Ethics and Morality of Hacking: A Complex Universe

Francisco Catarino Mendes
Department of Informatics Engineering
University of Coimbra
Coimbra, Portugal
uc2019222823@student.uc.pt

***Abstract*—Hacking comprises different versions of individuals and their motivations. The two most known are white hat hackers and black hat hackers. This paper analyzes them and a series of other types that will be merged into a term called "Middle Ground". From a systematic literature review that demonstrates what has already been discussed concerning the topic, a discussion is then had to characterize the main and sub-categories of each form of hacker, containing information on their strengths, problems, and weaknesses, as well as real-life examples. The ethical and moral debate that follows goes into the importance of being knowledgeable about the existing and constant battle present in the cyber world and aims to raise people's awareness concerning the consequences of our actions. This conversation could be relevant to help identify the thin line between legality and criminality.**

Keywords: Ethical Hacking, Gray Hat Hacking, Black Hat Hacking, Ethics, Morals.

I. Introduction

Long before technology arose, the term "hacking" was used to describe "cutting in a rough and violent way, often without aiming exactly" around 1200 B.C [20]. Approximately in 1878, the word gained another meaning, despite still not being related to computers, as 2 years after the invention of the phone, young phone operators tricked callers by switching telephone lines. This showcased one of the first instances of a technical loophole being exploited [21]. Sometime after, between the 1960s and 1970s (the date differs a lot between reports), a major discovery was made. John Draper used the phreaking technique, where an individual uses a high-pitched noise to trick a phone into receiving operational commands thus changing the behavior of the telephone system. With it, he was able to execute free phone calls regardless of the distance [21].

Nowadays, hacking is the act of identifying and exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data [22]. As activities and processes keep transitioning to the online world, cybersecurity risks become more and more critical. For example, IoT (Internet of Things) cyberattacks alone are expected to double by 2025 [23]. Phishing attacks, ransomware attacks, and data breaches are among the most common crimes in recent times. Some relevant statistics are stated below:

- Since 2001, the victim count of data breaches has increased from 6 victims per hour to 97, a 1517% increase over 20 years [24];
- Cybercrime had a growth of 600% as a result of the COVID-19 pandemic [23];
- 73% of SMBs agree that cybersecurity concerns now need action, with 78% saying they will increase investment in cybersecurity in the next 12 months [24];
- From 2022, up to 40% of cyber threats now occur indirectly through the supply chain [24];
- Just 23% of security leaders monitor their partners and vendors in real-time for cybersecurity risks;
- But by 2025, it is estimated that 60% of organisations will use cybersecurity risk as a key factor when determining transactions and business engagements with third parties [24];
- Cybercrime cost the global economy around $7 trillion in 2022, and this number is expected to rise to $10.5 trillion by 2025 [24];
- According to Accenture's Cost of Cybercrime Study, 43% of cyberattacks are aimed at small businesses, but only 14% are prepared to defend themselves [27];
- According to IBM, it takes a company 197 days to discover the breach and up to 69 days to contain it [28];
- International Data Corporation (IDC) says AI in the cybersecurity market is growing at a CAGR of 23.6% and will reach a market value of $46.3 billion in 2027 [25, 29];
- According to Synopsys researchers, at least one open source vulnerability was found in 84% of code bases in 2023 [25, 30];
- The human element is the most common threat vector; it was the root cause of 82% of data breaches, according to Verizon's "2022 Data Breach Investigations Report" [31, 33];
- At the end of 2022, there was a security workforce gap of 3.4 million jobs globally [31];
- Ethical hackers were able to discover over 65,000 vulnerabilities in 2022 alone, up by 21% over 2021 [31, 32];

By analyzing these statistics, one can conclude that cybersecurity needs to be constantly evolving to keep up with cybercrime. At the moment there is still a lack of not only experts in the area but also organizations that prioritize their system's confidentiality, integrity, and availability, by putting in place the recommended methodologies and strategies.

One of those strategies is called ethical hacking. This paper does research on all kinds of hackers and focuses on the ethics and morals revolving around this complex universe. With that in mind, to achieve it, it was decided that a systematic literature review on the subject was going to be performed. Thus, the following research question was built:

RQ: Are ethics and morals relevant in the current hacking universe?

The remainder of this paper is structured as follows: Section II contains the research methodology of the literature review, which is analyzed in Section III. Characterizing the overall discussion is Section IV, which is composed of a description of the different types of hackers and a debate concerning the importance of principles and values in the hacking world. Lastly, the final remarks and future work are done in Section V - Conclusion.

II. Research Methodology

A systematic literature review was performed to answer the research question and gather the most relevant scientific papers. Having the literature review made in [1] and the article [2] as guidance, the Scopus database was chosen for this procedure, and the search query used to obtain the first sample of papers is represented in **Figure 1**:

```
TITLE-ABS-KEY ( "ethical hacking" OR “white hat hackers” OR “black hat hackers” OR “gray hat hackers” ) AND ( LIMIT-TO ( DOCTYPE,"cp" ) OR LIMIT-TO ( DOCTYPE,"ar" ) ) AND ( LIMIT-TO ( SUBJAREA,"COMP" ) ) AND ( LIMIT-TO ( LANGUAGE,"English" ) )
```

Figure 1: Search Query used in Scopus

Initially, only the keyword "ethical hacking" was thought about, which corresponded to 144 results. The problem was that most papers were related to Penetration Testing alone, and did not cover ethics, morals, or other types of hackers. So, the different main designations of hackers were added to the search query. In the end, 195 papers were acquired. The search was made by title, abstract, and keywords, restricting the results to the computer science area. The inclusion criteria were papers published in conferences and journals written in English with no date constraints [1].

Then, a .RIS file was exported to be used in Rayaan, a web-based collaborative tool to manage systematic literature reviews [3]. With the help of Rayaan, a duplicate was found and dealt with. After that, every result proceeded to be screened, being flagged as "Include", "Maybe", and "Exclude". An initial analysis gave the following outcomes: 12 "Include", and 28 "Maybe", which means that at this phase 155 papers were discarded. After going through a second examination of the "Maybes", the number of papers to be analyzed in-depth was fixated at 24. This conveys that in the end, 171 papers were deemed not inside the scope of the topic of this work. **Figure 2** represents the process of the literature review, step-by-step, using the 2020 PRISMA Flow Diagram for new systematic reviews [4].

Of the 24 papers, only 15 ended up in the final inclusion, as 4 were not available, 4 were behind a paywall, and 1 was not relevant after a full-text read. Speaking of type, 10 corresponded to conference papers, and the remaining 5 characterized journal articles. In terms of their chronological relevance, the majority has been published from 2019 and beyond, with 1 paper being released in 2015, 1 in 2017, 1 in 2018, 2 in 2019, 1 in 2020, 4 in 2021, and 5 in 2022. This implies that ethics and morality in hacking are of relative concern in the current days, and as technology evolves, illegal cyber practices grow with it, thus the importance of making discussions on the subject.

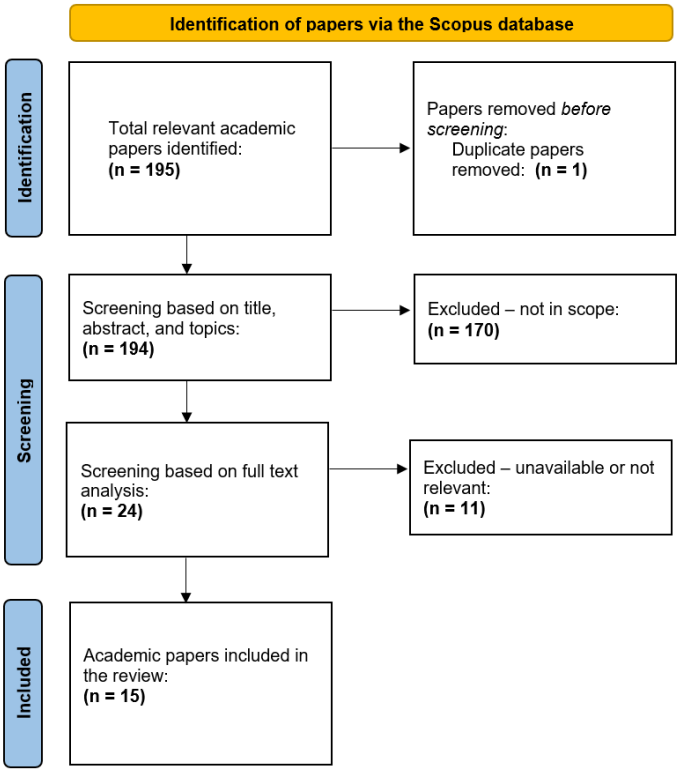

Figure 2: PRISMA Flow Diagram of the literature review

III. Analysis of the Literature

To determine the scope of the selected papers, a list of relevant terms regarding ethics and morals in hacking, as well as informatic systems, was put together. Terms like ”Privacy”, ”Cloud Computing”, ”Vulnerabilities” and ”Malware” were selected, due to them being well-known and commonly used expressions in the cyberspace. While the literature was being read, anytime one of those terms appeared in the text, its count would go up in the table. It should be mentioned that many other terms could have been considered, but in the end, these were the ones that were thought to better characterize the actual landscape of technology while having a good chance of being present in the literature.

