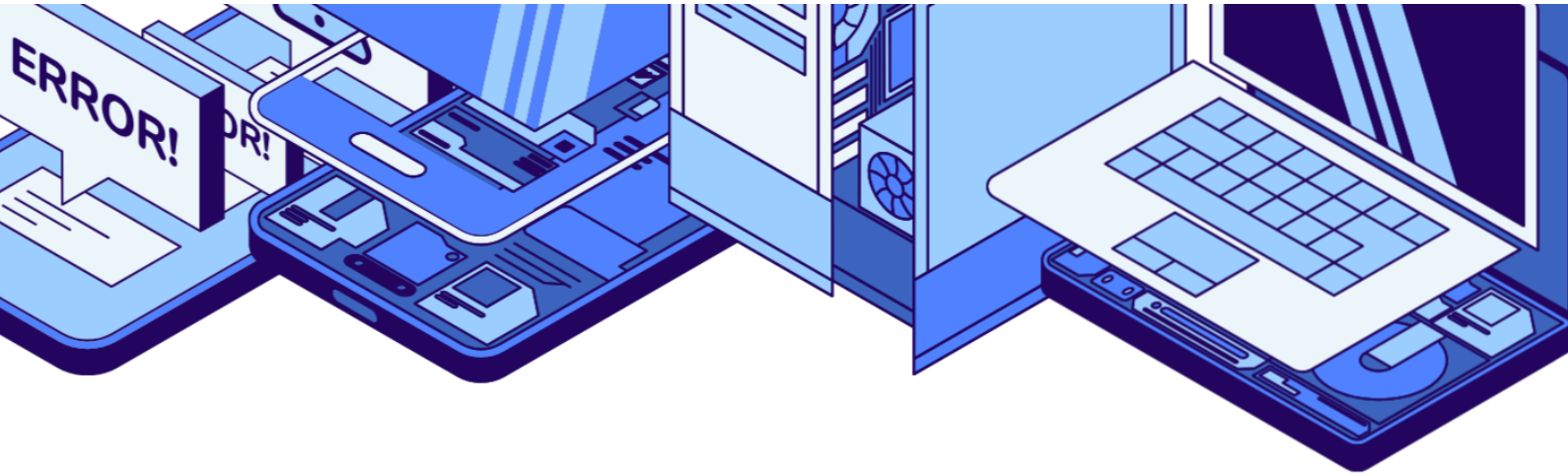

Proyect of

ETHICAL HACKING

A Business Perspective of the Small and Medium sized Enterprises

Group 5:
Israel de Pedro, Mauro Calderón, Pablo Bengoa, Pelayo Suárez, Julián Rero

Fundamentals of Computer Engineering | 2025

UFV

1. Introduction **3**
1.1 Motivation: 3
1.2 Specific Vocabulary: 3
1.3 Practical Work Outline 4
2. Ethical Hacking: A business perspective of the SMEs **5**
2.05 Short Introduction: 5
2.1 Description: 5
2.2 Advantages and Disadvantages: 10
2.3 The Future of the Technology 11
2.4 The Ethical View 13
3. Conclusion **15**
References: **16**

Abstract

This project analyzes ethical hacking from a business perspective, focusing on its relevance and application within small and medium-sized enterprises (SMEs). As digitalization continues to transform modern businesses, cybersecurity has become a decisive factor that is essential to consider. Ethical hacking, known as the authorized practice of testing and securing computer systems, plays a central role in detecting vulnerabilities before malicious actors exploit them.

The research explores how SMEs can benefit from implementing ethical hacking strategies, including penetration testing, threat analysis, and incident response. These techniques allow companies to strengthen their infrastructure while maintaining customer trust and data protection. However, the study also highlights several challenges, such as the financial and technical limitations that SMEs face when incorporating advanced cybersecurity measures.

Additionally, the project discusses the moral dimension of ethical hacking, underlining that the discipline depends not only on technical expertise but also on responsibility, transparency, and respect for privacy. The integration of emerging technologies such as Artificial Intelligence, IoT, and cloud computing, among others, will further expand both the opportunities and risks in this field, and will require a deeper level of control in the subject to ensure proper practice.

Ultimately, this work emphasizes that ethical hacking is more than a defensive tool if used correctly, it represents a cultural and strategic shift toward preventive cybersecurity, and a defense-by-offense mentality. By adopting ethical hacking practices, SMEs and others can enhance resilience, ensure compliance, prevent possible disasters, and ensure secure and safe information handling, inside and outside of the premises.

