A Novel Ethical Hacking Teaching Model: A Systematic Approach to Learn Cyber Attack Methods

Jason Cuneo, Daniel Tauritz
Auburn University, Auburn Cyber Research Center
Auburn, AL
jzc0105@auburn.edu, drt0015@auburn.edu

David Umphress
Auburn University, Auburn Cyber Research Center
Auburn, AL
david.umphress@auburn.edu

ABSTRACT

Due to extensive topical coverage across cybersecurity domains, the considerable in-depth knowledge required to effectively use and deploy cybersecurity technologies, and the speed of knowledge & skill obsolescence, it has become increasingly difficult to develop and maintain an ethical hacking curriculum that prepares students for the operational and technical challenges they will face upon entry into the cybersecurity workforce. Consequently, our objective in this paper is to introduce an adaptive teaching model that evaluates existing security frameworks, industry standards, and reconfigurable training environment to create an adaptive ethical hacking course curriculum. We demonstrate a teaching model for ethical hacking at the university level and highlight the positive educational outcomes that have resulted from our approach, followed by several suggestions for how to extend this line of inquiry.

ABOUT THE AUTHORS

Jason Cuneo is Chief Technologist of the Auburn Cyber Research Center and an Adjunct Professor in the Department of Computer Science and Software Engineering at Auburn University. Mr. Cuneo has successfully managed numerous cybersecurity-focused teams supporting defensive cyber operations, cyber training and exercises, vulnerability assessments, and development of cybersecurity policy. Mr. Cuneo has supported numerous government and industry organizations including the U.S. Army Aviation and Missile Research Development and Engineering Center, Missile and Space Intelligence Center, Software Engineering Directorate, Army Research Laboratory, Program Executive Office Missiles and Space, Redstone Test Center, and the U.S. Army Space and Missile Defense Command.

Daniel Tauritz is an Associate Professor in the Department of Computer Science and Software Engineering at Auburn University (AU), Interim Director and Chief Cyber AI Strategist of the Auburn Cyber Research Center, the founding director of AU's Biomimetic National Security Artificial Intelligence Laboratory (BONSAI Lab), a cyber consultant for Sandia National Laboratories, a Guest Scientist at Los Alamos National Laboratory (LANL), and founding academic director of the LANL/AU Cyber Security Sciences Institute (CSSI). He received his Ph.D. in 2002 from Leiden University. His research interests include the design and application of artificial intelligence techniques in cyber security and critical infrastructure protection. He was granted a US patent for an artificially intelligent rule-based system to assist teams in becoming more effective by improving the communication process between team members.

David Umphress is COLSA Professor of Cyber Security in Auburn University's Department of Computer Science and Software Engineering He has worked over the past 40 years in various software and systems engineering capacities in military, industry, and academia. His areas of expertise include general software engineering, systems engineering, secure software development, software vulnerability analysis, and software reverse engineering. Dr. Umphress is a retired Air Force officer. He holds the Institute of Electrical and Electronics Engineers (IEEE) Software Engineering Master Certification.

A Novel Ethical Hacking Teaching Model: A Systematic Approach to Learn Cyber Attack Methods

Jason Cuneo, Daniel Tauritz
Auburn University, Auburn Cyber Research Center
Auburn, AL
jzc0105@auburn.edu, drt0015@auburn.edu

David Umphress
Auburn University, Auburn Cyber Research Center
Auburn, AL
david.umphress@auburn.edu

INTRODUCTION

Adversary attack methods and techniques continue to expand in complexity and technical sophistication while the number of successful attacks challenges the security community's ability to adequately respond (Alert AA20-352A, 2020). These challenges are intensified by the expanding cybersecurity workforce gap and lack of technically skilled cybersecurity professionals to meet the demand (Oltsik, 2020) (Cybersecurity Supply and Demand Heat Map, 2021). One cybersecurity specialty that is particularly hard hit by this gap are cybersecurity professionals with technical knowledge and skill in ethical hacking methods. The objective of this paper is to demonstrate our implementation of a teaching model successful applied to an ethical hacking course at the university level and discuss the benefits of our methodology. Based on experience with evaluating and developing course content at the academic and professional levels, we have observed an ad hoc approach when developing ethical hacking content and our results indicate that a more methodical approach is achievable.

