To Teach to Hack or Not: the Grey Zone of Cybersecurity Education

Aleksandra Pawlicka
ITTI, Poznań, Poland,
and University of Warsaw,
Warsaw, Poland

Marek Pawlicki
ITTI, Poznań, Poland,
and Bydgoszcz University of Science and Technology,
Bydgoszcz, Poland

Rafał Kozik
ITTI, Poznań, Poland,
and Bydgoszcz University of Science and Technology,
Bydgoszcz, Poland

Michał Choraś
ITTI, Poznań, Poland,
and Bydgoszcz University of Science and Technology,
Bydgoszcz, Poland

Abstract

This paper explores the controversial role of hacker education in ethical hacking and its impact on enhancing cybersecurity. It discussed the nature and necessity of the "white-hat" hacking, examining the potential benefits and inherent risks associated with teaching hacking skills. The discussion covers the qualifications necessary to become an ethical hacker and proposes guidelines for responsible education in this field, emphasizing the importance of ethical and legal boundaries. Ultimately, the paper advocates for integrating hacking skills into educational curricula, arguing that, despite potential risks, ethical hackers are crucial for proactive cybersecurity strategies.

Keywords: cybersecurity, education, ethical hacking, ethics, hacker education

1. INTRODUCTION

In today's fast-changing digital world, the practice of ethical hacking has become very important, providing a fresh view on how to protect against cyber threats. Yet, the question of whether hacking is a skillset which ought to be taught or not sparks heating debates among researchers and cybersecurity experts. Thus, this paper aims to discuss this matter. It begins by defining ethical hacking and then discusses how it should be approached in order to ensure it is legal and helpful. The benefits that ethical hackers offer to organizations, making their digital spaces safer, are also looked at. Additionally, the authors consider who can become an ethical hacker. Then, the complex questions around teaching hacking skills are presented. The paper also suggests setting out a set of guidelines for teaching ethical hacking, aiming for a responsible approach that highlights the importance of ethics. Ending with a summary of the main points, this study adds to the conversation about ethical hacking, pushing for practices that are both informed and principled in the field of cybersecurity.

2. WHAT EXACTLY IS ETHICAL HACKING?

In the cybersecurity domain, hackers are often categorized by the color of their "hats" to distinguish their intentions and methodologies, the distinction dating back to the monochromatic spaghetti westerns, where the heroes wore white hats, whilst villains sported black-colored headgear (Townsend, n.d.). By this token, the useful, ethical hackers are called "White Hats", with the malicious ones dubbed "Black Hats".

The main differences between ethical and black-hat hacking are that the White Hats cooperate with organizations in a legal manner and report the potential security gaps back to their clients. On top of that, ethical hacking helps the organization come up with solutions and recommendations regarding their security flaws. Ideally, ethical hackers may help solve the security issues of the client (Okta, 2022).

Although White Hats do compromise systems and networks, it happens only within the set rules of engagement, and with the permission of the target (Dalalana Bertoglio & Zorzo, 2017). This way they are able to identify security flaws which could otherwise result in a data leak. The identified weak points are then reported to the organization that employed the hacker; the hacker may also be asked to advise the employers how to solve the issue (Goswami, 2021).

Jena discusses an alternative way of distinguishing between White and Black Hats. They say that there are four factors that hackers can be differentiated by, the first one being their motives. In the case of Black Hats, they hack with malicious intent (Pawlicka et al., 2021); whilst for White Hats, their motive is either seeking to eliminate vulnerabilities or by the goal of simply stopping Black Hats. This is the most significant factor. Besides this, they differ in the techniques they apply – White Hats tend to replicate the ones used by Black Hats, in order to uncover how the attack occurred or might occur. Then, there is legality – of the two groups, only the actions of White Hats are legally acceptable. Lastly, as far ownership is concerned, unlike Black Hats, who neither own the networks or systems nor work for their owner, White Hats are employed to test systems and networks by the rightful owners (Jena, 2022).

It is important to mention that some researchers believe that somewhere between the hackers belonging to either Black or White Hats, there are the so-called Grey Hats, that is hackers who do not obtain permission before accessing a system. This makes their actions illegal; however, unlike Black Hats, they usually do not hack with malicious intent . Rather, they access systems and networks for fun, as a challenge

or for other reasons; they sometimes let the owner of a system of the found vulnerabilities, too (Jena, 2022; Townsend, n.d.).

