Assessment 3 Information and Rubric

Subject Code	NTW 600
Subject Name	Computer Network and Security
Assessment Number and Title	**Assessment 3:** Cybersecurity Defence: Simulating and Mitigating Real-World Attacks
Assessment Type	Individual Assessment
Length / Duration	1500 ± 10% words
Weighting %	30%
Total Marks	100
Purpose of the assessment (with the learning outcome Mapping)	Assessment aims to develop students' practical cybersecurity skills by simulating network-based attacks and implementing defence strategies in a virtual lab, reinforcing theoretical knowledge through hands-on application and critical

Submission	On Moodle
Due Date	Week 10– Sunday at 23:59
Mode	Individual
Format	Microsoft Word
Late submission	Late report submission penalty may be applied (10% marks deduction per late day)
Academic Misconduct	Academic Misconduct is a serious offense. Depending on the seriousness of the case, penalties can vary from a written warning, zero mark, fail mark deduction to exclusion from the course or rescinding the degree. All the assessment with **similarity index > 25%** and **AI detection > 40%** will be reported.
	• All work must be submitted on Moodle by the due date along with a completed Assignment Cover Page.
Submission Guidelines	• Report must include clear headings and subheadings for all requirements mentioned below in the assessment description and instructions. • Report must be in MS Word format (**according to attached format**) New1.5 spacing, 12-pt, Times New Roman (Body) font, and 2 cm margins on all four sides of your page with appropriate section headings. • Reference sources must be cited in the text of the report and listed appropriately at the end in a reference list using *IEEE* referencing style.

Assessment Description

Assessment 3 is individual assessment, which bridges theory and practice, fostering technical competence and professional reporting skills. In this individual assessment, students are required to simulate at least two network-based cyber-attacks (e.g., Arp spoofing and SQL Injection) previously analysed in Assessment 2 and implement appropriate defence mechanisms (e.g., Firewall) in a controlled virtual lab environment using tools such as Kali Linux, Wireshark, Ettercap or sqlmap.

Students will document each stage of the simulation including lab setup, attack execution, mitigation techniques, and outcomes in a formal report supported by technical evidence. In

attack simulation, defence, highlighting tool usage and effectiveness.

Report Structure (Report Template)

Title Page

The title page must include the full assessment title, student's full name, student ID, unit code, lecturer's name, and the date of submission. This ensures the report is clearly identifiable and presented in a professional academic format.

Abstract

The abstract should be a concise summary (150–200 words) that outlines the purpose and scope of the report. It should briefly describe the two attacks selected, the simulation tools used, the defensive strategies applied, and the key outcomes or findings. This section should give the reader a snapshot of what to expect in the report.

Table of Contents

Ideally, but not necessarily, constructed using the hyperlink functions in Word. Lists of figures and tables are not required.

Main Body

1. Introduction

Reintroduce (in your words do copy from the previous assessment) any of the two network-based attacks previously discussed in Assessment 2, explaining why they were chosen and their relevance in modern cybersecurity contexts. Emphasize the importance of hands-on simulations for enhancing security understanding. Include a brief overview of the tools and technologies used during the simulation, such as Kali Linux, Ettercap, Wireshark or sqlmap.

2. Lab Environment Setup

Describe in detail how the virtual lab was prepared. Include the virtualization platform (e.g., VirtualBox, VMware), the operating systems and machines used (e.g., Kali Linux), IP addressing and networking setup, and all tools installed. Include screenshots, configurations, and diagrams to ensure that your lab setup is reproducible/understand able by others and demonstrates technical competency.

3. Attack Implementation – Attack 1

lab. List and explain the tools and commands used, include **screenshots of the attack** in

progress, and provide evidence (e.g., Wireshark captures, logs, affected service behaviour) showing the attack's success or impact. Ensure that the technical details are clearly explained for a non-specialist reader.

