

Empowering Ethical Hacking Education with Generative AIs: A ChatGPT-Infused Curriculum

Yang Wang, Kevin Beideman, Margaret McCoe
Department of Math and Computer Science
La Salle University
Philadelphia, USA

Maryam Jalalitar
Department of Computer Science
California State University, Northridge
Northridge, USA

Abstract—The last several years have witnessed a blossom of generative AI technologies with wide applications from business to healthcare. As revealed recently, generative AI tools can be incorporated in cybersecurity practices as both offensive and defensive vectors. This paper represents an initiative to empower Ethical Hacking (EH) education with ChatGPT-infused curriculum. As the first attempt of this nature, the proposed curriculum design has a few major innovative features. First, our design identifies and incorporates four ChatGPT-inspired EH areas including ChatGPT-powered Attack, ChatGPT-powered Defense, ChatGPT-powered Security Tasking, and ChatGPT-rooted Security. Second, our design is aligned with major EH certifications to prepare students to be industry ready. Third, we tackle both physical constraints (e.g., budget and space) and technical constraints (e.g., teaching offensive skills in compliance with campus policies), resulting in a cost-effective and IT-compliant design. Fourth, our design identifies and presents a course flow that integrates the diverse topics and ad hoc techniques for EH. Additionally, we discuss students’ performance and feedback on the design, and share learned lessons, with the hope of enlightening similar endeavors of other institutions.

Keywords—Ethical Hacking; ChatGPT; Course Design; Generative AI; Cybersecurity Education; AI-assisted Learning;

I. INTRODUCTION

With the growing market needs for cybersecurity professionals [1], our department is planning on an undergraduate Cybersecurity major. One key knowledge base in this new program is Ethical Hacking (EH), which has arisen as an independent career path in cybersecurity [2]. Meanwhile, the blossom of generative AI technologies in recent years has brought significant impacts to cybersecurity practices. The 2023 CS curriculum guidelines from ACM, IEEE, and AAAI [3] advocate for the inclusion of practical AI tools, such as generative models like ChatGPT, into course curricula. This paper represents an initiative to empower Ethical Hacking (EH) education with ChatGPT-infused curriculum to fulfill the above needs.

There are rich literature sources on the topic of Cybersecurity Education. The related course innovations range from designs for a general security course (e.g., [4]), for a singular security issue (e.g., EH for Web security [5]), for a specific platform (e.g., mobile device security in [6]), to designs for one particular system (e.g., NoSQL database security in [7]). One common theme treated in these designs is the choice and setup of the experiment testbed, which often includes

security practices that are offensive in nature and thus trigger legal or compliance issues [8]–[10]. Among the employed technologies, security lab sandbox can be broadly categorized into three major groups: virtualization-based lab design (e.g., [11]–[15]), Web-based lab design (e.g., [16]–[18]), and USB-drive-based lab design (e.g., [19]). Each of these choices can fulfill the need of providing students administrative privileges to perform security practices.

As a popular generative AI platform, ChatGPT has been recently identified as a key contributor to security practices as both offensive and defensive vectors. Given the ability of generating tailored response on demand, for instance, ChatGPT can be applied to craft and customize phishing emails [20], [21] in Social Engineering. ChatGPT can also be used to craft queries in SQL injection attack [22]. In contrast, ChatGPT can be used in defense such as guiding penetration testing [23] and simulating honey-bots [24]. Furthermore, generative AI platform like ChatGPT can also be the target of security exploits. For instance, prompt jail-breaking aims at bypassing the safety protocols of AI systems to obtain harmful, illegal or unethical information [25]. Despite the research on generative AI security implications above, there are considerable efforts in bring generative AI technologies into education [26]–[28], which spans different geographical regions [29], [30] and different subjects (e.g., digital art education [31]). However, only limited studies (e.g., [32], [33]) are dedicated to the incorporation of generative AIs for cybersecurity education or particularly ethical hacking education. As a field that is mostly impacted by emerging technologies, our EH course design aims at revamping both current ethical hacking techniques and new practices empowered or inspired by the state-of-arts generative AI technologies.

In this paper, we present an innovative design of an ChatGPT-infused Ethical Hacking course curriculum for the first time. Different from the literature, our design has a few major features. First, our design identifies and incorporates four ChatGPT-inspired EH areas including ChatGPT-powered Offense, ChatGPT-powered Defense, ChatGPT-powered Security Tasking, and ChatGPT-rooted Security. Second, to prepare students as industry-ready, our design is aligned with major EH certifications such as EC-Council Certified Ethical Hacker (CEH) and EC-Council Certified Penetration Testing (C|PENT) [34]. Third, we tackle both physical constraints

(e.g., budget and space) and technical constraints (e.g., teaching offensive skills in compliance with campus policies), resulting in a cost-effective and IT-compliant design. Fourth, our design identifies and presents a course flow that integrates the diverse topics and ad hoc techniques for EH. Additionally, we discuss students' performance and feedback on the design, and share our learned lessons.

