

Reconnaissance for Ethical Hackers - Notes



[Islam Diab | LinkedIn] → <https://www.linkedin.com/in/idiab1/>

Chapter 1: Fundamentals of Reconnaissance

What is ethical hacking?

- The term **hacking** is commonly used to **describe the techniques and activities that are performed by a person** with malicious intentions, such as a **hacker**, **to gain unauthorized access to a system or network**.

*Due to the curiosity of people around the world, the idea of **disassembling a system to further understand its functions created the foundation of hacking**. Early generations of hackers sought to understand how systems and devices work, and whether there was any flaw in the design that could be taken advantage of to alter the original function of the system.*

- For instance, during the 1950s and 1960s in the United States, **a security vulnerability was found in a telephone system** that enabled users to manipulate/alter telephone signals to allow free long-distance calls.
 - This technique was known as **phreaking** in the **telecommunication industry**. Specifically, a person could use whistles that operated at 2600 MHz to recreate signals that were used as the telephone routing

signals, thus enabling free long-distance calling to anyone who exploited this flaw.

- However, telecommunication providers had implemented a solution known as **Common Channel Interoffice Signaling (CCIS)** that separated the signals from the voice channel.

Important note

- A **vulnerability** is commonly **used to describe a security flaw or weakness** in a system.
- An **exploit** is anything that can be **used to take advantage of a security vulnerability.**
- A **threat** is anything **that has the potential to cause damage to a system.**
- A **threat actor** or **adversary** is **the person(s) who's responsible for the cyber-attack or creating a threat.**

Why someone would want to hack into another system or network?

- There are various motives behind each hacker, for instance, **many hackers will break into systems for fun, to prove a point to others, to steal data from organizations, for financial gain by selling stolen data on the dark web, or even as a personal challenge.**

While hacking seems all bad on mainstream media, it's not all bad because cybersecurity professionals such as ethical hackers and penetration testers use similar techniques and tools to simulate real-world cyber-attacks on organizations' networks with legal permission and intent to discover and resolve hidden security vulnerabilities before real cyber-attacks occur in the future.

Although threat actors and ethical hackers have similar skill sets, they have different moral compasses, with threat actors using their skills and abilities for malicious and illegal purposes and ethical hackers using their skills to help organizations defend themselves and safeguard their assets from malicious hackers.

The following are common types of threat actors and their motives:

- **Advanced Persistent Threat (APT) groups** – The members of an APT group design their attacks to be very stealthy and undetectable by most threat detection systems on a targeted network or system. The intention is to

compromise the targeted organization and remain on its network while exploiting additional systems and exfiltrating data.

- **Insider threats** – This is an attacker who is inside the targeted organization's network infrastructure. This can be a hacker who is employed within the company and is behind the organization's security defense systems and has direct access to vulnerable machines.
- **State actors** – These are cybersecurity professionals who are employed by a nation's government to focus on national security and perform reconnaissance on other nations around the world.
- **Hacktivists** – These are persons who use their hacking skills to support a social or political agenda such as defacing websites and disrupting the availability of or access to web servers.
- **Script kiddie** – This type of hacker is a novice and lacks the technical expertise in the industry but follows the tutorials or instructions of experts to perform cyber-attacks on targeted systems.
- **Criminal syndicates** – This is an organized crime group that focuses on financial gain and each person has a specialized skill to improve the attack and increase the likelihood of success.
- **White hat** – These are cybersecurity professionals such as ethical hackers, penetration testers, and red teamers who use their skills to help organizations prevent cyber-attacks and threats.
- **Gray hat** – These are people who use their hacking skills for both good and bad. For instance, a gray hat threat actor could be a cybersecurity professional who uses their skills in their day job to help organizations and at night for malicious reasons.
- **Black hat** – These are typical threat actors who use their skills for malicious reasons.

