**Name**: Tirumalasetti Mohan Sri Sai

**College**: MVR College of Engineering & Technology

**Rollno**: 208H1A0540

# Task-1 Top 10 Hackers

[**Kevin Mitnick**](https://en.wikipedia.org/wiki/Kevin_Mitnick)

**Type:** White Hat

**Description:** Once a notorious black hat hacker, Kevin Mitnick transformed his skills into a highly respected career in cybersecurity. He now works as a security consultant, helping organizations identify and mitigate vulnerabilities.

[**Anonymous**](https://en.wikipedia.org/wiki/Anonymous_(hacker_group))

**Type:** Black Hat

**Description:** The Anonymous group is a decentralized collective of hacktivists who use their skills to promote social and political agendas. Their actions can range from website disruptions to exposing sensitive information.

[**Adrian Lamo**](https://en.wikipedia.org/wiki/Adrian_Lamo)

**Type:** Grey Hat

**Description:** Adrian Lamo gained notoriety for hacking into high-profile organizations and then responsibly disclosing the vulnerabilities he found. This blurred the lines between ethical and malicious hacking, earning him the "grey hat" classification.

[**Albert Gonzalez**](https://en.wikipedia.org/wiki/Albert_Gonzalez)

**Type:** Black Hat

**Description:** Albert Gonzalez orchestrated major data breaches, stealing millions of credit card numbers and causing significant financial damage. His actions represent the epitome of black hat hacking, motivated by personal gain.

[**Mathew Bevan**](https://en.wikipedia.org/wiki/Mathew_Bevan) **and** [**Richard Pryce**](https://toptensofall.wordpress.com/mathew-bevan-born-june-10-1974/)

**Type:** Grey Hat

**Description:** Bevan and Pryce hacked into military and government systems, often to expose security weaknesses. While their intentions weren't inherently malicious, their actions without proper authorization fall under the grey hat category.

[**Jeanson James Ancheta**](https://en.wikipedia.org/wiki/Jeanson_James_Ancheta)

**Type:** Black Hat

**Description:** Ancheta developed and distributed malware like botnets, harming individuals and organizations. His actions clearly demonstrate the malicious intent characteristic of black hat hackers.

[**Michael Calce**](https://en.wikipedia.org/wiki/Michael_Calce)

**Type:** Black Hat turned White Hat

**Description:** Calce launched high-profile DDoS attacks in his youth, classifying him as a black hat hacker. However, he later transitioned to ethical hacking, using his skills to help secure systems.

[**Kevin Poulsen**](https://en.wikipedia.org/wiki/Kevin_Poulsen)

**Type:** Black Hat

**Description:** Poulsen's hacking exploits involved unauthorized access to phone systems, government databases, and classified information. These actions exemplify black hat hacking motivated by personal gain and curiosity.

[**Jonathan James**](https://en.wikipedia.org/wiki/Jonathan_James)

**Type:** Grey Hat

**Description:** James hacked into government and corporate networks, raising awareness about security vulnerabilities. While his intentions leaned towards ethical hacking, his unauthorized actions fall under the gray hat category.

[**Astra**](https://qr.ae/pKdWDE)

**Type:** Black Hat

**Description:** The Astra Hacker, part of the Astra Group, is a mysterious individual known for involvement in various cyber activities, including data breaches and hacking incidents. Little is known about their specific classification, but their actions align with those of a "black hat" hacker