# TASK 1

## Overview

Write about the top 10 hackers and which categories they fall into, like black, gray, or white hat hackers. And explain on what basis you categorize them as such.

## Hacker Categories

Hackers are categorized based on their ethical and legal stance in the realm of cybersecurity. Some of them are:

1. **Black Hat Hackers:** Black hat hackers are individuals who engage in hacking activities with malicious intent. They operate unlawfully, seeking to exploit vulnerabilities for personal gain, which often involves financial fraud, data theft, or causing harm to individuals, organizations, or systems. Their actions are typically in violation of the law and are driven by personal gain, making them the "bad actors" of the cybersecurity world.

2. **White Hat Hackers:** White hat hackers, often referred to as ethical hackers or cybersecurity professionals, use their hacking skills for legitimate and legal purposes. They work to identify and fix security vulnerabilities, protect systems, and prevent cyber threats. White hats are employed by organizations, government agencies, or cybersecurity firms, and they play a critical role in defending against black hat hackers and improving overall security.

3. **Gray Hat Hackers:** Gray hat hackers fall somewhere between black and white hat hackers. They don't have inherently malicious intentions, but they may operate in morally ambiguous territory. Gray hats may identify vulnerabilities without explicit permission (which is illegal) but disclose them to the affected parties. Their actions often raise ethical questions, as they operate in a legal gray area.

## Top 10 Hackers

1. Kevin Mitnick (United States):

Category: Former Black Hat, Now White Hat

Basis: Mitnick was a notorious black hat hacker who engaged in various illegal activities. After serving a prison sentence, he transformed into a white hat hacker, working as a security consultant and author.

2. Adrian Lamo (United States):

Category: Gray Hat

Basis: Lamo was known for ethical hacking but also faced legal issues for unauthorized access. His actions often blurred the lines between black and white hat activities.

3. Richard Stallman (United States):

Category: White Hat

Basis: Stallman is a respected programmer and advocate for free software. His hacking activities were primarily aimed at advancing open-source and free software.

4. Gary McKinnon (United Kingdom):

Category: Gray Hat

Basis: McKinnon, a UFO enthusiast, conducted unauthorized intrusions into U.S. government computers to uncover information about extraterrestrial activities, displaying gray hat motivations mixed with curiosity.

5. Linus Torvalds (Finland):

Category: White Hat

Basis: Linus Torvalds created the Linux operating system, a significant contribution to open-source software. His work aligns with white hat principles, as it aims to enhance technology for the common good.

6. Julian Assange (Australia):

Category: Gray Hat

Basis: Assange's activities with WikiLeaks involve publishing sensitive and classified information. His intentions often align with transparency and activism, but legal ambiguities exist.

7. Edward Snowden:

Category: Gray Hat

Basis: Snowden exposed extensive government surveillance programs, revealing gray hat qualities with a focus on whistleblowing.

8. LulzSec (Collective/Various Countries):

Category: Black Hat

Basis: LulzSec engaged in high-profile cyberattacks, displaying a disregard for legal boundaries and a focus on chaos and disruption.

9. Guccifer (Romania):

Category: Gray Hat

Basis: Guccifer, whose real identity is Marcel Lehel Lazar, gained notoriety for hacking high-profile individuals and politicians. His motivations were a mix of curiosity, political activism, and personal vendettas, placing him in the gray hat category.

10. Astra (India):

Category: Gray Hat

Basis: Astra, a prominent Indian hacker, gained notoriety for exposing vulnerabilities in government websites. While his actions were not entirely legal, they were aimed at highlighting security issues.