Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Patrick Schmid

Increasing the effectiveness of technical security testing methods with a comparative study

Master's thesis in Information Security
Supervisor: Prof. Dr. Bernhard Markus Hämmerli
December 2021

NTNU
Norwegian University of Science and Technology

Patrick Schmid

Increasing the effectiveness of technical security testing methods with a comparative study

Master's thesis in Information Security
Supervisor: Prof. Dr. Bernhard Markus Hämmerli
December 2021

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Abstract

Organisations use ethical hacking services as a key component to assess their overall cyber security posture. Basis for those services is a set of technical security testing methods such as vulnerability scanning, penetration testing, red teaming, social engineering and similar that are neither clearly and uniformly defined in relevant literature nor have consumers or providers of such methods a common understanding what is and is not part of a certain method. This imposes many problems for both sides: Providers are dealing with consumers requesting a specific security testing method without fully understanding the method itself or its properties. And consumers can request a quote for a specific security testing method and still get no easily comparable basis among different providers.

Therefore, the context of this study is this disbalance in knowledge between service providers of ethical hacking services and its consumers about the underlying technical security testing method used for an assessment. To address the issue at hand, this study proposes a security testing landscape model, providing definitions of the most relevant technical security testing methods based on best practice standards, guides and frameworks combined with insights from eight different subject matter experts. Further, the method landscape was enriched with a total of ten properties to characterise the specific nuances of each technical security testing method. This allows a detailed characterisation of each testing method based on its unique properties as well as compare different methods through different properties to aid in selecting a suitable technical security testing method and help reducing the disbalance in knowledge.

Sammendrag

This chapter is not present as the author is not proficient in any of the Scandinavian languages and thus excused from providing this chapter as part of his master thesis.

Acknowledgments

I would like to thank Prof. Dr. Bernhard Hämmerli as my supervisor for his continuous support, guidance and valuable inputs along the way of researching my topic and writing my master's thesis. His exemplary support, even during off-time, as well as his constant push for better and more enabled me to see my own ideas from a different view and helped me to stay focused during arduous phases of writing my master's thesis.

Also, I would like to thank all the involved interview partners and other involved people, that helped me with their time, valuable inputs and experience in answering my questions in order to help me gain a profound understanding of the field and gain new ideas and insights and especially my employer for providing me with the time and patience not only to complete my research but as well to pursue my studies at Norwegian University of Science and Technology (NTNU).

Lastly, I would like to thank my lovely wife for her patience and endurance during all my studies and her continuous support and appreciation along the way.

Patrick Schmid
Switzerland, December 2021

Contents

Figures

Tables

Acronyms

API application programming interfaces. 27

ASVS Application Security Verification Standard. 15

BLE Bluetooth low energy. 28

BSI Bundesamt fuer Sicherheit in der Informationstechnik. 8

CESG National Technical Authority for Information Assurance. 15

CISO Chief Information Security Officer. 20, 22, 58, 59, 63

CMMI Capability Maturity Model Integration. 33, 39, 45, 46

CSVS Container Security Verification Standard. 15

DSS Data Security Standard. 5, 9, 10

ENISA European Union Agency for Cybersecurity. 11, 13, 17

FSTM Firmware Security Testing Methodology. 15

ICS Industrial Control System. 7, 20, 57

ICT Information and Communications Technologies. 7

IDS Intrusion Detection Systems. 15

IoT Internet of Things. 13, 15

ISO International Organization for Standardization. 5, 17

ISSAF Information System Security Assessment Framework. 15

ISVS IoT Security Verification Standard. 15

ITHC IT Health Check. 15

MSTG Mobile Security Testing Guide. 15

MSVS Mobile Security Verification Standard. 15

NCSC National Cyber Security Centre. 15

NIST National Institute of Standards and Technology. 10, 11, 17

NTNU Norwegian University of Science and Technology. vii, 17, 20

OISSG Open Information Systems Security Group. 15, 16

OSINT open-source intelligence. 14

OSSTMM Open Source Security Testing Methodology Manual. 14–16

OWASP Open Web Application Security Project. 14, 16

PCI Payment Card Industry. 5, 9, 10, 17

PTES Penetration Testing Execution Standard. 13–16, 25, 30

SANS SysAdmin, Audit, Network, and Security. 13, 17

SME small and medium enterprises. 16

SMS short message service. 29

STAR Security Test Audit Report. 14

WLAN wireless LAN. 15, 28

WSTG Web Security Testing Guide. 14

Chapter 1

Introduction

Organisations across all industries and sizes use ethical hacking services as a key component to assess their overall cyber security posture [1]. Basis for such services is a set of technical security testing methods such as vulnerability scans, penetration tests, red teaming, social engineering or similar that all provide different advantages or disadvantages. However, this broad field of possibilities comes with certain problems as none of those security testing methods are clearly defined nor a provider or a consumer of such methods have a uniform understanding in regards of what is part of such a method and what not.

1.1 Problem description

The variety in security testing methods starts with commonly known methods such as penetration tests, red team exercises or vulnerability assessments and continue with more specific methods such as source code reviews, configuration review, social engineering, (spear) phishing, bug bounty programs, adversary simulations, assumed breach testing and much more. The difficulty with such a wide variety of potentially suitable testing methods is that some methods only differ in a few small but important details. For example, while a penetration test and a vulnerability assessment can both result in a list of technical vulnerabilities they differ heavily in their approach, the needed monetary investment and after all the sort of vulnerabilities they are able to identify and report upon. In case of approaches, a penetration test should be conducted with a semi-automated method in order to give a complete picture as possible while a vulnerability assessment is conducted in solely automated way through a vulnerability scanner. In case of investments a vulnerability scan can cover a rather large scope such as a complete subnet or network in a very short amount of time while a penetration test needs a rather narrowed down scope such as one application or service with a few systems behind it to conclude within a reasonable time frame. And in comparison of outcome, a vulnerability assessment can only provide a rather superficial analysis because a vulnerability scanner can currently not fully consider the context within a certain behaviour is observed and is therefore for example not able to identify logical

vulnerabilities or more complex vulnerabilities consisting of various stages or a chain of exploits. A penetration test on the other hand can certainly considers the observed behaviour in the context of the circumstances it occurred because the analysis is performed by a security professional that understands the application and its context [2].

As this initial example shows, it is not always straight-forward for a consumer of such security testing methods to spot and fully understand the small but important differences between certain security testing methods which makes it much more important for the provider of such testing methods to recommend and consult on the selection of the proper testing method.

1.2 Motivation

This is rather unproblematic if a consumer is more or less open in regards of methods and monetary investment, because during a quick exchange a security professional should be able to rather quickly identify the goals behind a certain request by asking specific questions but quite often a consumer cannot be as flexible as it would best support his goals, because internal policies or regulations demand a certain security testing method. In combination with the fact that the possible monetary investment is always somehow limited due to budget constraints, a consumer can potentially end up with a security testing method that cannot fully cover all his needs and goals and that can ultimately lead to missed vulnerabilities at various stages.

One rather well-known example of such a testing method mismatch could be observed in Switzerland during Swiss Post's e-voting project. Before starting a public bug bounty program [3], the system was evaluated with penetration tests that issued the platform an acceptable level of security [4]. During a so-called "Public Intrusion Test" (PIT), comparable to a public bug bounty program, a few people performed a source code analysis and were able to identified rather complex high-risk vulnerabilities in the underlying architecture of the platform [5] that ultimately led to an abrupt abandoning of the project in the end by Swiss Post [6]. If the project would have gone live right after the performed penetration tests, then the error would have been missed and could potentially have been exploited in public during elections and therefore potentially taking a severe influence on the Swiss democracy [7].

This imposes a handful of problems on both sides: Providers of such services are dealing with potential consumers requesting a very specific security testing method without fully understanding the method itself or its properties or consequences. And on the other side, a consumer of such methods can request a proposal for a specific testing method and still get various quotes that are not easily comparable as none of them share a common basis that would allow for easy

comparison. As a team leader and senior security tester with the Switzerland-based cyber security firm Redguard AG (`https://redguard.ch`), the main author of this research regularly encounters such problems mainly from a providers point of view and was further confirmed by other people with experience in similar positions [8] [9] as well as from consumers with a background in regularly using such testing methods to strengthen their own security posture [10]. Therefore, this study would like to understand the problem in greater detail and help to overcome some of the problems outlined before.

1.3 Scope

The initial idea of this study was to limit its scope to the situation of Switzerland and Norway. However, during the initial round of interviews with an expert from Norway and an expert from a world-wide company it got clear, that industries and their needs in regards of technical security testing methods tend to differ heavily across various countries and to include two different countries as scope of this research would result in two more or less distinctive analyses in the end that cannot be combined. Therefore, it was decided to focus on the situation in Switzerland as the author's place of residence to reduce the overall complexity.

1.4 Research questions

To structure the various characteristics of the presented problem, the following research questions will be investigated:

1.4.1 Question 1

Creating a relevant landscape of technical security testing methods (such as vulnerability scans, penetration tests, red teaming, social engineering and similar) means to add criteria for usage and performance. Which criteria must be analysed and added such that a relevant landscape will be generated?

1.4.2 Question 2

Comparing a consumer's initially requested technical security testing method with the method offered by a cyber security provider: Is there a difference in understanding of certain technical security testing methods that would lead a provider to offer a different method for security testing than initially requested by the consumer?

1.4.3 Question 3

Do specific methods require a minimum maturity level (CMMI) and does this imply, if the minimum maturity level has not been reached for a specific method,

another method must be used for preparation first?

Example: A public bug bounty program including all systems and services can get very expensive without maintaining a good level of security first.

1.4.4 Question 4

Knowing that each provider has its own understanding of a certain technical security testing methods, does applying the same method by a different provider lead to new insights or does applying the same method from the same provider create a fatigue and exhaust the vulnerability discovery process over time?

Example: From the author's personal experience, penetration-testing an application that other providers have already analysed before, lead often to findings that should have been detected during the previous test.

1.4.5 Question 5

Knowing about a potential mismatch in a provider and consumer's understanding of specific technical security testing methods, which tools and recommendations must be developed for removing mismatches and create an improved mutual understanding?

1.5 Contribution

Based on the research questions the main contribution of this study is to give a definition of various technical security testing methods aligned with the industry's understanding of such methods and assign usage and performance criteria to each method as well as to propose a model that could help in identifying the proper testing method based on a consumer's circumstances and goals to help overcome the described disbalance in knowledge. To the author's knowledge, currently there is no other research published covering this topic with the goal to give an overview over a large set of different security testing methods.

Chapter 2

Background and related work

This chapter provides insights into related work ranging from official standards, best practice guides and white papers from several well-respected organisations to gain an in-depth understanding of already established content in the field of technical security testing methods. In addition, relevant scientific work is analysed as well to complete the overall picture.

2.1 Best practice standards

A lot of standards in the cyber security field are covering the area of maintaining an acceptable level of cyber security risk for an organisation. Some of these standards are mandatory for certain industries such as Payment Card Industry (PCI) Data Security Standard (DSS) [11], while others can be applied on voluntary basis and are used to achieve a certification such as International Organization for Standardization (ISO) 27001 [12]. As it was already established earlier, technical security testing methods are an important part of a organisations' cyber security risk evaluation process to improve its security posture. Now, if guidance on how to maintain an acceptable risk level is provided by various best practice standards, it would be only reasonable if those standards would as well provide guidance in the definition or at least the selection of a proper technical security testing method based on an organisation's needs. Therefore, this study started by analysing various best practice standards as well as so-called "de-facto" standards from the industry to find out about definitions and guidance in selecting and applying the proper technical security testing methods.

2.1.1 ISO/IEC 27001:2013 - Information Security Management

ISO/IEC 27001:2013 defines a total of two controls referenced as "A.12.6.1" and "A.18.2.3" as part of Annex A out of 114 controls that are related to technical security testing methods [13]. If these controls as listed in table 2.1 are analysed, it can be seen, that these controls are defined on a rather high level. Basically, A.12.6.1 only states that some sort of technical security testing method should be

applied to gain a good understanding of current vulnerabilities but without any sort of guidance on how an organisation would be able to comply with that.

Table 2.1: Relevant controls from ISO/IEC 27001:2013 Annex A

A.12.6.1	*Management of technical vulnerabilities*	*Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk [13].*
A.18.2.3	*Technical compliance review*	*Information systems shall be regularly reviewed for compliance with the organisation's information security policies and standards [13].*

This impression gets even clearer, once the various areas used by ISO/IEC 27001:2013 to structure its own control are analysed more closely [13]:

- Information security policies (A.5)
- Organization of information security (A.6)
- Human resource security (A.7)
- Asset management (A.8)
- Access control (A.9)
- Cryptography (A.10)
- Physical and environmental security (A.11)
- Operations security (A.12)
- Communications security (A.13)
- System acquisition, development and maintenance (A.14)
- Supplier relationships (A.15)
- Information security incident management (A.16)
- Information security aspects of business continuity management (A.17)
- Compliance (A.18)

The covered area by the standard ranges from organisational, technical and physical risks as well as defensive measures and even incident response. Therefore, it is understandable that not every single control can be defined in broad details because otherwise this already rather comprehensive list of controls would get a lot longer. However, the standard is leaving somebody with the intention of complying with the standard with a rather vague idea most likely leading to the initially described problem.

2.1.2 ICT minimum standard

The ICT minimum standard, originally named "IKT Minimalstandard", is a standard written by Switzerland's Federal Office for National Economic Supply (FONES) and provides a "*minimum standard for improving ICT resilience*" for critical infrastructure in Switzerland [14]. The standard is based on various other, well-known standards such as NIST, ISO 2700x, COBIT, BSI and the ENISA "Good Practice Guide" and is split in high level topics and includes a subset of relevant controls that should an organisation help to record and rate its own level of resilience. In regards of technical security testing methods, the standard includes a single topic as listed in table 2.2 and provides a description split by Information and Communications Technologies (ICT) and Industrial Control System (ICS) systems. Further into the standard, it lists three controls as part of risk assessments as listed in table 2.3 [14].

Table 2.2: Relevant topics from ICT minimal standard

Topic	**ICT**	**ICS**
Testing and audit methods	*Use modern (poss. automated) methods. Systems are usually resilient and reliable enough to handle assessments during normal operation [14].*	*Automated assessment may be unsuitable, e.g. owing to the high degree of individual development. There is a greater probability of failure during testing, so assessments during normal operation tend to be more difficult [14].*

Table 2.3: Relevant controls from ICT minimal standard

ID.RA-1	*Identify the (technical) vulnerabilities of your assets, and document them [14].*
ID.RA-3	*Identify and document internal and external cybersecurity threats [14].*
ID.RA-4	*Identify the possible business impacts of cybersecurity threats, and calculate the probability of their occurring [14].*

However, similar problems as before can be seen with ICT minimal standard. While the standard provides a direction in what to achieve, it does not provide

any help in how this can be achieved. For example, the standard states that an organisation should use "*modern methods*" but does not provide any help or direction in what is consider as modern or not. In addition to that, the controls require an organisation to "*Identify [...] vulnerabilities*" but again without any guidance on how to properly fulfil this control. The reason for that is most likely again because the standard is aiming for an organisation's resilience as a whole and can therefore not provide detailed guidance in how to achieve each control in broad detail. Therefore, ICT minimal has similar drawbacks in regards of technical security testing methods as already seen in ISO27001.

2.2 Special publications and guides

As already seen in the previous chapters, best practice standards often tend to have a broader focus as there is often no space for rather specific and specialised topics as it would be needed in the case of providing guidance in selecting an appropriate technical security testing method. As the authors of these standards are fully aware of this problem, a lot of additional information in addition to an official best practice standard is provided through additional publications and guides that help to guide in more specific fields. Therefore, such publications were analysed as well as part of this study.

2.2.1 BSI - IT Baseline Protection Manual

Named *IT Baseline Protection Manual*, the Bundesamt fuer Sicherheit in der Informationstechnik (BSI) provides a comprehensive set of controls, guides and manuals to help an organisation to achieve and maintain an acceptable risk level [15]. This includes a guide named *Ein Praxis-Leitfaden fuer IS-Penetrationtests* than can roughly be translated as "a field manual for penetration testing" that provides in-dept guidance in how to plan and task a security professional with performing a penetration test. Part of that includes a formal definition of a penetration test, that BSI is referring to as "IS-Penetrationtest" through its documents. Furthermore, the guide provides a differentiation to other technical and non-technical testing methods. This includes *IS-Revision* (internal or external audit), *Code-Review* (code review) and *IS-Webcheck* (web application penetration test), however the last one is described as a more specialised form of IS-Penetrationtest and not a differentiation but listed in the same part of the guide anyways [16]. While this guide is way more comprehensive and detailed than the before discussed standards, it only covers a limited subset of possible technical security testing methods. If an organisation already knows the most suited testing method for its needs, then this guide can be a good and efficient way to structure and provide guidance along the various steps from preparing to performing and finalising for example a penetration test. However, as a shortcoming, this guide is using its own wording to differentiate technical security testing methods that sometimes heavily tend to differ from the wording other standards use for the same or similar technical security testing

methods. This can for example be seen on the testing method "IS-Webcheck" that describes more or less a classical web application penetration test.

2.2.2 PCI DSS - Penetration Testing Guidance

PCI DSS is a standard mostly only relevant to the finance industry processing so-called card data. If an organisation is processing such data, it is mandatory to fully comply with the standard and its specifications [11]. Accordingly, this standard is only relevant for a small subgroup of organisations. However, the "Penetration Test Guidance Special Interest Group" as part of the "PCI Security Standards Council" published a comprehensive guide on how to perform penetration testing. This includes information about how such tests can be performed in accordance with PCI DSS, but in addition to that, the guide provides valuable information and insights even if a compliance to PCI DSS is not mandatory for an organisation. The guide for example provides a short definition of the security testing method penetration testing and vulnerability scanning as show in table 2.4.

Table 2.4: Differences between a vulnerability scanning and penetration testing

	Vulnerability Scanning	**Penetration Testing**
Purpose	*Identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system [17].*	*Identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components [17].*
When	*At least quarterly and after significant changes [17].*	*At least annually and upon significant changes [17].*
How	*Typically a variety of automated tools combined with manual verification of identified issues [17].*	*A manual process that may include the use of vulnerability scanning or other automated tools, resulting in a comprehensive report [17].*

The standard even describes various types of penetration testing such as external / internal or application and network penetration tests. In addition to that, the guide provides a definition of the testing method "social engineering" as well:

> *Social engineering is the attempt to gain information, access, or introduce unauthorized software into the environment through the manipulation of end users [17].*

While this guide can provide some very comprehensive insights and includes valuable definitions it also includes very specific wording such as "card holder data environment". This is mostly only relevant inside the context of PCI DSS and describes all systems tasked to process card data, as this represents the main focus of interests for PCI DSS.

2.2.3 NIST - Special Publication

The National Institute of Standards and Technology (NIST) is not only a framework and standard but provides various guides and tools as well. One of these tools is the "NIST Risk Management Framework". Part of this framework is the NIST special publication "SP 800-53" that provides controls to help an organisation to create a resilient baseline in regards of information and IT security [18].

Table 2.5: Relevant controls from NIST SP 800-53 Rev.5.1

CA-8	*Penetration Testing*	*Conduct penetration testing on organisation-defined systems or system components [18].*
RA-5	*Vulnerability Monitoring and Scanning*	*Monitor and scan for vulnerabilities in the system and hosted applications and when new vulnerabilities potentially affecting the system are identified and reported, remediate legitimate vulnerabilities in accordance with an organisational assessment of risk [18].*
RA-10	*Threat Hunting*	*Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organisational systems and detect, track, and disrupt threats that evade existing controls [18].*

This publication includes various controls related to technical security testing methods as listed in table 2.5. In addition, the following definition is provided for penetration tests:

> *Penetration testing is a specialised type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application-level security. Penetration testing can be used to validate vulnerabilities or determine the degree*

> *of penetration resistance of systems to adversaries within specified constraints [18].*

Another relevant publication in this field is the special publication 800-115 titled "Technical Guide to Information Security Testing and Assessment". In regards of security testing methods this publication starts of by stating "*Dozens of technical security testing and examination techniques exist that can be used to assess the security posture of systems and networks*" and provides a good collection of potential security testing methods [2]. The publication lists potential methods in one of the following three categories:

- ***Review Techniques**: These are examination techniques used to evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities, and are generally conducted manually. They include documentation, log, ruleset, and system configuration review; network sniffing; and file integrity checking [2].*
- ***Target Identification and Analysis Techniques**: These testing techniques can identify systems, ports, services, and potential vulnerabilities, and may be performed manually but are generally performed using automated tools. They include network discovery, network port and service identification, vulnerability scanning, wireless scanning, and application security examination [2].*
- ***Target Vulnerability Validation Techniques**: These testing techniques corroborate the existence of vulnerabilities, and may be performed manually or by using automatic tools, depending on the specific technique used and the skill of the test team. Target vulnerability validation techniques include password cracking, penetration testing, social engineering, and application security testing [2].*

Based on these categories the publication lists various methods including the capabilities each testing method can provide during application. These methods are listed in table 2.6. As this collection of security testing methods is rather comprehensive compared to other standards, this collection can provide a very valuable basis to gain a good understanding of technical security testing methods and their possibilities and capabilities especially in combination with the comprehensive glossary NIST provides [19] as well. But as the publication stated at the very beginning, this is only a rather small subset of potential testing methods and can only provide a short description of capabilities and for example does not list potential limitation and weaknesses of certain methods.