Besides this black and white (or rather, grayscale) division, some researchers also distinguish hackers of other hat colors, such as:

- **Green Hats** – would-be hackers, or hackers on the make; may lack advanced technical skills or education but are eager to learn (Kranz et al., n.d.; Okta, 2022)
- **Blue Hats** – this term may be imprecise, as it is used to refer to a number of different entities; it usually means either someone engaged in the Blue Teams (cybersecurity specialists tasked with defending the networks and systems), a professional contracted to find security gaps, someone invited to the BlueHat conference organized by Microsoft, or someone who hacks as a means of retaliation (Kranz et al., n.d.; Okta, 2022)
- **Red Hats** – this name refers to a number of different hackers, too – usually either to the members of the Red Teams, i.e., cybersecurity specialists posing as cyberattackers in a controlled environment, or the vigilante hackers who crack (usually Linux-based) systems in order to cripple the black hats, by destroying their resources (Coursera, 2022; Kranz et al., n.d.; Okta, 2022).

In the context of the Red Team/Blue Team division, one may also distinguish the so-called Purple Hats – the members of Purple Teams, who bring blue and red together and coordinate their actions (Coursera, 2022).

Nevertheless, although there may exist various colors and shades of "hats", when talking about the "good", acceptable hackers and the ones who break the law, only the white- and black-hat hackers are usually mentioned. While it may not be certain which came first, the malicious hackers or their benign counterparts, it has been argued that one type begets the other and that they could not exist without each other (Banda et al., 2019).

Lastly, once the differences between the "good" and the "bad" hackers have been outlined, it is worth comparing ethical hackers with cybersecurity professionals on the whole. Sometimes the two terms are used interchangeably, yet they do differ in certain ways. The main goals of those two groups align – they strive to make systems and data secure. However, cybersecurity is a broader, more general field, encompassing network and data security, digital forensics, and many more. Ethical hacking should also be perceived as a field of cybersecurity, so it is *de facto* its subdiscipline. The other popular way of making the distinction between cybersecurity and ethical hacking is by the measures each of them takes; cybersecurity is generally concerned with protecting and defending whilst ethical hackers employ offensive tools and methods (InteliPaat, 2022).

On the other hand, ethical hacking is sometimes called penetration testing; this also needs clarifying. Penetration testing (or simply "pentesting") is a term referring to the controlled trial in order to penetrate into a system and the measure taken to rid the identified security vulnerabilities (Dalalana Bertoglio & Zorzo, 2017). So, penetration testing is in fact what ethical hacking does, but the terms are not fully interchangeable, with ethical hacking being the more general one (CompTIA, n.d.).

2.1.How to hack ethically?

If done right, ethical hacking helps strengthen the security of the information system of an organization, assess the organizations' overall cybersecurity, identify

vulnerabilities and anticipate unforeseen attacks (Iberdola, n.d.).

Okta mentions five phases that ethical hacking usually follows in order to test a network or a system:

- **Reconnaissance:** when the data about a system is collected, be it through active or passive footprinting, or both. By active footprinting one understands a process of employing network scanning tools to gather the information on the system; passive footprinting includes all the data gathering, which is not performed in a direct way, for example by browsing the organization's social media or any information available on the Internet.
- **Scanning:** tools like dialers, network mappers, port scanners, sweepers, vulnerability scanners, and so on, are used to scan the system for security gaps. In other words, in this phase, the simplest ways to access the target system/network are explored.
- **Gaining access:** the data collected in the previous phases as well as all the necessary means are used here to gain unauthorized access to the target systems, applications or networks. This phase is considered to be the actual hacking phase, or "owning the system".
- **Zombie system:** once the access has been gained, the hacker proceeds to simulate any malicious activity that a black-hat hacker would engage in at this point, such as installing malicious software, launching an attack, stealing data, etc. They also aim at maintaining access as long as possible, without the target becoming aware of it. The system becomes a "zombie system" when it has been changed so that legitimate users or personnel are no longer able to access it.
- **Evidence removal**: the phase of clearing the hacker's tracks and any other data which could serve as evidence of their being in the system, ideally without losing the connection to the system (Okta, 2022).

The whole process may also involve a consecutive re-test, in order to assess if the security gaps have been addressed. It should be noted that ideally, the ethical hackers who test a given system should not possess any prior knowledge of it besides what they are told; this should contribute to the evaluation being more objective (Goswami, 2021).

