UNIVERSIDAD FRANCISCO DE VITORIA

ESCUELA POLITECNICA SUPERIOR

FUNDAMENTALS OF COMPUTER ENGINEERING

Practical work I

29/09/2024

Security: Ethical Hacking

Group 3:

Juan Cisneros Amengual

Beltrán Espinosa de los Monteros de Uña

Karla Patricia Casillas Peñaloza

Jaime Felices García

Javier Fuentes Guzmán

Samuele Moranzoni

Borja Rincón Lozada

Table of contents

Table of figures

Abstract

In this practical work we explore ethical hacking as a crucial area of computer science. Due to its relationship with general hacking, ethical hacking is sometimes misinterpreted. It involves authorizing practices to identify and fix security vulnerabilities and flaws in digital systems. This work aims to define the functions of ethical hackers, investigate their resources and techniques and evaluate their impact in reducing cybersecurity threats.

The objectives include understanding the different types of hackers, distinguishing between ethical hacking from malicious practices, and assessing the need for ethical hackers in society. The work explores the techniques and tools, this includes malware analysis, vulnerability analysis. The work dives into tools such as Metasploit, Nmap and Nessus, which enable penetration testing. Additionally, the work also studies the advantages and disadvantages of ethical hacking, such as improves security, following legal requirements, and raise awareness, while also acknowledging its limitations such as possible services interruptions and privacy issues.

More in depth in the work, it addresses the evolving challenges and the new opportunities posed by technologies such as AI and IoT, emphasizing how these technologies can be used by both ethical hackers and cybercriminals (hackers). Ethical frameworks will be discussed in this paper as the EC-Council code, are cited as essential guidelines for ensuring the integrity of the field experts.

Through this analysis the paper emphasizes the growing necessity of ethical hacking in and in an increasingly digitalized world. It concludes with a reflection on the future of ethical hacking, specifically the incorporation of AI driven tools, which will enhance productivity but also raise new ethical questions.

Introduction

1.1 Motivation

For the search of the topic, each member proposed several topics, and we all have this topic in common, so the choice was quite simple. We have chosen this topic because it seems to us an interesting topic in relation to the subject we are taking. Hacking is a particularly important branch of computer science, and we consider it to be one of the fundamentals of it.

1.2 Objectives

Among the objectives of the work, we find the following points:

- Describe what a hacker is and the types there are (following their own ethical).

- What is ethical hacking?

- Why are ethical hackers necessary in our society?

- Advantages and limitations of ethical hacking.

- The future of this technology.

- Make a prediction of the potential that hacking has (currently and in the following years)

1.3 Practical Work Outiline

The paper begins by giving a detailed summary of the project. Furthermore, the skeleton of the project starts by giving a broad description of what ethical hacking is. In addition, we describe what a hacker is, including the diverse types of hackers that are nowadays according to their own ethical. To be more precise, we go on in depth about ethical hackers, and the tools most used by them.

Once this content has been explained, we will make a more general description: ethical hacking, what consists of, the technologies it uses and other described in more detail in this document.

Ethical Hacking

This section should include a short introduction about why this technology or topic has been researched or built or discovered.

2.1 Description of the technology/topic

In order to give an accurate description of Ethical hacking is important to know what a hacker is. According to the Cambridge dictionary “a person who is skilled in the use of computer systems, often one who illegally obtains access to private computer systems” (*Cambridge Free English Dictionary and Thesaurus*, 2024). With this definition in mind, hacking has become a serious problem over the years as technology keeps advancing, since hackers adapted by learning how to gain access to more complex Technologies, representing what could lead to a widespread catastrophe in the wrong hands. This is why ethical hackers have been appearing over the years, going back to the start of computer science, the first generation of hackers where computer engineers' university students that participated in the post-sputnik, cold war embrace of technology, the saw breaking into new, allegedly secure data as a challenge and a harmless prank. Consider White hat hackers, which we would explain in depth in the next point. But white hat hacking, also known as ethical hacking, uses the same tools, methods, and procedures as hacking, but it differs significantly in that they have been authorized to access the system by the owner. The primary goal is to identify and address security flaws before harmful hackers may take advantage of them.

As cyberattacks become more frequent and sophisticated, the role of ethical hackers has gained distinction. According to INFOSEC, there has been a 38% increase in cyberattacks year over year. In response, the market for ethical hacking services is expected to grow significantly from $3.4 billion in 2023 to $10.25 billion by 2028. (*Understanding Cyberattacks: Types, Risks And Prevention Strategies (2023) | Infosec*, s. f.).