2.2.4 ENISA - Good Practice Guide

Another valuable source for best and good practice guides are the "Good Practice Guides" by European Union Agency for Cybersecurity (ENISA). The guides published by ENISA, in contrary to NIST special publications, do not cover a specific

Table 2.6: Methods and capabilities from NIST SP 800-115

Documentation Review	*Evaluates policies and procedures for technical accuracy and completeness [2].*
Log Review	*Provides historical information on system use, configuration, and modification. Could reveal potential problems and policy deviations [2].*
Ruleset Review	*Reveals holes in ruleset-based security controls [2].*
System Configuration Review	*Evaluates the strength of system configuration. Validates that systems are configured in accordance with hardening policy [2].*
Network Sniffing	*Monitors network traffic on the local segment to capture information such as active systems, operating systems, communication protocols, services, and applications. Verifies encryption of communications [2].*
Network Discovery	*Discovers active devices. Identifies communication paths and facilitates determination of network architectures [2].*
Network Port and Service Identification	*Discovers active devices. Discovers open ports and associated services/ applications [2].*
Vulnerability Scanning	*Identifies hosts and open ports. Identifies known vulnerabilities (note: has high false positive rates). Often provides advice on mitigating discovered vulnerabilities [2].*
Wireless Scanning	*Identifies unauthorized wireless devices within range of the scanners. Discovers wireless signals outside of an organisation's perimeter. Detects potential backdoors and other security violations [2].*
Password Cracking	*Identifies weak passwords and password policies [2].*
Penetration Testing	*Tests security using the same methodologies and tools that attackers employ. Verifies vulnerabilities. Demonstrates how vulnerabilities can be exploited iteratively to gain greater access [2].*
Social Engineering	*Allows testing of both procedures and the human element (user awareness) [2].*

testing method but rather a specific product or category of products such as healthcare, Internet of Things (IoT) or smart cars and provide insights in how to properly secure those. But in all of these guides, some testing methods such as "penetration testing" or "vulnerability assessment" are mentioned and described as to be part of good security practice but not explained in more detail [20] [21] [22]. An additional guide on how to properly perform such tests is currently missing. However, ENISA published a guide comparing different risk management and assessment methodologies and standards providing a rating on how complete a specific standard covers various aspects during risk assessment. One of these aspects is a rating of the exposure assessment, that defines how good a certain standard can guide during the selection of a suitable security testing method. Therefore, this guide was used to challenge and complete the list of included standards and best practices guides [23].

2.2.5 SANS - White Papers

Another institution that provides a lot of resources in the field of security testing is SysAdmin, Audit, Network, and Security (SANS). While SANS mainly provides training courses and certifications, it publishes additional material in form of cheat sheets and white papers in various fields and depts. However, the main focus of these white papers is more focused on how to apply a certain testing method rather than provide a good classification of certain testing methods [24].

2.3 Security testing frameworks

In addition to white papers and best practice standards, different security testing frameworks exist that focus on how to perform a certain security testing method and provide guidance along each and every step of the method including hints on how to test and what tools to use [25]. However, these frameworks focus either on one single form of security testing and are therefore very specific or try to cover any sort of technical security testing method in one go and are thus rather generic [26]. In either way they are either only applicable to a specific security testing method or are again nearly as general as already encountered during the analysis of the previous resources.

2.3.1 Penetration Testing Execution Standard

The Penetration Testing Execution Standard (PTES) is a rather generic framework with the goal of providing guidance for various kinds of technical security testing methods by splitting any testing method into seven phases. Theses phases include [27]:

1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modeling

4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting

Along these phases the standard provides guidance on what objectives should be considered and how they can be applied along the way. Because the standard is rather generic, this standard can be applied to a large set of relevant security testing methods. This can be achieved because not all phases need to be passed in the same depth for all testing methods. This means that one security testing method can for example be rather specific in case of the phase "Exploitation" while another testing method do not cover this phase at all because exploitation is not a key element for this method. Or certain methods include a rather extensive and detailed part on "Intelligence Gathering" through open-source intelligence (OSINT) as a potential adversary would do as well while other methods cover this phase collecting these information during preparation as a precondition to increase efficiency [27].

2.3.2 Open Source Security Testing Methodology Manual

The Open Source Security Testing Methodology Manual (OSSTMM) is a framework very similar to PTES. The main goal of OSSTMM is to provide reliable and repeatable security testing through various testing methods. The framework covers the following questions along the way [28]:

- What is tested (scope)?
- How were they tested?
- What was discovered?
- What was not covered by the applied method?

In addition to that, OSSTMM provide a standardised model called Security Test Audit Report (STAR), that combines all findings together with the current state of the scope and inputs this into a complex formula. According to the framework, this allows for a "*clear statement of the security metrics and details for comparisons with previous security tests or industry test averages*" [28].

2.3.3 Open Web Application Security Project

The Open Web Application Security Project (OWASP) is a non-profit foundation working towards improving the overall security of the internet by providing guidance, tools and education in the field of application security through various, community-driven open-source projects. In the field security testing framework, OWASP maintains and publishes various guides and de-facto standards detailing about how to test different aspects of application security. This includes the following frameworks [29]:

- Web Security Testing Guide (WSTG) [30]

- Application Security Verification Standard (ASVS) [31]
- Mobile Security Testing Guide (MSTG) [32]
- Firmware Security Testing Methodology (FSTM) [33]
- IoT Security Verification Standard (ISVS) [34]
- Mobile Security Verification Standard (MSVS) [35]
- Container Security Verification Standard (CSVS) [36]

Each of these frameworks focus on one specific form of penetration testing covering either web applications, IoT devices, mobile applications or containers and are thus rather specific. Therefore, they can provide not only a generic methodology through various steps but provide detailed checks and tools for every check. Accordingly, they can be seen more or less as a checklist to ensure the performed penetration test is able to cover all possible angles and provide the most complete analysis of the scope's security posture.

2.3.4 IT Health Check Scheme

UK's National Cyber Security Centre (NCSC), formerly National Technical Authority for Information Assurance (CESG), published a methodology to standardise penetration testing of governmental networks as well as organisations being part of critical infrastructure. This methodology is called IT Health Check (ITHC) and covers penetration testing in general providing definitions as well as inputs in regards of scoping or output as well as checks that need to be conducted [37]. In addition to the previous testing frameworks such as PTES or OSSTMM, that a provider of security testing methods can use and adapt to its own needs and provide to its customers, organisations can certify their penetration testing methodology according to NCSC's CHECK and are then listed by the NCSC as a CHECK-approved provider [38]. However, this methodology is heavily focused on UK organisations and accordingly only of limited interest to this study as it falls out of scope.

2.3.5 Information System Security Assessment Framework

The Information System Security Assessment Framework (ISSAF) by Open Information Systems Security Group (OISSG) is a very extensive security framework covering various forms of network and system penetration tests [39]. These various forms include for example switches and routers, firewalls, Intrusion Detection Systems (IDS) and anti-virus systems, wireless LAN (WLAN), storage, traditional host operating systems such as Windows, UNIX, Linux, Novell as well as typical services such as web servers and more. The framework even includes a chapter about social engineering. For each of these forms of penetration testing the framework includes an extensive description of the security testing method itself along with various objectives and guidance on the methodology including specific checks a provider testing this specific type of system or network should conduct.

The framework therefore combines various aspects in regards of methodology

as already seen in PTES and OSSTMM as well as guidance on how to test as seen in various resources by OWASP but focusing not on web applications but rather on networks as well as systems and services. However, the initial framework was never released as a stable or final release and the OISSG is discontinued since mid 2019 [40], so while it potentially could provide a lot of insight it covers rather old systems and techniques that are only of limited value today and is thus only of limited value to this research.

2.4 Related scientific work

In the field of related scientific work there can be seen similar problems as already encountered during the analyse of various best practice standards, white papers and guides: Some papers just broadly summarise various testing methods into one single method without considering the difference in execution and results each and every of these security testing methods would provide. For example Epling et al. states, while proposing a new methodology for reducing costs on penetration tests, that a vulnerability scan can be seen as an equal testing method to a penetration test [41]. Or Bishop states, while providing an introduction to ethical hacking services, that both ethical hacking and red teaming can be used as a synonym for penetration testing [42]. Other publications such as a paper by Saalem gives an introduction into security testing and ethical hacking as well as provides insights into its up- and downsides and even concludes about the importance of regularly perform security testing but without any guidance on potentially suited methods or further information on how to perform such activities [43]. Other research provide good definitions of specific security testing methods such as the definition about penetration testing and social engineering provided by Berger and Jones in their publication about ethical hacking services for small and medium enterprises (SME) [44]. However, ironically enough, the research papers able to provide a good and comprehensive definition did not use other scientific work as their main source of information but rather reference to websites of third party vendors and providers of ethical hacking services such as Rapid7 (`www.rapid7.com`) [44]. And even if various security testing methods are correctly explained and compared as done by Khera et al. [45], it only considers two or three technical security testing methods at most and therefore still lacks a broader overview and comparison of relevant technical security testing methods in one single analysis.

Chapter 3

Methodology

This chapter describes what research methods were applied and why a specific research method was chosen to answer the research questions from the previous chapter. In addition, it is explained how various methods were applied throughout this study.

3.1 Research model

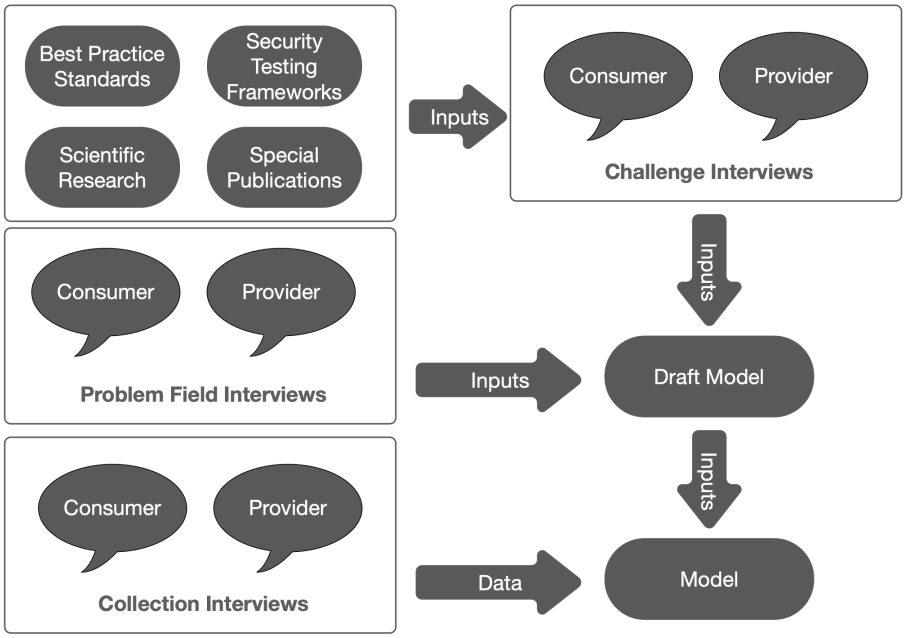
This research methodology can be summarised through the following high-level model including the various stages of this study as illustrated in 3.1.

3.2 Literature review

To gain the initial knowledge about the research area to start this study, a literature review was conducted. During this review not only scientific research and publications were analysed and considered but as well official best practice standards such as ISO 27001, PCI or NIST and best practice publications by well-known organisations such as NIST, ENISA or SANS to collect the necessary understanding about the current situation and challenges. The method applied during the literature review was based on a method published by Cronin et al. along the following four steps [46]:

- **Selecting a review topic**: Based on the initial idea for this study the broad topic for the literature review was established as described in the previous chapter.
- **Searching the literature**: In a next step the initial topic was structured in keywords that can be used to search the literature. Existing keywords were challenged, and new keywords added along the way of the literature review as soon as new insights about the field could be gathered. Main sources for the literature review were NTNU's Oria (`https://innsida.ntnu.no/en/litteratur`) as well as Google Scholar (`https://scholar.google.com/`).

Figure 3.1: High-level research model



- **Analysing the literature**: The most time-consuming step of the literature review was to scan through and review all relevant literature identified through the initial two steps. In order to conduct this step in an as efficient way as possible, literature was initially collected in JabRef (`https://www.jabref.org/`) and in a second step briefly analysed to identify not relevant literature. In a third step, the remaining literature was analysed in detail and tagged and commented along the way for further reference.
- **Writing the review**: The review was then written and included in the chapter "Background and Related Work" and the structure of the literature review was adapted to fit the template provided.

3.3 Research design

In a second step, a research design was decided on. The two models to decide on where either quantitative research or qualitative research. According to Blanche, quantitative research is based on a larger collection of data and use statistical methods of analysing the data in order to answer a research question, while qualitative research collects information based on written or spoken language and analyse this data based on observations and categorisation [47]. Because the field to be observed is a rather new and young field of science a lot of knowledge about it is held solely by subject matter experts within various organisations or even

military and governmental institutions and is normally not openly shared or even available to the academic community. Therefore, a broad collection as this would be the case with quantitative research, is not feasible as it would be rather tough to reach a critical mass to get a reliable data set or even get the proper answers for the research questions. Thus, it was decided to use a qualitative research approach, focusing on gathering information based on selected subject matter expert interviews.

3.4 Expert interviews

Based on the decision on a research design, subject matter expert interviews are the main source of information in order to answer the research questions. In regards of different ways to perform an interview, according to Heery two main form of interviews are to be considered: Structured interviews, where all questions are defined in advance and each interviewee is asked the exact same set of questions. Or unstructured interviews, where questions are not planned beforehand and not each interviewee is asked the same set of questions depending on the progress of the interview [48]. While the first form of interview is highly structured and therefore allows for direct comparison between various interviewees, the second form allows to collect broader insights and gives the interviewer room to ask additional questions in order to let the interviewee elaborate more on specific nuances or new insights. Accordingly, this allows the interviewer to collect more information in potentially less interviews. While both interview techniques have their advantages, a third form of interviews can be considered as well: Semi-structured interviews, according to Galletta combines all advantages of structured and unstructured interviews and can provide enough structure to allow for comparison and in the same time allow enough flexibility to allow the interviewees to introduce new meanings into the field of study [49]. Consequently, semi-structured interviews were defined as the form of expert interviews to be used during this study while using more unstructured interviews throughout the first phase to gain enough insights into the field of study and the problems within and then move onto more structured interviews for the second and third phase as the study progresses.

In order to maintain the level of trust towards the interview partners while they are sharing potentially sensitive and company-internal information through various interviews, all interview partners were anonymised, and their names were replaced with a short description about the interviewees and their current positions or experience in the field. The company name is further anonymised as well and replaced with a brief description of the broad industry the company is assigned to. Furthermore, each conducted interview is labelled with a reference that can be used to link a reference with a certain interviewee. And as most of the conducted interviews were held in the writer's native language either in high German or Swiss German, no transcript for each interview was generated as it would

not be in the same language as this thesis and was replaced with an interview summary translated to English as included in the appendix in A.1.

3.4.1 Selection of interview partners

As most of this study's insight depends on input and insights from interview partners, access to relevant subject matter experts available for one or more interviews is key to its success. To gain access to various interview partners, the author of this research utilised his own direct and indirect network based on over ten years of working in the field as well as through specific key people. As the author's network is mainly located within Switzerland, connections established during the author's studies at NTNU with other part-time students working in the field were used additionally to gain access to relevant interview partners in Norway. Also, the personal network of the thesis's supervisor, Prof. Dr. Bernhard Haemmerli with extensive and numerous connections throughout Switzerland and Norway's security community [50] was utilised as well.

3.4.2 Phase 1: Problem field interviews

To gain insights into to problem field, an initial round of rather unstructured and open interviews was conducted with two subject matter experts from a provider's side as well as with a subject matter experts from a consumer's side to get a better insight into the area of research. During this phase the following three interviews were conducted:

Table 3.1: List of problem field interview partners

Date	Form	Interviewee	Topic	Reference
2021/03/17	Online	Cyber security specialist in Norway's ICS sector [P-001]	Problem field interview about security testing in Norway.	INT-001 (A.1.1)
2021/03/18	Online	Chief Information Security Officer (CISO) in the insurance sector [P-002]	Problem field interview about traditional and new forms of system security testing and verification.	INT-002 (A.1.2)
2021/03/22	Online	Lecturer about cyber security and former ethical hacker [P-003]	Problem field interview about security testing in Switzerland.	INT-003 (A.1.3)

3.4.3 Phase 2: Challenge interviews

During the second phase of interviews, two more interviews with a subject matter expert from a provider's and a consumer's side were conducted to challenge, extend and sharpen the initially defined definitions as well as the defined criteria for usage and performance:

Table 3.2: List of challenge field interview partners

Date	Form	Interviewee	Topic	Reference
2021/08/29	Online	Cyber security manager in the financial sector [P-004]	Challenge interview about relevant security testing methods, their definitions as well as possible criteria for usage and performance.	INT-004 (A.1.4)
2021/09/23	In-person	Head cyber security for a cyber security firm [P-005]	Challenge interview about relevant security testing methods, their definitions as well as possible criteria for usage and performance.	INT-005 (A.1.5)

3.4.4 Phase 3: Collection interviews

After combining all collected information from the interviews from phase one and two into the initial method landscape model, a third round of interviews were conducted to fill the model with relevant data based on the insights from five subject matter experts. During this phase the following five interviews were conducted:

Table 3.3: List of collection field interview partners

Date	Form	Interviewee	Topic	Reference
2021/11/07	Online	Cyber security manager in the financial sector [P-004]	Collection interview to collect data for the defined model from a consumer's perspective.	INT-006 (A.1.6)

Date	Form	Interviewee	Topic	Reference
2021/11/09	In-Person	Head cyber security for a cyber security firm [P-005]	Collection interview to collect data for the defined model from a provider's perspective.	INT-007 (A.1.7)
2021/11/09	In-Person	Penetration tester for a cyber security firm [P-006]	Collection interview to collect data for the defined model from a provider's perspective.	INT-008 (A.1.8)
2021/11/10	Online	Cyber security manager in the financial sector [P-007]	Collection interview to collect data for the defined model from a consumer's perspective.	INT-009 (A.1.9)
2021/11/11	Online	CISO in the health sector [P-008]	Collection interview to collect data for the defined model from a consumer's perspective.	INT-010 (A.1.10)

3.5 Ethics

In order to gain insights through interviews, a large set of information needs to be collected and analysed in a responsible way. Furthermore, the interviewee demands a high level of trust from the interviewer to disclose various insights into sometimes an organisation's internal processes as well as his or her own personal experiences. Therefore, the author of this study committed to the following principals of ethics to honour the interviewees trust:

- **Personal data**: All personal data collected through our interviews where stored with a reference and a description as listed in the previous chapters and not with a full name or additional information about the interviewee and can accordingly not be directly linked by just gaining access to our notes and documents. All data was stored encrypted throughout this research and will be deleted upon completion of this study.

- **Informed consent**: All interviewees were informed before the interview about the form of the interview and our intention of usage as part of this study and consented to the interview by accepting our meeting invitation and agreeing to the interview as the first question of each interview.
- **Anonymity**: As already stated in the previous chapter, all interviewees were anonymised to protect the information and insights they contributed to this research and honour the level of trust provided in us while disclosing insights and personal experience.
- **Deletion**: Once information collected for this study is no longer needed, all notes and documents related for example to a specific interview will be destroyed.

Chapter 4

Results

In this chapter, the results of this study are described in detail to answer the research questions while applying the described research method.