Ethical hacking was explained in almost every piece of literature reviewed. From **Table 1**, it can be said that ”Penetration Testing”, ”Data Breaches”, ”Network”, ”Vulnerabilities”, and ”Malware” were the most used expressions among the 15 articles. This was somewhat expected, as whenever ethical hacking was brought up, the concepts circulating the term followed. One of the ways to perform ethical hacking is Penetration Testing, which occurs by hiring white hat hackers to try and breach the corresponding organization systems in order to find vulnerabilities. This usually involves trying to find points of entry in the company’s network. This practice exists to find and mitigate the system’s vulnerabilities before a malicious entity does so, by, for example, using malware, which can result in data breaches.

Some other mentions go to ”Social Engineering” and ”Privacy”, which usually came up whenever black hat hackers were debated. As for less used, the results were ”Disinformation”, ”Artificial Intelligence”, and ”Capture the Flags (CTFs)”. The first two are relatively new expressions in the cybersecurity domain, with artificial intelligence gaining more and more relevance as time passes. Disinformation is associated with AI, as it can be a consequence of its misuse. Therefore, they end up appearing in, at most, 2 papers. Concerning CTFs, it was discovered that only one paper mentioned this term, which was found to be surprising as the organization of CTFs in the education of ethical hackers is often put into practice to further develop their skills and practical knowledge.

Regarding the literature, the following considerations were made:

Shlyakhtunov [5], from the military domain, dives deep into cyberwarfare, explaining the different types of hackers, their motivations and purposes, and their impact in the cyberspace. The author does this by giving examples of real-life events in a diverse range of countries that end up affecting their criminal and political scenario, such as interference in election processes and attacks on government

List of Relevant Terms and their Frequency of Appearance	
Term	**Number of Academic Papers where present**
Information Security	5
Cyber War	3
Disinformation	1
Espionage	3
Penetration Testing	13
Data Breaches	12
Privacy	8
Network	14
Cyberspace	4
Cryptography	5
Artificial Intelligence	2
Confidentiality	7
Integrity	2
Availability	4
Compliance	6
Vulnerabilities	14
Identity Theft	4
Internet of Things (IoT)	3
Bug Bounty Programs	5
Capture the Flags	1
Malware	11
Social Engineering	8
Risk Management	4
Cloud Computing	5

Table 1: List of Relevant terms and their Frequency of Appearance

websites. Furthermore, gives some insights about Russian hackers in particular and finalizes with a description of methods to increase cybersecurity and help the good side of the “war”.

Following the line of studying different country cases, Thomas et al. [6] focus on breach disclosure laws, that vary depending on the zone of the globe, as well as the various forms of hackers. Then, the authors make a research approach to ethical hacking, one of the methods to prevent data breaches, by questioning a selected group of individuals about the possible ethical considerations of Penetration Testing, and finally discussing the results, which included confidentiality and regulation as the main themes.

Rakshitha [7] even though considered inside the scope of the topic of this paper, wrote in a very unclear way, with some errors and sudden changes of concepts. Nonetheless, the paper mainly targeted ethical hacking, by enumerating its process phases as well as justifying the need for the term to exist, finishing with an explanation of information security controls.

Aibekova and Selvarajah [8], in a sense, made a much-

improved version of Rakshitha [7], exposing everything one needs to know about Penetration Testing. The authors begin by laying down the diverse types and strategies of Penetration Testing, continuing by evaluating the tools used in this procedure in terms of their purpose and cost. To sum up, complementing the information, an attack example of a vulnerable machine was given, to demonstrate the practical side of things.

Filiola, et al. [9] also analyzed Penetration Testing, but provided some historical background and spoke about a subcategory of white hats, called red hat hackers. The paper suggested a new method that automatically discovers and mitigates vulnerabilities, using a mix of the existing Pen Testing software and tools. The experiment made at the end shows the potential of this approach if extended to more services, as the authors only focused on six.

Thomas, et al. [10] appear once again, this time with an older article. Here, ethics are key, as the main topic discussed is the implied trust companies must have to use ethical hacking as a form of defense. As there is no universal or mandatory code of conduct, organizations cannot know for sure what type of individuals they are hiring, even though on paper they correspond to white hats. This is a worrying matter and one of the reasons further discussions must be made on the theme. Moreover, the various kinds of hackers are described, a definition of trust is given, and different codes of ethics are analyzed.

Harrington [11] studied distinct real-life incidents relative to breaches in high-profile organizations in order to give lessons about attack anatomies and how to be prepared for them. It was determined that a white-box approach was a more thorough and cost-effective testing method compared to a black-box approach (ethical hacking), with mitigation strategies only appearing in the white-box assessment, due to the lack of information in the black-box assessment. The truth is, to guarantee the minimum vulnerabilities possible, both approaches must be used together.

Smith, et al. [12] argued that teaching security concepts and hacking methodologies in education may have unintended consequences, as one may be contributing to the growth of malicious hackers, even though the purpose is to educate white hats. Once more, it all falls in the moral category, where individual beliefs rule over everything else. The authors also mentioned the fact that ethical hackers must be certificated to operate, but this is inaccurate, as certificates only boost reputation within the working environment, and, after all, are optional. If a company chooses to or is unaware of the certificates' existence, it can end up recruiting ethical hackers who do not possess them.

Going back to tools and techniques used in ethical hacking, Ashraf, et al. [13] have written about ethical hacking modes, describing them, and ethical hacking techniques, showing a table containing the techniques themselves, objectives, working mechanisms, and conclusions on what to do at a social awareness level. Finally, the authors gave another table characterizing a comparison of the relevancy of a set of tools in each of the steps of the testing procedure, which ended up resulting in a score-based ranking.

Yash, et al. [14] paper was found to be very lackluster, as the authors tried to explain the process of ethical hacking but ended up falling into the confusing category. It contains errors, repeats itself, and has unclear language overall. Nonetheless, it tried to provide some knowledge regarding the phases of Penetration Testing but lacked information like the tools used in each step. A case study is also included concerning an attack on an organization, but its exposure was considered generally weak.

Ding, et al. [15] tackled some concepts not yet deeply discussed by the literature at this point, those being Bug Bounty Programs (BBPs), Responsible Disclosure (RD), and the Internet of Things (IoT). A case is made for the adoption of BBPs and RD as security strategies, as these Crowdsourced Security Practices can have some advantages over typical Penetration Testing. Then, the focus was shifted to the IoT security challenges and vulnerability management. A research question was developed, and to answer it, interviews with experts in the area were carried out. In the end, it was concluded that Crowdsourced Methods should be initiated only after companies perform initial security testing.

Vishnuram, et al. [16] went in-depth into the ethics and definitions of ethical hacking. The authors enumerated the skills required to become an ethical hacker, stated many sorts of hats, and had a conversation about both the ethical and the moral sides of the equation. Concerning ethics, codes of conduct and their respective components were talked about. As for morals, some dilemmas and controversies that organizations might face while running ethical hacking programs as part of their overall security mechanisms were discussed.

Cohen, et al. [17] did a correlation between the "disclose or exploit" dilemma and the actions of a gray hat hacker. The dilemma originates when a vulnerability is discovered by an organization and is composed of two sides: holding the announcement of the vulnerability until a patch is ready to be put in place, or disclosing immediately the vulnerability's existence. As one can imagine, with a gray hat hacker in the mix, the scenario becomes much more complex. By way of creating algorithms to determine the best approaches an organization can have when faced with this genre of situation, the authors determined that if the organization and the gray hat decide to cooperate, then the organization gains the upper hand in terms of minimizing risk and "controlling" the hacker. Should also be mentioned that both parties prefer to deal

with low-level vulnerabilities so that the losses are minimized.