The following agreements need to be signed between the cybersecurity service provider and the customer:

- **Non-Disclosure Agreement (NDA)**
- **Statement of Work (SOW)**
- **Master Service Agreement (MSA)**
- **Permission of Attack**

The **NDA** is commonly referred to as a *confidentiality agreement*, which specifies that the ethical hacker, penetration tester, or red teamer **will not disclose**, **share**, or **hold on to any private**, **confidential**, **sensitive**, or **proprietary**

information that was discovered during the security assessment of the customer's systems and network infrastructure.

the SOW documentation usually *contains all the details about the type of security testing that will be performed by the ethical hacker*/service provider for the customer and the scope of the security testing, such as **the specific IP addresses and ranges**.

The MSA is a *general agreement that contains the payment details and terms, confidentiality and work standards of the provider, limitations and constraints, and delivery requirements*. This type of agreement helps the cybersecurity service provider to reduce the time taken for any similar work that needs to be provided to either new or existing customers.

Permission of attack is a *very important agreement for ethical hackers*, penetration testers, and red teamers as it contains the legal authorization that is needed to perform the security testing on the customer's systems and network infrastructure.

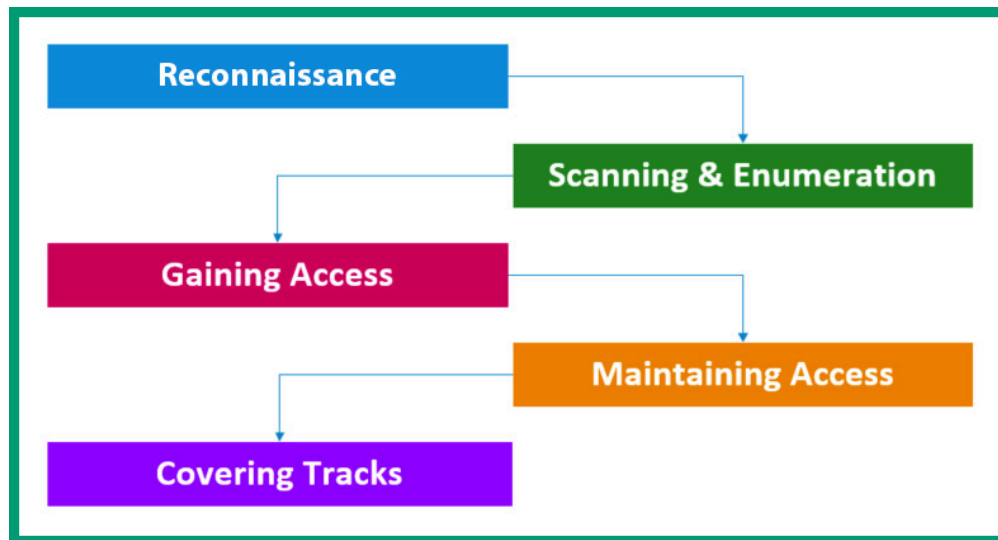
Mindset and skills of ethical hackers

- There are different types of hackers and groups around the world, and each of **these has its own motive and rationale for their cyber-attacks**:
 - **Personal accomplishment/challenge**, such as proving they have the skills and capabilities to break into an organization and its systems
 - **Financial gain**, such as stealing confidential data from organizations and selling it on various dark web marketplaces
 - **Supporting a social or political agenda** such as defacing and compromising websites that are associated with a social/political movement
 - **Cyber warfare**, such as compromising the **Industrial Control Systems (ICS)** that manage the critical infrastructure of a country
- The following are common **technical skills of ethical hackers** in the cybersecurity industry:
 - **Administrative-level skills** with various operating systems such as Windows and Linux
 - **Solid foundational knowledge of networking**, such as routing and switching
 - **Understanding the fundamentals of common security** principles and best practices
 - **Familiar with programming languages** such as Go and Python, and scripting languages such as Bash and PowerShell

- Familiarity with **virtualization**, **containerization**, and **the cloud**
- The following are **non-technical skills of ethical hackers**: - Being proficient in oral and written communication between technical and non-technical persons - Being an **out-of-the-box** thinker - Being self-motivated and driven to learn about new topics and expand knowledge - Ensuring you understand the difference between using knowledge for good and bad intentions

if you want to find the security vulnerabilities that real hackers are able to discover and exploit, then you need to adapt your mindset while using the same techniques, tools, and procedures to help you do the same, with legal permission and good intentions.