In their work, Jena emphasizes which principles hacking has to be underlain by in order to classify as ethical:

- Gaining complete approval prior to performing any testing
- Determining the scope of assessment, making the organization aware of the plan
- Reporting any vulnerabilities found in a system
- Keeping what has been found confidential, respecting any non-disclosure agreements
- Removing all the traces of the hack after the assignment has been completed, in order to prevent any potential hackers from accessing the network or application through the identified gaps (Jena, 2022).

Beniwal and Sneha add that obeying the ethical hacking commandments should be accompanied by working in an ethical way, i.e., based on high professional morals, in a transparent way that has been approved by the company beforehand, so as to remain trustworthy, respecting privacy and data confidentiality at all stages of the test (Choraś et al., 2024), choosing the right tools for the task, in order not to crash the tested system, and sticking to the plan (Beniwal & Sneha, 2015).

2.2. Advantages of employing ethical hackers

Ethical hackers have been called the "great ally" of cybersecurity (Iberdola, n.d.), and their services "the need of the hour" (Goswami, 2021). Undoubtedly, employing this kind of specialist brings benefits to businesses, organizations and individuals alike. The most significant advantages include:

- Keeping the data "out of hostile hands"
- Improving the security of networks
- Helping to avoid breaches
- Detecting the possible security gaps and vulnerabilities,
- Being able to come up with suggestions on how to solve the found issues
- Protecting the customer products and information, which translates into an increased trust of customers
- Being able to see a system like a hacker and put themselves into the attackers' shoes, i.e., use the malicious actors' point of view to their advantage
- Being the only cybersecurity actors able to play a more offensive role.
- Being able to patch any possible gaps before an attack happens
- Helping protect a country from cyber-terrorists (Beniwal & Sneha, 2015; Goswami, 2021; Yerak, 2014).

Other, less obvious benefits of ethical hackers are that they greatly reduce computer system downtime, help rule out industrial espionage, and contribute to protecting the integrity of the data an organization collects. Lastly, they help raise the awareness of cybersecurity, both on the general level and at the level of the organization they work for (Coursera, 2022; Iberdola, n.d.; Ramalingam, 2019).

A number of scientists have pondered upon the dilemma of whether cybersecurity actions should be more offensive or defensive in nature. They point out that at the very root, cybersecurity actions mostly encompass reacting to the threats, for example by making the effort to detect and rid of viruses and other kinds of malicious software, and protecting access to networks and systems. They ask whether, in the context of the ever-evolving threat landscape, the actions of cybersecurity experts should become more proactive. This is why ethical hackers, who are the only way cybersecurity can switch to the offensive, play such an important role in the ecosystem ("Offense or Defense? An Ethical Hacker's Approach to Cybersecurity," n.d.).

In this vein, Kost argues that crucial data can be protected in the most optimal way only if there is cooperation between cybersecurity professionals and ethical hackers. In order to make this clearer, they describe the experts as the architects of the systems, whilst the hackers play the roles of the quality control team. The former identifies security risks pertaining to a system and develops strategies for security control. In turn, the latter search for potential vulnerabilities and access points. The cybersecurity team addresses the identified loopholes; the White Hats attempt to break into the updated system, and so the cycle continues. The ultimate goal is to secure the system to such a degree that the hackers are unable to exploit any gaps thereof (Kost, 2022).

The author also notices that this ideal model is not always followed in organizations; in contrast, the ones who do acknowledge the significant role of ethical hackers do not employ them as a regular part of their staff working for the company on a daily basis; rather, they commission them to perform occasional penetration testing. In such a case, it is especially important to perform such tests after any major updates and changes to the system, both at the technology and application levels (Kost, 2022).

2.3. Who can become an ethical hacker?

According to a study, one usually begins hacking at school, due to boredom or the need to compete. The researchers emphasize the fact that people usually start without malicious intentions, but they are encouraged to push the boundaries further if they are not caught or disciplined (Xu et al., 2013). Sometimes they may just not be aware of the fact that what they are doing is against the law, especially if they are unaware of the social context (Adams, 2019).

On the other hand, HackerOne, a platform designed to match organizations and ethical hackers, claims to congregate over a million hackers from all over the world; amongst them, there mainly are young individuals who have been around computers all their lives, both for school, work and entertainment (Murphy, 2022).

Besides a solid foundation in information sciences, a person who wishes to engage in professional ethical hacking should be knowledgeable in the theoretical concepts of hacking, and be able to hack into various systems and networks. Their tasks include reacting to cyberattacks, so they also have to be able to perform all kinds of proper countermeasures to them (Okta, 2022).

