MODULE NAME:	MODULE CODE:
PRINCIPLES OF SECURITY	PRSE6212/d

ASSESSMENT TYPE:	**TAKE-HOME EXAM (PAPER ONLY)**
TOTAL MARK ALLOCATION:	**120 MARKS**
TOTAL TIME:	**21 Hours (midnight to 9 PM on the same day)**

By submitting this assessment, you acknowledge that you have read and understood all the rules as per the terms in the registration contract, in particular the assignment and assessment rules in The IIE Assessment Strategy and Policy (IIE009), the intellectual integrity and plagiarism rules in the Intellectual Integrity and Property Rights Policy (IIE023), as well as any rules and regulations published in the student portal.

INSTRUCTIONS:

1. *Please **adhere to all instructions**. These instructions are different from what is normally present, so take time to go through these carefully.*
2. ***Independent work is required**. Students are not allowed to work together on this assessment. Any contraventions of this will be handled as per disciplinary procedures in The IIE policy.*
3. ***No material may be copied from original sources, even if referenced correctly, unless it is a direct quote indicated with quotation marks.***
4. *All work must be adequately and correctly referenced.*
5. *You should paraphrase (use your own words) the concepts that you are referencing, rather than quoting directly.*
6. *This is an open-book assessment.*
7. *Assessments must be typed unless otherwise specified.*
8. ***Ensure that you save a copy of your responses.***
   - 8.1. *Complete your responses in a Word document.*
   - 8.2. *The document name must be your **name.student number.Module Code**.*
   - 8.3. *Once you have completed the assessment, upload your document under the **submission link** in the correct module in Learn.*

Additional instructions:

- *Calculators are allowed.*
- *Answer all questions.*
- *Show all calculations, where applicable (marks may be awarded for this).*

Referencing Rubric

Providing evidence based on valid and referenced academic sources is a fundamental educational principle and the cornerstone of high-quality academic work. Hence, The IIE considers it essential to develop the referencing skills of our students in our commitment to achieve high academic standards. Part of achieving these high standards is referencing in a way that is consistent, technically correct and congruent. This is not plagiarism, which is handled differently.

Poor quality formatting in your referencing will result in a penalty **of** according to the following guidelines **a maximum of ten percent being deducted from the overall percentage**. Please note, however, that **evidence of plagiarism in the form of copied or uncited work (not referenced), absent reference lists, or exceptionally poor referencing, may result in action being taken in accordance with The IIE's Intellectual Integrity Policy (0023)**.

Markers are required to provide feedback to students by indicating **(circling/underlining) the information that best describes the student's work.**

Minor technical referencing errors: 5% deduction from the overall percentage. – the student's work contains **five or more errors** listed in the minor errors column in the table below.

Major technical referencing errors: 10% deduction from the overall percentage. – the student's work contains **five or more errors** listed in the major errors column in the table below**.**

If both minor and major errors are indicated, **then 10% only** (and not 5% or 15%) is deducted from the overall percentage. The examples provided below are not exhaustive but are provided to illustrate the error.