Ethical hacking is a legal method of testing personnel, systems, networks, and infrastructure by employing adversary attack methods for the purpose of identifying technical, administrative, and physical vulnerabilities across an organization (Palmer, 2001). Cybersecurity professionals with knowledge of attacker techniques and tools can utilize those same methods, in a legal way, to identify vulnerabilities and recommend mitigation strategies to improve the security posture of an organization. Although ethical hacking is a highly technical skill set, we recognized that our teaching model cannot focus solely on technical factors but must also account for strategic and operational considerations. The bullets below describe the purpose of each tier and the associated framework that we will use in support of our teaching model.

- *Strategic Tier*: This tier includes frameworks that assist with defining course learning objectives, but do not provide lower-level guidance for technical implementation. Several national programs have assisted cybersecurity educators in the development of high-level learning objectives for cybersecurity courses and we will discuss our utilization of the National Initiative for Cybersecurity Education (NICE) at the strategic tier.

- *Operational Tier*: This tier includes frameworks that delve specifically into ethical hacking and penetration testing methods. Before applying any technical solution to a course, it is necessary to select a framework at the operational tier that provides guidance on how to identify and replicate attacker methods. We will introduce four operational frameworks that could be used in our teaching model and provide recommendations on why the MITRE ATT&CK framework was the most suitable for our needs.

- *Technical Tier*: This tier includes technical platforms that users interact with to solidify learning objectives identified at the strategic and operational tiers. At this tier we will introduce four technical methods that could have been used for the implementation of our course and provide rationale for why we selected the *HackTheBox* (HTB) platform and why it provided the greatest level of flexibility versus the other potential solutions.

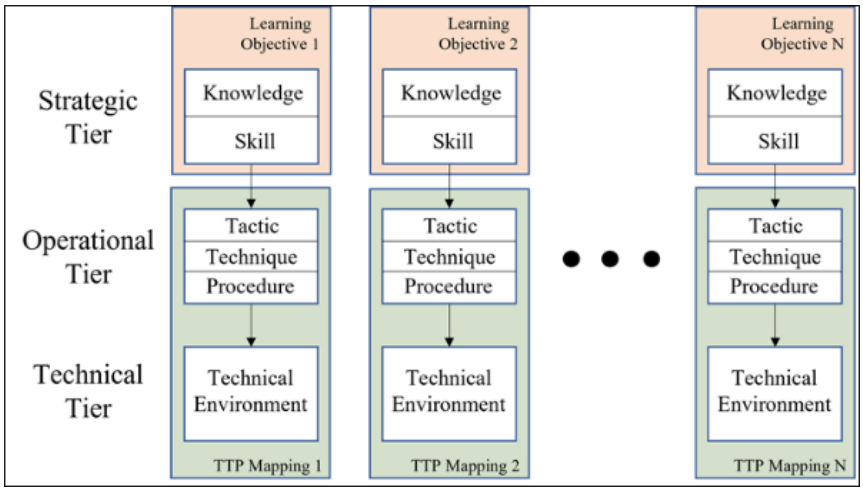

Figure 1. Relationship of Strategic, Operational, and Technical Tiers.

STRATEGIC TIER

We start our survey at the strategic tier by introducing NICE which "provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams" and was developed to "connect Government employees, students, educators, and industry with cybersecurity training providers throughout the Nation" (Workforce Framework for Cybersecurity, 2021). Maintained by the National Institute for Standards and Technology (NIST), NICE provides strategic level guidance to cybersecurity educators and professionals by identifying cybersecurity specialty areas and work roles that currently exist across the workforce. In the development of our teaching model, we identify knowledge and skills required for those taking positions in support of ethical hacking tasks.

There are currently 628 knowledge items and 374 skills specified in NICE, but not all entries apply to ethical hacking capabilities. As a result, we first developed a comprehensive list of all knowledge and skills required to identify the high-level learning objectives for our course. Table 1 illustrates the first of many knowledge and skill combinations that form the basis of our course learning objectives.

