Task 1- Hackers

Kevin Mitnick:

Kevin Mitnick, a prominent figure in the history of computer hacking in the United States, began his professional life when he was just a teenager. In 1981, he was accused of stealing computer manuals from Pacific Bell and was arrested for the crime. His accomplishment of hacking the North American Defence Command (NORAD) in 1982 served as the impetus for the film War Games, which was released in 1983. In 1989, he broke into the network of Digital Equipment Corporation (DEC) and stole copies of the company's software. This act catapulted Mitnick to prominence at a time when DEC was the preeminent computer manufacturer in the industry. He was eventually apprehended, tried, and sentenced to time behind bars. During the time that he was out on conditional release, he broke into the voicemail systems of Pacific Bell.

Throughout his entire career as a hacker, Mitnick never made use of the access or data he obtained illegally. It's common knowledge that he once took complete command of Pacific Bell's network for no other reason than to demonstrate that it was possible. In connection with the incident involving Pacific Bell, a warrant was issued for his arrest; however, Mitnick evaded capture and remained in hiding for over two years. After being apprehended, he was sentenced to multiple terms of imprisonment for the crimes of wire fraud and computer fraud.

Even though Mitnick eventually wore the white hat, he may still fall into the grey area of wearing both hats. According to Wired, in 2014 he established "Mitnick's Absolute Zero Day Exploit Exchange," a platform that offers critical software vulnerabilities that have not been patched to whoever places the highest bid.

Type of Hacker: Kevin Mitnick is a former hacker turned cybersecurity consultant. He was primarily known as a Black Hat Hacker before his capture in 1995. He engaged in various cybercrimes, including hacking into computer networks, stealing sensitive information, and wiretapping.

Anonymous (Collective):

In 2003, Anonymous got its start in an unnamed forum on the message boards of the website 4chan. The group is not very well organised, and its attention is only tangentially concentrated on the idea of social justice. For instance, in 2008, the organisation had a disagreement with the Church of Scientology and began to disable its websites. This had a negative impact on the websites' search rankings in Google, and the organization's fax machines were inundated with images that were all black. When a group of "Anons" marched past Scientology centres around the world in March 2008, they did so while wearing the now-famous Guy Fawkes mask. According to an article that was published in The New Yorker, despite the fact that the FBI and other law enforcement agencies have been successful in locating some of the group's more active members, the absence of any real hierarchy makes it nearly impossible to identify or eradicate Anonymous as a whole.

Type of Hackers: Anonymous is a loosely organized group of hackers, hacktivists, and activists. They can be considered Hacktivists or Gray Hat Hackers, as their actions range from exposing government or corporate wrongdoing to engaging in distributed denial of service (DDoS) attacks.

Adrian Lamo:

In 2001, a young man named Adrian Lamo, then 20 years old, used an unprotected content management tool at Yahoo to alter a Reuters article and add a fake quote that was supposed to be attributed to a previous Attorney General named John Ashcroft. Lamo frequently broke into computer systems and then informed both the press and the people he had hacked. In certain situations, he would assist in cleaning up the mess in order to improve their safety. However, as Wired points out, Lamo went too far in 2002 when he hacked into the intranet of The New York Times, added himself to the list of expert sources, and started conducting research on prominent members of the public. Lamo's actions were inappropriate. Lamo was given the nickname "The Homeless Hacker" due to the fact that he frequently went about his days carrying little more than a backpack and frequently did not have a permanent address.

Type of Hacker: Adrian Lamo was known as a Gray Hat Hacker. He was involved in various activities, including ethical hacking and exposing security vulnerabilities. Lamo gained notoriety for turning in Chelsea Manning (formerly Bradley Manning), who had leaked classified information to WikiLeaks.

Albert Gonzalez:

Gonzalez, also known as "soupnazi," is said to have gotten his start as the "troubled pack leader of computer nerds" at his Miami high school, as reported by the New York Daily News. After some time, he started using the illicit trade website Shadowcrew.com and quickly rose through the ranks to become one of the site's most respected hackers and moderators. At the age of 22, Gonzalez was taken into custody in New York on charges of debit card fraud related to the theft of data from millions of card accounts. In order to avoid serving time in prison, he turned himself in to the Secret Service as an informant and ultimately assisted in the prosecution of dozens of members of Shadowcrew.

Gonzalez did not stop his involvement in illegal activities even while he was working as a paid informant. Gonzalez, along with a group of confederates, was responsible for the theft of more than 180 million payment card accounts belonging to various businesses, such as OfficeMax, Dave and Buster's, and Boston Market. According to an article published in the New York Times Magazine, Gonzalez's attack on the American retailer TJX in 2005 was the first serial data breach of credit information. This infamous hacker and his team created back doors in several corporate networks by using a technique known as basic SQL injection. They used these back doors to steal an estimated $256 million from TJX alone. In 2015, during Gonzalez's sentencing, the federal prosecutor described the human victimisation that Gonzalez caused as "unparalleled."

Type of Hacker: Albert Gonzalez was a notorious Black Hat Hacker involved in credit card and identity theft. He orchestrated the infamous Heartland Payment Systems data breach and is considered one of the most significant cybercriminals in recent history.

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. Bevan claims he was looking to prove a UFO conspiracy theory, and according to the BBC, his case bears resemblance to that of Gary McKinnon. Malicious intent or not, Bevan and Pryce demonstrated that even military networks are vulnerable.

