ISSN: 2473-4901
v12 n6849

Teaching Case:

Developing Hacker's Mindset and Skillset: An Ethical Hacking Project

Fang Chen
fang1.chen@umontana.edu

Shawn Clouse
shawn.clouse@umontana.edu

David Firth
David.Firth@umt.edu

Management Information Systems Department
College of Business
University of Montana
Missoula, MT, 59812, USA

Hook

Organizations may lock their digital doors, yet unknowingly leave the keys under a clear doormat, beside the garage, or in the backyard. Hackers can quietly locate these keys and use them to enter the system without triggering an alarm. What common tools can help hackers locate the keys?

Abstract

The paper describes a project implemented in an Ethical Hacking course with a focus on training hacker's mindset and skillset by surveying a broad attack surface, using a variety of passive reconnaissance techniques and tools, studying the security incidents that happened in the real world, and collecting open-source intelligence (OSINT) for two organizations from a hacker's perspective. The reconnaissance tools used include DNS lookup tools (Whois, NSlookup, Dig, and Host), Shodan search, Google Dorking, and Wayback Machine search. The paper also discusses students' feedback on the project and future improvements.

Keywords: Cybersecurity, ethical hacking, hacker's mindset, adversarial thinking, reconnaissance, Shodan search.

Developing Hacker's Mindset and Skillset: An Ethical Hacking Project

Fang Chen, Shawn Clouse and David Firth

1. INTRODUCTION

Cybersecurity is becoming increasingly important. According to a report by the Identity Theft Resource Center (ITRC), there was a record high of 3,332 data compromises in 2025, which increased by 4% from 2024 (Alder, 2025). Meanwhile, in 2025, the cybercrime-related financial loss peaked at $20.9 billion US dollars, beating the previous record of $16.6 billion in losses set in 2024 by 26% (Federal Bureau of Investigation, 2025). The demand of cyber professionals is high, but the shortage of qualified cyber professionals is an issue. According to the 2025 CyberSeek/NIST data, the U.S. needs about 265,000 additional cybersecurity professionals, and the current workforce is sufficient to fill only 74% of cybersecurity jobs (CyberSeek, 2025).

Cybersecurity jobs vary vastly, Ramezan (2023) groups these jobs into 9 sub-fields: architecture, auditing, education, GRC (governance, risk, and compliance), management, operations, penetration testing, software security, and threat intelligence / research. Cybersecurity education has traditionally focused on defensive activities such as identifying attack surfaces, mitigating vulnerabilities, and hardening systems. However, effective defense requires more than a purely defensive perspective. The Cybersecurity Curricula, published in 2017 by ACM, IEEE-CS, and AIS, specifies that "*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. All the knowledge areas include knowledge units that can be taught from both cyber-defense and cyber-offense perspectives*" (Association of Computing Machinery, 2017, p. 21), and the report also emphasizes 6 crosscutting concepts which are fundamental to students' ability to understand knowledge areas regardless of the disciplinary subject: Confidentiality, Integrity, Availability, Risk, Adversarial Thinking, and Systems Thinking. These crosscutting concepts provides organizational schema for the knowledge in cybersecurity (Association of Computing Machinery, 2017). However, in practice, the adversarial thinking has not received enough attention, as Chou and Mohammed (2022) pointed out "*cybersecurity education has put a lot of effort on the protection of information infrastructure, but much less on the perspective of cyberattack modelling and ethical hacking strategies. However, we believe the study of attack should be considered as equally important as defense*." (p.3)

Schoenmakers et al. (2023) use the term security mindset and define the security mindset as the tendency to search for security flaws in nearby systems. They specified that being a cybersecurity professional is neither necessary nor sufficient to have a security mindset, and technical knowledge is not sufficient for a security mindset either. In other words, simply teaching students hacking skillsets is not sufficient for students to develop hacker's mindset organically, the hacker's mindset needs to be cultivated with explicit purpose and activities. In our ethical hacking course, we cultivate students' holistic view of attack surface and systems vulnerabilities through offender's/hacker's perspective by designing a project of using a variety of tools for passive reconnaissance combined with case studies.

In this paper, we use the term hacker's mindset instead of adversarial thinking or security mindset, because adversarial thinking can be applied to military, sports, politics in addition to information security; and security mindset has an emphasis of a defense perspective. The hacker's mindset is about information security with an emphasis of the offensive perspective.

Students are encouraged to use AI thoughtfully for the project, because the cybersecurity industry increasingly uses AI. According to a new World Economic Forum report, "*94% of cyber leaders identify AI as a defining force and 77% of organizations already use it in their cyber operations*" (World Economic Forum, 2026). Our project is not designed for students to learn AI in cybersecurity, rather we encouraged students to use AI, and students are required to disclose and reflect on their AI usage.