1. Introduction

In today's society, information is highly valuable, this has made cybersecurity fundamental for protecting it from external threats. Therefore, in this project, we will discuss ethical hacking and how it helps identifies and correct vulnerabilities in the computer systems

1.1 Motivation:

The motivation for researching this topic comes from our curiosity inspired by the cybersecurity course that we are currently studying. In particular ethical hacking, because of the practical and technical difficulties that it entails. Additionally, we want to examine how information affects people's daily lives,often without their awareness,both positively and negatively, and how to somewhat protect or prevent vulnerabilities.Most importantly to see how cyberattackers think and what motivates them to do what they do, knowledge that will be valuable for our future careers.

1.2 Specific Vocabulary:

Word	Definition
Network	Combination of two or more devices and the interconnecting links facilitating the transmission of information among them
Computer Network	Is a group of interconnected computers that enables communication between devices, allowing them to share resources, data, and applications seamlessly.
Endpoints	The devices connected to the network.
Attack vector	Routes, and methods that an attacker uses to gain unauthorized access.
Vulnerability	A weakness in that vector that can be exploited(make full use of and derive benefit from).
Pentesting (Penetration Testing)	Ethical and digital method of penetrating possible digital components of a company's digital structure.
Threat Hunting	All technical procedures to detect an inside threat, for more information about inside threat go to 2.4.
Mitigation Plan	It consists of endpoint quarantine, which involves disconnecting devices from the network; subnet isolation, which separates a group of devices from the network; and file deletion, which removes malware files
Log Collection	Log collection is the systematic gathering of event data from multiple digital systems such as firewalls, operating systems(OSes), applications, etc. To store and analyze it.
Structured Query Language(SQL) injection	Is a code injection technique used to modify or retrieve data from SQL databases. By inserting specialized SQL statements into an entry field, an attacker is able to execute commands that allow for the retrieval of data from the database, the destruction of

	sensitive data, or other manipulative behaviors (Cloudflare).
Cross Site Scripting(XSS)	Is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application (PortSwigger).
HyperText Transfer Protocol(HTTP) / HyperText Transfer Protocol Secure(HTTPS)	HTTP is a protocol used by browsers and servers to exchange web pages and data over the internet. It is the most common protocol for sending data between a web browser and a website. HTTPS is the secure variant of HTTP and is used to communicate between the user's browser and the website, ensuring that data transfer is encrypted for added security(GeeksforGeeks).
Cloud Services	Wide range of services delivered on demand to companies and customers over the internet. These services are designed to provide easy, affordable access to applications and resources, without the need for internal infrastructure or hardware. Examples: Netflix, One Drive, Microsoft365, etc (Citrix).
IT teams:	Staff that manages and supports an organization’s technology and systems.
GDPR (General Data Protection Regulation)	European Union law meant to reshape how personal data are collected and processed by giving all individuals living in the European Union new rights to access and control their data on the Internet (Koch, R.)

1.3 Practical Work Outline

The short introduction (2.05) explains the definition of ethical hacking from a business perspective, focusing on the Small Medium sized Enterprises (SME).
Section 2.1 describes how ethical hacking operates within the business perspective of an SME.
Section 2.2 clarifies and discusses the advantages and disadvantages of ethical hacking in SMEs.
Section 2.3 explores the existing and future challenges of this field.
Finally, section 2.4 examines the ethical perspective, explaining the moral difficulties and threats ethical hacking contains, highlighting the essentiality of ethical hacking for SMEs.

2. Ethical Hacking: A business perspective of the SMEs

2.05 Short Introduction:

Ethical hacking is the practice of defending digital assets against unauthorized access and/or digital attacks. The main objective is to provide security for the information and business continuity. Ethical hacking involves an eternal cycle that consists in three main stages.

3 Main Stages:	What does it consist of:	Examples:
Prevention	Preventing and reducing attacks with security measures and tests	Pentesting, employees continuous training, back-ups.
Detection	Being able to identify (if the intruder is inside) threats inside the system or suspicious activity.	Log collection, data analysis, anomaly detection, and threat hunting.
Response	Actions to contain and mitigate incidents after they happened, restore systems to their full capacity and improve future security.	Incident investigation, mitigation plan, file restoration.

2.1 Description:

To describe ethical hacking on SMEs, means to describe the most important methods ethical hackers use to prevent, detect, and respond to any source of digital attacks.

