Faculty of Science and Engineering

Referred Coursework – 2024/2025 Academic Year

PLEASE NOTE: If you have been referred in the COURSEWORK element of this module and are required to be reassessed by COURSEWORK, please complete this referred work.

Module Code:	COMP1002
Module Title:	Cyber Security & Networks
Module Leader:	Dr Hai-Van Dang
School:	Engineering, Computing and Mathematics

DEADLINE FOR SUBMISSION: Thursday 7th August 2025 at 3pm

SUBMISSION INSTRUCTIONS FOR CANDIDATES
Referred coursework must be submitted electronically using the online submission facility in the DLE by the deadline above. When you submit your assessment, you are stating that it is your own work. Please ensure you are familiar with the relevant referencing guidelines and our procedures by familiarising yourself with the **Assessment Offences and Research Misconduct Procedure.** This procedure can be found in the Academic Regulations. If you have any queries on submission or in relation to the referred work, please contact the Module Leader in the first instance, if they are unavailable, please contact the Faculty Office on 01752 584584 immediately so any problems can be rectified. **PLEASE NOTE that we cannot accept work submitted via email.**

Faculty of Science and Engineering
T: +44 (0)1752 584584
E: science.engineering@plymouth.ac.uk

Instructions to Candidates

This is an individual piece of work.

Assessment Criteria:

The report **MUST** be structured as specified in the **Table 1 (see page 5)**. Please be very careful and pay close attention to these instructions.

Format your report as follows: Use Arial as the font, with a minimum size of 11pts, all margins should be at least 2cm. **The maximum page limit is 7 pages (excluding the list of references and the addressing table).** Please note that anything exceeding the maximum number of pages will not be assessed by the markers. References should be cited as proofs to your statements where relevant. Please submit the reports as a single PDF on the DLE.

A Rubric will be used to assess and provide feedback on the submissions. The template for this can be found on **Table 2**: Feedback Template for Assessment **(see page 6).**

MODULE AIMS

- To familiarise students with fundamentals of information security and networking.
- To develop an understanding of security threats, vulnerabilities, and countermeasures.
- To understand common network protocols and design common network infrastructures.

ASSESSED LEARNING OUTCOMES (ALO):

1. Describe the types of risk that may threaten an IT system and available countermeasures.
2. Explain the conceptual underpinnings of computer networking and data representation.
3. Explain the nature and role of networking and security protocols/controls and how they combine to provide system-level objectives.

The referred assessment in this module is focused upon answering the following questions.

1. Cyber Security – NHS is seeking to improve their patient data management system and internal networking infrastructure. Recently, The Times Health Commission has published ten recommendations to address the areas the NHS is struggling with. One of them is to create digital health accounts for patients, called **patient passports**, accessed through the NHS app to book appointments, order prescriptions, view records, test results or referral letters and contact clinicians. It would track a patient's records for life, allowing any GP, NHS hospital, pharmacy or social care agency to access information. You are to provide a brief report to

   (a) analyse the security of the system and identify the security requirements using the Parkerian Hexad. There must be **at least one security requirement** per each element of the Parkerian Hexad.

   (b) propose **one solution** for each element in the Parkerian Hexad.

2. Networking – A boat builder company has grown rapidly over the past year, increasing its workforce from 60 to 120 employees. The company is seeking to redesign its network to support the increase in staff and to segregate the network traffic of its Production (**80 users**), Marketing (**10 users**), Management (**10 users**) and Development (**20 users**) departments. The existing network comprises a single router connected to a non-managed switch where all users are directly connected to it.

   (a) Your work is to design a new scalable and low-cost network architecture with:

      i) a scalable IP addressing (choose private **192.168.64.0/20** or/and public addresses **209.220.160.0/30** as needed) scheme with subnetting to support different departments.

      ii) VLAN implementation for segregating network traffic between the Production, Marketing, Management and Development departments

      iii) Internet connection is available to all users.

   (b) By connecting to this network infrastructure, an employee accesses France 24 website (https://www.france24.com/) in their browser (e.g. Google Chrome) to view news. Consider the link, network, transport and application layers required for a web page to be displayed on the browser and explain the network activities (in terms of relevant network protocols) taking place in each layer.

Relevant supporting information may be included as appendices if required. Your report must be supported by references/citations where appropriate. Please refer to the end of this assessment pack for information and links to resources on referencing. The use of Tables and Figures are a useful approach of conveying complex information in an efficient manner.

<table>
<tr><th>Content</th><th>Details</th><th>Marks</th></tr>
<tr><td>Section 1 – Question 1a and 1b</td><td>1a) The focus of question 1a should be on analysing the security of the system to identify its security requirements using the Parkerian Hexad. For instance, for confidentiality element in the Parkerian Hexad, what data needs to be protected and when does it need to be protected (in transit or at rest)? Why does it need to be protected? What are the possible threats/ risks/ attacks/ consequences against its confidentiality?

There must be at least one security requirement per each element of the Parkerian Hexad (e.g. confidentiality, possession/ control, integrity, authenticity, availability, utility)

Please provide a clear rationale for your analysis and provide details to support your statements.

