España | digital 2026

Study of tools for recognition activity

Financiado por la Unión Europea
NextGenerationEU

MINISTERIO DE TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

September 2023

INCIBE-CERT_STUDY_TOOLS_FOR_RECOGNITION_ACTIVITY_2023_v1.1

La presente publicación pertenece a INCIBE (Instituto Nacional de Ciberseguridad) y está bajo una licencia Reconocimiento-No comercial 3.0 España de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- Reconocimiento. El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INCIBE o INCIBE-CERT como a su sitio web: https://www.incibe.es/. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- Uso No Comercial. El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE-CERT como titular de los derechos de autor. Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/3.0/es/.

Index

1. About this study

The reconnaissance tactic is a fundamental process in cybersecurity, which aims to obtain detailed information about the systems and networks that you want to attack or defend. In this sense, the present study focuses on this tactic, its **application** in different scenarios and the **mitigation measures** that can be implemented to prevent possible attacks.

The guide has a technical approach, aimed at explaining all aspects related to the reconnaissance tactic, both for users who do not know it, and for those who want to improve the security features of their systems and networks.

The order of the contents is structured so that it begins with a general theoretical explanation of the most important concepts, and then focuses on the explanation of particular techniques and subtechniques, indicating some of the tools that can be used in each case.

In summary, the objective of this study is to provide detailed guidance on the reconnaissance tactic and its importance in the field of cybersecurity, with the main objective of helping organizations better understand how attackers can collect information about them and their systems, and how the risks associated with this tactic can be mitigated.

2. Organization of the document

This study focuses on reconnaissance tactics, widely used in Red Team exercises and security analysis. It begins with the **3.- Introduction**, which establishes the context and importance of recognition in cyberattacks, highlighting how attackers use this technique to collect information that can be used to plan future operations.

Subsequently, the **4.- The recognition technique** is framed in the MITRE ATT&CK reference framework and its TTP, focusing specifically on how to collect valuable information about the target.

Once the reference framework has been introduced and established, the **5.- Techniques and tools** are addressed, where the different subtechniques and possible tools to carry them out are shelled. In addition, it proposes mitigation measures that organizations can adopt to reduce the associated risk, ranging from general recommendations to specific strategies that can be used to detect and prevent recognition.

Finally, in the **6.- Conclusion**, the main points of the document are summarized, providing some recommendations on how they can improve their security against the tactic of reconnaissance. These recommendations include the importance of limiting the quantity and quality of public information available, adopting advanced detection and response tools, and improving employee training and awareness.

3. Introduction

Reconnaissance has been a fundamental tactic throughout the history of cybersecurity, from the early days of computing and network security, when early hackers explored systems out of curiosity, personal challenge, or seeking recognition; to the present day, where security experts seek to detect vulnerabilities in their own systems. to fix them before they can be exploited by attackers.

Reconnaissance has evolved over time into a very sophisticated and structured tactic for understanding systems and networks. In the same way, the tools used have been improving and automating the tasks of port scans, online information search or penetration tests.

As systems and networks became more complex, the importance of recognition grew. **Today, reconnaissance is a crucial phase in the process of ethical hacking and security analysis**, and is used to discover vulnerabilities, configuration flaws, or sensitive data exposed about systems and networks in all industries, from private companies to critical infrastructure systems to government agencies, and of course, people.

During this phase, information is collected through different techniques and tools in **order to obtain as much information as possible** about the system or network in question, without damaging the integrity of the system**.** Once the necessary information is collected, security experts can analyze it to identify potential weaknesses that could be exploited. In this way, protective measures can be implemented to prevent possible attacks or security compromises.

Importantly, the reconnaissance tactic **is not only used by security experts, but also by malicious attackers**. In fact, it is common for cybercriminals to perform prior reconnaissance before launching an attack to know the weaknesses of the target network or system. Therefore, it is essential that companies and organizations are aware of this tactic and take steps to protect themselves.