The following diagram shows the EC-Council's five stages of ethical hacking:



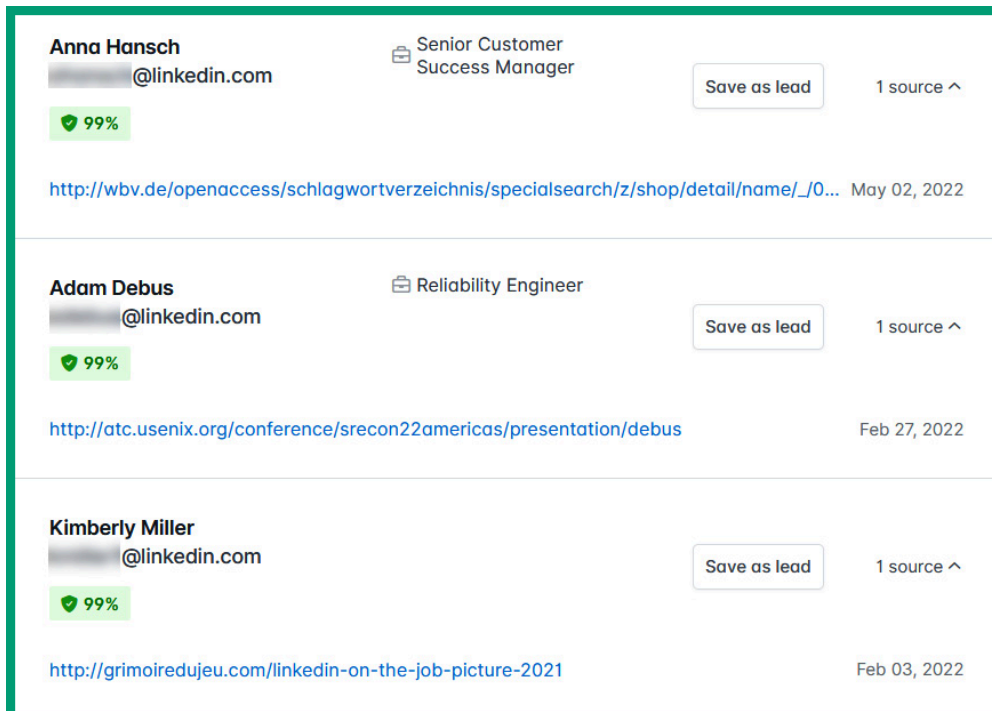
The importance of reconnaissance

- The first phase of ethical hacking is **reconnaissance** – **the techniques and procedures that are used by the ethical hacker to collect as much information as possible about the target** to determine their network infrastructure, cyber defenses, and security vulnerabilities that can be compromised to gain unauthorized access and improve attack operations accordingly.
 - **Collecting information about the target** helps the attacker to **determine** the **points of entry**, **type of infrastructure**, **assets owned**, and **the target's strengths and weaknesses**.

*Using reconnaissance techniques enables the ethical hacker to identify any **running services** and **open ports** and **the service and software versions***

on a system, all of which can be used to identify and determine potential attack vectors on the target.