Table 1. Knowledge and Skill Pairing from NICE.

Knowledge	Knowledge of ethical hacking principles and techniques.
Skill	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.

Although selection of all relevant knowledge and skills provides an extensive list of learning objectives for our course, it does not provide the level of granularity necessary for course implementation. In our case, the next step in the process was the selection of an operational framework that is specifically suited for the technical rigors of an ethical hacking course.

OPERATIONAL TIER

Once knowledge and skills were consolidated and course learning objectives were specified, the next step in the process focused on identifying operational frameworks that evaluate adversary attack methods. Based on lessons learned in both cybersecurity research and professional spheres, we identified four operational frameworks / checklists specifically used for understanding adversary attack methods. In our case, we considered the following:

Adversary Attack Frameworks

- *Lockheed Martin Cyber Kill Chain (CKC)*: The Department of Defense (DoD) added cyberspace as a warfare domain in 2011 and in response to this, Lockheed Martin defined the term "Cyber Kill Chain" in a seminal paper that provides an "intelligence-driven, threat-focused approach to study intrusions from an adversaries' perspective" (Hutchins and Cloppert and Amin, 2011). The objective of the cyber kill chain is to assist

defenders to identify, degrade, or stop cyber attacks and consists of seven steps that attackers use when conducting attacks, namely: 1) Reconnaissance, 2) Weaponization, 3) Delivery, 4) Exploitation, 5) Installation, 6) Command and Control, and 7) Actions on the Objective. (Hutchins and Cloppert and Amin, 2011).

- *Penetration Test Execution Standard (PTES)*: The PTES is a legacy standard that identifies seven areas related to a penetration test: 1) Pre-engagement Interactions, 2) Intelligence Gathering, 3) Threat Modeling, 4) Vulnerability Analysis, 5) Exploitation, 6) Post Exploitation, and 7) Reporting. Each of these areas provides knowledge of operational considerations when considering attack methods, but one of the specified drawbacks of the standard is that it "does not provide technical guidelines on executing a penetration test" (Pentest Execution Standard, 2014).

- *MITRE Common Attack Pattern Enumeration and Classification (CAPEC)*: CAPEC provides a dictionary of known adversary attack patterns when exploiting known weaknesses in cyber-enabled systems. The patterns are categorized either by attack mechanisms or by cybersecurity domain, making it easy to group adversary methods (MITRE CAPEC, 2021). Unlike the previous introduced operational frameworks, CAPEC provides the added benefit of specifying technical methods used to conduct an attack.

- *MITRE ATT&CK Framework (ATT&CK)*: The MITRE ATT&CK framework is defined as a community provided "knowledge base of adversary tactics and techniques based on real-world observations." and specifies attack methods against enterprise and mobile systems (MITRE ATT&CK, 2021). By taking structures developed by both the CKC and CAPEC and expanding on them, ATT&CK provides a more robust method of understanding attacker tactics, techniques, and procedures (TTPs) at the operational level.

Ultimately, our analysis led to selection of the ATT&CK framework as the operational layer for numerous reasons. First, ATT&CK expands on the CKC phases by providing a more granular list of tactics, making it more comprehensive for our needs. Second, ATT&CK TTP's also account for attack patterns defined in the CAPEC framework which highlights the methods and tools attackers use during attack planning and execution. Lastly, as we will discuss in our results, we found that introduction of each TTP followed by immediate technical walkthroughs in the training environment rated as the most critical factor to solidification of learning objectives.

TACTICAL TIER – TRAINING ENVIRONMENT SELECTION

Once NICE knowledge and skills and ATT&CK TTP's were selected as the strategic and operational tiers, the final component of our model was the selection of a technical environment with which users interact during the course. Although numerous training environments including on-premises training networks, Capture-the-Flag (CTF) platforms, research focused cyber ranges, and government training cyber ranges exist, we determined that the first two would provide the most openly available access from an education and training perspective.