The rest of this paper is organized as follows. Section II presents the background and learning objectives of this EH course. In Section III, we elaborate the role of ChatGPT in EH practices. In Section IV, we present the detailed course curriculum. In Section V, we discuss student performance and feedback on the design, and share learned lessons. Finally, we conclude this paper in Section VI.

II. BACKGROUND AND COURSE OBJECTIVES

Our Math and Computer Science Department offers both Computer Science (CS) and Information Technology (IT) programs. Since Summer 2024, the department is examining our curriculum to align with the 2023 CS curriculum [3] by ACM, IEEE, and AAI. A new proposed program in Cybersecurity is currently under review. This new EH course design extends a penetration testing (PT) course developed in 2020 [35]. This EH course will serve as a core course at sophomore/senior level for the Cybersecurity major or as elective course for CS/IT majors who have already taken pre-requisites in networking, database, and security. Based on the student background, the learning outcomes with the corresponding Bloom's level taxonomy are shown in Table I.

III. CHATGPT, SECURITY, AND ETHICAL HACKING

Recent research revealed that ChatGPT can serve as contributing vectors for both offensive and defensive operations in Cybersecurity. In this work, we classify ChatGPT-relevant security issues into four major categories as shown in Table II. Specifically, ChatGPT-powered Attack refers to offensive operations enabled by ChatGPT (e.g., crafting phishing emails for Social Engineering). ChatGPT-powered Defense covers hardening practices enabled by ChatGPT (e.g., vulnerability assessment of symmetric encryption algorithm). Given the nature of the generative AIs, ChatGPT can assist security tasking such as generation a PT plan on demand (i.e., the third category). Finally, with the rampant development of exploits on generative AI platforms (e.g., prompt jail-breaking [25]), it is critical to examine security issues rooted in the ChatGPT platform.

Even though above security issues were sporadically addressed in the literature, it remains an open question about how ChatGPT can be organically integrated in Ethical Hacking (EH) or Penetration Testing (PT)¹ across its workflow. Note that EH is typically divided into phases including reconnaissance, scanning, gaining access, maintaining access, and covering tracks. In our design, we aim to seamlessly embed

the innovative use of ChatGPT from all four categories into the discussion of different phases of EH.

IV. ETHICAL HACKING COURSE CURRICULUM DESIGN

Other than the five phases of EH workflow, we incorporate a sets of needed knowledge for EH professionals including: legal/ethical awareness, PT documentation, PT reporting, and system hardening techniques. In the following, we present the course flow based on intertwined coverage of the five phases of EH and the knowledge set.

A. Introduction

The beginning module serves three major purposes. First, it presents the workflow of EH, certifications in EH/PT, and course structure. Second, it re-visits major security concepts (e.g., access control, rainbow table, hashing) and introduces major tools for later use (e.g., Ettercap, and NMAP). Third, it guides students to build the lab sandbox. As shown in Table III, in the first lab, students create four virtual machine (VM) images (i.e., Windows, Ubuntu Desktop, Metasploitable, and Kali Linux) on a portable USB drive. Note that the created VMs are connected in a virtual VMWARE NAT-ed LAN. This configuration provides students full privileges for EH operations (on the VMs) while posing no threats or compliance issues to the campus network. Fourth, students are introduced to ChatGPT platform, prompt engineering, and potential security issues therein (i.e., the second lab from Table III).

B. Legal/Ethical Perspectives and PT Documentation

Addressing the potential legal and ethical issues is important when teaching offensive skills in ethical hacking [8]–[10]. As the second module in our curriculum, we prepare students with knowledge on legal and ethical implications of EH before diving into “hacking” skills. Specifically, we adopt a use-case based approach to study security-related laws and regulations such as HIPAA, HITECH, PCI-DSS, ISO/IEC 27001, Computer Fraud and Abuse Act, and CAN-SPAM Act, and discuss issues arising in uncommon scenarios such as third party Cloud system and cross-states compliance. We leverage the power of generative AIs with a role of a legal consultant in the lab (i.e., the first lab in Table IV) where students can explore legal/ethical consequences for each EH use case (e.g., see Fig. 1). Additionally, this module explores the types and formats of PT documents. In the second lab in Table IV, students create a Rule of Engagement (RoE) document by prompting ChatGPT to generate the file based the NIST format (i.e., see Fig. 2).

