ASSIGNMENT BRIEF

HTU Course No: 10203362	**HTU Course Name:** Ethical Hacking
BTEC Unit Code:	**BTEC UNIT Name:**

Student Name/ID Number/Section	
HTU Course Number and Title	10203362 Ethical Hacking
BTEC Unit Code and Title	
Academic Year	2024-2025 2
Assignment Author	Sami Almashaqbeh
Course Tutor	Sami Almashaqbeh
Assignment Title	DPSR Attack
Assignment Ref No	1
Issue Date	01/04/2025
Formative Assessment dates	From 09/04/2025 to 29/05/2025
Submission Date	13/06/2025
IV Name & Date	Isra' Hasan 31/03/2025

Submission Format

The submission for this assignment is:

1. An individual written **detailed report** (word format) that provides thorough, evaluated, or critically reviewed technical information on all the points illustrated in the *Assignment Brief and Guidance* section. **All snapshots must be very clear, with a computer timestamp and date. This will serve as evidence of your work. Additionally, you should include a watermark by using any watermarking tool to place your first and last name on the snapshots**. ***Including signed student assessment submission and declaration form in a separated file.***
2. **An in-class written exam will be held on 31-05-2025.**
3. **An oral discussion about the report, followed by a practical presentation to demonstrate students' skills. If there is a failure in any criteria during the oral discussion or the practical presentation, the criteria will not be considered fulfilled, even if they were done correctly in the submitted report.**

Report guidelines:

In your report, you should make use of headings, paragraphs, and subsections as appropriate. The expected word limit is about 5000 words (recommended 15-20 pages not including snapshots), although you will not be ***penalised*** for exceeding the total word limit. Do your best to be within the word limit. Your report should be:

1. In a form of a **soft copy** submitted via the URL below.
2. Written in a formal business style using **single spacing and font size 12 Times New Roman (Headings CS)**.
3. Must be supported with research and referenced using the Harvard or APA referencing system.

Note: Soft copies submissions should be done through the university's eLearning system within the deadline specified above from below link: https://elearning.htu.edu.jo/

Unit Learning Outcomes

LO1 Gain a solid foundation in ethical hacking and information security controls.

LO2 Develop advanced skills in reconnaissance techniques, and vulnerability analysis.

LO3 Master packet-sniffing, password cracking, and social engineering techniques, along with web application hacking strategies.

LO4 Acquire proficiency in using the Metasploit Framework for penetration testing and exploit assessment.

Assignment Brief and Guidance

The Department of Public Safety and Regulation (DPSR) is responsible for ensuring the security and proper oversight of various public safety services. The department utilizes a comprehensive IT system designed to streamline critical functions, including license application management, weapons registration, and statistical monitoring. By integrating advanced data traceability and security tools, the system ensures compliance, transparency, and efficiency in public safety operations.

Below is a list of the main IT servers required for the Department of Public Safety and Regulation:

Application Servers: Host essential software applications for managing license applications, weapons registration, and regulatory oversight, ensuring smooth departmental operations.

Database Servers: Store crucial data, including citizen records, license details, weapon registrations, incident reports, and compliance logs.

Web Servers: Power the official department website, providing citizens with seamless access to licensing procedures, regulatory information, and public safety updates.

Email Servers: Ensure secure communication among departmental staff, law enforcement agencies, and stakeholders for efficient coordination and regulatory enforcement.

Authentication Servers: Manage secure access to IT systems, ensuring only authorized personnel can access critical tools and sensitive regulatory data.

Citizen Engagement Channels:

Website: Citizens can apply for licenses, check application statuses, and access regulatory guidelines through an intuitive online platform.

Mobile App: Provides on-the-go access for submitting applications, receiving notifications, and tracking license approvals via Android and iOS devices.

Payment Options: Secure and convenient payment methods, including online gateways and contactless transactions, facilitate regulatory fee processing and service payments.

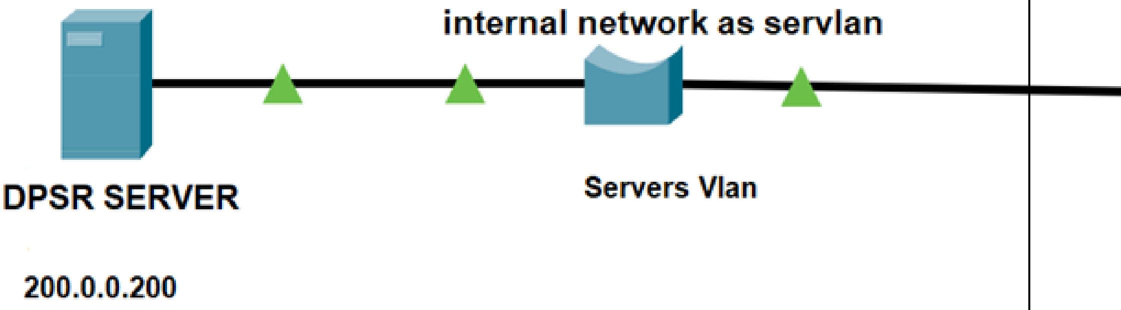
By leveraging robust IT infrastructure, the Department of Public Safety and Regulation enhances operational efficiency, improves public service accessibility, and upholds security and compliance standards.

