

2024571_ACCA6020_ProjectPro posal

by Mohammed Ansari

Submission date: 17-Oct-2025 12:17PM (UTC+0100)

Submission ID: 265622980

File name: 28549_Mohammed_Ansari_2024571_ACCA6020_ProjectProposal_695044_95574103.docx
(101.14K)

Word count: 1414

Character count: 9127



A Study of the use of Digital Forensics, Securing Cyberspace and Analysing Digital Evidence (Proposal)

By

Mohammed Ansari (2024571)

Supervisor (potential): Dr. Nitheesh Kaliyamurthi

Second Marker (potential): Gaynor Thomas

Project submitted as part of the requirements for the award of
BSc (Hons) Computing - Computer Networks and Cybersecurity

May 2026

Table of Contents

1. Introduction	3
2. Background to the Proposed Research (Literature Review)	3
3. Research Problem Statement.....	4
4. Research Aim & Objectives.....	4
5. Methodology.....	5
5.1 Methods.....	5
5.2 Materials	5
6. Project Plan.....	6
7. References.....	6

1. Introduction

The rapid expansion of digital networks, cloud computing, and Internet-of-Things (IoT) technologies have significantly broadened the global attack surface for cyber threats. Both organizations and individuals are increasingly exposed to risks of system compromise, data exfiltration, and operational disruption due to sophisticated and evolving vulnerabilities. A 2024 IBM Security report indicates that the average cost of a data breach reached USD 4.45 million worldwide, marking a 15% increase over the past three years [1]. This rise highlights the pressing need for practical, hands-on cybersecurity research that emphasizes vulnerability identification, analysis, and mitigation across various computing environments.

This project seeks to replicate a realistic networked environment utilizing four distinct operating systems: Windows 10, Windows Server 2022, Ubuntu Linux, and Kali Linux, to perform systematic vulnerability assessments and implement effective mitigation strategies. Each of these systems serves as a common target in real-world enterprises or academic networks. By configuring and securing them within a controlled laboratory setting, the project connects theoretical cybersecurity principles with practical network defense techniques.

The impetus for this study stems from the growing complexity of cyberattacks, the deficit of qualified cybersecurity experts, and the necessity for practical technical expertise in vulnerability management [2]. Tools like Nmap, Nessus, and Wireshark have become integral to both academic and industry practices in cybersecurity for the purposes of threat detection and system auditing [3]. Nevertheless, numerous network administrators and students do not possess a systematic comprehension of how vulnerabilities interact within diverse systems.

Consequently, this project aims to enhance cybersecurity education and practice by providing a detailed case study on vulnerability assessment and mitigation across various platforms. It will not only pinpoint two minor and two major vulnerabilities but also devise and assess the effectiveness of relevant countermeasures. The results will offer valuable insights into proactive defense strategies, system hardening techniques, and optimal practices for managing enterprise-level network security.

2. Background to the Proposed Research (Literature Review)

The realm of computer networks and cybersecurity has progressed in response to increasing threats and advancements in technology. This discipline amalgamates concepts from computer science, information systems, and risk management to ensure the integrity, confidentiality, and availability of data.

Traditionally, network security emphasizes the prevention of unauthorized access and the maintenance of service continuity [4]. A fundamental aspect of this domain, vulnerability management, entails the identification, classification, and remediation of weaknesses within IT systems. As noted by ENISA [5], proactive vulnerability management can diminish the success rates of cyberattacks by as much as 70%. Tools such as Nessus and OpenVAS facilitate automated vulnerability scanning and benchmarking against databases like the Common Vulnerabilities and Exposures (CVE) repository.

Various operating systems pose distinct security challenges. Windows platforms are frequently targeted due to their extensive usage and integrated services [6]. Conversely, while Linux systems are often regarded as more secure, they are not exempt from vulnerabilities related to privilege escalation and misconfiguration [7]. By evaluating both Windows and Linux systems, this project aims to provide a comprehensive perspective on network security management within diverse environments.

Nmap is extensively utilized for port scanning and service enumeration [8]. In contrast, Nessus offers more sophisticated vulnerability detection, providing CVSS ratings and remediation recommendations [9]. Wireshark enables thorough inspection of network traffic, assisting in intrusion detection and protocol-level vulnerability assessment [10]. The integration of these tools establishes a robust framework for identifying and analyzing vulnerabilities from both external and internal viewpoints. Despite considerable progress in vulnerability management tools, there is a scarcity of studies that offer a comprehensive, cross-platform experimental methodology for the identification and mitigation of vulnerabilities in both Windows and Linux systems. Numerous academic publications tend to concentrate on the development of tools or theoretical evaluations instead of engaging in practical comparative experiments [11]. This project seeks to fill this void by conducting a multi-system vulnerability assessment and mitigation experiment, which facilitates the empirical assessment of defense strategies within a realistic laboratory setting.

3. Research Problem Statement

There is an increasing demand for effective, multi-platform strategies for vulnerability assessment and mitigation within networked environments. Current research frequently falls short in providing empirical analysis regarding the manifestation of vulnerabilities and their resolution across various operating systems. This project seeks to fill this void by conducting a comparative analysis of vulnerability assessment and mitigation on Windows 10, Windows Server 2022, Ubuntu, and Kali Linux systems.

