LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Synergies in the Cybersecurity profession

Exploring the Interplay of Hard Skills, Soft Skills, and Team Organization in Penetration Testing

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Alexander Bengtsson
Elias Sirviö

Handledare: Nicklas Holmberg

Rättande lärare: Paul Pierce, Umberto Fiaccadori

Synergier i cybersäkerhetsyrket: En undersökning av samverkan mellan hårda färdigheter, mjuka färdigheter och teamorganisation inom penetrationstestning

ENGELSK TITEL: Synergies in the Cybersecurity profession: Exploring the Interplay of Hard Skills, Soft Skills, and Team Organization in Penetration Testing

FÖRFATTARE: Alexander Bengtsson och Elias Sirviö

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, Docent

FRAMLAGD: maj, 2024

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 54

NYCKELORD: Cybersecurity, Computer Security, Penetration Testing, Skills, Abilities, Team Organization, Collective Efficacy, Information Systems

SAMMANFATTNING (MAX. 200 ORD):
This thesis investigates the enhancement of technical tasks in penetration testing through the integration of soft skills, contrasting them with hard skills within the cybersecurity profession. The research utilized a conceptual framework developed for this study, alongside empirical data gathered from semi-structured, qualitative interviews with 3 penetration testers and 2 information security specialists. The main finding is that while both soft and hard skills are essential for the profession, soft skills significantly enhance the effectiveness of technical tasks. Effective communication is identified as an element that improves technical execution in both traditional work settings and more flexible environments. Soft skills were found to not only promote better teamwork but also to strengthen the management of client relationships and project coordination. This study demonstrates that soft skills are integral to optimizing technical processes in penetration testing, facilitating better outcomes in various work scenarios.

Table of Contents

List of Figures

List of Tables

1 Introduction

The structure of this thesis is as follows. Chapter 1 argues for a problem affecting penetration testing professionals and presents the research question of this study. Chapter 2 presents a conceptual framework for penetration testing. Chapter 3 explains the study's interview research methodology. Chapter 4 presents the gathered data, whilst chapter 5 compares the previous academic literature with the data. Finally, chapter 6 draws this study's conclusions.

This first chapter will start this thesis by explaining the foundational background to the problem. The problem is about individuals who practice penetration testing and how they value hard and soft skills. Penetration testing is a specific type of offensive cybersecurity.

1.1 Background

This thesis argues that the field of offensive cybersecurity, specifically penetration testing, is ripe for further academic exploration. Penetration testing, a key component of offensive cybersecurity, involves authorized simulated attacks on a system to identify vulnerabilities. This is a proactive security measure in contrast to a reactive defense measure.

The demand for skilled cybersecurity professionals, particularly penetration testers, is rising as cyber threats become more complex and pervasive. Researchers like Towhidi & Pridmore (2023) and Withers et al. (2020) have identified a growing need for individuals who are not only technically proficient but also adept in soft skills such as communication, teamwork, and ethical decision-making. These skills are crucial for effectively identifying and mitigating security risks, yet they are often undervalued in the traditional technical-centric view of cybersecurity.

Based on the previous literature, there is a debate about what defense and offense are within cybersecurity, where little attention is given to the nuanced skills required in offensive roles. This study aims to focus on both the hard and soft skills essential in penetration testing. The interplay between these skills and their impact on the practice of penetration testing remains underexplored, with a lack of rigorous scientific evidence supporting the effectiveness of integrating soft skills into technical training.

To begin, it's essential to define penetration testing itself. According to Happe & Cito (2023), penetration testing is a security assessment designed to identify and fix vulnerabilities before they are exploited by malicious actors. This study will utilize this definition initially, as a jumping-off point. Penetration testers typically utilize methodologies such as those outlined in the OWASP penetration testing guides, which test if systems are vulnerable to the most

common attack vectors, such as those listed in the OWASP Top 10 (OWASP, 2021). Among the vulnerabilities listed in the OWASP Top 10, notable examples include Broken Access Control, Cryptographic Failures, and Injection. OWASP describes (2021) that Broken Access Control typically allows unauthorized users to access privileges usually reserved for administrators, among other security issues. Cryptographic Failures refers to the use of outdated or insecure cryptographic methods. Injection vulnerabilities occur when user-supplied data is not properly sanitized or parameterized, which could allow malicious SQL queries to access or modify data, among other potential risks.

Happe & Cito (2023) argue that it is important that a given system can protect itself from malicious actors. They argue that this practice of penetration testing requires that individuals or teams are organized and equipped with the right technology measures. This thesis argues that the correlation between the soft skills and hard skills of a team, or individual, should be examined. The effects this correlation has within the practice of penetration testing lacks a rigorous body of scientific evidence. This thesis seeks to contribute to the body of knowledge surrounding penetration testing, as a part of the broader information systems (IS) research domain.

The information systems (IS) research discipline, defined by Recker (2021) and Oates et al. (2022) as concerned with the development and use of information systems by various entities, provides a fitting definition for this study. It emphasizes the socio-technical systems aspect, wherein both social and technical skills play a critical role. This thesis argues that a deeper understanding and clear indexing of hard and soft skills are necessary to better prepare individuals and teams for the complexities of penetration testing.

This thesis will use the specific term 'penetration testing' throughout, focusing solely on this practice without referring to synonymous terms such as 'ethical hacking' or 'white hat.' This focused approach will help clarify the thesis's scope and contribution to the understanding of the socio-technical skills required in penetration testing. The figure below indicates that penetration testing is a specific area within offensive cybersecurity and general cybersecurity. It signifies that the focus of this study is mainly on penetration testing.

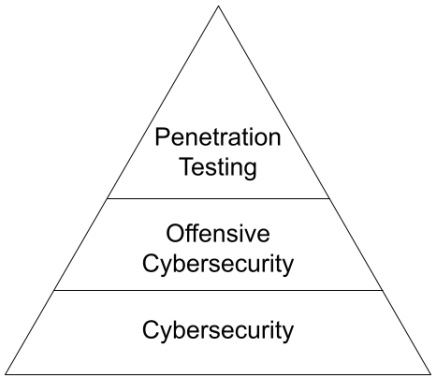

Figure 1.1: Penetration testing as a narrow focus area of cybersecurity

1.2 Problem Statement

This thesis identifies a critical gap in the understanding of essential interpersonal (soft) skills for effective penetration testing, a critical profession within the field of cybersecurity. While technical (hard) skills are well recognized and emphasized, the equally vital soft skills remain largely underestimated and misunderstood. This gap poses a risk as it leads to a shortage of penetration testers who are adept not only technically but also in essential soft skills. Examples of soft skills are communication or ethical judgment.

There is less previous literature on the specific skill demands of penetration testing. Despite the diverse nature of cybersecurity roles discussed by Dawson and Thomson (2018), Zantua et al. (2018) argue that traditional cybersecurity categories defined by the NICE framework are inadequate to fully encompass penetration testing roles, highlighting a notable deficiency in focused research (The NICE framework will be discussed in the next chapter). This inadequacy is particularly concerning given the profession's use of technologies and methods also employed by malicious actors, as argued by Ledin (2011). “We cannot protect ourselves from what we do not know. We must not remain stuck in a weak, purely reactive, defensive mode” (Ledin, 2011, p. 33). Sharif & Mohamed (2022) argues that the lack of general cybersecurity in 2020 cost the global economy, a sum of $945 billion. An indication that the costs on people, as a global whole, are tremendous.

The role of soft skills in effectively detecting and mitigating vulnerabilities is slowly increasingly recognized. Jones et al. (2018) highlights the substantial economic impacts of cybersecurity breaches, underscoring the need for penetration testers who can navigate complex interpersonal dynamics as well as technical challenges. This thesis underscores the pressing need for a deeper understanding of both hard and soft skills in the penetration testing field. There is still an underestimation of interpersonal skills in this traditionally technical profession.

1.3 Research Question

How do soft skills enhance the effectiveness of technical tasks in penetration testing?

1.4 Purpose

The primary purpose of this thesis is to address a significant academic gap on the topic of hard and soft skills in the profession of penetration testing. Especially on the interplay and relative importance of them. Unlike previous research, which predominantly identifies and evaluates these skills in isolation, this study will create a conceptual framework constructed from a review of existing literature. This framework will help analyze how these skills are valued individually, and also how they interact and influence each other in real-world scenarios.

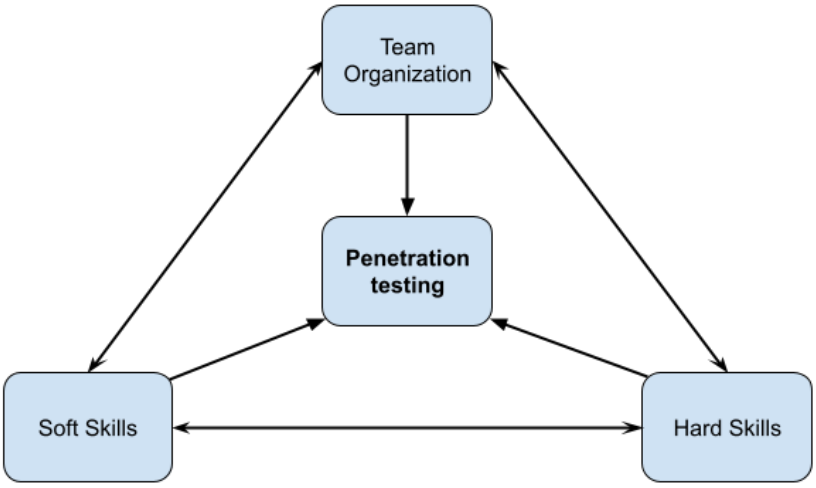

Figure 1.2: The conceptual framework

This framework will be compared with results gathered from interviews with experienced penetration testers and information security experts. This will allow a unique examination of how these skills are balanced and operationalized by individuals within penetration testing teams. This study will focus on assessing which combinations of skill sets are deemed most valuable for effective practice, aiming to elucidate the interplay between hard and soft skills and how they jointly contribute to the proficiency and adaptability of penetration testers.

