, R. When you mess up, get up: the power of failure in building resilience, 2017.

[66] SHERMAN, A. T., OLIVA, L., DELATTE, D., GOLASZEWSKI, E., NEARY, M., PATSOURAKOS, K., PHATAK, D. S., SCHEPONIK, T., HERMAN, G. L., AND THOMPSON, J. Creating a Cybersecurity Concept Inventory: A Status Report on the CATS Project.

[67] STALLINGS, W., AND BROWN, L. *Computer Security: Principles and Practice, 4th Edition*. Pearson, 2018.

[68] STEIN, D., SCRIBNER, B., KYLE, N., NEWHOUSE, W., WILLIAMS, C., AND YAKIN, B. National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators. Tech. Rep. NISTIR 8193 (Draft), National Institute of Standards and Technology, Nov. 2017.

[69] STROM, B. E., BATTAGLIA, J. A., KEMMERER, M. S., KUPERSANIN, W., MILLER, D. P., WAMPLER, C., WHITLEY, S. M., AND WOLF, R. D. Finding Cyber Threats with ATT&CK-Based Analytics. Tech. Rep. Technical Report MTR170202., The MITRE Corporation, 2017.

[70] VIGNA, G., BORGOLTE, K., CORBETTA, J., DOUP, A., FRATANTONIO, Y., INVERNIZZI, L., KIRAT, D., AND SHOSHITAISHVILI, Y. Ten Years of iCTF: The Good, The Bad, and The Ugly. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)* (San Diego, CA, 2014), USENIX Association.

[71] WEEK, M. CCDC and CTFs Addressing the Criticisms, 2014.

[72] WHITE, G. B., WILLIAMS, D., AND HARRISON, K. The CyberPatriot national high school cyber defense competition. *IEEE Security & Privacy 8*, 5 (2010), 59–61.

[73] WHITTAKER, J. A., AND FORD, R. How to think about security. *IEEE Security Privacy 4*, 2 (Mar. 2006), 68–71.

[74] WILLIAMS, D. National Collegiate Cyber Defense Competition, 2019.

[75] ZADELHOFF, M. V., AND LURIE, L. It's not where you start-it's how you finish: Addressing the cybersecurity skills gap with a new collar approach. *IBM Institute for Business Value Executive Report - Security* (May 2017), 24.