University of Westminster
School of Computer Science and Engineering

6COSC019C Cyber Security Assignment Specification (2024/25)

Module leader	UoW Module Leader Dr. Ayman El Hajjar / IIT Module Leader Rathesan Sivagnanalingam
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:	Wednesday 12 February 2025
Due Date	Monday 05 May 2025 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/Academic-Regulations-section-17-framework-%20for-undergraduate-taught-courses.pdf

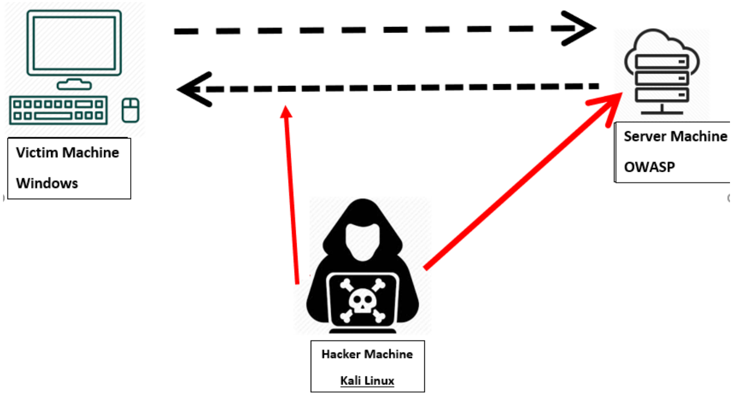
Penalty for Late Submission

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

Requirements

You are expected to complete all lab activities conducted during the term. Each section in the coursework is associated with a lab activity . For all the questions in the document, you are investigating the Owasp Vulnerable machine except **question 1.A** where you are conducting your investigation on the module testing domain name cwscenario.site.



1. OSINT and Passive reconnaissance

A. During your initial assessment, you conducted an in-depth investigation of the domain name you are testing for penetration on. For this question, you are investigating the Domain name provided for testing for this module cwscenario.site.

1. Show two examples of DNS enumeration that you have performed.

   2 marks

2. Explain the potential dangers that the information provided by the examples in the previous question may pose to an organisation.

   1 mark

3. Explain the difference between DNS reconnaissance and DNS enumeration.

   1 mark

4. Suggest one method an organisation can use to minimise the information exposed through DNS analysis activities.

   1 mark

B. Penetration testers conduct passive reconnaissance an organisation's resources that are publicly available, looking for information that can help them with their investigations.

1. Show an example of information you were able to find by simply browsing various pages of the OWASP Vulnerable Machine.

1 mark

2. Explain why the information you obtained in the previous question could potentially pose a threat to the organisation.

   1 mark

3. What should an organisation do to mitigate the risk of this type of threat?

   2 marks

C. One place that penetration testers and hackers alike look for in the early stages of their investigations is the **robots.txt** file for the organisation site.

1. Explain what the robots.txt file is and why it is an important source that hackers investigate.

   2 marks

2. Show the contents of the **robots.txt** file for the OWASP VM and how you leveraged that information to discover additional findings.

   2 marks

3. What should an organisation do to mitigate the risk posed by the exposure of information in the robots.txt file?

   1 mark

2. Active reconnaissance - Scanning and Enumeration

A. During your initial passive reconnaissance, you discovered that the OWASP Vulnerable Machine hosts several different web applications and services.

1. Show the process you followed to discover folders in order to enumerate the running web applications.

   1 mark

2. Explain why conducting extensive passive reconnaissance beforehand is essential for achieving successful folder enumeration results.

   1 mark

3. Explain how the folder enumeration tools determine whether a folder exists or not.

   1 mark

B. The scanning and enumeration phase of a penetration test usually yields useful information.

1. Show your scanning process to identify hosts while minimising the risk of triggering any firewall or intrusion detection system

1 mark

2. Explain why you chose this specific method to identify hosts.

   1 mark

3. Show the results of two different types of TCP scans. For each scan, your results should clearly explain the status of each port, including the reasoning behind its state.

   2 marks

4. For each type of the TCP scans you conducted, explain and justify why you chose that specific scan.

   1 mark

5. In addition to the open TCP ports you identified, show the open ports that operate using the UDP transport layer protocol.