Required: Technically correct referencing style	Minor errors in technical correctness of referencing style Deduct 5% from overall percentage. Example: if the response receives 70%, deduct 5%. The final mark is 65%.	Major errors in technical correctness of referencing style Deduct 10% from the overall percentage. Example: if the response receives 70%, deduct 10%. The final mark is 60%.
Consistency • The same referencing format has been used for all in-text references and in the bibliography/reference list.	Minor inconsistencies. • The referencing style is generally consistent, but there are one or two changes in the format of in-text referencing and/or in the bibliography. • For example, page numbers for direct quotes (in-text) have been provided for one source, but not in another instance. Two book chapters (bibliography) have been referenced in the bibliography in two different formats.	Major inconsistencies. • Poor and inconsistent referencing style used in-text and/or in the bibliography/ reference list. • Multiple formats for the same type of referencing have been used. • For example, the format for direct quotes (in-text) and/or book chapters (bibliography/ reference list) is different across multiple instances.
Technical correctness • Referencing format is technically correct throughout the submission. • The correct referencing format for the discipline has been used, i.e., either APA, OR Harvard OR Law • Position of the reference: a reference is directly associated with every concept or idea. • For example, quotation marks, page numbers, years, etc. are applied correctly, sources in the bibliography/reference list are correctly presented.	Generally, technically correct with some minor errors. • The correct referencing format has been consistently used, but there are one or two errors. • Concepts and ideas are typically referenced, but a reference is missing from one small section of the work. • Position of the references: references are only given at the beginning or end of every paragraph. • For example, the student has incorrectly presented direct quotes (in-text) and/or book chapters (bibliography/reference list).	Technically incorrect. • The referencing format is incorrect. • Concepts and ideas are typically referenced, but a reference is missing from small sections of the work. • Position of the references: references are only given at the beginning or end of large sections of work. • For example, incorrect author information is provided, no year of publication is provided, quotation marks and/or page numbers for direct quotes missing, page numbers are provided for paraphrased material, the incorrect punctuation is used (in-text); the bibliography/reference list is not in alphabetical order, the incorrect format for a book chapter/journal article is used, information is missing e.g. no place of publication had been provided (bibliography); repeated sources on the reference list.
Congruence between in-text referencing and bibliography/ reference list • All sources are accurately reflected and are all accurately included in the bibliography/ reference list.	Generally, congruence between the in-text referencing and the bibliography/ reference list with one or two errors. • There is largely a match between the sources presented in-text and the bibliography. • For example, a source appears in the text, but not in the bibliography/ reference list or vice versa.	A lack of congruence between the in-text referencing and the bibliography. • No relationship/several incongruencies between the in-text referencing and the bibliography/reference list. • For example, sources are included in-text, but not in the bibliography and vice versa, a link, rather than the actual reference is provided in the bibliography.
In summary: the recording of references is accurate and complete.	In summary, at least 80% of the sources are correctly reflected and included in a reference list.	In summary, at least 60% of the sources are incorrectly reflected and/or not included in reference list.

Overall Feedback about the consistency, technical correctness and congruence between in-text referencing and bibliography:

Question 1		**(Marks: 20)**
Q.1.1	Without providing a description, definition, or explanation of the term, explain one example of different categories of threat actors below. In your answer, give an appropriate example and then explain how the example relates to the category. Categories: A. State actors. B. Competitors. C. Cyberterrorists.	(9)
Q.1.2	Describe one example of each of the following cybersecurity vulnerabilities: A. Platforms vulnerabilities. B. Configurations vulnerabilities. C. Zero-day vulnerabilities.	(3)
Q.1.3	Using suitable examples, differentiate between the **snoop** and **evade** actions of malware. Your answer must give the types of malware as examples and use the examples to show the difference between the two actions.	(8)