One of the first training environments evaluated during the development of our model was a locally hosted closed network that provided users with access to numerous networking devices, operating systems, and applications. Users were given physical network access and provided with segmented enclaves so that they could conduct attacks and deploy tools of their choosing without negatively impacting other users on the platform. By deploying both virtual and physical systems on the network, users can apply ethical hacking methods to determine the security posture of a given enclave. One of the lessons learned from deploying a physical environment of this type was the extensive configuration control required to maintain system architecture, operating system configurations, and application versioning.

Outside of on-premises networks, we also evaluated the effectiveness of CTF platforms due to extensive development of recent open-source and commercial solutions which has aided in the technical development of cybersecurity students and professionals. We found CTF platforms fell into four general categories: 1) Canned, 2) Jeopardy-style, 3) Vulnerable System, and 4) Attack-Defense. Although selection of a given CTF platform depends on the project objectives, often it is driven by the experience level of the user. For example, canned CTF platforms are used to provide new users a high level of scripted content and to establish confidence in basic skills and capabilities. A step up from a canned CTF platform is a Jeopardy-style CTF which uses a question-and-answer format where users have an opportunity to respond to questions about a specific cybersecurity domain.

Although both solutions provide an effective way to meet introductory learning objectives, they fell short of the dynamic environment that effectively models real-world infrastructure and network interaction. A third CTF platform to consider is one that is intentionally misconfigured and vulnerable for the express purpose of testing ethical hacking methods. In such "boot-to-root" (BTR) configurations, the user must determine what techniques are required to gain user or root level access once the system communicates over the network. Before the expansion of online services, many BTR systems were provided as openly available virtual machines where users could download, configure, start, and apply ethical hacking methods. Several commercial platforms have since emerged in the place of traditional downloadable BTR virtual machines, namely *TryHackMe* (THM) and HTB. During our transition from a locally hosted closed restricted network, we experimented with several online platforms due to academic license availability and found that the HTB platform would provide the best mechanism to map systems to TTP's and provide the best opportunity to solidify learning objectives within the course.

The last, and most advanced, environment that we considered was an Attack-Defense CTF platform where a specified number of systems are divided between teams and team members are responsible for the defense of one or more systems. A platform of this nature requires previously developed skills in both offensive and defensive cyber operations and extensive coordination among team members. Many professional cybersecurity teams use this type of platform to coordinate activities and adjust defensive capabilities. After evaluation, we determined that a platform of this type would be useful for intermediate and advanced users, but felt it was not suited for an introductory ethical hacking course.

SYSTEM-TO-TTP MAPPING

Utilization of strategic, operational, and technical tiers in the development of this course, by itself, is not a unique approach; however, the novelty of our teaching method comes from the mapping of systems within the training environment to specific ATT&CK TTP's with an example of this shown in Figure 2. In this example, users of the training environment solidify learning objectives by conducting the same type of SQL Injection (SQLi) successfully executed by attackers in the wild. This type of mapping only works if users have access to systems that contain misconfigurations or vulnerabilities that align with ATT&CK TTP's.

