

FMP Proposal

by Kieran Brown

Submission date: 20-Oct-2025 01:28PM (UTC+0100)

Submission ID: 265733488

File name: 50539_Kieran_Brown_FMP_Proposal_695044_1182609238.docx (217.79K)

Word count: 1960

Character count: 13175



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Design and Implementation of a Cyber Resilient Virtual Network using Oracle VM

by
Kieran Brown

Supervisor: Niteesh Kaliamurthy

Project Proposal submitted as part of the requirements
for the award of
BSc (Hons) Computing

October 2025

Introduction / Aims and Objectives

This project aims to design, implement, and evaluate a cyber resilient virtual network using Oracle VM Virtualbox as the virtualisation platform. The network will incorporate windows and Linux operating systems to simulate a realistic, enterprise environment. The windows server and its client systems will replicate a typical work infrastructure, while the Linux server and its client will add network operating system diversity resilience testing opportunities. Once the network topology has been completed an attacker node that uses Kali Linux will be deployed to conduct penetration testing and vulnerability scanning. A penetration test simulates an attack and is used to “identify any weak spots in a systems defence which attackers could take advantage of” [1] This can be used as a major factor to an organisation becoming cyber resilient as being aware of “security vulnerabilities before an attacker can exploit them” [2] enables proactive resolving, reduces potential attack surfaces, and strengthens the organisations overall security posture.

The problem statement comes from the gap between well established theoretical cyber resilience frameworks such as those outlined by NIST “which is a set of guidelines that help evaluate business security system and guide the company to improve its security posture” [3] and ENISA and their practical, cost effective implementation within small to medium sized organisations (SMEs). While existing resilience strategies are often comprehensive, they are typically designed to best suit large organisations relying on advanced infrastructure, specialised personnel, and financial resources. Research has shown that many SMEs face barriers such as lack of in house expertise, competing operational priorities and limited budgets, which makes it difficult to implement the required frameworks effectively. “Many SMEs may struggle to afford the tools and services necessary to protect their systems and data” [4] This creates a critical vulnerability gap, as smaller organisations are then exposed to cyber attacks.

SMART Objectives:

1. To design and configure a multi platform virtual network topology using Oracle VM Virtualbox that simulates realistic enterprise infrastructure
2. To conduct vulnerability assessments and penetration testing using Kali Linux and associated tools to identify network weaknesses
3. To implement security controls to improve cyber resilience

4. To evaluate the impact of implemented security measures by detection time, recovery time and vulnerability reduction over a period of time

Background to this project / Literature Review

The increasing frequency and severity of cyber attacks have placed network infrastructure at the forefront of organisational security challenges. The traditional perimeter-based security models are no longer sufficient to guarantee service availability and integrity. As a result of this, cyber resilience, and the ability for “an organisation to protect itself from, detect, respond to and recover from cyber attacks.” [5] is at its highest level of importance. This is particularly critical as modern organisations rely heavily on interconnected systems, remote access and cloud services which expand the attack surface and increase the potential impact of a successful breach. Effective cyber resilience doesn’t only mitigate financial and operational losses. It also ensures business continuity, as well defined recovery plans can “ensure that critical operations can continue in the event of a security breach” [6]

Frameworks such as those developed by the National Institute of Standards and Technology (NIST) and the European Union Agency for Cybersecurity (ENISA) provide guidance on how to “improve their cybersecurity measures” [7] The NIST Cybersecurity Framework is organised into five core functions: Identify, Protect, Detect, Respond. “The framework provides a catalog of cybersecurity outcomes based on existing standards” [8] which offers a comprehensive approach to securing digital networks and maintaining operational continuity during attacks. ENISA gives complementary guidance to emphasise operational resilience. Its main purpose is to “provide a common level of cybersecurity knowledge and skills across different sectors and organisations.” [9] The strategies used in this are made to be adaptable for organisations of different sizes.