Types of cyberattacks:	**Short Description:**
Malicious Software (**malware**):	Software designed to cause harm or gain unauthorised access to a system: *Virus*: Spreads when executed by the user. It can have any objective, such as damage or data theft. *Worm*: Self-replicates and spreads automatically across systems or networks. *Trojan*: Appears to be legitimate software (a “Trojan horse”) but secretly performs malicious actions. Ransomware: Encrypts data and demands a ransom for decryption. Spyware: Monitors user activity, records keystrokes, or steals sensitive information.
Networks:	MitM (Man-in-the-Middle): Common on unsecured Wi-Fi networks. The attacker intercepts all the information transmitted over the network.

	DoS (Denial of Service)**:** Generates massive traffic to disrupt a service, network, or server.

Moreover, it is important to detail that today's most common attack on SMEs are phishing attacks. In fact, according to the UK government, over 90% of identified cyber crimes were of that matter.

Furthermore, UK businesses have experienced approximately 7.78 million cyber crimes of all types(which all have included phishing) and approximately 116,000 non-phishing cyber crimes in 2024 (UK Government 6.4).

Social engineering: user as the target.	Phishing**:** fraudulent emails designed to trick users into revealing sensitive information. Spear-phishing**:** a more sophisticated and targeted form of phishing. Smishing (SMS) and Vishing (voice call): phishing attempts delivered via text message or phone call. Spoofing: Identity theft. Email spoofing, Caller ID (phone) spoofing, Website or domain spoofing.

Regardless if the attack is successful or not, it is clear that the main vulnerability hackers are focusing on are phishing methods. However, there are still other ways and types of attacks an ethical hacker has to face.

Before moving on, it is important to also define a zero day. A zero-day attack target vulnerability that has no known patch or defense, making it impossible to stop at the time of the attack. The most important methods ethical hackers use to prevent, detect, and respond to any source of digital attacks to SMEs:

- **Prevention stage**:

The prevention stage explains the security methods to prevent and reduce cyber attacks. One is pentesting, which is used to identify, highlight, and ultimately mitigate vulnerabilities. It often measures the hackability of an organization's systems, networks or applications.

Attack vector:	**Pentesting**:
The user, through messaging, calling, email websites, or apps:	Testing the employees by using weekly social engineering attacks such as email spoofing, *typo-squatting(MITRE, ‘Acquire Infrastructure: Domains’), or caller ID.
The network infrastructure:	External: attacks from the outside of the organization's network perimeter. Internal: vulnerabilities within the internal network.

*Typo-squatting is a cyber attack technique registering a look-alike email address, domain name, or website; to the legitimate one. It exploits barely noticeable changes like common misspellings.

External Network Infrastructure:	**Internal Network Infrastructure**:
Web Servers and Applications: Checking for issues like SQL injection and cross-site scripting. Firewalls and Routers: Evaluating configurations to block unauthorized access effectively. Public IP Addresses and Domains: Scanning for open ports and services that could serve as entry points. Knowing which ports are open tells an attacker what programs are being used. Knowing the program lets the attacker choose the correct approach to test weaknesses. Passwords and credentials: attempting to obtain passwords by brute force, also dictionary attacks. Making sure a high percentage pass a test password strength, or multi factor authorization.	User Access Controls: Ensuring appropriate permissions and preventing privilege escalation. Network Segmentation: Verifying proper segmentation to contain breaches. If one endpoint gets hacked, make sure subnet isolation happens. Sensitive Data Protection: Identifying unsecured data accessible to unauthorized users. System Configuration and Patch Management: Checking that systems are up-to-date to mitigate known vulnerabilities. Insider Threat Assessment: Evaluating risks from employees or contractors who might misuse access. For more see 2.4.

Table 2.1, continuation of attack vector - pentesting, (Kovalenko)

Another method is the blue versus red team. This simulation strategy is based on pentesting in a superior and larger way. The following table explains it:

Red Team: Ethical hackers who simulate attacks against the organization	**Blue Team**: Responsible for protecting the organization's systems, networks, and data from attacks. They are the first line of defense, in charge of prevention, detection, and real-time response to threats.
*Objective***:** Test the effectiveness of the organization's defenses, identify weak points, and validate existing security measures. *Techniques*: Penetration testing / Adversary simulations / Social engineering to trick employees / Discover unknown security flaws, including zero-day vulnerabilities.	*Objective*: Build, maintain, and improve the organization's defenses. *Techniques*: Security monitoring / Vulnerability analysis / Incident management / Forensic analysis / Implementation of security measures: configuring and maintaining firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), etc.