4. The recognition technique

For the elaboration of this study, the MITRE ATT&CK framework has been taken as a reference, which provides a global knowledge base on tactics, techniques, and procedures (TTP) of the adversaries, that is, the offensive actions that can be used against the systems and that have been collected, classified, and categorized with a common taxonomy. from events observed in real life. This tool provides detailed information about more than 100 threat actor groups. Through the use of ATT&CK, it is possible to identify and evaluate defensive gaps, as well as the capabilities of security tools. This framework can be used to run security or incident response analysis, search for threats, participation in [1]*Red Team* activities or validation of mitigation controls, among others.

MITRE ATT&CK arrays are a visual representation of the ATT&CK framework that is used to provide a contextualized view of TTPs throughout the attack lifecycle. Although there are different types of matrices, we will focus on the Enterprise[2], since it is of interest to most organizations, which covers different stages of the life cycle of an attack in the ICT field, with specific objectives that attackers pursue. These objectives are also known as **tactics** and serve to categorize and organize concrete techniques. These include: reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact.

In the context of **tactics**, it is important to understand the relationship between threat actors, tools, and techniques. Threat actors are the individuals or groups that carry out attacks. Techniques are the methods used to carry them out, and **tools** are the programs or devices used in practice. Figure 1 graphically explains this relationship.

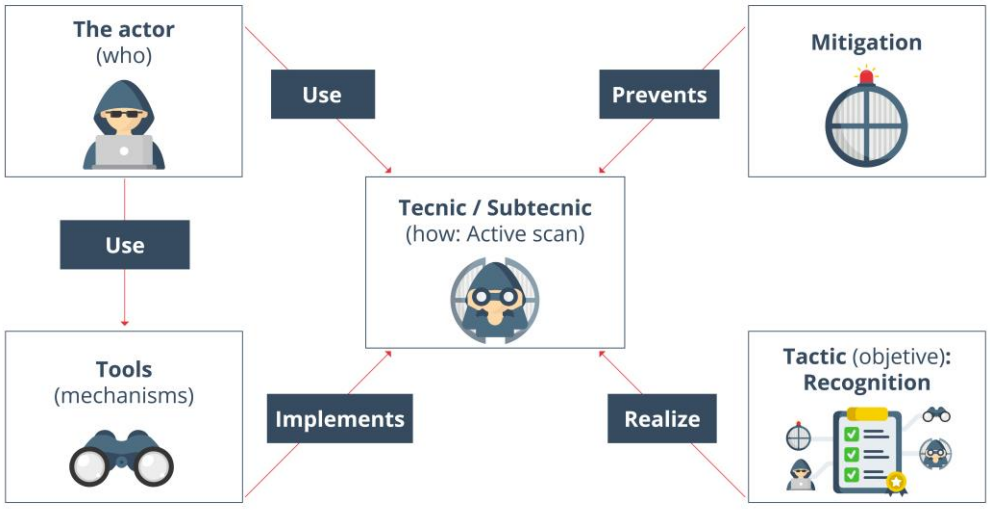


Figure 1 - Actor-technique-tool relationship

[1] https://attack.mitre.org/

[2] https://attack.mitre.org/matrices/enterprise/

Reconnaissance is one of the most important tactics during the planning phase, because it provides attackers with crucial information to make decisions and organize the execution of the attack according to their objectives. It involves gathering information about the network target, such as network topology, systems, services being executed, user credentials, etc., that allows attackers to identify vulnerabilities and weaknesses of the target, so that they can select and execute specific attacks with a higher degree of success. In addition, reconnaissance can also help attackers avoid detection because, if attackers know the structure and security tools used in the network, they will be able to adapt their attacks to elude detection by network security systems.