- Using reconnaissance techniques such as **Open Source Intelligence (OSINT)** enables the ethical hacker to passively collect information about their target that's publicly available on the internet. **Such information** - usernames - email addresses - job titles of employees of the targeted organization. **The following screenshot shows an example of employees' information that's publicly available on the internet:**



- A threat actor could look for patterns in their email addresses to determine the format that's used for all employees of the company.
- For instance**, - let's imagine there's an employee whose name is **John Doe** and his email address is jdoe@companyname.com and another employee is **Jane Foster** with an email address of jfoster@companyname.com. - This information shows a pattern and format for employees within the same organization: **{f}{lastname}@domain-name.com**, where **f** is the initial letter of the person's first name followed by their last name and the company's domain name. *Reconnaissance is not only important to adversaries but cybersecurity professionals use the gathered information to help organizations.*

Reconnaissance is divided into the following types:

- Passive reconnaissance**
 - Active reconnaissance**
- Passive reconnaissance** enables the ethical hacker to leverage OSINT techniques to **gather information that's publicly available from various sources on the internet without making direct contact**

with the target. The following are some examples of OSINT data sources:

- Job websites
 - Online forums
 - Social media platforms
 - Company registry websites
 - Public **Domain Name System (DNS)** servers
1. **Active reconnaissance** involves a more direct approach by the threat actor and ethical hacker to gather information about the target.
 - The ethical hacker uses scanning and enumeration techniques and tools to obtain specific details about the targeted systems and networks.
 - For **instance**, to determine **running services** and **open ports on a server**, the ethical hacker can use a network and port scanning tool such as **Nmap** to perform host discovery on a network.
-

Understanding attack surface management

- The **attack surface** is **simply the number of potential security vulnerabilities** that can be exploited to gain access to a system, network, and organization using attack vectors.
- **Attack Surface Management (ASM)** is not a new study in the cybersecurity industry, rather **it's a new focus for cybersecurity professionals and organizations around the world.**
- **ASM is a strategy that's used by cybersecurity professionals** that enables them to focus on **identifying, analyzing, and reducing the attack surface of an organization.**
 - As a result, by reducing the attack surface of an organization, it reduces the risk of being compromised by cyber-attacks and threats while safeguarding its assets, resources, and sensitive information.
- The **Common Vulnerability Scoring System (CVSS)** is commonly referenced within many vulnerability scanning tools to provide vulnerability of between **0** and **10**, where **0** is the least impact and **10** is critical. *These scores help cybersecurity professionals to apply high priority and resources to remediate security vulnerabilities with higher severity.*

Base Score

9.4
(Critical)

Attack Vector (AV)

Network (N)

Adjacent (A)

Local (L)

Physical (P)

Attack Complexity (AC)

Low (L)

High (H)

Privileges Required (PR)

None (N)

Low (L)

High (H)

User Interaction (UI)

None (N)

Required (R)

Scope (S)

Unchanged (U)

Changed (C)

Confidentiality (C)

None (N)

Low (L)

High (H)

Integrity (I)

None (N)

Low (L)

High (H)

Availability (A)