By exploring this interplay, this thesis seeks to offer deeper insights into the complex skill landscape of penetration testing, providing a nuanced understanding that can guide training and professional development in the field. The outcome of this research is expected to clarify the combined effects of hard and soft skills. This will show their collective impact on successful penetration testing operations and inform curriculum development for future cybersecurity professionals.

1.5 Delimitations

The delimitations' aims are to focus the scope and scientific output of this thesis. Due to the wide breadth of the topic of general cybersecurity, the focus of this study is simply on the profession of penetration testing. This focus means that this study will not concern itself with other topics within general cybersecurity. This study is limited to the academic discipline of information systems. Any literature or discipline that does not contribute to answering the research question directly will be disregarded. Mainly literature from the academic disciplines of Information Systems, and Computer Science will be used. But only if the given academic literature contributes to the research question and relates to penetration testing.

2 Literature Review

In this chapter, a conceptual framework on team organization, soft skills, and hard skills will be presented. The sourced literature draws primarily from previous research in the information systems discipline. In other cases, it draws from related articles from the computer science discipline. The literature review consists of three main factors. These will help to interpret the study's research question once it is compared with the empirical data.

2.1 Team Organization of Penetration Testers

By understanding the team organization factor, one can then better put the soft skills into the right context. To understand how penetration testers work, it's also important to understand where they work. This study will initially follow the definition of a team, as follows. "A team can be defined as a social system of three or more people, which is embedded in an organization..." (Hoegl & Gemuenden, 2001, p. 436). Below are the most commonly identified types of employment where penetration testers work.

2.1.1 In-House Teams

In instances of security breaches, penetration testers within in-house teams take the lead in incident response and forensic analysis, as discussed by Happe and Cito (2023). Their skills are crucial in containing breaches, analyzing their origins, and understanding their impact, which is essential for preventing future incidents and for legal proceedings against attackers. Withers et al. (2020) notes that a continuous improvement in in-house security measures is driven by penetration testers. They monitor the evolving cybersecurity landscape to anticipate new threats. Their recommendations for advanced security technologies and methodologies ensure that the team's defenses remain resilient against emerging cyber threats.

2.1.2 Consulting Teams

According to Hartley (2015), penetration testing in cybersecurity consulting roles are distinct individuals who protect clients through specialized services like vulnerability assessments and incident response. Penetration testing as a consulting role benefits from exposure to a range of technological environments and security scenarios within different firms, broadening their experience. Hartley (2015) continues to underscore the act of penetration testing in externally reviewing and auditing existing information security to evaluate its effectiveness. This provides consulting teams with the necessary information to implement the right measures.

2.1.3 Bug Bounty Programs

Noordegraaf & Weulen Kranenbarg (2023) describes bug bounty programs, also known as Coordinated Vulnerability Disclosure (CVD), as providing an opportunity for penetration testing to improve the security of software and systems by identifying and reporting vulnerabilities. These programs are based on testers' own initiative by having an open invitation for penetration testers to find security flaws in exchange for reward or recognition. This leverages the collective expertise of the penetration testing community to enhance security and has proven to be effective. Certain protective legislation, like in the United States, has taken measures to offer penetration testers freedom from prosecution to help this type of program.

2.1.4 Collective efficacy and self-efficacy

The previous three points have presented common types of employment. The following text is dedicated to examining how teams actually affect performance. A study by Yoo et al. (2020) highlights the pivotal role of collective efficacy in enhancing the team effectiveness of cybersecurity measures. Collective efficacy refers to the shared belief among team members in their combined ability to execute tasks and achieve goals effectively. This concept can be argued to be particularly relevant to penetration testing teams where individual technical skills and collaborative team efforts determine the success of security operations.

Individual self-efficacy, defined as an individual's confidence in their ability to perform specific tasks effectively, is crucial in shaping collective efficacy within cybersecurity teams. As highlighted by Yoo et al. (2020), in the realm of cybersecurity, where challenges are both complex and continuously evolving, the self-efficacy of each team member is fundamental. It empowers professionals to proactively address threats, swiftly adapt to emerging technologies, and confidently implement robust security measures. This individual confidence collectively enhances the team's overall capability, significantly impacting the team's ability to execute cybersecurity protocols and respond to security incidents effectively.

Yoo et al. (2020) continues and demonstrates that teams characterized by high collective efficacy, which is partly built upon the self-efficacy of individual members, are better prepared to manage the complexities and dynamic challenges inherent in cybersecurity. This effectiveness is primarily attributed to the team's enhanced capacity for cooperation and mutual support. Such traits enable teams to operate more cohesively and respond more effectively to incidents, highlighting the importance of soft skills—such as communication, coordination, and mutual support—in fostering robust collective efficacy. This is further supported by Cheng & Yang (2014) where they discover that high quality interaction is an important factor in best utilizing all the skills present in a team (team knowledge). Thus, high quality interaction requires good communication and social skills. Cheng & Yang (2014) argue that teams without high quality interaction won't be able to utilize the team knowledge as team members will not balance each other's strengths and weaknesses and be able to identify group experts.

By understanding and fostering collective efficacy, individuals can better organize their penetration testing teams to optimize both individual and collective performance. This approach not only improves the technical handling of security tasks but also enhances the soft skills that are essential for successful team dynamics.

2.2 Soft Skills

Penetration testing seemingly demands many technical skills. However, penetration testing also requires a robust set of soft skills. While hard to define, the soft skills can be defined, according to Towhidi and Pridmore (2023), as critical thinking, problem-solving, and written and verbal communication. These definitions have been chosen as a starting point but will naturally progress as the literature offers many other definitions of soft skills.

2.2.1 Communication

'General communication skills,' as a metric, was the number one most important soft skill recognized in a questionnaire study by Jones et al. (2018), followed by the metric of 'written communication'. "Communication was by far the most important soft skill that cyber professionals found important for their job." (Jones et al. 2018, p. 10). According to Hartley, 2015), penetration testing is not just about technical prowess. Soft skills, such as communication and ethical judgment, are crucial. Jones et al. (2018) argues that penetration testers often need to explain complex technical issues to non-technical stakeholders and make critical decisions about the ethical implications of their actions.

2.2.2 Ethics and Virtue

According to Withers et al. (2020) The given nature of practicing penetration testing requires an adherence to a high ethical practice within the bounds of the organization, respecting privacy, data integrity, and legal boundaries. Noordegraaf & Weulen Kranenbarg (2023) argue that the stimulation of moral duty and access to a sense of community are motivating factors for young individuals to even consider penetration testing. Dawson & Thomson (2018) argues a similar position; that an ethical code must be developed, or a potential risk for exploitation increases.

2.2.3 Continuous Learning and Adaptability

Dawson & Thomson (2018) note that new threats emerge regularly in the ever-evolving cybersecurity landscape. Jones et al. (2018) continues by mentioning that professionals must commit to continuous learning and adapt to new tools, technologies, and attack vectors. As Mansfield-Devine (2017) highlights, penetration testing requires staying abreast of the latest developments, tools, and attack methodologies. A gap in their current knowledge can render their skills less effective against new and emerging threats.

Noordegraaf & Weulen Kranenbarg (2023) suggest that to improve skills in general, organizations can invest in continuous education and training for their penetration testing teams, encourage participation in cybersecurity communities and conferences, and foster a culture of interdisciplinary collaboration. Additionally, integrating penetration testing more deeply into information security curricula can prepare future professionals more effectively.

2.2.4 Teamwork and Collaboration

A study by Lindsjørn et al. (2016) found that the quality of teamwork is especially important for the success and quality of software teams and projects. Pirta-Dreimane et al. (2023) found that experience of working together as a team was an important factor in performance in cybersecurity exercises. According to Hoegl & Gemuenden (2001), it is possible to empirically measure teamwork quality by examining six defining facets: communication, coordination, balance of member contributions, mutual support, effort, and cohesion.

2.2.5 Soft Skills Matrix

The following is a matrix of all the soft skills identified from the literature review. The matrix includes a brief description of the skill and in what previous literature they are presented.

Table 2.1: Soft skills matrix

Skill	Description	Literature
Communication Skills	Communication skills involve conveying information effectively through verbal, written, and non-verbal means.	Hartley (2015) Jones et al. (2018)
Ethics and Integrity	Ethics and integrity encompass adhering to moral principles and conducting oneself with honesty and fairness. It involves making ethical decisions and respecting privacy and confidentiality.	Dawson & Thomson (2018) Kranenbarg (2023) Noordegraaf & Weulen Withers et al. (2020)
Continuous Learning and Adaptability	Continuous learning and adaptability involve the willingness to acquire new knowledge to stay updated in an evolving field. It requires flexibility and the ability to embrace new technologies and methodologies to meet evolving challenges.	Dawson & Thomson (2018) Jones et al. (2018) Mansfield-Devine (2017) Noordegraaf & Weulen Kranenbarg (2023)
Teamwork and Collaboration	Teamwork and collaboration involve working effectively with others to achieve common goals. It includes communication and cooperation.	Hoegl & Gemuenden (2001) Lindsjørn et al. (2016) Pirta-Dreimane et al. (2023)

2.3 Hard Skills

To answer the research question, and to understand how the soft and hard skills interplay, one should understand the hard skills in the context of the penetration testing profession. To begin defining hard skills, this study will look at the NICE framework. Jones et al. (2018) argues for the use of the NICE framework, it summarizes the skills of different specialty areas in cybersecurity. One of these areas is focused on penetration testing. The framework was developed by the National Institute of Standards and Technology, and the Department of Homeland Security. They developed a list of skills for the specialty area of 'Vulnerability Assessment and Management.' This specialty area will be used to define the hard skills, because this thesis argues that this specialty area is comparative to other academic sources on hard skills within penetration testing. Therefore, the combination of the NICE framework's definition of skill, and the list of skills of the specialty area, will be used as an initial definition of hard skills.

