Assignment task 1 draft (deadline 4pm Thursday 6th February 2025)

- In the Week 2 folder on BB, there is a VulnNewApp.exe application which you need to attack.
    - You will notice there is an issue in exploiting the VulnNewApp. Please briefly explain the issue in your report and how to overcome it. (Only explain; don't show a walkthrough. You can present only one screenshot for this).
    - Also attack vulnApp on the Windows 7 machine and show a working exploit and walkthrough. (Note: the application listens on port 9999).
- Using the proof-of-concept script on Blackboard (named vulnapp_POC_script.txt in the Scripts folder) develop a working exploit for vulnApp.
- Provide documentation and proof of your exploit in your report.
- Remember to record every step and take screenshots of all the steps.

Practical Assignment 2 Deadline Thursday 6th March 2025 at 4pm

- In OWASP Broken Web Applications Project, use either the
    - OWASP Mutillidae II
    - or DVWA
    - Demonstrate you can obtain a shell with the following
    - An LFI vulnerability in the web application with file upload;
    - An LFI vulnerability in the web application with contaminated logs; and
    - An RFI vulnerability in the web application.
    - Demonstrate attacks using SQL injection and Cross Site Scripting
- Provide documentation and proof of useful attacks in your report

Task 3 – Password Attack Draft due 4pm Thursday 13th March

- Use different tools that are covered (or not covered) in this module to demonstrate a range of password attacks.
- You could perform the attack against either Windows XP or any other attackable VM that you could find in https://fym.cs.salford.ac.uk/pentest . You should attack different network services such as http, ftp, ssh, rdp, etc. We have covered HTTP authentication here; you can try other things. (Target at least 2 protocols).
- For offline attacks, you have been provided a file on BB called password_hash.txt which contains four password hash. The password hashes have been encoded using md5, sha256, sha512, and sha256 with salt respectively. The passwords are relatively easy as they are common. Crack the password offline, and check which you can discover using wordlists and using crunch.
- A password-protected Word file has been provided called TradeSecret.docx. Try to crack the password using (**office2john**, **zip2john** etc). Hint: the creator of the file likes animals, and the password is relatively easy.
- Perform an in-memory attack using the pass-the-hash technique to remotely authenticate into the Windows XP system.
- In the assignment report provide proof of successful attacks. I would like to see if you have understood how to use a range of tools, I leave it up to you what you want to do. You might want to generate your own dictionary, or use the existing dictionaries, wordlists etc that you could find on the Internet or the Kali tools.

Metasploit Task (Assessment) Deadline: 4pm Thursday 20th March

- Using results from enumeration/vulnerability scanning, use Metasploit Framework to exploit one vulnerability of your choice on each of the following targets, to obtain Administrative/System privileges:
    - Windows 7 Lab Machine

    - Windows XP Machine
    - Rookie VM
- Do not exploit the same vulnerability on multiple targets.
- Previous vulnerabilities such Shellshock, SLMail and MS08-067, which we have exploited, will not be accepted.
- Provide documentation and proof of your exploits in your report