The rest of the paper is organized as the following: Section 2 describes the major components covered in the ethical hacking course and defines hacker's mindset. Section 3 introduces projects design,

ISSN: 2473-4901
v12 n6849

implementation and results. Section 4 reports students' reflection of their learning and their AI usage for the project. Section 5 discusses our reflections, limitations and future improvements and Section 6 presents the conclusion.

2. BACKGROUND

2.1 Ethical Hacking Course Structure

Our Ethical Hacking course is required for third-year cybersecurity majors and covers legal compliance, penetration-testing frameworks, methodologies, and tools. We use Cisco's free online "Ethical Hacker" course (netacad.com), which includes 10 modules and hands-on labs using a customized Kali Linux virtual machine (VM) in VirtualBox. Appendix A shows the module content. Students install the VM on their laptops, allowing them to complete all labs independently. Figure 1 displays some basic information about the course. Our project includes content from three Cisco labs: Cisco Lab 3.1.9, which covers DNS tools such as nslookup, whois, dig, and host; Cisco Lab 3.1.19, which covers advanced search such as Google Dorking and Wayback machine search; and Cisco Lab 3.1.21, which is about Shodan search. However, our project design was not tied to the Cisco labs, therefore, as long as students learned how to use the tools involved in the project, they will be fine.

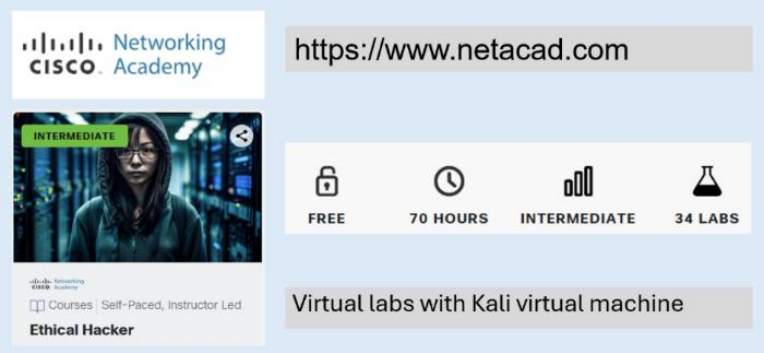

Figure 1. Cisco's Ethical Hacker Course Overview

The Cisco's "Ethical Hacker" course covers all five phases of a cyber-attack execution: reconnaissance, scanning, gaining access, maintaining access, and clearing tracks (Fahid, 2025). As displayed by Figure 2, a cyber-attack starts with reconnaissance where a hacker gathers information about potential targets to identify weaknesses. Scanning (probing the target) refers to the hacker use tools to scan the networks, identifying open ports and detecting exploitable vulnerabilities in the target's infrastructure. Gaining access is to compromise the system by exploiting the vulnerabilities discovered. Maintaining access refers to keep persistent access to the compromised system even if the original vulnerability is patched by creating backdoors and using reverse shells, etc. Clearing tracks is the last phase, which refers to removing any logs or files that could reveal their presence (Fahid, 2025).

Figure 2. Five Phases of Hacking (created with ChatGPT)

2.2 Hacker's Mindset

Ethical hacking consists of three major components: hacker's mindset, hacker's skillset, and legal boundaries and ethical conduct for ethical hacking. In their systematic review of adversarial thinking in cybersecurity, Browne & Pardede (2026) identified several terms used to describe hacker's mindset, such as adversarial thinking (e.g., Association of Computing Machinery, 2017; Hamman & Hopkinson, 2016; Schneier, 2023) or security mindset (Schoenmakers et al., 2023). Schoenmakers et al. (2023, p.2) defined hacker's mindset is "*thinking like a hacker*", "*thinking like an attacker*", or "*thinking about failures and how to trigger them*."

Schoenmakers et al. (2023) pointed out that security mindset can be defined as an ability, trait, belief, value or habit, but "*most existing discussions of the security mindset emphasize that it involves engaging in an active cognitive process to identify security vulnerabilities*" (p. 4). To examine the cognitive process of the security mindset, they interviewed 21 cybersecurity professionals in a variety of job roles about self-identified security mindset. From the interview transcripts, they conceptualized security mindset into three sequential processes: "*monitoring*," "*investigating*," and "*evaluating*". Monitoring refers to people who "*spotted potential security flaws in the digital, physical, and social worlds around them*" (p. 5). These people seem to use a cognitive filter to spot the abnormal thing, item, or feature from the context. This monitoring ability and process can be viewed as situational awareness. Investigating is a conscious process to figure out how the system works and how the flaw could be exploited. Evaluating refers to conscious estimate about the possibility of exploitation of the flaw and severity of the consequences. Figure 3 illustrates these three processes. The monitoring process does not necessarily involve understanding the technical details of a flaw but investigating and evaluating require understanding the technical details of the flaw.