In addition to this, the desirable skillset one should possess if one wishes to become an ethical hacker includes:

- In-depth, strong and working knowledge regarding relevant systems, networks, security measures, security protocols, attacks, evasion tactics and countermeasures, etc.
- Programming skills, preferably in multiple coding languages, such as Java, C and C++, Python, SQL, and PHP
- Understanding of databases
- Knowledge of platforms/operating systems
- The ability to employ the various available hacking tools
- Knowledge of search engines and servers (Jena, 2022).

Career-wise, the specific paths an ethical hacker may follow include:

- penetration tester
- network defender
- security analyst
- vulnerability assessor
- security consultant
- information security manager
- quality assurance tester
- certified ethical hacker (CEH) (Jena, 2022; Okta, 2022).

Thus, while the journey to becoming an ethical hacker may begin with a simple curiosity or a competitive spirit, it evolves into a profession demanding a comprehensive skill set, a deep understanding of cybersecurity principles, and a commitment to legal and ethical conduct in safeguarding digital spaces. This brings one to the ensuing discussion. Having analyzed the concept of ethical hacking, it emerges as a multifaceted discipline encompassing an array of benefits, reinforcing its indispensability in the contemporary cyberspace. Yet there are a number of ethical dilemmas surrounding the education of hacking practices, and an ongoing debate on the ethical implications of teaching people how to hack. In other words, experts and researchers wonder if people should even be taught to hack, and if so, under what guidelines and moral considerations (Hartley et al., 2017). The following section discusses the possible pros and cons of hacker education.

3. DILEMMAS IN ETHICAL HACKING EDUCATION: YES OR NO?

On the one hand, experts argue that equipping students with hacking skills may

contribute to worsening the issue with malicious hackers, that is, that the students, equipped with the same knowledge that the Black Hats possess, will start behaving like ones. This dilemma especially concerns teaching people hands-on teaching methods, which may tempt them to apply the tools in "an irresponsible manner" (Hartley et al., 2017; Trabelsi, 2011). Jamil et al. go even further, and compare equipping students with hacking knowledge to trusting them "with a loaded gun" (Jamil & Ali Khan, 2011). A crucial concern is whether students have the necessary foundational knowledge and maturity at such an early stage to grasp the ethical complexities of hacking. The fear is that students, influenced by the glamorous depiction of hacking in media, might form incorrect ideas about what constitutes ethical behavior in cybersecurity. As Ramezanifarkhani puts it, "Instead of promoting genuine ethical hacking, the course could end up encouraging a risky hacking mindset, and embolden them, resulting in unforeseen risks in the future" (Ramezanifarkhani, 2023b). Studies have indeed shown that students, especially the younger ones, may not be able to be entrusted with the hacking tools and techniques, as they may still lack in both proper maturity and ethical reasoning (Radziwill et al., 2015).

A considerable number of scientists seem to agree that as long as the students and participants of hacking courses are not told about the ethical and legal consequences of their actions, as well as about what is expected of them once they engage in these activities, it may turn out that future hackers are being trained alongside security professionals (Hartley et al., 2017; Logan & Clarkson, 2005; Pashel, 2006; Patil et al., 2017; Radziwill et al., 2015). This concern highlights the importance of a thoughtful approach in designing the curriculum, ensuring that students understand the ethical implications and the responsibilities they bear in the field of cybersecurity (Ramezanifarkhani, 2023b). The author also points it out that equipping more and more people with the "hacking mindset" is likely to adversely influence the behavior and actions of at least some of the students (Ramezanifarkhani, 2023a).

In this context, the aforementioned distinction between "ethical hacking" and "penetration testing" also becomes critical. Ramezanifarkhani claims that although both of the aim at identifying vulnerabilities within systems, their foundational philosophies and approaches vary significantly. Ethical hacking encompasses a wider array of activities, often resulting in ethical dilemmas, as opposed to penetration testing, which adopts a more focused and objective-driven methodology. This methodology aims at pinpointing and mitigating specific vulnerabilities, potentially offering a more straightforward and ethically unambiguous pathway for student engagement with cybersecurity. As explained by the author though, there are students who believe penetration testing is thus "less cool". Such thinking is what ought never to be fostered within the context of the educational system; just the opposite, it is the penetration testing career path that should be taught, not the hacking one (Ramezanifarkhani, 2023b).

