

Creativity and Value Creation



Figure 1: Creativity

Student Name: Ehsan Samiee
Student ID Number: 2419475
Lecturer Name: Dr Osman Elgawi

Content

17 June 2026 11:39

Contents

Task 1: Ideation & Mind Map

Ideation:

Mind Map:

Task 2: Aim and Objective

Project Aim:

Objectives:

Research Philosophy:

Research Area:

Search Tools and Research Strategy:

Task 3: Research Strategies:

Validity, Reliability, Generalisability and Ethical Considerations:

Research Strategy and Data Collection Methods:

Pilot Data Collection:

Quantitative and Qualitative Analysis:

Appendix:

References:

Task1 :Task 1 – Ideation & Mind Map

17 June 2026 11:14

Task 1: Ideation & Mind Map

Ideation:

“Developing a Penetration Testing Framework to Improve Cybersecurity for Small Businesses”



Figure 2: Cyber Attack

Introduction:

The idea for this project was developed by exploring how innovation and cybersecurity can create value for society [1]. Small businesses were identified as a suitable focus area because they often face cyber threats but may have limited resources and security expertise [4],[6]. Several cybersecurity project ideas were considered, including phishing detection, cybersecurity awareness applications, and vulnerability scanning. After evaluating these options, developing a penetration testing framework was selected because it offers a practical and structured approach to identifying vulnerabilities and improving cybersecurity for small businesses. This project aligns with personal interests in penetration testing and supports the development of problem-solving and research skills.

Mind Map:



Figure 3 : Mind map

The mind map illustrates how creativity and innovation can support the development of cybersecurity solutions and create value for society. Different areas of interest related to computer science were explored, including ethical hacking, vulnerability assessment, network security, and emerging cybersecurity technologies. The map also considers the wider impact of cybersecurity through improved data protection, digital trust, and business security. Several project ideas were generated and evaluated before selecting the development of a penetration testing framework for small businesses [2], [10]. This project was chosen because it offers a structured and practical approach to identifying vulnerabilities and improving cybersecurity practices for organisations with limited security resources. The selected topic also aligns with personal interests in penetration testing and supports future development of technical and research skills.

Task 2 – Aim, Objectives & Research Area

17 June 2026 11:15

Task 2: Aim and Objective

Introduction:

Cybersecurity has become increasingly important as small businesses continue to adopt digital technologies while facing growing cyber threats [4]. Many small businesses have limited cybersecurity expertise and resources, making them more vulnerable to attacks. This project proposes the development of a penetration testing framework designed to support small businesses in identifying vulnerabilities and improving their security practices. The project will explore research methods, investigate current cybersecurity approaches, and identify practical recommendations to create value through improved digital protection.