4.1 Technical security testing methods

In order to answer the research questions and assign various criteria for usage and performance to specific security testing methods, a set of relevant technical security testing methods needs to be established first. Based on the relevant scientific work as well as the analysis of best practice standards and special publications from various sources, the following set of relevant security testing methods was compiled and enriched with a formal description as listed in table 4.1. Where possible, already existing definitions were used directly or used as template and adapted or extended to represent all the nuances of the describing technical security testing method. In addition, a mapping for all security testing methods to the seven phases of the well-known cyber kill chain framework by Lockheed Martin [51] as well as PTES was created to illustrate the peculiarities of each method in a summarised and graphical overview. Both results were then further challenged and completed through the second phase of expert interviews and further improved along the progress of this study:

Table 4.1: Landscape of relevant security testing methods

Method	Description	Synonym(s)
Vulnerability Scanning	Identify vulnerabilities that, if exploited, may result in a compromise of an information system or its connected resources by testing a given set of currently known weaknesses fully-automated against the evaluated system(s) [2].	Vulnerability Assessment or Analysis [19]

Method	Description	Synonym(s)
Penetration Testing	Identify and exploit vulnerabilities while circumventing security measures through a combination of automated and manual testing for each component of an information system to identify inter- or intracomponent vulnerabilities that can be exploited to compromise the evaluated system or its connected resources [52].	Security Audit, Security Assessment
Phishing	*Tricking individuals into disclosing sensitive personal information by claiming to be a trustworthy entity in an electronic communication (e.g., internet web sites) [53]* as a form of social engineering.	Spear Phishing, Mass Phishing
Social Engineering	*The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust [54].*	-
Red Teaming	*An exercise, reflecting real-world conditions that is conducted as a simulated adversarial attempt to compromise organisational missions or business processes and to provide a comprehensive assessment of the security capabilities of an organisation and its systems [18]* without the knowledge of an organisation's defensive (blue) team [55].	Red Team Assessment or Exercise, Attack Simulation, Assume-Breach Simulation
Bug Bounty Program	A reward program offered by an organisation for other organisations or private ethical hackers, so called "hunters", allowing them to attack the systems in scope to identify, exploit and report vulnerabilities. A hunter under such a program gets compensated for his work with a "bounty" for each reported and valid, that means reproducible and not excluded in this specific program, vulnerability. The bounty's amount depends on the program itself as well as on the level of criticality an organisation assigns a specific vulnerability [56].	-

4.1.1 Sub-Methods

While some of these technical security testing methods are rather specific, other methods combine various sub-types of testing methods that all still fulfil the formal definition of the greater method but in addition to that are more specific for a certain type of technology or form of delivery. This includes mainly the technical security testing method *penetration testing*, *phishing*, *social engineering* as well as *bug bounty programs* that commonly are divided further.

Penetration testing

Penetration tests as a technical security testing method can be divided further in regards of the type of system or technology it is used against while still following the greater definition of a penetration test [57]. Commonly the type of system or technology it is applied against is prepended to the testing method to describe a specific type of penetration testing. For example a penetration test of a web application is commonly referred to as *web application penetration testing* [58]. Such combinations can be crafted with nearly all types of systems or technology. According to related scientific work as well as best practice standards, the following sub-categories are most commonly used:

Table 4.2: Landscape of penetration testing sub-methods

Sub-Method	Description	Synonym(s)
Application Penetration Testing	Testing of applications of any kind. This includes web applications and application programming interfaces (API), common applications such as thick clients as well as mobile apps in order to gain more control over a certain application than intended by its developer [17].	IS-Webcheck [16]
Network Penetration Testing	Testing of network devices, subnets and whole networks in order to gain more control over connected systems and services than intended by its system administrator or engineer. This category gets often divided further into internal and external network penetration testing depending on the accessibility of the tested systems [58].	-

Sub-Method	Description	Synonym(s)
Client Penetration Testing	Testing of a host in order to gain more control over the host itself or its resources than intended by its engineer [57]	Host Penetration Testing, Hardening Review
Physical Penetration Testing	Testing of any physical security measures by simulating a physical intruder or burglar while trying to get physical access to information or to a network or host [58].	-
Wireless Penetration Testing	Testing of wireless systems including various wireless protocols such as WLAN, Bluetooth, Bluetooth low energy (BLE), Zigbee and similar to gain access to information or access to a host or network in order to continue with another type of attack [58].	-
Hardware Penetration Testing	Testing of any device with focus on its hardware. While client penetration testing most commonly focuses on a host's functionality on a digital layer, a hardware penetration test focuses on a host or device's hardware itself in order to gain more control over the hardware.	IoT Penetration Testing

In addition to various forms of penetration testing, different approaches of penetration tests are distinguished as well. This includes the following three approaches [1]:

- **Black-box testing**: Black-box testing describes an approach, where the penetration tester do not get any additional information or insights into the to-be-tested scope mimicking the same level of information an external attacker would have.
- **White-box testing**: White-box testing describes the opposite of black-box testing, where the penetration tester have full insight and access to any information about the scope including but not limited to documentation, designs, credentials as well as source code and technical personnel responsible for the scope's engineering and operation.
- **Grey-box testing**: Grey-box testing describes an approach between black- and white-box testing. This approach describes, that the penetration testers have certain basic insights and knowledge as for example an insider would have about the to-be-tested scope. However, the amount of information and

insights a penetration tester get about the scope is not standardised and is normally discussed and defined during preparation.

Phishing

In regards of phishing, the main testing method gets divided further by the way a phishing message is delivered to its victim. Mainly the following three categories are distinguished [59]:

- **Phishing**: While phishing can be used for any kind of phishing attack it normally refers to a phishing message delivered by e-mail.
- **Vishing**: This form of phishing is short for voice phishing and describes a phishing message that is delivered via a phone call.
- **Smishing**: This form of phishing is short for SMS phishing and describes a phishing message delivered via short message service (SMS).

Social engineering

In regards of social engineering, the main testing method can be further divided into different forms of attack vectors. While phishing can be considered a sub-category of social engineering as it exploits the human factor as well [60] for this research it was decided to list it as a separate testing method after the initial round of problem field interviews as the general knowledge of phishing attacks is much higher and the usage of phishing as a testing method in comparison to other forms of social engineering is much more common [10]. Therefore, the following attack forms are considered a sub-form of social engineering attacks [60]:

- **Baiting**: Through dropping "bait" mostly in form of USB devices in front of strategic locations such as parking lots of an organisation's main entrance an attacker tries to deploy malicious files on a victim's computer.
- **In-person**: Through directly approaching an organisation's employees in-person an attacker can gain access to an organisation's building or collect relevant information. An important technique as part of such attacks is named "tailgating" or "piggybacking" during which an attacker just follows an employee or a group of employees inside an organisation's building or to circumvent physical security measures by for example picking a lock.

Bug Bounty

In regards of bug bounty programs, normally the openness of a specific program is distinguished. This is described by labelling a bug bounty program as public or private and prepending this term. A public bug bounty program therefore describes a program that is open to any kind of hunters while a private bug bounty program is only accessible by invitation and thus limited to a specific group of bug bounty hunters [61].

4.1.2 Not-covered security testing methods

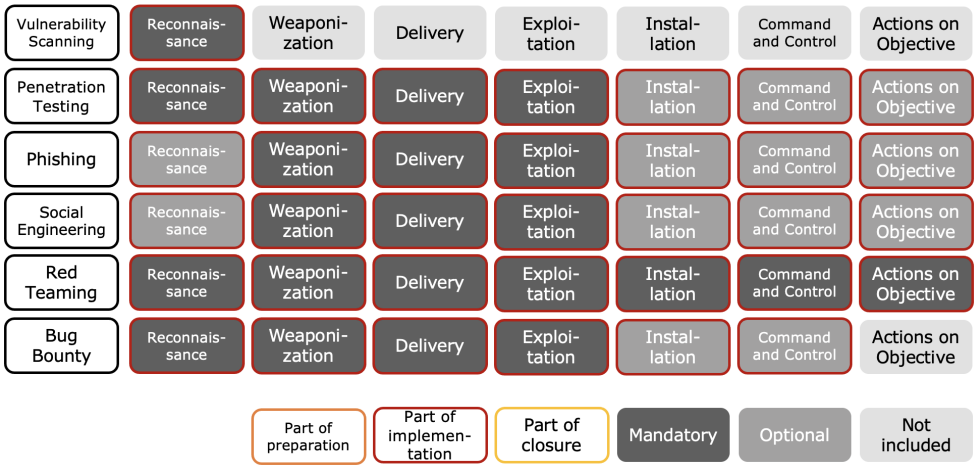
Not covered by this research are all non-technical security testing methods. This means, that for example classical forms of auditing based on interviews or workshops are not included even if these methods include a certain degree of technical verification in form of a spot check through a given sampling rate. Further not included are any type of theoretical methods such as table-top exercises or static analysis methods such as various types of reviews like source code or configuration reviews. This delimitation was necessary to create a subset of relevant security testing methods that share similarities up to a certain degree that would allow for meaningful comparison among these methods. Further it was necessary because the consideration of too many different security testing methods would automatically have led to less focused criteria for usage and performance, as otherwise it would not be possible to apply each criterion to each testing method equally. This would have inevitably introduced a high degree of blurriness into the final landscape model as not all testing methods would have been comparable to each other anymore. To avoid this, the group of relevant security testing methods was narrowed down to only methods that allow for direct comparison by considering only technical security testing methods.

4.1.3 Peculiarity model

To illustrate the technical security testing method's unique peculiarity based on the gained insights through the literature review and the expert interviews, a peculiarity model was created that maps out the different phases for each of the security testing methods. As basis for such a model, initially a mapping to the seven phases of the well-known cyber kill chain framework by Lockheed Martin [51] was conducted. For this model each phase and each testing method was analysed and decided, if this phase is considered mandatory, optional or not covered at all to complete the testing method. Furthermore, each phase indicates, if the steps within this phase are covered as part of the method's preparation, implementation or closure. This results in the model as show in figure 4.1. However, as the model shows clearly, the cyber kill chain is strictly focused on the implementation of an attack itself. While this reflects the main field of application for the cyber kill chain [62], this introduces a fair amount of blurriness into the model as all actions taken prior and after the implementation are not visible through the model and therefore not visible.

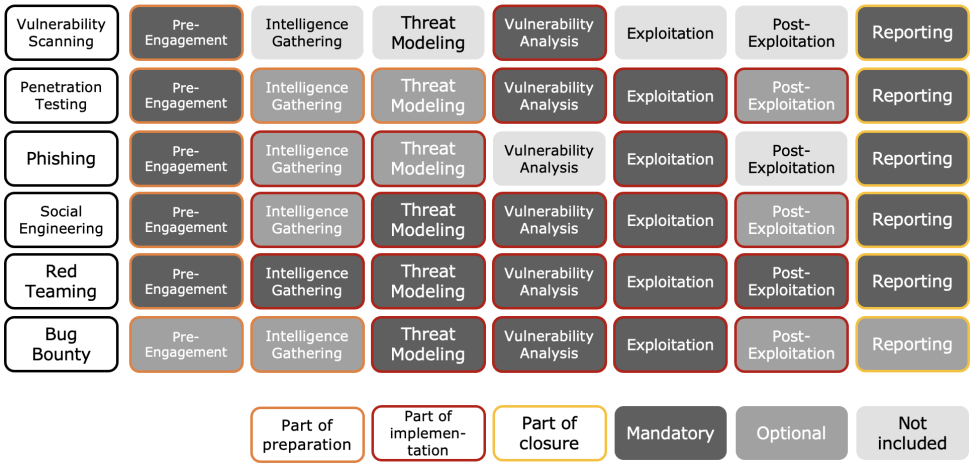
To reduce this blurriness, the same mapping was again conduced based on the seven phases of PTES as this framework contains additional phases covering the preparation, the implementation, as well as the closing of the applied security testing method and therefore potentially allows for a more ideal comparison across various testing methods. This then results in the model as listed in figure 4.2. While this model provides a good overview and illustrates a specific testing method's peculiarity very clear, it still holds a small amount of blurriness in re-

Figure 4.1: Security testing methods mapped to the cyber kill chain's phases



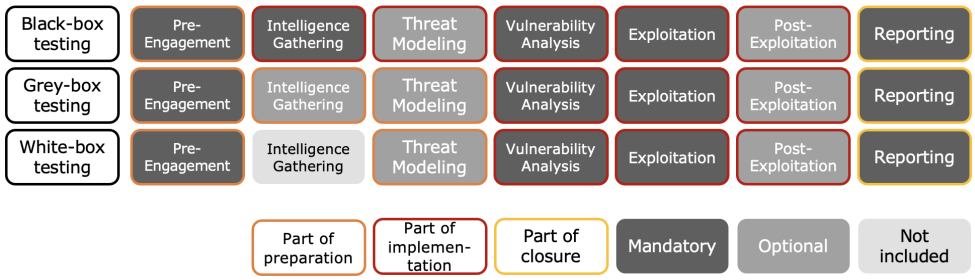
gards of certain subcategories of a specific testing method. For example, while a penetration test may or may not include intelligence gathering as part of the preparation, this fact really depends on the approach chosen to perform the penetration test. This can be clearly seen if the same mapping is created for different approaches of penetration testing as shown in figure 4.3. Here it can see that certain phases are more affected by the chosen approach in comparison to the testing method in figure 4.2 while others not.

Figure 4.2: Security testing methods mapped to PTES phases



A larger version of the peculiarity model is included in the appendix in chapter A.2 for further reference in landscape format.

Figure 4.3: Different approaches of penetration testing mapped to PTES phases



4.2 Criteria for usage and performance

To generate a method landscape of relevant technical security testing methods it is important to have a qualitative and comprehensive set of criteria for usage and performance in order to further define and categorise each testing method and allow for further comparison inside the method landscape. Therefore, the following subset of criteria was established and further challenged and improved along the way with feedback from related work as well as expert interviews:

- **Insight**: Defines the amount of insight an organisation can get in regards of the defined scope while applying a specific method. Accordingly, this property helps defining how much insight a certain method can provide in regards of the scope.
- **Depth**: Measures, how complete a certain method can cover the overall scope in regards of identifying all potentially to-be-identified risks in a certain scope.
- **Management Attention**: In some situation a certain method is applied not in order to gain new insights and identify new risks but rather to enable management attention to get a certain projects or management decisions approved. With this criterion the attention towards the management a certain method can generate is measured.
- **Comprehensibility**: This criteria measures, how easy understandable a certain method and its deliverables are. As easier a specific method or its deliverable are to understand, as easier it is to apply and use it along all levels.
- **Structuredness**: Especially in regards of coverage and repeatability a high structuredness for a specific method is desired. In addition to that, as more structured a certain method is as easier it is to get comparable results across various providers. Conversely, as unstructured a certain method is, as more dependant is a successful result from a specific provider.
- **Duration**: Various methods have different durations in regards of time needs to pass before the testing method can be completed and results can be provided. As this impacts the overall project duration and various other aspects such as for example the complexity to handle the project on the consumer's side.

- **Preparation**: The preparation varies across different testing methods as certain methods can be applied right away without further preparation while other methods demand various action items to be prepared beforehand to efficiently and successfully apply a certain testing method.
- **Costs**: The costs a consumer has to pay for a certain testing method to the provider in order for him to provide this testing method.
- **Maturity**: Technical security testing methods have different preconditions that an organisation has to meet in order to gain the optimum out of a certain testing method. This maturity is measured by applying the Capability Maturity Model Integration (CMMI) maturity model [63].
- **Knowledge**: The overall level of confidence in regards of the rated technical security testing method based on the expert's theoretical or practical experience.

All the above criteria except for the maturity and the knowledge are meant to be rated from one to ten, while one is meant to be the lowest or minimum and ten the highest or maximum value. The maturity is rated from one to five as defined by the CMMI maturity model [63] while the knowledge is rated from one to six according to the Swiss school grading system where one is considered the lowest and six the highest grade.

To provide meaning through various criteria and allow for comparison of different security testing methods, the listed criteria need to be summarised and combined without losing its initial value. To achieve that, two additional summary criteria where defined that combine the detailed criteria through a formula each.

4.2.1 Performance

One of the important factors while comparing different security testing methods is the benefit it can provide the organisation that is applying a certain method. This is summarised as the overall performance (PF) and combines the following detailed criteria:

- Insight (IN)
- Depth (DE)
- Management Attention (MA)
- Comprehensibility (CO)
- Structuredness (ST)

These detailed criteria are considered through the following formula:

$$PF = round(mean(DE, CO, ST, max(IN, MA)), 1)$$

This formula calculates the arithmetic mean across all included values and rounds the value to one decimal place. However, the formula only considers the

higher value for the criterion IN and MA. The reason for that is that both criteria are competing values and working mainly against each other. While IN is mainly focused on providing maximum insight through results and is therefore more focused on technical personnel, MA is more focused on provide understanding or even a moment of shock and is accordingly more focused on management personnel that manage the budget and do not have a very deep technical understanding. If these counteractive values would now be combined through the arithmetic mean the overall formula would lose both criteria because they would nullify each other. Hence, only the higher criterion was considered in the overall performance formula. However, to compensate for this slight blurriness introduced, two additional sub-criteria were defined as well:

- **Management Performance (MP)**: The management performance additionally summarises the criteria MA and CO in order to measure the level of suitability for non-technical personell.
- **Technical Performance (TP)**: The technical performance additionally summarises the criteria IN and DE in order to measure the overall benefit a certain method can provide not only in regards of the defined scope but rather a company as a whole.

These additional sub-criteria allow for a comparison that provide additional insight for the ideal target audience while still allowing a full comparison in regards of the overall performance. Both sub-criteria are based again on the arithmetic mean and rounded to one decimal place according to the following formula:

$$MP = round(mean(MA, CO), 1)$$

$$TP = round(mean(IN, DE), 1)$$

4.2.2 Usage

The other important factor while comparing different security testing methods is the overall feasibility and practicability a method can provide an organisation with. This is summarised as the overall usage (UG) and combines the following detailed criteria:

- Duration (DU)
- Preparation (PR)
- Costs (CT)

These detailed criteria are summarised through the following formula that utilises also the arithmetic means across all included values and rounds the result on one decimal place. In contrary to the performance where a certain criterion is considered better as higher it gets, in regards of usage this is inverted because a criterion is better as lower it gets. But in order to still allow for direct comparison, the result is inverted again by subtracting the result from the maximum value on the scale:

$$UG = round(10 - (mean(DU, PR, CT)), 1)$$

4.2.3 Maturity and knowledge

The only remaining criteria now are the maturity (MT) and knowledge (KN). Both criteria are considered as a statement on their own as the knowledge will be used to rate the provided input by the experts while the maturity is considered more as a go/no-go criterion defining if a certain technical security testing method is recommended to apply for a specific organisation. Thus, both criteria are not used in any calculation but rather used directly.

4.3 Method landscape model

Based on the detailed and summary criteria as well as the initially defined relevant technical security testing methods a method landscape can now be generated.

4.3.1 Initial landscape

As the first step an initial landscape was generated by rating each of the detailed criteria according to the defined rating schema based on the author's experience. This was used to test the model itself and the applied formulas and to build a hypothesis as a basis for the landscape that can then be used as starting point for the collection interviews with various subject matter experts. For the initial landscape, the following initial rating was used for the performance criteria as shown in table 4.3 and the usage criteria as shown in table 4.4.

Table 4.3: Initial landscape for performance (PF)

	IN	DE	MA	CO	ST	PF
Vulnerability Scanning	6	5	1	2	10	**5.8**
Penetration Testing	9	10	3	4	8	**7.8**
Phishing	3	5	7	8	4	**6.0**
Social Engineering	4	2	6	8	2	**4.5**
Red Teaming	6	4	8	8	3	**5.8**
Bug Bounty Program	5	2	2	3	3	**3.3**

Table 4.4: Initial landscape for usage (UG)

	DU	PR	CT	UG
Vulnerability Scanning	2	2	2	**8**
Penetration Testing	4	5	5	**5.3**
Phishing	2	2	4	**7.3**
Social Engineering	2	4	3	**7**

	DU	PR	CT	UG
Red Teaming	8	5	8	**3**
Bug Bounty Program	10	8	6	**2**

4.3.2 Final landscape

This initial landscape was then further improved by replacing the initial data with the data collected through the collection interviews from various subject matter experts. In order to get a summarised view on the final method landscape all the experts' inputs were combined through calculating again the arithmetic mean across each property but weighting each individual input according to the stated expert's knowledge of the individual testing method. For the through that generated "weighted mean" of criterion X, while $P_n(X)$ represents the collected value for X of Person N, this would result in the following formula:

$$weighted\_mean(X) = round(\frac{P_1(X) * P_1(KN) + ... + P_N(X) * P_N(KN)}{P_1(KN) + ... + P_N(KN)}, 1)$$

Through applying this formula for all criteria, this results in the final method landscape for the performance (table 4.5) and usage (table 4.6) criteria as well as the maturity (table 4.7). As the knowledge is used throughout the calculation as a weighting factor it is not listed anymore.