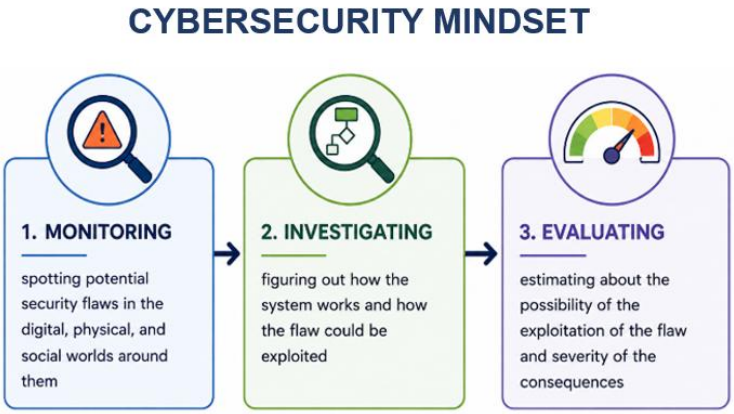

Figure 3. Three Processes in Security Mindset (created with ChatGPT)

The study by Schoenmakers et al. (2023) also reported that the security mindset was largely motivated or driven by sense of curiosity and rewarded by discovery. Even though sense of curiosity can be reviewed as a personal trait, they encourage educators to nurture and enhance students' security mindset deliberately through activities such as free exploration, reading case studies and real-world security reports, and discussing about high-priority targets and commonly used attack routes and techniques.

Our project design is a deliberate effort to cultivate student's hacker's mindset which involves searching for system's vulnerabilities, examining the root causes of the vulnerabilities, and the consequences of the vulnerabilities exploitation. The project focuses on free passive reconnaissance tools. Passive reconnaissance is the covert process of gathering information about a target system, network, or organization without directly interacting with its IT infrastructure. By relying exclusively on public sources and third-party databases, security teams and threat actors build a target profile while remaining completely undetected. Conversely, active reconnaissance utilizes tools to interact with a target system, network, or application to gather intelligence. Unlike passive reconnaissance, active

ISSN: 2473-4901
v12 n6849

methods involve sending probes, packets, or requests to the target systems, which yield more detailed and real-time data but risks triggering security alerts and leaving traces in system logs.

Reconnaissance is often considered "*the most critical phase of a cyberattack because it lays the groundwork for the entire attack operation*" (Alabdulatif & Thilakarathne, 2025, p. 3). It is completely legal for people to conduct passive reconnaissance to collect information, often referred to as open-source intelligence (OSINT). Active reconnaissance and scanning are usually illegal unless the actor obtains the system owner's written permission. It is challenging to obtain organizations' written permission for active reconnaissance and scanning due to the possibility that students could bring down the systems during the scan. As a result, our project focuses on passive reconnaissance.

Our project includes DNS (Domain Name System) lookups tools and advanced search. The DNS lookup tools include Whois, NSlookup, Dig, and Host. These DNS tools are pre-built in Kali VM, and are covered in Cisco's Ethical Hacker Lab 3.1.9. Hackers can use these DNS tools to map a target's network infrastructure, identify active IP addresses, and find misconfigured DNS servers. The advanced search includes Shodan search, Wayback Machine search and Google Dorking. Shodan is a specialized search engine that indexes and displays Internet-connected devices, such as servers, routers, security cameras, smart home appliances, and Industrial Control Systems (ICS). Shodan is covered in Cisco's Ethical Hacker Lab 3.1.21.

Google Dorking (also known as Google Hacking) uses advanced search operators in Google search to find specific, often sensitive, information or vulnerabilities that are indexed by the search engine but are not searchable with regular Google search and usually are not meant to be accessible by the public. The search interface is the same as regular Google search, but the search terms need to conform to the syntax of search operators, as displayed by Figure 4.

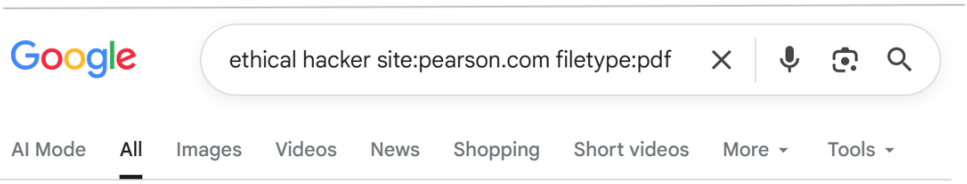

Figure 4. Google Dorking Operators

In this query, "ethical hacker" is the search key words, this search is only limited to website named "pearson.com", and to the pdf file type. So, the query means "find PDF documents on Pearson's website that contain information related to ethical hacking".

