# **Module 28 Information Gathering**

# 1. What are the types of hackers?

Ans: There are multi types of Hackers but it’s very popular is there are three types of hackers

1.White hat Hacker

2.Black hat Hacker

3.Grey hat Hacker

1. **White Hat Hackers**: Also known as ethical hackers, they use their skills to improve security by finding vulnerabilities and informing the organizations so that they can fix them. They work with the permission of the system owners.
2. **Black Hat Hackers**: These hackers engage in unauthorized activities for personal gain or to cause harm. They may steal data, disrupt systems, or engage in other illegal activities for financial gain, espionage, or simply to create chaos.
3. **Grey Hat Hackers**: This category is somewhat in between white and black hat hackers. They may break into systems without permission but do not have malicious intent. Sometimes they do it to point out vulnerabilities but without authorization.
4. **Script Kiddies**: These individuals lack technical expertise and rely on pre-written scripts or tools to exploit vulnerabilities. They often engage in basic attacks without a deep understanding of the underlying technology.
5. **Hacktivists**: These hackers are motivated by political or social causes and use their skills to promote their beliefs or agendas. They may engage in activities like website defacement, DDoS attacks, or data leaks to draw attention to their cause.
6. **State-Sponsored Hackers**: These hackers are employed or supported by governments to carry out cyber espionage, sabotage, or other activities that further their nation's interests. They often target other governments, organizations, or critical infrastructure.
7. **Cyber Terrorists**: Unlike hacktivists who aim to promote causes, cyber terrorists aim to create fear and panic by targeting critical infrastructure or causing significant disruption through cyber-attacks.
8. **Insiders**: These are individuals who have authorized access to systems or networks but misuse their privileges for personal gain, espionage, or sabotage. They may be employees, contractors, or business partners with malicious intent.

These categories are not mutually exclusive, and individuals may shift between them depending on their motivations and circumstances. Additionally, within each category, there can be further specialization based on the specific skills and techniques used by hackers.

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

Ans: Ethical Hacking: Ethical hacking, also known as penetration testing or white-hat hacking, involves legally breaking into computers, networks, or systems to identify security vulnerabilities. Ethical hackers use the same techniques as malicious hackers, but their purpose is to improve security rather than cause harm. They work with the permission of the system owners to assess the security posture of an organization's IT infrastructure. Ethical hacking helps organizations identify and fix vulnerabilities before they can be exploited by malicious actors, thus enhancing overall cybersecurity.

Cybersecurity: Cybersecurity refers to the practice of protecting computers, networks, systems, and data from unauthorized access, theft, damage, or disruption. It encompasses various technologies, processes, and practices designed to safeguard digital assets and ensure confidentiality, integrity, and availability. Cybersecurity measures may include firewalls, antivirus software, encryption, access controls, incident response plans, and employee training. The goal of cybersecurity is to mitigate cyber risks and threats, including malware, phishing attacks, data breaches, and other cybercrimes, to protect individuals, organizations, and critical infrastructure from cyber threats.

Top of Form

# 3. Explain Foot printing Methodology

Ans: Footprinting is the process of gathering information about a target system or organization with the intent of discovering vulnerabilities, weaknesses, and potential points of entry for unauthorized access. It is often the first step in a hacker's reconnaissance phase and is crucial for planning and executing successful cyber-attacks. Footprinting can be conducted using various techniques and tools, and it typically follows a structured methodology, which can be summarized as follows:

