University of Westminster
School of Computer Science and Engineering

6COSC019C Cyber Security
Assignment Specification (2023/24)

Module leader	Saman Hettiarachchi
Unit	Coursework
Weighting:	50%
Qualifying mark	30%
Description	Scenario-based lab report: Answers are based on weekly lab activities
Learning Outcomes Covered in this Assignment:	LO3 Evaluate security architecture and design and provide the means to enhance operation security. LO4 Examine cryptography protocols and vulnerabilities and identify attack vectors to exploit them. LO5 Synthesise emerging trends through engagement and analysis with current research.
Handed Out:	Thursday 22 February 2024
Due Date	Tuesday 07 May 2024 at 01:00 pm
Expected deliverables	Single Report
Method of Submission:	Electronic submission on TurnitIn (in PDF format); name your file with your student number and the module code. i.e.: WXXXXXXX_6COSC019W
Type of Feedback and Due Date:	Written feedback and marks will be given 15 working day (3 Weeks) after the submission deadline. **All marks will remain provisional until formally agreed by an Assessment Board.**

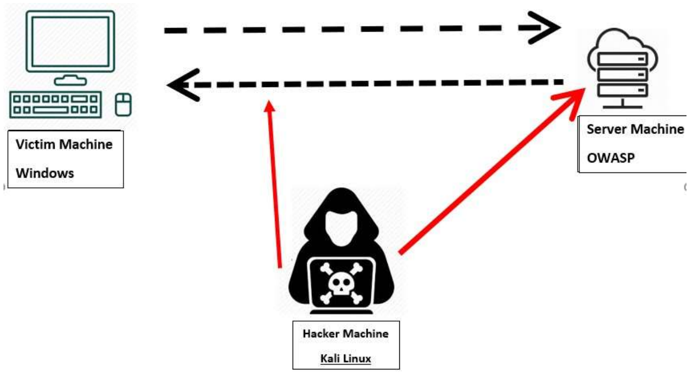
Assessment regulations

Refer to section 4 of the "Framework for undergraduate course" guide for undergraduate students for a clarification of how you are assessed, penalties and late submissions, what constitutes plagiarism etc. https://www.westminster.ac.uk/sites/default/public-files/general-documents/Section-17-Framework-forundergraduate-taught-courses-2022.pdf

Penalty for Late Submission

If you submit your coursework late but within 24 hours or one working day of the specified deadline, 10 marks will be deducted from the final mark, as a penalty for late submission, except for work which obtains a mark in the range 40 – 49%, in which case the mark will be capped at the pass mark (40%). If you submit your coursework more than 24 hours or more than one working day after the specified deadline, you will be given a mark of zero for the work in question unless a claim of Mitigating Circumstances has been submitted and accepted as valid. For more detailed information regarding University Assessment Regulations, please refer to the following website:**http://www.westminster.ac.uk/study/current-students/resources/academic-regulations**

Coursework description



Tobeabletocompleteyourassessmentusethelabexercisesandactivitiestomapto yourallocatedscenario.Youwillhavethreemachines,theVictimmachine(**Host computer**),theservermachine (**OWASPVM**) andthehackermachine (**Kali LinuxVM**).

Building your scenario [3 marks]

Each of you will need to build their own scenario for a company.

Your scenario must have the following requirements:

- Your scenario public website is https://cwscenario.site/ - **ONLY TO CONDUCT OSINT activities.**
- A database and web services
- Users

Your should define the following assumptions for your scenario:

1. **Type and size of business:**
   - it could be any type of business as long as you define it.
   - This is important as it will also define the type of users and data for your information system environment.
   - For example: A school, an estate agent, an engineering company, etc..
   - The size of the organisation is important as it will dictate how many users there are, where do they access, etc..
   - For example a business can be a startup with 10 users working in one office, a small school with 20 teachers and 200 students or a multi national company with thousands of users.

2. **Type of data:**
    - The type of data is relevant to the business type you chose.
    - For example a school will hold information about the students. This could be financial information, personal information or marks and progress records.
    - The type of data the organisation holds will dictate the type of controls you put to protect your data.
3. **Type of users:**

- The type of users is relevant to the business type you chose.
- For example a school can have teachers and parents as users.
- The type of users the organisation have will dictate how complex accessing your system is.

- it could be any type of business as long as you define it.
- This is important as it will also define the type of users for your information system environment.
- For example: A school, an estate agent, an engineering company, etc..

The idea for each of you to have your own scenario is because, although you are all conducting the same activities, the impact of those activities on users in an E-Commerce business, for example, is different than the impact of those activities on users in a hospital.

- In an E-Commerce business, all the CIA tenets are important; however, there is no risk of life if any gets violated at some point. For example, the confidentiality of customers' data is important and valuable. Integrity is also crucial since you want to ensure that business transactions are valid and genuine at all times. Availability is important because if users lose access for some time, they might go and conduct their E-Commerce business somewhere else, leading to a loss of business for the company.
- In a hospital, all the CIA tenets are critical! Confidentiality of patients' data, integrity of that data, and the system must be available at all times!