The Wayback Machine is a free digital archive of the Web created by the Internet Archive (https://web.archive.org/). It allows users to view past versions of websites, track how pages have changed over time, and access content that has been deleted or taken offline. It has archived over 1 trillion web pages, with some snapshots dating back to 1996. Users can find deleted articles, old personal blogs, and old employee names, etc. Journalists and researchers use archived pages to verify historical claims. Hackers may use Wayback Machine to find deleted files containing sensitive information. Google Dorking and the Wayback Machine are covered in Cisco's Ethical Hacker Lab 3.1.19.

Previous studies report class projects that use these passive reconnaissance tools. For example, a project by Fernández-Caramés & Fraga-Lamas (2020) focused on cybersecurity audits on IoT systems and devices with Shodan search. The project was implemented in a cybersecurity master program, and students were recent graduates from CS and electrical engineering, who had good coding skills, but no previous experience with IoT or Shodan. To prepare for the projects, students learned technical components of IoT architecture and different types of attacks to IoT architecture. The project included 1) labs of Shodan search for unsecured Webcams, video surveillance systems, smart alarm system, and other smart home appliances; 2) analysis of how to prevent Shodan-based attacks on IoT devices, such as minimizing the number of open ports, and blocking Shodan crawler to prevent IoT devices from being indexed, etc.

Another study reports a project of Google Dorks, Shodan, and Censys (Alabdulatif & Thilakarathne, 2025). Censys is similar to Shodan, but it has a different focus. Shodan emphasizes real-time identification of exposed devices, services, and vulnerabilities, whereas Censys focuses on structured analysis of hosts, certificates, and network infrastructure, providing deeper datasets for research and asset discovery. For the project, after students familiarized themselves with operations of Google Dorks, Shodan, and Censys, they developed an automated all-in-one tool that integrates the functionalities of Google Dorks, Shodan, and Censys. The project was designed for CS students, and the focus is on developing a tool by integrating existing tools.

The above projects illustrate the importance of using passive reconnaissance tools such as Shodan and Google Dorking. However, these projects focus on the technical components of the reconnaissance tools and digital infrastructure. Our project is designed for students of cybersecurity in a business school, so a more application-oriented project is a better fit for our students.

3. PROJECT IMPLEMENTATION AND RESULTS

3.1 Project Design and Implementation

We implemented the project in the Spring of 2026. This was the first time Ethical Hacking course was offered, and the first time this project was implemented. There were 15 students in the class, and they formed 4 teams (Three teams had 4 members, and one team had 3 members). Each team chose a certain region or area of US 48 continental states for the project. We divided the 48 states into the "West" and "East", two teams were assigned to explore the West, and the rest were assigned to explore the East, as displayed by Figure 8. The instructor wanted to give teams enough freedom to explore but prevent teams from focusing on exploring to just one or two places.

Figure 5. Teams' Region Assignment

The main body of the project report includes four parts as displayed by Table 1. The final deliverables were a formal report of 20 – 35 pages, and a 10–15-minute group presentation about the project with a PPT file.

Each team used Shodan to search for four types of unsecured systems, explain common vulnerabilities of these systems, measures to secure them, and report security incidents that happened in the real world related to these vulnerabilities. The instructor chose these systems to broaden students' view of attack surface. Webcams are widely used by individuals and organizations, ICS are part of critical infrastructures, Virtual Network Computing (VNC) is used for remote system control and collaboration, and databases are used to store and retrieve data. After the Shodan search, teams need to profile two organizations from a hacker's perspective. Teams were required not to choose any government agencies or companies that were too large or well-known (e.g., Amazon, Microsoft). We want to prevent students from accidentally clicking Shodan search-result links and triggering a government agency's security alerts. At the same time, investigating well-known enterprises may not offer enough novelty for meaningful student exploration.

Part	Tasks
Executive Summary	Summarizing the entire report so that a reader can understand the key points without reading the report.
Part 1: Shodan Search	Searching for four types of systems in the chosen region: • Webcam (for two cities) • ICS (4 protocols, for two cities) • VNC (for two states) • Databases (3 databases, the entire US)
Part 2: Cases of Real Security Incidents	Reporting several real security incidents for each type of system identified above.
Part 3: Profiling Two Organizations	Profiling two organizations from a hacker's perspective • Regular google search for basic information. • DNS lookup tools for digital infrastructure information. • Advanced google search for information above and beyond regular google search. • Searching for the organization's old data archived by Wayback Machine.
Part 4: Reflections	• Reflecting about learning hacker's mindset & skillset. • Disclosure and reflection about AI usage.