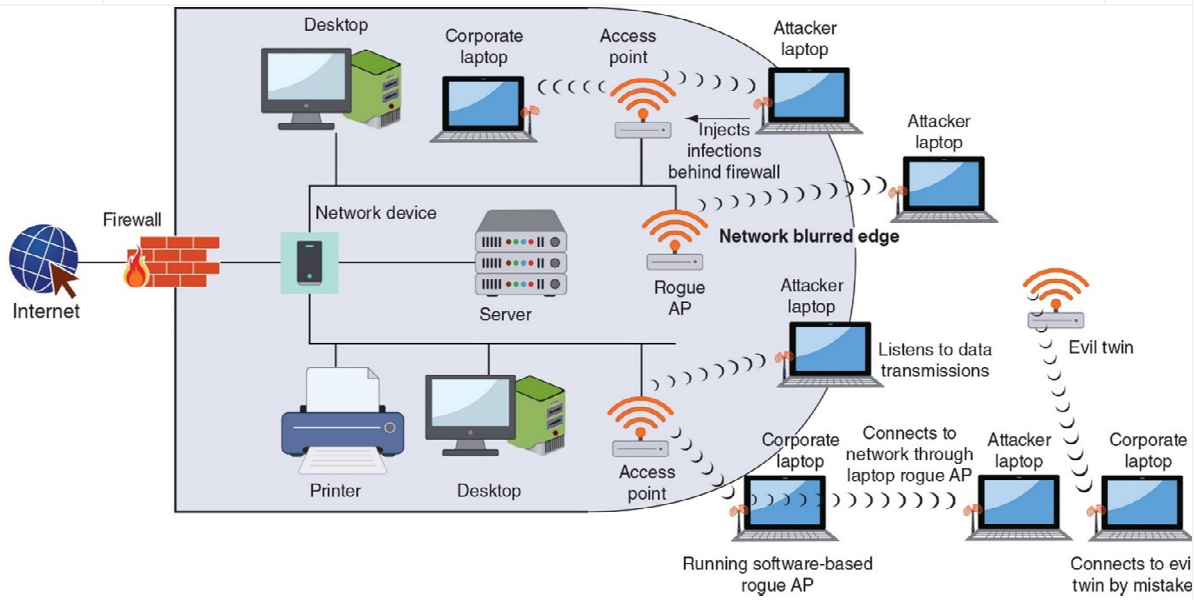
Question 2		**(Marks: 20)**
Q.2.1	Using suitable examples, differentiate between the **Domain Name System (DNS)** and **Interception** network attacks. Your answer must give types of network attacks as examples and use the examples to show the difference.	(8)
Q.2.2	State the main use of each of the access technologies below. In your answer, give one example to explain how each access technology can be used to secure a student record system in a tertiary college.	(6)
	Access technologies: A. Access Control List (ACL). B. Network Access Control (NAC). C. Data Loss Prevention (DPL).	
Q.2.3	Discuss the importance of configuration management in the context of security. In your answer, give examples of tools that can be used in configuration management.	(6)

Question 3 **(Marks: 20)**

Q.3.1	Using detailed examples, discuss the differences between **symmetric** and **asymmetric** encryption. Your discussion must include the uses of keys and state with a motivation, which encryption method can provide increased security and protection.	(10)
Q.3.2	Using an example in the business or finance industry, describe how the following cryptographic protocols work: A. Secure sockets layer (SSL). B. Hypertext transport protocol secure (HTTPS). C. Secure shell (SSH). D. Secure real-time transport protocol (SRTP). E. IP Security (IPsec).	(10)

Question 4 **(Marks: 30)**

Q.4.1	Study the diagram regarding the Enterprise WLAN below and then answer the question that follows:	(15)
	Diagram:	



	Using the diagram, explain how a **network blurred edge** is a cause of concern for the Enterprise. In your answer, use suitable examples to describe how **a Rogue Access Point** and an **Evil Twin** can be used in a WLAN enterprise attack. In addition, describe how the **configurations** for wireless protections below can be used to strengthen the security of the WLAN: A. Signal strength settings. B. Spectrum selection. C. Antenna placement and type.	
Q.4.2	Over several years, many industry-led initiatives have attempted to address security vulnerabilities on the Internet of Things (IoT) and embedded devices. However, the initiatives did not represent a comprehensive solution to the problem. Discuss using any suitable examples, how governments and other security organisations can work towards resolving the problem.	(10)

Q.4.3	As the cost of consumer wireless routers has fallen, the problem of rouge APs has risen. Substantiate the statement above with one example. In your answer, also briefly describe what the **Rogue Access Point Detection** involves using the same example.	(5)

Question 5 **(Marks: 30)**

Q.5.1 Using any type of security attack scenario, describe the purpose of each of the control types used in risk management below. In your answer, provide a suitable example for each type. (15)

NB: A scenario must be provided in your answer as well as each example of the control types. Examples taken or copied from the prescribed textbook will be awarded zero or no marks.

Control type	Description	Example
A. Deterrent control		
B. Preventive control		
C. Physical control		
D. Detective control		
E. Corrective control.		
F. Compensation control		

Q.5.2 Compare **vulnerability scan** to **penetration test** using example under the following headings: (10)

A. Procedure.

B. Process.

C. Goal.

D. Frequency.

E. Personnel.

Q.5.3 Provide one example that shows the importance of each of the following acronyms/ concepts when reducing risk and verifying compliance and performance in any agreement: (5)

A. SLA.

B. BPA.

C. MOU.

D. NDA.

E. EOL.

END OF PAPER