CYBER SECURITY

TYPES OF HACKERS:

1. ***Black Hats Hackers:*** *Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes. This category of hacker is often involved with criminal activities. They are also known as crackers.*
   Example *: harvest passwords and banking information or surreptitiously take over the computer and use it to launch attacks on others.*
2. ***White Hats Hackers:*** *White hat hackers, also referred to as ethical hackers are the cybersecurity experts who help the govt. and organizations by performing penetration testing and identifying loopholes in their cybersecurity. They even do other methodologies and ensure protection from black hat hackers and other malicious cyber crimes. Simply stated, these are the right people that are on your side. they're going to hack into your system with the great intention of finding vulnerabilities and help you remove virus and malware from our system.*
   Example: *who do the work in company ,and report the bugs.*
3. ***Gray Hats Hackers****: Gray hat hackers fall somewhere in between white hat and black hat hackers. While they'll not*

use their skills for personal gain, they can, however, have both good and bad intentions.

***Example:** A hacker who hacks into a corporation and finds some vulnerability may leak it over the web or inform the organization about it. It all depends upon the hacker. Nevertheless, as soon as hackers use their hacking skills for personal gain they become black hat hackers. there's a fine line between these two. So, let me make it simple for you. Because a gray hat hacker doesn't use his skills for personal gain, he's not a black hat hacker. Also, because he's not legally authorized to hack the organization's cyber security, he can't be considered a white hat either.*

4. ***Blue Hats Hackers:** These are another form of novice hackers very similar to script kiddies whose main agenda is to require revenge on anyone who makes them angry. they need no desire for learning and should use simple cyber attacks.*

   ***Example :** flooding your IP with overloaded packets which can result in DoS attacks. A script kiddie with a revengeful agenda are often considered a blue hat hacker.*
5. ***Suicide Hackers:** Suicide hackers are individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment. They are similar to suicide bombers.*

Example : *who sacrifice their life for an attack and are thus not concerned with the consequences of their actions.*

6. ***Script Kiddies Hackers:*** *A derogatory term often used by amateur hackers who don't care much about the coding skills. These hackers usually download tools or use available hacking codes written by other developers and hackers. Their primary purpose is usually to impress their friends or gain attention. However, they don't care about learning. By using off-the-shelf codes and tools, these hackers may launch some attacks without bothering for the quality of the attack.*

   Example : *Commponest cyber attacks by script kiddies might include DoS and DDoS attacks.*

7. ***Malicious Insider :*** *A malicious insider(or a whistle blower) could also be an employee with a grudge or a strategic employee compromised or hired by rivals to garner trade secrets of their opponents to remain on top of their game. These hackers may take privilege from their quick access to information and their role within the corporate to hack the system**.***

   Example*: Adware. Adware serves unwanted or malicious advertising. ...Fileless Malware. ...Viruses. ...Worms. ...Trojans. ...Bots. ...*

8. ***Red Hat Hackers:****Red Hat Hackers have an agenda almost like white hat hackers which in simple words is halting the*

acts of Black hat hackers. However, there's a serious difference within the way they operate. they're ruthless when it involves dealing with black hat hackers. instead of reporting a malicious attack, they believe taking down the black hat hacker completely. Red hat hacker will launch a series of aggressive cyber attacks and malware on the hacker that the hacker may also have to replace the entire system.

Example : who workin company but work for company**.**

9. **State/Nation Sponsored Hackers:**State or Nation sponsored hackers are those that have been employed by their state or nation's government to snoop in and penetrate through full security to realize tip from other governments to stay at the highest online. they have an endless budget and extremely advanced tool.

   Example : disposal to target individuals, companies or rival nations.

10. **Hacktivist Hackers:** Hacktivist is when hackers break into government or corporate computer systems as an act of protest. Hacktivists use hacking to increase a political agenda by hacking, especially by defacing or disabling websites.

    Example : Common hacktivist targets include government agencies, multinational corporations, or any other entity that they perceive as a threat. It remains a fact, however, *that gaining unauthorized access is a crime, irrespective of their intentions.*

11. ***Elite Hacker**: Elite hacker is a social designation indebted to hackers who are most skilled in hacking. They have expert skills to break into information systems and pull in data and information from the same with ease. Elite hackers can use their expert skills in both white hat hacking and black hat hacking*

    Example :** lurking on a system for months and months without getting found out**.