Table 1. Project Report Structure

As educators, we are concerned that students use AI to skip learning. This should not be a major concern for this project due to the nature of the project. Students must use specific tools to produce results, and they are required to provide the screen shot of the search results. Additionally, the screen shot of the DNS tools often has time stamps as well. It is very difficult for students to fake the screen shots with AI. Teams are required to disclose AI usage and write reflections about human-AI interaction.

To ensure students engage in the project legally and ethically, the instructor emphasized in writing that students are not allowed to click on any live link for the identified devices/systems, and also orally emphasized this legal requirement multiple times during classes. The additional legal and ethical safeguard for the course and this project was a signed "Code of Conduct" by every student. On the Code of Conduct, students agree to conduct all practices within legal boundaries, and not to share any security vulnerabilities identified from this course to people outside of this class.

3.2 Evaluation Project Results

Teams had about 4 weeks to work on the project, and each team was given two opportunities to submit the report: initial submission and revision/resubmission. After the initial submission, the instructor marked all reports with detailed feedback about how to improve the places that students lost marks, teams had the opportunity to revise and resubmit the report for another round of marking (Please see Appendix B for the marking rubric). The initial marking was 10% of the final grade, and the second round of marking was 5% of the final grade. The scores of the initial marking were from 89.3% to 97.8%. Only one team revised and resubmitted for the second round of the marking, and that team received 100% for the resubmission. Other teams seemed to be ok with the initial scores. This was the first time the instructor used this project, therefore was not sure how the students' submissions would look like. The purpose of giving students chance to revise and resubmit is to reduce students' worry about receiving low scores. Fortunately, to the instructor's relief, all teams' reports were good, with required content, specific screen captures, and detailed explanations. Additionally, all reports were formatted nicely.

4. STUDENTS' REFLECTIONS

4.1 AI USE DISCLOSURE AND REFLECTION

Teams are required to disclose and reflect their AI use by answering the following questions.
Q1. Did you use AI for this project? If you did, which tasks did you use it for?
Q2. Was it useful?
Q3. Did you have to revise the AI output? If yes, why?
Q4. What was your role and AI's in completing these tasks?

ISSN: 2473-4901
v12 n6849

All teams used AI for this project, they used Google Gemini, ChatGPT and Claude, as displayed by Figure 9. The instructor read each team's answers to the AI usage questions, manually summarized the content, and explicitly wrote all text for ChatGPT to generate this figure.

Students used AI for understanding the Shodan search results and technical terms, as displayed by the following comments:

> "*Claude was asked to explain in plain language what a Shodan eol-product tag means, how MongoDB's wire protocol differs from MySQL's, and why a 20-second DNS TTL is significant. This was particularly useful when a team member hit an unfamiliar acronym or protocol detail and did not want to disappear into a long manual read*".

Students used AI to draft individual sections, as displayed by the following quotes:

"*We did use AI to aid in the composition and completeness of the executive summary and conclusion sections*."

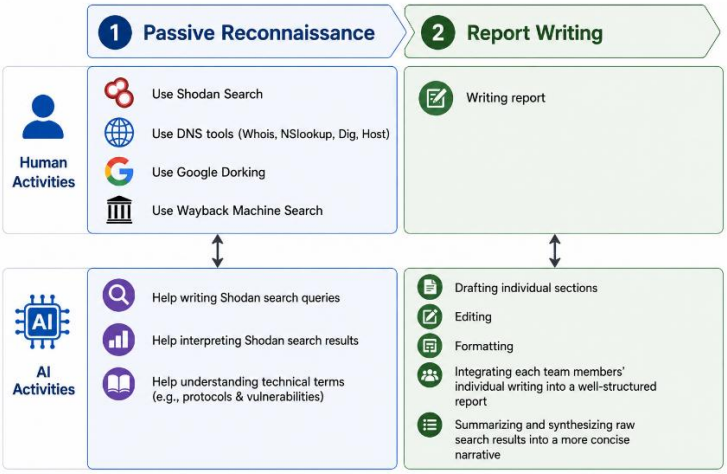

Figure 6. Human-AI Interaction for the Project (Made with ChatGPT)

Teams specified that they revised AI output for accuracy, tone and specificity, and for length and focus as the comments cited below.