C. Reconnaissance

Module 3 starts the coverage on the sequence of EH workflow. Given the diverse topics in EH, we adopt classification in our design to identify and organize representative techniques. We classify reconnaissance techniques into three major categories: Web-based (information retrieval through web surfing), social-based (information probing through social

¹The terms of EH and PT are used interchangeably hereafter as in typical sense.

TABLE I
COURSE OBJECTIVES

| Bloom's Level | Detailed Objective |
|---------------|--|
| Understand | Explain the goal and the workflow of EH. |
| Understand | Explain the security implications of generative AIs. |
| Analyze | Explain and analyze security issues rooted in the generative AI systems. |
| Analyze | Explain and analyze ethical and legal implications of EH operations. |
| Apply | Perform EH workflow with representative tools and techniques (including generative AI tools). |
| Create | Prepare required documentation and reports for PT (including assistance from generative AIs). |
| Create | Identify system vulnerabilities and create remediation plans for hardening (including application of generative AI tools). |

TABLE II
CHATGPT SECURITY IMPLICATIONS

| Category | Use Cases |
|----------------------------------|--|
| ChatGPT-powered Attack | SQL Injection, Social Engineering (SE), Offensive Script/Code Generation |
| ChatGPT-powered Defense | Honey-pots, Vulnerability Analysis, ChatGPT-guided Hardening |
| ChatGPT-powered Security Tasking | Security Legal Consulting, Log Analysis, Document Generation, Report Writing |
| ChatGPT-rooted Security | Jail-break ChatGPT system itself, ChatGPT Privacy |

TABLE III
MODULE 1 LAB DESIGN

| Name | Coverage |
|----------------------|--|
| Sandbox Preparation | Virtual NAT-ed LAN build-up for VMWare Virtual Machines |
| ChatGPT and Security | ChatGPT basic introduction, and overview of associated security issues/goals |

Based on NIST SP 800-115, please produce a Role of Engagement document for a penetration testing, targeting on La Salle University's Website

Sure! Below is an example Rules of Engagement (RoE) document for a penetration testing engagement, based on NIST SP 800-115, targeting La Salle University's website. The RoE document outlines the necessary guidelines, limitations, and permissions for conducting the penetration test to ensure that it is performed safely, legally, and ethically.

Rules of Engagement (RoE) for Penetration Testing: La Salle University Website

Prepared By:
[Your Name / Team Name]
Date: December 31, 2024
Engagement Title:
Penetration Test of La Salle University Website

1. Introduction

Fig. 2. Automated RoE Document Generation

connection or social networks), and physical-based (information collection with physical presence). Three labs as shown in Table V are developed for the three categories, respectively. Specifically, for Web-based reconnaissance, students can apply tools such as Google hacking, WaybackMachine, job posting sites, WHOIS to retrieve information about the target. In social-based reconnaissance, students are guided to apply ChatGPT to craft and to detect phishing emails applying social engineering tactics (e.g., adding urgency). For physical-based reconnaissance, students apply hardware and software key-loggers to obtain credentials via keystroke recording.

D. Scanning

This module covers scanning, which represents a phase of active engagement with the target to extract in-depth information. We classify scanning techniques into four cate-

You are a legal consultant now. I need you to provide analysis for hacking attempts, explain what are the laws or regulations that are violated, and provide the consequences for each provided case.

Sure, I can help with that. When analyzing hacking attempts, several laws and regulations typically apply, depending on the jurisdiction, the nature of the hack, and the specific actions taken by the perpetrator. I will provide a general framework for legal violations and potential consequences based on common laws governing hacking.

Please provide the cases or scenarios related to hacking that you want analyzed, and I will break down the legal violations and consequences for each.

The first case: a student planted a keylogger in professor's computer to steal credentials, so he can alter his grades.

In this scenario, the student's actions are a clear violation of multiple laws and regulations, both criminal and civil. Here's a detailed analysis:

Legal Violations:

- Computer Fraud and Abuse Act (CFAA) - United States
 - The CFAA is the primary U.S. law regulating computer-related crimes. It criminalizes unauthorized access to computers and computer systems, including actions like planting

Fig. 1. Role Play as a Legal Consultant

TABLE IV
MODULE 2 LAB DESIGN

| Name | Coverage |
|--------------------------------------|---|
| Legal Consulting | Investigate security use cases and resulting legal/ethical consequences via ChatGPT Role Play |
| ChatGPT and Security Task Automation | Auto-generation of RoE document based on NIST template |

TABLE V
MODULE 3 LAB DESIGN

| Name | Coverage |
|-------------------------------|---|
| Web-based Reconnaissance | Apply Web-based tools for reconnaissance |
| Social-based Reconnaissance | Apply ChatGPT for social engineering |
| Physical-based Reconnaissance | Apply Key-logger tools for reconnaissance |