As an Ethical Hacker at Department of Public Safety and Regulation (DPSR), your mission is to conduct comprehensive security assessments of our IT systems, ensuring the protection of critical operational data and customer information. Your goal is to identify vulnerabilities and provide actionable recommendations to enhance our cybersecurity. To support your work, you'll receive a full replica of our servers, available as "ova" files, which can be run through Oracle VirtualBox. Download the virtual environment here: DPSR.ova . These virtual servers mirror our live infrastructure, providing a realistic testing environment for your assessments. Also, you may need some files from this folder; they may help you. Needed files

Your responsibilities include simulating cyberattacks on these virtual systems to detect potential weaknesses. Your findings will help us evaluate and improve the security of our operations, ensuring they remain resilient to real-world threats. By identifying vulnerabilities and proposing enhancements, your efforts will safeguard our infrastructure, maintain customer trust, and support the continued success of Department of Public Safety and Regulation (DPSR).

Your setup environment must be as below:

http://200.0.0.200/index.php
http://200.0.0.200/dpsr
http://200.0.0.200/ dpsr2



The tasks that need to be completed are listed below this line. Please carefully review the specified goals for achieving them.

- ***Each goal should be met using the designated method, and no alternative methods should be employed. Ensure that the testing requirements for each task serve as the basis for accomplishing each goal.***
- ***You must provide snapshots to support your work documentation for each point. Choose the best two snapshots that conclude your work.***

Part1: *An in-class written exam will be held on 31-05-2025.*

P1 P2 P3 P4 P5 P7 M1 D1

Part2: Ethical hacking foundations:

Before starting your role as an Ethical Hacker at DPSR, the CEO requires a detailed explanation of the following points. This will help evaluate your readiness for the task and ensure a professional approach to the assignment. Please provide a clear and thorough discussion of each topic to demonstrate your expertise and suitability for the role.

A. Please provide a comprehensive discussion of the various hacking techniques used in cybersecurity attacks, including **packet sniffing**, **password cracking**, and **social engineering**. Explain how each technique operates in detail. Additionally, discuss the **preventive measures and security practices** that individuals and organizations can implement to defend against these methods.

B. How does web application architecture work, and what is the role of HTTP and HTTPS in securing communication between clients and servers? In addition, delve into the details of common web vulnerabilities, including SQL injection, command injection, cross-site scripting (XSS). Explain how these vulnerabilities can be exploited and what measures can be taken to mitigate them in web applications.

C. Examine the various components of Metasploit, including its modules, payloads, exploits, auxiliary tools, and post-exploitation modules

Part3: Reconnaissance and vulnerability analysis phase

A. The Department has these websites, “https://bnm.mr/”, 41.188.113.109, 82.151.67.232. Use passive information gathering tools to collect information about this website. (don’t use Nmap or any active scanning tools it is illegal).

B. Utilize active information gathering and scanning tools to collect data about the target system, ***which in this case is the virtual machine for DPSR.ova.*** Create a table containing the system name, IP addresses, open ports, running services and their versions, the operating system, and any other pertinent information necessary for identifying vulnerabilities and planning potential exploits in the next phase.

C. Conduct a vulnerability assessment for ***DPSR.ova*** with the goal of identifying vulnerabilities in their systems, networks, and applications. The responsibility includes documenting vulnerabilities, assessing their risks, and providing clear mitigation recommendations. Your report should present the top 20 vulnerabilities in a table format for easy reference. (use Nessus or any equivalent software)

Part4: Exploitation phase

A. Use Wireshark or any sniffing tools to capture packets during a Telnet and FTP connection and provide a snapshot of the credentials captured using the sniffing tool. (username : sami ,password: P@ss1234 for telnet and username : admin ,password: Hard4u2025 for FTP).

B. Utilize the DPSR employee server (http://x.x.x.x/dpsr2), replacing "x.x.x.x" with the server IP address obtained during the reconnaissance phase, to execute a password cracking attack using THC Hydra or any another equivalent tool.

C. Utilize the DPSR web server (http://x.x.x.x/), replacing 'x.x.x.x' with the server IP address obtained from the reconnaissance part, ***to exploit the following vulnerabilities:***

1. SQL injection attacks can be carried out manually or by using tools like SQLMAP to bypass the login page.
2. Find cross-site scripting (XSS) vulnerabilities, obtain the session ID, and record it for use in the next task.
3. Find another SQL vulnerability on the welcome page, use SQLMAP to identify the database name, dump the entire database, and obtain an OS shell.
4. Find a command injection vulnerability, use it to create a username and password on the server, and give this username administrator privileges.
5. Using a manual SQL approach without relying on automated tools to find all user accounts and passwords, snapshot the main four steps (database name, information schema table names, information schema column names, and the obtained user accounts results).