The NICE framework defines a skill as: "The capacity to perform an observable action." (Petersen et al. 2020, p. 5). The penetration testing specialty area contains a list of 12 skills, summarized in the list below:

1. Conducting vulnerability scans and recognizing vulnerabilities in security systems.
2. Assessing the robustness of security systems and designs.
3. Detecting host and network based intrusions via intrusion detection technologies.
4. Mimicking threat behaviors.
5. Using penetration testing tools and techniques.
6. Using social engineering techniques. (e.g., phishing, baiting, tailgating).
7. Using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap).
8. Reviewing logs to identify evidence of past intrusions.
9. Conducting application vulnerability assessments.
10. Performing impact/risk assessments.
11. Developing insights about the context of an organization's threat environment
12. Applying cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

Figure 2.1: 12 Skills of Vulnerability Assessment and Management (adapted from CISA, n.d.)

This study has derived 5 prioritized hard skills from this original list of 12 NICE framework skills. This thesis' 5 prioritized hard skills are the most relevant to this study's research question. These prioritized skills are: 1) Network Security 2) Scripting 3) Operating Systems Security 4) Web Application Security 5) Compliance and Legal. These 5 will later (in chapter 5) be compared with the soft skills to try and answer the study's research question.

2.3.1 Network Security

According to Dawson & Thomson (2018), using analytical tools for network scanning, network mapping, and vulnerability analysis is a significant skill. Networks were a prioritized important skill in a quantitative study, according to Jones et al. (2018). Understanding the security robustness of computer networks and systems is a key component. According to Gollman (2011), Domain Name System (DNS) is a part of network security. Web hosts are

usually known by a DNS name. He continues to explain that the DNS is used for looking up IP addresses. Towhidi & Pridmore (2023) indicate briefly that to learn Intrusion Detection and Prevention Systems, one needs to examine DNS data and traffic.

2.3.2 Scripting

Scripting languages, according to Gollman (2011), is a command (or script) from predefined, user input, code fragments. A given script can be passed to another software component, like a web browser or operating system. Bacudio et al. (2011) argues that knowledge of scripting languages such as Python, JavaScript, or other scripting languages is crucial. This skill enables penetration testers to write custom scripts and tools for testing security and automating tasks.

2.3.3 Operating Systems Security

Dawson & Thomson (2018) previously argued for using analytical tools for such things as network scanning, network mapping, and vulnerability analysis. They relate this skill directly to computer operating systems as well. Kaluarachchilage et al. (2020) argues that proficiency and knowledge of vulnerabilities in various operating systems - Windows, Linux, macOS - is necessary. Kaluarachchilage et al. (2020) highlights the differences in vulnerabilities between different operating systems. Furthermore, the importance of penetration testing with specific operating systems such as Kali Linux and BlackArch are discussed by Kumar et al. (2023).

2.3.4 Web Application Security

Le Blanc & Freeman (2016) report that 98% of tested web applications were found to be vulnerable. With the proliferation of web applications, penetration testers must be skilled in identifying and exploiting web-based vulnerabilities such as SQL injections, according to Alanda et al. (2021). Cross site scripting (XSS), as discussed by Singh et al. (2020), is also a big weakness for many web applications.

2.3.5 Compliance and Legal

This last prioritized skill of compliance and legal is harder to categorize than the other skills in this list as it is not dependent on a tool. It could be argued that it belongs in the soft skills category, but this thesis argues that compliance with regulations is related to skills numbered 11 and 12 in the NICE framework, therefore it is categorized as a hard skill in this thesis.

According to Bacudio et al. (2011), the skill of compliance and legal policies related to cybersecurity, including data protection laws and industry-specific regulations, is important. Penetration testers must ensure their activities are within legal boundaries, and that they adhere to ethical standards. Furthermore, Bacudio et al. (2011) continues to argue that the penetration tester profession must navigate a complex legal landscape and ensure that their activities are

compliant with relevant laws and regulations. A gap in this knowledge can lead to unintended legal violations and undermine the legitimacy of their work.

Crumpler & Lewis (2019) argues against compliance audits. They argue that employers are in critical need of more cybersecurity professionals, but do not want more compliance officers or cybersecurity policy planners. Compliance audits have less impact on the security of an organization, compared to tasks enabled by a deep technical background.

2.3.6 Hard Skills Matrix

The following table is a matrix of the 5 prioritized hard skills, based on the literature review. The hard skills matrix utilizes the initial 12 NICE framework skills to plot which of the prioritized skills relate to the ones in the framework. Related academic literature is also presented.

Table 2.2: Hard skills matrix

Hard Skill	Related NICE Framework skills	Literature
Network Security	#1 Conducting vulnerability scans and recognizing vulnerabilities in security systems. #3 Detecting host and network based intrusions via intrusion detection technologies. #4 Mimicking threat behaviors. #5 Using penetration testing tools and techniques. #6 Using social engineering techniques. #7 Using network analysis tools to identify vulnerabilities. #10 Performing impact/risk assessments.	Dawson & Thomson (2018) Gollman (2011) Jones et al. (2018) Towhidi & Pridmore (2023)
Scripting	#1 Conducting vulnerability scans and recognizing vulnerabilities in security systems. #2 Assessing the robustness of security systems and designs. #4 Mimicking threat behaviors. #5 Using penetration testing tools and techniques. #10 Performing impact/risk assessments.	Bacudio et al. 2011 Gollman, 2011
Operating Systems Security	#1 Conducting vulnerability scans and recognizing vulnerabilities in security systems. #2 Assessing the robustness of security systems and designs. #5 Using penetration testing tools and techniques. #8 Reviewing logs to identify evidence of past intrusions. #10 Performing impact/risk assessments.	Dawson & Thomson (2018) Kaluarachchilage et al (2020) Kumar et al. (2023)
Web Application Security	#1 Conducting vulnerability scans and recognizing vulnerabilities in security systems. #5 Using penetration testing tools and techniques. #6 Using social engineering techniques. #8 Reviewing logs to identify evidence of past intrusions. #9 Conducting application vulnerability assessments. #10 Performing impact/risk assessments.	Alanda et al. (2020) Le Blanc & Freeman (2016) Singh et al. (2020)
Compliance and Legal	#11 Developing insights about the context of an organization's threat environment. #12 Applying cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Bacudio et al. (2011) Crumpler & Lewis (2019)

2.4 Literature summary

To summarize this chapter, the following table will present the three factors again. It highlights the important aspects of each factor and groups its respective literature.

Table 2.3: Literature summary

Factors	Aspects	Literature
Team organization	• Employment type • Collective efficacy • Self-efficacy • Team composition	Cheng & Yang (2014), Happe and Cito (2023), Hartley (2015), Hoegl & Gemuenden (2001), Noordegraaf & Weulen Kranenbarg (2023), Withers et al. (2020), Yoo et al. (2020)
Soft skills	• Problem solving • Communication • Ethics and virtue • Continuous learning • Teamwork and collaboration	Dawson & Thomson (2018), Hartley (2015), Hoegl & Gemuenden (2001), Jones et al. (2018), Lindsjørn et al. (2016), Mansfield-Devine (2017), Noordegraaf & Weulen Kranenbarg (2023), Pirta-Dreimane, R. et al. (2023), Towhidi and Pridmore (2023), Withers et al. (2020)
Hard skills	• Network security • Scripting • Operating systems security • Web application security • Compliance and legal	Alanda et al. (2021), Bacudio et al. (2011), Crumpler & Lewis (2019), Dawson & Thomson (2018), Gollman (2011), Jones et al. (2018), Kaluarachchilage et al. (2020), Kumar et al. (2023), Petersen et al. (2020), Singh et al. (2020), Towhidi & Pridmore (2023)

3 Methodology

This study was inspired by the interview-based data collection method, as well as the interpretive philosophy. This chapter will explain exactly how this study gathered empirical interview data, and how this study structured its interview process. The main purpose of this chapter is to explain what was done, and by which means the scientific rigor of this study was maintained.

3.1 Using Interpretive Philosophy

The research question wanted to answer how soft skills relate to technical skills and how they complement each other within penetration testing. Because it looked at soft skills and the social elements within, it was therefore deemed appropriate to do the study with an interpretive research philosophy. According to Oates et al. (2022), interpretive research in IS and computing is concerned with understanding the social context of an information system. To adhere to the interpretive philosophy, the research approach oriented itself around the examination of two classes of data: the literature review and the interview data. The two sets of data were compared to find overlap.

"All interpretive traditions emerge from a scholarly position that takes human interpretation as the starting point for developing knowledge about the social world" (Prasad, 2018, p. 13). This study combined Prasad's argument and the definition by Oates et al. as research inspiration. Therefore, the empirical data focused on the given respondents' interpretations. Interpretations on hard and soft skills, to be exact.