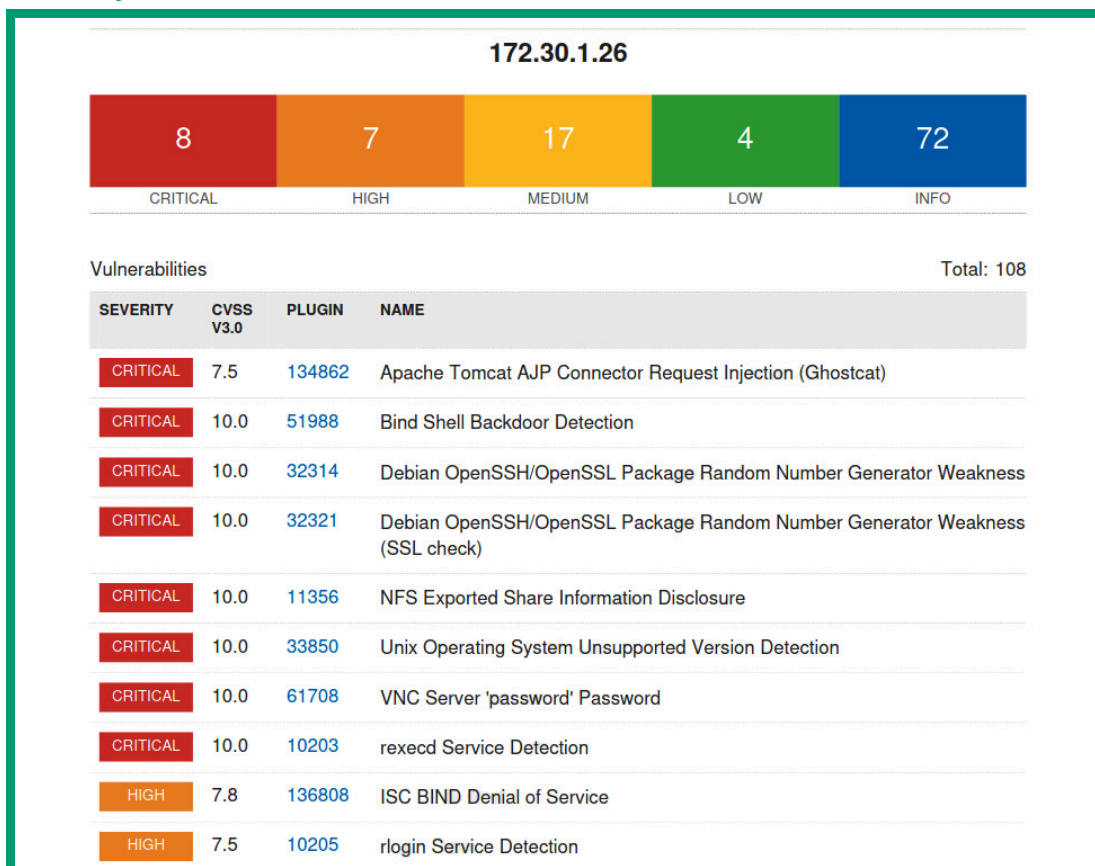
None (N)

Low (L)

High (H)

Vector String - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

As shown in the preceding snippet, the metrics within the base score influence the vulnerability score. To learn more about the CVSS calculator, please see <https://www.first.org/cvss/calculator/3.1>. The following snippet shows the results of a Nessus vulnerability scan, displaying the number of security flaws and their scores:



- **Another benefit of ASM** is its capability of helping organizations efficiently monitor their attack surface and identify any suspicious activities.
- This improves real-time threat detection and response within the company, enabling the security team to take immediate action to prevent, contain, or remediate the threat from systems and networks.

- Lastly, when ASM is implemented properly, it helps security teams to identify whether any malicious activities or threats that evaded security solutions have gone undetected on their systems and networks.

The following are the major benefits of ASM within the cybersecurity industry:

- **Reducing risk**
 - Organizations that adopted ASM are able to identify and reduce their own attack surfaces, thereby reducing the risk of potential cyber-attacks and threats, and protecting their assets from threat actors.
 - *Hence, by identifying and remediating security vulnerabilities, it becomes more difficult for threat actors to compromise systems and gain a foothold.*
- **Prioritization**
 - ASM helps companies to prioritize their resources to remediate security vulnerabilities that are more critical than others.
- **Continuous monitoring**
 - For organizations to ensure their attack surface is small, continuous monitoring and maintenance are needed.
- **Improving incident response**
 - ASM helps security teams to efficiently identify and respond to security incidents on their network in real time, as a result, reducing the impact and spread of a threat.
- **Compliance**
 - There are regulatory standards and frameworks that are needed within organizations that operate in certain industries.
 - For instance, organizations that operate in the payment card industry need to ensure their systems and networks are compliant with the **Payment Card Industry Data Security Standard (PCI DSS)**. Being compliant means the organization's systems and networks have the specific security controls in place to ensure data is protected.
- **Cost-effectiveness**
 - Since ASM helps organizations to improve the identification and remediation of security vulnerabilities, it reduces the risk of data breaches and increases the availability of systems that are critical to the organization.