D. Utilize the DPSR server (http://x.x.x.x/dpsr), replacing "x.x.x.x" with the server IP address obtained during the reconnaissance phase, ***to exploit some of OWASP Top 10 vulnerabilities as follows:***

1. Find Broken Authentication and Session Management vulnerabilities to update Adrian's profile.
2. Search for Sensitive Data Exposure to discover the database password and Sami's comments.
3. Find Security Misconfiguration, use Gobuster or any equivalent tool to list all files, find the password file, and access it to obtain the passwords.

E. Use ***The Metasploit framework*** to perform the following tasks on the DPSR server. Use the server's IP address that you obtained from the reconnaissance part:

1. Identify the vulnerable services on the server using Metasploit auxiliary modules.
2. Exploit well-known vulnerabilities that you find, such as EternalBlue or the VSFTPD backdoor, using Metasploit modules.
3. Use the auxiliary module or Hydra to brute force the FTP service and find the login password using the provided username and password list.
4. Migrate your payload with proof, extracting passwords (don't forget to de-hash the passwords), sharing the victim's screen, and taking screenshots remotely from the victim machine.
5. Create a username (you may use your name) and add the user to the local 'Administrator' and 'Remote Desktop Users' groups. Connect to the target machine using the created username and password through Remote Desktop Connection.
6. Utilize ***the patch file*** located on the targeted server desktop to address this vulnerability. Subsequently, employ Metasploit auxiliary or attempt to exploit the vulnerability again. Provide evidence demonstrating that you are unable to exploit it after applying the patch.
7. Create a custom payload (Shell, not Meterpreter) using MSFvenom and integrate it into exploits using a multi-handler. After that, upgrade the obtained shell to Meterpreter.

F. **CTF (Capture the Flag):** Locate the 10 flags on ctf.htu.edu.jo.

Learning Outcomes and Assessment Criteria			
Learning Outcome	**Pass**	**Merit**	**Distinction**
LO1 Gain a solid foundation in ethical hacking and information security controls.	**P1** Explain the principles of ethical hacking and its importance in securing systems. **P2** Discuss the legal and ethical implications of hacking activities.	**M1** Compare the top five ethical hacking and penetration testing certificates.	**D1** Analysis of the differences between ethical hacking, penetration testing, and vulnerability assessment.
LO2 Develop advanced skills in reconnaissance techniques, and vulnerability analysis.	**P3** Explain and demonstrate various reconnaissance methods, such as passive and active information gathering. **P4** Discuss a variety of tools and technologies commonly used in reconnaissance, such as Nmap, Shodan, or OSINT (Open Source Intelligence) techniques.	**M2** Capability to efficiently gather information about target systems, networks, or organizations. **M3** Proficiency in identifying potential vulnerabilities in systems, networks, and applications.	**D2** Ability to create clear vulnerability assessment summary reports, including evidence of vulnerabilities, and recommended mitigation strategies.
LO3 Master packet-sniffing, password cracking, and social engineering techniques, along with web application hacking strategies.	**P5** Discuss different hacking techniques, such as packet-sniffing, password cracking, and social engineering. **P6** Explain the web application architecture, HTTP, HTTPS, and common web vulnerabilities: SQL injection, command injection, XSS, and CSRF. **P7** Ability to configure and use password cracking tools like John the Ripper or Hashcat.	**M4** Proficiency in using packet sniffing to capture and analyze network traffic. **M5** Demonstrated skills in executing social engineering attacks, such as phishing campaigns or pretexting or proficiency in exploiting web application vulnerabilities using tools like Burp Suite or SQL map.	**D3** Manually exploiting web application vulnerabilities: SQL injection, command injection, CSRF, and XSS, including persistent XSS (XSS store), without relying on automated tools.

LO4 Acquire proficiency in using the Metasploit Framework for penetration testing and exploit assessment.	**P8** Explain the purpose of modules, payloads, exploits, auxiliary modules, and post-exploitation modules within Metasploit. **P9** Identify vulnerable services and hosts using Metasploit's auxiliary modules.	**M6** Create custom payloads using MSFvenom and integrate them into exploits using a multi-handler. **M7** Exploit common vulnerabilities, such as buffer overflows, SQL injection, remote code execution, as well as well-known exploits like EternalBlue and the VSFTPD backdoor, using Metasploit modules.	**D4** Demonstrates proficiency in using Metasploit, such as upgrading a shell to Meterpreter, migrating a payload with proof, extracting passwords, sharing the victim's screen, capturing webcam snapshots, taking screenshots, or employing any advanced Meterpreter capability.