The *Enterprise* matrix establishes 10 different techniques within recognition, some of these techniques include the use of public information search tools, the exploration of network services, the search for information in social networks and the collection of information in emails. **It is important to note that reconnaissance techniques can be used by both malicious actors and security teams to assess exposure and improve an organization's security posture**. Therefore, knowing these techniques and being prepared is essential to prevent and detect possible threats. Below, we present the most representative recognition techniques along with their identifiers:

- **T1595 Active** scanning: Sending packets to a system or network to obtain information about the services, ports, and operating systems running on them.
- **T1592 Collect information about the target's hosts**: Find information about the *hosts* that are part of the target's infrastructure, such as IP addresses, host names, and operating systems.
- **T1589 Collect information about the** target's identity: Obtain information about the target's employees and users, such as names, email addresses, phone numbers, and roles in the organization.
- **T1590 Gather target network information**: Collect information about the target's network architecture and topology, including network devices, network segments, and protocols used.
- **T1591 Gather information from the** target's organization: Seek information about the target's organizational structure, policies, and procedures.
- **T1598 Information spoofing**: using techniques to impersonate a trusted entity and obtain information about the target.
- **T1597 Search for closed sources**: Search for information in non-public sources, such as private forums or information exchange networks between criminals.
- **T1596 Search open technical databases**: Use search tools and queries in open databases to obtain information about the target.
- **T1593 Search for open domains/websites**: Identify and search information about domains and websites that belong to the target and are publicly available.
- **T1594 Search for victim-owned websites**: Search for websites that belong to the target's organization, and that are publicly available for information about the organization's infrastructure and systems.

These reference techniques will be of great help to classify different existing tools within the state of the art.

5. Techniques and tools

Recognition is a crucial stage in any red *teaming* or *pentesting* exercise. Most of their techniques are based on **Open-Source Intelligence (OSINT),** an information gathering strategy that uses public and open sources of information to obtain information about a target such as social networks, search engines, public databases, and websites. The information obtained may include details about the target's infrastructure, IP addresses, domain names, emails, usernames, passwords, employee names, physical locations, contact details, information about products and services, and any other relevant information that may be useful to carry out a security operation.

To carry out the recognition correctly, it is necessary to follow the **rules of engagement** that establish limits and conditions in the use of techniques and tools. These rules typically include guidelines on what systems can and cannot be scanned, the time of day that tests can be performed, the data that can be collected, and how it can be used, among other aspects.

This section describes some of the most common reconnaissance techniques and tools used in these exercises, from port scanning to target information search tools.

5.1. T1595 Active Scan

This is the technique used to identify the services and systems in a network, as well as their vulnerabilities and configurations. This technique involves sending network packets to the target systems to obtain information about their open ports, operating systems, applications, and versions.

The level of intrusiveness of active scanning can vary depending on the configuration of the target systems and the number of packets sent, but in general, it is considered more aggressive than passive scanning, as it involves sending network traffic to the target systems. This technique can be detected by defense tools, such as intrusion detection systems and leaves a trail in the form of IP addresses or information about the technology used, which increases the chances of discovery of the reconnaissance team operation. For this reason, *pentesters* or members of the *Red Team* should be cautious when using this technique, taking measures to go unnoticed, such as using IP address hiding techniques or adjusting the scanning speed.

5.1.1. **Subtechniques**

There are several active scanning subtechniques that are used in identifying systems and services on a network. Some of the most used are:

Subtechniques	Detail	Tools
Getting ICMP responses in an IP or domain range	Obtaining Internet Control Message Protocol (ICMP) responses is an option used to determine whether a *host* is active or online. One of the most common ways to use ICMP to obtain information is by sending "echo request" packets using the Ping tool. If the target *host* is active and online, it will respond to the "echo request" packet with an "echo reply" packet. If a response is not received or if an ICMP error message is received, it could indicate that the target *host* is down, inaccessible, or blocking ICMP traffic.	Ping, Fping, Traceroute
Scanning TCP ports in an IP range or domain	It relies on sending TCP packets to a range of ports on a target system to determine whether they are open or closed. There are several types of TCP port scans, such as SYN scan, Connect scan, FIN scan, Xmas scan, and Null scan. Each of these methods uses different alternatives to interact with the target system's ports and determine their status.	Nmap, Masscan
Scanning UDP ports in an IP range or domain	It consists of sending UDP packets to a range of ports on a target system to determine whether they are open or closed. This option is more difficult to perform than scanning TCP ports because systems may not send a response if the port is closed, making scanning slower.	Nmap, Masscan
Scanning for vulnerabilities in an IP range or domain	Packets specifically designed to recognize existing vulnerabilities in target systems are sent. This alternative can be very intrusive and should be done with caution, as it can be detected and blocked by defense systems.	OpenVas, OwaspZap.
Dictionary scanning on an IP range or domain	The idea is to test multiple combinations of words or characters (usually taken from a dictionary) common in the network infrastructure within a range of IP addresses or in a target domain to identify sensitive network information.	DirBuster, Dirsearch, Gobuster