Type of Hackers: Matthew Bevan and Richard Pryce were known as Hacktivists. They gained attention for hacking into U.S. military computers in the late 1990s as a form of protest against nuclear weapons testing.

Jeanson James Ancheta:

Jeanson James Ancheta had no interest in hacking systems for credit card data or crashing networks to deliver social justice. Instead, Ancheta was curious about the use of bots—software-based robots that can infect and ultimately control computer systems. Using a series of large-scale "botnets," he was able to compromise more than 400,000 computers in 2005. According to Ars Technica, he then rented these machines out to advertising companies and was also paid to directly install bots or adware on specific systems. Ancheta was sentenced to 57 months in prison. This was the first time a hacker was sent to jail for the use of botnet technology.

Type of Hacker: Jeanson James Ancheta was a Black Hat Hacker who created a network of compromised computers (a botnet) and used it to launch various attacks and distribute malware, making him a Botnet Operator.

Michael Calce (aka MafiaBoy):
In February 2000, 15-year-old Michael Calce, also known as "Mafiaboy," discovered how to take over networks of university computers. He used their combined resources to disrupt the number-one search engine at the time: Yahoo. Within one week, he'd also brought down Dell, eBay, CNN and Amazon using a distributed-denial-of-service (DDoS) attack that overwhelmed corporate servers and caused their websites to crash. Calce's wake-up call was perhaps the most jarring for cyber crime investors and internet proponents. If the biggest websites in the world—valued at over $1 billion—could be so easily sidelined, was any online data truly safe? It's not an exaggeration to say that the development of cyber crime legislation suddenly became a top government priority thanks to Calce's hack.

Type of Hacker: Michael Calce was a Black Hat Hacker known for launching large-scale DDoS attacks in the early 2000s. He targeted high-profile websites, including Yahoo!, eBay, and Amazon.

Kevin Poulsen:
In 1983, a 17-year-old Poulsen, using the alias Dark Dante, hacked into ARPANET, the Pentagon’s computer network. Although he was quickly caught, the government decided not to prosecute Poulsen, who was a minor at the time. Instead, he was let off with a warning.

Poulsen didn’t heed this warning and continued hacking. In 1988, Poulsen hacked a federal computer and dug into files pertaining to the deposed president of the Philippines, Ferdinand Marcos. When discovered by authorities, Poulsen went underground. While he was on the run, Poulsen kept busy, hacking government files and revealing secrets. According to his own website, in 1990, he hacked a radio station contest and ensured that he was the 102nd caller, winning a brand new Porsche, a vacation, and $20,000.

Poulsen was soon arrested and barred from using a computer for three years. He has since converted to white hat hacking and journalism, writing about cyber security and web-related socio-political causes for Wired, The Daily Beast and his own blog Threat Level. Paulson also teamed with other leading hackers to work on various projects dedicated to social justice and freedom of information. Perhaps most notably, working with Adam Swartz and Jim Dolan to develop the open-source software SecureDrop, initially known as DeadDrop. Eventually, Poulsen turned over the platform, which enabled secure communication between journalists and sources, to the Freedom of Press Foundation.

Type of Hacker: Kevin Poulsen was a Black Hat Hacker who gained notoriety for hacking into phone systems and rigging radio station contests. After serving time in prison, he became a respected journalist specializing in cybersecurity.

Jonathan James:
Using the alias cOmrade, Jonathan James hacked several companies. According to the New York Times, what really earned James attention was his hack into the computers of the United States Department of Defense. Even more impressive was the fact that James was only 15 at the time. In an interview with PC Mag, James admitted that he was partly inspired by the book The Cuckoo's Egg, which details the hunt for a computer hacker in the 1980s. His hacking allowed him to access over 3,000 messages from government employees, usernames, passwords and other sensitive data.

James was arrested in 2000 and was sentenced to a six months house arrest and banned from recreational computer use. However, a probation violation caused him to serve six months in jail. Jonathan James became the youngest person to be convicted of violating cyber crime laws. In 2007, TJX, a department store, was hacked and many customer's private information were compromised. Despite a lack of evidence, authorities suspect that James may have been involved.

In 2008, James committed suicide by gunshot. According to the Daily Mail, his suicide note stated, “I have no faith in the 'justice' system. Perhaps my actions today, and this letter, will send a stronger message to the public. Either way, I have lost control over this situation, and this is my only way to regain control.”

Type of Hacker: Jonathan James was a Black Hat Hacker who, at a young age, hacked into various high-profile systems, including NASA's. He was known for his technical skills but tragically took his own life in 2008.

ASTRA (Pseudonym):
This hacker is distinct from the others on this list in that he has never been outed to the general public in any capacity. On the other hand, the Daily Mail reports that certain information regarding ASTRA has become public. In particular, the fact that he was apprehended by authorities in 2008 and identified as a 58-year-old Greek mathematician at the time of his capture. According to reports, he had been breaking into the computers of the Dassault Group for nearly half a decade. During that time, he was dishonest and stole data and software related to cutting-edge weaponry technology, which he later sold to 250 different people in different parts of the world. Damages totaling 360 million euros were incurred by the Dassault Group as a result of his hacking. The reason why his full identity has never been disclosed is a mystery to everyone, but the word "astra" can be translated as "weapon" in Sanskrit.

Type of Hacker: ASTRA was a Black Hat Hacker who targeted online gaming companies, particularly in the MMO (Massively Multiplayer Online) gaming community. ASTRA stole in-game items and currency for profit.