Table 2.12, Blue vs Red Team, (CREST 5)

The implementation of cybersecurity hardware devices/software programs is a key role on the prevention stage. Ethical hackers will recommend and even install a cybersecurity

asset inventory. Focusing on SMEs we can divide in two groups the cybersecurity asset inventory:

- 1. Primary network perimeter tools for SMEs:

Technology	HW/SW - Location	Function:
Firewall	Both, and can be Hybrid. It is located at the network edge. At the point where the internal network connects to external networks.	Perimeter security: network traffic control and prevention of unauthorized access to a network. It is based on previous rules established. Monitoring and filtering of incoming and outgoing traffic between networks (North/South, East/West). Example: from the university to the internet: North–South. Within the university, between users: East–West. Layers 3/4 (Network/Transport): Examines packet headers — source IP, destination IP, port, and protocol. Security policies: “Allow / Deny” — rules that determine whether specific network traffic is permitted or blocked based on defined criteria.
Intrusion Prevention System (**IPS**)	Both, and can be hybrid. It is located after the firewall, behind it, “second line of defense”.	Active protection, detection, and blocks against malicious activity. Traffic monitoring to detect suspicious behavior patterns or known attack signatures. Threat blocking (malicious traffic). Layers 3 to 7(Network/Transport/Session/Presentation/Application), Deep Packet Inspection (DPI): examines both the header and the content of packets. Types: NIPS (Network-based Intrusion Prevention System): monitors traffic at strategic points in the network. HIPS (Host-based Intrusion Prevention System): installed on servers or individual computers.
Secure Web Gateway (**SWG**)	Software. Located in between the user and the network.	Intermediary between user and web server. Privacy and anonymity. IP masking (prevent tracking). Content filtering: Malicious or disallowed URLs. Layer 7 / Application-level (HTTP/HTTPS).

Additionally, employees who need to access their company's network from off-site locations or want to securely connect to a private network from a public area frequently use a remote access virtual private network (VPN).

Explanation of how a VPN works: “Remote access VPNs work by encrypting data sent between an external user and your organization's internal network. Regardless of the

user's location, remote access VPNs build private tunnels between a company's network and a remote user. Due to their encryption capabilities, remote access VPNs are considered the industry standard for remote security. Users can safely access and use company applications and resources as they would in the office" (Fortinet, n.d.).

Least but not less important tool, the Cloud Access Security Broker(CASB). A CASB is primarily a network perimeter - focused tool, whose objective is to extend enterprise security controls to Software as a Service(SaaS) solutions. Main functions:

- Visibility: CASBs give organizations insight into how cloud services are being used. They detect Shadow IT, which refers to apps or services used by employees without the organization's approval.

- Regulatory compliance: help ensure that the use of cloud applications complies with legal and industry regulations.

- Data protection: prevent data exfiltration(DLP); the unauthorized transfer of sensitive data outside the organization.

- Threat protection: protect against malware and other threats in cloud applications. It scans files.

- 2. Primary endpoint protection tools for SMEs:

Name:	**Antivirus (AV)**	**EPP (Endpoint Protection Platform)**	**EDR (Endpoint Detection and Response)**
Objectives:	Protect the single device.	Protects multiple devices.	Detect and respond to the attacks in the endpoints.
Reach:	Individual users, one endpoint.	All the endpoints from the network.	All the endpoints of the network.
Cyberattack:	Already known malware.	Known malware and possible zero days.	Advanced cybersattacks, ransomware, zero day, etc.

Finally, another prevention tool method would be: the back up information process. This is done to prevent any kind of malware that could put digital information in danger. Moreover employees will be trained to not fall on social engineering attacks such as phishing, smishing, or vishing.

- **Detection stage**:

Since the average of SMEs outsource the detection stage to external providers, this stage is mostly based on these three activities: log collection, data analysis, and anomaly detection. Which are manually performed by, if possible a technology department, or external provider.

Nonetheless sometimes the company will invest money on Managed Security Service Providers (MSSPs). It offers network security services to an enterprise. As a third party, an MSSP can alleviate the strain on IT teams, as well as free up crucial time the organization needs to support and expand operations.

Besides all of his functions the most important one for the detection stage is the: Managed detection & response (MDR). This service combines advanced tools and skilled analysts to detect, investigate, and respond to cyber threats in real-time. MDR is prepared for an organization's unique environment and security goals. This provides precise defense against advanced persistent threats (Fortinet).

- **Response stage**:

The response stage mainly focuses on: Incident investigation, mitigation plan, file restoration. The mitigation plan is usually performed by the EDR.

It does the following functions: endpoint quarantine, which involves disconnecting devices from the network; subnet isolation, which separates a group of devices from the network; and file deletion, which removes malware files.