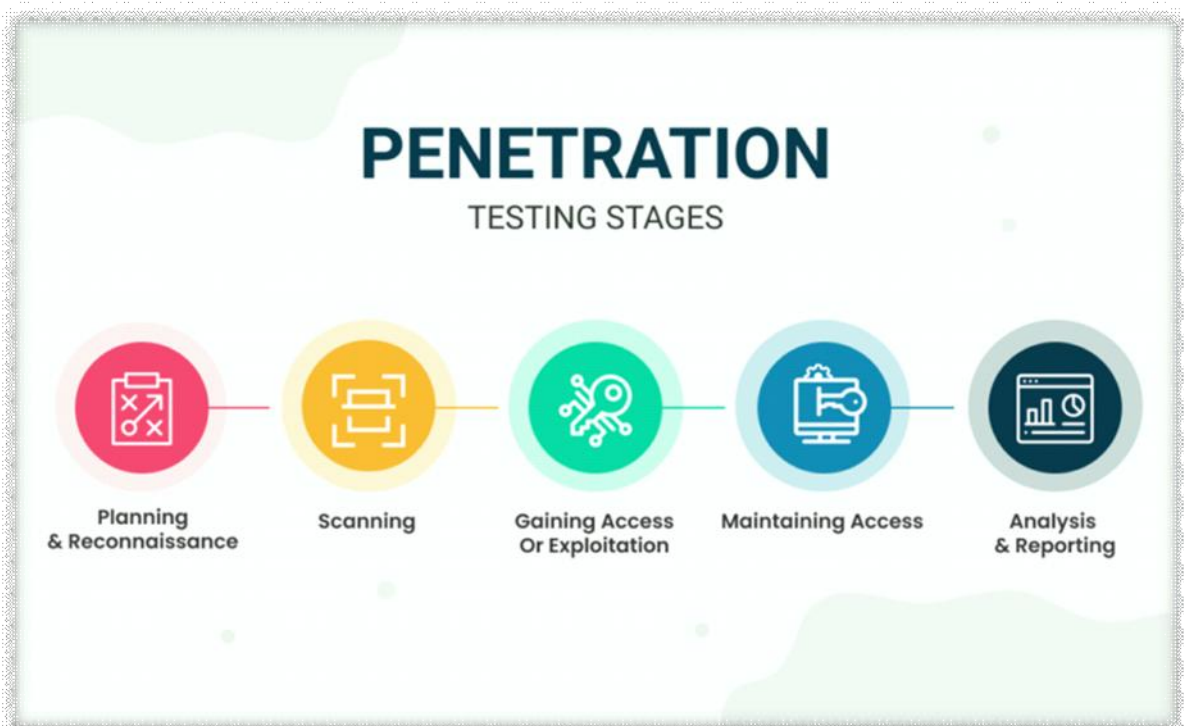


Figure 4 :penetration testing

Project Aim:

To develop a penetration testing framework that supports small businesses in identifying cybersecurity vulnerabilities and improving their overall security practices.

Objectives:

1. To investigate common cybersecurity threats affecting small businesses.
2. To review existing penetration testing approaches and cybersecurity frameworks.
3. To identify appropriate methods for vulnerability assessment.
4. To design a structured penetration testing framework suitable for small businesses.
5. To evaluate how the proposed framework could improve cybersecurity awareness and protection.

Research Philosophy:



Figure 5: Research Philosophy

The research philosophy selected for this project is **Pragmatism** [3]. Pragmatism focuses on solving real-world problems by selecting research methods that best address the research objectives rather than relying on a single theoretical perspective [3]. This philosophy is suitable for cybersecurity research because it allows both qualitative and quantitative approaches to be used where appropriate. In this project, pragmatism supports the investigation of cybersecurity challenges faced by small businesses and the development of a practical penetration testing framework. By combining evidence from academic literature, industry reports, and collected feedback, the research aims to produce realistic and useful outcomes.

Research Area:

This project is positioned within the fields of cybersecurity and penetration testing, with a particular focus on improving security practices for small businesses. The research area explores vulnerability identification, ethical security testing, cybersecurity frameworks, and practical methods that organisations can adopt to reduce cyber risks. The project also considers how structured penetration testing can create value through improved digital resilience and business protection.



Figure 6 :Area of Research

Search Tools and Research Strategy:

To identify relevant research for this project, multiple academic and professional search tools will be used. Academic databases allow access to peer-reviewed and reliable sources related to cybersecurity and penetration testing [3].

