




May 2024

Improving Ethics Surrounding Collegiate-Level Hacking Education: Recommended Implementation Plan & Affiliation with Peer-Led Initiatives

Shannon Morgan
University at Albany, SUNY, somorgan@albany.edu

Dr. Sanjay Goel
University at Albany, SUNY, goel@albany.edu

Follow this and additional works at: <https://digitalcommons.usf.edu/mca>

 Part of the [Cognitive Psychology Commons](#), [Cognitive Science Commons](#), [Computer and Systems Architecture Commons](#), [Computer Law Commons](#), [Digital Communications and Networking Commons](#), [Intellectual Property Law Commons](#), [Other Computer Engineering Commons](#), and the [Systems Science Commons](#)

Recommended Citation

Morgan, Shannon and Goel, Dr. Sanjay (2024) "Improving Ethics Surrounding Collegiate-Level Hacking Education: Recommended Implementation Plan & Affiliation with Peer-Led Initiatives," *Military Cyber Affairs*: Vol. 7 : Iss. 1 , Article 8.

Available at: <https://digitalcommons.usf.edu/mca/vol7/iss1/8>

This Article is brought to you for free and open access by the Open Access Journals at Digital Commons @ University of South Florida. It has been accepted for inclusion in *Military Cyber Affairs* by an authorized editor of Digital Commons @ University of South Florida. For more information, please contact digitalcommons@usf.edu.

Improving Ethics Surrounding Collegiate-Level Hacking Education: Recommended Implementation Plan & Affiliation with Peer-Led Initiatives

Cover Page Footnote

This publication was supported by Award Number SA10012022020481 from the Griffis Institute for the VICEROY program. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the sponsor.

Improving Ethics Surrounding Collegiate-Level Hacking Education: A Framework for Building a Comprehensive Implementation Plan

Shannon Morgan and Dr. Sanjay Goel

Introduction

The emergence and subsequent consistent nature of hacking has turned into a widespread concern on a global scale. Hacking can be defined as accessing a system without proper authorization or beyond one's permission and is perpetrated by a vast group of individuals with varying intentions. The main classes of hackers include black hats (malicious intent), white hats (ethical hackers), and grey hats (either malicious or ethical intent, depending on context). During hacking episodes, these individuals modify "computer hardware, software, or the networks to accomplish certain goals which are not aligned with the user goals" (Gupta & Anand, 2015). Both ethical hackers and those with malintent perform similar actions, but the main difference is the intent behind their actions (Hartley et al., 2017). Technological infrastructure and advanced components have allowed a new form of criminality – cybercrime. Hackers can launch attacks using a surplus of strategies, tools, and techniques to violate data confidentiality, integrity, and availability from almost anywhere. Thus, colleges worldwide must educate students about hacking and cybercrime – how they are perpetrated and how to protect against them.

The contrasting classifications between hackers highlight why hacking education on the collegiate level is a moral conundrum. Educators might find themselves simultaneously instructing a potential malicious hacker and a prospective cybersecurity professional. For example, Student A and Student B are both full-time, tuition-paying college students enrolled at the same university. They have an intended major in cybersecurity and are currently juniors in the program. Therefore, they have moved on to upper-level, highly technical courses. Students A and B are learning about Structured Query Language (SQL) Injection Attacks in their Database Security & Forensics course. Using an intentionally vulnerable website, they are performing various forms of SQL Injection attacks and have been able to steal the test data successfully. However, while Student A works on completing the lab report after class for submission, Student B uses SQLiv to find potentially vulnerable websites and then launches SQL injection attacks against them based on what they learned during class. Thus, while one student is utilizing their knowledge to become a future cybersecurity professional, another student of the same status is using their expertise for unethical hacking purposes. This

situation emphasizes the moral quandary presented by incorporating technical hacking training in collegiate coursework.