4. Attack Implementation – Attack 2

Repeat the same structured approach used in section 3 for the second attack. Choose a different type of threat vector (e.g., If the first was a network-based attack (e.g Arp Spoofing), this one might target a web application, database (sqlmap)). Maintain clarity in your execution steps, outputs, and supporting evidence.

5. Defence Strategy Implementation

Describe the defence strategies applied for each attack and how they were implemented in your lab. This may include configuring firewall rules, deploying IDS/IPS tools (e.g., Snort), or implementing authentication/encryption controls. Support your implementation with configuration steps, screenshots, and evidence that shows reduced attack effectiveness or complete mitigation.

6. Analysis and Evaluation

Critically analyse the effectiveness of your defensive implementations. Was each attack fully blocked, detected, or only partially mitigated? Present objective evidence (e.g., firewall logs, blocked logs, failed exploits) to support your claims. Reflect on any performance trade-offs, technical constraints, or misconfigurations encountered during testing.

Reflect on your personal experience during the assessment. Discuss the challenges you faced in setting up the lab and performing the simulations. Highlight what new skills or knowledge you acquired and how this experience has enhanced your ability to understand, detect, and respond to cybersecurity threats in real-world contexts.

8. Conclusion

Summarize the key findings and learning outcomes of the assessment. Restate the significance of simulating cyber-attacks and implementing defensive measures in a virtual lab environment. Briefly revisit the effectiveness of the chosen tools and strategies in mitigating the two selected attacks. Highlight the practical value of this exercise in bridging theoretical knowledge and real-world application, reinforcing the importance of proactive cybersecurity practices in professional environments.

9. References

These should be formatted in IEEE style. At least ***10*** recent and relevant academic resources (i.e., peer-reviewed journal articles and conference papers, books) are needed in the report.

A. B. Author, "Title of article," Journal Name, vol. 10, no. 2, pp. 123-145, Feb. 2023.

H. Zeng, Z. Ahmad, J. Zhou, Q. Wang, and Y. Wang, "DOA estimation algorithm based on adaptive filtering in spatial domain," China Commun., vol. 13, no. 12, pp. 49–58, 2016.

Assessment 3 Marking Rubric- Cybersecurity Defence: Simulating and Mitigating Real-World Attacks- 30%

Criteria	Fail (0–49%)	Pass (50–64%)	Credit (65–74%)	Distinction (75–84%)	High Distinction (85–100%)
Introduction (10%)	Unclear or missing; no justification or context.	Basic info with limited relevance and tool mention.	Reasonably clear, some relevance shown.	Clear and relevant with good context and tool use.	Excellent clarity, justification, in relevance.
Attack 1 Simulation (20%)	Poor or incomplete steps; missing evidence.	Limited explanation and screenshots.	Reasonable execution with some evidence.	Clear steps, commands and visuals provided.	Detailed, well-docum clear and supported by ev
Attack 2 Simulation (20%)	Repetitive or poorly explained; little to no differentiation.	Basic explanation, weak documentation.	Clear implementation, distinct from first attack.	Well-structured, relevant evidence provided.	Excellent technical clarity comparative insights.
Implementation (20%)	unclear defences, no evidence.	attempts, weak support.	explanation with some technical detail.	good configs/screenshots.	full supporting evidence.
Analysis & Evaluation (20%)	No evaluation or unsupported claims.	Basic analysis, limited insight.	Some reflection with partial evidence.	Good evaluation with logs/screenshots.	Critical, well-sup insightful analysis.
Conclusion, Referencing (IEEE Style), and Report Format (10%)	Missing or off-topic conclusion. No references or incorrect format. Poor formatting, structure, or hard to follow.	Weak or unclear conclusion. Few references or several formatting issues. Weak structure; lacks clarity.	Basic summary; limited connection to next assessment. Some formatting or quality issues with references. Basic adherence to format; minor issues.	Clear conclusion with reference to future work. Minor errors in IEEE format; sources are mostly relevant. Mostly clear structure and formatting; minor issues.	Strong summary with e linkage to next assessm sources are credible correctly formatted in Excellent structure, forn and professional presenta