University of Westminster
School of Computer Science and Engineering

6COSC008C Security and Forensics
Assignment Specification (2021/22)

Module leader	Saman Hettiarachchi
Unit	Coursework
Weighting:	50%
Qualifying mark	30%
Description	Scenario based lab report: Answers are based on all labs.
Learning Outcomes Covered in this Assignment:	LO1: Have a critical understanding of the principles of computer systems security. LO4: carry out basic forensic analysis of a computer system and the artifacts involved. LO5: synthesize emerging trends through engagement and analysis with current research
Handed Out:	Tuesday 22 February 2022
Due Date	Monday 29 April 2022 at 01 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.: W000000000_7BUIS022W
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.**

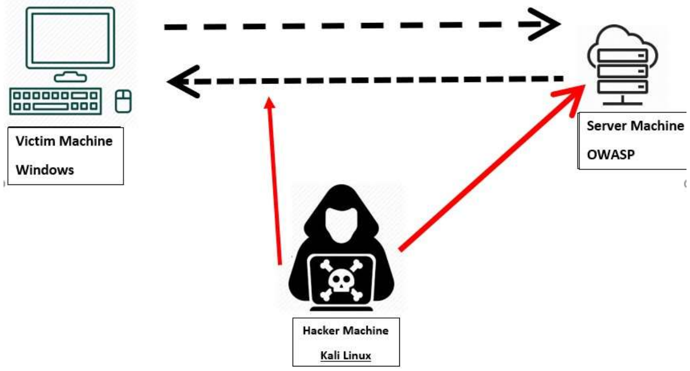
Assessment regulations

Refer to section 4 of the “How you study” guide for undergraduate students for a clarification of how you are assessed, penalties and late submissions, what constitutes plagiarism etc.

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/academicregulations**

Coursework description



To be able to complete your assessment use the lab exercises and activities to map to your allocated scenario. You will have three VMs, the Victim machine (**Windows**), the server machine (**OWASP**) and the hacker machine (**Kali Linux**).

Scenarios

IMPORTANT NOTE

- **Each of you is allocated a scenario. The allocation of the scenarios is on blackboard. You can click here to open it**
- **Failing to complete the assignment using your allocated scenario will result in a <u>10%</u> penalty on your final mark.**
- **You will need to refer to the scenarios document to find the scenario allocated for you.**

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 three 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) Reconnaissance

‹ Show some of the information you were able to obtain by testing web applications in the lab. [3 marks]

‹ *Scenario assessment:* Explain how the information obtained by testing the web applications can be used at a later stage to exploit company's web services? Give an example of information that can be relevant to your scenario. [4 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? [4 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 information 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? [2 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 is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [2 marks]

(4) 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]

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? [5 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? [5 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- Recommendations to protect the scenario company server

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

(2) Briefly research what port knocking is and explain how it can protect against threats you have identified 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) 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 [2 marks]

(6) 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. [2 marks]

(7) 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]

(8) Intrusion Detection and Prevention systems

‹ Show some examples of firewall and iptables rules that can protect your scenario company against attacks you identified in the assessment you carried out before. [4 marks]

‹ Evaluate the effectiveness of the following tools and specify which is more suitable for your scenario and justify you answers. [4 marks]

- Firewall (ufw)
- iptables

‹ Explain the differences between Intrusion Detection System IDS and Intrusion prevention System IPS. [3 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:

‹ **LO1** Have a critical understanding of the principles of computer systems security.

‹ **LO2** evaluate security architecture and design and provide the means to enhance system security.

‹ **LO5** Synthesize emerging trends through engagement and analysis with current research.

Instructions

‹ You should not exceed **2500 words** in total excluding references page and any appendix you can include.

‹ References should follow Harvard referencing.