Task-1

Date- 23/8/23

Top 10 most notorious hackers of all time in this internet world

1. Kevin Mitnik-

Kevin David Mitnick (August 6, 1963 – July 16, 2023) was an American computer security consultant, author, and convicted hacker.
He is best known for his high-profile 1995 arrest and five years in prison for various computer and communications-related crimes. Mitnick's pursuit, arrest, trial, and sentence along with the associated journalism, books, and films were all controversial. After his release from prison, he ran his own security firm, Mitnick Security Consulting, LLC, and was also involved with other computer security businesses.
Kevin Mitnick is a former black hat hacker who later transformed into a white hat hacker. So we can call him a grey hat hacker. In his early years, he engaged in various cybercrimes, including hacking into computer systems, stealing sensitive information, and evading law enforcement agencies. His actions as a black hat hacker led to his arrest and imprisonment.

2. Anonymous-

Anonymous is a decentralized international activist and hacktivist collective and movement primarily known for its various cyberattacks against several governments, government institutions and government agencies, corporations and the Church of Scientology.
Dozens of people have been arrested for involvement in Anonymous cyberattacks in countries including the United States, the United Kingdom, Australia, the Netherlands, South Africa, Spain, India, and Turkey.
Anonymous originated in 2003 on the imageboard 4chan representing the concept of many online and offline community users simultaneously existing as an "anarchic", digitized "global brain" or "hivemind".
Anonymous' media profile diminished by 2018, but the group re-emerged in 2020 to support the George Floyd protests and other causes.

A grey hat hacker their activities depend on the specific actions and goals of the individuals or groups involved at any given time.

3. Adrian Lamo-

Adrián Alfonso Lamo Atwood (February 20, 1981 – March 14, 2018) was an American threat analyst[] and hacker. Lamo first gained media attention for breaking into several high-profile computer networks, including those of *The New York Times*, Yahoo!, and Microsoft, culminating in his 2003 arrest.
Lamo was best known for reporting U.S. soldier Chelsea Manning to Army criminal investigators in 2010 for leaking hundreds of thousands of sensitive U.S. government

documents to WikiLeaks. Lamo died on March 14, 2018, at the age of 37. Lamo was a grey hat hacker.

4. Albert Gonzalez-

Albert Gonzalez (born 1981) is an American computer hacker, computer criminal and police informer, who is accused of masterminding the combined credit card theft and subsequent reselling of more than 170 million card and ATM numbers from 2005 to 2007, the biggest such fraud in history. Gonzalez and his accomplices used SQL injection to deploy backdoors on several corporate systems in order to launch packet sniffing (specifically, ARP Spoofing) attacks which allowed him to steal computer data from internal corporate networks.

Albert Gonzalez was a black hat hacker. He is best known for his involvement in several high-profile cybercrimes, including one of the largest credit card thefts in history.

5. Jeanson James Ancheta-

On May 9, 2006, Jeanson James Ancheta (born April 26, 1985) became the first person to be charged for controlling large numbers of hijacked computers or botnets.

Ancheta was going to Downey High School in Downey, California until 2001 when he dropped out of school. He later entered an alternative program for students with academic or behavioral problems. He worked at an Internet cafe and according to his family wanted to join the military reserves. Around June 2004 he started to work with botnets after discovering rxbot, a common computer worm that could spread his net of infected computers.

In November 2005 he was captured in an elaborate sting operation when FBI agents lured him to their local office on the pretext of collecting computer equipment.

Jeanson James Ancheta was not a "white hat" hacker (ethical hacker) who works to improve computer security or protect systems, nor was he a "grey hat" hacker who operates in a morally ambiguous space. He was a "black hat" hacker or cybercriminal who engaged in illegal and malicious activities, particularly in creating and operating botnets for nefarious purposes. So, in the context of hacker types, he would be categorized as a "black hat" hacker.

6. Michael Calce-

Michael Calce, also known by his online handle "Mafiaboy," was a black hat hacker. In 2000, when he was just a teenager, he launched a series of high-profile distributed denial-of-service (DDoS) attacks against various major websites, including Yahoo!, Amazon, eBay, and CNN. These attacks caused significant disruption and garnered significant media attention.
Calce's actions were malicious and illegal, as DDoS attacks involve overwhelming websites with traffic to make them inaccessible. He was eventually arrested and convicted for his cybercrimes. After serving his sentence, Calce has since expressed remorse for his actions and has spoken about his experiences to raise awareness about cybersecurity and hacking ethics.

He also launched a series of failed simultaneous attacks against nine of the thirteen root name servers.

7. Kevin Poulsen-

Kevin Lee Poulsen is a well-known figure in the realm of computer security and hacking. He gained prominence for his hacking activities in the late 1980s and early 1990s, and later transitioned to a career in journalism and writing. Poulsen's story is often seen as a transformation from a black-hat hacker to an influential journalist covering cybersecurity and technology.
In the late 1980s, Poulsen was involved in various hacking activities, including breaking into computer systems and manipulating phone lines. He notably gained attention for hacking into radio station phone lines to ensure he would be the winning caller for a contest, winning a Porsche 944 S2. This led to his arrest and subsequent conviction.
Kevin Poulsen, also known by his online handle "Dark Dante," was a black hat hacker in his earlier years.
So, similar to Kevin Mitnick, Kevin Poulsen transitioned from being a black hat hacker to a white hat hacker, using his expertise for legal and ethical purposes in the realm of computer security and journalism. He must be a grey hat hacker.

8. Jonathan Joseph James-

Jonathan Joseph James, often referred to as "c0mrade," was a notable figure in the hacking community. He gained attention for his hacking activities during the late 1990s and early 2000s. James was involved in a high-profile case that attracted significant media coverage due to its implications.

In 2000, at the age of 15, Jonathan James became known for hacking into various computer systems, including those of NASA and the U.S. Department of Defense. His most significant intrusion was into NASA's computer systems, where he accessed sensitive information related to the International Space Station. James claimed that his intention was to expose security vulnerabilities rather than maliciously exploit the data.

However, his actions led to an investigation by law enforcement, and he was eventually arrested and charged with multiple counts of computer intrusion and related offenses. In 2000, he pleaded guilty and was sentenced to house arrest and probation.
James' actions were illegal and malicious, falling into the category of black hat hacking. His hacking activities eventually led to his arrest and legal troubles. Unfortunately, in 2008, Jonathan Joseph James took his own life at the age of 25.

9. Astra-

Astra is the pseudonym of a French hacker who was active in the early 2010s. He was known for hacking into high-profile websites, including the French television network TF1, the French Ministry of Defense, and the FBI's Virtual Academy. In 2012, Astra was arrested by French authorities and later convicted of computer-related crimes. He was sentenced to five years in prison, but was released on parole after serving only two years. It can be classified under black hat as it uses illegal activity for weapon sell.

10. Mathew Bevan and Richard Pryce-

They were 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).
In 1996 Mathew was arrested for hacking into secure U.S. Government networks under the handle Kuji.
Pryce had been charged in June 1995, 13 months after his arrest. With 12 offenses under section 1 of the computer misuse act and conspiracy three days before Mathew's arrest.
They both are grey hat hackers.