Certainly, Hartley et al. have presented a number of cases where students of an ethical hacking course used the newly acquired skills "outside the classroom", for example by attacking the faculty computers right after experimenting with the DoS attacks, trying to break into the university computers (admitted to by 70% of the surveyed students), or sniffing the university traffic (as indicated by the overwhelming 88% of the studied hackers in the making) (Hartley et al., 2017; Trabelsi & McCoey, 2016). Another study confirmed that 85% of the students tried the newly acquired hacking skills outside the isolated laboratory equipment; 89% of them claimed it was only "for fun", though (Trabelsi & McCoey, 2016).

This all also raises the question of accountability for malicious hacking, if the hacker was given the knowledge of how to do it by a school, i.e., the concern of whether the institutions, or even individual teachers and instructors that teach hacking techniques, may face ethical and even legal repercussions (Hartley et al., 2017; Radziwill et al., 2015).

There are also critics who argue that courses on ethical hacking might not sufficiently prepare students for the complex realities of cybersecurity. These courses are often accused of merely scratching the surface, failing to provide a deep and thorough understanding of the field (Crowly, n.d.). This criticism extends to the broader educational strategy within IT, where a foundational knowledge of computer systems, programming, and network infrastructure is seen as essential before engaging in cybersecurity.

This viewpoint suggests that achieving proficiency in cybersecurity, similar to mastering any complex discipline, requires an in-depth and comprehensive understanding of fundamental principles and systems, and hacking is not "something that can easily be learned out from a text book and a course" (Crowly, n.d.). Such mastery enables the kind of innovative problem-solving and system manipulation characteristic of skilled cybersecurity professionals. Thus, the journey to becoming a proficient hacker, ethical or otherwise, is viewed not as a shortcut through specific courses but as a long-term dedication to understanding the complexity of computer systems and networks (Crowly, n.d.). In other words, this viewpoint suggest that learning how to hack, especially through a course, is simply a waste of time.

However, acknowledging the benefits of ethical hacking, it is necessary to recognize its role in enhancing cybersecurity strategies and that ethical hacking serves not only as a tool for identifying vulnerabilities but also as an educational catalyst that empowers IT professionals with a proactive approach to security. A number of researchers and experts in the field have voiced their opinions in favor of teaching and learning how to hack at schools.

Primarily, learning about ethical hacking greatly increases awareness about cyber security. It helps people understand the weak spots in computer systems and networks. This knowledge makes it easier to discover and prevent security problems, helping to keep both personal and organizational data safe from unauthorized access (Sinha, 2023).

In addition, ethical hacking is leading the way in cybersecurity careers, driven by a growing need for experts who can deal with online security challenges. By gaining skills in ethical hacking, individuals can move into well-paying jobs like ethical hacker, penetration tester, security analyst, or consultant. These opportunities are supported by a strong job market (Sabharwal, 2023; Sinha, 2023).

Ethical hacking is key for organizations looking to improve their system security. It is about actively searching for and fixing security weaknesses. This not only strengthens security but also helps organizations get ready to deal with cyberthreats. Ethical hacking is a core part of a thorough cybersecurity plan, giving professionals the skills needed to create strong defenses and take proactive steps to protect against attacks. In addition to this, the philosophy behind ethical hacking is about using technology responsibly. It stresses the importance of following legal and ethical rules, helping to build a sense of honesty and integrity in the cybersecurity world (Sinha, 2023).

On top of that, getting into the mindset of a hacker is crucial for protecting networks from cyberthreats. This understanding helps cybersecurity experts to focus on and reduce

the risk of attacks, making sure resources are used effectively to defend networks. Ethical hacking also reveals hidden methods and pushes for the adoption of better security measures, playing a significant role in the development and quality assurance of software. This knowledge speeds up the fixing of security gaps, following the best practices in the industry to lower security risks (Sabharwal, 2023). Lastly, from a financial standpoint, ethical hacking offers good salaries due to the high demand and limited supply of cyber security professionals. With cyber-attacks increasing worldwide, there is a big need for ethical hackers. This opens up many chances for them to work in different sectors or start their own businesses, showing the broad potential of a career in this field (Sabharwal, 2023).

The ones against teaching ethical hacking worry that once students learn to hack, they will eventually turn to the "dark side". However, although this may sound very alarming, studies have shown that the majority of hackers do not have malicious intentions right from the beginning; they are driven by curiosity, a sense of competition or by such innocent motives as the desire to play games on school computers (Radziwill et al., 2015; Xu et al., 2013).