   1 mark

C. While the scanning activity revealed open ports on the OWASP vulnerable machine, it did not provide us with information on the vulnerable machine services nor on what exactly is behind those ports.

1. Show how you enumerated two different services on the OWASP vulnerable network.

   2 marks

2. Explain what the Operating system results mean. Compare the results you know with your actual prior knowledge of the operating systems. How accurate the results are.

   1 mark

3. Show the enumeration process of the services behind the TCP ports while obfuscating your IP address.

   2 marks

4. What measures can the administrators of the OWASP Vulnerable Machine take to reduce the effectiveness of scanning and enumeration, making the results less valuable to a hacker?

   1 marks

D. Using basic service enumeration in Nmap can provide useful information about the services running. However, Nmap's scripting engine offers the capability to conduct more in-depth enumeration on specific services.

1. Show how you conducted extensive enumeration on the SSH service using two different scripts.

2 marks

2. Show how you conducted one enumeration activity on the IMAP service.

   1 mark

3. What types of Nmap scripting engine scripts are typically avoided by both hackers and ethical hackers during the early stages of their assessment?

   1 mark

E. During the early stages of your scanning, you identified that the Samba service is running on the OWASP Vulnerable Machine.

1. Show how you conducted an extensive enumeration on the Samba service using the enum4linux tool.

   2 marks

2. Show two examples of Nmap engine scripts that you could have used to conduct Samba service enumeration instead of using the enum4linux tool.

   1 mark

3. Recommend two security measures that could reduce the importance of the Samba service enumeration results.

   1 mark

3. Exploiting Network Vulnerabilities

A. Spoofing attacks can be conducted on various layers depending on the access the attacker has prior to the attack.

1. Show how you hijacked the session between the host machine and the OWASP vulnerable machine using the Ettercap tool.

   1 mark

2. Show how you conducted a Man-in-the-Middle (MiTM) attack by spoofing the MAC addresses of both the OWASP machine and the host machine using only networking commands.

   2 marks

3. Explain what session hijacking is and the threats it poses when exploited.

   2 marks

4. Explain how an attack can be prevented from conducting a session hijacking attack.

   2 marks

B. During the initial scanning and enumeration, you identified several services running on the OWASP vulnerable machine.

1. Show the process of enumerating and exploiting the SSH service using the Metasploit tool to obtain a session shell.

   2 marks

2. Show the process of exploiting the SSH service using the Metasploit tool to obtain a session shell.

   1 mark

3. Briefly show the two other services that you have exploited (or attempted to exploit) using the Metasploit tool.

   2 marks

4. Explain how you identify which service to exploit and how you decide on which method of exploitation to use.

   2 marks

5. Explain what is meant by escalating privileges in a shell.

   1 mark

C. Denial of Service (DoS) attacks are one of the most challenging attacks that organisations must deal with continuously.

1. Show two methods you used to carry out a Denial of Service attack on the OWASP vulnerable machine.

   2 marks

2. Briefly explain the various methods of conducting Denial of Service attacks and the impact of each.

   1 mark

3. Demonstrate how DoS attacks can be conducted using the Nmap scripting engine.

   1 mark

4. Briefly explain what organisations can do to mitigate the threats posed by DoS attacks.

   1 mark

4. Exploiting Web applications Vulnerabilities

A. During your vulnerability analysis and exploitation phase, you have identified and exploited the SQL injection vulnerability in the DVWA (Damn Vulnerable Web Application).

   1. Show how you can identify if DVWA is vulnerable to SQL injection and specify the type of database it uses.

      1 mark

   2. Show that you were able to exploit the SQL injection vulnerability by showing the steps of your database enumeration and an important type of information you were able to obtain.

      3 marks

   3. Explain what an SQL injection vulnerability is and the threats it poses to an organization.

      2 marks

   4. Which security principles does SQL injection violate?

      1 mark

   5. Briefly explain how an organisation can protect its web applications against SQL injection.

      1 mark

B. You have identified during a penetration testing activity that the Security Shepherd application is vulnerable to Cross-Site Scripting (XSS).