Silic and Lowry [18] presented extensive work on black hat hackers and how they manage their nerves while committing criminal offenses. The authors started by providing definitions of the general strain theory, which says that emotions and negative feelings may lead to the individual's desire to perform illegal activities, and RAT, which explains the fact that often there are no capable guardians of systems in place, which creates opportunities. Also, the fact that proximity is no longer physical in this environment, but virtual, helps in nerve management. The method used in this investigation was interviewing a selected set of black hats, that met previously defined criteria, like experience and activity. From their answers, five strategies of nerve management were spotted. The shunting technique is the way hackers use to argue that they are not hurting anyone or doing violent acts, so their actions are not in the wrong. The negative thoughts are put aside, and only the positive outcomes are kept in mind. Then, there is the minimization strategy, characterized by arguments like "I'm never hacking a company based in my country – no police will come and take me down for such a small cost" [18]. In essence, as they are not making huge breaches, the risk of authorities coming for them is minimal. Plan B and the thrill sensation are other methods used by the black hats, the first being the reliance on a backup plan if things go wrong, and the latter the ability to only focus on the feeling of excitement while executing malicious procedures. This further helps them to reduce stress and fear. Lastly, the lens widening technique is also described and characterizes the belief that their actions are not dangerous compared to other criminal offenses, like physical ones. After the techniques were exposed, a discussion followed, where it was primarily said that hackers are in a state of denial and try to escape reality in order to continue their activities. Only when confronted directly by the authorities do they recognize the gravity of their actions.

Concluding the analysis, DeMarco [19] discussed a subcategory of Penetration Testing, made by what is called a Red Team. This team essentially tries to simulate a cyberattack on the organization that makes the request, attempting to identify unknown vulnerabilities. This operation is done with little to no warning to the employees of the organization, with the aim of making sure the simulation is as realistic as possible. This paper then referred to the legal risks of this procedure, in the event of something going wrong or of possible errors being made by the hired personnel. To finalize, a definition of the best practices to be followed during the simulation was given, such as whenever a critical type of vulnerability is discovered, it must be reported immediately, even if it means ending the secrecy of the operation. Safety is always first.

To discuss the analysis, five key concepts were defined. **Table 2** shows whether or not those concepts were addressed by each one of the papers. Four were categorized as the most relevant: Shlyakhtunov [5], Thomas, et al. [10], Vishnuram, et al. [16], and Silic and Lowry [18]. This number illustrates a lack of both ethical and moral discussions in the cyber community, and despite ticking all the boxes in Table 2: Shlyakhtunov [5] makes his point from a military perspective, with the concept of morality being barely present; Thomas, et al. [10] give most of their attention to trust and ethics, with morality ending up being secondary; Vishnuram, et al. [16] treat every concept with care and attention, but the potential left unscathed on the table is almost capable of leaving an expert desperate; and Silic and Lowry [18] although having done a superb job in their article of black hats nerve management, leave the concepts of white hat hacking and gray hat hacking screaming for a similar paper.

As for the others, the results show a large number of articles prioritizing Penetration Testing. Some papers briefly discuss ethics in their work, but not enough to earn a tick in the concept table. An honorable mention has to be made for [17], as it dives deep into the interactions between organizations and gray hat hackers, which can sometimes give uncertainty on which actions should both sides take.

Negatively speaking, it has to be said that Rakshitha [7] and Yash, et al. [14] have their work damaged due to the language barrier, as their written English is not the best. This consequently makes the papers, at times, unreadable and with a probability of confusing the reader instead of enlightening him.

Concept Matrix					
Articles	Concepts				
	Ethics	Morality	White Hat Hackers	Gray Hat Hackers	Black Hat Hackers
[5]	(X)	(X)	(X)	(X)	(X)
[6]	(X)		(X)	(X)	(X)
[7]			(X)		
[8]	...		(X)		
[9]			(X)	(X)	(X)
[10]	(X)	(X)	(X)	(X)	(X)
[11]			(X)		(X)
[12]	(X)		(X)	(X)	(X)
[13]			(X)		
[14]			(X)		
[15]			(X)		
[16]	(X)	(X)	(X)	(X)	(X)
[17]	(X)	(X)	(X)	(X)	(X)
[18]	(X)	(X)	(X)		(X)
[19]	(X)		(X)		

Table 2: Matrix of the key concepts discussed by the literature

IV. Discussion

A. White Hat Hacker

Despite being mostly associated by the general public with crime and malicious intentions, hacking can also be put to good use. That is what is called "ethical hacking". Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating the strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them [26]. The main methodologies used in this activity are Penetration Testing and Crowdsourced Security Practices like Bug Bounty Programs and Responsible Disclosure.

Ethical hackers have a set of required skills if they want to be successful in their operations. In [34], one can realize that concepts like networking, operating systems, cryptography, and programming languages are fundamental and should always be mastered. In addition, a degree in informatics systems related to cybersecurity, field experience, and certifications are the usual combination in terms of achieving recognition. Certifications in particular weigh a lot in terms of reputation and acknowledgement of capacities. CompTIA PenTest+ and Certified Ethical Hacker (CEH) through EC-Council are among the most well-known industry certifications. White hats also need strong analytical skills, given that their work involves examining data to identify potential issues. Therefore, to break into this field, superior problem-solving skills, creative strategy skills and attention to detail are a must.

Moving on to the details of Penetration Testing, to begin with, an organization must decide on the type of approach to carry. There are three types of approaches to Penetration Testing:

- White-Box: involves sharing full network and system information with the tester, including network maps and credentials, which helps to save time and reduce the overall cost of an engagement [39];
- Gray-Box: only limited information is shared with the tester, striking a balance between depth and efficiency. Usually useful to help understand the level of access a privileged user could gain and the potential damage they could cause [39];
- Black-Box: no information is provided to the tester, making him follow the approach of an unprivileged attacker, from initial access and execution through to exploitation. Despite being more costly and time-consuming, this scenario can be seen as the most authentic, demonstrating how an adversary with no inside knowledge would compromise an organization [39].

The level of the test must also be taken into account. [8] assists in this procedure. The testing can happen at three levels, them being the physical level of the system, the logical level of the system, and the workflow of the system. The physical level characterizes the network or the cloud, where a tester wants to safely identify flaws and vulnerabilities in the architecture and operation of the network or the cloud. Testers aim to penetrate the target by launching exploits and analyzing whether network devices and connections are prone to any attacks. The logical level corresponds to the application. This englobes the employing of simulated attacks to reveal the efficiency of the application's security, as even with a firewall and monitoring systems implemented, the application can still be hacked by way of traffic being allowed to pass through the firewall. The workflow correlates to the human side of things, social engineering. Social engineering makes use of psychological schemes to trick people into revealing information about an organization and its informatics systems. Social engineering tests are performed inside the organization to determine the level of security awareness among the staff employed.

Then, methodologies have to be addressed. There are various frameworks and standards to conduct the operation. The five most common are:

- OSSTMM (Open-Source Security Testing Methodology Manual): a peer-reviewed methodology for performing security tests and metrics maintained by the Institute for Security and Open Methodologies (ISECOM) [35, 36];
- OWASP (Open Web Application Security Project): developed and updated by a community keeping in trend with the latest threats. Apart from application vulnerabilities, this also accounts for logic errors in processes [35, 37];
- NIST (National Institute of Standards and Technology): offers a very specific Pen Testing methodology for pen testers to help them improve the accuracy of the test [35, 36];
- PTES (Penetration Testing Execution Standard): designed by a team of information security professionals to create a comprehensive and up-to-date standard for Penetration Testing, as well as to build awareness among businesses on what to expect from a pen test [35, 38];
- ISSAF (Information System Security Assessment Framework): a Pen Testing guide supported by the Open Information Systems Security Group (OISSG), no longer updated [35].

All of the existing frameworks contain similar steps of execution. Depending on the type of approach, some steps

may not be needed. The stages described subsequently are considered common to most Pen Testing standards and have their origin in [40].

Stage 1 is called Reconnaissance. In this phase, the tester gathers as much information about the target system as they can, including information about the network topology, operating systems and applications, user accounts, and other relevant information. The goal is to gather as much data as possible so that the tester can plan an effective attack strategy. This process can also be categorized as either active or passive depending on what methods are used to gather information. Passive reconnaissance pulls information from resources that are already publicly available, whereas active reconnaissance involves directly interacting with the target system to gain information [40].