In addition to this, the ones advocating for teaching how to hack believe that hackers will exist no matter if students are taught hacking or not; if they are not taught at schools, they will be self-taught. This in turn means that they will have the skills but no proper ethical training. If schools do teach students how to hack, they are able to promote hacking in an ethical and legal way, which should prevent at least some students from putting black hats on. It has also been argued that the only way for students to be able to identify intruders and cope with them is to adopt their viewpoint, i.e., the "attacker's approach" (Radziwill et al., 2015). Some go even further, suggesting that it is impossible to develop proper defense mechanisms without experiencing attacks first-hand (Trabelsi, 2011). Hartley et al. add that only when at school, future hackers can safely perform their actions in a controlled environment, without malicious intentions, after obtaining the target's consent (Hartley et al., 2017).

4. RECOMMENDATIONS REGARDING TEACHING PEOPLE HOW TO HACK

Transitioning from the broader ethical debates surrounding the teaching of hacking, the focus now shifts towards practical considerations. Specifically, this section discusses the recommendations and best practices for making the process of teaching how to hack as ethically unambiguous as possible. In order to avoid the possible ethical issues related to employing ethical hackers as a cybersecurity measure in general, researchers have proposed a number of rules and recommendations to follow (see: (Arora et al., 2021; Georg et al., 2018; Goldberg, 2019; Kanouse, 2019).

As far as teaching hacking techniques is concerned, Trabelsi and McCoey provide a set of specific guidelines aimed at helping keep the training ethical. The first principle pertains to preparing the environment, e.g. providing an isolated network which allows exploring the newly acquired knowledge without posing any danger to the institutional network, regardless of whether it results from accidents or deliberate actions. On top of that, the teaching program ought to specifically draw the students' attention to the information on the ethical and legal implications of using hacking skills outside the lab environment (Trabelsi & McCoey, 2016). Although it is the student who decides how they are going to use their hacking skills and the knowledge they had obtained, it has been argued that it is the instructors' and institutions' duty to include moral values and ethics in the training (Hartley et al., 2017).

When it comes to deeming whether a person should be taught to hack or not, some authors go as far as to imply it is not a bad idea to screen students for criminal background activities, as well as unstable or malicious behavior, or perform a comprehensive background check, before they even get admitted to the hacking training (Logan & Clarkson, 2005). Students may also be required to pass a suitable psychological test in order to be admitted to a course. If it is not possible to perform this kind of screening, Logan and Clarkson advise to at least make students complete a course in ethics before they are allowed to apply for enrolment in a hacking course. These recommendations are especially valid in the context of organizations dealing with vast amounts of sensitive data, such as governments, healthcare or Law Enforcement (Logan & Clarkson, 2005).

Similarly to the profession of a White Hat in general, students of a hacking course should sign up for a code of conduct detailing what is unacceptable and what the implications of this kind of behavior are. If such code explicitly prohibits students from testing malicious techniques outside the lab environment, the school's liability for students' unethical/illegal actions could be limited (Trabelsi & McCoey, 2016).

Lastly, there is a burning need for introducing a mandatory, uniform code of ethical conduct for ethical hackers. In spite of the fact that there exist codes of ethics for similar professions, like IT workers in general, they do not fully align with the peculiarities of ethical hacking. In addition to this, oftentimes adherence to these codes is considered voluntary anyway (Georg et al., 2018).

5. CONCLUSIONS

This paper has discussed the concept of ethical hacking, as well as its advantages and the ethical challenges related to teaching how to hack.

Despite there being some limitations to ethical hacking, it is "an indispensable part of the current technological ecosystem" (Shetty & Shetty, 2019), and the challenges are outshone by all the advantages it brings. At the moment, it seems that thinking like hackers, and understanding their mindset is the only path to enhancing cybersecurity (Esteves et al., 2017; Kanouse, 2019; WSJ's The Future of Everything, 2021). Ethical hackers are game-changers in cybersecurity, as they create value, have a positive influence over the business community and are a key part of the organizations' security plans (Cybersecurity Exchange, 2022).

A general consensus has been reached by a number of scientists that hacking is a set of skills which should be included in the curricula of educational programs. Still, the dilemma remains and other researchers believe this will only result in the rise of a new generation of cybersecurity professionals or the young people, once given a set of hacking tools, will become online criminals. The solution to overcome this latter problem is to equip future cybersecurity specialists with profound ethical and legal knowledge and clear boundaries, as well as make them aware of the implications of their actions (Radziwill et al., 2015).