5.1.2. **Mitigation measures**

It is impossible to completely eliminate the risk of active scanning, as it is beyond the control of the organization. However, measures can be implemented to reduce the exposure area, such as limiting the opening of ports to those necessary and modifying the standard ports used by services in order to make their recognition difficult. In addition, it is possible to detect scanning patterns by analyzing *logs* and trigger blocking rules in the *firewall* to prevent future scanning attempts. With these measures, you can significantly reduce risk and improve network security.

5.2. T1592 Collect Information about the target's hosts

This technique focuses on obtaining details about systems, services, and system configurations. It is essential for identifying potential vulnerabilities and helps security professionals plan and conduct security testing efficiently and effectively. It can be both passive and active, depending on the approach and tools used.

- In the case of a passive approach, information is collected without interacting directly with the target systems. For example, specialized search engines such as Shodan can be used to obtain information about IP addresses, services, and open ports on target systems without sending them network traffic. Also, information can be collected through the extraction of metadata from public documents, with the *software* with which they were created, or their version.
- On the other hand, an active approach involves interacting directly with target systems, sending them network traffic directly. Unlike active scanning, it is used to obtain more accurate information related to *hosts*, such as the versions or architectures of their systems. These active approaches can be more intrusive and therefore carry a higher risk of being detected by defense systems.

5.2.1. Subtechniques

There are several sub-techniques employed in gathering information about the *target's hosts* . Some of them are:

Subtechniques	Detail	Tools
Search for information from IP or domains through indexers	It allows you to obtain information about IP addresses, such as your services and open ports, potential vulnerabilities, physical location, or *hosting* data. All this through information displayed in the header of the web server's response to a connection request.	Shodan, Censys

Metadata extraction	This option is mainly used to find metadata and hidden information in documents that are scanned within the target. These documents can be on web pages and can be downloaded and analyzed with specific tools. Among the metadata, you can discover information about the *hosts* such as the device where the document was prepared, user space paths or the *software* used by them.	FOCA, ExifTool
Collection of configurations in public sources	Configuration harvesting is a sub-technique used by adversaries to obtain details about system parameters such as architecture information, time zones, languages, etc. For example, through monitoring public forums, social media profiles, and other online resources where target users can discuss their system configurations.	Search engines, forums
Recognition of operating systems or *fingerprinting* in an IP range or domain	It is based on sending packets to a target system to determine its operating system, from the response received. Information can be obtained about the version and type of operating system you are running. An example is through the -O parameter of Nmap.	Nmap, p0f
Enumerating services in an IP or domain range	By sending packets to a target system, you determine which services are running on it from the received response. Information can be obtained about the type and version of the service that is running.	Nmap, OpenVas, Nessus, OwaspZap

5.2.2. **Mitigation measures**

The technique, although it cannot be fully mitigated, because it relies on actions carried out outside the scope of enterprise security controls, can be effectively mitigated through a series of proactive measures. Organizations should minimize the amount of publicly exposed technical and sensitive data, including restricting metadata information in documents and limiting server information in response headers. It is also essential to keep operating systems and applications up to date, regularly apply security patches, and employ robust security controls. In terms of information obtained from public forums and social media, a strong and well-communicated privacy and security policy can help limit the information employees share publicly.