Table 4.5: Method landscape for performance (PF)

	IN	DE	MA	CO	ST	PF
Vulnerability Scanning	6.8	6.1	3.4	5.6	8.7	**6.8**
Penetration Testing	7.6	8.2	4.9	5.4	7.8	**7.2**
Phishing	5.0	4.9	7.1	8.7	5.9	**6.6**
Social Engineering	4.4	2.8	5.1	7.1	4.4	**4.9**
Red Teaming	6.8	5.0	7.1	6.0	5.4	**5.9**
Bug Bounty Program	6.3	6.3	5.1	5.0	4.9	**5.6**

Table 4.6: Method landscape for usage (UG)

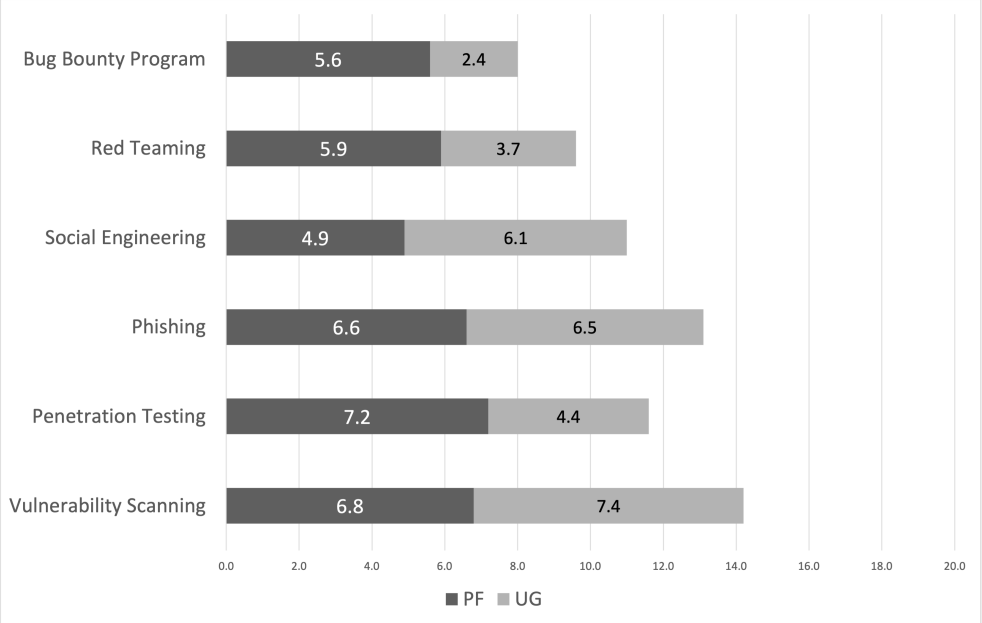
	DU	PR	CT	UG
Vulnerability Scanning	2.2	2.7	2.9	**7.4**
Penetration Testing	5.6	5.3	5.8	**4.4**
Phishing	3.0	4.4	3.2	**6.5**
Social Engineering	3.5	4.4	3.8	**6.1**
Red Teaming	6.5	5.2	7.1	**3.7**
Bug Bounty Program	7.7	7.9	7.1	**2.4**

Table 4.7: Method landscape for maturity (MT) according to CMMI

	MT	$Range$
Vulnerability Scanning	2.9	**2 - 3**
Penetration Testing	2.4	**2 - 3**
Phishing	1.8	**1 - 2**
Social Engineering	1.6	**1 - 2**
Red Teaming	3.2	**3 - 4**
Bug Bounty Program	3.7	**3 - 4**

Based on the final and weighted data, the two summary criteria (PF, dark-grey) and (UG, light-grey) can now be plotted in combination with each other to visualise the final method landscape model as shown in figure 4.4 and allow for a certain prioritisation across the final method landscape.

Figure 4.4: Method landscape combining PF and UG



4.3.3 Insights from method landscape

Based on this data, different plots can now be generated to provide various insights based on the method landscape model and the detailed and summary criteria.

Criterion-based analysis

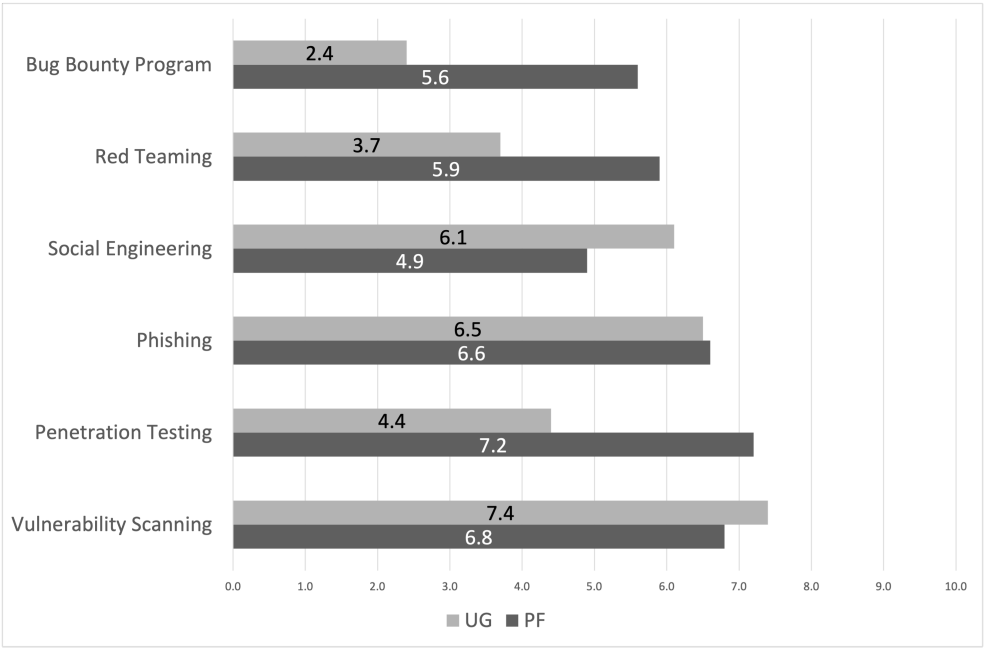
For example each criterion can be plotted individually as included in A.3 to get sort of a ranking across various technical security testing methods based on a specific

criterion. For example, in regards of potential insights a specific testing method can provide, the plot in figure A.14 shows that penetration testing can provide the most insight across all compared testing methods directly followed by vulnerability scanning and red teaming. However, social engineering and phishing can still provide some insights but not as extensive as the others. However, in regards of the duration, the plot in figure A.19 shows that phishing and social engineering can be conducted in much shorter time frame while bug bounty programs and red teaming will take up the highest amount of time.

Performance and usage analysis

In addition to that, the method landscape can be plotted by including the two summary criteria "performance" (PF, dark-grey) and "usage" (UG, light-grey) in comparison to each other allowing for direct comparison between performance and usage for each of the analysed security testing methods as shown in figure 4.5. Based on this and figure 4.4, it can be seen that vulnerability scanning and phishing have overall the best results for performance and usage together while bug bounty programs and red teaming seems to get a bit short. However, it must be considered, that the formula used to calculate the performance is only using the higher value of either the insight (IN) or the management attention (MA) and therefore presents a good overall ranking but can be biased up to a certain degree.

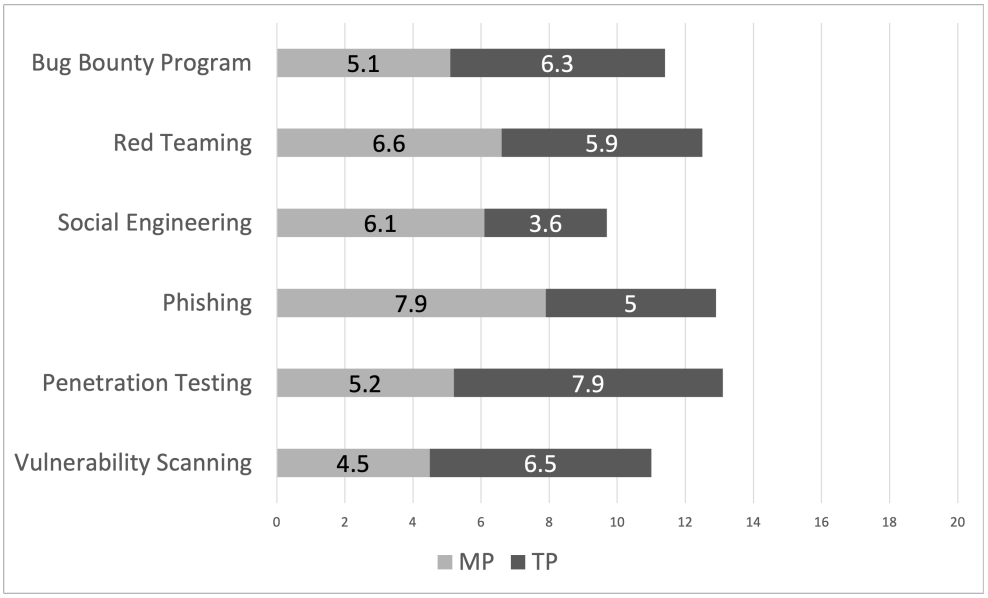
Figure 4.5: Method landscape comparing PF and UG



Technical / management trade-off

To resolve this bias, the management (MP) and technical (TP) performance as alternative indicators were introduced for this study. Those consider only the management attention (MA) in combination with the comprehensibility (CO) and the insight (IN) in combination with the depth (DE) of the testing method (figure A.22 and A.23). Based on this it can be seen, that while phishing has clearly the best management performance, it has some shortfalls in regards of the technical performance while penetration testing is exactly the opposite. In order to get an unbiased ranking across all testing methods, the technical / management trade-off can be further analysed by combining the management performance (MP) and the technical performance (TP) in a single plot. As shown in figure 4.6 it can be seen that red teaming seem to have a well-balanced ratio between management and technical performance while still providing a good performance overall directly followed by bug bounty programs while penetration testing and vulnerability scanning tend to rank higher on the technical point of view and social engineering and phishing tend to rank higher from a management point of view.

Figure 4.6: Management (MP) and technical (TP) performance in comparison

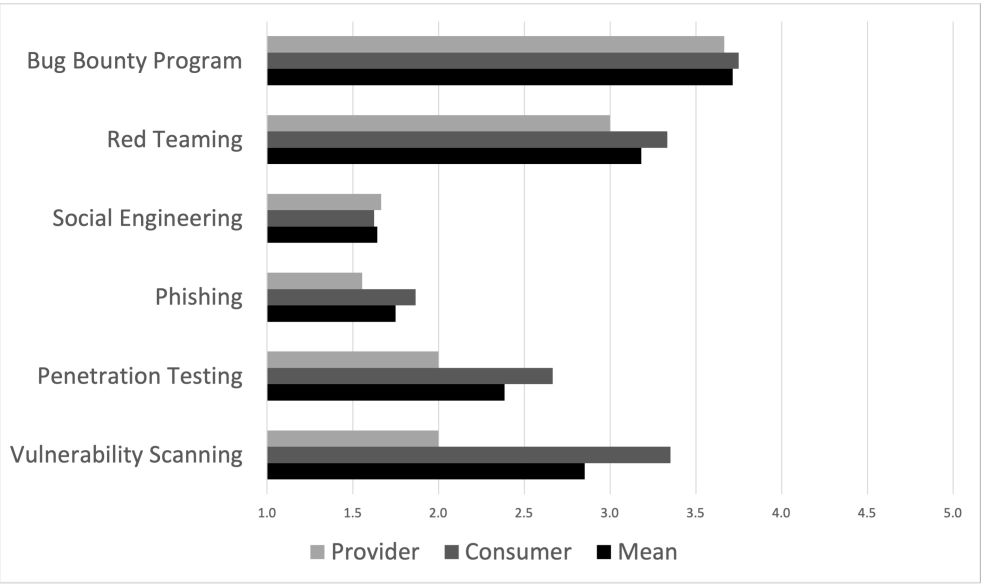


Maturity analysis

In addition to the performance and usage criteria, the maturity level according to CMMI an organisation should have to apply a certain testing method and the expert's overall knowledge about each testing method was also collected during the expert interviews, that can now be used for further insights. Based on the data regarding the maturity as show in figure 4.7 in black it can be seen that

testing methods such as bug bounty programs and red teaming exercises tend to require the highest maturity for an organisation to properly apply the method, while phishing and social engineering require the lowest maturity level and vulnerability scanning and penetration testing rank in between. If this ranking is compared to the individual plots of all criteria, this correlates with the two usage criteria "duration" (DU) and "costs" (CO). This correlation can most likely be explained through the fact that a longer duration and higher costs normally result from a more complex testing method and thus require more complex prerequisite from a consumer that automatically result in more complex project planning that again need a higher maturity level to fulfil this prerequisite efficiently. Another interesting difference can be identified once the weighted mean of the maturity required for a certain testing method is split up by experts from the provider and the consumer's perspective. As shown in figure 4.7 in dark and light-grey it can be seen, that experts from the consumer's side tend to rate the required maturity for a certain testing method slightly higher than experts from the provider's side. This study could not conclude on a reliable reason for this difference in the data.

Figure 4.7: Maturity of method landscape

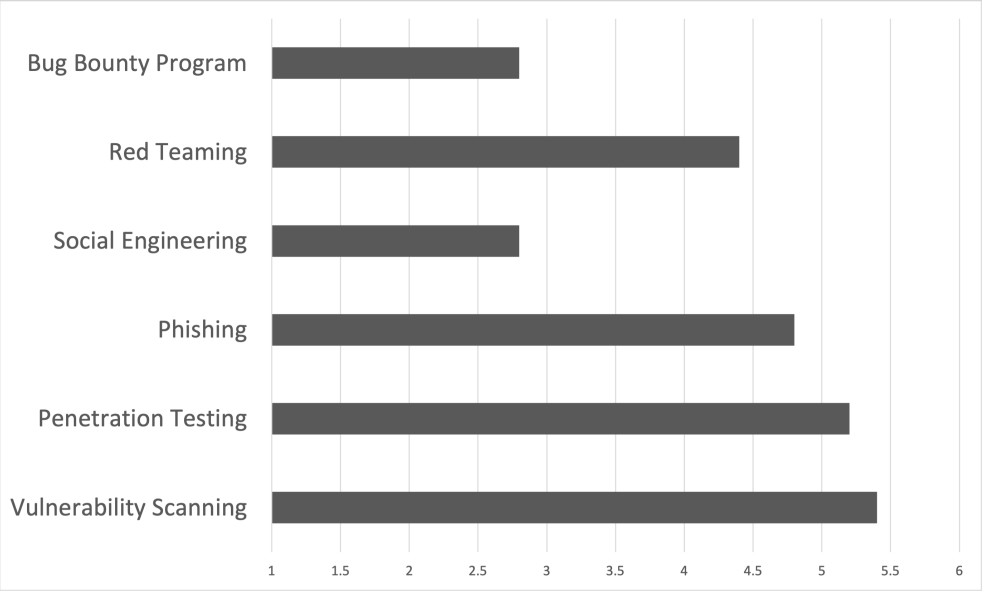


Knowledge analysis

A similar analysis can be conducted in regards of the expert's knowledge. This was rated by the subject matter experts about their own knowledge based on Swiss grading system. Based on this analysis as shown in figure 4.8, it can be seen certain testing methods such as vulnerability scanning, penetration testing and phishing are mostly well known, while testing methods such as bug bounty programs and social engineering tend to be more unknown. In regards of bug

bounty, this can be explained as this testing method is relatively new especially in Switzerland [64]. In regards of the testing method social engineering, if this testing method is compared with the individual plots of the performance criteria, social engineering usually ranks within the last place on insight, depth and structuredness as shown in figure A.14, A.15 and A.18 while still requiring a level of preparation similar to penetration testing as shown in figure A.20 at costs higher than phishing and vulnerability scanning as shown in figure A.21. Because of this lower overall performance combined with a still considerable amount of preparation needed and costs higher than other methods, this security testing method is most likely not commonly used across organisations and would consequently result in only a limited knowledge across the interviewed experts.

Figure 4.8: Expert's knowledge about method landscape



Further analysis

These analyses and conclusions just represent a small subset of potential interpretations that can now be deviated based on the created method landscape model and the collected data in order to proof certain assumptions and hypotheses. For example, it would be possible to compare specific testing methods against each other based on the complete set or just a sub-set of the used criteria or even to generate further summary criteria that suit the specific need of certain hypotheses to be explored.

Chapter 5

Discussion

This chapter reflects and discusses the various aspects of this study by reflecting on the initially defined research questions and this study's ability to conclude on them.

In general, this study could be completed as initially defined and planned at the beginning of the process. Only adoption to the initial goal was made to the fact, that it was initially planned to include not only the knowledge of subject matter experts about testing methods common in Switzerland but as well about testing method common in Norway to achieve a larger landscape and provide valuable inputs not only to organisations in Switzerland but for organisations in Norway as well. However, during the initial problem field interviews it could be seen that this would lead to more or less two disjunctive studies and therefore along the process it was decided to further reduce the initially planned scope to include only Switzerland as the author's place of residence. The main reason for this decision was that the two countries are more different in the testing methods that organisations normally apply than initially expected. More on this is explained in section 1.3 of this study.

Other than that, this study was able to conclude on all the initially defined research questions.

5.1 Research question 1

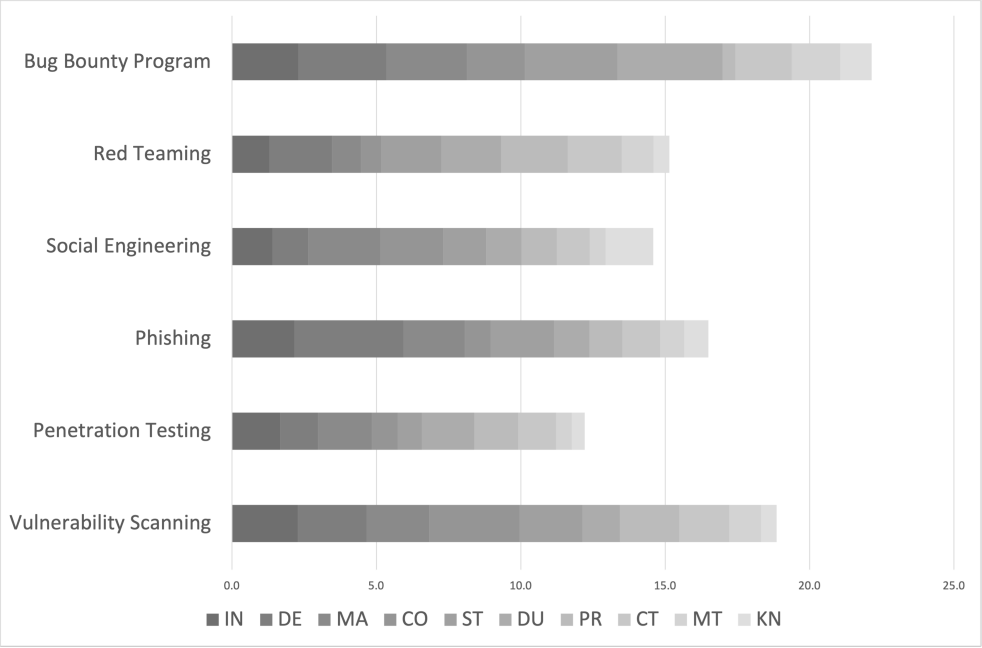
The goal of the first research question was to create a method landscape of relevant technical security testing methods and add relevant criteria for usage and performance to give the landscape more relevance. Based on related work and various inputs such as best practice standards, special publications and testing frameworks an initial set of testing methods was derived and defined and then further refined and improved through interviews with subject matter experts until a final set of technical security testing methods along with proper definitions could be created. The final set was then enriched with relevant criteria for usage

and performance and challenged as well through expert interviews. In the end, this resulted in the work presented in section 4.1 and 4.2 and was summarised in the peculiarity model as included in figure 4.2.

5.2 Research question 2

The goal of the second research question was to understand differences in the understanding of certain technical security testing methods across providers and consumers. During the initial phases of this study certain differences in understanding could be identified rather quickly during the analysis conducted on the background and related work as well as in the conducted expert interviews. Even during the collection interviews a certain degree of differentiation between experts could still be seen based on the collected data even though the experts were provided with a definition for each testing method resulting from the first research question. This allows us now to visualise this differentiation in understanding. Based on the collected data the standard deviation of all criteria for each testing method can now be plotted.