> "*We had to revise AI output in three patterns. First, factual checking: when Claude described a CVE or historical incident, we cross-checked details against a primary source (CVE database, vendor advisory, news report) before committing them to the report, and we found a few cases where the AI's phrasing was slightly overstated or conflated related incidents. Second, voice and specificity: AI-generated text tends toward generic, smooth prose, whereas our report is stronger when it uses specific IPs, version numbers, and organizations we observed — we therefore rewrote several paragraphs to put our specific evidence in the foreground. Third, length and focus: the AI's default output is a bit longer than our page budget allowed, so we condensed draft text to the level of detail the assignment and the reader actually need".*

As for the AI' role and human's role in the project completion, team members were the researchers, digging out facts and information by using tools, and AI were used as a tutor to explain concepts, and tools for drafting, editing, and formatting the findings, as displayed by the following quote.

> *"Despite the extensive use of these tools, the team maintained a strict human in the loop protocol to ensure the integrity of the report. Every piece of technical information, including DNS resolution results and revenue figures, underwent a manual verification process against primary sources. Information was cross referenced with SEC filings, official company websites, and direct outputs from technical utilities. This auditing process was essential to correct potential inaccuracies and ensure that the final document complied with all academic constraints. The*

> *team functioned as the final authority on all technical assertions, prioritizing evidence based reasoning and factual accuracy above all else."*

Students' claim of checking information accuracy was verified by the instructor. Teams reported about 40 concrete security incidents, the instructor checked every one of them and found only one mistake about one incident. The incident did exist; the only mistake was that the name of the criminal group involved was not accurately reported by the team. The high accuracy rate of students' report reflected that students were conscious about AI hallucination, and they actively check and verify AI output.

4.2 Reflection about Hacker's Mindset and Skillset

Teams are required to discuss the hacker's mindset and skillset learning in the final report. Some teams write a team's narrative, and some teams have each member of the team write his/her comments and put them in the report. In the literature review, we discussed the security mindset with three processes "*monitoring*," "*investigating*," and "*evaluating*". The monitoring process can be viewed as situational awareness. In the cybersecurity context, it is the situational awareness of the attack surface, such as webcam, industrial control systems, VNCs, and databases. The following comments are about situational awareness.

> "*Working with things like Shodan, DNS lookups, and database analysis showed me how easy it is to find vulnerabilities if systems are not properly secured. It was interesting to see how different types of technologies, like webcams, ICS systems, and VNC services, all have similar issues. Such as weak authentication, misconfigurations, and outdated software*."

> "*The company investigation part helped me understand how much information is publicly available and how it can be used to analyze a company's infrastructure."*

> *"Investigating real-world vulnerabilities was interesting, because it gave a good perspective of what the actual cybersecurity threat landscape looks like*."

The process of investigating involves technical skills about the system configurations and tools of breaking into the system, such as unauthenticated access to a webcam and moving laterally once get into the network to access other parts of the system. When teams examined the root cause of the vulnerabilities, they utilized CVE information. CVE stands for Common Vulnerabilities and Exposures, which is an industry-standard database that acts as a universal dictionary for publicly disclosed cybersecurity flaws in software and hardware. Each discovered security flaw is assigned to a unique tracking number so security professionals and vendors can all refer to the exact same issue using a single name. The CVE Identifier follows a standard naming format: CVE + {Year} + {Sequence Number}. For example, a database vulnerability named MongoBleed was assigned as CVE-2025-14847, and PostgreSQL Zero-Day in BeyondTrust Compromise was assigned as CVE-2025-1094. Two teams mentioned 1 or 2 CVEs in their reports, and the other two teams specified more than a dozen of the CVEs respectively in their reports. The instructor did not require students to link vulnerabilities to specific CVEs, but all teams did so, which indicates that students tried to use the cybersecurity standard databases to understand the technical details and severity of the vulnerabilities.

The process of evaluating is about understanding the possibility of exploitation of the vulnerabilities and the consequences of the exploitation. The following comment illustrates the students' understanding of this. *"Systems that are left open and vulnerable can easily be exploited and can cause real and extreme damage to an organization or even lives."*

One team did a great job in summarizing the hacker's mindset, they specified that the hacker's mindset has three components: the first is to search the attack surface and identify an entry point. "*First is treating every piece of public information as a clue… The mindset is fundamentally about noticing the connection between a piece of evidence and the action it enables…*". Second is to understand the tools. "*Nothing in this project required any single advanced skill — nslookup, dig, whois, and host are first-year networking material; Shodan, the Wayback Machine, and advanced Google operators are all free and self-taught*. *The important skill is knowing which tool to reach for, and in what order, to build a complete picture*". The third is to identify a real target by "*persistence and sampling. The Modbus search in Los Angeles returned 6,659 hosts, most clearly not real industrial equipment. A patient attacker is*

willing to sample, filter out honeypots and scanners, and concentrate on the 1–2% that look like genuine PLCs. The economy favors this behavior: the marginal cost of one extra host is negligible and the payoff for a single real target can be enormous".

