TASK 1 (TOP TEN HACKERS)

Name : Addada Bindu
Date : 26-08-23

Overview of the Assignment : 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.

1.Kevin Mitnick : Kevin Mitnick got his career start as a teen.In 1981, he was charged with stealing computer manuals from Pacific Bell. In 1982, he hacked the North American Defense Command (NORAD).In 1989, he hacked Digital Equipment Corporation's (DEC) network and made copies of their software. Because DEC was a leading computer manufacturer at the time, this act put Mitnick on the map.

He was later arrested, convicted and sent to prison. During his conditional release, he hacked Pacific Bell's voicemail systems.Throughout his hacking career, Mitnick never exploited the access and data he obtained.Due to his history of engaging in hacking activities for personal gain and malicious activities he falls into the black hat category but he can be categorized as a **gray hat hacker** as he ultimately went white hat ,using his expertise to help organizations enhance their security protocols.

2.Anonymous : Anonymous is a loosely organized collective of hacktivists known for their online protests and actions against perceived injustices.Operating as a decentralized group, they have conducted distributed denial of service (DDoS) attacks, defaced websites, and leaked sensitive information to draw attention to issues like censorship, privacy, and corruption. Anonymous is characterized by its use of Guy Fawkes masks and slogans.

While their actions can be controversial and illegal, their motivations often center around advocating for transparency and challenging oppressive systems. They fall under the category of "**hacktivists**," as they use hacking techniques to promote social and political causes.

3.Adrian Lamo : Adrian Lamo was a computer hacker and security analyst and also known as the “Homeless Hacker” . He is best known for turning in whistleblower Chelsea Manning, who had leaked classified information to WikiLeaks. Lamo was not driven by financial gain or malicious intent. Lamo's actions were controversial, as he faced criticism for betraying Manning's trust while also being credited with revealing potential security risks.

He seemed to fit the **"gray hat hacker”** category. This category includes hackers who don't strictly adhere to black or white hat distinctions, as they may engage in hacking activities without authorization, but often with some sense of ethics or a broader goal.

4.Albert Gonzalez : Albert Gonzalez was a hacker known for stealing credit card data. He's in the "black hat" category, which means he did bad stuff without permission. Gonzalez led a group that hacked into big companies' systems, taking millions of credit card numbers. They used these stolen cards to buy stuff and make money. But he got caught by law enforcement, and he ended up in prison.

His actions showed how serious cybercrime can be and how it can hurt a lot of people. Unlike some hackers, he wasn't trying to help or make things better – he was just after personal gain, which is why he's considered a **"black hat."**

5.Matthew Bevan and Richard Pryce : Matthew Bevan and Richard Pryce, also known as "Kuji" and "Datastream Cowboy," were hackers during the 1990s. They can be categorized as **"gray hat"** hackers, operating between ethical and malicious boundaries. They accessed sensitive systems, prompting debates over their intentions—whether driven by curiosity or mischief.

Their actions unveiled vulnerabilities, especially in military networks, raising concerns about cybersecurity. Despite not causing major harm, their activities underscored the potential risks of unauthorized intrusion. The duo remains emblematic of hackers navigating the fine line between exploration and disruption in the evolving digital landscape.

6.Jeanson James Ancheta: Jeanson James Ancheta was a notorious hacker and cybercriminal known for his involvement in creating and spreading malicious software, particularly botnets. He falls firmly into the **"black hat"** hacker category, as his actions were driven by malicious intent and personal gain.

Ancheta specialized in controlling networks of compromised computers, or botnets, which he used for various criminal activities such as sending spam emails, stealing sensitive information, and launching cyberattacks. His activities caused widespread damage, disruption, and financial losses to individuals and organizations.

7.Michael Calce: Michael Calce, also known by his online handle "Mafiaboy," is a Canadian hacker who gained infamy for launching a series of high-profile distributed denial of service (DDoS) attacks in the late 1990s. He carried out these attacks at a young age, causing widespread disruption to major websites, including Yahoo!, Amazon, and CNN.

Calce's actions had a significant impact on the internet and brought attention to the vulnerabilities of online systems.Calce's motivations were not financially driven; rather, he sought recognition and notoriety within the hacking community. His actions classified him as a **"black hat"** hacker because of engaging in unauthorized and malicious activities.

8.Kevin Poulsen : Kevin Poulsen, also known as "Dark Dante," is a former hacker He gained notoriety in the late 1980s and early 1990s for manipulating phone systems and winning radio contests through hacking. Poulsen's actions led to legal issues, but he later used his skills for positive contributions, covering technology and cybersecurity as a journalist.

He can be categorized as a **"Gray hat hacker** " because of his transition from a hacker to becoming a respected journalist and cybersecurity expert .His story illustrates the potential for personal growth and redemption within the hacking community, highlighting the complexities of the hacker's world and the possibility of channeling skills into legitimate and ethical pursuits.

9.Jonathan James : Jonathan James, also known as "cOmrade," was a young American hacker who was active in the early 2000s .His hacking allowed him to access over 3,000 messages from government employees, usernames, passwords and other sensitive data. In 2007, TJX, a department store, was hacked and many customer's private information were compromised.

At the age of 16, he became the first juvenile to be imprisoned for hacking in the United States. Tragically, James took his own life at the age of 24. His story highlights the legal and personal consequences associated with malicious hacking, underscoring the need for understanding and addressing the complexities of the hacking world.He can be categorized as a **"Black hat hacker"** due to his engagement in unauthorized and malicious activities, gaining notoriety for his cybercrimes

10.ASTRA : He was identified as a 58-year-old Greek mathematician. Reportedly, he had been hacking into the Dassault Group, for almost half a decade. During that time, he stole cutting edge weapons technology software and data which he then sold to 250 individuals around the world. His hacking cost the Dassault Group $360 million in damages.

No one knows why his complete identity has never been revealed, but the word 'ASTRA' is a Sanskrit word for 'weapon'.He can be categorized as a **"Black hat hacker"** due to his unauthorized access to the Dassault servers and selling the information for his financial gain.