1. **Reconnaissance**: This initial phase involves passive information gathering using publicly available sources such as search engines, social media platforms, company websites, online forums, and public records. Hackers look for information about the target organization's structure, employees, partners, technologies, and infrastructure.
2. **Scanning**: In this phase, hackers actively probe the target's network to gather additional information about its systems, devices, and services. Techniques such as port scanning, network mapping, and vulnerability scanning are used to identify potential entry points and security weaknesses.
3. **Enumeration**: Once potential targets are identified, hackers enumerate further details about them, such as user accounts, network shares, software versions, and configurations. This phase involves techniques like querying domain name servers (DNS), querying network services, and using enumeration scripts to extract valuable information.
4. **Footprinting Tools**: Various tools and techniques are used throughout the footprinting process to automate tasks and gather information efficiently. These tools include network mapping tools like Nmap, vulnerability scanners like Nessus, information gathering tools like Maltego, and social engineering techniques like phishing.
5. **Documentation and Analysis**: Throughout the footprinting process, hackers document all gathered information meticulously. This documentation includes details such as IP addresses, domain names, network configurations, software versions, and potential vulnerabilities. The gathered information is then analyzed to identify potential attack vectors and develop a strategy for further exploitation.
6. **Ethical Considerations**: It's important to note that while footprinting is a necessary step in security testing and penetration testing, it should only be conducted with proper authorization and in compliance with applicable laws and regulations. Unauthorized or malicious footprinting activities can have serious legal consequences and ethical implications.

By following a structured foot printing methodology, hackers can gather valuable information about their targets, assess their security posture, and identify potential weaknesses that can be exploited in further stages of a cyber-attack.

Top of Form

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

1. Ans: **Google Advanced Search Operators**:

Google's advanced search operators allow you to refine your search queries to find specific information. Here are some commonly used operators:

* **site:** - Restricts results to pages from a specified website or domain.
* **intitle:** - Limits results to pages with specific words in the title.
* **inurl:** - Limits results to pages with specific words in the URL.
* **filetype:** - Filters results to a specific file type, such as PDF, DOC, or XLS.
* **related:** - Finds pages related to a specified URL.
* **link:** - Finds pages that link to a specified URL.
* **cache:** - Displays the cached version of a webpage.

For example, to find basic information about "OpenAI" on its official website, you can use the query:

site:openai.com

This will return results from OpenAI's website.

1. **Pipl Search**:

Pipl is a people search engine that aggregates information from various online sources to provide detailed profiles about individuals. To use Pipl effectively:

* Visit the Pipl website (pipl.com).
* Enter the name of the person you're searching for in the search bar.
* Optionally, you can add additional information such as location, email address, username, or phone number to narrow down the search.
* Click on the search button to view the results.

Pipl may provide basic information such as name, age, location, occupation, social media profiles, and more, depending on the available data.

Remember to use these tools responsibly and ethically, respecting privacy and legal boundaries when conducting searches for personal information.

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

Ans: There are several vulnerability assessment tools available that can check for open ports and services on a network. One popular tool is Nmap (Network Mapper). Nmap is a powerful open-source network scanning tool that can be used for network discovery, security auditing, and vulnerability assessment.

Here's a basic overview of how to use Nmap to check for open ports and services:

1. **Install Nmap**: Nmap is available for various operating systems, including Windows, Linux, and macOS. You can download and install it from the official Nmap website: <https://nmap.org/download.html>
2. **Run Nmap Scan**: Once installed, you can run Nmap from the command line. Here's a simple command to scan a target host for open ports and services:

phpCopy code

nmap <target>

Replace **<target>** with the IP address or hostname of the target system you want to scan.

1. **Specify Port Range**: By default, Nmap will scan the 1000 most common ports. You can specify a custom port range using the **-p** option. For example, to scan ports 1 through 1000:

cssCopy code

nmap -p 1-1000 <target>

1. **Service Version Detection**: Nmap can also attempt to detect the version of services running on open ports using the **-sV** option:

phpCopy code

nmap -sV <target>

This will provide additional information about the services running on open ports, including their version numbers.

1. **Output Formats**: Nmap can generate output in various formats, including plain text, XML, and grepable format. You can specify the output format using the **-o** option. For example, to save the scan results in XML format:

phpCopy code

nmap -oX scan\_results.xml <target>

Remember that scanning networks without proper authorization may be illegal and unethical. Ensure that you have permission from the network owner before conducting any scans. Additionally, always comply with applicable laws and regulations when performing security assessments.