• What are the types of hacker?

#Hackers are broadly categorized into white hat, black hat, and gray hat hackers, based on their motivations and ethical considerations. White hat hackers are ethical hackers who use their skills to identify and fix vulnerabilities with permission. Black hat hackers are malicious actors who exploit systems for personal gain or to cause harm. Gray hat hackers operate in a moral gray area, sometimes exploiting vulnerabilities without permission, but often with the intention of notifying the affected party.

• Explain in brief - Ethical hacking and cyber security.

#Cyber security encompasses the broad field of protecting systems and data from cyber threats, while ethical hacking is a specific practice within that field, involving the authorized and intentional attempt to find vulnerabilities in a system to improve its security. Ethical hackers use the same techniques as malicious hackers.

• Explain Foot printing Methodology

#Foot printing, also known as reconnaissance, is a systematic methodology used to gather information about a target system or organization before launching an attack or conducting a security assessment. It involves actively or passively collecting publicly available data to create a comprehensive understanding of the target's infrastructure, security posture, and potential vulnerabilities. Foot printing, also known as reconnaissance, is a systematic methodology used to gather information about a target system or organization before launching an attack or conducting a security assessment. It involves actively or passively collecting publicly available data to create a comprehensive understanding of the target's infrastructure, security posture, and potential vulnerabilities

• Find basic information using Google advance search operator and Pipl search

#To effectively use Google Advanced Search and Pipl, start by identifying your search topic and determining the scope of your search. Then, utilize specific operators like site:, filetype:, inurl:, and others to refine your results. Pipl is specifically designed for people searches, allowing you to find individuals using their name, email, phone number, or username. Combining these tools can lead to more targeted and efficient information gathering.

• Find vulnerability tool and check open port and service.

#Vulnerability scanning tools are used to automatically detect security weaknesses in networks, systems, or applications. Some popular tools include Nessus, Qualys, OpenVAS, Burp Suite, and Nmap. These tools help organizations identify potential attack vectors and prioritize remediation efforts.

If you would like to test ports on your computer, use the Windows command prompt and the CMD command netstat -ano. Windows will show you all currently existing network connections via open ports or open, listening ports that are currently not establishing a connection.