**ASSIGNMENT 1**

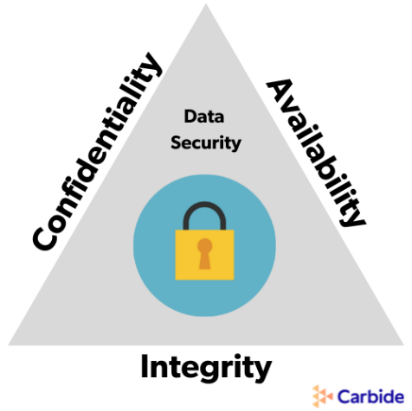
**Introduction To Ethical Hacking**

# **Topic: Introduction to Ethical Hacking**

ASSIGNMENT 1 Date: 27/06/2022

**1.CIA Triad Introduction & Real time case scenario.**

* CIA triad refers to Confidentiality, integrity and availability. It is a model designed to guide policies for information security within an organization.

****

* **Confidentiality:** It refers to privacy. It measures are designed to prevent sensitive information from unauthorized access attempts.
* **Integrity:** It involves in maintaining the consistency, accuracy and trust of data over entire life cycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people
* **Availability: It** means information should be consistently and readily accessible for authorized parties.

Real time scenario:

The situation in an ATM:

ATM allows users to access bank balances and other such information. It incorporates measures to cover the principles of triad

* **Confidentiality:** The two-factor authentication (debit card with the PIN code) provides confidentiality before authorizing access to sensitive data.
* **Integrity:** The ATM bank software ensure data integrity by maintaining all transfer and withdrawal records made via the ATM in the user’s bank accounting.
* **Availability: The ATM provides availability as it is for public use and is accessible at all times.**

**2.Blue Team & Red Team Introduction**

Blue Team:

* It is the group responsible for defending an enterprise’s use of information systems by maintaining its security posture against a group of mock attackers.
* A blue team consists of security professionals who have an inside out view of the organization.
* Their task is to protect the organization’s critical assets against any kind of threat.
* If the red team is playing offense, the blue team is playing defence to protect an organization’s critical assets.
* Defending a company against attack involves understanding what assets need to be protected and how to best protect them. So the skills required for Blue Team are:
* **Risk Assessment:** Risk assessment helps you identify key assets that are most at risk for exploitation so you can prioritize your resources to protect them.
* **Hardening techniques:** Recognizing weaknesses in your organization's security is only helpful if you know the techniques for fixing them.
* **Threat intelligence:** You’ll want to know what threats are out there so you can plan appropriate defenses. Blue teams have to stay a step ahead of attackers.
* **Monitoring and detection systems:** As a blue team professional, you’ll need to know how to use packet sniffers, security and information event management (SIEM) software, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

Red Team:

* A group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture.
* The red team plays the part of the attacker or competitor with the intention of identifying vulnerabilities in a system.
* A red team consists of security professionals who act as adversaries to [overcome cyber security controls](https://purplesec.us/security-controls/).
* Red teams often consist of independent ethical hackers who evaluate system security in an objective manner.
* The mindset of red team activities requires its own set of skills such as:
* **Software development:** When you know how applications are built, you’re better able to identify their possible weaknesses (as well as write your own programs to automate the attack process).
* **Social engineering:** An organization’s biggest vulnerability is often its people rather than its computer network. Social engineering tactics like phishing, baiting, and tailgating can sometimes be the easiest way past security defences.
* **Penetration testing:** Much of a red team’s job is to identify and try to exploit known vulnerabilities on a network. This includes familiarity with vulnerability scanners.
* **Threat intelligence and reverse engineering:** Knowing what threats are out there—and how to emulate them—can make a more effective attacker.
* **Creativity:** Finding ways to beat a blue team’s defence often requires creating new and innovative forms of attack.

**Name: I PRASANTI**

**Sic: 20BCEA56**

**Branch: CEN**