TABLE VI
MODULE 4 LAB DESIGN

| Name | Coverage |
|------------------------------|---|
| Port, OS, Vulnerability Scan | Apply NMAP, Nessus for scanning |
| ChatGPT for Scanning | Apply ChatGPT for Python scanning script generation |

gories: Port Scan, which involves network and host discovery via port status probing; Operating System (OS) scan, which obtains fingerprints of the target OS; Banner Scan, which grabs the banner information (i.e., software version) of a target service/system; and Vulnerability Scan, which identifies vulnerabilities of a target system (e.g., missing patches). There are two labs designed in this module as shown in Table VI. The first lab introduces port/OS scanning with various types of nmap scanning (e.g., Open/Half Open), and applies Nessus and nmap-script-based scan for vulnerability identification (with the results mapped to the Common Vulnerability Scoring System). In the second lab, students apply ChatGPT to create customized scanning scripts in Python.

E. Gaining Access

This module covers the most important phase of EH that obtains the access rights to the target system. We classify the representative approaches into four categories: crack passwords (e.g., apply dictionary, brute-force, or rainbow table to decipher the password hash); bypass password (e.g., session hijacking to bypass authentication); steal passwords (e.g., via SE or sniffing); and apply default passwords. As shown in Table VII, the first three labs are devoted to three techniques, respectively. Note that in the first lab, ChatGPT is also used to assist the generation of a customized dictionary file (see Fig. 3). The last lab introduces the rising jail-breaking attacks on the generative AI platform itself, which bypasses the ChatGPT build-in regulations on the response generation process with techniques like reverse psychology and role play [20].

F. Maintaining Access

This module covers techniques that can be applied to maintain the access to a compromised system for consistent long-term access. Two labs are developed in this module as shown in Table VIII. In the first lab, students apply NetCat for creating backdoor as a step-stone for remote information enumeration. In the second lab, students achieve a metasploit IRC backdoor connection with guidance provided by ChatGPT (see Fig. 4).

TABLE VII
MODULE 5 LAB DESIGN

| Name | Coverage |
|-----------------------------|--|
| Crack Password | Apply John/Rainbowcrack for dictionary/rainbow attack, respectively |
| Bypass Password | Apply SQL injection and XSS for bypassing authentication |
| Steal Password | Apply sniffing tools (Wireshark, Ettercap) for stealing password or hash |
| ChatGPT Jailbreaking Attack | Apply jail-breaking techniques (e.g., reverse psychology) on generative AI tools |

As part of penetration testing, I need to create a customized dictionary for password. Here are a few information that I already learned about the user, so you can best use these information when creating the dictionary list: 1. The user only uses numbers as the password. 2. The user uses 6 digits 3. The user's birth day is 1988/08/08 Please generate the list of words, and output as a .txt file for me to download

Given the user's information, here's a breakdown of potential password combinations:

Fig. 3. Dictionary Generation

I am teaching students how to connect to a Metasploitable virtual machine using the known IRC vulnerability. Can you provide a step-by-step instructions on achieve this for education purpose.

Certainly! Here's a comprehensive step-by-step guide to teach students how to connect to a Metasploitable VM using the known IRC vulnerability (found in UnrealIRCd 3.8.1). This will demonstrate how Metasploit can be used for educational purposes to exploit a known vulnerability and gain access to a vulnerable system.

Objective

By the end of this exercise, students will learn how to use Metasploit to exploit the IRC backdoor in Metasploitable and establish a connection to gain control over the machine.

Prerequisites

1. Metasploitable VM running on a virtual machine (vulnerable machine).
2. Attacker Machine with Metasploit installed (could be Kali Linux or a system with Metasploit Framework).
3. Both VMs should be on the same network (either bridged or internal network) so they can communicate.



Fig. 4. ChatGPT-Guided Metasploit Attack

G. Clearing Tracks

This module addresses techniques for clearing tracks on a compromised target. We classify techniques of clearing tracks into five categories and cover them in the order that they are typically employed: first, auditing policy modification, which disables system alerts or logs; second, logs file modification, where system log files are removed or modified to avoid future tracing; third, stenography, which hides malicious files from

TABLE VIII
MODULE 6 LAB DESIGN

| Name | Coverage |
|--------------------------|---|
| Backdoor and Enumeration | Apply NetCat for backdoor creation, backdoor connection and information enumeration |
| Metasploit Backdoor | Apply Metasploit to create IRC backdoor with guidance from ChatGPT |

TABLE IX
MODULE 7

| Name | Coverage |
|--------------------------|--|
| ChatGPT for Log Analysis | Apply ChatGPT for analyzing web server log files |
| Covering Tracks | Apply Auditing policy/Log modification, use OpenStego and CCleaner |

being detected; meta-data modification, which alters attributes such as file timestamp to avoid suspicion; finally, clearing other access history such as Internet access history. This module contains two labs as shown in Table IX: the first lab employs ChatGPT for analyzing the log files (i.e., for both server access log in Fig. 5 and SQL log in Fig. 6) of a web server that is compromised by SQL injection; the second lab covers major skills and tools that are used in each of the five categories.