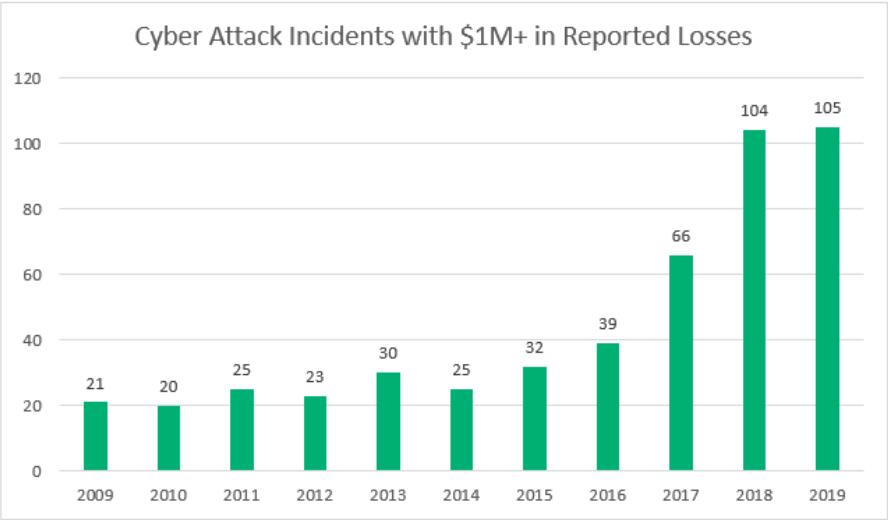

Figure 1 - Vertical bar chart cyberattacks losses per year - Source here

An example of this is the Equifax data breach in 2017. Equifax, one of the largest credit reporting agencies in the US, failed to patch a known vulnerability in its system, resulting in the exposure of personal data of 147 million people. Ethical hackers if they had been employed, they could have identified and fixed the vulnerability. (*Equifax Data Breach Settlement*, 2024)

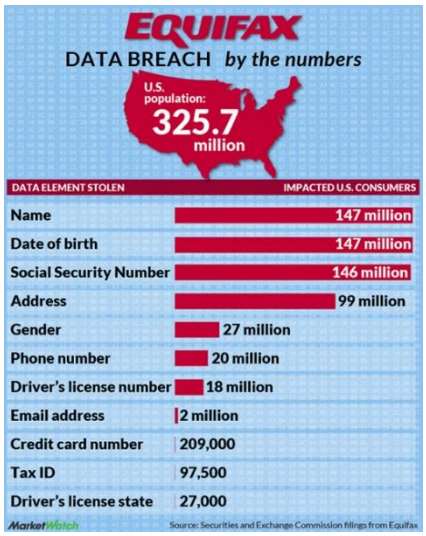

Figure 2 - Equifax Data Breach Settlement - Source here

Knowing the importance of ethical hackers and the threat that are hacker, it is also important to know the types of hackers, the mostly common hacker according to IBM known are (IBM, 2024):

- **White Hat hackers:** These are the ethical hackers who legally test systems to improve their security and detect liabilities in their systems.
- **Black Hat hackers:** Malicious hackers (cybercriminals) who break into systems without permission to exploit vulnerabilities for personal gain. When a black hat hacker discovers a security flaw, they attempt to take advantage of it by frequently installing malware like trojans or viruses.
- **Grey Hat hackers:** Hacker who operate in legal grey area by identifying vulnerabilities without permission, sometimes reporting them, but often raveling them publicly without malicious intent.

Figure 3 - Piechart intentions of each type of hacker - Source here

Technologies Used by Ethical Hackers

For ethical hackers to do their job they test with different technologies to identify any security breach and fix it, some of these tests are:

1. **Penetration test:** Ethical hackers simulate cyberattacks to identify weaknesses in security defenses. These controlled attacks mimic real-world scenarios, giving organizations the opportunity to fix vulnerabilities before black hat hackers exploit them.

The tools this test use are:

Metasploit: A widely used open source farmwork for penetration testing, allowing ethical hackers to test for vulnerabilities across the system and networks.

Nmap: A network scanning tool used to discover open ports and map the network's structure, making it easier to find weak points.