3.2 Research Approach

3.2.1 Conceptual Framework

This study created a conceptual framework of three factors to help answer the research question. The framework was used to define the main themes of the study. These definitions helped the study by being a comparison tool for identifying similar themes across different written sources and different empirical data. The framework's three definitions of the respective three factors were initially used as a jumping-off point to examine other different, or prevalent, definitions within the same factor (presented in chapter 2). This is how the three factors relate conceptually. Soft and hard skills are grouped into separate categories of skills. The basis for this separation is that cognitive and communicative skills are more prevalently associated with the concept of soft skills. Skills that specify how to do a task or use a tool are

more prevalently associated with the concept of hard skills. This thesis argues that the two skills can be compared with each other based on a given type of profession. As has been previously mentioned, this study's given profession is penetration testing. The figure below is a visual representation of the conceptual framework. It shows how the three factors relate to each other and penetration testing.

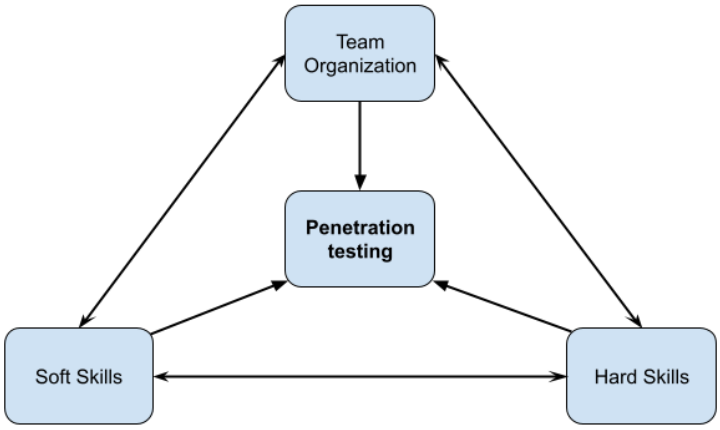

Figure 3.1: The conceptual framework

3.2.2 Thematic analysis

Themes were identified on the simple basis of how similar they were to the definitions in the conceptual framework. They were also identified by weighing their prevalence in text. Themes were the foundation of the conceptual framework, and it is the main tool to derive this study's results. The literature review (in chapter two) was this study's use of previous text to answer the research question. It was then used for the later discussion chapter, where the literature was compared to the empirical data. In other words, the transcripts generated from the interviews were drawn into comparison with the texts in the literature review. The purpose of this comparison was to find where the identified themes and skills overlap, and where they do not. As a side note, one should be aware that the limits of this study - influenced by qualitative and interpretive science - puts us in a position where our personal experiences and subconscious opinions might accidentally interfere with the quality, rigor, and results of the study. By pointing this out, we want to express awareness of this risk, and point out that this bias was consciously mitigated.

3.2.3 Searching For Literature

The process of searching for relevant literature was a broad and difficult task. By showcasing which databases were used to search for literature, we strive to explain this study's search process as thoroughly as possible. This search process assisted in increasing the general academic quality of the previous literature.

Databases utilized:

- ACM Digital Library
- AIS eLibrary
- IEEE / IET Electronic Library (IEL) - IEEE Xplore
- Google Scholar

This study referred to the Scimago Journal & Country Rank to measure the rankings of its used journal sources. This study aimed to only use articles from higher ranked journals. Additionally, the study also tried to cite literature with the most citations.

3.2.4 Interview Subjects

This thesis conducted its empirical data collection through semi-structured interviews. The interviews were done with experienced subjects on the topic of penetration testing. The subjects were mainly found by searching for relevant work titles on LinkedIn, but also via reaching out to pentesting and cyber security companies and asking if individuals were interested in participating. To increase the richness of the generated data, a list of certain criteria were created to make the selection process of the interview subjects suited to the research question.

As mentioned, we employed a semi-structured interview format. For this, we created an interview guide with a predefined set of topics and questions. Key to this approach was the freedom to dynamically adjust the sequence of questions based on a given interview's natural progression. The semi-structured format also allowed the freedom to introduce spontaneous questions whenever appropriate. This flexibility enhanced the depth of discussion. It also allowed respondents to introduce issues they considered relevant. Our application of this method involved using the interview guide as a flexible tool, intentionally allowing different wordings of the premade questions. This would help to better accommodate the unique expertise of each respondent.

We believed that the semi-structured interview format, as opposed to the standard questionnaire or unstructured interview, provided the opportunity to better examine exactly how some of the hard or soft skills were more important to the profession. The following were the criteria to deem a subject viable. To maintain scientific rigor and consistency within the selection process of respondents. Each contacted respondent had to follow these criteria:

1. Individual with five years or more experience of higher education and/or employment.
2. Of the combined years, higher education was loosely related to cybersecurity.
3. Of the combined years, employment was within cybersecurity roles.
4. Of the combined years, one or more years direct experience with a role that included penetration testing tasks and/or skills.

This search process resulted in six completed interviews. However, due to a late change in scope and research question, the first interview was discarded from this study. The five interviews which were used for this study’s discussion were all done within the span of one week.

The willing respondents of this study were Swedish public organizations and privately owned companies, as well as a German privately owned company. Before each interview was conducted, the ethical protocol document was sent out to them. Before each recording of a given interview was started, an oral agreement was sought. Following this study's completion, the recordings were deleted.

3.3 Data Collection

According to Oates et al. (2022), a data generation method is the means by which one produces empirical data. The interview method is one of the described data generation processes. This was the main method utilized by this study. The interview method was initiated for this study with the following methods and themes as an interview guide.

3.3.1 Qualitative Interview Method

Mayo's (1933 cited in Kvale & Brinkmann, 2009) method of interviewing is an old method which still offers a contemporary guide for qualitative interviews. It was used as inspiration for this study. The following list is the original method:

1. Give your whole attention to the person interviewed and make it evident that you are doing so.

2. Listen─don't talk.

3. Never argue; never give advice.

4. Listen to:

    (a) what he [sic] wants to say
    (b) what he [sic] does not want to say
    (c) what he [sic] cannot say without help

5. As you listen, plot out tentatively and for subsequent correction the pattern (personal) that is being set before you. To test this, from time to time summarize what has been said and present for comment (e.g., "is this what you are telling me?"). Always do this with the greatest caution, that is, clarify in ways that do not add or distort.

6. Remember that everything said must be considered a personal confidence and not divulged to anyone
(Mayo, 1933 cited in Kvale & Brinkmann, 2009, p. 45).

The conducted interviews followed this method. This ensured a sense of uniformity and standardization of how we approached the respondents. The method assisted the interview process, while at the same time keeping the interview open to divulge on different topics of interest a given subject wished to explore.

3.3.2 Interview Guide

An interview guide document was constructed. The document's parts included an introduction, the ethical considerations, the oral agreement, the above-mentioned interview method, and a predefined set of themes and questions. The set worked as a reminder of which themes and questions this study primarily wanted to explore and examine. The set of questions was used loosely. It was diverged from if the respondent wanted to talk about other topics or themes. The interview guide can be found in the appendix as appendix B.

3.3.3 Overview of Conducted Interviews

The following two tables give two different overviews of the interviews conducted. The first table summarizes the details of a given respondent. The second table summarizes the details of a given interview.

Table 3.1: Summary of Respondent Details

Respondent	Organization	Country	Role	Appendix
R1	Freelance	Sweden	Consultant	D
R2	Penetration testing company	Germany	Founder, manager	E
R3	Public sphere	Sweden	Information security specialist	F
R4	Public sphere	Sweden	Information security coordinator	G
R5	Software/service company	Sweden	Senior penetration tester	H

Table 3.2: Summary of Interview Details

Interview Date	Duration	Respondent	Location	Language Spoken	Appendix
22-04-2024	60 mins	R1	Remote	Swedish	D
22-04-2024	40 mins	R2	Remote	English	E
23-04-2024	60 mins	R3	Remote	Swedish	F
23-04-2024	60 mins	R4	Remote	Swedish	G
25-04-2024	30 mins	R5	Remote	Swedish	H

3.4 Data Analysis

The analysis was conducted by utilizing a thematic analysis, as previously mentioned. The recorded interviews were first transcribed using OpenAI's 'Whisper' software to automatically transcribe the interviews. Afterwards, the interviews were relistened to. The errors generated by the automatic transcriptions were corrected. Once the transcriptions went through a human check and a first complete transcript was completed, the transcriptions were sent by email to the respective respondents. At this point, the respondents were able to view the transcript to verify that the accuracy and confidentiality of the transcript was satisfactory. The respondents were asked to give a reply if they accepted or declined the transcript.

Once the respondents accepted their transcript, potentially after corrections, the given transcript was thematically analyzed. This was done, as recommended by Oates et al. (2022), by starting to break down the data and by putting it into three different categories:

1. Non-relevant segments
2. Descriptive segments to define the context of our research
3. Segments that appear relevant to our research

This approach enabled us to efficiently analyze the segments that were most relevant to our research. We adopted an inductive method to categorize the data initially. After categorizing the data, we further refined the relevant segments into themes that were significant to our study. By refining our responses from the different participants, it allowed us to identify common themes and issues effectively. These identified themes were then presented in our results chapter. We strived to present our findings impartially, ensuring that all respondents' views were represented fairly, without unduly favoring any single respondent's perspective. After identifying the relevant segments, we started coding the transcripts. This was done by reading through the marked relevant parts of the transcripts and categorizing them according to the factors of our conceptual framework. This allowed us to then easily cross-reference our transcripts and literature review when writing our results in the discussion chapter.

Table 3.3: Themes with codes

Theme	Code
Team organization	T
Soft skills	S
Hard skills	H

3.5 Ethical Considerations

According to Kvale & Brinkmann (2009), ethical issues permeate interview research, as one must examine aspects such as personal relationships, clear communication, neutral setting between the interviewer and interviewee. They continue by recommending preparing an ethical protocol for an interview study. This recommendation was followed by this study, and the aspects below were taken into consideration.