The file restoration process is usually performed manually by restoring all the back ups created during the prevention stage. Moreover, the incident investigation is mainly done manually by ethical hackers, since forensics are needed to carefully understand how the zero day happened.

On top of that, the response stage finally creates a concise report for the authorities, to make sure higher rank national departments in cybersecurity can document and work on future solutions for zero days.

2.2 Advantages and Disadvantages:

Aspects	Advantages	Disadvantages
Security improvement Vulnerability identification	Detects system vulnerabilities before cybercriminals exploit them, strengthening overall defense mechanism(Berger and Jones, ACM Proceedings, 2016). Encourages proactive risk mitigation and ongoing system assessment(Tribbey, Old Dominion University, 2022). Provides SMEs with realistic insight into their current security posture(Alshehri and Alhamed, IEEE ComNet, 2024).	SMEs often lack the expertise or internal staff to interpret results or patch vulnerabilities effectively (Sukumar, Risk Analysis, 2023). May temporarily expose systems to instability during testing phases (Chhetri, University of Turku, 2025).
Cost efficiency Business continuity	Ethical hacking can prevent costly data breaches and operational downtime (Lloyd, Computer Fraud and Security, 2020).	Upfront costs for penetration testing or hiring ethical hackers can strain SME budgets (Tribbey, 2022).

	Long-term savings arise from identifying risks early, avoiding financial penalties and reputation damage (Arroyabe et al., Technology and society, 2024). Can reveal inefficiencies and optimize IT infrastructure for future growth (Berger and Jones, 2024).	Requires regular retesting and follow-up which may be financially unsustainable for smaller firms (Sukumar, 2023).
Regulatory compliance and reputation	Demonstrates commitment to data protection, helping SMEs meet GDPR, ISO or local data standards (Arroyabe et al., 2024). Builds customer and partner trust through transparent security practices (Lloyd, 2020).	Poorly executed tests could cause confusion or mistrust among clients if disclosed publicly (Tribbey, 2022). Some SMEs mismanage compliance documentation, reducing the perceived benefit (Sukumar, 2023).
Employee awareness and security culture	Highlights human factors in security, motivating employees to adopt better cybersecurity habits (Berger and Jones, 2016). Provides realistic training opportunities and phishing simulations for staff (Alshehri and Alhamed, 2024).	Without clear communication, ethical hacking can cause fear, stress or mistrust among employees (Tribbey, 2022). SMEs often lack training frameworks to capitalize on insights gained from ethical hacking(Chhetri, 2025).
Innovation and resilience	Encourages digital transformation by making SMEs more confident to deploy new technologies securely (Arroyabe et al., 2024). Fosters innovation in cybersecurity practices and tool adoption (Lloyd, 2020).	Reveals legacy systems or outdated technology that may require costly upgrades (Sukumar, 2023). SMEs may face difficulty integrating new security measures with existing IT infrastructure (Chhetri, 2025).
Third party Partner assurance	Ethical hacking reports offer evidence of robust security to partners, suppliers or investors (Lloyd, 2020). Builds credibility in competitive markets where cybersecurity assurance is a differentiator (Berger and Jones, 2024).	Overreliance on external consultants can inhibit internal skill development (Tribbey, 2022). Risk of sensitive information leakage if third-party testing is not carefully controlled (Sukumar, 2023).

2.3 The Future of the Technology

The future of ethical hacking for SMEs is defined by a fundamental strategic shift: moving beyond sporadic, isolated audits to embrace a continuous, collaborative model of security validation. This change is driven by the rapid evolution of technology, which leaves SMEs increasingly vulnerable to sophisticated cyber threats.

1. AI as the Future of Ethical Hacking: AI is reshaping the cybersecurity landscape, it is becoming an indispensable tool for both attackers and defenders. In the near future, failing to leverage AI for either offensive simulations or defensive measures will result in a significant strategic disadvantage.

Defensive AI:	**Offensive AI**:
➔ It is shifting from a reactive to a predictive model, focused on neutralizing threats before they can materialize ➔ AI systems analyze vast amounts of data to learn an organization's normal behavior. It detects anomalies that could indicate an attack. Furthermore, AI automates repetitive and time-consuming tasks, enabling human experts to focus on more complex strategic challenges.	➔ Cybercriminals are using AI to create more sophisticated attacks. Developing adaptive malware that can alter its behavior in real-time to evade traditional defenses. ➔ AI is also used to launch large-scale, highly convincing phishing campaigns, generating realistic deepfakes for social engineering purposes. ➔ It lowers the barrier to entry, enabling less technically skilled individuals to execute sophisticated attacks.