Burp Suite: A tool for evaluating the security of web applications, specifically useful for finding vulnerabilities such as SQL injections and cross-site scripting (XXS)

2. **Vulnerability Assessment:** White hat hackers use manual and automated tools to find and prioritize vulnerabilities within a system, providing organizations with a comprehensive list of potential risks.

The tools this test use are Vulnerability scanners.

Nessus: One of the most popular vulnerably scanners, designed to identify weaknesses such as outdated software or misconfigured settings.

OpenVAS: an open-source tool for detecting and managing security risks across a network.

3. **Malware Analysis:** Some white hat hackers specialize in analyzing ransomware and other types of malwares to understand how the malicious programs work and how to defend against them.

Tools Used:

IDA pro: A versatile disassembler tool, it supports multiple file types and architectures, offering a user-friendly interface and robust debugging feature to identify malicious code behavior.

Wireshark: A network traffic analysis that records and examines any suspicious activity patterns in order to identify and investigate malware that runs over networks.

4. **Risk Management:** Some hackers also assist in high level strategic risk management. They identify new and emerging threats, and they give a detailed analysis on how the company could counterpane the threats.

There can be other types of Technologies, and tools involve in ethical hacking such as:

Exploitation Frameworks: Platforms that create advance attack simulations often used to test the defense mechanism of an organization.

Password cracking tools: Tools used to test the strength of passwords.

Web security tools: tools used to find security vulnerabilities in web applications.

Social Engineering tools: They simulate social engineering attacks such as phishing and spear-phishing.

One of the most important roles of Ethical hackers is in an incident report. Since ethical hackers are increasingly involved in incident report efforts. When a security breach occurs, ethical hackers are often called upon to analyze and attack, determine how the breach happened, and recommend strategies to prevent future incidents. Their expertise in understanding the tactics of malicious hackers make them invaluable assets in post- breach investigations.

2.2 Advantages and limitations

Advantages of Ethical Hacking:

1) Identification of vulnerabilities in security systems:

Ethical Hackers adopt the same potential strategies used by malicious hackers into a legal framework. This strategy is useful to find potential security vulnerabilities that traditional security systems could not consider. Subsequently ethical hackers provide key insights in order to create more effective security systems.

2) Mitigation of Data Breach Risks:

A data breach occurs when unauthorized parties access sensitive and confidential information. A data loss occurs in a data breach and the data itself is destroyed.

Ethical hackers help companies to prevent harmful data breaches and associated data losses that may lead to huge financial and reputational damage. In fact, the expenses related to data breaches can directly include regulatory fines by GDPR (General Data Protection Regulation) , legal fees to deal with lawsuits, investigation costs and other major expenses. So it could be a good investment for a company to invest in ethical hacking.

Furthermore, this aspect is very important because it helps maintain trust between consumers,partners, and stakeholders so that their data are well-protected.

3) Help to fulfill conformity standards

Several companies are governed by strict conformity standards recognized as regulatory compliance that require regular security checks such as penetration testing, network vulnerability scan , security audits .Ethical hackers help check that all requisites are fulfilled by companies and allow them to avoid regulatory fines of non-standard conformity.

4) Improve securities knowledge and training

Ethical hackers within the companies train employees on the latest strategies used by malicious hackers to obtain sensible information. This training helps employees to recognise and respond efficiently to security threats and allows to create a better “security culture” within the companies.

Disadvantages and limitations of Ethical Hacking:

1) Potential Disruption of Services

When ethical hackers test the security of a system , they may need to push it to its limits , which can cause disruptions. This could be especially critical for some security systems supported by essential services, such as healthcare and banking .

2) Violation of individual’s privacy

When ethical hackers test a security system, they can access sensitive information such as medical records or financial data, which can itself be a privacy violation. Additionally, if the data is not properly handled, it is potentially exposed to malicious hackers even during the test phase.

3) Legal and company limitations:

Ethical hackers operate within a legal framework to avoid regulatory fines by the GDPR. They also can only test within the predefined boundaries set by the company. In addition some companies restrict certain testing methods that lead the servers to crash (e.g., denial-of-service (DoS) attacks)

These limitations restrict their ability to fully test systems, potentially leaving some vulnerabilities in some not-accessible areas. In fact malicious hackers don't have to face all these constraints and they can use more resources to attack a security system.

