**Group Member:**

Aimen Tahir (181400179)

Arslan Ahmad (181400019)

Assignment: 1

**Qno:1**

**GitHub**

GitHub is a website and cloud-based service that allows developers to store and manage their code while also tracking and controlling modifications. To fully grasp what GitHub is, you must first comprehend two interconnected principles:

* Version control
* Git

**What is version Control**

Developers can use version control to keep track of and manage changes to a software project's code. Version control becomes increasingly important as a software project expands.

 version control lets developers safely work through **branching** and **merging**.

**What is Git**

Git is a distributed version control system, which implies that every developer's computer has access to the whole codebase and history, allowing for easy branching and merging.

**Features**

* **Repository (repo)**

Repositories in [GIT](https://www.geeksforgeeks.org/git-lets-get-into-it/) contain a collection of files of various different versions of a Project. These files are imported from the repository into the local server of the user for further updations and modifications in the content of the file.

* **Branch**

A branch is a version of the repository that diverges from the main working project. It is a feature available in most modern version control systems. A Git project can have more than one branch. These branches are a pointer to a snapshot of your changes.

* **Commit Changes**

Commit changes **is** a saved record of a change made to a file within the repo.

**Qno:2**

**What is Zero Day Attack?**

The phrase "zero day" or "day zero attack" refers to the threat of an undiscovered security vulnerability in computer software or an application for which no fix has been provided or for which the application developers were unaware of or did not have enough time to resolve.

Zero-day is sometimes written as 0-day. The words vulnerability, exploit, and attack are typically used alongside zero-day, and it’s helpful to understand the difference:

* A zero-day vulnerability is one that has been discovered by attackers before the vendor is aware of it. Because vendors are ignorant of zero-day vulnerabilities, no fix exists, making assaults more likely to succeed.
* A zero-day exploit is a technique used by hackers to attack systems that have a previously unknown vulnerability.
* A zero-day attack is when a zero-day exploit is used to harm or steal data from a system that has been exposed to a vulnerability.