2. The Expansion of the Digital Attack Surface: the traditional concept of a secure network "perimeter" has become obsolete. The widespread adoption of technologies such as the Internet of Things (IoT) and cloud computing has created a vast and fragmented attack surface, introducing significant new security challenges and vulnerabilities.

IoT	**Cloud**
➔ The proliferation of IoT devices means that every connected camera, sensor, and smart device becomes a potential entry point for attackers. ➔ Many of these devices have inherent security weaknesses, such as default credentials or unpatchable firmware, which requires security strategies to be expanded beyond traditional endpoints.	➔ As organizations migrate to the cloud, the security focus must shift from protecting the network perimeter to safeguarding data and identities, regardless of their location. ➔ This paradigm shift is governed by the "Zero Trust" principle, which dictates that no user or device should be trusted by default and every access request must be verified.

3. The Democratization of Cybersecurity for SMEs: given the escalating threat landscape, advanced cybersecurity is no longer exclusive to large corporations. New delivery models, such as Security as a Service (SECaaS) and bug bounty platforms, are making enterprise-grade security services accessible and affordable for SMEs.

Security as a Service (SECaaS)	Bug Bounty Programs
➔ This model allows SMEs to outsource their security management to a specialized provider through a subscription-based service. ➔ Instead of making large capital investments in hardware and personnel, businesses gain access to enterprise-grade tools and expert management at a predictable operational cost, making it an ideal solution for small businesses.	➔ These programs operate on a pay-for-results model, where organizations reward ethical hackers for discovering and reporting valid vulnerabilities. ➔ This approach provides SMEs with access to a diverse, global pool of security talent and ensures continuous testing, offering a highly cost-effective and thorough alternative to traditional, time-boxed audits.

4. On-the-Horizon Trends: certain emerging developments, while not immediate threats for most SMEs today, are poised to fundamentally shape the long-term future of cybersecurity. These include the advent of quantum computing and the evolving regulatory landscape.

Quantum Threat	The new regulations
➔ The advancement of quantum computing poses a significant future threat to current cryptographic standards, as it could render many existing encryption algorithms obsolete. ➔ In response, the cybersecurity community is actively developing "Post-Quantum Cryptography" (PQC), a new generation of algorithms designed to be secure against attacks from both classical and quantum computers.	➔ The regulatory landscape is becoming stricter. For instance, the European Union's Directives mandates (General Data Protection Regulation) that many organizations, including medium-sized enterprises, report significant security incidents within 24 hours. ➔ This transforms ethical hacking from a recommended best practice into a legal necessity for demonstrating compliance and verifying the effectiveness of security measures.

2.4 The Ethical View

Ethical hacking follows certain principles based on the protection of highly valuable information. As a result, protecting information ultimately means defending human rights such as privacy, and security. Therefore, it helps prevent harm, promote trust within society and the company, and ensure business continuity.

The fundamental principles of cybersecurity and ethical hacking are the core for any ethical hacking procedure. This are the most important:

Confidentiality:	Integrity:	Availability:

The information is only accessible for authorized people.	Guaranteeing no modified / manipulated data.	Information and software would be accessible when needed.

Table 2.4, (“Confidencialidad, Integridad y Disponibilidad”).

Unfortunately, sometimes ethical hacking has not followed these principles. Members of cybersecurity companies had exploited their ethical hacking skills in many ways for evil. These members are commonly referred to as insider threats.

To prevent these events from happening, cybersecurity companies have established less software privileges to certain workers. Moreover, not only privileges rules, but tools are essential to prevent insider threats. The most important one is the Security Information and Event Management(SIEM).

To understand the detection tool SIEM and its vital function, an anomaly is defined in the table below as a suspicious relationship between data indicating unusual activity compared to the typical online behavior of an employee. SIEM detects insider threats when they are on their way to steal or share privileged information, or gain unauthorized access to data. The table below illustrates step by step how the system works:

1. **Data collection**	2. **Data normalization**	3. **Correlation**	4. **Alerts**
Detects all sources of data such as network devices, endpoints, etc.	Converts all data from the sources into a common standard format	Rule-based catalogs and behavioral analysis identify patterns in the data.	The system focuses on notifying potential issues by detecting behavioral anomalies.

Table 2.41, (“González-Granadillo et al. 2021”).

Additionally, companies have also fixed these issues by applying social tools. The most common social tools consist of internal report channels made up by groups of workers where detected anomalies feedback are reported.

Another common social tool is interviewing and testing the future or current employees. By observing their past behavior, ethical culture, and moral principles, it becomes easier to declare who should remain in the company.

