Module 2

Q.1 What are the types of hacker?

Ans: **Black Hat Hackers**

They are illegal hackers who try to steal other person's dat and stuffs without asking the admin.

White Hat Hackers

They are also known as Ethical Hackers pr a Penetration tester, they are good guys of the hacker world.

Gray Hat Hackers

They are hybrid between black hat hackers and white hat hackers.

Q.2 Explain in brief - Ethical hacking and cyber security.

Ans: **Ethical Hacking**

Ethical Hacking is the practice of attempting to penetrate a computer system, application, or data with the goal of identifying vulnerabilities and weaknesses in order ti improve security.

Ethical hackers re authorized to perform these tests and are tasked with accessing risk and testing systems for security-related issues.

They act like malicious intruders to reveal vulnerabilities to system owners.

Cyber Security

Cyber security is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

It involves the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks.

Cyber security is used by individuals and organizations to protect agains unauthorized access to data centers and other computerized systems.

Q.3 Explain Foot printing Methodology

Ans: Footprinting is an ethical hacking technique used to gather as much data as possible about a specific targeted system computer system, infrastructure, and organization.

Footprinting through search engines is a passive information gathering process where information about the target is gathered is gathered from social media.

The goal of footprinting is to find ways to enter a target system by gathering as much information as possible.

Footprinting in ethical hacking businesses identify and secure IT infrastructure before a threat actor exploits a vulnerability.

Q.4 Find basic information using Google advance search operator and Pipl search

Ans:

1. Start by identifying the person or entity you want to search for. Gather any available information such as their name, location, and any other relevant details.
2. Begin with Google advanced search operators. Open Google search and enter the following search query:
3. site:domain.com "keyword" -inurl:directory
4. Replace "domain.com" with the website you want to search within, "keyword" with the term you want to search for, and "-inurl:directory" with any directories or subfolders you want to exclude from the search.
5. If the search query does not provide enough information, try Pipl search. Pipl is a search engine that specializes in finding information about people. Open the Pipl website and enter the person's name, username, email address, or phone number into the search bar.
6. Refine your search results by using Pipl's advanced search options such as location, education, employment, and social media profiles.
7. Review the search results and gather any available basic information about the person or entity, such as their name, address, phone number, email address, social media profiles, and professional background.

Q.5 Find vulnerability tool and check open port and service.
Ans:

-> Start by identifying the system or network you want to test for vulnerabilities.

-> Search for vulnerability scanner tool that is compatible with the system or network you want to test.

-> Download and install the vulnerability scanner tool on your computer or device.

-> Configure the vulnerability scanner tool to scan for open ports and services.

-> Run the vulnerability scan and wait for results.

-> Review the scan results and identify any open ports and services that may be vulnerable to attack.

-> Take appropriate action t mitigate the vulnerabilities.