**Module 28: Information Gathering**

1. What are the types of hacker?

There are various types of hackers, each with their own motivations, skills, and techniques. Some of the most commonly recognized types of hackers include:

White hat hackers: Also known as ethical hackers, white hat hackers are individuals who use their skills for ethical purposes, such as identifying and fixing security vulnerabilities in systems and networks.

Black hat hackers: Black hat hackers are individuals who use their skills for malicious purposes, such as stealing sensitive information, causing damage to systems or networks, or disrupting services.

Grey hat hackers: Grey hat hackers are individuals who engage in both ethical and unethical hacking activities. They may use their skills to identify and report vulnerabilities, but may also engage in hacking activities for personal gain.

Script kiddies: Script kiddies are individuals who use pre-existing tools and scripts to conduct hacking activities, without necessarily possessing advanced technical skills or knowledge.

State-sponsored hackers: State-sponsored hackers are individuals or groups who are employed or funded by government agencies to conduct hacking activities for political or economic gain.

Hacktivists: Hacktivists are individuals or groups who use hacking techniques to promote political or social causes and bring attention to issues they care about.

Cybercriminals: Cybercriminals are individuals who engage in criminal activities online, such as identity theft, credit card fraud, or ransomware attacks, for personal or financial gain.

In summary, hackers can be classified into various types based on their motivations, skills, and techniques. Some of the most commonly recognized types of hackers include white hat hackers, black hat hackers, grey hat hackers, script kiddies, state-sponsored hackers, hacktivists, and cybercriminals.

1. Explain in brief - Ethical hacking and cyber security.

Ethical hacking is the practice of using hacking techniques and tools to identify and fix security vulnerabilities in systems and networks. It is a proactive approach to security that involves testing the security of systems and networks to identify weaknesses before they can be exploited by malicious attackers. Ethical hacking is typically conducted by trained professionals who follow a strict code of ethics and adhere to legal and industry standards.

Cybersecurity refers to the practice of protecting systems, networks, and data from unauthorized access, theft, or damage. It involves a range of practices and technologies, including firewalls, intrusion detection systems, encryption, and user authentication. Cybersecurity is essential to protect sensitive information and critical infrastructure from cyber attacks, which are becoming increasingly common and sophisticated.

Ethical hacking and cybersecurity are closely related, as ethical hacking is one of the tools used in the broader practice of cybersecurity. By conducting ethical hacking, cybersecurity professionals can identify and address security vulnerabilities before they can be exploited by attackers. Ethical hacking can also help organizations ensure compliance with industry standards and regulations, such as HIPAA and PCI DSS. Overall, ethical hacking and cybersecurity are essential practices to ensure the security and integrity of systems and networks in the face of ever-evolving cyber threats.

1. Explain Foot printing Methodology

Footprinting is the process of gathering information about a target system or network to identify potential vulnerabilities and attack vectors. It is a reconnaissance technique used by attackers to gather information about their target before launching an attack. The goal of footprinting is to identify weaknesses in the target's security posture that can be exploited in further stages of the attack.

Footprinting methodology typically involves the following steps:

Passive Footprinting: This involves gathering information about the target system or network without directly interacting with it. This can include searching for publicly available information about the target, such as social media profiles, job listings, and news articles. Passive footprinting techniques are often legal and do not involve any direct interaction with the target.

Active Footprinting: This involves directly interacting with the target system or network to gather information. Active footprinting techniques can include port scanning, network mapping, and vulnerability scanning. These techniques are more invasive and can potentially trigger alerts or alarms on the target system or network.

Analysis: Once the information has been gathered, it is analyzed to identify potential weaknesses and attack vectors. This can include identifying open ports, vulnerable software or services, and potential entry points into the target system or network.

Reporting: Finally, the results of the footprinting activity are compiled into a report that outlines the identified vulnerabilities and attack vectors. This report can be used to plan further stages of the attack, such as exploitation and post-exploitation.

It is important to note that footprinting can be both legal and illegal, depending on the techniques used and the target being analyzed. Legal footprinting is often conducted by security professionals to identify vulnerabilities in their own systems or networks. However, illegal footprinting can be used by attackers to gather information about targets for malicious purposes.

1. Find basic information using Google advance search operator and Pipl search

Google Advance Search Operator:

Google advanced search operators can be used to refine search results and find specific information. Some of the most commonly used operators include:

"site:" - This operator allows you to search within a specific website or domain. For example, "site:wikipedia.org coronavirus" would search for pages on the Wikipedia website related to coronavirus.

"intitle:" - This operator searches for pages with a specific word or phrase in the title. For example, "intitle:cybersecurity tips" would search for pages with "cybersecurity tips" in the title.

"inurl:" - This operator searches for pages with a specific word or phrase in the URL. For example, "inurl:pdf cybersecurity" would search for PDF documents related to cybersecurity.

"filetype:" - This operator searches for specific file types, such as PDF or DOC files. For example, "cybersecurity filetype:pdf" would search for PDF documents related to cybersecurity.

"related:" - This operator finds pages related to a specific website. For example, "related:wikipedia.org" would search for websites related to Wikipedia.

Pipl Search:

Pipl is a search engine that specializes in finding people and their information online. It can be used to find basic information such as name, email address, phone number, and social media profiles. To use Pipl, simply enter the name or email address of the person you are searching for, and the search engine will return any public information it can find.

Pipl also offers advanced search options that allow you to narrow down your search results by location, job title, or other criteria. However, some of these advanced features may require a paid subscription.

Overall, Pipl can be a useful tool for finding basic information about

5. Find vulnerability tool and check open port and service.

There are several vulnerability scanning tools available that can be used to check for open ports and services on a target system. Here are a few examples:

Nessus: Nessus is a popular vulnerability scanning tool that can be used to scan for open ports and services on a target system. It can also identify vulnerabilities and provide recommendations for remediation.

OpenVAS: OpenVAS is an open source vulnerability scanner that can also be used to scan for open ports and services. It includes a database of known vulnerabilities and can provide recommendations for remediation.

Nmap: Nmap is a network exploration and security auditing tool that can be used to scan for open ports and services. It is a command-line tool that is available for Windows, Linux, and macOS.

To use these tools to check for open ports and services on a target system, you would typically need to provide the IP address or domain name of the target. The tool will then scan the target system to identify open ports and the services running on those ports. It is important to note that scanning for vulnerabilities without the proper authorization can be illegal and may result in criminal charges. Always ensure that you have the proper authorization before conducting any vulnerability scans.