After Reconnaissance, it is time for Scanning, Stage 2. In this phase, the tester uses various tools to identify open ports and check network traffic on the target system. Because open ports are potential entry points for attackers, penetration testers need to identify as many open ports as possible [40].

Recognition is followed by Assessment. Therefore, Stage 3 is Vulnerability Assessment. Here, having the data collected until this stage as the starting point, the objective is to identify potential vulnerabilities and determine whether they can be exploited. Several resources can help determine vulnerability risk. For example, the National Vulnerability Database (NVD) is a repository of vulnerability management data created and maintained by the U.S. government that analyzes the software vulnerabilities published in the Common Vulnerabilities and Exposures (CVE) database [40].

With the results of Stage 3, Stage 4 can start, which is the Exploitation phase. The penetration tester attempts to access the target system and exploit the identified vulnerabilities using a determined set of tools. This is probably the most critical step, as the expert must be extremely careful with his actions [40]. Also, this is the zone where debates regarding ethics and values could take place.

Finally, after the technical procedure is concluded, all that is left is to report. Thus, Stage 5 is Reporting. The report generated in this final Penetration Testing phase can be used to fix any vulnerabilities found in the system and improve the organization's security posture [40]. It must be well-documented, containing the course of action taken and providing solutions to mitigate or resolve the found vulnerabilities. The penetration test is now concluded.

Next, a discussion of the tools and techniques utilized is required. There is a certain combination of materials normally used, and some of the most known are described below:

- Nmap: a highly functional tool that is used to scan the network for open connections. Essential to assess the security of network systems. Commonly used in Stages 1 and 2 [8, 13];
- Wireshark: a network analysis tool that can capture packet data from a network and decode it into readable form. Also relevant in the first two Stages [13, 40];
- Metasploit: a vulnerability exploitation mechanism that has a variety of programs and operating systems, as well as a wizard that can assist penetration testers in capitalizing on known vulnerabilities. Suits Stage 4 well [40];
- Burp Suite: an all-in-one web application security testing tool that is able to scan websites for vulnerabilities, manipulate requests and responses, and intercept traffic between the client and server. Useful in Scanning and Vulnerability Assessment [40];
- HashCat: the most powerful, advanced, and fastest password cracker. Consists of five attacking modes that go through 200 efficient hashing algorithms. Good for Scanning and Exploitation [8, 13];
- SQLMap: a tool that automates the process of finding SQL injection types of vulnerabilities. It is a great tool as it can participate in all Stages bar Stage 6, due to its power of attack and gathering valuable data [13, 41];
- Phishing: by sending malicious e-mails to previously selected members of the tested organization in order to test their awareness.

As the initial point of the Crowdsourced Practices, with the help of [13], a comparison between those and Penetration Testing is made, which at the same time highlights the limitations of the latter. For example, achieving the readiness needed to start the process can take a while in Pen Testing, as an organization needs to research and hire available experts on the matter. On the other hand, Crowdsourced Testing can start within as little as 1 hour. Another example is while Pen Testing is often done by 2 or 3 individuals, Crowdsourced Testing can have up to thousands of people working with the same goal [15]. So, as one can understand, Penetration Testing has time, productivity, and personnel weaknesses. On the other hand, the perspective of having countless individuals trying to break the security of an organization's system might be scary. Crowdsourced Testing involves the participation of large numbers of ethical hackers, reporting vulnerabilities to companies in exchange for rewards that can consist of money or just recognition.

Two techniques are going to be discussed. Starting with Bug Bounty Programs, these represent a reward-driven Crowdsourced Security Testing Mechanism where ethical hackers who successfully discover and report the vulnerabilities to companies are rewarded. The objective of BBPs is to prevent vulnerabilities from being discovered and exploited by malicious hackers and to enhance corporate security [13]. These can also be categorized as public or private. In public cases, they are usually open to an entire community of ethical hackers, unlike private ones, which are made specifically for a sub-group of hackers and dispose of a time limit [13]. Companies should be extremely careful when adopting this strategy, because if they make available a version of the system that was not deeply tested by its engineers, a lot of vulnerabilities will end up being found, which results in companies having to hand out lots of monetary rewards. Depending on the quantity, this can have a considerable impact financially and even at a reputational level.

Responsible Disclosure consists of rules and guidelines from companies that allow individuals to report vulnerabilities to organizations. The RD policies will define the models for a controlled and responsible disclosure of information upon vulnerabilities discovered by users. These rules were made as a way to ensure that organizations and individuals have a channel of communication regarding their system's security issues [13]. This practice correlates with gray hat hacking, differing only in the fact that RD is a way for organizations to give consent about exploring and trying to get inside their systems. Gray hat hackers on the other hand were not given permission, therefore making their activities of vulnerability finding fall into the illegal side, despite not having malicious intentions.

The differences between these two methodologies are in invitation and rewards. While a BBP is invitation-based, RD is just a set of guidelines that people should follow if they want to report a vulnerability to a company. Furthermore, a BBP offers a monetary reward, opposite to RD [13].

1) Blue Hat Hacker

: Blue hat hackers are white hat hackers hired externally by companies to perform Penetration Testing and sniff out bugs and vulnerabilities before a big launch. Whereas white hat hackers are usually part of the company, blue hat hackers are outsourced. Therefore, they distinguish themselves a little from white hats [46].

Blue hats often work as part of a team, and they may not be responsible for carrying out hacks on their own. They usually work for IT departments in large companies, or they may work for cybersecurity agencies that sell white hat hacking services to clients [42]. Their threat level is in the "Low" category [43], as they work to improve the cybersecurity of the organization in question.

A second version of a blue hat is called a revenge seeker. These individuals are in the middle of a transformation to a black hat as they correspond to experienced hackers who use their skills for personal revenge against an individual or organization [43]. For example, in 2014, an EnerVest (a US oil and gas company) employee sabotaged the company's systems after finding out he was going to be fired. The network engineer reset everything to factory settings, which also deleted a lot of data, and EnerVest couldn't operate for a month [46].

2) Red Hat Hacker

: Also known as vigilante or eagled-eye hackers [43, 45], red hat hackers are motivated by the desire to fight back against black hat hackers. They see themselves as the "superheroes" of the hacking world. Sometimes Government-Hired [44], they specifically focus on finding and disarming black hat hackers. Additionally, they involve themselves in classified intel like a country's defense and research sectors, being part of anything that falls under the category of sensitive information [16]. Red hat hacking can be intertwined with hacktivism, whenever hacktivists have non-malicious objectives.

They are known to be particularly ruthless in their hunt for black hat criminals and typically use any means possible to take them down. This often looks like using the same tactics as black hat hackers against them, like using the same malware, viruses, and other strategies to compromise their machines from the inside out [44]. Another tactic used by red hats is infiltrating black hat communities on the dark web and launching hacking attacks against their networks and devices [43]. Their threat level can even be categorized as "Very Low", as their main goal is not only to defend against black hats but also to go even further and destroy them.

3) Purple Hat Hacker

: Purple hats are self-learners. They train their skills by hacking their own computer system as an exercise. This entails using one PC to hack another PC that they own and then assessing their hacking techniques [43]. This type of hacker poses minimal risk to anyone besides themselves, as their main goal is to improve their skills in a controlled environment [47]. Therefore their threat level can be determined as "Very Low".

One professional who made a career out of teaching people how to do things like this is an IT (informatic systems) professional called "Eli the Computer Guy". He creates YouTube videos teaching people how to self-study cybersecurity, and how to build their own at-home labs to gain experience, among other types of IT videos [47].

B. Middle Ground

In this section, all of the different forms of hackers that do not represent either white hats or black hats are treated. Notwithstanding the fact that gray hat hackers are the ones usually associated with the fame of not being either criminals or ethical hackers, the reality is that this middle-ground contains a lot more depth than what is commonly thought.

1) Gray Hat Hacker

: Starting with the most well-known ”in the middle” type, gray hat hackers are computer security experts who often look for vulnerabilities in a system without the organization's permission or knowledge. If issues are found, they may report them to the organization, sometimes requesting a fee to reveal the problems in the process [17]. In the case that the victim company does not want to collaborate, gray hat hackers will probably not attempt to retaliate and cause harm, but will also not disclose to said company what vulnerabilities were found, leaving it in a state of security uncertainty [42].