The purpose of this research study is to analyze the ethical ramifications of hacking education on the collegiate level in relation to cybersecurity majors and minors. Educators and university officials must take action to prevent the misuse of the information, skills, and knowledge gained from being a student in a cyber-related course. With the increasing dependence on technology, it is crucial that future professionals are effectively trained and taught the ins and outs of the field to better protect users from becoming victims of cyberattacks. The outcome of this study is to compile a list of recommendations that build a framework for a comprehensive implementation plan to make hacking education safer in terms of legality and ethics. The provided framework and techniques will aid universities in better navigating the hacking education that cyber students receive throughout their studies.

Literature Review

Past literature explored the concept of collegiate-level hacking education by detailing the pros, cons, and subsequent implications of this matter within the cyber realm. However, it is essential to understand how education with a tech-related major is delivered. According to Regina D. Hartley, there are two main methods of instruction: the theoretical side and the hands-on technical side (Hartley R. D., 2015). However, it is further explained that to have a thorough information security education, students must receive instruction in accordance with both components – not just one or the other. In other words, students must understand the theories explored during hands-on technical labs to get the most out of their education and become effective future professionals. Conversely, this raises the ethical and legal question of whether teaching students how to hack is moral and should be permitted in universities on a global scale. Within this argument, it is mainly the hands-on component that is brought into question, as students are taught methods to conduct hacking episodes along with the software or hardware that aids in launching these attacks.

Patricia Y. Logan and Allen Clarkson discussed the four core issues that arise from students taking part in hacking education while studying within an institution – “appropriate hands-on course content for security and forensics classes, the design and use of security labs, student awareness of ethical behavior in computing, [and] university response to student attacks” (Logan & Clarkson, 2005, p. 158). They concluded that by implementing specific solutions to combat these issues, students can practice their hacking skills more securely, safely, and ethically. Moreover, Mollie Brogdon introduced the importance of a robust university-wide computer security policy that should be implemented and strictly enforced to make students aware of the safety measures and consequences of violations (Brogdon, 2021). The argument states that failing to inform students of

the potential repercussions of wrongfully utilizing their hacking skills outside the classroom would be a disservice to them at such an influential point in their careers.

Being that hacking is consistently occurring to a wide range of victims, “future cybersecurity professionals must have the knowledge and the skills to defend against these cyber-attacks,” and that begins by learning the necessary skills during their courses in college (Wilson, 2017, p. 1). Wilson also further notes that the world of cybersecurity is dynamic, and as these attacks and techniques are altered, so must the profession and education behind the workforce. A lack of understanding regarding how attacks occur and how vulnerabilities are exploited impacts an individual’s ability to devise a plan to protect future systems. Because of this, technical skills are necessary in conjunction with theoretical knowledge. However, it is key to note the risks of this form of teaching, as some students may attempt to use their newfound skills for an unethical or illegal purpose afterward.

Nicole Radziwill et al. explain that students who attempt hacking often initially have innocent intentions. They experiment with the skills they were taught to learn more about computers, modify computer policies, or test their skills in the “real world.” Yet, despite a seemingly harmless motive at first, these actions are dangerous, as no matter what level, hacking is a conscious decision that that violates ethics and is illegal (Radziwill et al., 2015). This idea brings up how often students use what they learn for harm outside of class. In 2014, a study was conducted that released results that of the surveyed students, 82 percent of them tried to repeat a lab activity outside of class, 70 percent confessed they attempted to hack into faculty computers, and 88 percent admitted to trying to “sniff” the university network (Trabelsi & Ibrahim, 2013). This information is a key indicator that despite the preconception that students are just curious and exploring, a large percentage of individuals also perform malicious activity within the university system. Overall, current literature highlights the need for both theoretical and technical education of future cyber security professionals while clarifying why it is a dangerous practice if not strictly monitored.