Table 3.4: Ethical Issues at Seven Research Stages (adapted from Kvale & Brinkmann, 2009, p. 63)

Thematizing	The purpose of an interview study should, beyond the scientific value of the knowledge sought, also be considered with regard to improvement of the human situation investigated.
Designing	Ethical issues of design involve obtaining the subjects' informed consent to participate in the study, securing confidentiality, and considering the possible consequences of the study for the subjects.
Interview Situation	The personal consequences of the interview interaction for the subjects need to be taken into account, such as stress during the interview and changes in self-understanding.
Transcription	The confidentiality of the interviewees needs to be protected and there is also the question of whether a transcribed text is loyal to the interviewee's oral statements
Analysis	Ethical issues in analysis involve the question of how penetratingly the interviews can be analyzed and of whether the subjects should have a say in how their statements are interpreted.
Verification	It is the researcher's ethical responsibility to report knowledge that is as secured and verified as possible. This involves the issue of how critically an interviewee may be questioned.
Reporting	There is again the issue of confidentiality when reporting private interviews in public, and of the consequences of the published report for the interviewees and for the groups they belong to.

According to Kvale & Brinkmann (2009), this table is a list of the seven common ethical issues one needs to consider when creating an ethical protocol. It was used as a guide for the creation of this study's ethical protocol. These seven stages guided this study's empirical data collection and analysis process. It should be noted that the ethical protocol has a previous thesis working title written on it. As mentioned briefly earlier, this protocol was sent out to each respondent before their respective interviews. This study's created interview guide used the ethical protocol as inspiration for how to conduct a uniform style of interviewing.

3.6 Scientific Quality

Prasad (2018) argues that two conventional criteria of positivist research are reliability and validity. However, these are criteria often asked of non-positivist research as well. This, according to Prasad, is detrimental to the study. To quote, “Researchers working in many genres of non-positivism are often asked how their work meets conventional criteria of reliability and validity employed to judge positivist research” (Prasad, 2018, p. 9).

Therefore, this study followed Prasad’s argument and disregarded criteria like reliability and validity. Instead, this study focused on dynamic examination of the empirical data. To maintain a dynamic examination of the empirical data, this study optioned to approach the research by creating a conceptual framework. This framework would fit both the previous literature and the interview transcripts.

Once again, ethical considerations were also highly regarded for this study as inspiration. This included a large priority on respondent confidentiality.

4 Empirical Findings

This chapter presents the key results from this study's interviews. A total of five interviews were conducted. The results have been grouped in accordance with the three factors of this study's conceptual framework - team organization, soft skills, and hard skills.

4.1 Team Organization

4.1.1 In-House or Consulting

R1 works as a freelance consultant. They work mostly alone and highlight the importance of having a wide span of skills.

> *"There is so much within this field which makes it hard to master it. So you could only become this specific thing. Like, this is it. You can of course live off of that, we have built so much with web apps and API:s so that that's possible. But you will become very restricted." (R1:66)*

R1 is a member of a community of similar professionals where they can help each other by providing services of their specific niches. The importance of having a network of people with whom you can exchange knowledge with and work together with is a common theme throughout the interviews.

R2 and R5 also have a community, but they work mostly within their own organizations' network.

> "Internally we of course work with teams, so if it's like a larger test then there's like two, three, four sometimes even more people assigned to this test and they, of course, work together." *(R2:9)*

R5 notes that there are different pros and cons to using in-house penetration testers versus external penetration testers. In-house penetration tests allow for more in-depth analysis. However, the team will be more dependent on the competencies of the in-house testers.

> *"You actually get more worth if you take in different third parties, as there will be more different competencies." (R5:24)*

4.1.2 Bug bounty programs

A type of work system called bug bounty program was mentioned in two interviews. This was seen as an alternative way of working as a team.

R1 thinks that the bug bounty programs have created a better environment for penetration testers to learn and experiment with. It attracts more interested people.

> *"Because it's an environment which isn't as square as how it is in a university environment maybe. I don't know, I didn't study at university myself now. But, I think that they create like, 'here is a system, find the five bugs'. You know which bugs you should find. While in 'bug bounty' it's for real. There you need to find the system, hack something someone else has built. That is much more worth it, I think." (R1:45)*

R3 described a bug bounty program as a good way to set up a clearly defined, transparent business case for penetration testers to find vulnerabilities. R3 argues that this is a good system, if carefully set up, that should be utilized more by the industry in the future. R3 points out that they have mostly seen a few banks lead the initiative on this.

> *"It is not so common in Sweden, but I have seen several promising initiatives but they have never really flown with "bounty programs." This is also relevant to strict scope and transparency. You are allowed to basically shoot at us under these conditions. If you find something, tell it to us and you get a reward." (R3:67)*

4.1.3 Collective efficacy

In relation to collective efficacy, the respondents talked about team compositions, and the freedom to work remotely as a team.

Respondent R2, R4 and R5 mentioned that their organizations allowed the freedom to work remotely for a majority of their schedule. R2 said that their organization was completely built on this type of work, and that this was also a big part of their work culture.

> *"We do believe in remote work, so we don't have an office, and most people work from remote. Most people use a text or chat tool to communicate during the tests." (R2:36)*

R2 explains that his job as a manager is to make sure that teams have a balance of both the right technical competencies and the right social fit, in order to provide their customers with the best possible quality.

> *"Exactly, so that's like one of the tasks that is for me, and for the operations team, to make sure that we pick the team composition well and make sure that both technically and also socially the right people work together and*

> *then it kind of gives like a good overall package to the customer, attempting to make sure that we cover all the things as best as we can." (R2:25)*

R4 is positive towards working remotely. However, R4 emphasizes the social need as people are social creatures in the end.

> *"Sure, you perform much better. There are no people who are bothering you. But then again, you need to have the social. In the end we're social creatures." (R4:41)*

R4 says this on team composition. That a team of penetration testers should have different types of individuals. both people who can lead, and people who are nerdier.

> *"You need to have other skills which can drive and motivate. You need a little bit of everything in a team. I don't think that it gets the job done [otherwise]. You need to have differences. (R4:39)*

R5 says that working in pairs is the common team composition.

> *"Well, traditionally when you have your projects as a pentester, no matter where you work you often don't do them alone. Two and two is pretty much the standard way to run it so that you can brainstorm together. But then if you drive to your workplace or if you decide to work remotely, it is often up to yourself." (R5:26)*

4.2 Soft Skills

The need for soft skills was identified in all the five respondents' answers. The following are the more prevalent skills discussed during the conducted interviews.

4.2.1 Communication

A common theme visible throughout all the conducted interviews is the importance of communication when it comes to penetration testing. It is evident that being a good communicator is a highly valued skill.

R1 highlights that the ability to teach and communicate cybersecurity terms and potential weaknesses and having a good relationship with clients is very important.

R2 recognizes similarly that communication is very important for a member of a penetration testing team but also states that it's only really crucial for the members of the team that are in contact with clients, and that members can perform very well without great communication skills as long as they fit in socially.

R3 said this when asked about which soft, human attributes they personally value:

> *"Pedagogy, good communicator, depending on if you're working on a technical level or a more managerial level. Well, you need different abilities. But the analytical ability is necessary in all types of tests really." (R3:59)*

R3 continues on to give an example. A colleague to R3 had a bad relationship with a large customer once. The customer did not communicate properly. This unravelling issue led to the colleague being reported for data breach. But it could have been avoided had his colleague only maintained a good relationship and good communication channels with the customer (R3:34).

R5 states that there are two typical types of penetration tester / ethical hacker, on the one hand the more stereotypical hacker persona who has very high technical competencies but doesn't enjoy talking and presenting results, and on the other hand the type of person that both have good technical knowledge and has the ability to translate these technical findings into something the customer will understand (R5:14).

R5 says that teams with different competencies have individuals who need to collaborate to understand each other's findings.

> *"So we have those who understand technical findings which are found and then we have those who maybe translate and help present these to customers so that it actually is evident what has been exposed." (R5:8)*

4.2.2 Integrity, ethics, honesty, and transparency

Some of the respondents seem to have the idea that honesty and transparency are key aspects of working as a penetration tester.

R1 touches a lot on the role of honesty and integrity in building trust with clients, and thus enabling a better working relationship.

R3 argues that full transparency is one of the key principles within penetration testing. Beyond that, one should also have a moral duty.

4.2.3 Focus and analytical ability

R3 mentions that an analytical ability is necessary regardless of the test or audit. According to R3, the ability to focus is important for one's analytical ability.

R5 believes similarly that the ability to see and understand how different parts of a system fit together and communicate with each other is a key skill to be a successful penetration tester.

4.2.4 Curiosity and keeping up-to-date

R5 mentions that being curious and driven to find new things is a very important characteristic of a penetration tester. R5 mentions that as a penetration tester you have a knowledge base that is a standard that all penetration testers use, but that then you also need to be curious and learn new things so that you can begin to find potential vulnerabilities by thinking outside of the box (R5:12).

> *"...to be able to take this extra step when you feel like there is nothing, but you continue with your curiosity to try and find something that maybe in the end, is something"(R5:10).*

4.2.5 Penetration testing as a social field

It is clear from our interviews that some of our respondents have different views of the role of penetration testers. More specifically, in regard to how social or technical oriented penetration testing is.

> *"You can't just run tools. Anyone can do that." (R1:29)*

R1 is the respondent that subscribes the most to the view of penetration testing as a social field. They focus mostly on finding organizational/cultural issues within an organization and don't like the idea of penetration testing being just a technical box checking exercise.

R2 basically only performs technical penetration tests, while reserving usage of social engineering for very rare occasions, in contrast to R1's view on the profession.