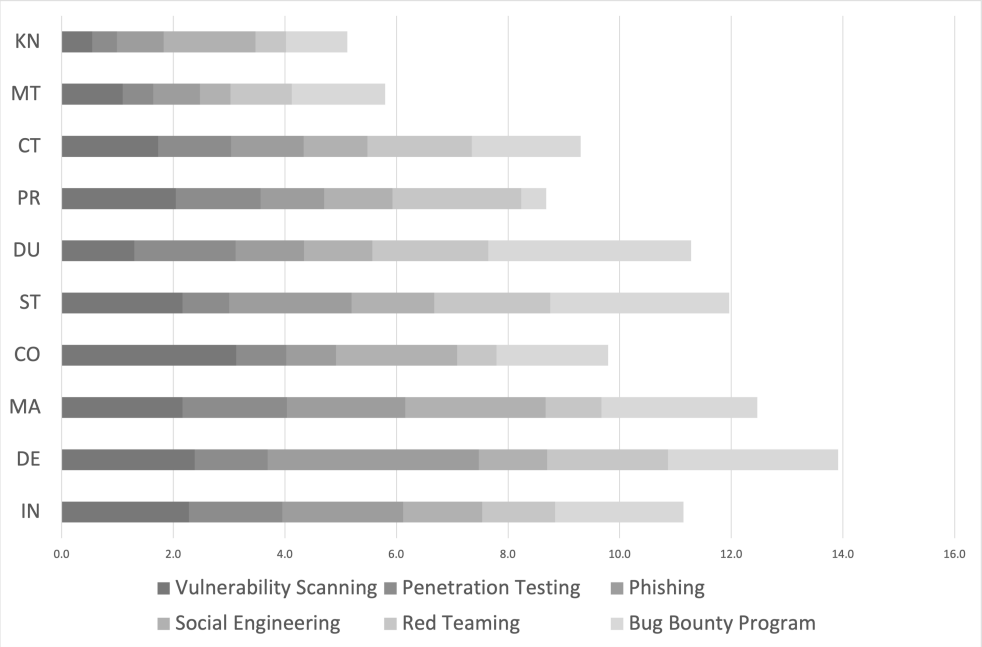
Figure 5.1: Deviation of method landscape by testing methods



In figure 5.1 it can be seen that especially for newer testing methods such as bug bounty programs an overall larger deviation could be observed as for example for more established testing methods such as penetration testing. This not only relates to certain testing methods but can also be observed in certain criteria once the standard deviation of all testing methods for each criterion is plotted. As show in figure 5.2 while certain criteria such as the required maturity (MT) or

preparation (*PR*) have a smaller overall standard deviation, other criteria such as the provided depth (*DE*) or the achieved management attention (*MA*) seem to be much harder to characterise among experts.

Figure 5.2: Deviation of method landscape by criterion

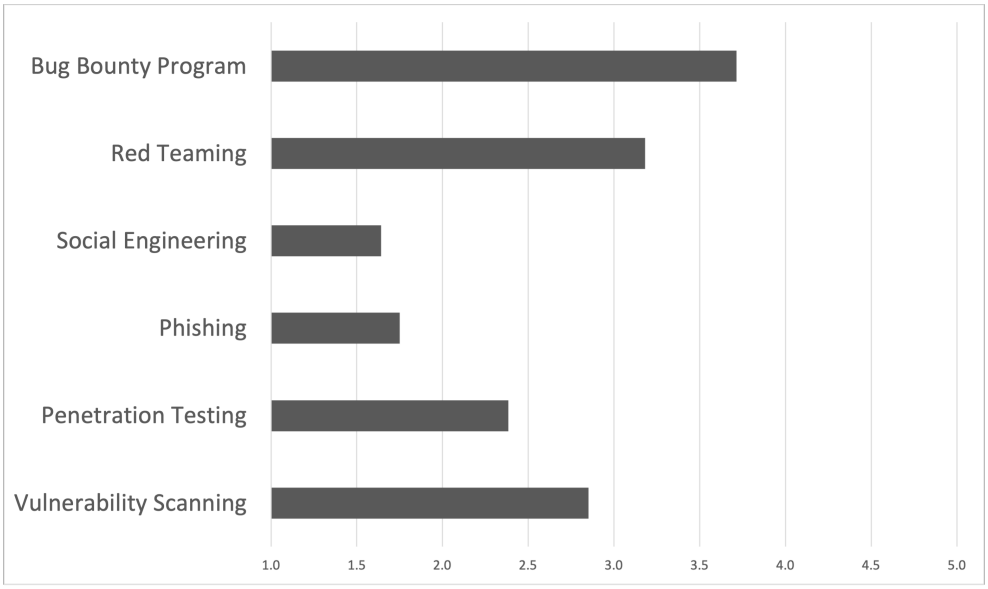


Based on these insights, this study concludes that even amongst subject matter experts there is a different understanding of certain technical security testing methods that would lead a provider to offer a different method for security testing method than initially requested by the consumer because most likely the provider and the consumer have not the exact same understanding throughout all testing methods from the security testing method landscape.

5.3 Research question 3

The overall goal of the third research question was to answer the question if certain technical security testing methods require a minimum maturity level according to the well-known CMMI model in order to properly being able to apply the analysed technical security testing method. Therefore, this criterion was collected during the collection interviews based on the expert's insights in addition to the other criteria. Based on the collected data it can be seen as shown in figure 5.3 that only a few methods seem to be suited once an organisation is still at the first maturity level according to CMMI. This includes technical security testing methods such as phishing and social engineering while other testing methods such as bug bounty programs and red teaming seem to require a higher level of maturity.

Figure 5.3: Maturity of method landscape



This fact can be further narrowed down and explained once the individual criterion plots are analysed in addition. In figure A.18 it can be seen that phishing as well as social engineering are rather unstructured methods compared to other testing methods but are, according to figure A.17 rather easy to understand and do not need a lot amount of preparation and project time as shown in figure A.20 and figure A.19. Unlike bug bounty programs and red teaming, that need nearly the highest amount of preparation and have the highest project duration that automatically result in a higher project complexity and more prerequisites to be fulfilled by the applying organisation. Based on this, this study concludes that not all testing methods can be properly applied across all levels of CMMI and simpler security testing methods such as phishing and social engineering should be conducted in preparation to increase an organisation's maturity level in regards of security before applying more advanced methods such as red teaming and bug bounty programs.

5.4 Research question 4

The goal of the fourth research question was to analyse and understand the difference between various providers of security testing methods and the question if a new provider can lead to new insights while applying the same security testing method. As already established during the discussion of the previous research questions, even amongst experts there is no consistent definition for certain security testing methods. Based on this, every security provider seems to use a slightly different definition and utilises his own understanding of certain technical secur-

ity testing methods that he applies once he conducts an assessment or analysis for an organisation as shown through the standard deviation in figure 5.1. Based on this, this study concludes that a new provider can lead to new insights even while applying the same testing method because every provider has its own definition of the same technical security testing method and thus utilises a different approach that could lead to the detection of still undetected vulnerabilities.

5.5 Research question 5

The last research question aims to reduce the already described mismatch in understanding of certain technical security testing methods and potential tools and recommendations that need to be developed to remove or reduce this mismatch. During this study it got clear, that even technical security testing is only what is referred to as "people business" and it is important for provider and consumer to have a good relationship from the start and once a provider gets to know a consumer and vice versa everything gets much easier over time. This is the reason why larger organisations run trial assessments together with a handful of providers in order to pick one or two providers that provide the expected results and put them on a short list to conduct all upcoming assessments for a specific period of time before the process starts all over again [10]. However, as especially smaller organisations cannot afford several trial runs in order to identify a suitable provider, this study concludes that the most efficient way of reducing a potential mismatch between a provider and a consumer is to establish a common understanding of the security testing method. During this study, this could be observed across the various stages of interviews. During the initial problem field interviews it was harder to get a common basis as the outcome of the first research question was not yet present. During the later interviews, the set of relevant security testing methods and their definitions could be used to gain a common understanding of the topic to be discussed. This made it significantly easier to collect the proper information needed. Accordingly, this study concludes that everybody seeking a common understanding in this field, should as well start off with a common basis and a clear definition. As tool to achieve that, this study provides a comprehensive set of security testing methods as well as definitions as included in chapter 4.1 that represents the best definitions across various best practice standards and related work as well as the opinion of selected subject matter experts in this field. This could for example be used by a consumer once he contacts different providers for his security testing project for a quote or vice versa, by a provider that offers his services to a consumer to provide a clear picture of what the consumer can expect and what he will provide after finishing the assignment.

5.6 Limitation of results

While this study was able to answer all of the initially defined research questions and can provide valuable insights into specific technical security testing methods and their most relevant properties it must still be considered that this study was conducted based on the opinion of a total of eight subject matter experts that can offer deep insight into the field in combination with a good reputation but just represent a small subset of all potential opinions that could potentially be considered and included as well. Due to the time-constraint a master thesis imposes, the used research model was not able to further collect a broader set of opinions for example through questionnaires that would have helped to reduce a certain bias through the selected experts. In addition to that, it must be considered that security testing is a very short-living field, and it is thus always possible that even during this study new sources of information arise that tend to provide a different or more in-depth view. And after all effort in selecting an appropriate and suitable security testing method, it must always be considered that certain industries tend to have regulations that require a certain testing method to be applied regardless of its suitability and an organisation then must comply with such regulations without having the flexibility to profit from this study by selecting the most suitable technical security testing method.

Chapter 6

Conclusion

During this study various security testing methods have been analysed in a structured and comprehensive way as, to the author's knowledge, no other research has done so far. The goal was to provide a set of relevant technical security testing methods along with broadly applicable definitions for each of the testing methods as well as a structured overview of each individual testing method's properties to provide a unified understanding across various testing methods as well as to aid in selecting an appropriate and suitable testing method for diverse requirements.

To achieve that, this study initially started with a literature review and collected extensive information from relevant scientific work as well as best practice standards and commonly known special publications and security testing frameworks in order to identify relevant security testing methods and identify previous work in the field. This information was then used to prepare and structure the following three phases of totally ten expert interviews with eight different subject matter experts each covering a specific topic along the research model. The outcome of this study now is a clearly defined set of technical security testing methods together with clear definitions summarising various best practice standards and other relevant sources and related work that were refined and further clarified and revised based on the inputs from subject matter experts in the field. In addition to that, this study provides a comprehensive overview of an individual testing method's properties through a set of relevant performance and usage criteria collected through interviews as well. Based on these data then various insights for specific use cases such as prioritisation of certain testing methods and other comparisons can be conducted that let to interesting new insights and a good model for further research.

Based on the initial research, the author hopes, that others can use this study as a basis for further research into the field helping to overcome the problems presented. Potential suggestions for further research could potentially include:

- Perform further analysis to prove specific hypotheses based on the collected data from the method landscape model.

- Add new testing methods and criteria to gain new insights based on the proposed model.
- Re-run the same research model for different countries or specific industries and gain insights based on differences between the involved parties.
- Replace data collected through the collection interviews with more scalable methods such as questionnaires to give the method landscape model more statistical relevance by including a broader view of opinions.

Bibliography

[1] J. N. Goel and B. Mehtre, 'Vulnerability assessment & penetration testing as a cyber defence technology', *Procedia Computer Science*, vol. 57, pp. 710–715, 2015. DOI: 10.1016/j.procs.2015.07.458.

[2] K. A. Scarfone, M. P. Souppaya, A. Cody and A. D. Orebaugh, 'Technical guide to information security testing and assessment (SP 800-115)', Tech. Rep., 2008. DOI: 10.6028/nist.sp.800-115.

[3] PIT Management Committee, 'Public intrusion test (PIT): Online voting system with universal verifiability', Tech. Rep., Jun. 2019. [Online]. Available: https://www.post.ch/-/media/post/evoting/dokumente/abschlussbericht-oeffentlicher-intrusionstest-post.pdf?la=en.

[4] M. Zumbühl, *Participative Security – How to co-operate with hackers successfully?*, Feb. 2021. [Online]. Available: https://www.ciso-summit.ch/wp-content/uploads/sites/19/2021/01/2021-01-CISO-Summit-Invitation.pdf.

[5] T. Haines, S. J. Lewis, O. Pereira and V. Teague, 'How not to prove your election outcome', in *2020 IEEE Symposium on Security and Privacy (SP)*, IEEE, May 2020. DOI: 10.1109/sp40000.2020.00048.

[6] Swiss Post, *Ballot box not hacked, errors in the source code – Swiss Post temporarily suspends its e-voting system*, Mar. 2019. [Online]. Available: https://www.post.ch/en/about-us/media/press-releases/2019/swiss-post-temporarily-suspends-its-e-voting-system.

[7] J. Walker, *Swiss Post puts e-voting on hold after researchers uncover critical security errors*, Nov. 2019. [Online]. Available: https://portswigger.net/daily-swig/swiss-post-puts-e-voting-on-hold-after-researchers-uncover-critical-security-errors.

[8] P. Schmid and P-003, *Problem field interview about traditional and new forms of system security testing and verification [personal interview int-003]*, Mar. 2021.

[9] P. Schmid and P-001, *Problem field interview about security testing in norway in the ics sector [personal interview int-001]*, Mar. 2021.

[10] P. Schmid and P-002, *Problem field interview about security testing in switzerland [personal interview int-002]*, Mar. 2021.

[11] E. A. Morse and V. Raval, 'PCI DSS: Payment card industry data security standards in context', *Computer Law & Security Review*, vol. 24, no. 6, pp. 540–554, Jan. 2008. DOI: 10.1016/j.clsr.2008.07.001.

[12] C. Everett, 'Is ISO 27001 worth it?', *Computer Fraud & Security*, vol. 2011, no. 1, pp. 5–7, Jan. 2011. DOI: 10.1016/s1361-3723(11)70005-7.

[13] 'Information Security Management, Iso/iec 27001 (annex a) controls(c) iso', International Organization for Standardization, Standard, 2013.

[14] 'Ict minimal standard', Federal Office for National Economic Supply (FONES), Standard, 2018.

[15] *IT-Grundschutz-Kompendium*. Köln: Bundesanzeiger Verlag, 2018, ISBN: 9783846209066.

[16] 'Ein praxis-leitfaden für is-penetrationstests, Minimum standard for improving ict resilience', Bundesamt für Sicherheit in der Informationstechnik, Standard, 2016.

[17] 'Penetration Testing Guidance, Pci data security standard (pci dss)', Payment Card Industry (PCI), Standard, 2017.

[18] 'Security and privacy controls for information systems and organizations (sp 800-53 rev. 5)', Tech. Rep., Sep. 2020. DOI: 10.6028/nist.sp.800-53r5.

[19] *Glossary*. [Online]. Available: https://csrc.nist.gov/glossary.

[20] D. Catteddu and G. Hogben, 'Cloud Computing: Benefits, risks and recommendations for information security', European Union Agency for Cybersecurity, Tech. Rep., 2009.

[21] European Union Agency for Cybersecurity, *ENISA good practices for the security of smart cars*. Publications Office, 2019. DOI: 10.2824/17802.

[22] European Union Agency for Cybersecurity, *Good practices for security of IoT: Secure software development lifecycle*. Publications Office, 2019. DOI: 10.2824/742784.

[23] 'Inventory of riskassessment and riskmanagement methods', European Union Agency for Cybersecurity, Tech. Rep., 2006.

[24] *Sans information security white papers*. [Online]. Available: https://www.sans.org/white-papers/.

[25] Chief Security Office, 'Security Standard -Application SecurityTesting (SS-027)', Departement for Work and Pensions, Tech. Rep., Mar. 2020.

[26] P. Mehta, *Penetrationstests: Methodologie und Standards*, Aug. 2017. [Online]. Available: https://www.computerweekly.com/de/ratgeber/Penetrationstests-Methodologie-und-Standards.

[27] The PTES Team, 'The Penetration Testing ExecutionStandard Documentation', PTES, Tech. Rep., Jun. 2021.

[28] P. Herzog, 'OSSTMM 3 - The Open Source Security Testing Methodology Manual', ISECOM, Tech. Rep., Dec. 2010.

[29] *OWASP Foundation | Open Source Foundation for Application Security*. [Online]. Available: https://owasp.org/.

[30] E. Saad and R. Mitchell, 'Web Security Testing Guide', OWASP, Tech. Rep., Dec. 2020.

[31] A. van der Stock, D. Cuthbert, J. Manico, J. C. Grossman and M. Burnett, 'Application Security Verification Standard', OWASP, Tech. Rep., Oct. 2020.

[32] B. Mueller, S. Schleier, J. Willemsen and C. Holguera, 'Mobile Security Testing Guide', OWASP, Tech. Rep., Jul. 2021.

[33] A. Guzman, 'Firmware Security Testing Methodology', OWASP, Tech. Rep., 2019.

[34] A. Guzman and C. Bassem, 'IoT Security Verification Standard', OWASP, Tech. Rep., Dec. 2020.

[35] C. Holguera, B. Mueller, S. Schleider and J. Willemsen, 'Mobile Application Security Verification Standard', OWASP, Tech. Rep., May 2021.

[36] S. Vetsch, A. Hermann, D. Meier, D. Nufer, P. Schmid and D. Tschabold, 'Container Security Verification Standard', OWASP, Tech. Rep., Jul. 2019.

[37] National Cyber Security Centre, *IT Health Check (ITHC): supporting guidance*, Nov. 2018. [Online]. Available: https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance/it-health-check-ithc-supporting-guidance.

[38] National Cyber Security Centre, *CHECK - penetration testing*, Mar. 2019. [Online]. Available: https://www.ncsc.gov.uk/information/check-penetration-testing.

[39] 'Information systems security assessment framework (issaf) draft 0.2.1b', Open Information Systems Security Group, Tech. Rep., 2006.

[40] Internet Archive - Wayback Machine, *Open Information Systems Security Group*, Jun. 2019. [Online]. Available: http://web.archive.org/web/20190626004349/https://www.oissg.org/.

[41] L. Epling, B. Hinkel and Y. Hu, 'Penetration testing in a box', in *Proceedings of the 2015 Information Security Curriculum Development Conference on InfoSec'15*, ACM Press, 2015. DOI: 10.1145/2885990.2885996.

[42] M. Bishop, 'About penetration testing', *IEEE Security & Privacy Magazine*, vol. 5, no. 6, pp. 84–87, Nov. 2007. DOI: 10.1109/msp.2007.159.

[43] S. A. Saleem, 'Ethical hacking as a risk management technique', in *Proceedings of the 3rd annual conference on Information security curriculum development - InfoSecCD'06*, ACM Press, 2006. DOI: 10.1145/1231047.1231089.

[44] H. Berger and A. Jones, 'Cyber security & ethical hacking for smes', in *Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society - KMO'16*, ACM Press, 2016. DOI: 10.1145/2925995.2926016.

[45] Y. Khera, D. Kumar, Sujay and N. Garg, 'Analysis and impact of vulnerability assessment and penetration testing', in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, IEEE, Feb. 2019. DOI: 10.1109/comitcon.2019.8862224.

[46] P. Cronin, F. Ryan and M. Coughlan, 'Undertaking a literature review: A step-by-step approach', *British Journal of Nursing*, vol. 17, no. 1, pp. 38–43, Jan. 2008. DOI: 10.12968/bjon.2008.17.1.28059.

[47] M. J. Blanche, *Research in practice : applied methods for the social sciences*. Cape Town: University of Cape Town Press, 1999, ISBN: 9781919713359.

[48] E. Heery, *A dictionary of human resource management*. Oxford: Oxford University Press, 2017, ISBN: 9780191827822.

[49] A. Galletta, *Mastering the semi-structured interview and beyond : from research design to analysis and publication*. New York: New York University Press, 2013, ISBN: 9780814732939.

[50] Lucerne University of Applied Sciences and Arts, *Hämmerli Bernhard HSLU I*. [Online]. Available: https://www.hslu.ch/en/lucerne-university-of-applied-sciences-and-arts/about-us/people-finder/profile/?pid=630.

[51] Lockheed Martin, *Cyber Kill Chain*®. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[52] A. Singhal, T. Winograd and K. A. Scarfone, 'Guide to secure web services (sp 800-95)', Tech. Rep., 2007. DOI: 10.6028/nist.sp.800-95.

[53] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams and A. Hahn, 'Guide to industrial control systems (ICS) security (sp 800-82 rev. 2)', Tech. Rep., Jun. 2015. DOI: 10.6028/nist.sp.800-82r2.

[54] P. A. Grassi, M. E. Garcia and J. L. Fenton, 'Digital identity guidelines (sp 800-63-3)', Tech. Rep., Jun. 2017. DOI: 10.6028/nist.sp.800-63-3.

[55] X-Force Red, *Adversary simulation: Put your incident responseprograms to the test*, Feb. 2021. [Online]. Available: https://www.ibm.com/downloads/cas/JZ38L39E.

[56] H. Hata, M. Guo and M. A. Babar, 'Understanding the heterogeneity of contributors in bug bounty programs', in *2017 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*, IEEE, 2017, pp. 223–228.

[57] D. Geer and J. Harthorne, 'Penetration testing: A duet', in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, pp. 185–195. DOI: 10.1109/CSAC.2002.1176290.

[58] M. Mitnick, *Understanding the 6 Main Types of Penetration Testing*, May 2020. [Online]. Available: https://www.mitnicksecurity.com/blog/understanding-the-6-main-types-of-penetration-testing.

[59] E. O. Yeboah-Boateng and P. M. Amanor, 'Phishing, smishing & vishing: An assessment of threats against mobile devices', *Journal of Emerging Trends in Computing and Information Sciences*, vol. 5, no. 4, pp. 297–307, 2014.

[60] C. Hadnagy, *Social engineering : the art of human hacking*. Indianapolis, IN: Wiley, 2011, ISBN: 9780470639535.