Methodology

To conduct research related to safer and more ethical collegiate hacking education, meta-synthesis was utilized to perform a “review and integration of findings from [several] qualitative studies” (Lachal et al., 2017, p. 1). As represented in *Figure 1*

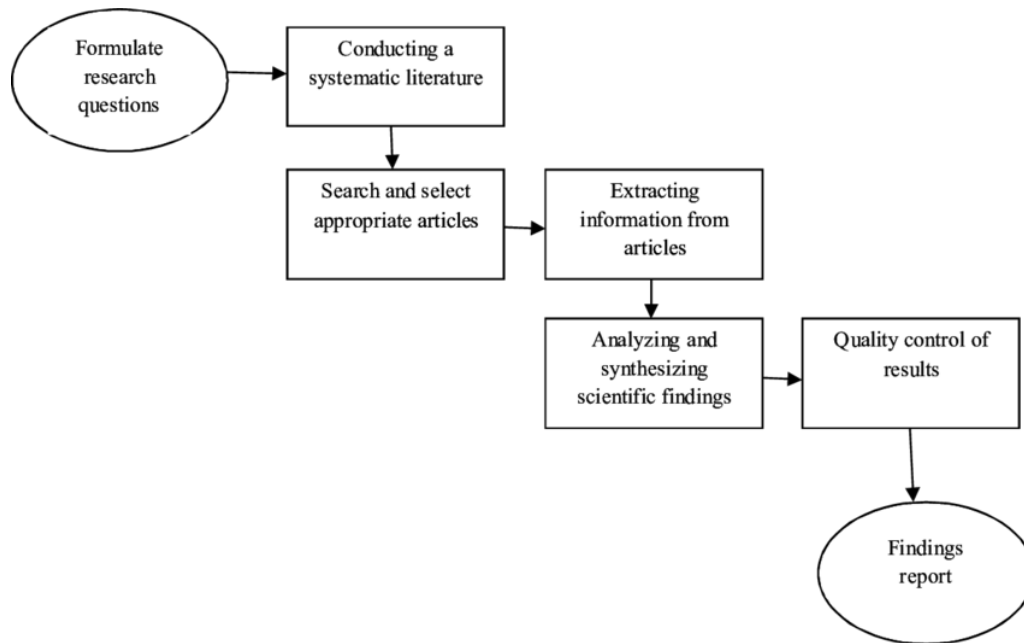


Figure 1: A visual depiction of the processes involved in the meta-synthesis (Arabsorkhi et al., 2014, p. 1901).

below, meta-synthesis generally contains seven steps – formulating research questions, conducting a systematic literature review, searching and selecting appropriate articles, extracting information from articles, analyzing, and synthesizing the findings, performing quality control of the results, and producing a findings report. Meta-synthesis was the selected methodology for this study due to the utilization of previously produced qualitative research papers, which is conducive to the study’s timeline, range of institutions, and background knowledge required to make the anticipated conclusion/contribution.

The research question defined in this study is centered around the ethics of collegiate-level hacking education and, with consideration, how academic institutions can attempt to make their cyber programs more secure. Meta-synthesis is appropriate for this specific study due to its utilization of current literature. While collecting articles, reoccurring discussion points included the different types of hackers, the pros and cons of hacking education, various suggestions for university implementation, and the theoretical and technical components of cyber majors. This paper’s framework will utilize these areas of conversation while also building upon them to provide a cohesive implementation plan to help mitigate the risk of a student becoming an unethical hacker instead of a cybersecurity professional.

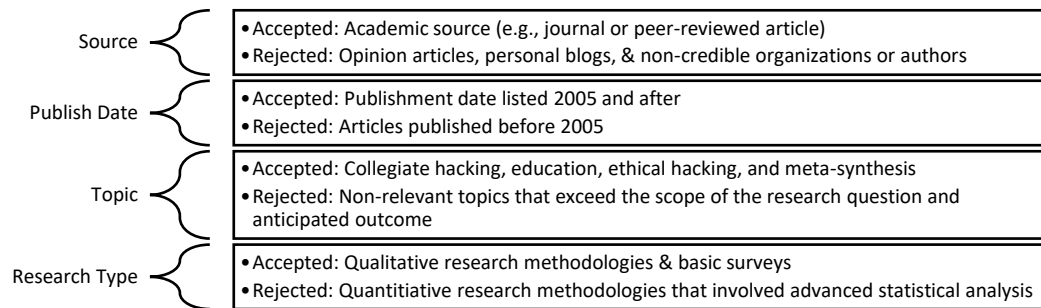


Figure 2: A chart showing the criteria for literature selection or rejection for the meta-synthesis process.