5.3. T1589 Collect Information about the identity of the target

Obtaining the information about the identities of individuals, groups or systems within a target organization is of great interest to attackers, to better understand the structure of the organization, the relationships between its members, roles, and responsibilities. This makes it possible to plan future attacks or create better-targeted, more convincing, and effective social engineering campaigns.

5.3.1. Subtechniques

We can identify some sub-techniques linked to the collection of information about the identity of the target, such as, for example:

Subtechniques	Detail	Tools
Generalist search engines	It uses search operators (*dorking*) to filter information in search engines, allowing to obtain data such as emails, employee names and credentials.	Search engines, LinkedIn
Search in engines specialized in data leaks	It employs specialized intelligence tools of data leakage from input parameters such as email, domain, IP, CIDR, Bitcoin address even in all kinds of sources, including Tor network.	Intelligence X, Haveibeenpwned
Searching for mail patterns	Identifies common patterns in an organization's email addresses. It also helps generate potential email addresses based on employee names and identified syntax.	Email Permutator+, VoilaNorbert, Email Generator, Name2Email
Collection of emails and telephones	Search for personal data such as professional emails and phone numbers. It does this through domains and social networks, especially LinkedIn.	theHarvester, Hunter, RocketReach, Lusha
Metadata extraction	Gets metadata from documents available on target websites, including people names, roles, employee email addresses. These can be used in future attacks.	FOCA, ExifTool
Analysis of relationships and connections	Using data mining and graph analysis to collect and visualize information about specific entities or people, such as domains, emails, and phone numbers.	Maltego

5.3.2. Mitigation measures

To mitigate the risks linked to overexposure of the target's identity, organizations can adopt practices such as training and raising awareness of employees in the safe use of social networks and online platforms. DLP monitoring policies and tools can be implemented to counter search in specialized data leak engines. To prevent the identification of patterns that could serve to identify people, obfuscation of information is recommended, applying techniques such as:

- Data anonymization that involves removing or modifying identifiable information.
- Masking that replaces real data with fake data.
- Depersonalization that alters data so that it cannot be attributed to a specific entity.
- Pseudonymization that replaces unique identifiers with pseudonyms.

You must also control the metadata held by the documents. Although these techniques can be effective, they are not foolproof and must be complemented with robust information security policies.

5.4. T1590 Gather Information from the target's network

This technique focuses on obtaining detailed information about a target organization's network assets and infrastructure to better understand its network environment and potential vulnerabilities. Data collection includes identifying domains, subdomains, virtual servers, IP addresses, and IP blocks assigned to the organization. The primary purpose of this technique is to discover potential entry points into the target's network, which can be of great value to attackers in their efforts to compromise and exploit systems.

To achieve this, attackers use various methods and tools. Among the most common we find some such as identifying domains and subdomains through reverse DNS lookups and Whois queries, employing trackers to discover websites managed by the same team or company, searching the *favicon* in order to identify related subdomains, listing existing assets (such as servers, databases and other resources), investigating virtual servers to discover weaknesses in domains hosted on the same machine, determine blocks of IP addresses and autonomous system numbers (ASNs) assigned to the organization, explore IP ranges to identify additional assets on the same target network, and generate intelligence by trying to reconstruct the target's network topology.

5.4.1. **Subtechniques**

The technique of gathering information from the target network is carried out by several sub-techniques that allow a thorough and detailed exploration of the target network.

Subtechniques	Detail	Tools
Search for domains and subdomains	Perform reverse DNS lookups from the IP ranges obtained from the target, in order to identify possible domains and subdomains associated with those IP addresses. Through the DNS, valuable information can be found, including registered name servers, subdomain records, email servers, and other *target hosts* . They can also identify the use of third-party cloud and SaaS providers through DNS records such as MX and TXT (e.g., SPF).	Reverse DNS of DNSRecon, Hurricane Electric BGP Toolkit
	Through reverse Whois lookup, it is possible to obtain information related to a primary domain, such as the organization name, email addresses, physical addresses, or even other domains and subdomains associated with that primary domain.	Reverse Whois of ViewDNS
	Identify possible sites managed by the same team or company through the search for the technologies used on the target site. Also, you can identify third parties who have a strong link with the target organization.	Trackers like: BuiltWith, PublicWWW, SpyOnWeb
	The *favicon* search consists of looking for the icon that appears in the browser tab when visiting a website, in order to identify possible subdomains associated with the target.	Favihash
	Apply dorking techniques to filter domains or subdomains more accurately. For example, using the name of the target in double quotes, in order to identify possible domains and subdomains associated with the target. Another option is to add some identifying phrase, such as *the copyright* that is included at the end of many websites.	Search engines
	Obtaining domains with a close expiration date can be a vulnerability, since once the domain expires, it can be registered by someone else. To obtain this information, WHOIS services can be used.	Whois, Reverse Whois of ViewDNS