1b) For each element in the Parkerian hexad (e.g. confidentiality, possession/ control, integrity, authenticity, availability, utility), propose one solution. Describing the solutions in detail. The answer should provide enough details to understand the selected security mechanisms/components, and what security requirements each mechanism/component provides.

Citation: References should be cited in support of your statements, and the writing should be concise and easy to follow</td><td>50</td></tr>
<tr><td>Section 2 - Question 2a and 2b</td><td>2a) The answer for the scalable and low-cost network architecture design should be clear and correct and should provide enough details about how the IP addressing, subnetting and VLAN are considered in the network architecture design. Describing the addressing table using the provided template, listing the basic information for each network (network address, netmask, number of hosts, first host, last host). Use the following addressing table template.

<table>
<tr><td>Network name</td><td>Network Address</td><td>Netmask</td><td>Usable range: first address to last address</td><td>Broadcast address</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

2b) For the network protocol analysis, the answer should provide enough details about the working mechanism of the link, network, transport and application layer to support web application.

Citation: References should be cited in support of your statements, and the writing should be concise and easy to follow.</td><td>50</td></tr>
</table>

Table 1

Criteria	Fail (<40%)	3rd/Pass (40%+)	2.2 (50%)	2.1 (60%+)	1st (70%+)	Grade
Section 1 – Question 1a and 1b	Inadequate security requirements have been identified. Few if any relevant explanation. Inappropriate solutions have been identified Few if any relevant references.	Some security requirements have been identified with some explanation Some proposed security solutions with some explanation Few evidence of appropriate references.	Appropriate security requirements have been identified with some explanation Appropriate security solutions have been identified with some explanation Some evidence of appropriate references.	Appropriate security requirements have been identified with good explanation Appropriate security solutions have been identified with good explanation Good use of a number of relevant sources in an appropriate manner.	An excellent list of security requirements has been identified with excellent explanation Appropriate security solutions have been identified with excellent explanation An excellent set of appropriate peer-reviewed references.	**50**
Section 2 – Question 2a and 2b	Little or no analysis of network architecture and network protocols. Minimum of results, and results are largely incorrect. Little understanding of the subject. Almost no evidence of investigation, evaluation and research on answering the questions.	Brief discussion and little analysis/investigation of network architecture and network protocols. Results are partially correct and/or complete. Little evidence of investigation, evaluation and research on answering the questions.	The majority of the results are correct and complete. Answers are given at an appropriate level of detail and are explained clearly. Some evidence of investigation, evaluation and research on answering the questions.	A significant majority of the results are correct and complete. Answers are given in great details and are well explained. Clear and concise description of how results are obtained. Good evidence of investigation, evaluation and research on answering the questions.	The results are correct and complete. Especially clear, ambitious and well-justified analysis and description. Demonstrating ideas for original thoughts and stretched work. There is strong evidence of investigation, evaluation and research on answering the questions (e.g. deep analysis, full investigation and good summary of the investigation).	**/50**
Feedback/ Overall	*Additional feedback*					**/100**

Table 2: Feedback Template for Assessment

General Guidance

Responsible use of Artificial Intelligence (AI) in assessments

Please refer to.

https://dle.plymouth.ac.uk/pluginfile.php/3558454/mod_resource/content/0/FoSE%20AI%20statement%2024-25.pdf for guidelines about what you can use AI and what you cannot use AI for when writing or submitting assessment.

Extenuating Circumstances

There may be a time during this module where you experience a serious situation which has a significant impact on your ability to complete the assessments. The definition of these can be found in the University Policy on Extenuating Circumstances here: https://www.plymouth.ac.uk/student-life/your-studies/essential-information/exams/exam-rules-and-regulations/extenuating-circumstances

Plagiarism

All of your work must be of your own words. You must use references for your sources; however, you acquire them. Where you wish to use quotations, these must be a very minor part of your overall work.
To copy another person's work is viewed as plagiarism and is not allowed. Any issues of plagiarism and any form of academic dishonesty are treated very seriously. All your work must be your own and other sources must be identified as being theirs, not yours. The copying of another persons' work could result in a penalty being invoked.
Further information on plagiarism policy can be found here:

Plagiarism: https://www.plymouth.ac.uk/student-life/your-studies/essential-information/regulations/plagiarism

Examination Offences: https://www.plymouth.ac.uk/student-life/your-studies/essential-information/exams/exam-rules-and-regulations/examination-offences

Turnitin (http://www.turnitinuk.com/) is an Internet-based 'originality checking tool' which allows documents to be compared with content on the Internet, in journals and in an archive of previously submitted works. It can help to detect unintentional or deliberate plagiarism.

It is a formative tool that makes it easy for students to review their citations and referencing as an aid to learning good academic practice. Turnitin produces an 'originality report' to help guide you. To learn more about Turnitin go to: https://guides.turnitin.com/hc/en-us/categories/21850416398221-Student-hub

Referencing

The University of Plymouth Library has produced an online support referencing guide which is available here: http://plymouth.libguides.com/referencing.

Another recommended referencing resource is Cite Them Right Online; this is an online resource which provides you with specific guidance about how to reference lots of different types of materials.