Qualifications for selecting appropriate literature were developed and strictly defined while conducting the meta-synthesis. As depicted in *Figure 2* below, the general criteria areas include the source, publishing date, topics, and research type. The accepted and rejected attributes allow meta-synthesis to be conducted due to the commonalities in the compiled literature. The literature source should be academic rather than one that includes opinion-based or biased ideas. The source of the literature should also originate from a credible organization or outlet to bolster its credibility. The publication date should be listed as 2005 or later to ensure that the information regarding hacking and technology remains relevant and applicable to the present day. The topic of the article should relate to the scope of the research, encompassing areas such as hacking, computing technology ethics, meta-synthesis, and cyber-related education. All other non-relevant literature was rejected to ensure the information utilized was relevant to the issue at hand. Since this paper selected a qualitative approach, the chosen literature should have also used this methodology, yet primary survey data was accepted. Advanced statistical analysis studies were rejected, as the quantitative data presented did not relate to ethics in most cases.

After the completion of this process, there were a total of thirteen articles chosen from a variety of perspectives that would allow for a full, complete, and accurate synthesis of information. While meta-synthesis does require the collection of literature, it also includes the “reconceptualizing of the findings and then [interpreting them] to create new insights, beyond those attained from individual studies” (Chrastina, 2018, p. 114). Developing a new conceptual model based on the proposed research inquiry is crucial, particularly in response to the gaps identified in the current research. Going through the meta-synthesis process after the literature selection allowed the eventual creation of the initially anticipated outcome proposal.

Results

After performing a meta-synthesis on the current research surrounding hacking/technical instruction to cyber-related majors on the collegiate level, a thorough implementation plan was devised to make hacking education safer for all stakeholders involved. To draw accurate results, the existing research was analyzed, the gaps in the study were identified, and then a meta-synthesis was performed to produce the anticipated outcome. As exemplified in the literature review, there was sufficient previous work regarding the need for theoretical and technical instruction, the issues that exist with hacking education, and the need for competent cybersecurity professionals. However, there were not sufficient recommendations for solutions to these matters. Below, *Figure 3* shows five of the

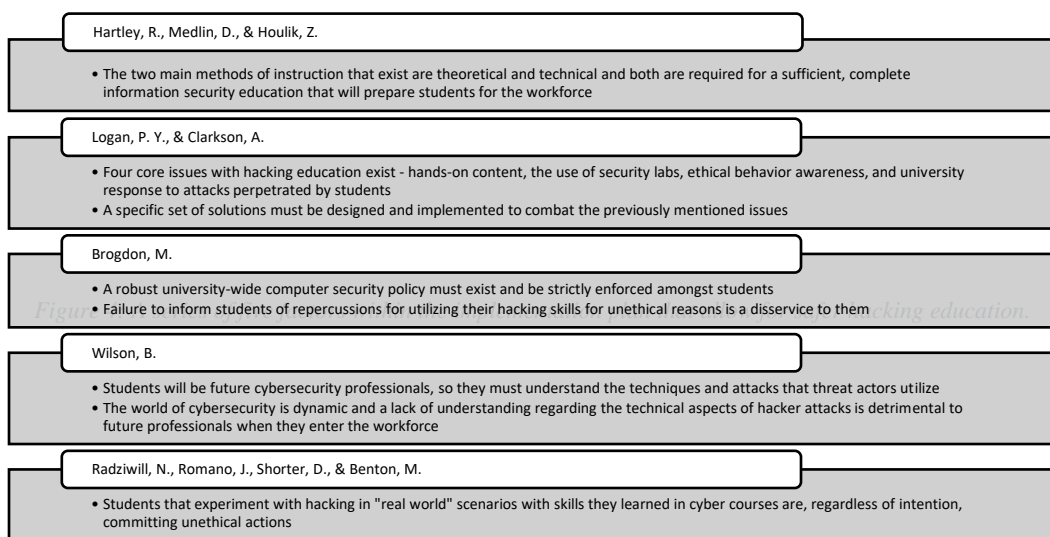
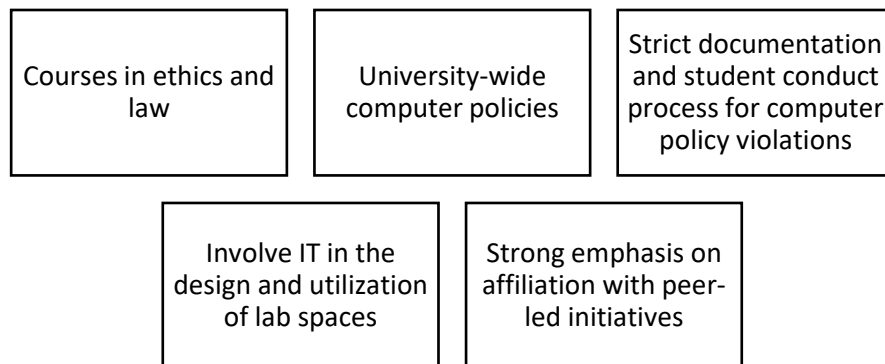