Corresponding to the hacker's mindset, the team also specified that "*The defender's mindset has to mirror these observations in three ways: minimize what is visible because every visible detail is a clue; run reconnaissance against your own perimeter because that is the only way to see what attackers see; and design the system so that any single mistake by a developer, sysadmin, or contractor cannot translate directly into ownership of the entire environment*."

This team's reflection illustrates that after the students went through the activities from a hacker's perspective; they gained a more in-depth understanding of defending strategy and techniques.

5. INSTRUCTOR'S REFLECTION AND FUTURE IMPROVEMENTS

There are two limitations for this study. First, there is no formal instrument to measure hacker's mindset quantitatively, therefore, we used students' reflection papers to estimate their learning of hacker's mindset. Second, there were only 15 students in the class; students' reflection papers were primarily by teams, and there were only 4 teams, so the students' feedback may not be as comprehensive as it should be. For related future research, more studies need to be done to define hacker's mindset in the education setting, and to develop instrument to measure hacker's mindset.

When we implement this project the next time, we will change the reflection paper for each student so that we will have a more thorough understanding of students' feedback. As for the project itself, we will improve the project in the following aspects. First, as suggested by one team, the instructor needs to post a Word template for students' final report, which functions as an academic conference submission template. Each individual team member would use this template for his/her own assigned part, and it will be much easier to consolidate the report from each team member. Second, the instructions for reporting the security incidents in the real world need to explicitly require teams to report the major factors such as when the incident occurred, what caused it, the consequences of the incidents, and a citation for each incident. For this term, not every team reported all these factors, therefore, some incidents reports read as incomplete.

6. CONCLUSIONS

Cybersecurity Curricula 2017 explicitly specifies that training adversarial thinking is one of the six foundational concepts for cybersecurity training and emphasizes that all cybersecurity knowledge areas can be taught from "both cyber-defense and cyber-offense perspectives" (Association of Computing Machinery, 2017, p. 21). Echoing this education requirement, Shoemaker et al. (2023) specified that industry is looking for a security mindset when recruiting and trying to cultivate it among their employees. They specified three cognitive processes involved in adopting the cyber offender's perspective: monitoring, investigating, and evaluating. Our project was to answer the call of cultivating the hacker's mindset through surveying a broad attack surface, using a variety of passive reconnaissance techniques and tools, studying the security incidents that happened in the real world, and collecting open-source intelligence (OSINT) for organizations from a hacker's perspective. Through these activities, students gained a deeper understanding of how attackers gather information, identify potential vulnerabilities, and exploit publicly available data during the early stages of a cyberattack. This hands-on experience helps develop critical thinking and practical cybersecurity skills that are essential for both offensive security analysis and defensive risk assessment.

7. REFERENCES

Alabdulatif, A., & Thilakarathne, N.N. (2025), Hacking Exposed: Leveraging Google Dorks, Shodan, and Censys for Cyber Attacks and the Defense Against Them. *Computers* 2025, 14, 24. https://www.mdpi.com/2073-431X/14/1/24.

Alder, S. (2025). U.S. Data Compromises Hit Record Breaches in 2025, https://www.hipaajournal.com/u-s-data-breach-record-2025/

Browne, T. O., & Pardede, E. (2026). A Systematic Review on Adversarial Thinking in Cyber Security Education: Themes and Potential Frameworks. *Computers & Security, https://doi.org/10.1016/j.cose.2025.104803*

Chou, T., & Mohammed, T. (2022). The Role of Ethical Hacking and Penetration Testing in Cybersecurity Education. Paper presented at the 2022 ASEE Annual Conference & Exposition, Minneapolis, MN. June 26 – 29, 2022. American Society for Engineering Education (ASEE). (Paper ID #36857). *https://doi.org/*10.18260/1-2--40754

Association of Computing Machinery (2017), Cybersecurity Curricula 2017, https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

CyberSeek (2025). Cybersecurity Supply/Demand Heat Map, https://www.cyberseek.org/heatmap.html.

Fahid (2025), What Are the CEH Hacking Phases Explained? https://www.ethicalhackinginstitute.com/blog/what-are-the-ceh-hacking-phases-explained?