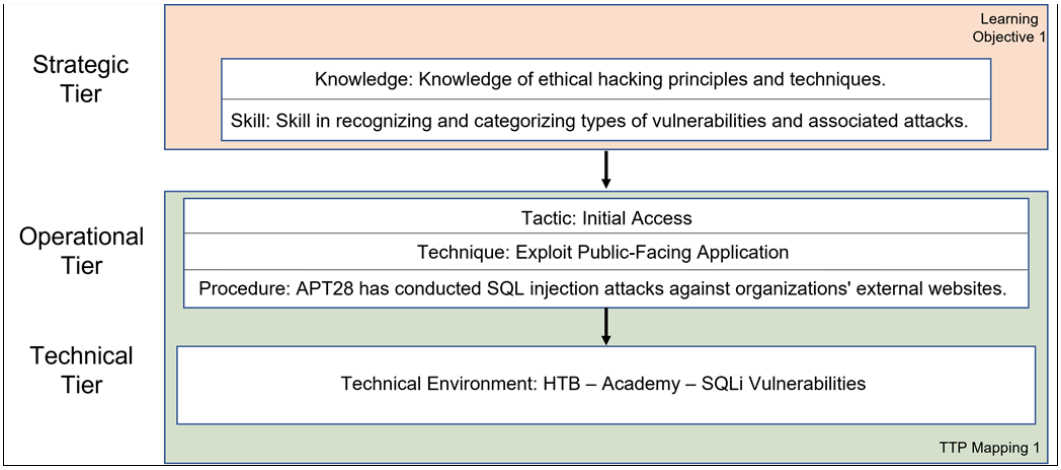

Figure 2. TTP to Technical Environment Mapping

Figure 3 expands on a single ATT&CK TTP mapping by highlighting not just one, but all TTP's relating to the system codenamed "Academy" introduced in Figure 2. Notice that under each tactic shown (i.e., Reconnaissance, Resource Development, Initial Access) all underlying techniques and procedures are highlighted since they apply to the system. One thing to note in Figure 3 is that although only 3 out of 14 ATT&CK tactics are shown our application maps all relevant ATT&CK categories.

Machine Name	IP Address	Operating System	Reconnaissance		Resource Development		Initial Access	
Academy	10.10.10.215	Linux	T1595	Active Scanning	T1583	Acquire Infrastructure	T1189	Drive-by Compromise
Access	10.10.10.98	Windows	.001	Scanning IP Blocks	.001	Domains	T1190	Exploit Public-Facing Application
Active	10.10.10.100	Windows	.002	Vulnerability Scanning	.002	DNS Server	T1133	External Remote Services
Admirer	10.10.10.187	Linux	T1592	Gather Victim Host Information	.003	Virtual Private Server	T1200	Hardware Additions
AI	10.10.10.163	Linux	.001	Hardware	.004	Server	T1566	Phishing
Apocalyst	10.10.10.46	Linux	.002	Software	.005	Botnet	.001	Spearphishing Attachment
APT	10.10.10.213	Windows	.003	Firmware	.006	Web Services	.002	Spearphishing Link
Aragog	10.10.10.78	Linux	.004	Client Configurations	T1586	Compromise Accounts	.003	Spearphishing via Service
Arctic	10.10.10.11	Windows	T1589	Gather Victim Identity Information	.001	Social Media Accounts	T1091	Replication Through Removable Media
Ariekei	10.10.10.65	Linux	.001	Credentials	.002	Email Accounts	T1195	Supply Chain Compromise
Arkham	10.10.10.130	Windows	.002	Email Addresses	T1584	Compromise Infrastructure	.001	Compromise Software Dependencies and Development Tools
Attended	10.10.10.221	OpenBSD	.003	Employee Names	.001	Domains	.002	Compromise Software Supply Chain
Bank	10.10.10.29	Linux	T1590	Gather Victim Network Information	.002	DNS Server	.003	Compromise Hardware Supply Chain
Bankrobber	10.10.10.154	Windows	.001	Domain Properties	.003	Virtual Private Server	T1199	Trusted Relationship
Bart	10.10.10.81	Windows	.002	DNS	.004	Server	T1078	Valid Accounts
Bashed	10.10.10.68	Linux	.003	Network Trust Dependencies	.005	Botnet	.001	Default Accounts
Bastard	10.10.10.9	Windows	.004	Network Topology	.006	Web Services	.002	Domain Accounts
Bastion	10.10.10.134	Windows	.005	IP Addresses	T1587	Develop Capabilities	.003	Local Accounts
BigHead	10.10.10.112	Windows	.006	Network Security Appliances	.001	Malware	.004	Cloud Accounts
Bitlab	10.10.10.114	Linux	T1591	Gather Victim Org Information	.002	Code Signing Certificates		
Blackfield	10.10.10.192	Windows	.001	Determine Physical Locations	.003	Digital Certificates		
Blocky	10.10.10.37	Linux	.002	Business Relationships	.004	Exploits		
Blue	10.10.10.40	Windows	.003	Identify Business Tempo	T1585	Establish Accounts		
Blunder	10.10.10.191	Linux	.004	Identify Roles	.001	Social Media Accounts		
Book	10.10.10.176	Linux	T1598	Phishing for Information	.002	Email Accounts		
Bounty	10.10.10.93	Windows	.001	Spearphishing Service	T1588	Obtain Capabilities		
Brainfuck	10.10.10.17	Linux	.002	Spearphishing Attachment	.001	Malware		
Breadcrumbs	10.10.10.228	Windows	.003	Spearphishing Link	.002	Tool		
Bucket	10.10.10.212	Linux	T1597	Search Closed Sources	.003	Code Signing Certificates		
Buff	10.10.10.198	Windows	.001	Threat Intel Vendors	.004	Digital Certificates		
Cache	10.10.10.188	Linux	.002	Purchase Technical Data	.005	Exploits		
Calamity	10.10.10.27	Linux	T1596	Search Open Technical Databases	.006	Vulnerabilities		