Figure 3: A chart showing five of the thirteen academic publications' conclusions/research results.

thirteen academic publications analyzed as part of meta-synthesis and presented in the literature review.

The proposed implementation plan amalgamated the conclusions and research results of the selected papers to produce the intended outcome. As shown in *Figure 4*, the plan includes extensive courses in ethics and law, university-wide computer policies, strict documentation and student conduct processes for policy violations, the involvement of IT in the design and utilization of lab spaces, and a strong emphasis on affiliation with peer-led initiatives. The proposed implementation plan is designed to be buildable; however, the more enlisted components, the more effective the institution will be at creating a safe environment

for hacking education. It is essential to take note of current institutionalizations prior to implementing the plan.



Discussion

The proposed elements within the implementation plan dictate crucial steps in creating an ethical way of instructing cyber-related technical skills on a collegiate level. The first factor highlights that courses in ethics and law should be given to students at multiple course levels (e.g., 100, 200, 300, or 400). As a whole, “universities should never assume that students learn ethical behavior [or] the laws on illegal network/computer access” before they begin attending the university (Logan & Clarkson, 2005, p. 160). It is crucial to build knowledge of cyber ethics not only as a freshman or sophomore but also as a junior and senior while students learn the technical components of their major. Therefore, the university must require that students take some combination of the various levels of ethics courses in their academic plan to graduate. Having students learn ethics throughout their college career will give them a strong foundation on what is considered “right or wrong” within cyberspace.

The institution should also take the initiative to develop and institutionalize a university-wide computer policy. This in-depth document should include acceptable computer usage behavior expected of the students. It may contain certain unacceptable activities outside the classroom, such as sniffing the university network. During the formation of these guidelines and policies, multiple university-affiliated departments should contribute to the drafting and finalization process (e.g., Dean of Students, cyber department, ITS, legal team, etc.) since there needs to be a wide range of perspectives and considerations incorporated within the document. To ensure students are aware of the policy, it should be reviewed in the previously discussed ethical courses beginning in the student’s first year. The university should also consider whether cyber-related students who consistently use computer workstations should be required to sign a document that outlines the university’s computer policies. By doing so, they would agree to abide by it, and if there is a case where it is abused later, the college can refer to the signed “contract” that was previously agreed to.

This factor directly relates to the next part of the plan, which is to clearly outline a strict documentation and student conduct process for those who choose to violate the university computer policy. It is essential that students not only understand the computer policy but also understand what will happen if they decide to breach it. However, when the university creates the computer policy document, it is necessary that they strictly enforce it; otherwise, its true purpose – to deter students from misusing university digital assets – will not be ensured. Students should also be advised that as a cyber major, having a documented breach of the computer policy at an influential point in their cyber career is a risk to their future job security.