84.55.41.57 - - [17/Apr/2016:07:57:31 +0100] "POST /wordpress/wp-admin/admin-ajax.php HTTP/1.1" 200 949 "http://www.mywebsite.com/wordpress/wp-admin/admin.php?page=file-manager_settings"

Based on the Apache server log entries you have provided, there are some signs that suggest a potential malicious attack or compromise of your WordPress site. Below is an analysis of the log and key suspicious activities to watch out for:

1. Repeated Access to WordPress Login Page (wp-login.php)

```
plaintext
84.55.41.57 - - [17/Apr/2016:06:57:24 +0100] "GET /wordpress/wp-login.php HTTP/1.1" 200 15
84.55.41.57 - - [17/Apr/2016:06:57:31 +0100] "POST /wordpress/wp-login.php HTTP/1.1" 302 1
```

- Login attempts:** The attacker first accesses the login page (GET wp-login.php), followed by a POST request with an attempt to authenticate. The response 302 indicates a redirection, which might happen after a failed login attempt or a successful login followed by a redirect to another page.
- Suspicious:** A large number of failed login attempts within a short period is a common sign of brute-force attacks trying to guess credentials.

2. Access to Admin Dashboard (wp-admin)

Fig. 5. Analysis of Web Server Log

```
SELECT
CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NU
LL,NULL-- HTTP/1.1" 200 182 "-" Mozilla/5.0 (Windows; U; Windows
NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR
3.5.30729)"
```

Looking at the additional logs you've provided, there are several suspicious activities that indicate an attempt at SQL injection attacks targeting your WordPress site. Let's break it down:

Detailed Analysis of New Log Entries

1. SQL Injection Attempts (Time: 08:22:13)

```
plaintext
84.55.41.57 - - [14/Apr/2016:08:22:13 +0100] "GET /wordpress/wp-content/plugins/custom_plu
```

- The attacker is attempting a SQL injection using a payload in the `user_id` parameter in the URL. This is a classic technique where an attacker tries to run arbitrary SQL queries on the database.

Fig. 6. SQL-Injection Log

H. Hardening Techniques and PT Reporting

This module covers hardening techniques and PT report writing, where the former is often included in the latter

as *recommendation or remediation*. A summary of major techniques for hardening are listed below according to the PT phases. Note that these techniques are already sporadically covered in respective phases and are explored in related labs. This module only provides a holistic review and classification of these techniques.

- 1) **[Reconnaissance:]** Employee training; Limit DNS/WHOIS information; Network segmentation; Web application firewall.
- 2) **[Scanning:]** Regular patch management; Intrusion detection system; Firewall; Service auditing.
- 3) **[Gaining Access:]** MFA; Account and password policy auditing and enforcement; Security monitoring and logging; Enhanced remote access security (e.g., VPN); Hardware encryption (e.g., BitLocker)
- 4) **[Maintaining Access:]** Anti-malware; Continuous system auditing; System regular backup.
- 5) **[Covering Tracks:]** Implement log integrity; Centralized logging; Automated alerts; Regular incident response testing.

I. Term Project and Demonstration

As the final module, as a term project, students study a choice of EH topic in groups. The chosen topic can be either an emerging topic or a classic topic with new development that has not been covered in depth during the course. At the end of the semester, each group presents their findings and demonstrates the practical component of their project to the class.

V. STUDENT PERFORMANCE, FEEDBACK, AND LESSONS LEARNED

In this section, we discuss student performance and feedback, and share our learned lessons.

A. Student Performance

With the teaching of this EH course cross three sections, both the student engagement and the overall student performance are very satisfactory. The average grade distribution is shown in Fig. 7 below. Clearly, nearly 90% students obtained grades in the range of $[A, B]$. Students have completed many exciting term projects on emerging topics such as Bluetooth Security, Cloud Security, Credit Card Security, to name a few. In addition, multiple students continue pursuing certifications towards the Cybersecurity career path after taking this course, with considerable credits attributed to this course.

