Project: Design & Implementation of a Security Solution

Total Weight: 40% (20% Report + 20% Presentation/Demonstration)

1 Project Overview

In this project, students will design and implement a cybersecurity solution to address a real-world or industry-specific threat. The project emphasizes hands-on application of tools, critical analysis of vulnerabilities, and adherence to ethical and compliance standards.

---

2 Learning Outcomes

This project aligns with the following unit learning outcomes:

- **LO3**: Analyse a system for deploying security solutions.
- **LO4**: Design and implement a security solution under constraints.
- **LO5**: Exhibit ethical hacking methodologies.
- **LO6**: Engage critically with academic principles and integrity.

---

3 Project Components

3.1 Research & Threat Analysis

- Identify a cybersecurity threat (e.g., ransomware, phishing, IoT vulnerabilities).
- Analyse its impact on a specific industry (e.g., healthcare, finance, SMEs).
- Reference real-world incidents (e.g., Colonial Pipeline ransomware attack).

3.2 Security Solution Design

- Propose a solution using tools like Kali Linux, Snort, Wazuh, or cloud security frameworks.
- Include diagrams (e.g., network topology, encryption workflows).

3.3 Implementation & Testing

- Configure tools to mitigate the threat (e.g., firewall rules, IDS/IPS setup).
- Test the solution using simulated attacks (e.g., Metasploit, SEToolkit).

3.4 Demonstration & Ethics

- Present a live or recorded demo showing the solution in action.
- Reflect on ethical boundaries and compliance (e.g., GDPR, PCI-DSS).

---

4 Submission Requirements

4.1 Report (Max 10 Pages)

- Format: PDF or Word.
- Sections: Threat analysis, solution design, implementation steps, testing results, ethics reflection.
- Templates provided for structure guidance.

4.2 Presentation (Max 5 Slides)

- Format: PowerPoint or PDF.
- Focus: Problem, solution, demo highlights, results, and future work.

4.3 Code/Configuration Files

- Submit scripts, logs, or tool configurations (e.g., Snort rules, iptables).

---

5 Grade Milestones

Grade	Key Expectations
P (Pass)	Basic threat analysis, single-layer defence (e.g., firewall rules), minimal testing.
C (Credit)	Moderate threat analysis, multi-tool solution (e.g., Snort + Wazuh), structured testing.
D (Distinction)	Advanced threat modelling (MITRE ATT&CK), layered defence (WAF + MFA), automated testing.
HD (High Distinction)	Enterprise-grade solution (Zero Trust, SIEM), compliance alignment (NIST/ISO 27001), AI-driven automation.

---

6 Marking Rubric

Criteria	P (50-64%)	C (65-74%)	D (75-84%)	HD (85-100%)
Research Depth	Basic threat description.	Industry examples.	MITRE ATT&CK mapping.	Compliance frameworks.
Technical Execution	1 tool configured.	2+ tools integrated.	Automated workflows.	AI/ML integration.
Real-World Impact	Minimal testing.	Logs/evidence.	Metrics (e.g., 50% risk reduction).	Enterprise scalability.
Ethics & Reflection	Simple reflection.	Compliance mention	GDPR/PCI-DSS alignment.	Audit-ready reporting.

7 Templates Provided

7.1 Project Report Template (Max 10 Pages)

Title Page

- Unit Code & Name (NIT2102 Cyber Security Essentials)
- Project Title
- Student Name & ID
- Submission Date

7.1.1 Executive Summary (0.5 pages)

- Brief overview of the problem, solution, and key outcomes.
- **HD Tip**: Link to industry frameworks (e.g., NIST, ISO 27001).

7.1.2 Threat Analysis & Research (2 pages)

- **Problem Statement**: Industry context and identified threat.
- **Threat Impact**: Real-world examples (e.g., ransomware in healthcare).
- **Current Security Gaps**: Why existing measures fail.
- **Grade Alignment**:
    - **P/C**: Basic/moderate threat analysis.
    - **D/HD**: APTs, MITRE ATT&CK mapping, compliance gaps.

7.1.3 Security Solution Design (2 pages)

- **Proposed Solution**: Tools, technologies, and workflows.
- **Architecture Diagram**: Network topology, encryption flow, etc.
- **Grade Alignment**:
    - **P/C**: Single-layer defense (firewall rules).
    - **D/HD**: Multi-layered defense (Zero Trust, SIEM).

7.1.4 Implementation & Testing (3 pages)

- **Tools Used**: Kali Linux, Snort, Wazuh, etc.
- **Configuration Steps**: Code snippets, screenshots, logs.
- **Testing Methodology**: Simulated attacks (e.g., DoS, phishing).
- **Grade Alignment**:
    - **P/C**: Basic tool setup.
    - **D/HD**: Automated threat response, AI integration.

7.1.5 Ethical & Legal Considerations (1 page)

- **Ethical Reflection**: Penetration testing boundaries.
- **Compliance**: GDPR, PCI-DSS, or industry-specific standards.

7.1.6 Results & Future Improvements (1 page)

- **Effectiveness Metrics**: Reduced vulnerabilities, attack detection rate.
- **Limitations**: Scope constraints.
- **Recommendations**: Scalability, AI enhancements.

7.1.7 References (0.5 pages)

- Academic papers, industry reports, tools documentation.

7.2 Presentation Template (Max 5 Slides)

Slide 1: Problem & Industry Relevance

- **Title + Hook**: "Securing Healthcare IoT: A Zero Trust Approach."
- **Threat Impact**: Statistics (e.g., "70% of ransomware targets SMEs").
- **Visual**: Graph of attack trends.

Slide 2: Solution Design

- **Architecture**: Diagram of security layers (e.g., firewall + MFA).
- **Tools**: Icons/logos of tools used (Snort, Metasploit, AWS).
- **HD Tip**: Overlay with compliance badges (ISO 27001, NIST).

Slide 3: Implementation Highlights

- **Key Steps**: 3-4 bullet points (e.g., "Configured Snort IDS rules").
- **Screenshot**: Kali Linux terminal with attack simulation.
- **Grade Alignment**:
  - **P/C**: Basic setup.
  - **D/HD**: Live demo snippet or video.

Slide 4: Results & Metrics

- **Before/After**: Vulnerability scan comparisons.
- **Ethics**: Compliance alignment (e.g., "GDPR-ready access controls").
- **Visual**: Bar chart showing reduced attack surface.

Slide 5: Reflection & Q&A

- **Lessons Learned**: "Automation reduced response time by 40%."
- **Future Work**: "Integrate AI-driven threat hunting."
- **Closing**: Thank you + Contact info.

---

8 Alignment with Marking Criteria

Rubric Component	Report Section	Presentation Slide
Research Depth	Threat Analysis (p. 2-3)	Slide 1
Technical Execution	Implementation (p. 4-6)	Slide 2
Real-World Impact	Results (p. 7)	Slide 3
Ethics & Compliance	Ethical Considerations (p. 5)	Slide 4
Innovation (HD)	Future Improvements (p. 7)	Slide 5

---

9 Style Guidelines

- **Report**: Use headings, bullet points, and diagrams. Avoid walls of text.
- **Presentation**: Use <100 words per slide; prioritize visuals (diagrams, logs, screenshots).
- **HD Differentiation**: Include compliance frameworks, attack simulations, and metrics.