Typically, they engage in hacking activities for the pure enjoyment of finding gaps in computer systems, for monetary reasons, or to make a name for themselves, becoming famous in the cybersecurity community and advancing their career [44, 48]. However, the interactions that inevitably happen between these individuals and the victims have a considerable degree of complexity, potentially leading to various consequences, like the transition of the cybersecurity expert to a black hat, or a white hat.

According to [17], organizations from most sectors do not appreciate unauthorized forays into their business information infrastructure. Instead, an anxious feeling prevails that gray hat hackers might attempt to retaliate in instances of non-cooperation, becoming black hats by disclosing the vulnerabilities found on the internet or even exploiting those vulnerabilities to cause harm. This creates a dilemma for companies, as they usually prefer to make the found vulnerabilities public only after patching them. However, the gray hacker factor may oblige them to make the disclosure as soon as possible, as the scenario would be worse if the IT community found out the information from the hacker. Another aspect is the fact that the gray hat may use the first vulnerability as an entry point to other areas of the system, making the alarms go off for the victim, as the event would double in its critical nature. This creates a situation where the best course of action for both parties is to actually work together.

For example, the hacker could be recruited by the victim, making the transition to the ethical side of hacking. The initial deal could involve having the gray hat keep searching for more vulnerabilities, while the organization tries to patch the first one as soon as possible in order to report it. As long as the company is active in this interaction game, it will always have the lead over the hacker, who will respond to its moves accordingly. Therefore, if the organization manages to predict the hacker's intentions, it will always have an overall advantage.

A well-known real-life example was when in 2013, computer security researcher Khalil Shreateh hacked Mark Zuckerberg's Facebook profile. He found a glitch that allowed him to post to anyone's Facebook wall and reported it to Facebook. The company ignored the hacker's report, so Khalil decided to post on Mark Zuckerberg's wall using the loophole that he found to gain their attention [48]. Despite his intentions being of a good nature, Khalil was not eligible to receive a reward, because, after all, he violated Facebook's terms of service by hacking the page of another user.

2) Green Hat Hacker

: Green hat hackers are “green” in the sense that they're inexperienced and may lack the technical skills of more experienced hackers [43]. Also known as newbies, “noobs“, or neophytes, their goal is to gain acceptance into the ranks of the hacker world [50]. Whether they already have malicious intentions and aspire to go the black hat route or are training to become white hat hackers, they can be dangerous. They may accidentally cause irreversible damage by trying out various cyberattack techniques and using all kinds of malware. New hackers are unaware of what consequences their actions might have and lack the skills to fix an attack gone wrong [51].

Due to their absence of knowledge in this sensitive world, their threat level is put at ”Medium”, as the slightest of unintended errors can potentially have a great impact on their learning process and learning subjects. Initially, green hats may not have technical skills, but can still use methods like phishing and other social engineering techniques to bypass security systems [43].

Action must be taken in order to push as many green hats as possible off the black route way. As they learn, they will eventually have the ability to become contributing members of the ethical hacking community. Even so, and with [50] as the source, there are several contributing factors that may tip a young individual into cybercrime. Individual characteristics, comprehensibly, have some weight in the formation of their ideas, as backgrounds differ from person to person, and some may feel the need for online affiliation and affirmation. Then, interests come into play. They may derive pleasure from the problem-solving of ever more complex hacks and the improved social ranking achieved by their exploits. The fact that it is much easier to make exploits in a videogame, or to illegally download music or other forms of copyrighted property may only increase interest in gathering information on how to actually become an expert in cyber intrusion and corruption. This is a result of the feel-good sensations the

adrenaline, and the increase in online reputation associated with being able to alter the state of something that was not supposed to be altered. In real life, these young individuals certainly would not dare to commit robbery in a music store, for example. Finally, the technology era the world is in today also plays a role. Most teenagers have known technology and the internet since they were born, and they can use it to have anonymity and access to dangerous tools like the dark web.

In order to fight this tendency, awareness of this subject must be raised in the education sector. Other sources of inspiration must be created relative to taking the path of becoming a white hat hacker. Competitions must take place so as to give teenagers their deserved recognition in cybersecurity aspects [50]. Overall, the industry needs to do better.

3) State/Nation Sponsored Hacker

: State-sponsored hackers work for governments. Some are white hat hackers who work to improve national cybersecurity, but others use black hat tactics to harm other countries, as they can act with a degree of impunity since they operate on behalf of their government. These hackers are the soldiers used whenever there exists digital warfare. They represent a "High" threat level to other countries and governments [42, 43].

Nation-state hackers usually aim for high-profile targets such as military secrets, infrastructures, massive-scale disinformation, or propaganda campaigns [52]. There are approximately two dozen countries around the world currently suspected of state-sponsored programs for governmental cyberattacks [53].

Regarding motivations, following [52], on the hacker's side, there is the principle of nationalism, which characterizes the pride in participating in cyberwarfare defending their country's interests, and the no accountability factor, meaning hackers can have freedom concerning the methods and approaches used, even if it means going the criminal route. Financial gains apply to both the hackers and the states, as governments give high remuneration to these experts so that they can gather the best staff possible, intending to generate cash from the attacks performed. As for the individual nation's benefits, obtaining confidential information and the potential influence power over other countries are among the reasons they act as described.

In [53], the major players are shown:

- Russia's group: represents a constant threat to an array of organizations and government agencies allied with Western countries. Their main targets are government elections, the media, and several global companies;
- North Korea's group: cybercriminals responsible for various attacks over the past decade, like the WannaCry Ransomware [54];
- United States of America's (USA) group: a cyberwarfare and intelligence-gathering unit which monitors and infiltrates enemies of the United States, both foreign and domestic.
- China's group: a cyberwarfare organization that focuses on stealing trade secrets and confidential information from corporations across every vertical, with emphasis on manufacturing, engineering, and electronics.

Some real-life examples include the Russian interference in the USA 2016 elections, the Stuxnet attack on Iran constructed by the USA, the WannaCry Ransomware attack made by North Korea, and the recent Russian cyberattacks on Ukraine with respect to the war between the two countries [52].

4) Hacktivist

: Hacktivism refers to hacking into a system for political or social purposes, such as human rights, free speech, and freedom of information. Hacktivists target corporations and governments to disrupt activities or raise public awareness of an issue [55]. Those who practice hacktivism generally intend to cause reputational damage or some other form of harm to their victims, even if they believe they are promoting the greater good [42].

Hacktivists are very belief-oriented, always engaging in activities to try and correct what, in their minds, needs to change. The problem is that this can be a subjective matter, which adds a layer of complexity to the situation. Their threat level is categorized as "High" to the targeted organizations.

The most famous hacktivist group is the Anonymous group, a decentralized international collective of tech activists and hackers. Their history of targets includes governments, state organizations, tech giants, and big enterprises [56]. Most recently, they declared cyberwar against the Russian government following the invasion of Ukraine. Since then, they have leaked the database of the Ministry of Defence and the Ministry of Economic Development of Russia, taken down many state websites, including government.ru, hacked Russian state TV channels, and intercepted Russian military communications [56].

Another example of a hacktivist is the Portuguese hacker Rui Pinto. Despite his self-designation as a whistleblower, as he was not part of the organizations he breached, the designation of hacktivist is better attributed, as the reasons for his attacks, besides financial, were most certainly opinion-oriented. Known for the case "Football Leaks",

which involved the divulgation of some corruption cases made inside football, where he disclosed a lot of different confidential data to the public, he is now accused of 147 crimes [57]. It can be said that the general public opinion concerning Rui's actions oscillates from person to person.

C. Black Hat Hacker

Black hat hackers, also called Crackers, are cybercriminals who illegally crack systems with malicious intent. Seeking to gain unauthorized access to computer systems is the definition of black hat hacking [43]. They aim to achieve financial gain from their knowledge by blackmailing, sabotaging, or engaging in other criminal activities [18], and they typically go to great lengths to hide their identities. Black hats can be solo, or be part of a criminal organization. Due to them being the most dangerous and versatile type of hacker, their threat level is naturally "Very High", and companies that deal with sensitive information should always keep their guard up.

In order to achieve profit, black hats can follow various courses of action, as shown in [58]. They can steal personal information to sell it or craft further attacks. They can hack and disturb systems just for fun, or to compete against peers at the cybercrime scene. They can create new malware for personal use, or just to bring more chaos and techniques for the community to use. They can use spying methods to gather confidential information. They can crack software released by companies and distribute it for free, expecting to receive donations for their work, as is usually seen in the gaming space. In insight, it really is frightening the amount of paths black hats can take to achieve their goals.