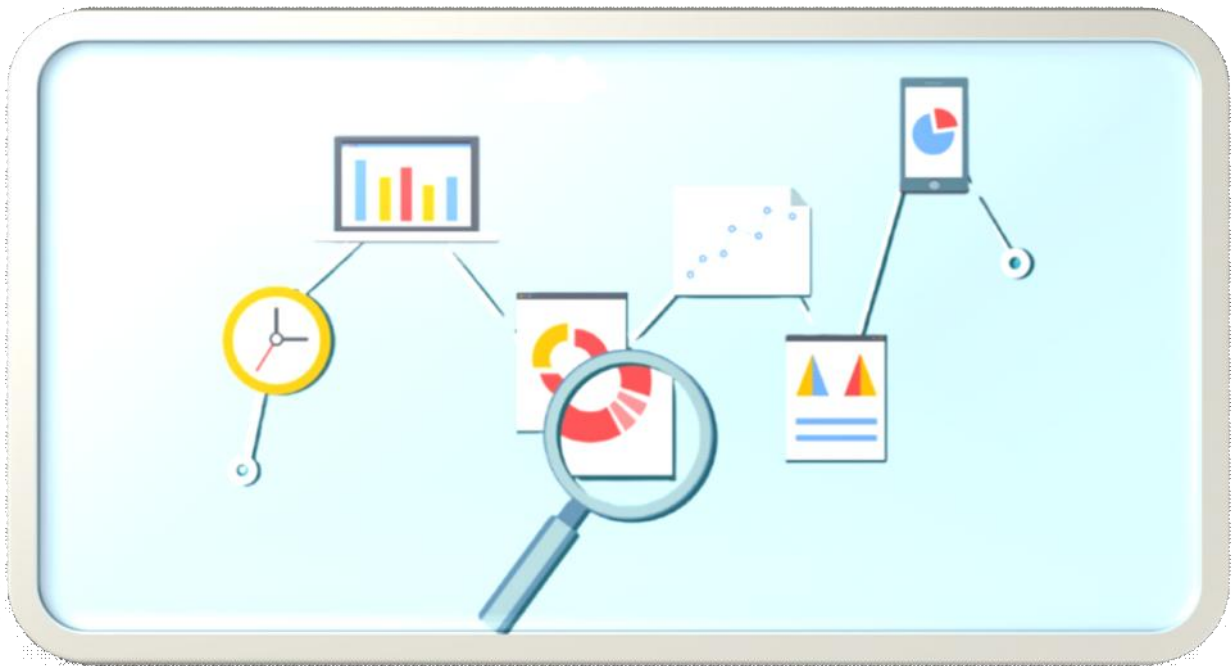


Figure 7:search strategy

Search Tools:

- Google Scholar
- IEEE Xplore
- ScienceDirect
- University Library Database
- ACM Digital Library

Example Search Terms:

- "Penetration testing framework for small businesses"
- "Cybersecurity challenges in SMEs"
- "Vulnerability assessment methods"
- "Ethical hacking and business security"
- "Small business cybersecurity"

Search Strategy:

- Use Boolean operators (AND, OR)
- Filter by publication year
- Prioritise peer-reviewed research
- Compare multiple sources
- Evaluate relevance and reliability

Summary

This task established the project direction by defining a clear aim, objectives, research philosophy, and search strategy. These elements provide a foundation for investigating how a penetration testing framework can improve cybersecurity practices for small businesses and support evidence-based project development[9].

Task 3 – Research Strategies

Task 3: Research Strategies:

Introduction:

This section outlines the research strategies that will support the development of the proposed penetration testing framework for small businesses. Effective research planning is important to ensure that collected information is trustworthy, ethically obtained, and relevant to the project objectives. Appropriate methods of data collection and analysis will support evidence-based decision making throughout the project.

Validity, Reliability, Generalisability and Ethical Considerations:

To improve the quality of this research, several research principles will be considered. Validity refers to ensuring that the research methods and collected data accurately address the project objectives and investigate cybersecurity challenges experienced by small businesses [3]. Reliability focuses on producing consistent findings by using structured procedures and documenting the research process clearly [7]. Generalisability will be supported by collecting information from a range of sources and considering findings that may apply across different small business environments.

Ethical considerations are important because cybersecurity research must be conducted responsibly [1],[6]. No real systems will be tested without permission, and no sensitive organisational data will be collected. Participants involved in surveys or feedback activities will be informed about the purpose of the research and participation will remain voluntary and anonymous where appropriate.

Research Strategy and Data Collection Methods:

A mixed research strategy will be adopted for this project to combine information from academic literature and user feedback. Secondary research will include reviewing journal articles, cybersecurity reports, and existing penetration testing frameworks. Primary research will be conducted through a short questionnaire designed to gather opinions and experiences related to cybersecurity awareness and security practices within small businesses.

The selected data collection methods support both technical understanding and practical insights that may influence the design of the proposed penetration testing framework.

Selected Data Collection Methods:

- Literature review
- Online questionnaire
- Industry reports
- Comparative analysis of existing frameworks

Pilot Data Collection:

Before full implementation, a pilot questionnaire will be conducted to gather initial feedback and improve the focus of the project. The pilot study will test whether the questions are clear, relevant, and aligned with the research objectives. Feedback collected during the pilot stage may be used to simplify questions, improve wording, and identify additional areas for investigation.

Example Pilot Questions:

1. How confident are you in your organisation's cybersecurity practices?
2. Has your organisation previously performed vulnerability testing?
3. What cybersecurity challenges are most common?
4. Would a structured penetration testing framework be useful?
5. Which areas of cybersecurity require improvement?