B. Student Feedback

This course is rated on average as 4.94/5 in terms of its overall value (excluding instructor factors). More than 90% of students give the highest ratings for all aspects of course features. When polled about the labs that contributed most to learning, as shown in Fig. 8, 68% of student votes are associated to ChatGPT-infused labs. Additionally, some representative student comments are provided below.

- 1) This course “covered every phase and showed us tools of EH ... if we sought a career in cybersecurity.”
- 2) This course has “good layout and flow to the material.”
- 3) This course is “interesting, excellent, latest.”
- 4) The course “really has a specific path into ... ethical hacking ... and penetration testing.”
- 5) This course is “the best course” at our university.
- 6) “I really enjoy the ChatGPT labs which allow me to learn AI’s applications in security ...”

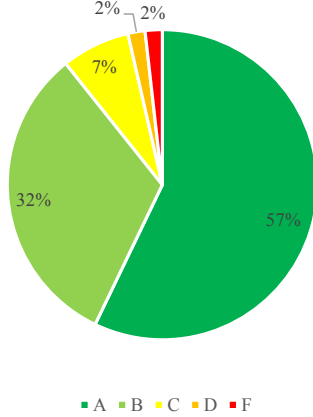


Fig. 7. Student Grade Distribution

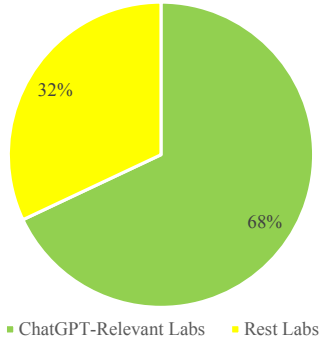


Fig. 8. Lab Preference

C. Lesson Learned

We summarize some of the major lessons that we learned below.

Keep the design cost-effective and IT-compliant: In many institutions, the major obstacle to running an EH course is the cost, space, and technical support. Our design features a VM+USB based lab solution. Our choice results in a cost-effective design by resorting to either free software (e.g., all build-in tools in Kali) or software with free education versions (e.g., Nessus community version). The cost per student is approximate 70 dollars for the portable USB driver and the keylogger hardware. Likewise, our choice poses no threats to campus network, we select the NAT-ed VMs solution as the sandbox network for EH activities, which ensures that

the solution is compliant with all university IT policies. VM+USB-based solution also addresses the need for space and technical support (i.e., students have administrative privileges on their own VMs).

Legal/Ethical reminders should be consistently provided: Even though our solution is IT compliant by design, in the process of teaching, we still encountered multiple incidents of policy violations, which were caused by students who overlooked instructions and attempted EH activities on physical lab computers. It is hence important to provide consistent reminders in each lab instruction for the compliance issues as well as legal/ethical consequences.

Effectiveness of security applications of generative AI tools: Among the four categories of security implications elaborated in Table II, based on our teaching, practices from the groups of ChatGPT-powered defense and ChatGPT-powered security tasking are very effective and repeatable (with minor variations in response). However, the practices from the groups of ChatGPT-powered offense and ChatGPT-rooted security often lead to unsatisfying answers due to the build-in safety filters of ChatGPT (that evolve overtime). It is thus important to take these limitations into consideration (i.e., making the lab open-ended or avoiding prompts that are likely trigger inconsistency). Additionally, there are many important practices are not yet supported with current generative AI tools. For instance, ChatGPT still lack the ability to analyze window log (.evtx) files.

Generative AI tools and Academic Integrity: The rapid development of generative AI tools definitely outpaces the establishment of academic integrity code for its use in academic works. Compared to traditional search engines, the information returned by generative AIs are tailored and generated on demand, which are challenging to detect. As a course design that prompts the use of generative AIs, our current policy is to ask students clearly declare their use of generative tools and clearly label their work that are AI-assisted or generated.

VI. CONCLUSION AND FUTURE WORK

In this work, for the first time, we present a ChatGPT-enriched course curriculum design for Ethical Hacking. ChatGPT is used in the context of ethical hacking under four categories: ChatGPT-powered Attack, ChatGPT-powered Defense, ChatGPT-powered Security Tasking, and ChatGPT-rooted Security. Among diverse and ad hoc topics, our design maintains a smooth flow that covers representative and certification-aligned techniques in EH. In addition, our lab design is cost-effective and IT-compliant with innovative ChatGPT applications therein. Our current work is only limited to the application of text-based generative AI tool ChatGPT. As the next step, we will further incorporate other types of generative AI tools as well as alternative text-based tools (e.g., Google Gemini) into consideration. Additionally, as we are developing a new program in Cybersecurity, the impact of generative AI tools to our curriculum will also be assessed in the future.