Therefore, Ethical Hacking is a tool that will generate positive results if used correctly, and the risk it poses is mostly controlled thanks to: software and social tools, and the hierarchy of privileges.

3. Conclusion

Concluding, we have explored ethical hacking from a business perspective, focusing on its importance, challenges, and ethical implications for small and medium-sized enterprises (SMEs). In the current and increasingly digital world, information has become one of the most valuable assets a company possesses, and ethical hacking stands as a proactive and essential practice to protect that asset.

The research showed that ethical hacking not only identifies vulnerabilities but also strengthens the digital infrastructure and resilience of organizations. By applying techniques such as penetration testing, continuous monitoring, and threat hunting, SMEs can anticipate and respond effectively to cyberattacks, reducing risks and ensuring business continuity.

Despite its advantages, it is also necessary to recognize the limitations and potential ethical dilemmas that arise from its misuse, emphasizing the need for professional integrity and adherence to cybersecurity principles such as confidentiality, integrity, and availability.

Furthermore, the future of ethical hacking will be deeply influenced by emerging technologies like Artificial Intelligence, cloud computing, and the Internet of Things (IoT). These innovations will redefine the role of ethical hackers, transforming the concept from occasional audits to continuous, collaborative cybersecurity models. SMEs will increasingly adopt solutions such as Security as a Service and Bug Bounty programs, making cybersecurity more accessible and efficient.

In conclusion, ethical hacking represents not only a technical necessity but also an ethical and strategic commitment. For SMEs, investing in cybersecurity is no longer optional, it is a necessary step toward sustainable growth, customer trust, and long-term survival.

References:

- **1.3 Specific Vocabulary**:

Cloudflare. *SQL Injection | What is SQL Injection?* Cloudflare, https://www.cloudflare.com/learning/security/threats/sql-injection/. Accessed 1 Nov. 2025.

PortSwigger. *Cross-Site Scripting (XSS)*. Web Security Academy, PortSwigger Ltd., https://portswigger.net/web-security/cross-site-scripting. Accessed 1 Nov. 2025.

GeeksforGeeks. *Explain Working of HTTPS*. GeeksforGeeks, 16 Oct. 2025, https://www.geeksforgeeks.org/html/explain-working-of-https/. Accessed 2 Nov. 2025.

Citrix. "What Is a Cloud Service?" *Citrix*, https://www.citrix.com/glossary/what-is-a-cloud-service.html. Accessed 2 Nov. 2025.

Koch, Richie. *"What Does GDPR Stand For?" GDPR.eu, https://gdpr.eu/what-does-it-stand-for/*

- **2.1 Description**:

UK Government. *Cyber Security Breaches Survey 2024*. GOV.UK, 2024, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024. Accessed 1 Nov. 2025.

MITRE. "Acquire Infrastructure: Domains." MITRE ATT&CK, MITRE Corporation, 21 Apr. 2023, https://attack.mitre.org/techniques/T1583/001/. Accessed 20 Oct. 2025.

Kovalenko, Olga. *Network Penetration Testing: All You Need to Know*. Iterasec, 17 Oct. 2024, https://iterasec.com/blog/network-penetration-testing-complete-guide/?utm_source=chatgpt.com. Accessed 1 Nov. 2025.

CREST. *A Guide to Penetration Testing 2022*. CREST Approved, 2022, pp. 1–56. https://www.crest-approved.org/wp-content/uploads/2023/04/A-Guide-to-Penetration-Testing-2022.pdf

Fortinet. "Remote Access VPN." *Fortinet*, https://www.fortinet.com/resources/cyberglossary/remote-access-vpn. Accessed 2 Nov. 2025.

Fortinet. "What Is an MSSP?" *Fortinet*, https://www.fortinet.com/resources/cyberglossary/what-is-mssp. Accessed 2 Nov. 2025.

First-year Computer Engineering course: Introduction to Cybersecurity, taught by Juan José Parra Bonilla.