The university's Information Technology Services (ITS) team should be involved with the cyber lab design and utilization. A robust communication network between the cyber department(s) and ITS is essential to effectively discuss the lab's required capabilities and the activities it should support. Considerations must be made to utilizing a network isolated from the main university internet, as if penetration testing is being run against the network connected to others, it could pose a possible security risk. Students should also be granted the proper rights and administrative privileges required to perform the labs. Actions requiring advanced privileges may include downloading software or running an application as an administrator. Moreover, the cyber department should maintain close oversight throughout the academic year to ensure it remains aware of technical labs conducted within the room. This is useful to ensure that the lab spaces are correctly configured and that ITS can look out for unusual network traffic that could be a sign of students attempting to use their technical skills outside of the controlled environment.

The final component of the implementation plan is a strong emphasis on affiliation with peer-led initiatives. A thorough "participation in the community and adherence to community standards develops a hacker's own ethical standings" (Brogdon, 2021, p. 2). For students specifically, involvement in community-related initiatives can help strengthen their foundational understanding of ethics and, thus, prevent them from future misconduct. However, it depends on the specific group's mission, as group affiliation and teamwork are evident on both sides of the cybersecurity field (white-hat and black-hat hackers (Pashel, 2006). Especially in cyber competitions (e.g., Capture the Flags), when students immerse themselves in a competitive, yet ethical, situation to practice their skills, they may shy away from using their skills for harm or in an unapproved manner. Examples of these "peer-led organizations" can range in their goal (e.g., promoting women in cyber or hosting cyber professional guest speakers). Still, the intended purpose of the organization must be ethical in nature. Not only will the peer group strongly influence the individual themselves, but also their categorizations for what constitutes a moral or immoral action. It is important to consider that "group affiliation and teamwork is evident on both sides of the cybersecurity field (white-hat and black-hat hackers)" (Pike, 2013). For example, if a student were to join an online group that teaches others how to join forums on the dark web that contain

illegal content, that should not be encouraged. Although the organization is cyber-related, they should not affiliate themselves with it, as this would likely be an example of a black-hat-related group.

Universities should encourage experiential learning opportunities with peer-related organizations and have their own organizations on campus that are available for students to join. For example, the VICOR (Virtual Institute of Cyber Operation and Research) Program hosted at SUNY University at Albany, located in upstate New York, funded by the Griffiss Institute, aims to train future cyber professionals for military or civilian roles. Funded by the Department of Defense, the program offers participants scholarships for training, experiential learning, networking, and research opportunities to further their education. By allowing students to receive extensive mentoring and additional professional development opportunities, programs like this help shape cyber students into ethically sound future professionals. To organizations like the Department of Defense, having a pool of potential candidates who possess ethical standards and theoretical knowledge, and technical skills is highly advantageous to their mission of protecting the country. Overall, the university should strongly emphasize not only having cyber organizations on campus but also encouraging students to attend meetings and become part of the community.

The relevance of the plan stems from the sheer number of stakeholders impacted by the ethical problem consideration and the existence of cybercrime. The groups involved span those linked to the institution (e.g., students, professors, university officials, IT staff, etc.) and the professionals, users, and businesses that have a stake in the cyber realm. The potential for future research includes applying the implementation plan to a specific university. Consideration should be given to the university's current setup, how closely the elements are utilized, the implementation of the plan, and the after impacts. The methodology should be tested to see if the students felt more or less likely to use their technical knowledge for only ethical purposes after the execution.

Conclusion

The need for future cyber security professionals in the workforce due to the existence of cybercriminals highlights the evident nature of cyber-related majors in universities. Graduates from these programs must possess the conceptual and technical skills necessary to combat this evolving type of criminal that no longer needs to leave their residence to commit a crime. However, the concern exists that cyber students can utilize the skills they learn during their coursework for harm rather than for ethical reasons. Because of this, universities must take the necessary steps to try and mitigate this moral and legal risk. Using meta-synthesis, relevant literature was collected to create an implementation plan that would still allow for technical labs and exercises but in a safer manner. These factors included the creation of required multi-level courses in ethics and law, university-wide computer policies and their strict enforcement, involving information technology

services within the lab design and use to prevent possible security risks, and the emphasis on peer groups with cyber affiliations.