4) False positive and False Negative

A False Positive occurs when an ethical hacker identifies a threat that doesn't exist or harmless software as malicious. These misinterpretations could lead to unnecessary costs and disorders. On the other hand, a False Negative occurs when an ethical hacker is not able to recognize a threat or vulnerability by a system or tool. This type of result can be risky as it can allow threats and vulnerabilities to cause harm to security systems.

2.3 The future of the technology

The hackers and Cyber-attacks are a threat to the technology and the internet, in a world where the technology is constantly evolving and the internet is more and more important to us, with some advances like internet of things and AI, the world is each day near to a global digitalization.

With the new advances there will be new threats like:

- "Weaponized AI and machine learning: Malicious acts are increasingly leveraging AI and machine learning to automate attacks and personalize them for maximum impact." (MSys Technologies, 2024)

- "*Supply chain attacks:* targeting vulnerabilities in third-party software components embedded within larger systems." (MSys Technologies, 2024)

- "The rise of ransomware 2.0: ransomware attacks continue to plague organizations. Expect to see a rise in double extortion tactics, where attackers not only encrypt data but also threaten to leak it publicly adding a layer of reputational risk." (MSys Technologies, 2024)
- "The expanding attack surface: the exponential growth of connected devices within the internet of things creates a cast attack surface ripe for exploitation." (MSys Technologies, 2024)

To prevent these threats, ethical hackers are necessary. Ethical hackers test programs and servers to find any vulnerabilities, correct them and prevent the attacks of cyber criminals. In the future these threats will increase, and we will need more ethical hackers.

With the new Technologies we could implement new tools of ethical hacking, and new ways to prevent the hackers of exploiting any vulnerability like:

- **Automated ethical hacking:** this tool can learn from past tracks and detect new ones, finding weaknesses quickly and before it turns into a bigger problem, they also can go deep into the systems and find hidden threats that might be missed.

- **AI and machine learning:** AI can shift through tons of data in second and machine learning helps it learn that data to stay ahead of new threats, the AI also can predict the evolution the threat and use the information to anticipate new tactics hackers might use. But the AI can also be used by cybercriminals.

In conclusion Ethical hacking is a practice that will be needed in the future causing it to evolve with the new technologies to protect us and our information from cyberattacks.

2.4 The ethical view

On a daily basis, ethical considerations are one of the most relevant issues they have to deal with. Just by having the word "hacking" on the name of their occupation, generates disagreement between people outside of the cybersecurity world, because of the stigma attributed to the word "hacking". And their role if it's not correctly controlled/regulated the damage to the companies that hire this type of workers could be massive. This doesn't sound accurate if we only see one side of the coin, that are these people that studied specifically for this occupation and are really aware of the ethics they must follow, and have been educated for not corrupting themselves, this ethics will be seen more in advance. But we can't ignore the other side, that besides it is a considerably less popular option for companies, it's still as important as the other side, black hat hackers that start working with companies to improve their cybersecurity.

This is not something new created by this occupation, there are plenty of examples in other areas where criminals start working with big companies due to their skills, one of the most high-profile cases was about Frank Abagnale Jr, a counterfeiter that started working for the CIA because of his abilities to identify this type of felonies, the even made a movie about it. So many companies, despite knowing the implications of hiring a criminal for their staff,

even give these kinds of people CIOs or CISOs positions. So, they have to guarantee that the ethical code is solid and easy to understand and follow, not only for these restructured hackers but also the professional ones. As we know, every company has their own specific code of ethics based on their ideals, but there are 4 pillars that every company follow to create yours, it was presented by the (ISC)^2 (International Information System Security Certification Consortium) one of the most well-known cybersecurity organizations:

1. “Act honorably, honestly, justly, responsibly, and legally.”
2. “Provide diligent and competent service to principals.”
3. “Advance and protect the profession.”
4. “Protect society, the common good, necessary public trust and confidence, and the infrastructure”
   (*ISC2 Code Of Ethics*, s. f.)

We can consider these parameters to create a detailed ethical code that ensures that cybersecurity professionals act in a professional manner and do not harm others. So, when an ethical rule is planned to be added to an ethical code, most cases meet each of these specifications.

For example, one of the most recognized ethical codes in ethical hacking is the one proposed by EC-Council, we can take any ethical rule and put it through these four parameters and will meet all the specifications. Let's take one:

- “Use the property of a client or employer only in ways properly authorized, and with the owner's knowledge and consent” (EC-Council, 2024b).