As for types, some are unique and distinguishable. With [43] in mind, one can list the following:

- Botnet hackers: black hats that turn previously infected devices into malware-laden zombies, which they control remotely and use to infect other devices. With a large enough botnet, these attackers can send large-scale spam and malware campaigns or carry out devastating DDoS attacks;

- Cryptohackers: individuals that steal cryptocurrency by manipulating crypto coin exchanges or DAOs. They mainly use phishing schemes to lure their victims into scam coin exchanges and software tools to steal digital currency;

- Cryptojackers: hackers that bypass the costs of crypto mining by infecting devices, to perform complex mining processes of cryptocurrency. In essence, they steal other system's computing power. Sometimes it is so noticeable to the owner that only then he might start investigating the causes of his computer's performance loss.

One public case of a black hat hacker is a man called Evgeniy Mikhailovich Bogachev. Taking into account his FBI's (Federal Bureau of Investigation) Most Wanted page [59], these are the details of the Russian's criminal activity: "Using the online monikers "lucky12345" and "slavik", is wanted for his alleged involvement in a wide-ranging racketeering enterprise and scheme that installed, without authorization, malicious software known as "Zeus" on victims' computers. The software was used to capture bank account numbers, passwords, personal identification numbers, and other information necessary to log into online banking accounts. While Bogachev knowingly acted in a role as an administrator, others involved in the scheme conspired to distribute spam and phishing emails, which contained links to compromised websites. Victims who visited these websites were infected with the malware, which Bogachev and others utilized to steal money from the victims' bank accounts."

1) Script Kiddie

: Script kiddies, or skiddies, refer to amateur hackers who use ready-to-run programs for malicious purposes. It is a derogatory term for individuals who do not understand how malicious tools and source code work and would not be able to modify or create them [60]. Although they do not possess the skills of their more experienced counterparts, the ease with which they can launch attacks and the fact that they often don't fully understand the damage they can do with the pre-created programs they use make them a real danger to internet security [43, 61].

Therefore, their threat level has to be defined as "Very High". Not only do they practice the same as black hats, but also at the same time they do not have the technical knowledge to understand what they really are doing. Unlike other hackers, these individuals are attention seekers, reckless, impulsive, create chaos, and want to have fun without the goal of growing and learning [60]. Additionally, the internet is flooded with prewritten hacking scripts and hacking tools available for use or purchase, making it easy for these amateur hackers to find the specific hacking script they are looking for [62]. While they may not be able to get results, the opposite can also happen where they cause even more damage than what they anticipated doing. The disregard and carelessness they show are scary.

As their goal is to make an impact regardless, they pay the price with indiscretion, which leads to them being easy targets to the authorities or cybersecurity professionals. There are some typical attacks script kiddies perform, as one can see in [62]. Firstly, website defacement, where they manage to penetrate a website and alter or delete content. Then, DoS (Denial of Service) attacks where they flood a network with traffic leading to it becoming unavailable to everyone. Ultimately, social engineering attacks, with the aim of infecting systems or stealing confidential information.

[61] shows the testimony of an anonymous skiddie, where he says that when he was about 12 years old, one day, he chatted with a friend online who told him he had found a ”really interesting little program” he wanted to try out. He proceeded to put the skiddie's telephone number into the software and was able to take over his whole WhatsApp account. That was the event that got him interested in the hacking universe. Another example is an incident where a 15-year-old script kiddie used a DoS attack to hack the telephone company TalkTalk in 2015. This attack led to a data breach, and eventually the arrest of the 15-year-old boy [62].

2) Whistleblower

: A whistleblower is a person who reveals activities or information within a corporate, public, or government establishment that are considered illicit, corrupt, or improper [63]. Whistleblowers typically work inside the organization where the thought wrongdoing is taking place [64]. Individuals who want to enjoy the protections and rewards of blowing the whistle cannot do it without a plan. They must oblige to what is written in the laws under which they are seeking formal whistleblower status [64].

Because these people work for the targets they hack, most of the time they already possess the security access needed to expose confidential information, making the technical aspect of the process somewhat easier [42]. Their threat level corresponds to ”Very High” for the organizations targeted, as the data exposed can be extremely impactful to their survivability and public opinion.

A well-known example of a whistleblower is the case of a man called Edward Snowden, who leaked classified information from his position within the United States of America's (USA) National Security Agency [42]. The way he did it was by traveling to Hong Kong to provide three journalists with thousands of top-secret documents about the USA intelligence agencies' mass programs of surveillance of American citizens, revealing privacy abuses made by the government itself. His story is told in [65].

D. Ethical and Moral Debate

Ethics refers to the discipline concerned with what is morally good, bad, right, or wrong, and to any system or code of moral rules, principles, or values [66]. Morality is defined as the moral beliefs and practices of a culture, community, religion, or a code or system of moral rules, principles, or values [67]. People, naturally, have a lot of different ideas and beliefs. This can lead to an immense level of complexity in some interactions. In the technological and cybersecurity context, there is a lot that can be said regarding these principles, which is exactly what is going to be addressed in this section. All of the main categories of hackers will be scrutinized in the next paragraphs. The papers [10, 16, 17, 18] deserve to be mentioned here as their help is fundamental for the making of this chapter.

Starting with white hat hackers, the ethical hacking procedure has a lot to be spoken of. In accordance with the Kant theory, which pinpoints rights and wrongs based on the duties of humans no matter the cause or outcome, ethical hacking is ethically wrong as it invades the right to privacy by gaining access to sensitive information of others. But under the Consequential theory, which defines ethicality based on the cause and outcome, it is ethically correct [16]. There is a sense of trust implied in cybersecurity experts when executing Penetration Testing. After all, an organization hires them to enhance its system's security. But what if something goes wrong? Let's consider an ethical hacker engaged in testing the security of an organization that holds personal or highly sensitive information, such as a financial institution or legal firm [10]. The first thing to be said is that some confidentiality is immediately lost by taking this approach, because if a test is successful, the white hats will unintentionally gain access to the sensitive data. Another aspect to consider is the potential the ethical hacker has of causing a negative condition to a system, like service disruption or corruption. In those events is the expert the sole responsible, or is the company liable for having put their trust in him? Besides, speaking of liability, what if a Pen Testing team performs a test in an organization, finds vulnerabilities, reports on how to patch them, and sometime later (1 month, for example) a black hat is able to gain unauthorized access? Is the testing team liable for failing in their job, or is the organization liable for not following the advice made by the experts?

Then, what if the psychological nature of one of the white hats making the test is to always take advantage of everyone? By accessing to confidential data of a company, they automatically gain the upper hand. Their immoral and unethical mind will lead them to bribe the company, for example, to continue to take their services for a higher price. What if one of the testers accesses information that goes directly against his morals and beliefs, like the example of Edward Snowden? What if an organization conducts a Bug Bounty Program? The odds of encountering a tester like that go up by a lot. If the information comes out, it could lead to serious consequences for an organization, all due to implied trust in someone who does not even make part of the staff, as penetration testers usually take jobs and leave after finishing them. Therefore, companies should always have minimum requirements in the process of hiring pen testers, like mandatory certificates and a code of ethics related to the specialty. In addition, background checking might be needed. The fact that the cybersecurity world has not yet made a universal and mandatory guide of conduct that cybersecurity experts must follow is worrying. It would solve a percentage of the issues. There are some, like the EC-Council Code of Ethics [10], but the key factor remains

in their optional nature. Medicine and law-related careers, for example, universally have to oblige to a certain set of rules regarding ethics, and the slightest misconduct can lead to the end of an individual's career. Also, what happens to the penetration tester who chooses to expose the confidential information? Well, as one can imagine, his credibility becomes shattered the moment he decides to commit an action of this genre. Events like these are where transitions can happen, as the former tester might be seen as some sort of whistleblower. From there, one can become a hacktivist, or make the full transition into the other side, turning into a black hat hacker. This is an extremely bad outcome, as the field of cybersecurity is already lacking professionals, and losing one to the criminals is the worst-case scenario. All in all, organizations should really be careful concerning who they hire to potentially gain access to their systems, as one can never be sure of what type of person stands in front of him.

