* TASK 1 -TOP 10 HACKERS

23-8-23 wednesday

Top 10 most notorious hackers in the world

**1-kevin mitnik- is top most hacker he is not a active hacker he worked in late 20,Mitnick was known for his high level of technical expertise in computer systems and telecommunications. He was skilled in social engineering techniques, which involve manipulating people into divulging confidential information.**

**He fits into black hat hacker  category *but Although Mitnick ultimately went white hat, he may be part of the both-hats grey area.***

2-Anonymous-they refers to a hidden hiearchy they worked as groups and they began in 2003 on 4chan message boards.they groups form little organization and major focus is on social justice they are impossible to catch up due to lack of their real hierarchy.

They are not defined into any hat category they can be called as hacktivism or if we have to categorize them we can also call them grey hat hacker as they do both

3-Adrian lamo-Lamo was often referred to as a "gray hat" hacker due to his actions falling between the realms of black hat (malicious hacking) and white hat (ethical hacking).in 2001 a 20 year old adrian hacked yahoo and add his own quote.One of Lamo's most notable actions was his involvement in the arrest of Chelsea Manning (formerly known as Bradley Manning), a United States Army intelligence analyst who leaked classified documents to WikiLeaks. Manning contacted Lamo in 2010 and confided in him about the leaks.he passed away at age of 37

4-Albert gonzalez-was a notorious hacker who was involved in several high-profile cybercrime activities. He is often associated with the largest credit card data breaches in history.

Gonzalez led a group of hackers responsible for stealing credit card data from major retailers, including TJX Companies (which owns TJ Maxx and Marshalls) and Heartland Payment Systems. These breaches resulted in the theft of tens of millions of credit card numbers and caused significant financial losses for individuals and companies.

Albert Gonzalez is generally classified as a "black hat" hacker due to his involvement in malicious and illegal cyber activities, specifically cybercrimes such as credit card data theft and subsequent fraud.

5-**Matthew Bevan and Richard Pryce-Matthew Bevan and Richard Pryce are a team of British hackers who hacked into multiple military networks in 1996, including Griffiss Air Force Base, the Defense Information System Agency and the Korean Atomic Research Institute (KARI). Bevan (Kuji) and Pryce (Datastream Cowboy) have been accused of nearly starting a third world war after they dumped KARI research onto American military systems.They demonstrated that even militiary networks are vulnerable.**

**The hacking activities attributed to Bevan and Pryce were not solely malicious or criminal in nature, as their actions were sometimes driven by curiosity and the desire to explore and understand computer systems. However, their actions also involved unauthorized access to computer systems and networks, which is a characteristic of black hat hacking.**

**The "gray hat" classification acknowledges that their motivations and activities might not fit neatly into the white or black hat categories. They were neither purely malicious nor strictly ethical hackers. Instead, their actions had shades of both, making their classification complex and open to interpretation.**

**6-Jeanson James Ancheta**

**Ancheta was involved in creating and controlling a network of compromised computers, known as a "botnet," for financial gain.Jeanson James Ancheta's activities highlight the criminal exploitation of compromised computers for financial gain. His case underscores the importance of cybersecurity measures to prevent the creation and control of botnets, as well as the legal consequences that cybercriminals can face when caught.**

**Jeanson James Ancheta is typically classified as a "black hat" hacker due to his involvement in various cybercriminal activities that involved unauthorized access to computers, creation and control of botnets, and distribution of malware for financial gain.**

**7-Michael Calce**

**Michael Calce, also known by his online handle "Mafiaboy," is a Canadian hacker who gained notoriety for launching a series of high-profile distributed denial-of-service (DDoS) attacks in the late 1990s. These attacks targeted several prominent websites, including major e-commerce and online platforms.Mafiaboy's most notorious attack occurred in 2000 when he launched a DDoS attack against several high-profile websites, including Yahoo!, Amazon, eBay, and CNN. These attacks overwhelmed the targeted websites' servers with a flood of traffic, causing them to become inaccessible to users.**

**Mafiaboy's activities fall under the category of "black hat" hacking, as he engaged in malicious activities that disrupted online services, caused financial losses to businesses, and impacted the experiences of countless internet users.**

**8-Kevin Poulsen- also known by his online handle "Dark Dante," is a former black hat hacker who gained notoriety in the 1980s and 1990s for his hacking activities. He was involved in several hacking incidents, one of which was particularly significant and led to his arrest.**

**Poulsen's most notable action was hacking into the telephone lines of a Los Angeles radio station, KIIS-FM, in 1990. He manipulated the station's phone system to ensure that he would be the 102nd caller in a contest, winning a Porsche 944 S2.**

**Poulsen's transition from black hat hacking to ethical cybersecurity work makes his story unique. He is often seen as an example of someone who managed to transform their skills and experiences for positive contributions to the field.**

**9-Jonathan James-, also known by his online handle "cOmrade," was a hacker known for his involvement in various cybercriminal activities during the late 1990s and early 2000s. He gained attention for being one of the youngest hackers to be arrested for cybercrimes.NASA hack.**

**His actions are generally categorized as "black hat" hacking due to their malicious nature and the legal ramifications they carried. His case also underscores the importance of addressing mental health issues and providing support to individuals, especially young ones, who may be drawn into cybercriminal activities.**

**10-ASTRA-his hacker differs from the others on this list in that he has never been publicly identified. However, according to THE daily mail some information has been released about ASTRA. Namely that he was apprehended by authorities in 2008, and at that time 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.**

**It can classified under black hat as it uses illegal activity for weapon sell.**