Figure 3. Mapping ATT&CK Techniques to HTB Systems - Linux System.

To get an appreciation for the benefit of our mapping method, we provide an example of a different system hosted on the HTB platform in Figure 4. Notice that in this case we have both a different operating system and applicable set of TTP's which indicates that each system has a unique mapping fingerprint. The current version of our mapping database only maps from system to applicable TTP; future versions will provide a reverse mapping where selection of specific TTP's will highlight all systems that contain that characteristic.

Machine Name	IP Address	Operating System	Reconnaissance		Resource Development		Initial Access	
Academy	10.10.10.215	Linux	T1595	Active Scanning	T1583	Acquire Infrastructure	T1189	Drive-by Compromise
Access	10.10.10.98	Windows	.001	Scanning IP Blocks	.001	Domains	T1190	Exploit Public-Facing Application
Active	10.10.10.100	Windows	.002	Vulnerability Scanning	.002	DNS Server	T1133	External Remote Services
Admirer	10.10.10.187	Linux	T1592	Gather Victim Host Information	.003	Virtual Private Server	T1200	Hardware Additions
AI	10.10.10.163	Linux	.001	Hardware	.004	Server	T1566	Phishing
Apocalyst	10.10.10.46	Linux	.002	Software	.005	Botnet	.001	Spearphishing Attachment
APT	10.10.10.213	Windows	.003	Firmware	.006	Web Services	.002	Spearphishing Link
Aragog	10.10.10.78	Linux	.004	Client Configurations	T1586	Compromise Accounts	.003	Spearphishing via Service
Arctic	10.10.10.11	Windows	T1589	Gather Victim Identity Information	.001	Social Media Accounts	T1091	Replication Through Removable Media
Ariekei	10.10.10.65	Linux	.001	Credentials	.002	Email Accounts	T1195	Supply Chain Compromise
Arkham	10.10.10.130	Windows	.002	Email Addresses	T1584	Compromise Infrastructure	.001	Compromise Software Dependencies and Development Tools
Attended	10.10.10.221	OpenBSD	.003	Employee Names	.001	Domains	.002	Compromise Software Supply Chain
Bank	10.10.10.29	Linux	T1590	Gather Victim Network Information	.002	DNS Server	.003	Compromise Hardware Supply Chain
Bankrobber	10.10.10.154	Windows	.001	Domain Properties	.003	Virtual Private Server	T1199	Trusted Relationship
Bart	10.10.10.81	Windows	.002	DNS	.004	Server	T1078	Valid Accounts
Bashed	10.10.10.68	Linux	.003	Network Trust Dependencies	.005	Botnet	.001	Default Accounts
Bastard	10.10.10.9	Windows	.004	Network Topology	.006	Web Services	.002	Domain Accounts
Bastion	10.10.10.134	Windows	.005	IP Addresses	T1587	Develop Capabilities	.003	Local Accounts
BigHead	10.10.10.112	Windows	.006	Network Security Appliances	.001	Malware	.004	Cloud Accounts
Bitlab	10.10.10.114	Linux	T1591	Gather Victim Org Information	.002	Code Signing Certificates		
Blackfield	10.10.10.192	Windows	.001	Determine Physical Locations	.003	Digital Certificates		
Blocky	10.10.10.37	Linux	.002	Business Relationships	.004	Exploits		
Blue	10.10.10.40	Windows	.003	Identify Business Tempo	T1585	Establish Accounts		
Blunder	10.10.10.191	Linux	.004	Identify Roles	.001	Social Media Accounts		
Book	10.10.10.176	Linux	T1598	Phishing for Information	.002	Email Accounts		
Bounty	10.10.10.93	Windows	.001	Spearphishing Service	T1588	Obtain Capabilities		
Brainfuck	10.10.10.17	Linux	.002	Spearphishing Attachment	.001	Malware		
Breadcrumbs	10.10.10.228	Windows	.003	Spearphishing Link	.002	Tool		
Bucket	10.10.10.212	Linux	T1597	Search Closed Sources	.003	Code Signing Certificates		
Buff	10.10.10.198	Windows	.001	Threat Intel Vendors	.004	Digital Certificates		
Cache	10.10.10.188	Linux	.002	Purchase Technical Data	.005	Exploits		
Calamity	10.10.10.27	Linux	T1596	Search Open Technical Databases	.006	Vulnerabilities		
Canape	10.10.10.70	Linux	.001	DNS/Passive DNS				
Caring	10.10.11.25	Windows	.002	WHOIS				
Carrier	10.10.10.105	Linux	.003	Digital Certificates				
Cascade	10.10.10.182	Windows	.004	CDNs				
Celestial	10.10.10.85	Linux	.005	Scan Databases				
Cereal	10.10.10.217	Windows	T1593	Search Open Websites/Domains				
Chainsaw	10.10.10.142	Linux	.001	Social Media				
Chaos	10.10.10.120	Linux	.002	Search Engines				
Charon	10.10.10.31	Linux	T1594	Search Victim-Owned Websites				