[61] *Private vs Public Programs | HackerOne Platform Documentation*. [Online]. Available: https://docs.hackerone.com/programs/private-vs-public-programs.html.

[62] R. Hoffmann, J. Napiórkowski, T. Protasowicki and J. Stanik, 'Risk based approach in scope of cybersecurity threats and requirements', *Procedia Manufacturing*, vol. 44, pp. 655–662, 2020. DOI: 10.1016/j.promfg.2020.02.243.

[63] G. O'Regan, *Introduction to Software Quality*. Springer-Verlag GmbH, May 2014, 354 pp., ISBN: 9783319061061.

[64] S. Nafzger, Jul. 2020. [Online]. Available: https://www.bugbounty.ch/bug-bounty-hunting/.

[65] P. Schmid and P-004, *Challenge interview about security testing methods and their properties [personal interview int-004]*, Aug. 2021.

[66] P. Schmid and P-005, *Challenge interview about security testing methods and their properties [personal interview int-005]*, Sep. 2021.

[67] P. Schmid and P-004, *Collection interview to collect relevant data from a consumer's perspective [personal interview int-006]*, Nov. 2021.

[68] P. Schmid and P-005, *Collection interview to collect relevant data from a provider's perspective [personal interview int-007]*, Nov. 2021.

[69] P. Schmid and P-006, *Collection interview to collect relevant data from a provider's perspective [personal interview int-008]*, Nov. 2021.

[70] P. Schmid and P-007, *Collection interview to collect relevant data from a provider's perspective [personal interview int-009]*, Nov. 2021.

[71] P. Schmid and P-008, *Collection interview to collect relevant data from a provider's perspective [personal interview int-010]*, Nov. 2021.

Appendix A

Additional material

This chapter includes additional material that is used throughout the thesis and included as a reference as it would disturb a reader's flow of reading.

A.1 Summary of interviews

In the following section, a summary of all the conducted interviews is included for further reference.

A.1.1 Interview "INT-001" with "P-001" [9]

This interview was conducted via an online video call with a cyber security expert in Norway's ICS sector. The main goal of the interview was to understand the current situation about ethical hacking services and the applied security testing methods in general in Norway in more detail to further analyse the problem field.

The interviewee elaborated on the current situation in Norway's ICS sector in general and provided insight into the current regulatory situation and for example what regulations the gas sector currently must comply with and that other sectors in the ICS field do not have to comply with any regulations despite being part of critical infrastructure. Furthermore, the interview explained based on his own insights and experience, that most players in the ICS field are generally aware of potential vulnerabilities and the risks this imposes but genuinely do not want to take actions to identify and address these risks in a structured way by applying various security testing methods. In addition to that, the interviewee states that based on his own experience if companies in Norway use ethical hacking services it mainly focuses on simpler and more straight-forward methods such as penetration tests or vulnerability scans and that more complex and advanced security testing methods such as red teaming assessment are not yet very well established with Norway's companies in general.

Later in the interview, the interviewee stated as well, that a lot of companies have no experience with ethical hacking services and therefore do not really

understand the differences and nuances of it. According to the interviewee this makes is very difficult for companies that would like to start off with such services because without regularly using such services they are not able to gain the needed knowledge to start using such services effectively. Furthermore, the interviewee agreed that this problem extends not only to the consumer but to the provider as well. The interviewee elaborates on a situation, he had to experience himself, where he was tasked to conduct a penetration test and agreed with a provider of such services on this security testing method but in the end got not much more than just a simple vulnerability scan from an automated tool that could not be a penetration test. According to the interviewee one of the main problems behind that is not only the mismatch in understand but especially in Norway the fact, that there are not to many qualified providers of ethical hacking services for a company in Norway to choose from.

A.1.2 Interview "INT-002" with "P-002" [10]

This interview was conducted via an online video call with a CISO from a worldwide insurance company. The main goal of the interview was to understand the current situation about ethical hacking services and the applied security testing methods in general in Switzerland as well as from a more global view from the viewpoint of a consumer of such services to better understand the problem field.

The interviewee first explained what ethical hacking services his company regularly performs. This includes various services such as threat modelling, social engineering and (spear) phishing tests as well as vulnerability scans, penetration tests of all kinds as well as red team assignments. Furthermore, the interviewee elaborates on what security testing methods they specifically do not apply and mentioned bug bounty programs because from a pure risk point of view this is already covered with regularly running vulnerability scan and penetration tests and furthermore because the publicly exposed perimeter is limited and therefore much easier to control.

The interviewee then elaborates on the problem of finding a proper vendor and the challenge to identify and apply the proper security testing method. He explains that this is a fairly common problem and was addressed within his company first of all by having an internal team of skilled security professionals that do not perform for example a penetration test them-self but fully understand the process of identifying vulnerabilities and conducting such tests and can therefore not only challenge whatever a provider of ethical hacking services offers but can already specify very clearly the specific security testing method they would like to apply before asking for proposals from various providers. In addition to that, the interviewee explains, that they overcome the problem of provider's differing understanding of various security testing methods by running some sort of a trial penetration tests with various providers and then evaluate each trial run and decide if the outcome was sufficient and a provider is added to the short list or not.

This provides the ability to already know what to expect from a provider once they ask for additional services in the future. However, the interview agrees, that this is a very advantageous situation because normally a company cannot afford to run various trial runs and employ a large team of security professionals them-self to overcome these problems. The only possibility for smaller companies he currently sees if that they work with a broker or intermediary they fully trust and can of course not provide the trial runs but help them in decide upon a proper security testing method and mainly challenge the suggestions a company gets as part of the proposals from a provider.

A.1.3 Interview "INT-003" with "P-003" [8]

This interview was conducted via an online video call with a lecturer in the field of cyber security and a former penetration tester in Switzerland. The main goal of the interview was again to understand the current situation about ethical hacking services and the applied security testing methods in Switzerland. Furthermore, the interviewee held a presentation titled *Security Testing Methods, Evaluation & Diversity: In which situation to apply which method?* at a closed-group conference for CISOs and was therefore of upmost relevance because the topic of this presentation directly relates to the field of research of this thesis and could thus help to better understand the problem field by understanding the interviewee's motivation in creating and giving such a talk.

As the mentioned presentation is not publicly available, the interviewee starts by giving a short summary of his presentation. He first elaborated on why he initially decided to create and hold such a presentation and explained that this is a clear need for various CISOs. He bases this not only on various insights and questions he gets from his network and reach as a lecturer in the field but as well on his experience as a penetration tester and provider for various ethical hacking services and mainly originated in the fact that various standards in the field do not provide enough insights or guidance if a company or consumer not already quite exactly know what they need or want to do. Furthermore, the interviewee explains that the outcome of his presentation was a brief overview based on applying a small set of properties to a selection of the most well-known security testing methods. He there mentioned that this was only collected for this presentation is all based on his own experience and not in any way complete. He then mentions that as further improvement for his summary of the problem, he would include more security testing methods and more properties and potentially add various layers of abstractions for different target audiences.

A.1.4 Interview "INT-004" with "P-004" [65]

This interview was conducted online with a cyber security manager working in Switzerland's financial sector. The main goal of this interview was to challenge,

clarify and complete the selected security testing methods as well as their definitions. The interview was initiated with a general discussion about potential technical security testing methods without disclosing the already compiled list of test methods to get unbiased insights because the interviewee organises various security assessments to test and ensure his company's security posture and has therefore experience with various technical as well as non-technical security testing methods.

During the initial phase of the interview various technical testing methods were brought up by the interviewee. During this phase the interviewee mentioned, amongst others, a technical testing method called "Attack Path Mapping" that was not yet included in the list of relevant technical security testing methods. However, based on the interviewee's definition of this testing method it was getting clear, that this seems to be a synonym of what is already included in the list of testing methods as an assume-breach simulation. This was further confirmed by the interviewee once the compiled list testing methods and their definitions were disclosed to the interviewee. Other than that, no other testing methods or definitions were altered.

A.1.5 Interview "INT-005" with "P-005" [66]

This interview was conducted in-person with the head of cyber security for a Swiss cyber security firm providing services in the field of cyber security across various industries in Switzerland and the near-abroad. The main goal of this interview was again to challenge, clarify and complete the selected security testing methods and their definitions. The interview was again initiated with a general discussion about technical security testing methods and quickly pinpointed out that the currently used definition for technical and non-technical security testing methods is not spot-on enough. Therefore, the initial minutes of the interview were used to elaborate and discuss potential suitable definitions. This resulted in a definition that non only differentiate technical and non-technical but as well dynamic and static testing methods to gain more precision and general understanding. Once this was cleared out the interview continued with the interviewee elaborating about various forms of testing methods his company provides for his customers. These methods were then together applied to the initial landscape resulting in an alternative definition for the testing method "phishing" which could be called "mass phishing" as well describing a specific form of phishing targeting masses instead of only a very narrowed-down group of targets as a "spear phishing" would do. Other than that, the interviewee agreed with the currently provided definitions from the initial landscape.

A.1.6 Interview "INT-006" with "P-004" [67]

This interview was conducted online with a cyber security manager working in Switzerland's financial sector. The main goal of this interview was to collect relev-

ant data based on the previously designed model. This resulted in the following data collected throughout the interview:

Table A.1: Collected data from interview "INT-006"

	IN	**DE**	**MA**	**CO**	**ST**	**DU**	**PR**	**CT**	**MT**	**KN**
Vulnerability Scanning	8	8	2	8	10	1	6	6	3	5
Penetration Testing	5	6	6	6	7	3	5	4	2	5
Phishing	8	10	10	10	9	2	4	2	1	6
Social Engineering	3	2	2	3	3	3	4	4	1	2
Red Teaming	7	6	6	6	4	3	5	4	3	4
Bug Bounty Program	6	9	8	7	5	1	8	10	4	2

A.1.7 Interview "INT-007" with "P-005" [68]

This interview was conducted in-person with the head of cyber security for a Swiss cyber security firm providing services in the field of cyber security across various industries in Switzerland and the near-abroad. The main goal of this interview was to collect relevant data based on the previously designed model. This resulted in the following data collected throughout the interview:

Table A.2: Collected data from interview "INT-007"

	IN	**DE**	**MA**	**CO**	**ST**	**DU**	**PR**	**CT**	**MT**	**KN**
Vulnerability Scanning	9	9	2	2	10	3	3	3	1	5
Penetration Testing	9	9	3	4	8	5	5	6	2	5
Phishing	3	3	4	8	5	3	4	3	2	5
Social Engineering	3	3	4	8	4	3	4	3	2	4
Red Teaming	5	5	8	7	7	8	5	8	3	5
Bug Bounty Program	3	2	3	4	2	9	8	5	3	4

A.1.8 Interview "INT-008" with "P-006" [69]

This interview was conducted in-person with a senior penetration tester for a Swiss cyber security firm providing services in the field of IT security and ethical hacking services across various industries in Switzerland. The main goal of this interview was to collect relevant data based on the previously designed model. This resulted in the following data collected throughout the interview:

Table A.3: Collected data from interview "INT-008"

	IN	DE	MA	CO	ST	DU	PR	CT	MT	KN
Vulnerability Scanning	3	3	1	2	9	2	1	2	3	5
Penetration Testing	7	9	3	5	7	6	4	5	2	6
Phishing	4	7	7	8	5	2	6	2	1	4
Social Engineering	5	5	7	7	4	2	5	3	1	2
Red Teaming	8	2	8	6	3	8	2	9	3	5
Bug Bounty Program	6	8	2	2	6	10	7	6	5	2

A.1.9 Interview "INT-009" with "P-007" [70]

This interview was conducted online with a cyber security manager responsible for coordinating technical security assessments for one of Switzerland's largest financial institutes. The main goal of this interview was to collect relevant data based on the previously designed model. This resulted in the following data collected throughout the interview:

Table A.4: Collected data from interview "INT-009"

	IN	DE	MA	CO	ST	DU	PR	CT	MT	KN
Vulnerability Scanning	7	5	5	8	10	1	1	2	4	6
Penetration Testing	8	8	6	6	8	6	5	7	3	5
Phishing	3	1	7	9	3	3	3	4	3	4
Social Engineering	3	3	2	8	2	2	2	2	1	1

	IN	DE	MA	CO	ST	DU	PR	CT	MT	KN
Red Teaming	6	5	7	5	5	6	7	7	2	4
Bug Bounty Program	8	5	8	6	1	7	8	8	1	2

A.1.10 Interview "INT-010" with "P-008" [71]

This interview was conducted online with the CISO of an IT outsourcing company focused on Switzerland and Germany's health sector and responsible for organising and coordinating cyber security assessments and audits. The main goal of this interview was to collect relevant data based on the previously designed model. This resulted in the following data collected throughout the interview:

Table A.5: Collected data from interview "INT-010"

	IN	DE	MA	CO	ST	DU	PR	CT	MT	KN
Vulnerability Scanning	7	6	6	7	5	4	3	2	3	6
Penetration Testing	9	9	7	6	9	8	8	7	3	5
Phishing	6	2	7	8	6	5	5	5	2	5
Social Engineering	6	2	7	8	6	5	5	5	2	5
Red Teaming	8	8	6	6	8	7	8	7	5	4
Bug Bounty Program	9	9	6	6	9	9	8	8	5	4

A.2 Peculiarity model

In the following section, the peculiarity model is included in a larger version for further reference.

Figure A.1: Security testing methods mapped to the cyber kill chain (large)

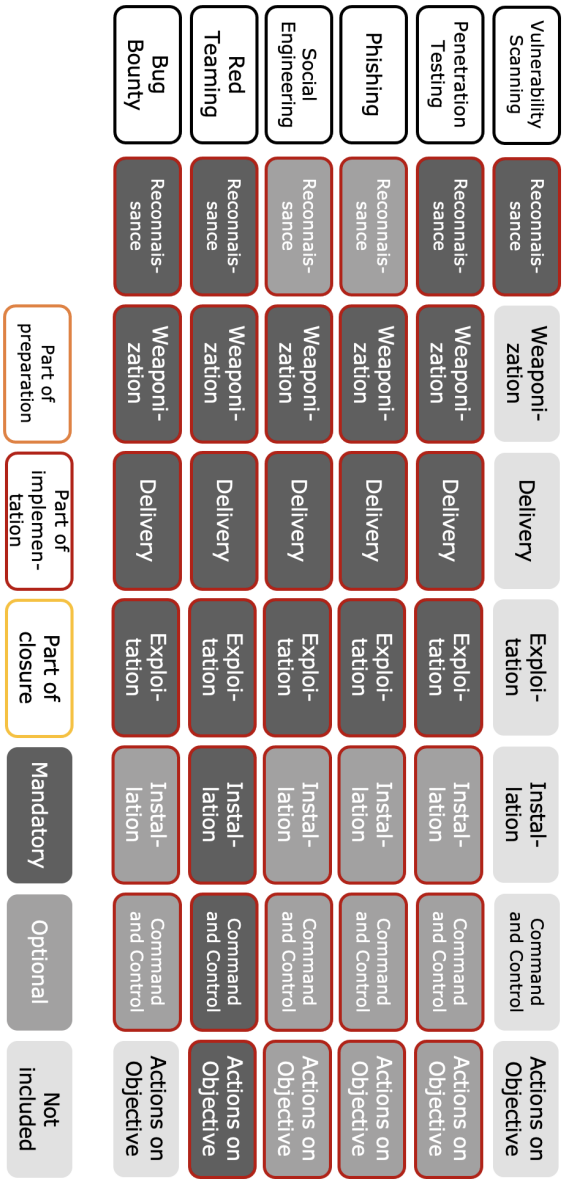


Figure A.2: Security testing methods mapped to PTES (large)

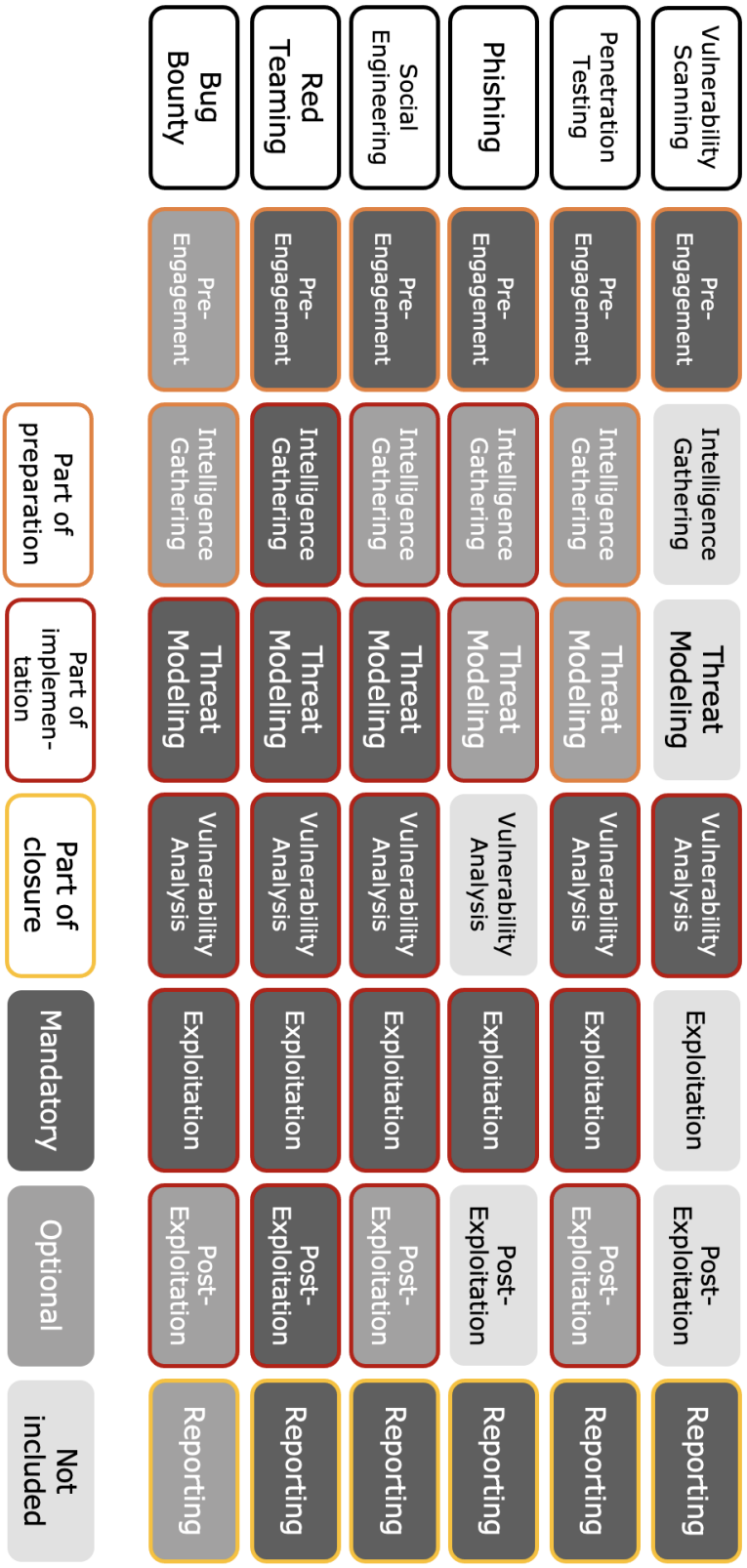


Figure A.3: Different approaches of penetration testing mapped to PTES (large)

A.3 Additional plots

In the following section, additional plots for the described landscape are included.