Despite the availability of these frameworks, research indicates that “SMEs are more vulnerable to cyber attacks than larger organisations” [10]. Limited budgets prevent these SMEs from adapting to the frameworks. As a result many lack formalised incident response or recovery plans. Studies show that “SMEs face cyber threats including 43% of all attacks” [11] this is due to them not having the frameworks. This approach has the potential to make resilience strategies more accessible, affordable and actionable for smaller organisations

Practical approaches to bridging this gap involve creating controlled virtual environments where resilience strategies can be tested and refined without risk to live systems. Virtualisation platforms such as Oracle VM virtualbox, allow the deployment of multiplatform networks incorporating both windows and Linux servers, which can simulate realistic enterprise infrastructures. Within these environments, penetration testing assessments using tools like Kali Linux as it is a “robust platform prepared with numerous vulnerability tools” [12] which can help enable the identification of weaknesses and evaluation of security controls, aligning the detect and respond phases of the NIST and ENISA frameworks.

In summary, while theoretical models provide clear guidance on building cyber resilience, a practical implementation gap persists for SMEs. This project addresses that gap by translating cyber resilience concepts into a virtualised network environment testing and implementing security controls and providing in depth insights to their effectiveness.

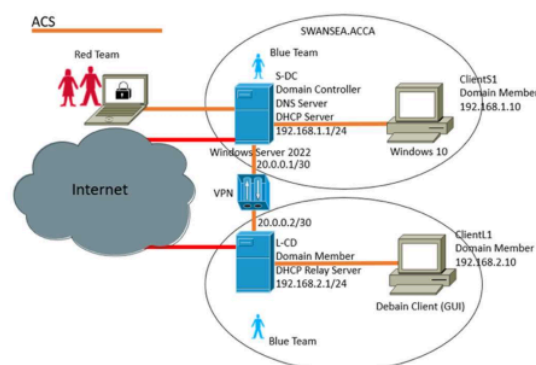
Project Design

This project is designed to focus on taking well known cyber resilience frameworks and apply them in a practical and controlled environment. A lot of existing research and guidance from organisations such as National Institute of Standards and Technology (NIST) and European Union Agency for cybersecurity (ENISA) show how organisations can build stronger security but these can be difficult for smaller enterprises. the aim is to create a virtualised network, implement layered security measures and evaluate the effectiveness against cyber attacks.

Network set up and configuration

The network topology will be built in Oracle VM Virutalbox, which is free and widely used as “the worlds most popular open source” [13] for creating virtual environments. The virtual network will be structured around a multi segmented netowkr topology which “divides a network into multiple segments or subnets”[14]. (see figure 1), which

(figure 1)



mirrors a small enterprise environment. The design consists of two internal network segments connected through a VPN and a Windows server as the domain controller and security control point.

The first segment includes the S-DC (Domain controller) server running DNS and DHCP services, connected to the windows 10 client. This simulates a typical windows based business environment. The second segment includes the L-CD which is the Linux Server (Domain Member) and Debian client. By using a multiplatform approach it introduces operating system diversity which ensures broader resilience testing.

The attacker node (red team) will be positioned outside the internal networks and will access the lab through a simulated cyber attack. The red team node will use Kali Linux to carry out penetration testing and vulnerability scanning. The blue teams side will represent the defensive organisation which will implement a layered defence in depth approach, consisting of baseline hardening, network segmentation with strict firewall and ACL policies to limit lateral movement, and least privileged access controls combined with multifactor authentication. It will deploy continuous monitoring and centralised logging alongside IDS/IPS sensors and periodic packet captures for detection and analysis, while conducting regular automated vulnerability scans and prioritised patch management. Additional defense will be explored to enhance visibility and resilience against sustained or advanced attacks

By using this structure, it enables realistic and in depth testing of how an organisation might defend its system across different platforms. It also supports testing scenarios involving VPN traffic inspection, credential attacks on domain services and privilege escalation on both the Windows and Linux systems.

Security Measures

The security measures will align with the five core functions of NIST framework "Identify, Protect, Detect, Respond, Recover"[15]

Identify and Protect: System Hardening will be carried out by restricting user permissions, patching known vulnerabilities and disabling unnecessary services.