   1. Show how you initially conducted your analysis to identify that the application is vulnerable to XSS.

      1 mark

   2. While conducting further analysis on the Security Shepherd web application, you discover another XSS vulnerability. However, this time the developer attempted to mitigate it by filtering the inputs. Show how you were able to overcome the filtering and exploit the XSS vulnerability.

      2 marks

   3. How dangerous are the threats of XSS attacks to an organisation, and how can a malicious actor leverage the XSS vulnerability to gain confidential information?

      1 mark

   4. Briefly explain how to protect your web application from Cross-Site Scripting attacks.

      2 marks

C. On the DVWA web application, a malfunctioning (and vulnerable) CAPTCHA prevented you from changing the password.

1. Show how tampering with server data from the client side can break the identification and authentication process and bypass it by exploiting an insecure CAPTCHA.

1 mark

2. Explain how CAPTCHA works and why the identification and authentication process failed when the client-side verification mechanism was tampered with.

1 mark

D. During your vulnerability analysis, you also found and exploited several other vulnerabilities.

1. Show how you conducted Remote File Inclusion (RFI) and website defacement.

2 marks

2. Show how you conducted Cross-Site Request Forgery (CSRF) on the DVWA web application.

1 mark

3. Show how you conducted OS Command Injection on the DVWA web application.

1 mark

5. Exploiting Cryptographic weaknesses.

A. During the exploiting phase you have conducted various cryptanalysis attacks including Brute force and Dictionary attacks.

1. Show how you successfully conducted brute force attack on one service (Web or network service)

2 marks

2. Show how you successfully conducted a dictionary attack on one service (Web or network service)

2 marks

3. Explain the threats that the brute force and dictionary attacks, may pose to an organisation.

1 mark

4. Explain what measures organisations should take to reduce the risks of their environments being compromised by brute force or dictionary attacks.

2 marks

B. When exploiting the SQL database of the DVWA application on the vulnerable machine, you managed to acquire the users' passwords in a Hash format.

1. Show how you identified the Hash function algorithm used in the SQL database (you exploited).

2 marks

2. Show the hashes for all the SQL users acquired, cracked back to their original plaintext format.

2 marks

3. Explain what a **Hash function** is and how it is used in modern web applications?

2 marks

4. Suggest one mitigation technique an organisation should implement to prevent hackers from breaking the password hashes of their systems. Justify your answer.

2 mark

6. Exploiting Users weaknesses

A. Many systems are compromised by exploiting user weaknesses, such as luring users to a fake website or service to capture their credentials.

1. Show how an attacker can lure a normal user of the server to your computer instead of the server machine and show the information obtained.

2 mark

2. Show how you can capture the information obtained from this attack using Wireshark..

1 mark

B. In the previous activity, we used a social engineering attack to capture the credentials of a victim using the OWASP Vulnerable Machine. However, most of the time, attackers need more than credentials, such as gaining initial access to a system for further enumeration and exploitation. To achieve this, hackers often use social engineering to trick victims into downloading malicious code.

1. Show the process of crafting the malicious code. .

1 mark

2. Show how an attacker would gain initial access once the victim executes the malicious code.

2 marks

3. Identify methods organisations can use to mitigate the threats of social engineering to protect their environments and users.

2 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.

Questions Icons

- Questions with this icon are for **Showing your lab work**: For these questions, you are required to complete the activity related to the topic and provide a screenshot of your work. The screenshot must clearly show your student ID on the terminal prompt to verify that the work is yours. Instructions on modifying the terminal prompt are provided in the lab documents. For each screenshot, you are required to provide a description of what it represents.
- Questions with this icon are for **Research**: For these questions, you are required to conduct research on the weaknesses, activities, or exploit methods you have used and provide a clear, well-structured answer. You should include external resources to support and strengthen your response.
- Questions with this icon are for **Mitigation Techniques and Recommendations**: For these questions, you are required to propose methods to mitigate the threats and weaknesses identified in each activity and justify your recommendations. The number of methods you should present depends on the specific question. Be sure to include external resources to support and strengthen your response.