R2 mostly performs technical penetration tests but adds that when they and their team actually do discover cultural and organizational issues, they report them as well.

R3 shares a view that many within the industry practice social engineering. Furthermore, R3 argues that the industry, as a whole, is also appreciative of the process of audits and governance, and that there is no large rivalry between the public, judicial bureaucracy and companies that practice IT-security or penetration testing.

R4 says that the main reason behind cybersecurity attacks is the human factor.

> *"Cybersecurity attacks. There are many studies which confirm that 60-70% is because of the human factor. I wanna argue that it is 90%, because the studies focus on the regular user, but I want to say that it is the IT-people who also are affected." (R4:45)*

R4 continues to give an example.

> *"For example, the second week that I was here on my job, I went in and hadn't gotten my pass card yet. Then I noticed how a colleague let me in*

> *without a word, without me needing to say something, I'm not kidding." (R4:45)*

R5 agrees that social and organizational aspects are very important but that the extra costs associated with conducting penetration testing in that manner is very costly compared to just performing a technical penetration test and therefore not as popular among clients.

4.3 Hard Skills

The need to have hard skills is a recurring theme in many of the interviews. It seems clear that deep technical competencies are critical to be a successful practitioner in the field of penetration testing *"...you need to be brutally technically competent"* (R1:27). The following are the most prevalently identified hard skills.

4.3.1 Network Security

R2 tries to put a percentage on how much they value technical skills compared to soft skills:

> *"So, I would say 70% technical, 30% social. Um, if you want to put numbers on it. But it could potentially even be more tending towards the social, just, the technical is of course of key importance, but without the social it wouldn't work out"(R2:36).*

This respondent's previous comment states that what he values the most when hiring a person is their technical competencies, and that good technical knowledge is kind of *"...the first barrier of being considered for the team"* (R2:35).

R4 was asked about which technical skills the respondent thinks one should have to be a penetration tester, they listed the following skills:

> *"Knowledge on networking, knowledge on scripting [and] programming languages. Python, PowerShell and also I think it was called Metasploit. Kali Linux and then another one which I forget. So, networking, scripting, and operating systems, I believe." (R4:51).*

R5 states that while you don't necessarily need to be a programmer, you need a good understanding of network security and how applications work and communicate between front end and back end, and that having a good knowledge of this is necessary as penetration testers are always encountering new systems and need to have the ability to understand their work (R5:8).

> *"Well, when it comes to penetration testing, then you need a good foundational understanding for networking and application security and a little bit of coding. You don't need to be a coder from the start to be a penetration tester." (R5:8)*

4.3.2 Web application security

Three respondents mention the OWASP methodology as being important, especially in relation to web application security (R1, R3, R5).

R5 describes one of the most common tests which are used.

> *"The most common which is tested is what you call a black box test on web applications. And that is actually how an attacker would go about and poking something over the internet without having any login credentials or any knowledge about how the application works." (R5:4)*

R5 differs from R1 and R2, who mainly work with gray box tests, that is, where the penetration testers collaborate with the customer by giving access to certain systems so that a penetration tester can investigate what could happen if a hacker somehow gained access to a certain system.

4.3.3 Compliance and legal

R2 said that their organization does not work with compliance, and instead focuses on technical tasks and jobs.

> *"I don't think that the discrepancies are large enough to not enjoy the synergies properly, but I also do know that compliance can be getting really annoying and that in some situations you have like kilometers of red tape that is unnecessary." (R2:68).*

R3 argues that compliance knowledge is important for penetration testing. They mention specifically in relation to the NIS2 directive and GDPR.

R5 mentions the PCI DSS (Payment Card Industry Data Security Standard). This standard requires that payment card providers perform penetration tests a certain number of times each year.

4.3.4 Penetration testing a technical field

R1 focused a lot on the social aspects of penetration testing, but respondents R2 and R5 were clearly more focused on penetration testing as a primarily technical field. Something they agree on though is that it's technical at its core, even though R1 argues that the organizational and social vulnerabilities are relatively more important.

R2 and R5 both seem to see a big value in organizational and social vulnerabilities as well but believe more that technical penetration tests are usually the only thing companies are looking for, partially due to them doing it for reasons such as certifications.

R3 continues on and mentions a common reason being that they are forced to by the GDPR or, for example, the new NIS2 EU-directive. R3 further argues that penetration testing is a test tool for checking that a system, for example, is secure and protected. Based on their experiences, this need for penetration testing is often driven by compliance demands.

R4 mentions AI when asked about future developments within penetration testing.

> *"Yes, I see it. I think that AI will contribute with a lot, but also a lot of risks. It is good to have that in mind that it is not only positive, there are negative aspects as well." (R4:43)*

R5 offers an overview of the technical parts of penetration testing.

> *"Before I became a penetration tester I worked as an IT security consultant. Then I did everything from migrating firewalls, configuring switches, changing switches, doing Wi-Fi access point plans for IoT assessments, vulnerability analyzes. All this knowledge you collect during your time suddenly becomes the foundation for your understanding of how everything works. Which you then can use when doing penetration testing, which is very technical and there's new systems." (R5:8)*

5 Discussion

This chapter compares the literature review with the empirical data. The findings will be examined to find out how they have contributed to answering the research question. The limitations of this study are discussed, as well as recommendations for future research.

5.1 Team Organization

The previous literature and empirical data seem to point to a conceptual connection between soft skills and team organization. Initially, this study defined a team as: "A team can be defined as a social system of three or more people, which is embedded in an organization..." (Hoegl & Gemuenden, 2001). All respondents mentioned that communication was a highly valued skill. Therefore, this thesis argues that there's a link between communication and team organization. This link contributes to the research question by strengthening the findings on soft skills.

The academic literature and empirical data both highlighted alternative approaches to traditional team-based penetration testing. Many respondents noted the flexibility of remote work during a regular work week. Additionally, bug bounty programs emerged as a prevalent method. It was described as an effective way of establishing a transparent job for different penetration testers to identify vulnerabilities. Respondents, such as R1 and R3, advocated for these programs, emphasizing that when properly structured, they offer valuable models that the industry should adopt more broadly in the future.

As is argued by Cheng & Yang (2014), high quality interaction is a very important factor in utilizing team knowledge, therefore this thesis argues that for a team to benefit fully from their members' high technical proficiency, the social skills are an important mediator in making sure members actually know each other and their own expertise. Thus, as our conceptual framework argues, there is a clear relationship between soft skills, hard skills, and team organization.

R1, as a freelancer, relies significantly on a broad set of both soft and hard skills due to the solitary nature of their work. This independence requires strong self-management and communication skills, not only for executing technical tasks but also for managing client relationships and coordinating with other freelancers. This contrasts with R2 and R5's consulting team context, where structured teamwork allows for specialized roles. In such settings, soft skills enhance technical tasks by fostering a collaborative environment where diverse technical expertise can be effectively integrated and leveraged.

In summary, the findings of this study illuminate the critical role of soft skills in enhancing team organization and, consequently, the effectiveness of technical tasks in penetration testing. Effective communication, a core soft skill, is paramount in both traditional and non-traditional team settings, facilitating improved coordination among team members. This study has shown that in structured environments, such as consulting teams where R2 and R5 work, soft skills like communication and collaboration enable the integration of diverse technical expertise, enhancing the team's overall performance. Conversely, in more autonomous settings like freelance or remote work, as experienced by R1, soft skills such as self-management and high-quality interaction are crucial for managing client relationships and coordinating projects independently.

Additionally, the adaptation to bug bounty programs highlights the flexibility required in modern cybersecurity practices, necessitating strong soft skills to navigate these less conventional team structures effectively. These programs require clear, structured communication and robust self-management to successfully identify and report vulnerabilities, further underscoring the value of soft skills in diverse organizational contexts.

5.2 The relative importance of soft and hard skills

5.2.1 Communication

It is clear to say that soft skills definitely are highly valued in penetration testing. The findings of both our own study, and that of Jones et al. (2018), point to communication skills being especially important, highlighting the need for penetration testers to be able to communicate difficult-to-explain cybersecurity concepts. Respondents such as R1 and R2 argue that when dealing with clients the ability to maintain these good relationships is very important, and that good communication skills are needed for good cooperation. Being able to tell a client what weaknesses have been exposed and why they matter is a very important part of what makes a good penetration tester.

The work of Jones et al. (2018), in many ways, echoes our own findings when it comes to the importance of communication skills. This study does, however, offer some nuance into how it is valued. As we've learned from some of our respondents, R2 and R5 mostly, the amount which communication skills play a part can vary, there is definitely room for lesser communicators within a penetration testing team as long as the team composition is built around it, not every member of a team necessarily needs to communicate directly with the client. R5 argues that it is definitely a plus to be able to translate these findings into something the customer will understand and that such skills are highly valued, but that the collaborative aspect of working in a team also leaves room for 'lesser' communicators.

However, we believe it's very important not to downplay the role that good communication has. As R2 touches upon, a team member has to be a good social fit in the organization, and

as shown by Cheng & Yang (2014), high quality interaction among team members is vital for improving a team's collective efficacy.

The empirical evidence strongly supports the notion that effective communication enhances the technical tasks involved in penetration testing. This thesis has illustrated that proficient communication is not just about exchanging information but about transforming technical data into understandable intelligence that team members and clients can understand and act upon. Enhanced communication skills enable penetration testers to explain complex vulnerabilities and security measures in a way that facilitates quicker decision-making and more effective team collaboration. This direct impact on the technical aspects of the job highlights the indispensable role of communication as a soft skill in improving the technical outcomes of cybersecurity efforts.