Below is a scenario example with all the assumptions and requirements defined.

> My company was hired to conduct a penetration test for a **medium sized estate agent company** with **many branches** across the UK. Their web application allows their potential customers to search for properties and book appointments. The website does not hold any financial data for the properties owners but stores **personal information** for **potential customers** who are interested in a property. **Staff** can access the web application to **manage properties on the web application**. Staff receive potential customers enquiries by email. **Staff credentials** are stored on the database.

You must not use the same example for your assignment.

Requirements and Deliverables

You have completed your penetration testing assessment on the scenario application and identified their vulnerabilities and weaknesses.

You are now expected to document your findings in a penetration testing report.

Your report should contain all the information below that are required by the company that hired you.

You should assume that the person reading the document does not have a technical background

You should show that you were able to identify or exploit vulnerabilities and explain them.

You should explain the impact of those vulnerabilities and exploits on the system.

Report requirements for your client

A- **Information Gathering**

(1) **OSINT Activities**

Show two examples of your Open-Source Intelligence (OSINT) investigation activities you have carried out on your scenario example. [3 marks]

Research and evaluate how OSINT can be effective and explain why it is one of the first activities that penetration testers carry out. [3 marks]

Scenario assessment: In your opinion, how dangerous are the information you were able to obtain for your allocated scenario [2 marks]

(2) **Website Reconnaissance**

Show some of the information you were able to obtain simply by browsing the applications in the lab and observing and analysing code and transactions. [3 marks]

Scenario Assessment: Explain how the information obtained by observing and analysing the web applications can be used at a later stage to exploit the company's web services. Provide an example of information that can be relevant to your scenario. [2 marks]

(3) **Port Scanning and Enumeration**

Show that you have identified the ports you found in the lab running on the server machine. [3 marks]

Research and explain what an open port means and identify threats an open port can potentially causes? [3 marks]

Scenario assessment: Explain the threats of the open ports you have identified when carrying the port scanning and how dangerous they are for your scenario and the data your scenario company holds. [3 marks]

B- **Server side exploits**

(1) **Data tampering**

Identify if the application is vulnerable to data tampering and exploit it if possible. [3 marks]

Briefly research and explain data tampering vulnerability. Which Cyber Security tenet this vulnerability violates? [2 marks].

Scenario assessment: What is the vulnerable information for data tampering that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [2 marks]

(2) **SQL injection**

Identify if the application is vulnerable to SQL injection and exploit it if possible. [3 marks]

Briefly research and explain SQL injection vulnerability. Which Cyber Security tenet this vulnerability violates? [3 marks].

Scenario assessment: What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [2 marks]

(3) **XSS Scripting**

Identify if the application is vulnerable to XSS vulnerability and exploit it if possible. [3 marks]

Briefly explain XSS scripting vulnerability. Which Cyber Security Tenet this vulnerability violates? [2 marks].

Scenario assessment: What are the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [2 marks]

(4) **Other vulnerabilities**

OWASP vulnerable machine contains several other vulnerabilities that can be exploited. Identify two other vulnerabilities you were able to identify in the vulnerable machine. [2 marks]

Scenario assessment: Research and investigate their threats for your scenario and identify which Cyber Security tenet these vulnerabilities violate? [2 marks]

(5) Cryptanalysis attack

Show how you can conduct cryptanalysis on your scenario environment. [2 marks]

Scenario assessment: What is the impact of cryptanalysis impact on your scenario if successful? [2 marks]

C- **Client side exploits**

(1) Man in the Middle Attack (MiTM)

Show how the attacker can capture traffic from a session between a genuine user and the server side of the application. [3 marks]

Scenario assessment: What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [3 marks]

(2) Social engineering attack

Show how an attacker can lure a normal user of the server to your computer instead of the server machine. [3 marks]

Scenario assessment: What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [3 marks]

D- **Denial of Service attacks**

(1) DoS the web server

Show how an attacker can carry on a denial of service attack on the web server. [2 marks]

Which Cyber Security Tenet this vulnerability violates? [1 mark]

Scenario assessment: What is the impact of this attack on your scenario company? [2 marks]

E- **Threats mitigation techniques & recommendations**

(1) Briefly research what you can do to minimise the threats to the findings in the reconnaissance phase when you tested the web application in section A.2. [2 marks]

(2) Briefly research how to prevent your company's servers from revealing too much information when an attacker conducts scanning and enumeration, similar to the activities in section A.3. [2 marks]

(3) Briefly research and explain how to protect your database against SQL injection exploited in section B.2. [3 marks]

(4) Briefly research and explain how to protect your web application against cross site Scripting attacks exploited in section B.3. [3 marks]

(5) Briefly research and explain how to protect your web application against cryptanalysis attacks exploited in section B.5. [3 marks]

(6) Investigate what activities a security analyst can carry out to protect, or at least minimize the impact of Man in the Middle attack carried out in section C.1 [3 marks]