REFERENCES

- [1] U. B. of Labor Statistics, "https://www.bls.gov/ooh/computer-and-information-technology," Last Accessed: 01/05/2025.
- [2] "Ethical hacking emerges as unique career path in cybersecurity," <https://tech.co/news/ethical-hacking-career-cybersecurity-2017-04>.
- [3] C. S. C. 2023, "https://csed.acm.org/," Last Accessed: 01/12/2024.
- [4] X. Wang, Y. Bai, and G. C. Hembroff, "Hands-on exercises for it security education," in *Proceedings of the 16th Annual Conference on Information Technology Education*, ser. SIGITE '15. New York, NY, USA: ACM, 2015, pp. 161–166. [Online]. Available: <http://doi.acm.org/10.1145/2808006.2808023>
- [5] A. J. Wu, "Project development for ethical hacking practice in a website security course," in *Proceedings of the Western Canadian Conference on Computing Education*. New York, NY, USA: Association for Computing Machinery, 2014. [Online]. Available: <https://doi.org/10.1145/2597959.2597963>
- [6] X. Yuan, W. He, L. Yang, and L. Simpkins, "Teaching security management for mobile devices," in *Proceedings of the 17th Annual Conference on Information Technology Education*, ser. SIGITE '16. New York, NY, USA: ACM, 2016, pp. 14–19. [Online]. Available: <http://doi.acm.org/10.1145/2978192.2978227>
- [7] L. Li, K. Qian, Q. Chen, R. Hasan, and G. Shao, "Developing hands-on labware for emerging database security," in *Proceedings of the 17th Annual Conference on Information Technology Education*, ser. SIGITE '16. New York, NY, USA: ACM, 2016, pp. 60–64. [Online]. Available: <http://doi.acm.org/10.1145/2978192.2978225>
- [8] B. A. Pashel, "Teaching students to hack: Ethical implications in teaching students to hack at the university level," in *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*. New York, NY, USA: Association for Computing Machinery, 2006, pp. 197–200. [Online]. Available: <https://doi.org/10.1145/1231047.1231088>
- [9] Z. Trabelsi and M. McCoe, "Ethical hacking in information security curricula," *Int. J. Inf. Commun. Technol. Educ.*, vol. 12, no. 1, pp. 1–10, Jan. 2016. [Online]. Available: <https://doi.org/10.4018/IJICTE.2016010101>
- [10] P. Y. Logan and A. Clarkson, "Teaching students to hack: Curriculum issues in information security," in *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education*. New York, NY, USA: Association for Computing Machinery, 2005, pp. 157–161. [Online]. Available: <https://doi.org/10.1145/1047344.1047405>
- [11] S. Peltserverger and C. Zhang, "Bottleneck analysis with netkit: Teaching information security with hands-on labs," in *Proceedings of the 15th Annual Conference on Information Technology Education*, ser. SIGITE '14. New York, NY, USA: ACM, 2014, pp. 45–50. [Online]. Available: <http://doi.acm.org/10.1145/2656450.2656479>
- [12] Y. Li and M. Xie, "Platoon: A virtual platform for team-oriented cybersecurity training and exercises," in *Proceedings of the 17th Annual Conference on Information Technology Education*, ser. SIGITE '16. New York, NY, USA: ACM, 2016, pp. 20–25. [Online]. Available: <http://doi.acm.org/10.1145/2978192.2978230>
- [13] Y. B. Choi, S. Lim, and T. H. Oh, "Feasibility of virtual security laboratory for three-tiered distance education," in *Proceedings of the 2010 ACM Conference on Information Technology Education*, ser. SIGITE '10. New York, NY, USA: ACM, 2010, pp. 53–58. [Online]. Available: <http://doi.acm.org/10.1145/1867651.1867666>
- [14] Y. Li, D. Nguyen, and M. Xie, "Ezsetup: A novel tool for cybersecurity practices utilizing cloud resources," in *Proceedings of the 18th Annual Conference on Information Technology Education*, ser. SIGITE '17. New York, NY, USA: ACM, 2017, pp. 53–58. [Online]. Available: <http://doi.acm.org/10.1145/3125659.3125699>
- [15] T.-S. Chou and J. Jones, "Developing and evaluating an experimental learning environment for cyber security education," in *Proceedings of the 19th Annual SIG Conference on Information Technology Education*. New York, NY, USA: Association for Computing Machinery, 2018, pp. 92–97. [Online]. Available: <https://doi.org/10.1145/3241815.3241855>
- [16] M. Ghiglieri and M. Stopczynski, "Seclab: An innovative approach to learn and understand current security and privacy issues," in *Proceedings of the 17th Annual Conference on Information Technology Education*, ser. SIGITE '16. New York, NY, USA: ACM, 2016, pp. 67–72. [Online]. Available: <http://doi.acm.org/10.1145/2978192.2978224>