Detect and Respond: Logging and monitoring will be implemented to detect suspicious activity supported by IDS and IPS

Recover: Simple recovery procedures will be used to restore services quickly after an incident.

These measures are realistic for SMEs ensuring that the project remains practical and relevant for its target audience.

Penetration testing and Evaluation

Once the network is established , the Kali Linux machine will be used to conduct controlled penetration testing. Which involves scanning for vulnerabilities, attempting to exploit weaknesses and evaluating the networks defensive response. Key metrics will include:

- The number and severity of vulnerabilities before and after controls are applied
- The detection speed and how effective the security measures are.
- The time it takes to recover following an attack.

By using this process it will provide measurable insights into how the security measures impact overall cyber resilience.

Ethical Considerations

All testing will be conducted in an isolated lab environment, to ensure that no real systems or data is at risk. All tools used are legal in this controlled context and no personal data will be used. The focus of the project will remain on defensive capability. This ensures that the project is conducted safely and legally.

Deliverables

The final deliverables will include the complete virtual lab environment, a record of security configurations, testing activities and an evaluation report. This report will assess the effectiveness of security controls and provide practical recommendations for SMEs looking to improve their cyber resilience without significant setback in budget.

Resources and Planning

Task	Resources Required	Deadline
Proposal	Word	20/10/2025
Network design and topology planning	Oracle VM, diagrams, project plan	10/11/2025
VM deployment	Host PC Oracle VM	17/11/2025
Security Hardening and controls implementation	IDS/IPS firewall, access control settings	21/11/2025
Penetration testing and vulnerability scanning	Kali Linux	12/12/2025
Monitoring and Evaluation	Logging tools, packet capture software, evaluation metrics	10/01/2025
Reporting and documentation	Word	10/03/2025

Bibliography

[1]

Cloudflare, "What Is Penetration Testing? What Is Pen Testing? | Cloudflare UK," *Cloudflare*, 2024. Available: <https://www.cloudflare.com/en-gb/learning/security/glossary/what-is-penetration-testing/>. [Accessed: Oct. 15, 2025]

[2]

K. Malik, "Learn Why Penetration Testing is Important," *www.getastra.com*, Oct. 12, 2021. Available: <https://www.getastra.com/blog/security-audit/why-penetration-testing-is-important/>. [Accessed: Oct. 15, 2025]

[3]

M. Grigutyte, "What is the NIST cybersecurity framework? Cybersecurity frameworks explained," *NordVPN*, Sep. 21, 2024. Available: https://nordvpn.com/blog/cybersecurity-framework/?nc=Pmax_-_UK_-_Generic_-_EN_-_DMT_-_USD&ns=google&nm=cpc&nt=&na=&gad_source=1&gad_campaignid=21317078835&gbraid=0AAAAADwsNkRXb-P3Cnt6mV1MVslzwtIvK&gclid=CjwKCAjwr8LHBhBKEiwAy47uUtA39IH_XIUkchv4VM0AZXe5QjU7hCI9fZBijkChYLRlLdB0odVB5hRoCwcMQAvD_BwE. [Accessed: Oct. 15, 2025]

[4]

N. Rawindaran, A. Jayal, E. Prakash, and C. Hewage, "Perspective of Small and Medium Enterprise (SME's) and their Relationship with Government in Overcoming Cybersecurity Challenges and Barriers in Wales," *International Journal of Information Management Data Insights*, vol. 3, no. 2, pp. 100191–100191, Nov. 2023, doi: <https://doi.org/10.1016/j.jjime.2023.100191>. Available: <https://www.sciencedirect.com/science/article/pii/S2667096823000381>. [Accessed: Oct. 16, 2025]

[5]

I. Governance, "What is cyber resilience | IT Governance UK," *Itgovernance.co.uk*, 2016. Available: <https://www.itgovernance.co.uk/cyber-resilience>. [Accessed: Oct. 15, 2025]