- **2.2 Advantages and disadvantages of ethical hacking**:

Arroyabe, Marta F., et al. "Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives." Computers & security 141 (2024): 103826. https://www.sciencedirect.com/science/article/pii/S0167404824001275

Berger, Hilary, and Andrew Jones. "Cyber security & ethical hacking for SMEs." Proceedings of The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society. 2016. https://dl.acm.org/doi/abs/10.1145/2925995.2926016

Lloyd, Guy. "The business benefits of cyber security for SMEs." Computer fraud & security 2020.2 (2020): 14-17. https://www.magonlinelibrary.com/doi/abs/10.1016/S1361-3723%2820%2930019-1

Sukumar, Arun, Hannan Amoozad Mahdiraji, and Vahid Jafari-Sadeghi. "Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors." Risk Analysis 43.10 (2023): 2082-2098. https://onlinelibrary.wiley.com/doi/full/10.1111/risa.14092

Tribbey, Nygia. "The Impact of Ethical Hacking within Small Businesses." (2022). https://digitalcommons.odu.edu/covacci-undergraduateresearch/2022fall/projects/16/

Alshehri, Jawaher, Almaha Alhamed, and Mounir Frikha. "Planning for Penetration Testing in Small & Medium Enterprises: Challenges and Best Practices." 2024 IEEE Eleventh International Conference on Communications and Networking (ComNet). IEEE, 2024. https://ieeexplore.ieee.org/abstract/document/10987546

Chhetri, Bhuwan. "Penetration Testing in Small and Medium-Sized Enterprises." (2025). https://www.utupub.fi/bitstream/handle/10024/182754/Chhetri_Bhuwan.pdf?sequence=1

- **2.3 The Future of the Technology**:

Bardají, Eduard. "Concepto Bug Bounty. ¿Qué Es y Por Qué Lo Necesitamos?" ESED, www.esedsl.com/blog/concepto-bug-bounty-que-es-y-por-que-lo-necesitamos. Consultado el 24 oct. 2025.

"Bug Bounty: Cómo Funciona el Hacking Ético en la Cacería de Vulnerabilidades." WeLiveSecurity, 21 enero. 2020, www.welivesecurity.com/la-es/2020/01/21/bug-bounty-como-funciona-hacking-etico-caceria-vulnerabilidades/.

"Cazadores de Recompensas Cibernéticas: Cómo los Programas de Recompensas por Errores Mantienen Segura a Su Empresa." Integrity360, insights.integrity360.com/es/cyber-bounty-hunters-how-bug-bounty-programmes-keep-your-business-secure. Consultado el 24 oct. 2025.

"¿Cómo Afecta la IA en la Propagación de los Ataques Cibernéticos?" Logicalis, 23 oct. 2023, *www.la.logicalis.com/es/Como-afecta-la-IA-en-la-propagacion-de-los-ataques-ciberneticos*.

"Directiva NIS2: El Nuevo Estándar de Ciberseguridad en la UE." Tecalis, *www.tecalis.com/es/blog/nis2-nis-2-directiva-ciberseguridad-aprobacion-cumplimiento-requisitos-medidas-sri2-normativa*. Consultado el 24 oct. 2025.

Intigriti - Global Crowdsourced Security Provider. Intigriti, www.intigriti.com/. Consultado el 24 oct. 2025.

Muncaster, Phil. "Las PYMES son Blanco Fácil del Ransomware." WeLiveSecurity, 22 sep. 2025, *www.welivesecurity.com/es/seguridad-corporativa/pymes-pequenas-empresas-mas-probabilidades-ataque-ransomware/*.

"Noticias Sobre Bug Bounty." Epic Bounties, www.epicbounties.com/es/news. Consultado el 24 oct. 2025.

"¿Qué es la búsqueda de amenazas?" IBM, www.ibm.com/es-es/think/topics/threat-hunting. Consultado el 24 oct. 2025.

"¿Qué es la Seguridad Como Servicio (SECaaS)?" Fortinet, www.fortinet.com/lat/resources/cyberglossary/security-as-a-service. Consultado el 24 oct. 2025.

Secur0 - Hackea Con Recompensas. Secur0, secur0.com/. Consultado el 24 oct. 2025.

"Tendencias Emergentes en Ciberseguridad Para 2025: Nuevas Amenazas y Tecnologías." Cybereop, www.cybereop.com/blog/tendencias-emergentes-en-ciberseguridad-para-2025-nuevas-amenazas-y-tecnologias.html. Consultado el 24 oct. 2025.

First-year Computer Engineering course: Introduction to Cybersecurity, taught by Juan José Parra Bonilla.

- **2.4 The ethical view**:

“Confidencialidad, Integridad y Disponibilidad.” *Ciberseguridad*, Universidad Pontificia Comillas, 8 May 2023, https://ciberseguridad.comillas.edu/confidentiality-integrity-and-availability/.

González-Granadillo, Gustavo, Susana González-Zarzosa, and Rodrigo Diaz. “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures.” *Sensors*, vol. 21, no. 14, 2021, article 4759. MDPI, DOI:10.3390/s21144759.