Figure A.4: Initial landscape for Insight (IN)

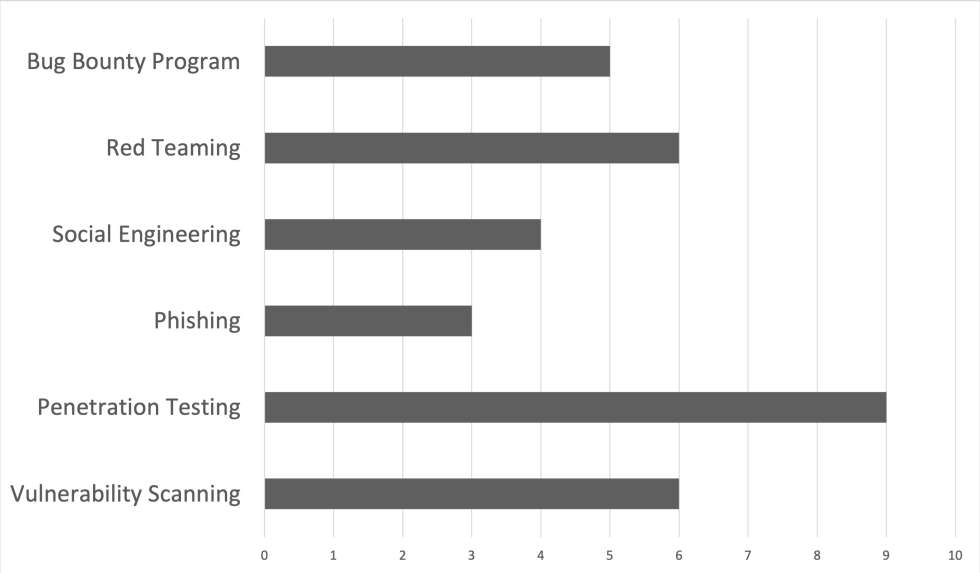


Figure A.5: Initial landscape for Depth (DE)

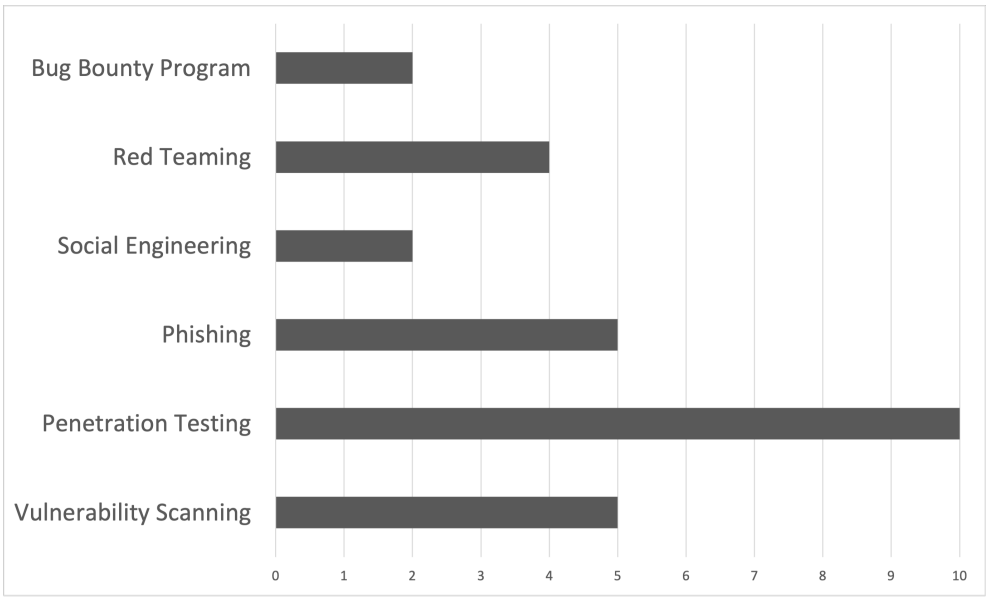


Figure A.6: Initial landscape for Management Attention (MA)

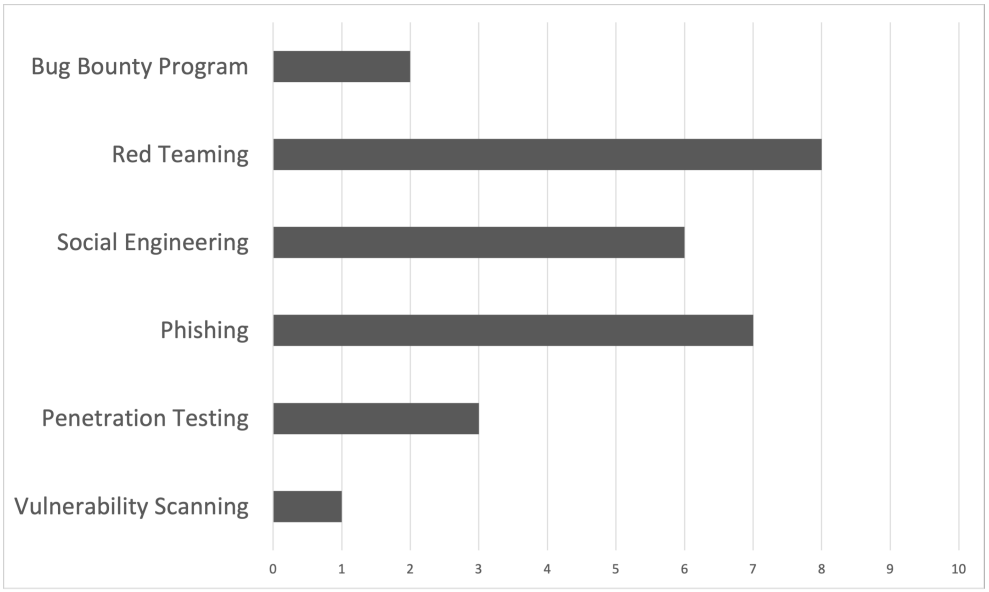


Figure A.7: Initial landscape for Comprehensibility (CO)

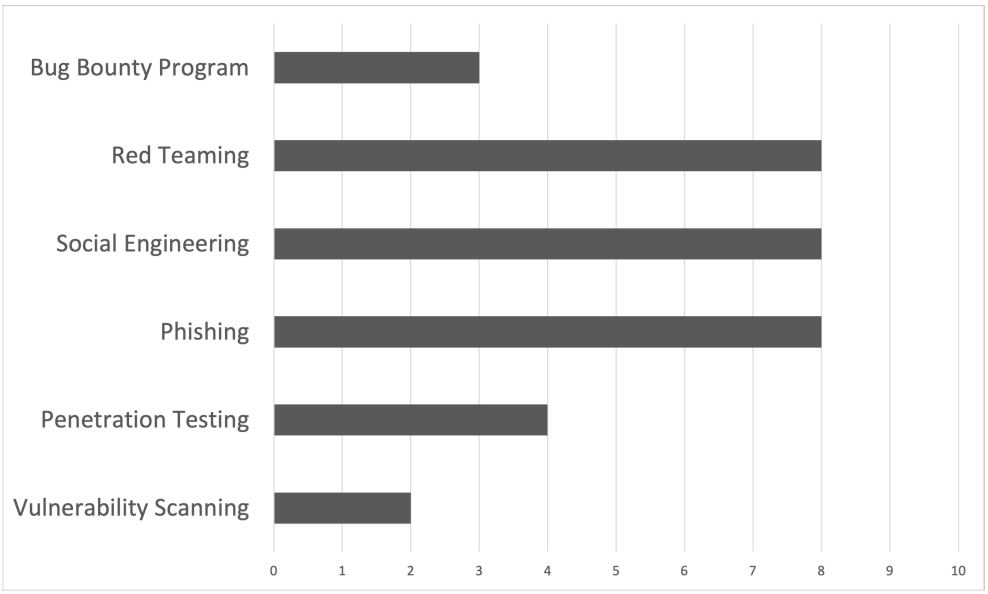


Figure A.8: Initial landscape for Structuredness (ST)

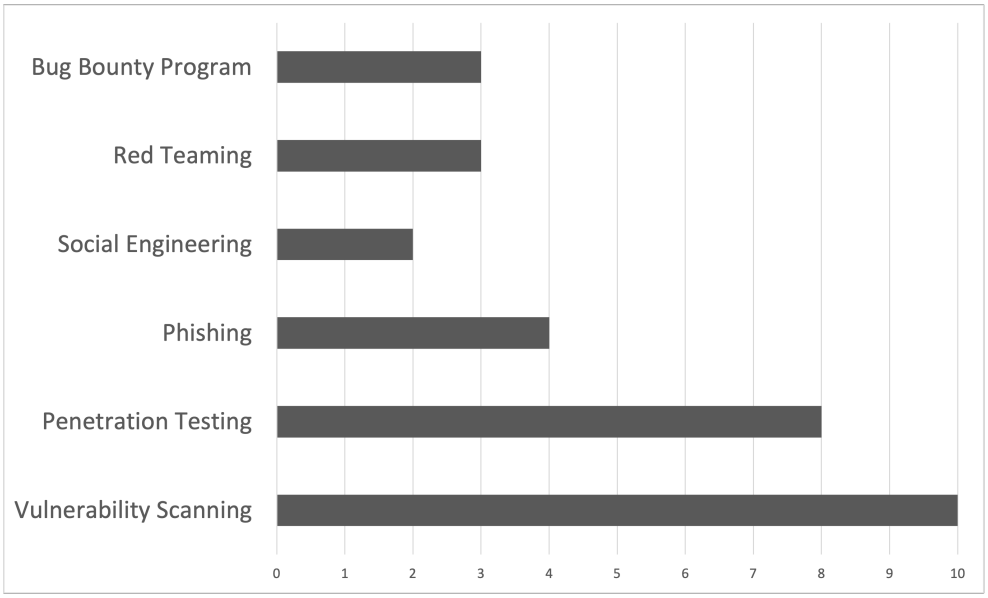


Figure A.9: Initial landscape for Duration (*DU*)

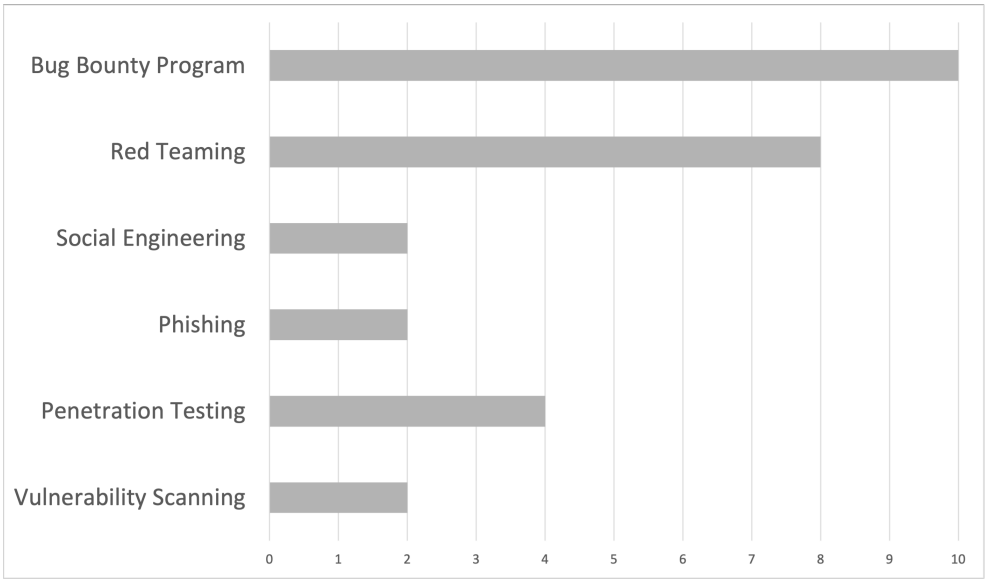


Figure A.10: Initial landscape for Preparation (*PR*)

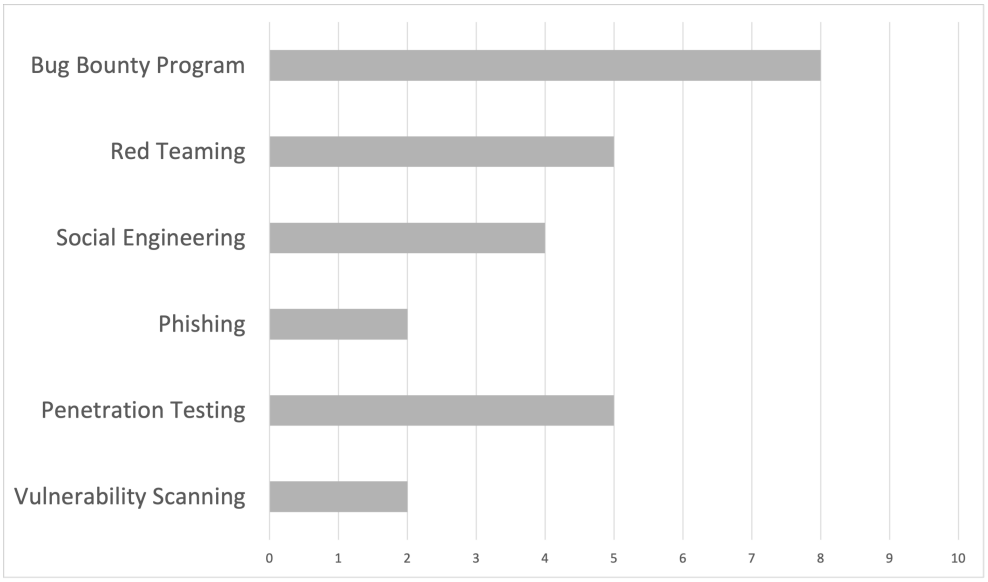


Figure A.11: Initial landscape for Cost (CT)

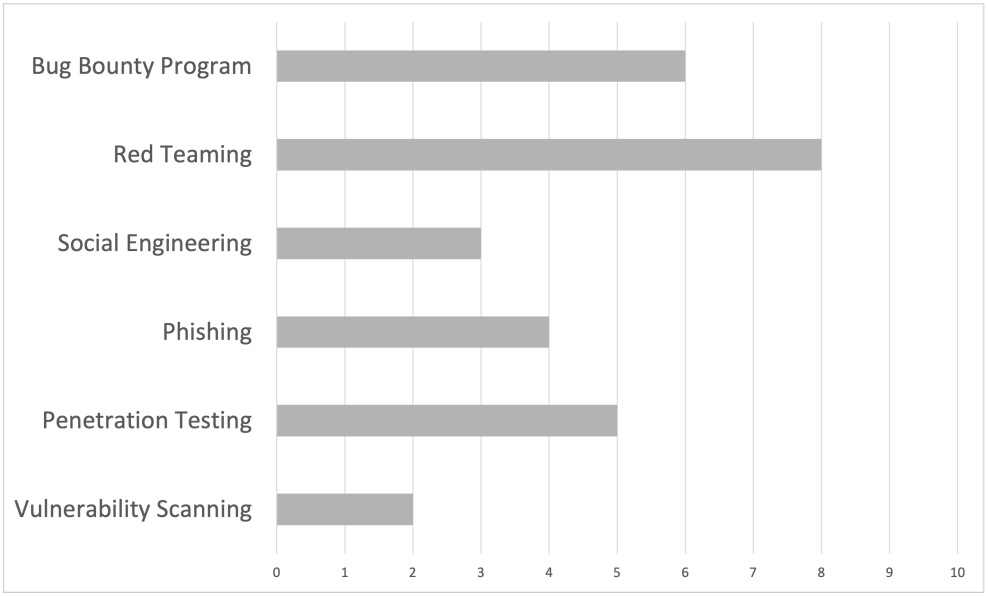


Figure A.12: Initial landscape for Management Performance (MP)

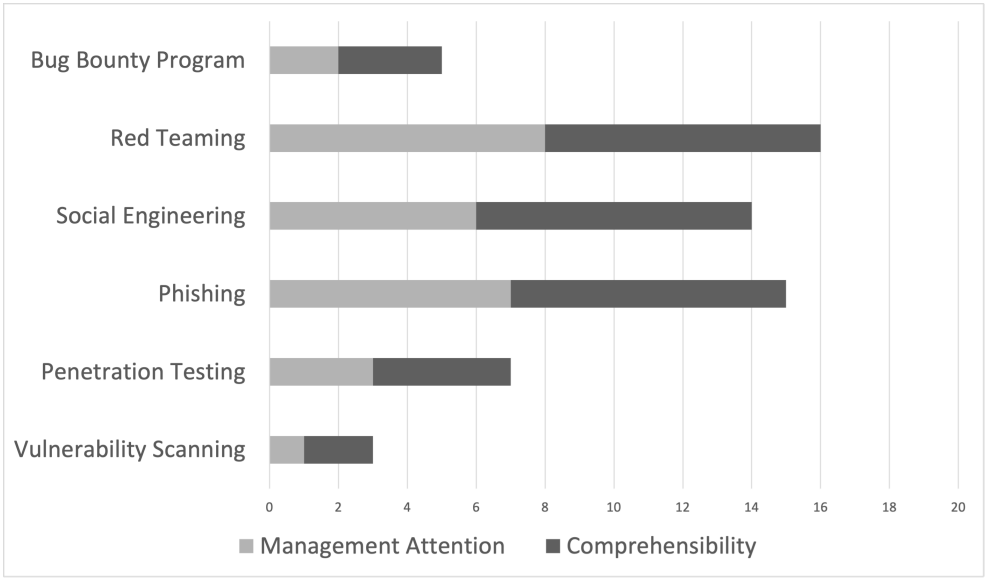


Figure A.13: Initial landscape for Technical Performance (TP)

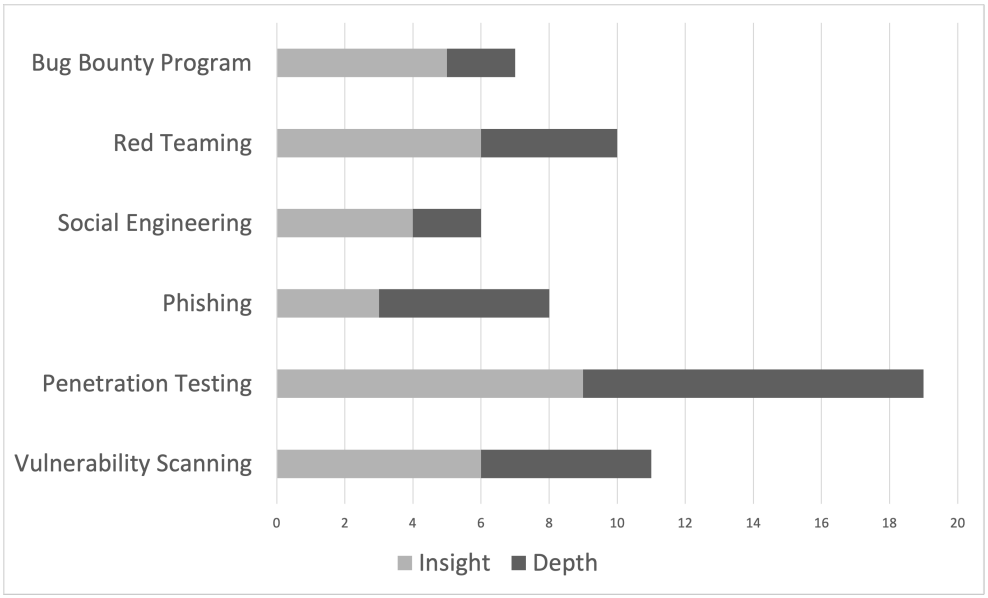


Figure A.14: Method landscape for Insight (IN)

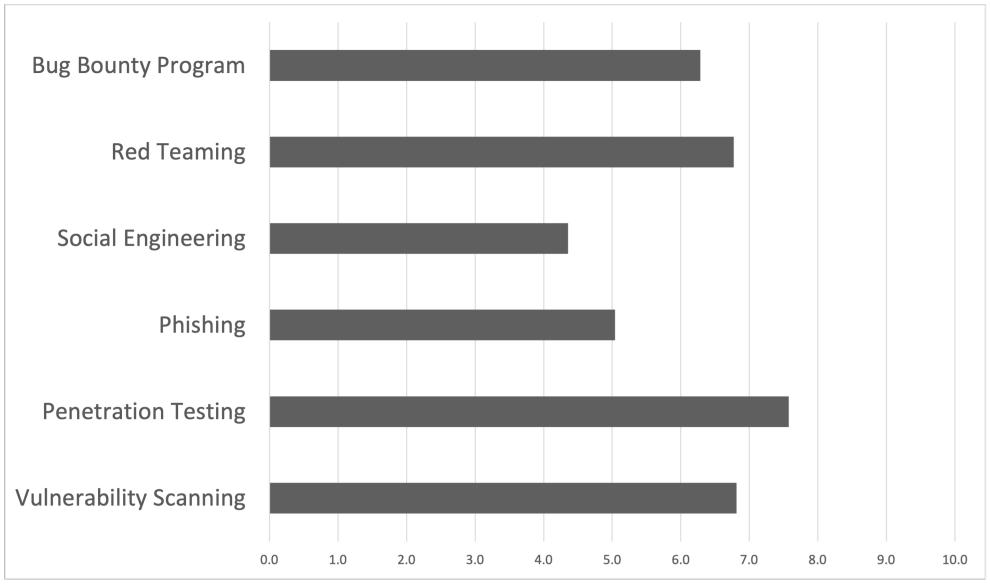


Figure A.15: Method landscape for Depth (*DE*)