Federal Bureau of Investigation (2025), FBI Internet Crime Report 2025. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Teaching and Learning Iot Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases. *Sensors*, 20(11), 3048. https://doi.org/10.3390/s20113048

Hamman, S. T., & Hopkinson, K. M. (2016). Teaching Adversarial Thinking for Cybersecurity. *Journal of The Colloquium for Information Systems Security Education*, *4*(1), 19. https://journal.cisse.info/jcisse/article/view/56

Ramezan, C. A. (2023). Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions By Sub-Field. *Journal of Information Systems Education, 34*(1), 94–105. https://aisel.aisnet.org/jise/vol34/iss1/8/, https://doi.org/10.62273/WICW4769.

Schneier, B. (2023). A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back. W. W. Norton & Company. ISBN 978-0393866667

Schoenmakers, K., Greene, D., Stutterheim, S., Lin, H., & Palmer, M. J. (2023). The Security Mindset: Characteristics, Development, and Consequences. *Journal of Cybersecurity*, 9(1), tyad010. https://doi.org/10.1093/cybsec/tyad010

World Economic Forum (2026). New Report Shows How AI Gives Cybersecurity Competitive Advantage, https://www.weforum.org/press/2026/05/new-report-shows-how-ai-gives-cybersecurity-competitive-advantage/

APPENDIX A. Cisco Ethical Hacker Course Modules

Module #	Title and (notes and/or tools)
1	Introduction to Ethical Hacking and Penetration Testing
2	Planning and Scoping a Penetration Testing Assessment (Penetration Test Compliance Standards and Legal, Ethical Framework)
3	Information Gathering and Vulnerability Scanning (Passive reconnaissance tools: • DNS lookups • Advanced search: Google Dork, Shodan, and Wayback machine Active reconnaissance tools: • Nmap, Scapy, Wireshark
4	Social Engineering Attacks (SET & BeEF)
5	Exploiting Wired and Wireless Networks (enum4linux & Ettercap)
6	Exploiting Application-Based Vulnerabilities (Nikto, Greenbone, SQL Injection attack, Password cracking tools)
7	Cloud, Mobile, and IoT Security
8	Performing Post-Exploitation Techniques
9	Reporting and Communication
10	Tools and Code Analysis

ISSN: 2473-4901
v12 n6849

APPENDIX B. Project Report Marking Rubric

Ethical Hacking Project Marking Rubric		
Tasks	**Full Marks**	**Received Marks**
Layout, Format & Style		
Name your document "Proj-Report-TeamX-Initial", replace "X" with your real team number.	0.05	
Title page	0.05	
>Report title (descriptive, not just the word "report")		
>Course number, Team # and all members' name		
>Page # at the bottom		
>Date of submission		
>Number of pages (20-35 pages, excluding references and appendices)	0.05	
Page layout	0.1	
>Margin (1 inch around)		
>Spacing: using 1.0 or 1.5 line of spacing for the body text		
>Using left alignment		
>Reference: use APA style		
Consistency. The entire report should read like made by one person, not from multiple people without final editing.	0.3	
Clear label for each section	0.1	
Content		
Table of contents: only one page, by itself	0.2	
The Executive Summary: only one page, by itself	0.5	
> Summarize the entire report in one page. (A reader should get the key points of your report without reading the rest of the report.)		
>Content: Briefly state the problem, the methods used, the key findings, and the final recommendations.		
>Tone: Concise and result oriented.		
Introduction	0.2	
>Briefly state purpose and report/analysis scope (this is the context or boundary of your analysis)		
Section 1		
>Webcam		
>>screen shot or data about two cities	0.5	
>>security problems and security measures	0.5	
>>one page summary of incidents report with unsecured Webcam	1	
>ICS (chose four of the ICS protocols)		

ISSN: 2473-4901
v12 n6849

>>screen shot or data about two cities	0.5	
>>security problems and security measures	0.5	
>>one page summary of incidents report with ICS	1	
>VNC		
>>screen shot or data about two states	0.5	
>>security problems and security measures	0.5	
>>one page summary of incidents report with VNC	1	
>Databases (3 databases)		
>>screen shot or report of the summary of US	0.5	
>>security problems and security measures (at least three versions)	0.5	
>>one page summary of database incidents report	1	
Section 2		
>Organization 1	1.2	
>Organization 2	1.2	
Marking notes: marking the following item for each organization		
>>Organization inform: location, founding year, products/services, company history milestones (0.2)		
>># of employees, annual revenue (0.2)		
>>DNS related information about the organization (0.2)		
>>use advanced google search to find something above and beyond regular google search (0.4)		
>>Use Wayback machine to dig out some useful information (0.2)		
Discussion of Hacker's Mindset and Skillset	0.5	
Using AI for this project	1	
Total	**13.45**	