(7) Research the work that companies should do to ensure that their users do not fall victims to social engineering attacks similar to the attack you carried out in section C.2. [3 marks]

(8) Research and explain what companies do to protect their web services against a DoS attack similar to the one you have carried out in section D.1. [2 marks]

(9) Intrusion Detection and Prevention systems

Explain the differences between Intrusion Detection System IDS and Intrusion prevention System IPS. [4 marks]

Scenario assessment: Suggest a recommendation for the scenario you have in hand and justify your answer. [3 marks]

Learning Outcomes

The following Learning outcomes will be addressed in this assignment:

LO3 Evaluate security architecture and design and provide the means to enhance operation security;

LO4 Examine cryptography protocols and vulnerabilities and identify attack vectors to exploit them;

LO5 Synthesise emerging trends through engagement and analysis with current research.

Instructions

You should not exceed **5000 words** in total excluding references page and any appendix you can include.

References should follow Harvard referencing.

Section	Questions	What needs to be done	Max Mark
A- Information gathering	OSINT activities	You will need to give two examples of OSINT activities you have done.	3
		Research and evaluate how OSINT can be effective and explain why it is one of the first activities that penetration testers carry out.	3
		Scenario assessment: In your opinion, how dangerous is the information you were able to obtain for your allocated scenario?	2
	Reconnaissance	You will need to show various information you were able to identify and obtain by carrying out your reconnaissance activities.	3
		Scenario assessment: You need to identify and explain how a malicious actor can use the information obtained to exploit the company's web services. It is essential that you give examples of information that you were able to identify that will be relevant to your scenario.	2
	Port Scanning and Enumeration	Show by the mean of screenshots and a brief explanation what are the ports that are used by the server you are carrying out the assessment on.	3
		Research and explain what an open port means and identify threats an open port can potentially causes. This question requires you to use external sources to justify your answer.	3
		Scenario assessment: This question requires to identify threats of open ports that are relevant to your scenario. Explain what the threat can potentially lead on your company's web services and your scenario.	3
B- Server-side exploits	Data tampering	Identify if the application is vulnerable to data tampering and exploit it if possible.	3
		Briefly research and explain data tampering vulnerability. Which Cyber Security tenet this vulnerability violates?	2
		Scenario assessment: What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario?	2
	SQL injection	Identify if the application is vulnerable to SQL injection and exploit it if possible	3
		Briefly research and explain SQL injection vulnerability. Which Cyber Security tenet this vulnerability violates?	3
		Scenario assessment: What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario?	2
	XSS Scripting	Identify if the application is vulnerable to XSS vulnerability and exploit it if possible.	3
		Briefly research and explain SQL injection vulnerability. Which Cyber Security tenet this vulnerability violates?	2
		Scenario assessment: What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario?	2

	Other vulnerabilities	Identify two other vulnerabilities you were able to identify in the vulnerable machine.	2
		Scenario assessment: Research and investigate their threats for your scenario and identify which Cyber Security tenet these vulnerabilities violate?	2

	Cryptanalysis attack	Show how to conduct a cryptanlalysis attack on your scenario envrionmentcryptanalysis	2
		Scenario assessment: Research and investigate the danger and impact of a succefful Cryptanalyis attack on your scenario and identify which Cyber Security tenet these vulnerabilities violate?	2
D-Client-side exploits	Man in the Middle Attack (MiTM)	Show how the attacker can capture traffic from a session between a genuine user and the server side of the application.	3
		Scenario assessment: What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario?	3
	Social engineering attack	Show how an attacker can lure a normal user of the server to your computer instead of the server machine.	3
		Scenario assessment: What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario?	3
C- Denial of Service attacks	Show how an attacker can carry on a denial-of-service attack on the web server.		2
	Which Cyber Security Tenet this vulnerability violates?		1
	Scenario assessment: What is the impact of this attack on your scenario company?		2
E- Recommendations to protect the scenario company server	Provide recommendations on how to minimise the threats of an attacker using the findings of the reconnaissance phase. There are many possible answers for this question. You will need to ensure that your answer is suitable for the scenario, and you should justify your answer. You should also cite some external sources to explain your choice.		2
	Explain what is port knocking and how it can protect the threats you found in the first section. You should use external sources to explain port knocking.		2
	Explain how SQL injection can be prevented. Use external sources.		3
	Explain how Cross site scripting injection can be prevented. Use external sources.		3
	Explain how cryptanalysis attacks can be prevented Use external sources.		3
	Investigate how companies protect their web services against Denial of services attacks. You		2
	Identify methods used to protect and mitigate man in the middle attack. Use external sources to		2
	Research methods and recommendations companies should follow to protect their employees against social engineering.		2
	Intrusion Detection and Prevention systems	Explain the differences between Intrusion Detection System IDS and Intrusion prevention System IPS	4
		Suggest a recommendation for the scenario you have in hand and justify your answer.	3

Technical contents total:			95
Structure and ease of read		Your document should be easy to follow and understand by readers. You should have clear references to examples to justify your choices	5
Total			100