In the context of penetration testing, the results underscore the pivotal role of communication skills in team dynamics. As indicated by Jones et al. (2018) and reinforced by empirical findings from this study, the ability to effectively communicate complex cybersecurity concepts not only bridges the gap between technical expertise and stakeholder understanding but also enhances collaborative efforts within teams. This finding aligns with the research model proposed by Cheng & Yang (2014), which suggests high-quality interactions are crucial for leveraging collective team knowledge. In practical terms, enhancing communication training for penetration testers could significantly improve the efficacy of cybersecurity measures by ensuring that all team members are on the same page and can efficiently collaborate on complex security tasks.

5.2.2 Collaboration

As mentioned in the previous sub-chapter, collaboration appears to be a highly valued skill. This is evident both by Jones et al. (2018) and our own empirical findings. Collaboration is highly connected with communication, and being a good communicator is usually an indicator that you'll be good at collaborating with others, but there are definite areas where the skills don't overlap as well. When a person is not the best at communicating hard technical concepts to clients, they might still be good at working and collaborating well within a team.

5.2.3 Ethics

Ethics were discussed during the interviews. It was a common subject in the previous literature, but not so common amongst the respondents. Many did not perceive this as a large issue as individuals with bad ethics were not common.

5.2.4 Continuous learning and curiosity key to acquiring hard skills

As evidenced by empirical findings, there is considerable value placed on the ability to continuously learn and enhance one's skill set, particularly in discovering new vulnerabilities.

Continuous learning directly enriches an individual's technical knowledge and skills. This links continuous learning directly with hard skills. A penetration tester should be inherently motivated to continually learn new techniques and information to achieve success in the field. This skill, understandably, is somewhat challenging to categorize as it intricately connects both hard skills and soft skills. However, it shows evidence that soft skills are necessary to acquire hard skills.

Respondents' emphasis on continuous learning resonates with Jones et al. (2018) and Mansfield-Devine's (2017) observation of the dynamic and evolving nature of cybersecurity threats. The empirical data and academic discussion highlight the crucial role of ongoing education in enhancing the effectiveness of technical tasks in cybersecurity. This suggests that training programs should not only equip cybersecurity professionals with the skills to deal with current technologies and threats, but also to foster the ability to adapt and learn continuously. This approach ensures that professionals can remain effective as the landscape of cybersecurity evolves, directly enhancing their technical capabilities in addressing emerging challenges.

The value placed on continuous learning by respondents underlines its role as a crucial soft skill that directly enhances technical capabilities. In penetration testing, where technologies and threats continuously evolve, the ability to learn and adapt is paramount. This skill enriches a tester's technical knowledge and allows for the effective application of new techniques and tools, thereby directly impacting the technical quality and thoroughness of penetration tests. Continuous learning not only keeps penetration testers technically competent but also adaptable and proactive in addressing new challenges.

5.2.5 The role of Compliance

There is debate, both in the previous literature and the empirical data, on how relevant compliance and governance is for penetration testing. This study argued initially that it is a hard skill because it is part of the profession when managing vulnerabilities. R2 is staunchly against working with compliance, but their organization is also focused on deeper technical and practical work.

5.2.6 On the overlap of skills

The following table is a combined table of the hard and soft skills, and which respondents mentioned which skills. There are 2 skills which all respondents agree on as necessary for penetration testing. The respondents differ largely in their opinion on which hard skills should be prioritized.

Table 5.1: Table of soft and hard skills, empirical data plotted against literature

Skills	R1	R2	R3	R4	R5
Communication Skills	X	X	X	X	X
Ethics and Integrity	X	X	X	X	X
Continuous Learning and Adaptability	X				X
Teamwork and Collaboration	X	X			X
Network Security	X	X		X	X
Scripting				X	X
Operating Systems Security	X			X	
Web Application Security			X		X
Compliance and Legal			X	X	

5.3 Recommendations & Limitations

The empirical data seems to indicate certain gaps in the previous literature. For example, there seems to be a lack of clear definition between penetration testing and its interchangeable synonyms, such as ethical hacking. This study's qualitative research was limited because of this academic discord.

This study recommends that more quantitative data is produced to study the impact of working with penetration testing in a team collective. For example, a survey on which tasks penetration testers do, or a survey on if they follow the skills set out in the NICE framework.

The shift towards remote work, as noted by R2, necessitates strong self-efficacy, corroborating literature that emphasizes adaptability in dynamic settings. This follows the findings by Yoo et al. (2020). However, this practical trend challenges traditional notions of collective efficacy, which typically relies on physical co-presence to foster team dynamics. The empirical data thus calls for a re-evaluation of how collective efficacy is facilitated in increasingly remote work environments. Collective efficacy might potentially help reshape training

approaches which emphasize digital communication and project management tools that bridge physical distances.

Although this study opted to limit itself from interdisciplinary studies, this study would recommend examining the discipline of cybersecurity and the topic of penetration testing more as an interdisciplinary field, for future research. This is because this thesis argues that penetration testing is a relatively new concept - only seemingly decades old - and has social aspects which delve into psychology, organization theory and cognitive ability.

A limitation of this study was the empirical data. More respondents from varying settings, cultures and geographies would benefit the quality of the empirical data.

To summarize, reflecting on the methodological approach of this study, the need for broader empirical data is apparent. Future research could benefit from quantitative analysis, e.g., to measure the impact of specific soft skills on the effectiveness of technical tasks in penetration testing. Such studies would provide a clearer statistical backing to the qualitative insights obtained, offering a more detailed understanding of how soft skills like communication, problem-solving, and continuous learning directly correlate with improvements in technical tasks.

6 Conclusion

This study sought to examine the research question of: *How do soft skills enhance the effectiveness of technical tasks in penetration testing?*

The findings of this thesis clearly demonstrate that soft skills significantly enhance the effectiveness of technical tasks in penetration testing. Through a detailed analysis of both empirical data and literature, it is evident that while technical prowess is fundamental, the integration of soft skills such as communication, collaboration, and continuous learning is crucial for success within the profession.

Communication skills, highlighted by both literature and empirical insights, create clearer presentation of technical vulnerabilities to clients, and within teams. This enhances the impact and comprehensibility of technical findings. Collaboration, another key soft skill, ensures that diverse expertise within a team is effectively harnessed, leading to more comprehensive penetration testing strategies and outcomes.

Continuous learning as a soft skill not only motivates the acquisition of advanced technical skills, but also keeps penetration testers adaptable to new threats and technologies. This adaptability is essential for the dynamic field of cybersecurity, where the technical landscape is constantly evolving.

Penetration testing is an interdisciplinary field that requires a blend of both soft and hard skills for effective practice. The empirical data and literature review demonstrate that technical skills are essential for penetration testers, but soft skills such as communication, collaboration, and continuous learning are equally crucial for the overall success of penetration testing endeavors. These soft skills facilitate effective teamwork, enhance the ability to convey complex technical issues to non-technical stakeholders, and foster an environment of continuous professional development and ethical practice.

To summarize this thesis, the first chapter introduced an observed problem within penetration testing. Thus, a research question was created which sought to examine the skills inherent in penetration testing professionals. The aim of this study was to contribute to an academic gap within this specific topic. This observed academic gap was about the inherent hard and soft skills of the topic. This meant that the study aimed to interpret and examine penetration testing skills by looking at the overlap between previous academic literature and empirical, qualitative data gathered from interviews. The aim was that this would help impact the advancement of effective practice and theories within the specific area of penetration testing. Moreover, this also meant that the study would indirectly contribute to the broader topic of offensive cybersecurity.

A conceptual framework for penetration testing was constructed based on the factors of the research question. The study's research methodology was based on a qualitative and interpretive philosophy, and the data was gathered through interviews. This thesis concludes that hard skills form the foundation of success in this field, but soft skills are indispensable for advancing to senior and managerial positions. Penetration testing is dependent on both soft and hard skills, and not just one set of skills. Penetration testing professionals require both types of skill, but believe soft skills enhance the work done by individuals. Although a strong technical background can ensure progress to a certain extent, the integration of effective communication and interpersonal skills is critical for further effectiveness in the penetration testing profession.

6.1 Future Research

This study wants to argue for future research on the strict definitions of penetration testing. It was difficult to find any different types of penetration testing as many of the terms for penetration testing are used interchangeably. In general, the terminology of penetration testing is used loosely. This made it difficult to find and examine previous literature. This study argues that research should be conducted to create clearer definitions of the terms.

Furthermore, we think it would be beneficial to examine the difference between more socially oriented penetration testing which utilizes social engineering and tries to find cultural and structural issues. This should be examined against purely technical penetration tests like OWASP. Having a better understanding of the benefits of these two types of penetration tests would likely be helpful in improving offensive cybersecurity and in further guiding relevant professional practices.

Finally, future research should also focus on generating quantitative data surrounding penetration testing. There are emerging areas of research within artificial intelligence and machine learning for penetration testing. When asked where research around penetration testing should head in the future, two respondents replied that artificial intelligence and machine learning looks promising.