The following are key steps that organizations and cybersecurity professionals can use to get started with ASM:

1. Asset management

- Ensure all assets within your organization are properly tracked and entered into your inventory.
- These may include **computers**, **servers**, **applications**, and **mobile devices**.
- This helps organizations to better understand which assets are to be protected and identify security flaws in them.

2. Identifying and mapping the attack surface

- At this stage, the cybersecurity professionals are to identify security vulnerabilities and map the attack surface of the organization.
- This stage includes potential attack vectors that could be used to deliver an exploit and points of entry such as open ports and vulnerable running services on systems and networks.

3. Assessing risk

- This stage focuses on assessing the risk of each security vulnerability and its impact on the organization.
- This phase helps with prioritizing and focusing on the most critical security vulnerabilities, then on less critical vulnerabilities.

4. Implementing security controls

- This phase focuses on **implementing security controls and solutions to remediate and mitigate security vulnerabilities** that were identified in the previous stages.
- Here, **the security team will implement network security devices**, **threat monitoring and prevention solutions**, **network segmentation**, and so on.

5. Monitoring and maintenance

- For ASM to be effective, continuous monitoring of all assets, systems, and devices is required.
- It's important to continuously monitor and maintain security controls that are responsible for mitigating cyber-attacks and threats from exploiting security vulnerabilities.
- In addition, continuous monitoring and maintenance help ensure security controls are effective in safeguarding the assets of the organization.

6. Continuously perform reconnaissance

- To identify new security vulnerabilities on the attack surface, organizations need to continuously perform reconnaissance on their assets, systems, and network infrastructure.
- Once new security vulnerabilities are identified, the lifecycle of ASM is repeated, taking the necessary steps to mitigate the security risk.

In addition to using the preceding key steps, there are several tools that will help both cybersecurity professionals and organizations with ASM:

- **Vulnerability scanners**

- These are specialized, automated tools that help cybersecurity professionals identify security vulnerabilities in a system and provide recommendations on how to remediate the issue.
 - Furthermore, these tools provide severity ratings, vulnerability scores, and potential impact.

- **Network scanners and mappers**

- This type of tool helps cybersecurity and networking professionals to determine live hosts, open service ports, and running applications on host devices.
- In addition, they help organizations to map their entire network infrastructure and identify unauthorized devices that are connected to the company's network.

- **Configuration management tools**

- This type of tool helps organizations track and manage their configurations on systems and networks.
- It also helps cybersecurity professionals to identify new security vulnerabilities such as misconfigurations that are introduced onto a device after a new change.

- **Application security testing tools**

- These are specialized tools that are commonly used by cybersecurity professionals to perform security testing on applications and software to identify any unknown security flaw.

- **Attack Surface Reduction (ASR) tools**

- These tools are designed to help organizations reduce their attack surfaces.
- It works by identifying and denying any malicious network traffic and disabling unnecessary services on systems and protocols.

- **Risk management tools**

- Risk management tools enable organizations to both track and manage the risk as it's associated with their attack surface.

- Furthermore, this tool helps cybersecurity professionals to monitor the effectiveness of the security controls that are in place to prevent cyber-attacks and threats.
 - **Security Information and Event Management (SIEM)**
 - This is a security solution that collects, aggregates, and analyzes security-related log messages generated from systems and devices within an organization to identify any potential cyber-attack and threat in real time.
-

Reconnaissance tactics, techniques, and procedures

- MITRE ATT&CK includes reconnaissance TTPs that help us to better understand the methods that are used by adversaries to collect information about their targets prior to launching an attack.
- These TTPs are also used by ethical hackers to efficiently identify security vulnerabilities and how a threat actor could compromise the attack surface of their client's network infrastructure.