About the Authors

Shannon Morgan

Shannon Morgan is a senior at SUNY University at Albany studying Digital Forensics and Informatics. Shannon has worked for the Big 4 accounting firm, PricewaterhouseCoopers, as an Investigations & Forensics Intern and will be continuing her work there as a Legal Managed Services Intern conducting digital forensic acquisitions. Furthermore, she is a research fellow at the Virtual Institute of Cyber Operation and Research (VICOR) where she has contributed to projects dealing with collegiate hacking education and active defense systems.

Dr. Sanjay Goel

Dr. Sanjay Goel is a professor and chair within SUNY University at Albany's School of Business for the Information Security and Digital Forensics department. He is also the Director of Research at the New York State Center for Information Forensics and Assurance at the University. He received his M.S. in Mechanical Engineering from Rutgers University and Ph.D. in Mechanical Engineering from Rensselaer Polytechnic Institute.

Acknowledgment

This publication was supported by Award Number SA10012022020481 from the Griffis Institute for the VICEROY program. Its contents are solely the authors' responsibility and do not necessarily represent the official views of the sponsor.

References

- Arabsorkhi, A., Khodabandeh, A., & Tashakori, L. (2014). A framework for the formulation of security issues in the field of e-learning using meta-synthesis method. *Management Science Letters*, 4(9), 1899-1906.
<https://doi.org/10.5267/j.msl.2014.8.037>
- Brogdon, M. (2021). Ethical hacking. *Culture, Society, and Praxis*, 13(4).
- Chrastina, J. (2018). Meta-synthesis of qualitative studies: Background, methodology, and applications. *NODSCI International Conference*. Finland.
<https://eric.ed.gov/?id=ED603222>

- Gupta, A., & Anand, A. (2015). Ethical hacking and hacking attacks. *International Journal of Engineering and Computer Science*, 6(4), 21042-21050. <https://doi.org/10.18535/ijecs/v6i4.42>
- Hartley, R. D. (2015). An ethical hacking pedagogy: An analysis and overview of teaching students to hack. *Journal of International Technology and Information Management*, 24(4). <https://doi.org/https://doi.org/10.58729/1941-6679.1055>
- Hartley, R., Medlin, D., & Houlik, Z. (2017). Ethical hacking: Educating future cybersecurity professionals. *Proceedings of the EDSIG Conference*. Austin: Information Systems & Computing Academic Professionals. <http://proc.iscap.info/2017/pdf/4341.pdf>
- Lachal, J., Revah-Levy, A., Orri, M., & Moro, M. R. (2017). Metasynthesis: An original method to synthesize qualitative literature in psychiatry. *Frontiers in Psychology*, 8. <https://doi.org/https://doi.org/10.3389/fpsy.2017.00269>
- Logan, P. Y., & Clarkson, A. (2005). Teaching students to hack: Curriculum issues in information security. *ACM SIGCSE Bulletin*, 37(1). <https://doi.org/https://doi.org/10.1145/1047124.1047405>
- Pashel, B. A. (2006). Teaching students to hack: Ethical implications in teaching students to hack at the university level. *InfoSecCD*. <https://doi.org/https://doi.org/10.1145/1231047.1231088>
- Pike, R. E. (2013). The "ethics" of teaching ethical hacking. *Journal of International Technology and Information Management*, 22(4).
- Radziwill, N., Romano, J., Shorter, D., & Benton, M. (2015). The ethics of hacking: Should it be taught? *Software Quality Professional*, 18(1), 11-15. <https://doi.org/https://doi.org/10.48550/arXiv.1512.02707>
- Trabelsi, Z., & Ibrahim, W. (2013). Teaching ethical hacking in informational security curriculum: A case study. *IEEE Global Engineering Education Conference (EDUCON)*. Berlin: IEEE. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6530097>
- Wilson, B. (2017). *Teaching security defense through web-based hacking at the undergraduate level*. George Fox University Department of Electrical Engineering and Computer Science.