References

Alanda, A., Satria, D., Ardhana, M. I., Dahlan, A. A. & Mooduto, H. A. (2021). Web Application Penetration Testing Using SQL Injection Attack, *JOIV : International Journal on Informatics Visualization*, vol. 5, no. 3, p.320

Bacudio, A. G., Yuan, X., Bill Chu, B. T. & Jones, M. (2011). An Overview of Penetration Testing, *International Journal of Network Security & Its Applications*, vol. 3, no. 6, pp.19–38

Cheng, H.-H. & Yang, H.-L. (2014). The Antecedents of Collective Creative Efficacy for Information System Development Teams, *Journal of Engineering and Technology Management*, vol. 33, pp.1–17

CISA. (2024). Vulnerability Assessment and Management, Available Online: https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/vulnerability-assessment-and-management [Accessed 2 May 2024]

Crumpler, W. & Lewis, J. A. (2019). The Cybersecurity Workforce Gap

Dawson, J. & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance, *Frontiers in Psychology*, [e-journal] vol. 9, Available Online: https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2018.00744/full [Accessed 10 April 2024]

Gollmann, D. (2011). Computer Security, Third edition., Chichester, West Sussex: Wiley

Happe, A. & Cito, J. (2023). Understanding Hackers' Work: An Empirical Study of Offensive Security Practitioners, in *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, New York, NY, USA, 30 November 2023, New York, NY, USA: Association for Computing Machinery, pp.1669–1680, Available Online: https://dl.acm.org/doi/10.1145/3611643.3613900 [Accessed 5 April 2024]

Hartley, R. (2015). Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack, *Journal of International Technology and Information Management*, [e-journal] vol. 24, no. 4, Available Online: https://scholarworks.lib.csusb.edu/jitim/vol24/iss4/6

Hoegl, M. & Gemuenden, H. G. (2001). Teamwork Quality and the Success of Innovative Projects: A Theoretical Concept and Empirical Evidence, *Organization Science*, vol. 12, no. 4, pp.435–449

Jones, K. S., Namin, A. S. & Armstrong, M. E. (2018). The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals, *ACM Transactions on Computing Education*, vol. 18, no. 3, pp.1–12

Kaluarachchilage, P. K. H., Attanayake, C., Rajasooriya, S. & Tsokos, C. P. (2020). An Analytical Approach to Assess and Compare the Vulnerability Risk of Operating Systems, *International Journal of Computer Network and Information Security*, vol. 12, no. 2, pp.1–10

Kumar, B., Bejo, S. P., Kedia, R., Banerjee, P., Jha, P. & Dehury, M. K. (2023). Kali Linux Based Empirical Investigation on Vulnerability Evaluation Using Pen-Testing Tools, in *2023 World Conference on Communication & Computing (WCONF)*, 2023 World Conference on Communication & Computing (WCONF), RAIPUR, India, 14 July 2023, RAIPUR, India: IEEE, pp.1–6, Available Online: https://ieeexplore.ieee.org/document/10235163/ [Accessed 16 April 2024]

Kvale, S. & Brinkmann, S. (2009). InterViews: Learning the Craft of Qualitative Research Interviewing, 2. ed., Los Angeles: Sage

Le Blanc, K. & Freeman, S. (2016). Investigating the Relationship Between Need for Cognition and Skill in Ethical Hackers, in D. Nicholson (ed.), *Advances in Human Factors in Cybersecurity*, Cham, 2016, Cham: Springer International Publishing, pp.223–228

Ledin, G. (2011). The Growing Harm of Not Teaching Malware, *Communications of the ACM*, vol. 54, no. 2, pp.32–34

Lindsjørn, Y., Sjøberg, D. I. K., Dingsøyr, T., Bergersen, G. R. & Dybå, T. (2016). Teamwork Quality and Project Success in Software Development: A Survey of Agile Development Teams, *Journal of Systems and Software*, vol. 122, pp.274–286

Mansfield-Devine, S. (2017). Hiring Ethical Hackers: The Search for the Right Kinds of Skills, *Computer Fraud & Security*, vol. 2017, no. 2, pp.15–20

Noordegraaf, J. E. & Weulen Kranenbarg, M. (2023). Why Do Young People Start and Continue with Ethical Hacking? A Qualitative Study on Individual and Social Aspects in the Lives of Ethical Hackers, *Criminology & Public Policy*, vol. 22, no. 4, pp.803–824

Oates, B. J., Griffiths, M. & McLean, R. (2022). Researching Information Systems and Computing, 2nd edition., SAGE

OWASP Top 10. (2024). , Available Online: https://owasp.org/Top10/ [Accessed 12 May 2024]

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A. & Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework), National Institute of Standards and

Technology, Available Online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf [Accessed 3 May 2024]

Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K., Grabis, J., Lugo, R. G. & Bonders, M. (2023). CyberEscape Approach to Advancing Hard and Soft Skills in Cybersecurity Education, in D. D. Schmorrow & C. M. Fidopiastis (eds), *Augmented Cognition*, Cham, 2023, Cham: Springer Nature Switzerland, pp.441–459

Prasad, P. (2018). Crafting Qualitative Research: Beyond Positivist Traditions, 2nd edition., New York London: Routledge, Taylor & Francis Group

Recker, J. (2021). Scientific Research in Information Systems: A Beginner's Guide, Springer Nature

Sharif, H. U. & Mohammed, M. A. (2022). A Literature Review of Financial Losses Statistics for Cyber Security and Future Trend, *World Journal of Advanced Research and Reviews*, vol. 15, no. 1, pp.138–156

Singh, M., Singh, P. & Kumar, P. (2020). An Analytical Study on Cross-Site Scripting, 14 March 2020

Towhidi, G. & Pridmore, J. (2023). Aligning Cybersecurity in Higher Education with Industry Needs, *Journal of Information Systems Education*, vol. 34, no. 1, pp.70–83

Withers, K., Parrish, J., Ellis, T. & Smith, J. (2020). Vice or Virtue? Exploring the Dichotomy of an Offensive Security Engineer and Government "Hack Back" Policies, in *53rd Hawaii International Conference on System Sciences*, 7 January 2020, Available Online: http://hdl.handle.net/10125/63963 [Accessed 5 April 2024]

Yoo, Jahyun Goo & Rao, H. R. (2020). Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness, *MIS Quarterly*, vol. 44, no. 2, pp.907–931

Zantua, M. A., Popovsky, V., Endicott-Popovsky, B. & Holt, F. B. (2018). Discovering a Profile for Protect and Defend: Penetration Testing, in P. Zaphiris & A. Ioannou (eds), *Learning and Collaboration Technologies. Learning and Teaching*, Cham, 2018, Cham: Springer International Publishing, pp.530–540

Appendix A - AI-Contribution Statement

Tools
ChatGPT, elicit.org, Whisper, Consensus.app

Level of Use
ChatGPT: Used throughout the duration of the thesis course. For text correction, context analysis, summarization of some previously written aspects/topics.

elicit.org: Used one week for assistance with structuring the literature review.

Whisper: Used to help speed up the process of transcribing the five interview recordings.

Consensus.app: Used to efficiently find sources on topics.

Appendix B - Ethical Protocol

Interview Invitation & Ethical Protocol

Thesis Working Title
Redefining the Hacker Persona:
How soft skills complement technical, hard abilities in penetration testing

Thesis Researchers
Elias Sirviö, Lund University: el3457si-s@student.lu.se
Alexander Bengtsson, Lund University: al5472be-s@student.lu.se

The Interview
Thank you for accepting to be interviewed for this bachelor thesis. You have been invited to speak for 30-60 minutes about your personal experience and history with penetration testing.

Study's Purpose
The transcript generated from our interview will be sent back to you to verify the data that was recorded. Afterwards, the transcripts' data will be compared with skills identified in the study's literature review.

Potential Risks
This study seeks to keep confidentiality of the respondents a priority. Therefore, we ask permission to anonymize your personal details, including workplace.
The respondent is free, at any point during the interview, to pause or stop the interview.
To give a clearer indication of which type of questions will be asked, please check the list on the next page.

List in English on the next page.

List of Predefined Questions

1. How does your organization utilize penetration testing?

2. What are the responsibilities and benefits of this?

3. Hard, technical skills: "In your experience, which are the top three technical, hard skills that you find most critical?”

4. Soft, social skills: "How important do you consider soft skills to be in the day-to-day operations of your team?

5. Can you share examples where soft skills played a key role?"

6. Skill development: "How does your organization support the development of both hard and soft skills among members of your penetration testing team?

7. Social dynamics: "Can you describe how you balance different individuals' abilities if you’re working in a team setting?

8. Consultancies: “When working for a customer, what is the first thing you do to establish yourself with the customer”?

8. Evolving skill sets: "How do you ensure that your team's skill sets remain up-to-date and relevant?

9. Are there specific emerging skills that you believe will become more important in the near future for penetration testing professionals?"

10. Is social engineering and psychology important when working?

11. Does your employment affect how you collaborate with others?

Appendix C - Interview Guide

Introduction

1. Quick round of introductions, where everyone introduces themselves
2. Present the essay: title, research question, purpose/scope, deadline
3. Inform that the interview will be anonymous
4. Ask for permission to record audio
5. Go through the ethical protocol, then ask if the respondent accepts the ethical protocol

Predefined questions

1. How does your organization utilize penetration testing?

2. What are the responsibilities and benefits of this?

3. Hard, technical skills: "In your experience, which are the top three technical, hard skills that you find most critical?”

4. Soft, social skills: "How important do you consider soft skills to be in the day-to-day operations of your team?

5. Can you share examples where soft skills played a key role?"

6. Skill development: "How does your organization support the development of both hard and soft skills among members of your penetration testing team?

7. Social dynamics: "Can you describe how you balance different individuals' abilities if you’re working in a team setting?

8. Consultancies: “When working for a customer, what is the first thing you do to establish yourself with the customer”?

8. Evolving skill sets: "How do you ensure that your team's skill sets remain up-to-date and relevant?

9. Are there specific emerging skills that you believe will become more important in the near future for penetration testing professionals?"

10. Is social engineering and psychology important when working?

11. Does your employment affect how you collaborate with others?

Identified skills in the literature

- Network Security
- Scripting
- Operating Systems Security
- Web Application Security
- Compliance and Legal Knowledge
- Communication Skills
- Ethics and Integrity

After interview

1. Transcribe
2. Send to respondent for verification before analyzing
3. Once accepted, analyze