Quantitative and Qualitative Analysis:

Introduction:

Data analysis is an important stage of research because it helps identify patterns, interpret findings, and support project decisions. This project will consider both quantitative and qualitative approaches to analyse collected information.

Quantitative analysis focuses on numerical data and statistical patterns [5]. For this project, questionnaire responses may be converted into percentages or charts to identify common cybersecurity concerns among participants. Quantitative analysis supports objective comparison and allows trends to be identified across responses.

Qualitative analysis focuses on non-numerical information and explores opinions, experiences, and themes [3]. Open responses collected during the pilot questionnaire and insights gathered from academic literature may be analysed through thematic analysis to identify recurring cybersecurity issues and practical recommendations for the proposed framework.

Combining both forms of analysis provides a broader understanding of cybersecurity challenges and supports evidence-based project development.

Analysis Type	Data Type	Example
Quantitative	Numerical	Survey percentages
Qualitative	text / opinions	Questionnaire responses
Mixed Method	Combined	Survey + literature

Summary:

This task identified research strategies that support the development of the proposed penetration testing framework. Consideration was given to research quality, ethical practice, data collection methods, and approaches to data analysis. The selected methods aim to produce reliable findings that contribute to improving cybersecurity practices for small businesses[8].

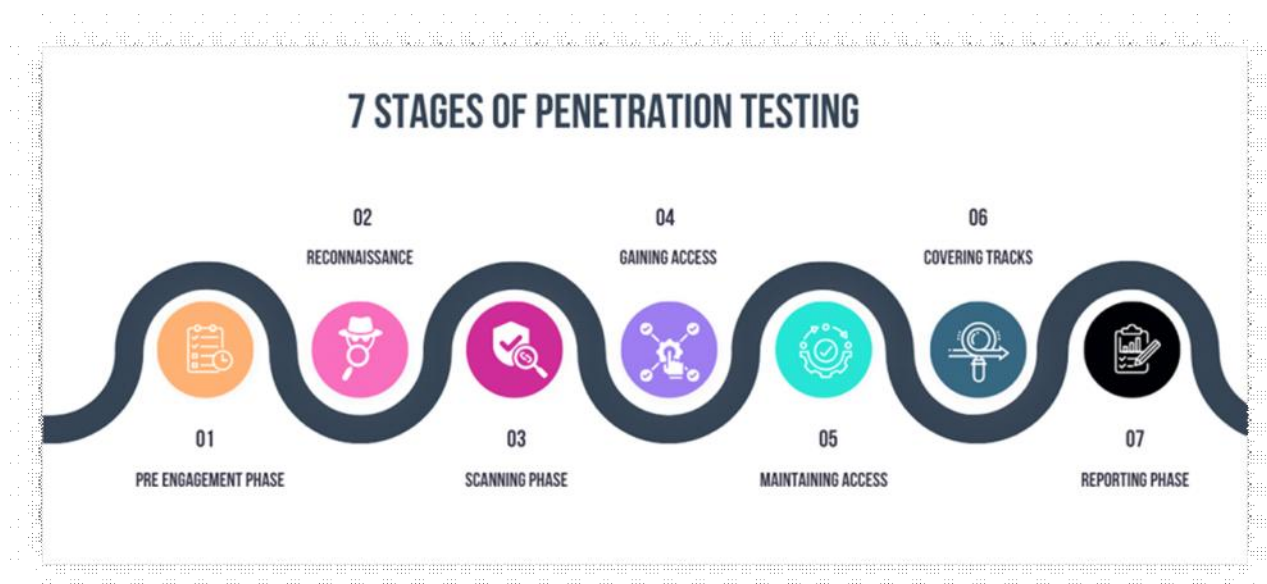


Figure 8: pentest stage

Appendices

17 June 2026 11:15

Developing a Penetration Testing Framework to Improve Cybersecurity for Small Businesses

Introduction

The idea for this framework and cybersecurity can come from many sources. Small businesses and individuals are a common focus area because they often have cyber threats but lack the resources and security expertise [1][2]. Small businesses and individuals often lack the resources and security expertise to defend against growing cyber threats. After exploring several potential cybersecurity solutions—such as phishing detection tools, network operations, and vulnerability scanners—the decision to develop a penetration testing framework emerged as the most practical and impactful choice. It provides a structured method for identifying weaknesses, strengthening security posture, and educating small businesses in building resilience. Additionally, the project aligns with personal interests in penetration testing and contributes to the development of essential research, analysis, and problem-solving skills, making it both socially relevant and personally rewarding.