It stands up for acting honorably, honestly, etc. It provides diligent and competent service to principals, it advances and protects the profession, and it protects society, the common good, etc.

And this could be done with every rule of their ethical code. Just to see where companies usually tend to go when creating ethical codes, let's see the whole code of EC-Council:

- Keep private and confidential information gained in your professional work, (in particular as it pertains to client lists and client personal information). Not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifier) to a third party without client prior consent.
- Protect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator.
- Disclose to appropriate persons or authorities potential dangers to any ecommerce clients, the Internet community, or the public, that you reasonably believe to be associated with a particular set or type of electronic transactions or related software or hardware.
- Provide service in your areas of competence, being honest and forthright about any limitations of your experience and education. Ensure that you are qualified for any project on which you work or propose to work by an appropriate combination of education, training, and experience.
- Never knowingly use software or process that is obtained or retained either illegally or unethically.
- Not to engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.
- Use the property of a client or employer only in ways properly authorized, and with the owner's knowledge and consent.
- Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.
- Ensure good management for any project you lead, including effective procedures for promotion of quality and full disclosure of risk.
- Add to the knowledge of the e-commerce profession by constant study, share the lessons of your experience with fellow EC-Council members, and promote public awareness of benefits of electronic commerce.
- Conduct oneself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in your knowledge and integrity.
- Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.
- Not to neither associate with malicious hackers nor engage in any malicious activities.
- Not to purposefully compromise or allow the client organization's systems to be compromised in the course of your professional dealings.
- Ensure all penetration testing activities are authorized and within legal limits. Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks.
- Not to be part of any underground hacking community for purposes of preaching and expanding black hat activities.
- Not to make inappropriate reference to the certification or misleading use of certificates, marks or logos in publications, catalogues, documents or speeches.
- Not convicted in any felony, or violated any law of the land.

Figure 4 - EC Council code of ethics - Source here

Apart from this ethical code, we have seen more, and apart from the previous rule, there are others that usually repeat in most ethical codes, such as protecting the data and information they are working with. As all data can be very dangerous if it gets in the wrong hands, ethical hackers should avoid keeping the data or doing something that would put data at risk.

But workers even having these long ethical codes, could still have problems because when they are working certain times they forget about few rules, and can make important mistakes that result in their layoff. Thats why many external sites encourage them to make certain general checks while working to avoid this, considering the ethical hacker’s limitations during their work time, such as computing power and budget, because ethical hackers often face constraints that malicious hackers don't. One of the most popular is the checklist proposed by “Hacking the box” which is the following one:

Figure 5 - Hacking the box checklist - Source here

We have seen why ethical codes are important, in which parameters could be based at the time of being created, a specific ethical code to have a general idea of how they are, and a checklist for ethical hackers while working to make sure they don't make silly mistakes.

But nowadays there are a lot of new tools that could affect future ethical considerations. We think the most relevant is the incredibly rapid progress with the AI revolution. As the future is unknown, we can only make suppositions on how the area of ethical hacking, specifically ethical considerations, could behave soon. But we can be sure there's going to be changes, because right now ethical hacking is evolving around AI.

There are several improvements such as boosting efficiency and accuracy, unveiling hidden vulnerabilities or enhancing collaboration and learning, but for us, the most significant one is auto healing, which was mentioned in the previous point. An AI doesn't need to rest, it only needs maintenance, it could be active 24 hours a day, running tests all day long, detecting and patching vulnerabilities, getting better every time, making the work of hackers a lot harder, which will result in a battle of who has the better AI, replacing human work. This would change the ethical considerations in the AI field, which is now making people struggle to define the ethic of using AI, and the limits it will have. It is in an early stage today, but we don't think they will set the AI free on their system, it probably be used as a tool, a very powerful one, but a tool at the end of the day, because it isn't “intelligent” like a person is, so the person behind will have the final word when decision making is required. But these are only suppositions.

Conclusions

Concluding this Practical work, it is important to talk about the difficulties we have faced as a team. There being seven people, we faced some problems related to organization. Because of the different schedules, finding time to sit down and organize the work became very difficult. We faced problems with making people's work fit together, each one of us had to search for information about the topic we had chosen, so making sure we didn't leave anything behind, or we didn't repeat the same thing was tough. For t5he next group activity it would be a good idea to make mini groups inside of our group and divide the people thinking about their schedules. That way we could organize the information in an easier way, and it would be easier to hold meetings with 2 or 3 people from the same classes instead of making 7 come together to organize the work.