- [17] R. Kalyanam and B. Yang, "Try-cybsi: An extensible cybersecurity learning and demonstration platform," in *Proceedings of the 18th Annual Conference on Information Technology Education*, ser. SIGITE '17. New York, NY, USA: ACM, 2017, pp. 41–46. [Online]. Available: <http://doi.acm.org/10.1145/3125659.3125683>
- [18] B. Yang, R. Kalyanam, C. Willis, M. Lambert, and C. Kirkpatrick, "Cheese: Cyber human ecosystem of engaged security education," in *Proceedings of the 20th Annual SIG Conference on Information Technology Education*. New York, NY, USA: Association for Computing Machinery, 2019, pp. 189–190. [Online]. Available: <https://doi.org/10.1145/3349266.3351393>
- [19] P. Shipman and R. Bull, "Lab on a stick," in *Proceedings of the 16th Annual Conference on Information Technology Education*, ser. SIGITE '15. New York, NY, USA: ACM, 2015, pp. 33–38. [Online]. Available: <http://doi.acm.org/10.1145/2808006.2808034>
- [20] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy," *IEEE Access*, vol. 11, pp. 80 218–80 245, 2023.
- [21] C. Hu and J. Chen, "A dimensional perspective analysis on the cybersecurity risks and opportunities of chatgpt-like information systems," in *2023 International Conference on Networking and Network Applications (NaNA)*, 2023, pp. 324–331.
- [22] X. Peng, Y. Zhang, J. Yang, and M. Stevenson, "On the vulnerabilities of text-to-sql models," in *2023 IEEE 34th International Symposium on Software Reliability Engineering (ISSRE)*, 2023, pp. 1–12.
- [23] P. Gallus, M. Štěpánek, T. Ráčil, and P. Františ, "Generative neural networks as a tool for web applications penetration testing," in *2023 Communication and Information Technologies (KIT)*, 2023, pp. 1–5.
- [24] J. Ragsdale and R. V. Boppana, "On designing low-risk honeypots using generative pre-trained transformer models with curated inputs," *IEEE Access*, vol. 11, pp. 117 528–117 545, 2023.
- [25] Jailbreak, "https://gist.github.com/coolaj86," Last Accessed: 02/16/2024.
- [26] N. Guillén-Yparrea and F. Hernández-Rodríguez, "Unveiling generative ai in higher education: Insights from engineering students and professors," in *2024 IEEE Global Engineering Education Conference (EDUCON)*, 2024, pp. 1–5.
- [27] M. E. S. Simaremare, C. Pardede, I. N. I. Tampubolon, D. A. Simanungsong, and P. E. Manurung, "The penetration of generative ai in higher education: A survey," in *2024 IEEE Integrated STEM Education Conference (ISEC)*, 2024, pp. 1–5.
- [28] A. K. Dey, V. K. Chauhan, P. K. Singh, and A. Sarkar, "Exploring the integration of generative ai in modern education systems: A comprehensive analysis," in *2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAQSA)*, 2024, pp. 1–8.
- [29] Y. Zhang, W. Ma, and M. Xiao, "Exploring teachers' perspectives and strategies on student assessment using generative ai in chinese universities," in *2024 4th International Conference on Educational Technology (ICET)*, 2024, pp. 403–407.
- [30] A. de la Torre and M. Baldeon-Calisto, "Generative artificial intelligence in latin american higher education: A systematic literature review," in *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, 2024, pp. 1–7.
- [31] C. Kicklighter, J. H. Seo, M. Andreassen, and E. Bujnoch, "Empowering creativity with generative ai in digital art education," in *ACM SIGGRAPH 2024 Educator's Forum*, ser. SIGGRAPH '24. New York, NY, USA: Association for Computing Machinery, 2024. [Online]. Available: <https://doi.org/10.1145/3641235.3664438>
- [32] Y. Wang, M. McCoe, Q. Hu, and M. Jalalitar, "Teaching security in the era of generative ai: A course design of security + chatgpt," in *2024 IEEE Integrated STEM Education Conference (ISEC)*, 2024, pp. 01–06.
- [33] B. Hamdan, "Integrating chatgpt in cybersecurity education: Use cases and implications," *J. Comput. Sci. Coll.*, vol. 40, no. 2, p. 105–114, Oct. 2024.
- [34] CEH, <https://www.eccouncil.org/>.
- [35] Y. Wang, M. McCoe, and Q. Hu, "Developing an undergraduate course curriculum for ethical hacking," in *Proceedings of the 21st Annual Conference on Information Technology Education*, ser. SIGITE '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 330–335. [Online]. Available: <https://doi.org/10.1145/3368308.3415366>