Aim

Cybersecurity has become a critical concern for small businesses because it is essential to their survival. However, many small businesses lack the resources and expertise to defend against growing cyber threats. This project proposes the development of a penetration testing framework designed to support small businesses in identifying vulnerabilities and improving their security practices. The project will explore research methods, investigate current cybersecurity approaches, and identify potential weaknesses to create value through improved digital protection.

Conclusion

In summary, this framework and cybersecurity can come from many sources. Small businesses and individuals are a common focus area because they often have cyber threats but lack the resources and security expertise to defend against growing cyber threats. After exploring several potential cybersecurity solutions—such as phishing detection tools, network operations, and vulnerability scanners—the decision to develop a penetration testing framework emerged as the most practical and impactful choice. It provides a structured method for identifying weaknesses, strengthening security posture, and educating small businesses in building resilience. Additionally, the project aligns with personal interests in penetration testing and contributes to the development of essential research, analysis, and problem-solving skills, making it both socially relevant and personally rewarding.

Objectives

- 1. To investigate common cybersecurity threats affecting small businesses.
- 2. To develop penetration testing approaches and cybersecurity frameworks.
- 3. To identify appropriate methods for vulnerability assessment.
- 4. To design a structured penetration testing framework suitable for small businesses.
- 5. To evaluate how the proposed framework could improve cybersecurity awareness and protection.

Mind Map

The mind map illustrates how credibility and innovation can support the development of cybersecurity solutions and create value for society. Different areas of interest related to computer science were explored, including threat hunting, vulnerability assessment, network security, and emerging cybersecurity technologies. The map also considers the wider impact of cybersecurity through improved data protection, digital trust, and business security. Several project ideas were generated and presented before selecting the development of a penetration testing framework for small businesses [1][2]. This project was chosen because it offers a structured and practical approach to identifying vulnerabilities and improving cybersecurity practices for organizations with limited security resources. The selected topic also aligns with personal interests in penetration testing and supports future development of technical and research skills.

References

- [1] National Institute of Standards and Technology (NIST). The Cybersecurity Framework: A Practical Guide to Improving Cybersecurity. Washington, DC: NIST, 2018.
- [2] Small Business Administration (SBA). Cybersecurity for Small Business. Washington, DC: SBA, 2020.
- [3] Cybersecurity and Infrastructure Security Agency (CISA). Cybersecurity for Small Business. Washington, DC: CISA, 2021.
- [4] Small Business Administration (SBA). Cybersecurity for Small Business. Washington, DC: SBA, 2020.

References

17 June 2026 11:16

- [1] National Institute of Standards and Technology (NIST), "The Cybersecurity Framework (CSF) 2.0," Gaithersburg, MD, USA, 2024.
- [2] OWASP Foundation, "OWASP Top 10: The Ten Most Critical Web Application Security Risks," 2021.
- [3] M. Saunders, P. Lewis and A. Thornhill, Research Methods for Business Students, 8th ed., Harlow, UK: Pearson, 2019.
- [4] IBM Security, "Cost of a Data Breach Report 2024," IBM Corporation, 2024.
- [5] W. Stallings and L. Brown, Computer Security: Principles and Practice, 5th ed., Pearson, 2020.
- [6] National Cyber Security Centre (NCSC), "Small Business Guide: Cyber Security," United Kingdom, 2023.
- [7] National Institute of Standards and Technology, "Getting Started with Cybersecurity Risk Management," 2024.
- [8] J. M. Camacho, A. Couce-Vieira, D. Arroyo and D. Rios Insua, "A Cybersecurity Risk Analysis Framework for Systems with Artificial Intelligence Components," 2024.
- [9] A. Pollini, M. Tedeschi and D. Gioia, "Cybersecurity Challenges and Security Practices in Small and Medium Enterprises," Journal of Cybersecurity, vol. 8, no. 1, 2022.
- [10] S. Yadav and P. K. Mishra, "Cybersecurity Risk Assessment and Penetration Testing Frameworks for Small and Medium Enterprises," IEEE Access, vol. 11, pp. 105233–105249, 2023.