4. Research Aim & Objectives

Aim:

To perform a cross-platform vulnerability assessment and mitigation experiment on both Windows and Linux systems utilizing standard cybersecurity tools, thereby improving the comprehension of network security management and practices for system hardening.

Objectives:

- 1- To establish and configure four interconnected virtual machines, namely Windows 10, Windows Server 2022, Ubuntu, and Kali Linux, within a secure testing network.
- 2- To identify and evaluate at least two minor and two major vulnerabilities employing tools such as **Nmap**, **Nessus**, and **Wireshark**.
- 3- To devise and implement suitable mitigation strategies to address the identified vulnerabilities.
- 4- To assess the effectiveness of the mitigation measures through post-remediation scanning and comparative analysis.
- 5- To document the results and recommend best practices for securing multi-platform networked systems.

5. Methodology

5.1 Methods

This project employs an experimental research strategy that integrates both quantitative and qualitative mixed methods approaches. The experimental method is appropriate as it entails controlled testing of systems to observe quantifiable changes following interventions [12]. The qualitative component focuses on interpreting the severity and nature of vulnerabilities, whereas the quantitative component emphasizes measurable parameters such as CVSS scores, patch effectiveness, and results from scan comparisons.

The research is grounded in a positive philosophy, positing that cybersecurity vulnerabilities can be objectively identified and quantified through empirical testing. The research design includes the establishment of four virtual machines interconnected via a simulated local network. Vulnerability scans will be performed utilizing **Nmap**, **Nessus**, and **Wireshark**. Subsequently, post-mitigation scans will confirm the effectiveness of the security interventions.

5.2 Materials

Data Sources:

- Vulnerability scan reports generated by **Nmap**, **Nessus**, and **Wireshark**.
- System logs and network traffic captures before and after mitigation.

Data Collection Tools:

- **Nmap** for network mapping and port scanning.
- **Nessus** for vulnerability detection and risk scoring.
- **Wireshark** for packet-level traffic analysis and anomaly detection.

Ethical Considerations:

All experiments will be conducted within an isolated virtual environment, ensuring no real network systems are impacted. The research complies with ethical guidelines for cybersecurity experimentation, avoiding unauthorized data access or network intrusion.

Software Tools and Techniques:

- Operating Systems: Windows 10, Windows Server 2022, Ubuntu, Kali Linux.
- Virtualization: VirtualBox.
- Security Tools: Nmap, Nessus, Wireshark.
- Documentation: Microsoft Word, Excel, and PowerPoint.

Hardware Requirements:

- Computer with at least 32GB RAM, multi-core CPU, and 500GB storage for virtualization.

6. Project Plan

Phase 1: Literature review and project proposal submission

Phase 2: Setup of virtual lab environment

Phase 3: Initial vulnerability scanning and analysis

Phase 4: Identification of vulnerabilities

Phase 5: Implementation of mitigation measures

Phase 6: Post-mitigation evaluation

Phase 7: Report writing and presentation preparation.

7. References

- [1] IBM Security, "Cost of a Data Breach Report," IBM Corporation, 2024.
- [2] NIST "Vulnerability Management Framework," National Institute of Standards & Technology, 2023.
- [3] K. Scarfone, P. Mell, M. Souppaya, "Guide to Vulnerability Management," NIST SP 800-40, 2020.
- [4] W. Stallings, "Network Security Essentials: Applications and Standards," Pearson, 2021.
- [5] ENISA, "Threat Landscape Report," European Union Agency for Cybersecurity, 2023.
- [6] W. Alasmary and A. Alharthi, "Windows Security Vulnerabilities and Mitigation Techniques," J. Inf. Security Res., vol. 12, no. 4, pp. 211–225, 2022.
- [7] H. Patel, R. Singh, and S. Bhattacharya, "Linux Security and Hardening Techniques," Int. J. Comp. Netw., vol. 15, no. 2, pp. 88–99, 2021.
- [8] G. Lyon, "Nmap Network Scanning: The Official Nmap Project Guide," Insecure.Org, 2018.
- [9] Tenable, "Nessus Professional User Guide," Tenable Inc., 2022.
- [10] G. Combs and A. Orebaugh, "Wireshark Network Analysis," Syngress, 2020.
- [11] T. Rahman et al., "Cross-platform Security Assessment: A Practical Approach," Int. J. Cybersecurity Res., vol. 9, no. 1, pp. 33–45, 2021.
- [12] J. Creswell, "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches," Sage Publications, 2020.

FINAL GRADE

GENERAL COMMENTS

65/100

PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT

Student **Mohammed Ansari**

Mark 65

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	15
Your Project aims to secure the Enterprise Network. This is a extensive work on the Advanced Cybersecurity Module, which is good. However, the title is misleading with Digital Forensics. What is the scope of Digital Forensics in this project?		

Could have added clarity on the identified problems. Your objectives must add reviewing existing literatures to identify the current issues and challenges in Enterprise Networks. 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, critical appraisals and strong arguments required. A detailed literature review could have helped you in documenting a wide range of tools that could be used.	20	13
Project Design (500 words)		
Clear statement of which development methods are to be used and why	30	17

they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will be analysed More description on the Development methods - details related to the Vuln. Assessments, Pen-Testing could have added value. The report mentions nmap, Nessus and wireshark. More clarity on what other tools are likely to be used 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 Project Planning (Gantt Charts) could have added more value.	15	8

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 of the report.	15	11
TOTAL	100	65

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6