[6]

S. Kauffman, "Importance of Cyber Resilience in Cyber Security Strategy," *Northdoor*, Feb. 19, 2024. Available: <https://www.northdoor.co.uk/insight/blog/why-cyber-resilience-may-be-more-important-than-cyber-security/>. [Accessed: Oct. 15, 2025]

[7]

D. P. F. Möller, "NIST Cybersecurity Framework and MITRE Cybersecurity Criteria," *Advances in Information Security*, vol. 103, pp. 231–271, 2023, doi: https://doi.org/10.1007/978-3-031-26845-8_5

[8]

A. Mahn, "Identify, Protect, Detect, Respond and Recover: The NIST Cybersecurity Framework," *NIST*, Oct. 22, 2018. Available: <https://www.nist.gov/blogs/taking->

measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework.
[Accessed: Oct. 16, 2025]

[9]

ENISA, "Cybersecurity Certification Framework | ENISA," *Europa.eu*, Jun. 24, 2025.
Available: <https://www.enisa.europa.eu/topics/product-security-and-certification/cybersecurity-certification-framework>. [Accessed: Oct. 16, 2025]

[10]

Sharp, "SMEs are the prime target for cyber attacks," *www.sharp.co.uk*, Mar. 23, 2023.
Available: <https://www.sharp.co.uk/news-and-events/blog/smes-are-the-prime-target-for-cyber-attacks>. [Accessed: Oct. 16, 2025]

[11]

NFP, "The threats cyber criminals pose to SMEs," *NFP*. Available:
<https://www.nfp.co.uk/media/insights/the-threats-cyber-criminals-pose-to-smes/>. [Accessed: Oct. 16, 2025]

[12]

T. Team, "Kali Linux – Vulnerability Analysis Tools - DataFlair," *DataFlair*, Dec. 29, 2023.
Available: <https://data-flair.training/blogs/kali-linux-vulnerability-analysis-tools/>. [Accessed: Oct. 16, 2025]

[13]

Oracle, "Oracle VirtualBox," *Oracle.com*, 2024. Available:
<https://www.oracle.com/africa/virtualization/virtualbox/>. [Accessed: Oct. 16, 2025]

[14]

PaloAltoNetwork, "What Is Network Segmentation?," *Palo Alto Networks*. Available:
<https://www.paloaltonetworks.co.uk/cyberpedia/what-is-network-segmentation>. [Accessed: Oct. 16, 2025]

[15]

StickmanCyber, "Stickman Cyber Security," *Stickmancyber.com*, 2021. Available:
<https://blogs.stickmancyber.com/cybersecurity-blog/nist-framework-functions-explained>.
[Accessed: Oct. 16, 2025]

FMP Proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

70/100

PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT

Student **Kieran Brown**

Mark 70

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project	20	18
Well identified Problem. SMART objectives achieved. Good understanding on the Advanced Cybersecurity Module's Assessment task and considering to develop from there for your Major Project. Addressed the deliverables, however further more quantifiable thresholds required. Overall a good start		

Background to the Project / Literature Review (400 words)		
Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8 journal papers and book chapters rather than just websites; Selection of relevant models & concepts More academic credible literatures required. Critical discussions and arguments required to clearly identify the gaps .	20	15
Project Design (500 words)		
Clear statement of which development methods are to be used and why they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will	30	17

be analysed Development methods (Topology, Environment etc) are clear, discussed in detail. More adequate details related to the Vuln. Assessments, Pen-Testing, Posture of Red Team/ Blue Team etc could have added value.		
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices Deliverables listed comprehensively. Project Planning (Gantt Charts) could have added more value.	15	10

Document Presentation		
Correct spelling, grammar and punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with bibliography; Strict word limit Good Flow. Proof reading is recommended to avoid mistakes.	15	10
TOTAL	100	70

PAGE 1
PAGE 2
PAGE 3
PAGE 4
PAGE 5
PAGE 6
PAGE 7
PAGE 8
PAGE 9