Hacking is neither inherently good nor bad; yet, depending on the context and the hackers' intent, it can be ethical or unethical, legal or illegal (Richa, 2018). A person equipped with proper hacking knowledge and tools is able to both protect a company from an attack and thus increase their revenue, or bankrupt it (Sahare et al., 2014; Vinitha, 2016). Yet, every security-minded organization, that wishes to tactically stay one step ahead of criminals, is advised to employ ethical hackers, as an extra layer of security, besides the regular cybersecurity force (Chenchu Lakshmi & Basarkod, 2015; Smith et al., 2022). Although no solution can guarantee perfect immunity against attacks,

ethical hackers may change the game in cybersecurity, and help protect the confidentiality, availability and integrity of data (Kanimozhi V.R. & Shanmugapriya, 2019). It seems it is worth taking the risk and keep educating hackers-to-be.

ACKNOWLEDGEMENT

The work described in this paper is performed in the H2020 project STARLIGHT ("Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats"). This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 101021797.

REFERENCES

Adams, D. (2019). UK Police Scheme Will Offer Teen Hackers White Hat Career Opportunities. *Digit News*.

Arora, P., Poojary, M., & Patel, I. (2021). A Review Paper on White Hat Hackers. *International Journal of Advanced Research in Science, Communication and Technology*.

Banda, R., Phiri, J., Nyirenda, M., & Kabemba, M. M. (2019). Technological Paradox of Hackers Begetting Hackers: A Case of Ethical and Unethical Hackers and their Subtle Tools. *Zambia ICT Journal*, *3*(1), 40–51. https://doi.org/10.33260/zictjournal.v3i1.74

Beniwal, S., & Sneha. (2015). Ethical Hacking: A Security Technique. *International Journal of Advanced Research in Computer Science and Software Engineering*.

Chenchu Lakshmi, S., & Basarkod, P. I. (2015). BASICS OF ETHICAL HACKING. *International Journal of Engineering Sciences & Emerging Technologies*, *7*(4).

Choraś, M., Pawlicka, A., Jaroszewska-Choraś, D., & Pawlicki, M. (2024). *Not Only Security and Privacy: The Evolving Ethical and Legal Challenges of E-Commerce* (pp. 167–181). https://doi.org/10.1007/978-3-031-54204-6_9

CompTIA. (n.d.). What Is Ethical Hacking? *CompTIA*. https://www.comptia.org/content/articles/what-is-ethical-hacking

Coursera. (2022). What Is Ethical Hacking? *Coursera*.

Crowly, B. M. (n.d.). How do I learn ethical hacking? *Quora*.

Cybersecurity Exchange. (2022). How Ethical Hackers Are Changing the Game in Cybersecurity. *EC Council*. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/ethical-hackers-changing-game-cybersecurity/

Dalalana Bertoglio, D., & Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society*, *23*(1), 2. https://doi.org/10.1186/s13173-017-0051-1

Esteves, J., Ramalho, E., & de Haro, G. (2017). To Improve Cybersecurity, Think Like a Hacker. *MITSloan*.

Georg, T., Burmeister, O., & Low, G. (2018). Issues of Implied Trust in Ethical Hacking. *The ORBIT Journal*, *2*(1), 1–19. https://doi.org/10.29297/orbit.v2i1.77

Goldberg, R. (2019). How to hire an ethical hacker. *Journal of Accountancy*.

Goswami, B. (2021). Why Ethical Hacking is the need of the hour. *Express Computer*.

Hartley, R., Medlin, D., & Houlik, Z. (2017). Ethical Hacking: Educating Future Cybersecurity Professionals. *2017 Proceedings of the EDSIG Conference*.

Iberdola. (n.d.). Ethical hacking, cybersecurity's great ally. *Iberdola*.

InteliPaat. (2022). Cyber Security vs Ethical Hacking. *InteliPaat*.

Jamil, D., & Ali Khan, M. N. (2011). Is ethical hacking ethical? *International Journal of Engineering Science and Technology*, *3*(5). http://digitalmediafys.pbworks.com/w/file/fetch/60359759/JamilD2011EthicalHacking.pdf

Jena, B. K. (2022). What is Ethical Hacking? A Comprehensive Guide [Updated]. *SimpliLearn*.