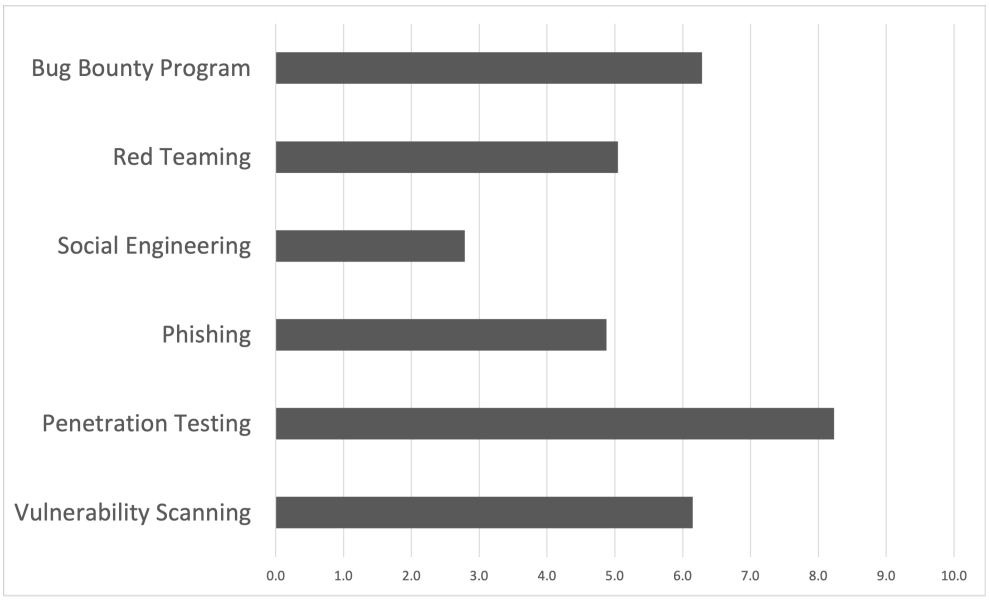


Figure A.16: Method landscape for Management Attention (*MA*)

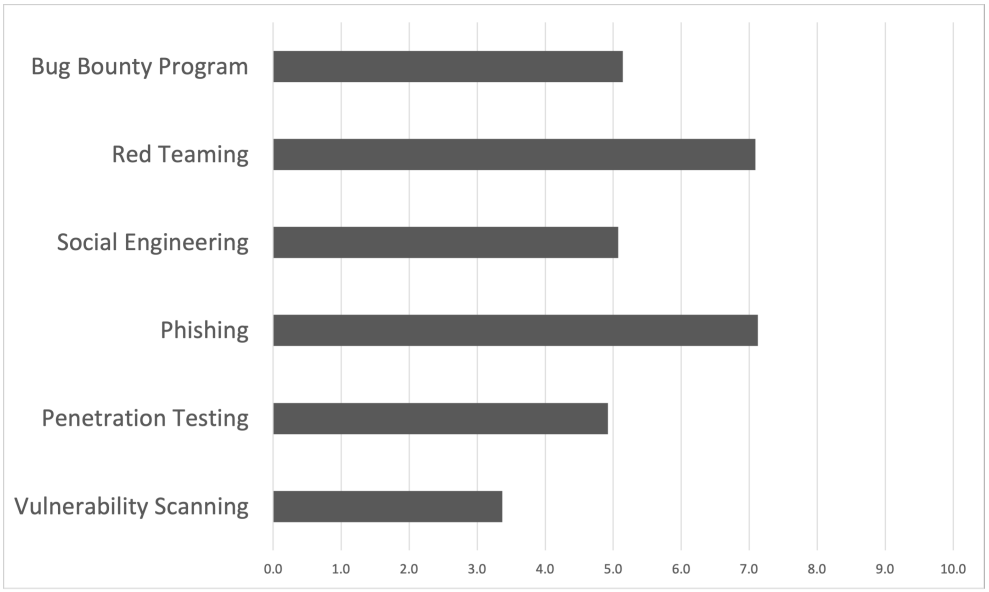


Figure A.17: Method landscape for Comprehensibility (CO)

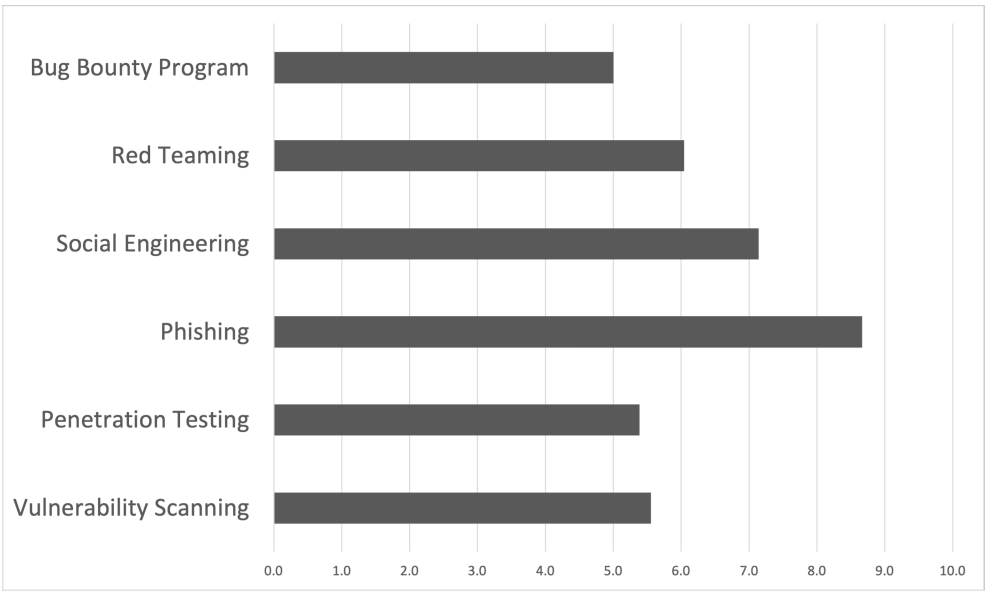


Figure A.18: Method landscape for Structuredness (ST)

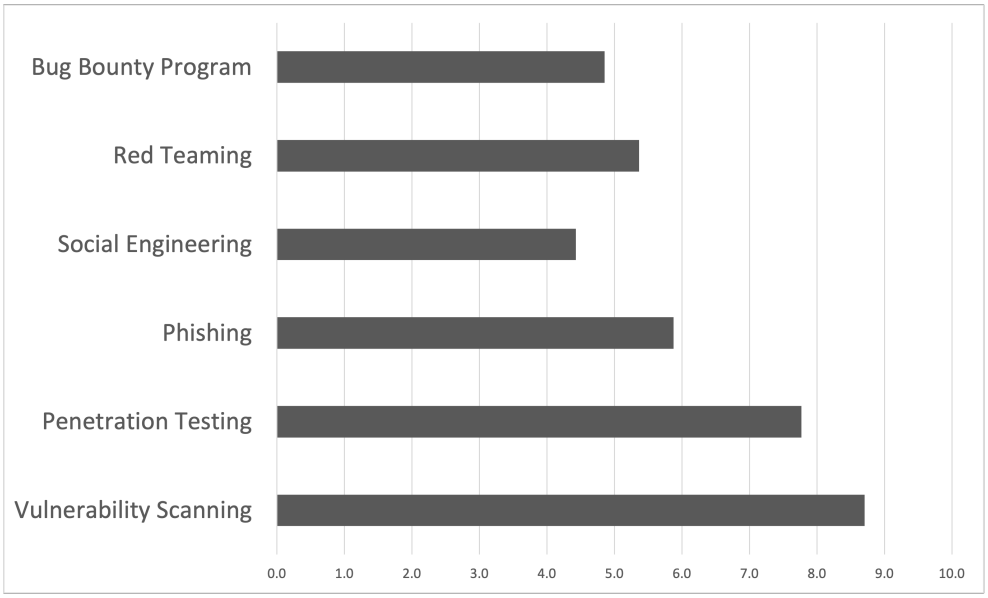


Figure A.19: Method landscape for Duration (*DU*)

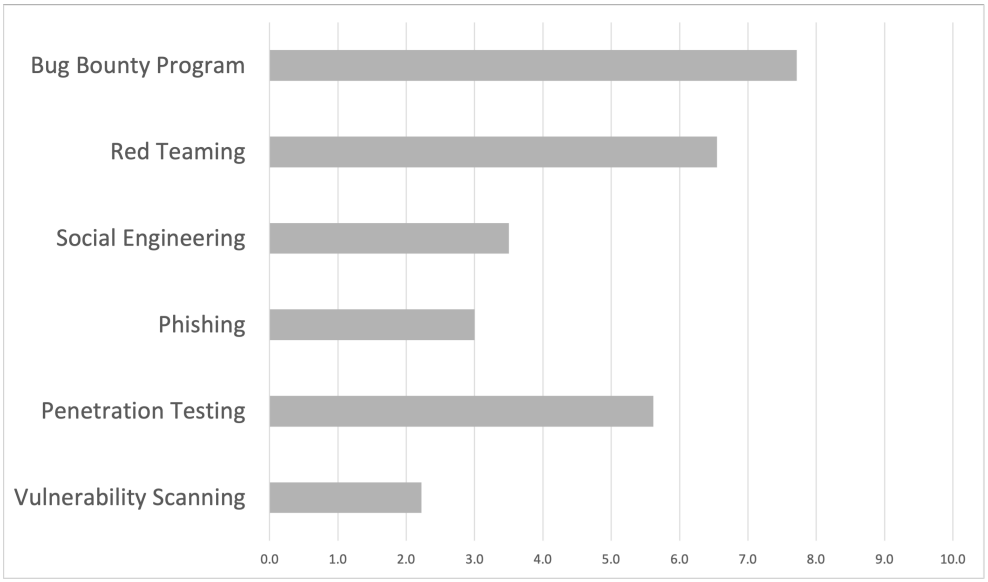


Figure A.20: Method landscape for Preparation (*PR*)

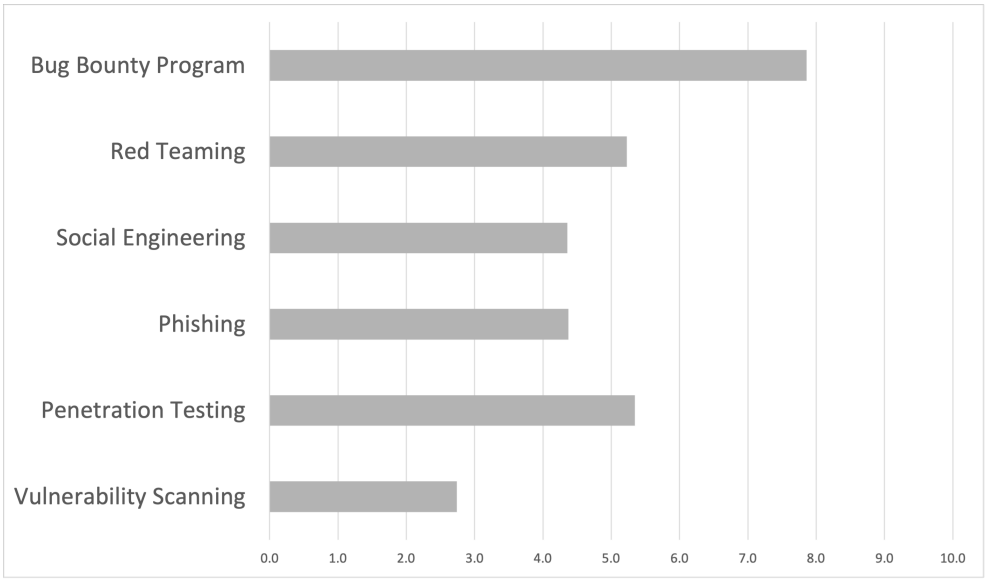


Figure A.21: Method landscape for Cost (CT)

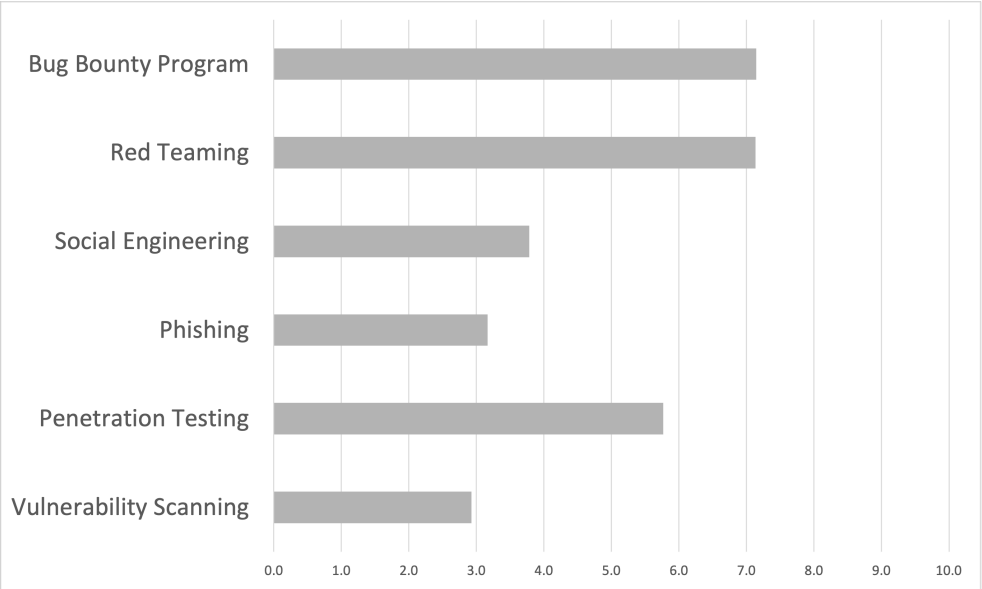


Figure A.22: Method landscape for Management Performance (MP)

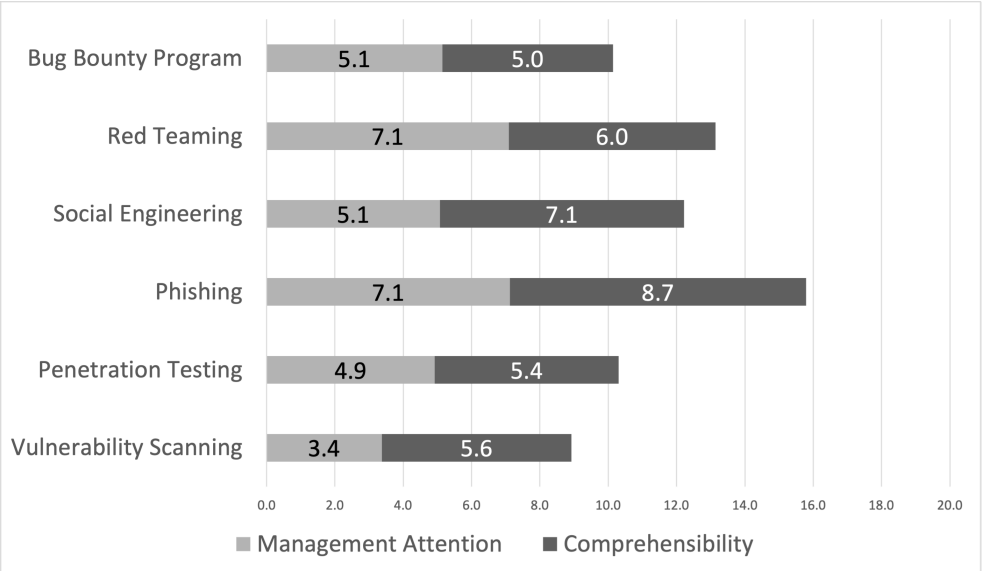
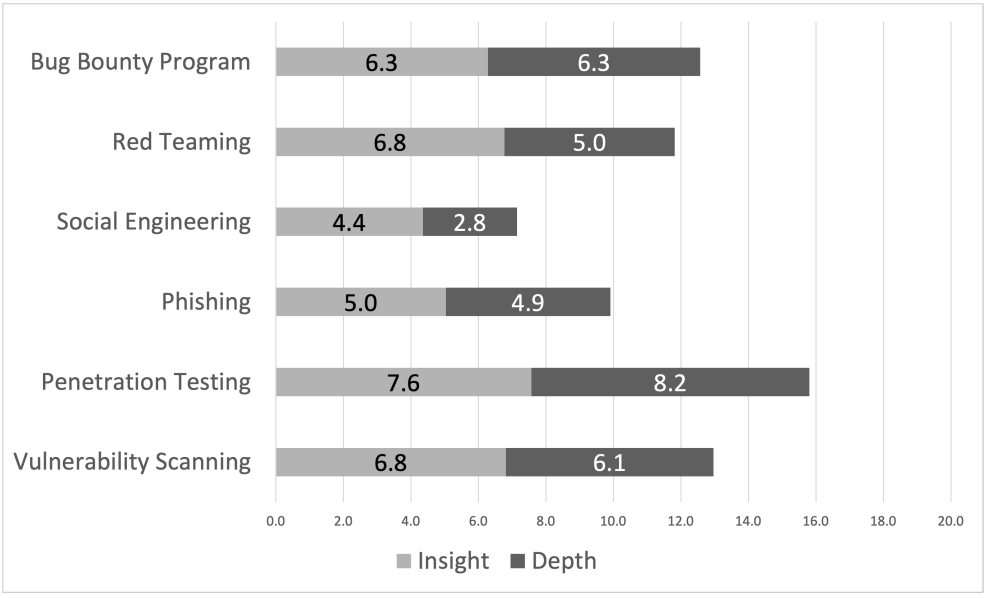
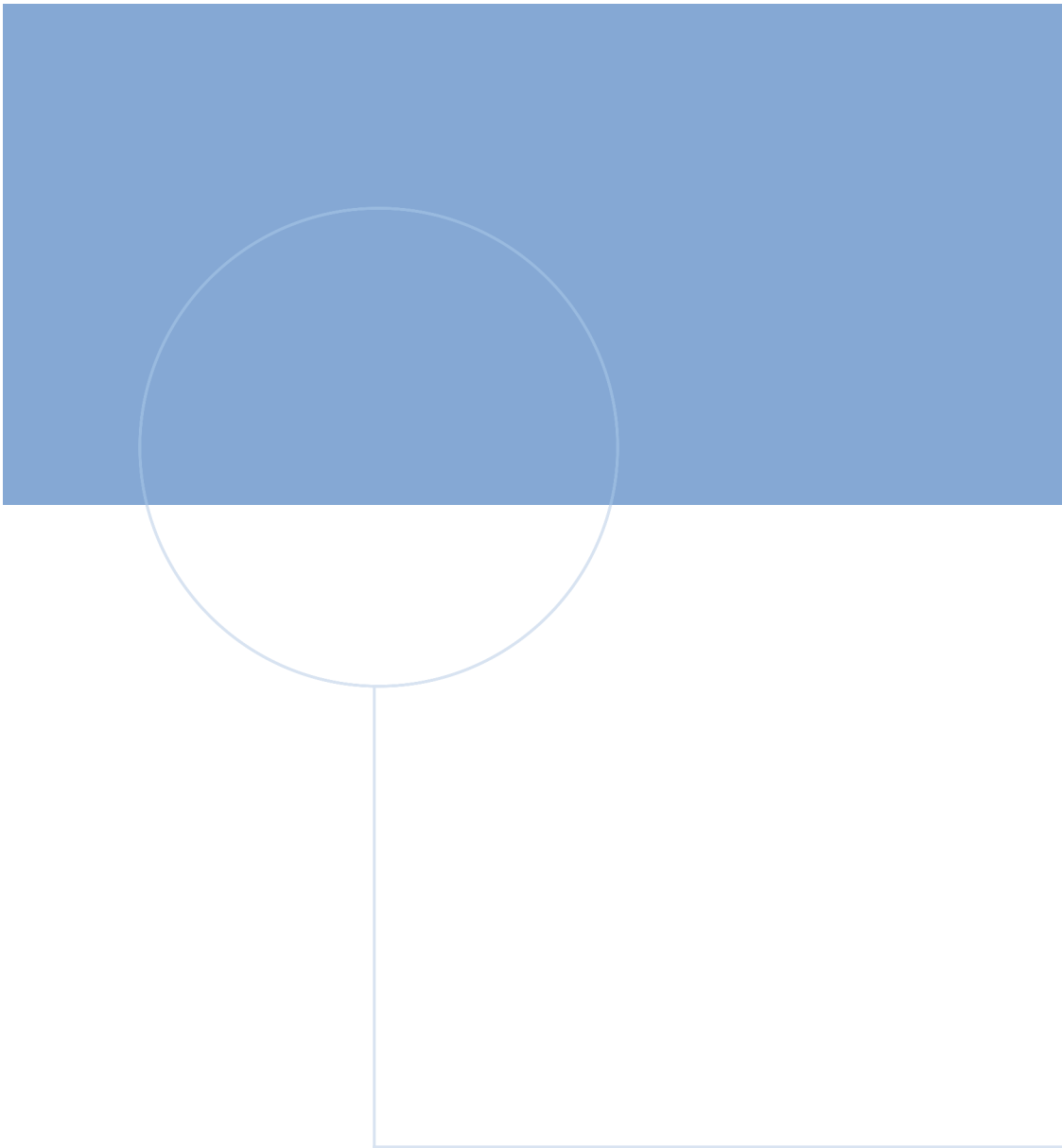


Figure A.23: Method landscape for Technical Performance (TP)





NTNU

Norwegian University of
Science and Technology