Figure 4. Mapping ATT&CK Techniques to HTB Systems - Windows System.

The mapping shown in Figure 3 and Figure 4 provide several benefits to both the academic and professional community. First, organizations that need to train their personnel on specific technical capabilities can consult the mapping to select systems that will be most applicable to their training objectives. Another benefit of this mapping is the ability to create repeatable training events outside of a particular course. Although our focus has been on development of a dynamic course in ethical hacking, other technical fields within cybersecurity could also use this

teaching model. Lastly, this mapping can also assist with parallel training of blue and red teams and wargame scenario development so that specific ethical hacking methods are introduced and solidified.

Although a significant amount of time is required to identify system characteristics, associated ATT&CK TTP's, and update the underlying Visual Basic Application (VBA), we believe the results seen in learning objective comprehension justifies the effort.

RESULTS AND CONCLUSIONS

At the conclusion of our most recent course, we collected user feedback to determine if the teaching model was effective at solidifying learning objectives. Table 2 provides part one of the evaluation which focused on three learning objectives from NICE framework knowledge-skill pairing.

Table 2. Proficiency Feedback

Question	Before	After
What was your level of proficiency with ethical hacking methods before and after the course?	2.9 / 10	6.7 / 10
What was your level of proficiency with reconnaissance and enumeration of networked systems before and after the course?	2.9 / 10	7.7 / 10
What was your level of proficiency with conducting vulnerability research before and after the course?	2.6 / 10	7.5 / 10

The results in Table 2 indicate a significant student perception of improvement in student knowledge and skills relative to ethical hacking methods in these three learning objectives. Although numerous knowledge and skills pairs were included in the actual course, we focused on a subset of learning objectives for survey brevity.

In addition to analysis of student technical proficiency, we also evaluated student perception of effectiveness relative to our teaching model. Table 3 highlights part two of the evaluation and focuses on operational and technical tier effectiveness.

Table 3. Effectiveness Feedback

Question	Rating
Rate the level of effectiveness of the MITRE ATT&CK framework	7.5 / 10
Rate the level of effectiveness of the HackTheBox environment	7.8 / 10
Rate the level of satisfaction with the MITRE ATT&CK framework tactics, techniques, and procedures followed by technical demonstrations	8.6 / 10

The results in Table 3 indicate that students believed that the use of the MITRE ATT&CK framework and the HTB environment provided a relatively high level of effectiveness in their learning. Interestingly, the level of satisfaction with introduction of ATT&CK TTP's followed immediately by technique demonstration received the highest rating of the course and is an area that we will continue to cultivate in future courses.