Kanimozhi V.R., & Shanmugapriya, N. (2019). Ethical hacking: the need for cyber security. *International Journal of Recent Scientific Research*, *10*(10(C)), 35339–35341. https://doi.org/http://dx.doi.org/10.24327/ijrsr.2019.1010.4083

Kanouse, J. (2019). Ethical Hacking is Evolving – Here's How Your Company Can Keep Up. *CPO Magazine*.

Kost, E. (2022). The Difference Between Cybersecurity and Ethical Hacking. *UpGuard*.

Kranz, G., Rosencrance, L., & Cobb, M. (n.d.). ethical hacker. *TechTarget Security*.

Logan, P. Y., & Clarkson, A. (2005). Teaching students to hack. *ACM SIGCSE Bulletin*, *37*(1), 157–161. https://doi.org/10.1145/1047124.1047405

Murphy, H. (2022). Ethical hackers 'hit the jackpot' as tech groups pay for protection. *Financial Times*.

Offense or Defense? An Ethical Hacker's Approach to Cybersecurity. (n.d.). *Wallix*.

Okta. (2022). Ethical Hacking: What It Is & Examples. *Okta*. https://www.okta.com/identity-101/ethical-hacking/

Pashel, B. A. (2006). Teaching students to hack. *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development - InfoSecCD '06*, 197. https://doi.org/10.1145/1231047.1231088

Patil, S., Jangra, A., Bhale, M., Raina, A., & Kulkarni, P. (2017). Ethical hacking: The need for cyber security. *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, 1602–1606. https://doi.org/10.1109/ICPCSI.2017.8391982

Pawlicka, A., Choraś, M., & Pawlicki, M. (2021). The stray sheep of cyberspace a.k.a. the actors who claim they break the law for the greater good. *Personal and Ubiquitous Computing*, *25*(5), 843–852. https://doi.org/10.1007/s00779-021-01568-7

Radziwill, N., Romano, J., Shorter, D., & Benton, M. (2015). *The Ethics of Hacking: Should It Be Taught?* http://arxiv.org/abs/1512.02707

Ramalingam, V. (2019). Impact of Hacking on Cyber Security. *Journal of Emerging Technologies and Innovative Research*, *6*(4).

Ramezanifarkhani, T. (2023a). *Why we should not teach hacking to IT bachelor students*. Kristiania.

Ramezanifarkhani, T. (2023b). Why we should not teach hacking to the IT students. *Khrono*.

Richa. (2018). White Hat Hacker : Ethical Hacking. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*.

Sabharwal, L. (2023). 5 Reasons why you should learn Ethical Hacking. *Great Learning*. https://doi.org/https://www.mygreatlearning.com/blog/reasons-why-you-should-learn-ethical-hacking/

Sahare, B., Naik, A., & Khandey, S. (2014). Study Of Ethical Hacking. *International Journal of Computer Science Trends and Technology*, *2*(6).

Shetty, S., & Shetty, K. (2019). Ethical Hacking: The Art of Manipulation. *International Journal of Advanced Scientific Research and Management*, *4*(12). http://ijasrm.com/wp-content/uploads/2019/12/IJASRM_V4S12_1672_07_10.pdf

Sinha, A. (2023). *Why Should You Learn Ethical Hacking?* LinkedIn.

Smith, L. A., Chowdhury, M., & Latif, S. (2022). Ethical Hacking: Skills to Fight Cybersecurity Threats. *EPiC Series in Computing*.

Townsend, C. (n.d.). What is the Difference Between a White Hat Hacker and Black

Hat Hacker? *United States Cybersecurity Magazine*.

Trabelsi, Z. (2011). Hands-on lab exercises implementation of DoS and MiM attacks using ARP cache poisoning. *Proceedings of the 2011 Information Security Curriculum Development Conference on - InfoSecCD '11*, 74–83. https://doi.org/10.1145/2047456.2047468

Trabelsi, Z., & McCoey, M. (2016). Ethical Hacking in Information Security Curricula. *International Journal of Information and Communication Technology Education*, *12*(1), 1–10. https://doi.org/10.4018/IJICTE.2016010101

Vinitha, K. P. (2016). Ethical Hacking. *International Journal of Engineering Research & Technology*. https://doi.org/10.17577/IJERTCONV4IS06008

WSJ's The Future of Everything. (2021). Outhacking the Hackers: The Future of Cybersecurity. *WSJ Podcasts*.

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM*, *56*(4), 64–74. https://doi.org/10.1145/2436256.2436272

Yerak, B. (2014). Wanted: Hackers with ethics to help FBI. *Albuquerque Journal*.