

Student Name: David Julian Rapado

Engagement with Literature Skills	4	7
Knowledge and Understanding Skills	8	13
Cognitive and Intellectual Skills	4	25
Practical Application Skills	13	40
Transferable Skills for Life and Professional Practice	4	15
Round-up Mark	33	100

Engagement with Literature Skills

To achieve a high mark in this section, you must demonstrate a comprehensive and diverse engagement with literature, a clear understanding of Blue Team operations based on real-world examples, case studies, critical appraisals of the literature, and consistent referencing throughout the report (Part 2) and for your Proposed Mitigations (Part 3). The assessment encourages you to demonstrate how current cybersecurity practices and research can be applied to your proposed network mitigations.

- + Few references are underexplored and could benefit from more critical analysis
- + Emerging technologies like AI and machine learning are mentioned, a deeper evaluation of their limitations or comparative analysis with traditional methods would further enhance the academic rigor.
- + Could have included more critical evaluation of cited sources, comparing their effectiveness or discussing potential biases in the literature. Also, could have analysed the literatures rather than just describing.
- + In-text citations done

Knowledge and Understanding Skills

To achieve high marks in this section, you must demonstrate a comprehensive understanding of both advancements and challenges in Blue Team operations. The discussions include real-world examples, critical analysis of current methodologies, tools, and strategies, highlighting both their effectiveness and limitations. Note that your Part 1, CBT marks are added here as well.

- + Key areas such as threat detection, incident response, and SOC optimization are well-articulated
- + Could have provided more detailed exploration of frameworks and their implications for operational efficiency. Addressed emerging technologies, acknowledging their limitations alongside their potential.
- + CBT - Knowledge based 2/5

Cognitive and Intellectual Skills

You are expected to propose basic and advanced security measures that form the foundation of any secure network. These measures are essential for minimizing risks from common vulnerabilities and ensuring that user access and activities are properly monitored. The

proposed measures must be benchmarked against industry standards to show an understanding of best practices in securing networks. You must also provide justifications for their choices and practical demonstrations during the demonstration. Note that your Part 1, CBT marks are added here as well.

- + CBT - Analysis:1.8/15
- + Mitigations on ICMP Timestamp requests was presented.
- + Attempted to describe some steps, like performing a vulnerability scan and interacting with IP tables, with limited understanding. There was an effort to submit work despite challenges.
- + The lack of clarity and structure in responses, combined with the inability to articulate basic concepts or justify decisions, reflects inadequate preparation and conceptual grounding

Practical Application Skills

To achieve high marks in this section, you must demonstrate practical skills in configuring, assessing, and securing a network environment. This involves setting up a working network, conducting a thorough vulnerability assessment, exploiting vulnerabilities, and implementing both basic and advanced mitigations. You are expected to demonstrate clearly showcasing a strong understanding of practical cybersecurity measures.

- + Network Setup is done. Screenshots provided
- + Reflected on Information Gathering aspects.
- + Vulnerability Assessments done. However, further reflection on the outcomes of automated vulnerability assessment tools could have assisted in completing this coursework.
- + Vulnerability Exploitation: More focus and practice on Exploits, Payloads and its security enhancement required.
- + The demonstration indicates lack of preparation and hands-on experience. The inability to configure or use fundamental tools and concepts severely impacted the demonstration. Failed to start basic services, manage snapshots, or differentiate between attack and victim machines, which are critical for this module.
- + There was no attempt to diagnose or resolve issues encountered during the demonstration.

Transferable Skills for Life and Professional Practice

To achieve high marks in transferable skills, you must produce a well-structured report and present your demonstration with in-depth analysis of current methodologies, deliver a clear and reflective demonstration, and professional communication skills. You should showcase resource management, and fluency in technical aspects throughout the report and demonstration process.

- + Flow of the Report is ok

Feedback for ACCB6000

Date of Assessment: 6, 13 &14/01/2025 Date of Feedback: 10/02/2025

- + Would recommend to spend significant time in a lab environment setting up, restoring VMs, starting services, and conducting scans, vulnerability assessments and mitigations to build confidence and familiarity. Learn to identify and resolve common issues.
- + Your effort to submit work despite challenges is commendable, but the lack of preparation and understanding of basic cybersecurity principles significantly hindered your performance.
- + To improve: Build a strong foundation in network security basics, vulnerability assessments, and mitigation techniques.