The education sector also faces some controversies. In the process of instructing individuals to become white hat hackers, depending on the attitude of the students, what can happen is the origin of new black hat hackers. Students might be lured by the black hat mindset and could just start using their recently acquired powerful knowledge for criminal activities. Another possibility is that if a student has these beliefs and goals previously defined, they can just take advantage of the learning process to achieve the technical capacities they need. Therefore, academic institutions must make their utmost efforts to sensibilize their cybersecurity prospects and highlight what is morally and ethically wrong. Another suggestion might be to do personality tests before letting students enroll in this career path.

Next, the concept of red teaming must be talked about. According to [19], Red teaming is a form of ethical hacking that involves the use of techniques and methods similar to those of a criminal hacker or state-sponsored organizations to simulate a real cyberattack (often paired with a physical intrusion) so that the corporation can learn about weaknesses in their defenses. The theory is that by simulating an attack, the Corporation can prompt appropriate changes and security improvements based on observed cyber weaknesses. It involves a more comprehensive cybersecurity assessment of a company, often over a longer period and usually with little or no warning to employees within the company. This last phrase is key. The fact that this procedure is done without the knowledge of the employees might be considered morally wrong. What is the probability that, if this strategy is found out, various employees get upset with the management? Arguments like these might contribute to companies not wanting to use this cybersecurity approach, which in theory, can be useful to simulate attacks and build better defenses.

Concerning gray hat hackers, as seen in [17], normative ethical theories from Mill, Kant, and Aristotle claim that gray hacking is morally wrong. They claim a "gray hat" is a different form of a "black hat" in ethical evaluations. But they also argue that gray hats believe their intent is morally right. Gray hat hackers neither want to be seen as bad guys nor are they ready to commit to being a white hat. It gets confusing when trying to interpret their morality, since they help organizations solve their security problems, but then again, they were not asked to do so. There is a chance that the fact they claim to have good intentions leads them to not feel guilty for the fact that, in essence, a crime is being committed.

As for hacktivists and whistleblowers, they are part of the same bracket, where despite technically practicing illegal actions, in the eyes of many they correspond to heroes and therefore deserve a lot of praise for exposing and fighting against what are commonly thought to be wrong-doings. The question is, not everyone has the same opinion. At the end of the day, they are still taking part in criminal activity. Attacking online systems or revealing confidential information is still illegal, even if that information corresponds to other criminal activity like corruption in the financial department. It could be said that these hackers lack ethics, as they are willing to go beyond what is written in the law to achieve their goals, while on the side of morality, it essentially depends on the beliefs and opinions of each individual. This debate will probably never see a clear answer. Beliefs will always remain aligned between some and conflicted between others.

To conclude this debate, black hat hackers need to be discussed. The AI (Artificial Intelligence) factor is gaining more and more relevance as it evolves. Right now, it is completely possible to manipulate ChatGPT's AI into developing malware [68]. With the ability to learn and adapt, AI has the potential to become highly sophisticated in the attacks it comes up with. This means that people with even less knowledge of the field than script kiddies will be able to hack and infect systems with little to no effort. This is extremely concerning, as there are people out there who just want to have fun with destruction. And as it is happening online, with no visible consequences, these individuals cannot picture the real impact of their efforts.

Transitioning to the topic of black hats' emotions and thoughts, and how they deal with them, the first thing that can be said is that commitment to an activity only happens if they determine that it is worth it regarding stress and possible gains. By analyzing [18], which handles their nerve management, a door opens to their usual psychological state. Black hat hackers believe that their actions do not fall into the criminal and dangerous side. As the damage in front of their eyes is not physical, their thought process is that no real harm is actually being done. They go even further as to compare their behaviour with physically violent situations, claiming once again that what they do is much less significant. Moreover, they only associate crime with, for example, breaching all of a company's systems. If only one is being breached and happens to belong to a foreign

country's company, they not only see it as a legal procedure but also live with the comfort of knowing the authorities would not bother to come after them. In the end, black hats are constantly tricking themselves, like a student postponing their assigned work until the day before the deadline, thinking he has enough time for its realization. Some may truthfully not even have bad intentions, they just really believe their actions do not correlate with crime. Their ethicality and morality might not be corrupted. The issue is that most of the time these hackers only face reality when they are caught by the authorities, or when something goes wrong and they realize the damage caused. In those scenarios, a transition can happen, eventually leading them to be accepted by the ethical hacking community and to become white hat hackers. Authorities must double down in their efforts to catch cybercriminals, as these are the kinds of transitions that should happen more frequently.

V. Conclusion

In this paper, a reflection of the hacking universe was made, including the ethics and morality revolving around it. Firstly, a systematic literature review was put together to gather intel concerning existing scientific papers on the topic, which resulted in 15 relevant articles. Those were read to their full extent, and an analysis of each one was provided. Then, the discussion section of this paper was built. Composing it was a definition of each type of hacker, including a set of different characteristics and a combination of real-life examples, and the ethical and moral debate, which touched on areas like liability, beliefs, ethicality, and morality regarding the most common categories of hackers.

Limitations to this work include the literature review being restricted to Scopus, potentially excluding relevant papers not indexed in this database, the fact that some information might have been left out regarding the characterization of the different forms of hackers, and the possibility of too much author biases when writing the ethical and moral debate.

As for future work, considering the pace of technological evolution in this day and age, reassessments of this subject will eventually be required in other to provide a better evaluation of the hacking landscape. In addition, to get closer to an ethical and moral consensus, more opinions on this matter are needed, especially from experts in all areas of cybersecurity.

References

[1] Rupino, P., Estima, J.: "Navigating the landscape of AI ethics and responsibility" (2023).

[2] Webster, J., Watson, R.: "Analyzing the Past to Prepare for the Future: Writing a Literature Review" (2002).

[3] Ouzzani, M., Hammady, H., Fedorowicz, Z., Elmagarmid, A.: "Rayyan — a web and mobile app for systematic reviews" (2016). Available at https://doi.org/10.1186/s13643-016-0384-4.

[4] Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ 2021;372:n71. doi: 10.1136/bmj.n71. Available at http://prisma-statement.org/prismastatement/flowdiagram.aspx.

[5] Shlyakhtunov, M. A.: "White-Grey-Black Hat Hackers Role in World and Russian Domestic and Foreign Cyber Strategies" (2021). Available at https://doi.org/10.14569/IJACSA.2021.0120849.

[6] Thomas, G., Burmeister, G., Low, G.: "The Importance of Ethical Conduct by Penetration Testers in the Age of Breach Disclosure Laws" (2019). Available at https://doi.org/10.3127/ajis.v23i0.1867.

[7] Rakshitha, C. M.: "Scope and Limitations of Ethical Hacking and Information Security" (2020). Available at https://doi.org/10.1109/ICESC48915.2020.9155846.

[8] Aibekova, A., Selvarajah, V.: "Offensive Security: Study on Penetration Testing Attacks, Methods, and their Types" (2022). Available at https://doi.org/10.1109/ICDCECE53908.2022.9792772.

[9] Filiola, E., Mercaldo, F., Santone, A.: "A Method for Automatic Penetration Testing and Mitigation: A Red Hat Approach" (2021). Available at https://doi.org/10.1016/j.procs.2021.08.210.

[10] Thomas, G., Burmeister, G., Low, G.: "Issues of Implied Trust in Ethical Hacking" (2017). Available at https://doi.org/10.29297/orbit.v2i1.77.

[11] Harrington, T.: "Hackers: Analysis of Attack Anatomies" (2015). Available at https://doi.org/10.1049/ibc.2015.0047.

[12] Smith, L. A., Chowdhury, M. M., Latif, S.: "Ethical Hacking: Skills to Fight Cybersecurity Threats" (2022). Available at https://doi.org/10.29007/vwww.

[13] Ashraf, M., Zahra, A., Asif, M., Ahmad, M. B., Zafar, S.: "Ethical Hacking Methodologies: A Comparative Analysis" (2021). Available at https://doi.org/10.1109/MAJICC53071.2021.9526243.

[14] Yash, T., Kumar, S., Dinki, Sharma, K.: "Ethical Hacking: A Technique to Enhance Information Security" (2022). Available at https://doi.org/10.1109/COM-IT-CON54601.2022.9850601.

[15] Ding, A.Y., De Jesus, G.L., Janssen, M.: "Ethical Hacking for Boosting IoT Vulnerability Management: A First Look into Bug Bounty Programs and Responsible Disclosure" (2019). Available at https://doi.org/10.1145/3357767.3357774.

