**ASSESSMENT BRIEF**

**L7 Network and Penetration Testing**

**Module Leader:** Kayode Adenuga

**Key Details and Requirements**

**Submission deadline:** 23 September 2025, no later than 16:30 (UK local time)

# **Learning Outcomes:**

1. Critical understanding of scope of network computing and their security challenges.
2. Ability to critically evaluate and manage networked environments including use of modern methods for application storage, processing and deployment.
3. Ability to recommend improvements and manage implementation of networking environments.
4. Ability to effectively assess and recommend actions to secure business continuity of cloud applications.

**Assessment details:** Individual Portfolio (tasks and activities accumulated over the semester), 100% (equivalent to 2,500 words)

**Referencing:** Students are expected to use Harvard Referencing throughout theirassignments where required. Please follow the [Harvard Referencing Handbook](https://law-uk.libguides.com/referencing) for all your assignments at the ULBS.

**Submission Method: Turnitin -** Your work will be put through Turnitin. All submissions will be electronically checked for plagiarism. You have the option to upload your work ahead of the deadline, more than once. ULBS will be reviewing your last submission only. You can only upload one file. For example if your work contains a word document and power point slides/Excel spreadsheet you will need to copy your slides/spreadsheet into the word document.

**Note:** Keep in mind that self-plagiarism (when you reuse your own specific wording and ideas from work that you have previously submitted without referencing yourself) is also a form of plagiarism and is not allowed.

**ASSIGNMENT DETAILS**

**This activity aims to assess your comprehension of the diverse concepts discussed in this module. You must use the frameworks and concepts covered in this module's delivery to respond to all the tasks below.**

**Scenario**

Synergic Solutions Ltd. is a growing software company with offices across three different cities. The company relies heavily on networked services and cloud-based applications to deliver its software products and services to clients worldwide. Recently, it has experienced a series of growing security incidents, including unauthorized access attempts, service interruptions, and suspicious outbound traffic.

Furthermore, staff have reported vulnerabilities such as cable tapping or physical eavesdropping, switch flooding, IP spoofing, port scanning, exploitation of open ports, token/session ID theft, SSL/TLS exploitation, malicious file uploads, and others that can be exploited by the threat actors.

The IT leadership has commissioned a comprehensive evaluation and improvement plan for their networked environment, which includes on-premise systems, inter-office networking, and cloud application infrastructure.

As a network security consultant, you have been engaged to achieve the following:

* Conduct a comprehensive vulnerability assessment using industry-recognized tools.
* Plan and execute a structured penetration testing process aligned with established standards.
* Deliver critical, evidence-based recommendations for improving Synergic Solutions Ltd. network security.

Your assessment should cover all phases of penetration testing—from reconnaissance to reporting—ensuring a thorough evaluation of the organisation's security posture.

**Task 1(LO1): Critical understanding of scope of network computing and their security challenges.**

1. Analyse the key current and emerging security challenges faced by Synergic Solutions Ltd. and evaluate their potential impact on the organization.
2. Critically assess the significance and application of network penetration testing within the operational framework of Synergic Solutions Ltd.

**Task 2 (LO1, LO2): Ability to critically evaluate and manage networked environments including use of modern methods for application storage, processing and deployment.**

1. Design a structured penetration testing plan that incorporates recognized testing standards and clearly defines each phase of the testing process.
2. Identify potential vulnerabilities affecting Synergic Solutions Ltd. and design a simulated penetration test targeting its network infrastructure, utilizing network and penetration testing methodologies based on the Cisco Ethical Hacking course.

**Task 3 (LO1, LO2, LO3): Ability to recommend improvements and manage implementation of networking environments.**

1. Design a network hardening plan for Synergic Solutions Ltd. following the discovery of key vulnerabilities through penetration testing done in Task 2b.
2. What steps would you take to implement your proposed changes, and how would you ensure minimal disruption to business operations?

**Task 4 (LO1, LO2, LO3, LO4): Ability to effectively assess and recommend actions to secure business continuity of cloud applications.**

1. Evaluate the current security posture of Synergic Solutions Ltd.’s cloud-based applications, identifying key risks and strengths, and recommend measures to ensure business continuity and operational resilience.
2. Critically examine the ethical considerations associated with conducting penetration testing and managing sensitive data within a professional networking context.

**Summary Report**

Once you have completed individual tasks, you should write a summary report (maximum approx. 800 words) that covers the entire task. This summary report serves as a platform for you to articulate and describe the key lessons derived from each task. It is an opportunity to synthesize insights, providing an overview of the knowledge and understanding acquired throughout completion of the assigned tasks.

**Portfolio instructions:**

For the assessment of this portfolio, students are required to generate a report using PebblePad.

• Use font size 11 and single spacing for all articles in the portfolio.  
• Proper citations are essential.

All tasks require the citation of academic and other sources, which should be listed in Harvard referencing style, along with a reference list presented at the end of the portfolio. Whenever you use external sources such as pictures, definitions, or lines of argumentation, clearly state the source at the end of the sentence or paragraph and provide a reference to the original article using the Harvard referencing style.

**Please refer to the marking criteria (below) for a breakdown of how this assignment will be marked.**

| **GRADE DESCRIPTORS**  **MARKING CRITERIA** | **Mark Weight** | **FAIL**  **(0 - 49%)** | **PASS**  **(50 – 59%)** | **COMMENDATION**  **(60 – 69%)** | **DISTINCTION**  **(70-100%)** |
| --- | --- | --- | --- | --- | --- |
| Exhibits an unsatisfactory grasp of the issues. Primarily descriptive and lacking in independent critical thought. Weak or no attempt at analysis, synthesis, and critical reflection. Little evidence of ability to tackle the issues. Poor structure/grammar/ | Satisfactory grasp of the issues, with limited independent critical thought appropriate to the tasks. Material is largely relevant to the tasks. Some evidence of analysis, synthesis, and critical reflection. Work is presented in acceptable manner, with some minor errors. | Good/very good understanding of the issue with some independent critical thought and approach to the tasks. Good attempt at analysis, synthesis, and critical reflection, with evidence of some ability to tackle issues. Work is clearly presented in a well organised manner. | Excellent level of understanding.  All requirements are dealt with to a high standard. Excellent analysis, synthesis, and critical reflection. Evidence of independent and original judgement in relation to resolution of problems Excellently presented. |
| **Knowledge and understanding:** Demonstrate critical analysis and reflection, applying knowledge and understanding of the extent of the issue highlighted across all tasks. | 10 |  |  |  |  |
| **Task 1 (LO1):** Demonstrate an understanding of networking concepts and their security challenges through a thorough analysis supported by relevant literature supported by appropriate literature. | 15 |  |  |  |  |
| **Task 2 (LO2):** Conduct a thorough analysis and critically evaluate networked environments using network and penetration testing for application storage, processing, and deployment supported by appropriate literature. | 30 |  |  |  |  |
| **Task 3 (LO3):** Analyse networked environments based on penetration testing conducted in Task 2, and recommend improvements to manage and secure application storage, processing, and deployment supported by appropriate literature. | 15 |  |  |  |  |
| **Task 4 (LO4):** Assess networked environments with ethical considerations in penetration testing, implement improvements, and ensure business continuity in the cloud supported by appropriate literature. | 20 |  |  |  |  |
| Summary / Conclusions: The report demonstrates excellent cohesiveness and logical conclusion, effectively supported by Harvard referencing and citations. | 10 |  |  |  |  |