12. ***Crypto jacker:** Cryptojacking is a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency. Like many forms of cybercrime, the motive is profit, but unlike other threats, it is designed to stay completely hidden from the victim.*

    ***Example :** exploit a device's computing power without the owner's authorization.*

13. ***Gaming hacker:** Is the process of editing the game's source code in order to gain an advantage.*

    ***Example:** you may hack a game to gain more health or lives. Hacking a game normally requires a sufficient understanding of how the game is built and knowing what you need to edit.*

14. ***Green Hat**: Hackers-in-Training: A green hat hacker is someone who is new to the hacking world but is intently focused on increasing their cyberattack skills. They primarily focus on gaining knowledge on how to perform cyberattacks on the same level as their black hat counterparts. Their main intent is to eventually evolve into a full-fledged hacker, so they spend their time looking for learning opportunities from more experienced hackers.*
***Example :** playing with various malware and attack techniques.*

15. ***Hacktivists:** Politically Motivated Hackers: A hacktivist is someone who hacks into government networks and systems to draw attention to a political or social cause—hence why the name "hacktivist" is a play on the word "activist." They use hacking as a form of protest, retrieving sensitive government information, which is used for political or social purposes.*

***Example :** To shed light on an alarming social or political cause or to make a political or ideological statement.*

16. Botnets:** Large-Scale Hackers: Botnet hackers are malware coders who create bots to perform high-volume attacks across as many devices as possible, typically targeting routers, cameras and other Internet of Things (IoT) devices. The bots operate by looking for unsecured devices (or devices who still have their default login credentials intact) to plant themselves in. Botnets can be used directly by the hacker **.

Example: *GameOver, Zeus****.***

17. ***Cyber terrorist:****To create political disruption.These are extremely dangerous because they are politically motivated and can easily instigate violence against non-combatant targets.*

    Example: *Disruption of major websites. The intent here is to create public inconvenience or stop traffic to websites containing content the hackers disagree with.*

18. ***Sponsored Hacker:****To create a warfare.These hackers are usually deployed by a country to spy on other countries and attempt to forcefully obtain trade secrets and information about defence systems with the goal of creating a war-like scenario.*

    Example : *Attacking critical infrastructure and companies: This can damage the defender and greatly diminish their defensive capabilities****.***

19. ***Whistle –Blower hacker :*** *These hackers exist with in organizations and leak sensitive information to the outside world,by staying within the umbrella of the organization or even within a country*

    Example : *criminal activity, such as theft or unethical or unjust behaviour in the workplace, including racist, sexist or homophobic behaviour****.***

20. ***SOCIAL ENGINEERING HACKER:*** *To manipulate people and system .These types of hackers aim to manipulate*

people and systems through psychological instigation to get them to divulge proprietary information

EXAMPLE : *Phishing. As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims.*

21. ***Insider hacker:****Insiders who crack the system to cause damage are often angered employees who have been fired from their jobs and have the computer skills to cause damage.*

Example : *plant logic bombs that do damage after the employees leave****.***

22. ***Ethical hacker :****An ethical hacker, also referred to as a white hat hacker, is an information security (infosec) expert who penetrates a computer system, network, application or other computing resource on behalf of its owners -- and with their authorization.*

Example : *login into an email account that is not supposed to have access, gaining access to a remote computer that you are not supposed to have access, reading information that you are not supposed to able to read is considered as hacking.*

23. ***Junior ethical hacker****:well designed for Hacking Enthusiasts Between 13 And 18 Years Of Age Who Believe In Hacking With A Right Ethical Conscience.*

Example *: Performing verification tests on web applications, to help our customers to verify if they have effectively resolved vulnerabilities.*

24. ***Government support hackers****: Performing verification tests on web applications, to help our customers to verify if they have effectively resolved vulnerabilities.*

Example *: The National Security Agency's PRISM program and Ethiopia's use of FinSpy are notable examples.*

25. ***Croatian Revolution Hackers (CRH):*** *It was a black hat hacking group originating in Croatia, known for using DDoS, defacement, and other methods against targeted websites in Croatia and neighboring countries*

Example : *exposing some user data, as a 14-year-old school pupil**.***