[16] Vishnuram, G., Tripathi, K., Tyagi, A.K.: "Ethical Hacking: Importance, Controversies and Scope in the Future" (2022). Available at https://doi.org/10.1109/ICCCI54379.2022.9740860.

[17] Cohen, D., Elalouf, A., Zeev, R.: "Collaboration or separation maximizing the partnership between a "Gray hat" hacker and an organization in a two-stage cybersecurity game" (2022). Available at https://doi.org/10.1016/j.jjimei.2022.100073.

[18] Silic, M., Lowry, P.B.: "Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes" (2021). Available at https://doi.org/10.1007/s10796-019-09949-3.

[19] DeMarco, J.V.: "An approach to minimizing legal and reputational risk in Red Team hacking exercises" (2018). Available at https://doi.org/10.1016/j.clsr.2018.05.033.

[20] Hiley, C.: "Brief history of cybersecurity and hacking" (2023). Available at https://cybernews.com/security/brief-history-of-cybersecurity-and-

hacking/.

[21] Fox, J.: ”A Brief History of Hacking” (2022). Available at https://www.cobalt.io/blog/history-of-hacking.

[22] Kaspersky - ”What is hacking? And how to prevent it”. Available at https://www.kaspersky.com/resource-center/definitions/what-is-hacking.

[23] Mclean, M.: ”2023 Must-Know Cyber Attack Statistics and Trends” (2023). Available at https://www.embroker.com/blog/cyber-attack-statistics/.

[24] Griffiths, C.: ”The Latest 2023 Cyber Crime Statistics (updated October 2023)” (2023). Available at https://aag-it.com/the-latest-cyber-crime-statistics/.

[25] Brooks, C.: ”Cybersecurity Trends & Statistics For 2023; What You Need To Know” (2023). Available at https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends–statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/.

[26] Synopsys - ”Ethical Hacking”. Available at https://www.synopsys.com/glossary/what-is-ethical-hacking.html.

[27] Accenture - Available at https://www.accenture.com/us-en/insights/cyber-security-index.

[28] IBM - ”Cost of a Data Breach Report 2023” (2023). Available at https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258.

[29] Columbus, L.: ”Experts predict how AI will energize cybersecurity in 2023 and beyond” (2023). Available at https://venturebeat.com/security/experts-predict-how-ai-will-energize-cybersecurity-in-2023-and-beyond/.

[30] Synopsys - ”[2023] Open Source Security and Risk Analysis Report” (2023). Available at https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-2023.pdf.

[31] Kerner, S., M.: ”34 cybersecurity statistics to lose sleep over in 2023” (2023). Available at https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020.

[32] HackerOne - 6th Annual Hacker-Powered Security Report (2022). Available at https://www.hackerone.com/reports/6th-annual-hacker-powered-security-report.

[33] Verizon - ”2023 Data Breach Investigations Report” (2023). Available at https://www.verizon.com/business/resources/reports/dbir/.

[34] CompTIA - ”What is Ethical Hacking?”. Available at https://www.comptia.org/content/articles/what-is-ethical-hacking.

[35] Keshri, A.: ”Top 5 Penetration Testing Methodologies and Standards” (2023).
Available at https://www.getastra.com/blog/security-audit/penetration-testing-methodology/.

[36] ScienceDirect - ”Open-Source Security Testing Methodology Manual”. Available at https://www.sciencedirect.com/topics/computer-science/open-source-security-testing-methodology-manual.

[37] OWASP - ”Penetration Testing Methodologies”. Available at https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies.

[38] Penetration Testing Execution Standard. Available at http://www.pentest-standard.org/index.php/Main_Page.

[39] The Redscan Team - ”Types of Pen Testing: Black Box, White Box & Grey Box” (2022). Available at https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/.

[40] EC-Council Cybersecurity Exchange - ”Understanding the Five Phases of the Penetration Testing Process” (2022). Available at https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/.

[41] Basu, S.: ”17 Best Penetration Testing Tools 2023 (by Popularity)” (2023). Available at https://www.getastra.com/blog/security-audit/best-penetration-testing-tools/#sqlmap.

[42] Ben, G.: ”Different Types of Hackers: White Hat, Black Hat, Gray Hat, and More” (2023). Available at https://www.avg.com/en/signal/types-of-hackers.

[43] Buxton, O., Ghimiray, D.: ”Hacker Types: Black Hat, White Hat, and Gray Hat Hackers ” (2023). Available at https://www.avast.com/c-hacker-types.

[44] Panda Security - ”14 Types of Hackers to Watch Out For” (2023). Available at https://www.pandasecurity.com/en/mediacenter/14-types-of-hackers-to-watch-out-for/.

[45] Kanugarng, Gajjarnisag78: ”Types of Hackers” (2022). Available at https://www.geeksforgeeks.org/types-of-hackers/.

[46] NordVPN - ”Blue hat hacker”. Available at https://nordvpn.com/pt/cybersecurity/glossary/blue-hat-hacker/.

[47] Brathwaite, S.: ”The 7 Hats of Hacking”. Available at https://www.softwaresecured.com/post/the-7-hats-of-hacking.

[48] NordVPN - ”Gray hat hacker”. Available at https://nordvpn.com/pt/cybersecurity/glossary/gray-hat-hacker/.

[49] Gross, D.: ”Zuckerberg’s Facebook page hacked to prove security flaw” (2013). Available at https://edition.cnn.com/2013/08/19/tech/social-media/zuckerberg-facebook-hack/index.html.

[50] Gunnell, M.: ”Green Hat Hacker” (2023). Available at https://www.techopedia.com/definition/green-hat-hacker.

[51] NordVPN - ”Green hat hacker”. Available at https://nordvpn.com/pt/cybersecurity/glossary/green-hat-hacker/.

[52] Ilevičius, P.: ”What are nation-state actors?” (2022). Available at https://nordvpn.com/pt/blog/nation-state-threat-actors/.

[53] Radware - ”A Guide to State-Sponsored Cyberthreats” (2019). Available at https://www.radware.com/blog/wp-content/uploads/2019/12/rad1867_GuideToStateSponsoredCyberthreats_v6_FIN.pdf.

[54] Kaspersky - ”What is WannaCry ransomware?”. Available at https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.

[55] NordVPN - ”Hacktivism”. Available at https://nordvpn.com/pt/cybersecurity/glossary/hacktivism/.

[56] Zhaddan, A.: ”Who are Anonymous and why are they fighting alongside Ukraine?” (2023). Available at https://cybernews.com/editorial/who-are-anonymous-and-why-are-they-fighting-alongside-ukraine/.

[57] Sportinforma - ”Entenda o caso Football Leaks e o papel do português Rui Pinto” (2020). Available at https://desporto.sapo.pt/futebol/artigos/entenda-o-caso-football-leaks-e-o-papel-do-portugues-rui-pinto-2.

[58] NordVPN - ”Black hat hacker”. Available at https://nordvpn.com/pt/cybersecurity/glossary/black-hat-hacker/.

[59] FBI - ”Most Wanted: Evgeniy Mikhailovich Bogachev”. Available at https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev.

[60] NordVPN - ”Script kiddie”. Available at https://nordvpn.com/pt/cybersecurity/glossary/script-kiddie/.

[61] Euronews, Kaspersky: ”Meet the Script Kiddies: Teenage hackers who make or break our world” (2023). Available at https://www.euronews.com/next/2023/05/26/meet-the-script-kiddies-teenage-hackers-who-make-or-break-our-world.

[62] Stouffer, C.: ”What is a script kiddie? Definition + examples” (2023). Available at https://us.norton.com/blog/emerging-threats/script-kiddie.

[63] NordVPN - ”Whistleblower”. Available at https://nordvpn.com/pt/cybersecurity/glossary/whistleblower/.

[64] National Whistleblower Center - ”What is a Whistleblower?”. Available at https://www.whistleblowers.org/what-is-a-whistleblower/.

[65] Davies, D.: ”Edward Snowden Speaks Out: ’I Haven’t And I Won’t’ Cooperate With Russia” (2019). Available at https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia.

[66] Singer, P.: ”ethics - philosophy” (2023). Available at https://www.britannica.com/topic/ethics-philosophy.

[67] Encyclopaedia Brittanica - ”morality - human behaviour”. Available at https://www.britannica.com/topic/morality.

[68] Mcneal, R.: ”A novice just used ChatGPT to create terrifyingly sophisticated malware” (2023). Available at https://www.androidauthority.com/chatgpt-malware-3310791/.