Finishing the technical part, we conclude that although ethical hacking is not only important now, but its importance will only be greater in the future, this means that we really need to work on the moral issues that can make ethical hacking less ethical and more similar too common black hat hacking. Due to the growth of the number entities working online this new branch of cybersecurity is going to need an exponential growth of workers, the problem, is that by giving formation to became a white hat hackers we can also give future online criminals a lot of tools that can be very harmful for his future victims, doe to this we should create a system not to give formation to people that are going to use that information to perpetrate crimes in the future.

References

Univ. Fco. de Vitoria - Sign In. (s. f.). https://research.ebsco.com/c/knvu46/viewer/html/kowcnaeuoz

Are hackers who go to work for big companies considered sell outs or do they generally maintain respect within the hacker community? (s. f.). Quora. https://www.quora.com/Are-hackers-who-go-to-work-for-big-companies-considered-sell-outs-or-do-they-generally-maintain-respect-within-the-hacker-community

Cry0l1t, & CyberMnemosyne. (2022, 21 marzo). Ethics of ethical hacking: A pentesting team's guide (& checklist). *Hack The Box*. https://www.hackthebox.com/blog/ethics-of-ethical-hacking-a-pentesting-teams-guide-checklist

EC-Council. (2024, 14 noviembre). *Code of Ethics | EC-Council*. https://www.eccouncil.org/code-of-ethics/

Johansen, R. (2023, 13 octubre). *Ethical Hacking Code of Ethics: Security, Risk & Issues*. Panmore Institute. https://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues

The Rise and Fall of Sabu: From Hacker Hero to FBI Informant | Black Hat Ethical Hacking. (2023, 7 abril). Black Hat Ethical Hacking. https://www.blackhatethicalhacking.com/articles/the-rise-and-fall-of-sabu-from-hacker-hero-to-fbi-informant/

TraceSecurity, L. (2024, 13 noviembre). *What is Ethical Hacking?* TraceSecurity. https://www.tracesecurity.com/blog/articles/what-is-ethical-hacking

What is ethical hacking | Cybersecurity | CompTIA. (s. f.). CompTIA. https://www.comptia.org/content/articles/what-is-ethical-hacking

Academysecurium. (2024, 19 enero). How AI is Supercharging Ethical Hacking - Academysecurium - Medium. *Medium*. https://medium.com/@academysecurium/how-ai-is-supercharging-ethical-hacking-3c3ca1a6b9ec

What Is Ethical Hacking and How Does It Work? | Black Duck. (s. f.). https://www.blackduck.com/glossary/what-is-ethical-hacking.html#A

Mishra, V., & Mishra, V. (2024, 17 enero). The Legal and Ethical Aspects of Ethical Hacking: Understanding Your Responsibilities - E&ICT Academy, IIT Kanpur. *E&ICT Academy, IIT Kanpur - E&ICT Academy, IIT Kanpur*. https://eicta.iitk.ac.in/knowledge-hub/ethical-hacking/the-legal-and-ethical-aspects-of-ethical-hacking-understanding-your-responsibilities/

Manoj. (2024, 2 mayo). *Ethical Hacking in 2024: A Deep Dive into Emerging Trends and Technologies*. MSys Technologies. https://www.msystechnologies.com/blog/ethical-hacking-in-2024-a-deep-dive-into-emerging-trends-and-technologies/

Harshi, T. (2024, 24 agosto). *The Future of Ethical Hacking: Trends to Watch in 2024 and Beyond*. WebOrion Cyber Security And Vulnerability Assessment Services. https://theweborion.com/blog/future-of-ethical-hacking-trends-2024/

K, H. . . (2023, 19 diciembre). *ETHICAL HACKING:* https://www.linkedin.com/pulse/ethical-hacking-harini-k-ia7af/

TheKnowledgeAcademy. (s. f.). *What are the Benefits of Ethical Hacking: Explained*. https://www.theknowledgeacademy.com/blog/benefits-of-ethical-hacking/

GeeksforGeeks. (2024, 26 junio). *Advantages and Disadvantages of Ethical Hacking*. GeeksforGeeks. https://www.geeksforgeeks.org/advantages-and-disadvantages-of-ethical-hacking/