The following are common reconnaissance TTPs that are used by adversaries:

- **Active scanning**
 - During active scanning, adversaries use various scanning tools to collect information about the target that can be leveraged in future operations.
 - These scanning tools send special probes to targeted systems and networks to determine live hosts, operating systems, open ports, and running services on the host machine.
 - Active scanning is an active reconnaissance technique that involves scanning IP network blocks and public IP addresses of the target, vulnerability scanning to identify security weaknesses that can be exploited, and wordlist scanning to retrieve possible passwords for future password-based attacks against the target.
- **Gathering victim host information**
 - This technique enables the attacker to collect specific details about the target's devices such as their hostnames, IP addresses, device types/roles, configurations, and operating systems.
 - Additionally, the adversary is able to collect hardware, software, and client configuration details that can be used to improve the plan of

attack.

- This technique involves **using a combination of both active and passive reconnaissance** as a threat actor can gain a lot of intelligence from OSINT alone and can perform active reconnaissance to identify specific details that are not easily available on the internet.

- **Gathering victim identity information**

- **This technique focuses on collecting details about the target's identity** – personal data such as **employees' names**, **email addresses**, **job titles**, and **users' credentials**.
- This type of information can be collected **using passive reconnaissance and leveraged for future social engineering attacks** and gaining access to the target's systems.

- **Gathering victim network information**

- Adversaries can **use passive reconnaissance techniques** to collect information on the target's network infrastructure such as **IP ranges**, **domain names**, **domain registrar details** (physical addresses, email addresses, and telephone numbers), and **DNS records**.
- However, **active reconnaissance techniques** will help the attacker **to better identify the target's network topology, networking devices, and security appliances**. Such information helps the adversary to better understand the target's network infrastructure.

- **Gathering victim organization information**

- **This technique enables adversaries to collect specific information** about the target's organization such as **names of departments, business operations and processes, and employees' roles and responsibilities**.
- Such information can be collected **using passive reconnaissance**. Furthermore, adversaries use this technique to determine **physical locations, business relations, and operating hours**.

- **Phishing for information**

- Adversaries send phishing email messages to employees of the target organization with the intention of tricking a victim into performing an action such as **downloading and installing malware on their system** or **even revealing sensitive information** such as their **user credentials**.
- Adversaries can use spear phishing services from online service providers, insert malicious attachments in email messages, and insert obfuscated links within the body of the email message.

- *Since the attacker is using a direct approach, this is an active reconnaissance technique.*
- **Searching closed sources**
 - The adversary may attempt to collect information about the target from closed sources, where the information is available as a paid subscription (passive reconnaissance).
 - Such information includes **threat intel vendors** such as private details from threat intelligence sources that can be used to compromise the target.
 - Furthermore, adversaries can purchase information about the target from **Dark Web** marketplaces/black markets.
- **Searching open technical databases**
 - There are many public online sources that enable anyone to collect information about a target.
 - This technique focuses on leveraging public information that can be used to improve the plan of attack against an organization.
 - For instance, the adversary can leverage **public DNS records**, **WHOIS data** (domain registration details), **digital certificates** (help identify sub-domains), and **public databases** that contain IP addresses, **open ports**, and server banner details about the target.
 - *This is another passive reconnaissance technique to collect information about the target.*
- **Searching open websites and domains**
 - Adversaries use this technique to search various online websites and platforms such as **social media**, **internet search engines**, and **code repositories** (such as GitHub) to collect information that can be used to compromise the target.
 - Searching open websites and domains is another **passive reconnaissance** technique for collecting public information.
- **Searching victim-owned websites**
 - This technique is used by the adversary to search the target's websites for any details that can be leveraged, such as **organizational details**, **physical locations**, **email addresses of employees**, **high-profile employees**, and **even employees' names** and **contact details**.
 - *This is an active reconnaissance technique since the attacker establishes a direct connection to the target's asset.*