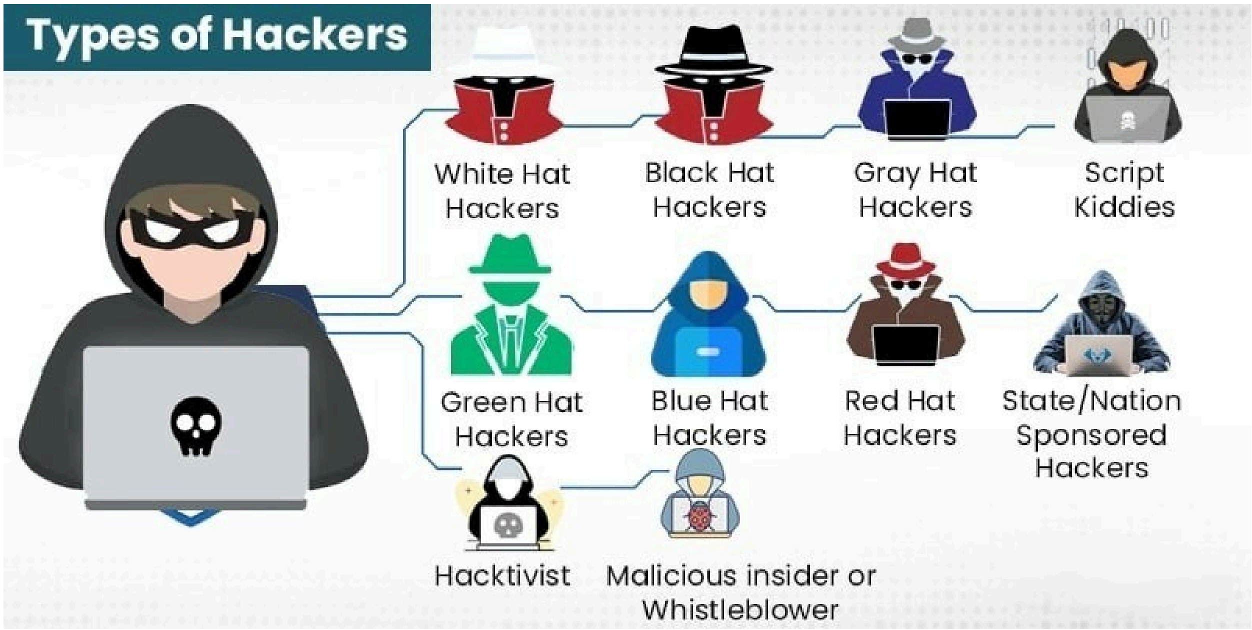
Cyber Security Honours : Assignment 1
Name : Ritesh Jha

Class : SY_IT (B2)
Roll No : 16010423076

1)Types of Hackers



1. White Hat Hackers:

Objective: Security improvement
Methods: Ethical hacking, penetration testing
Also known as ethical hackers, white hats are security professionals who make it possible for recognition of vulnerabilities & their fixation. They are legally involved & many times collaborate with different organizations in the attempt to enhance their cybersecurity posture.

2. Black Hat Hackers:

Objective: personal benefit or malicious purpose
Methods: malware distribution, data theft, system infiltration.
Black hats work illegally & they exploit vulnerabilities for financial gains, data theft, or any other dreadful activities. Quite often they are involved in cybercrime activities, which include identity theft, ransomware attacks, or unauthorized system breaches.

3. Gray Hat Hackers:

Objective: Often mixed - might look for attention or monetary gain.
Methods: Unapproved penetration testing, vulnerability disclosure.
Gray hats fall in between white hats & black hats. They might exploit security holes, but they don't have any malicious intent, yet they have no permission. They may inform an organization about their flaws after revealing the security holes to them for payment or credit, although this also is legally grey sometimes.

4. Script Kiddies:

Objective: Usually curiosity-driven or mischief-driven.
Methods: Running pre-written scripts & tools.
Script kiddies are unprofessional hackers who lean on already developed tools or scripts for attacks. They normally have no deep technical background, such hackers act mainly out of a desire to impress other people or make minimal disruptions.

5. Hacktivists:

Objective: Political or social activism.
Methods: Defacement of websites, leakage of information, attacks of DDoS.
Hacktivists are hackers who use hacking techniques to advance political agendas or social causes. Most of the time, they intend to increase awareness, protest against some perceived injustices, or disrupt some organizations/government they feel are against them.

6. Nation-State Hackers:

Objective: Espionage, sabotage, information war.
Methods: Advanced persistent threats, cyber espionage.
The hackers work for some government agencies or military organizations. They conduct cyber espionage, sabotage & information war against other nations or organizations. Most of their activities are very sophisticated & well-financed.

7. Insider Threats:

Objective: May include financial gain, revenge, or espionage.
Methods: Abusing the access privileges by leaking sensitive information
Insiders refer to individuals working in an organization who use their access to the system & data for personal benefit. They may be current employees, former employees, contractors, or even business partners who use the position against the organization for personal benefits.

2)Denial of Service attacks & the preventive measures taken later on

A Brief History

Denial of Service attacks have been around since the early days of the Web. Among the most famous & one of the oldest takes place in 1996. One of the oldest Internet Service Providers, Panix, had its service stop dead for days after falling victim to this SYN flood based DoS attack. As the Web developed, so did DoS attacks in complexity & size.

Recent DoS Attacks

1. **Cloudfare - 2023 (Reference)**

Incident: Cloudflare, one of the largest web infrastructure & security companies, called an attack in March 2023 that was nearly the biggest DDoS attack ever recorded. This attack peaked at 71 million requests per second against an unnamed cryptocurrency platform. What made this huge DDoS attack so particularly hard to mitigate was that it used HTTP/2 multiplexing to set a bigger punch.
Response: More sophisticated algorithms of traffic analysis were implemented, which enabled fast identification & filtering of ill-intentional requests. For improvement in traffic handling, mainly at the HTTP/2 level, areas such as HTTP/2 handling & the rate limiting functionality were the focus for Cloudflare. Not only that, but their network capacity & edge computing also increased to be able to digest & spread out such large volumes of attacks. It also shared, with the wider tech community, detailed insights into the attack methodology to help drive collaborative defense strategies across the industry.

2. **Amazon Web Services - 2020 (Reference)**

Incident: AWS experienced perhaps the world's largest DDoS attack to date, measuring 2.3 terabits per second. The target of the attack was an unidentified AWS customer & attackers used a method known as the CLDAP reflection.
Response: AWS had turned on its Shield Advanced DDoS protection service, which throttled the attack with minimal disruption to its service. Following this, AWS invested in additional DDoS mitigation infrastructure upgrades & enhanced its automated response capabilities, besides expanding its threat intelligence network, in order to keep up with evolving attack techniques.

3. **GitHub - 2018 (Reference)**

Incident: GitHub was hit with the largest-ever recorded DDoS, peaking at 1.35 terabits per second. Attackers targeted Memcached servers for amplification.
Response: It quickly turned on Akamai Prolexic, which reroutes traffic & soaks up evil floods. The GitHub incident response team worked to strengthen the resilience of its network infrastructure to help deal with such high volumes better in the future.