One area that we would like to address in this section is threats to validity of the course survey. Although proficiency questions provided in Table 2 evaluate students perception of their before and after proficiency and provide a level of objectivity, the questions relative to effectiveness and satisfaction in Table 3 may be less objective since it provides only a single data point. A recommended solution to this potential validity issue is to conduct a pre-course and end-of-course exam to collect more objective results in follow-on courses.

SUMMARY

In this paper we discussed the lack of an effective ethical hacking course model at the university level that harmonizes strategic and operational frameworks with a technical environment to solidify understanding of ethical hacking methods. We surveyed existing strategic and operational frameworks and determined that the NICE and MITRE ATT&CK frameworks provide a starting point for course content but noted that no mapping currently exists between

high level frameworks and technical environments. A mapping of this kind is critical because it provides educators with a tangible way to determine if learning objectives have been met. By leveraging our experience with technical course development at the academic and professional level, we surveyed potential technical solutions that could be used within our course model and mapped the high-level frameworks to these technical environments. Although technical solutions can be of the canned, local server, or remote server varieties, we have found that remote server environments with a wide variety of existing vulnerabilities and misconfigurations is best suited to solidify ethical hacking concepts. Lastly, we provided an example of how our model can be applied in the context of our course. By applying pertinent knowledge and skills specified in the NICE framework, TTP's specified in the MITRE ATT&CK framework, and mapping each learning objective to specific systems within the HackTheBox environment we were able to develop a dynamic teaching model that keeps pace with changing attacker methods and provides an effective teaching method for future ethical hacking courses at the university level. The results indicate strong student perception of improvement in knowledge and skills, but due to both small sample size and the inherent bias of self-assessment, these results need to be validated using large-sample pre- and post-testing assessments to determine true improvement in knowledge and skills.

FUTURE WORK

During the development of this teaching model, we have identified three areas of future research and analysis:

- *Reverse mapping of TTP's to systems*: Our mapping is currently configured to go only from HTB system to ATT&CK TTP; however, we recognized that it may be helpful to reverse the process. Instead of highlighting a system and identifying which TTP's apply, what if we wanted to select a TTP and determine all systems that contained that attribute.

- *Expansion of NICE knowledge - skill pairs*: There are currently 628 knowledge items and 374 skills specified in the NICE framework. Although not all of these will be applicable to ethical hacking, one future effort will be to consolidate all ethical hacking related knowledge and skill pairs and automate a mapping between those and ATT&CK TTP's.

- *Expanding the number of mapped HTB systems*: Out of the over 200 available systems in the HTB platform, we have mapped systems into our application. A future effort would focus on collecting attack methods for each of the remaining systems.

REFERENCES

Alert AA20-352A. (2020). Retrieved June 28, 2021, from https://us-cert.cisa.gov/ncas/alerts/aa20-352a

Cybersecurity Supply and Demand Heat Map. (2021). Retrieved June 28, 2021, from https://www.cyberseek.org/heatmap.html

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-Driven Computer Network Defense. Retrieved June 28, 2021, from https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Pentest Execution Standard. (2014). Retrieved June 28, 2021, from http://www.pentest-standard.org/index.php/Main_Page

MITRE CAPEC. (2021). Common attack pattern enumeration and classification. Retrieved June 28, 2021, from https://capec.mitre.org

MITRE ATT&CK. (2021). MITRE ATT&CK. Retrieved June 28, 2021, from https://attack.mitre.org

NIST SP 800-181. (2021). NIST Special Publication 800-181 Revision 1. Retrieved June 28, 2021, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Oltsik, J. (2020, August 21). The cybersecurity skills shortage is getting worse. Retrieved June 28, 2021, from https://www.csoonline.com/article/3571734/the-cybersecurity-skills-shortage-is-getting-worse.html

Palmer, C. (2001). Ethical Hacking. *IBM Systems Journal*, *40*, 769-780. doi:10.1147/sj.404.01011

Workforce Framework for Cybersecurity (NICE Framework). (2021). Retrieved June 28, 2021, from https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework