Exercise.4.

Task.1: **Side-channels**

1. Meltdown exploits a side-channel vulnerability in CPU speculative execution. It leverages the CPU's ability to perform out-of-order execution, allowing unauthorized access to kernel memory by bypassing memory protection. The attack uses timing-based cache analysis to read privileged data stored in cache memory.

2.

   mostly impacts Intel CPUs, although some ARM and IBM POWER processors are also at risk. It affects Windows, Linux, macOS, and other operating systems that use these CPUs as their foundation.

3.

   Unprivileged processes have access to sensitive data from kernel memory, including cryptographic keys, passwords, and personal information.

4. Meltdown has not been linked to any documented real-world attacks, but because of how serious the vulnerability was, its revelation caused a great deal of alarm and drove quick patching efforts.

5.

   Yes, software fixes have helped to lessen the effects of Meltdown. Kernel page-table isolation, or KPTI, was adopted by operating system vendors (such as Microsoft, Apple, and Linux versions) to keep kernel memory and user processes apart. Additionally, processor makers fixed issues related to speculative execution by releasing microcode upgrades.

Sources\\
National Institute of Standards and Technology (NIST). "Meltdown Vulnerability Summary."
National Vulnerability Database (NVD). U.S. Government, 2018. NVD Meltdown CVE-2017-5754 U.S. Computer Emergency Readiness Team (US-CERT). "Meltdown and Spectre Vulnerabilities."
Cybersecurity and Infrastructure Security Agency (CISA). US-CERT Advisory TA18-004A Intel Corporation. "Intel Analysis and Mitigation of Speculative Execution Side-Channel Vulnerabilities." Intel Security Advisory SA-00088

Task 2: Slow Loris

1-

Sending erroneous HTTP requests to a web server and leaving them open for a lengthy period is how the Slowloris attack operates. To prevent the server from cutting the connection, the attacker periodically transmits only a small portion of the request. The server eventually exhausts its connections, which prevents it from supporting actual users.

2- The reason Slowloris is unique is because it attacks with very minimal bandwidth. Slowloris can take down a server with just a few requests, in contrast to other DDoS assaults that send massive amounts of data to overwhelm the server. Instead than overwhelming the server with traffic, it focuses on how it handles connections.

3- The major result is that all of the connections are being occupied by the attacker's unfinished requests, which prevents the web server from handling legitimate user requests. This can result in a server outage, blocking regular users from accessing the website.

4- You may mitigate Slowloris's effects by:

restricting how many connections may come from a given IP address.
In order to quickly close unfinished requests, set shorter connection timeouts.
improving request handling by utilizing reverse proxies such as Nginx or Apache's mod_reqtimeout.
putting in intrusion detection systems (IDS) to stop questionable behavior.

5- During the 2009 Iranian election protests, Slowloris was utilized in assaults on Iranian government websites. The websites were successfully brought down by the attack without consuming a lot of resources.

Sources:

U.S. Cybersecurity and Infrastructure Security Agency (CISA). "Denial-of-Service Attacks Overview."

CISA DoS Attacks Overview

NIST National Vulnerability Database (NVD). "Denial of Service and Mitigation Techniques."

NIST NVD DoS Guide

Task 3: BurpSuite Introduction

1. **I faced issue to keep the change in edited post request, when I forward it to HTTP history it received without changes**
2. **With regard to Hydra task, in contrary all step went smoothly, the code run and complete with finding wrong password**

Subtask 2: Repeater

The DVWA Session cookie looks to be produced following a predictable pattern, most likely an incremental integer or a straightforward numeric value taken from the internal state of the server, based on the request and response parameters you gave.
• The DVWA Weak Session IDs page produces a new numeric session ID (such as 1727983968) each time a POST request is made to it.
• If you use BurpSuite's Repeater to submit this request again and over again, you should see that the session ID values vary in a predictable way—they could increment by a given amount or adhere to a particular pattern.

Session prediction attacks can exploit this gap in the session ID generating process. An attacker may create their own session cookie with the expected value and use it to spoof another user's session if they could predict the session ID generation procedure.

Subtask 3: Intruder

Session prediction attacks can exploit this gap in the session ID generating process. An attacker may create their own session cookie with the expected value and use it to spoof another user's session if they could predict the session ID generation procedure.