	Asset enumeration based on collecting information about existing assets, including domains, subdomains, IP addresses, servers, databases, and other resources. Enumeration can be passive through open-source query or active, based on dictionary query and *fuzzing*.	DnsRecon, Assetfinder, Subfinder, Amass, CRT, Domain Finder pentestools, Gobuster DNS
Virtual Hosts	The virtual *host*, or virtual server, is a form of web hosting that allows several web pages to run on the same machine. On many occasions, it is possible to find weaknesses not in the target domain, but in the weaker domain hosted on your same server. With *dorking* techniques, you can get a list of websites hosted on a specific IP address and detect domains hosted on the same IP address as the target.	Search engines
IP Lists	IP and ASN lookup consists of determining the IP address block assigned to a given company, as well as its Autonomous System Number (ASN). This information can be useful for identifying other assets that belong to the same organization or are located on the same network. By knowing the range of IP addresses used by a company, it is possible to perform more specific and effective searches when detecting new assets.	IPV4 info, Hurricane Electric BGP Toolkit, Amass
	Searching across the organization or network range involves searching for additional assets that may be on the same target network. This is achieved by using IP range scanning tools. Information can be found about the networks and subnets that belong to the organization in question, which helps identify potential targets. On the other hand, searching through a specific IP range can help discover new devices or servers that are part of the same target network. In this way, new targets can be identified that can be exploited.	Shodan, Censys
Network topologies	Network topology recognition is an activity that attempts to discover and map the structure and design of a network. This information can be useful for inferring the network architecture of the target system and determining the nature of *routers*, *switches*, and other network electronics devices.	Traceroute, Nmap, SNMPwalk, SNMPenum

5.4.2. Mitigation measures

Mitigating the collection of information from the target's network involves a number of interrelated strategies. First, you can improve DNS privacy and log data by using DNS Proxy services to hide the real IP of servers. Whois privacy services may replace the contact information in the Whois record with that of a privacy protection company. To complicate tracking online assets, the system can be configured to automatically switch domains or subdomains at regular intervals. In addition, it is crucial to ensure that HTTP headers and *favicon* information do not reveal the technologies used or the details of the website infrastructure.

Also, there are tools such as JavaScript Obfuscator or ProGuard for Java that can help obfuscate the source code of the website. Likewise, it is important to effectively manage web information and metadata to thwart [34]*dorking* techniques and maintain an updated registry of domains in order to prevent them from falling into the wrong hands. Limiting the exposure of technical details and properly managing access permissions for virtual *hosts* are also critical measures. Finally, segmentation, setting up a correct *firewall*, and using access control lists to limit who can access what part of the network can protect information about the network topology.

5.5. T1591 Gather Information from the target's organization

The technique focuses on collecting valuable data about the organizational structure, strategic employees, policies, and processes of a target organization. This information is useful to attackers as it allows them to better understand the business environment and internal dynamics, which can be used to adapt and refine their attacks more effectively. To carry out this technique, attackers use various methods and tools, such as investigating the target company's website and analyzing its public communications or searching news and social media posts to identify key employees, roles, and organizational structures. They can also search for information about the organization in databases and public records, such as company registration data and patents.

In addition, attackers can employ methods that include monitoring social media and online forums to identify discussions and comments related to the targeted company, its employees, and its products. This can provide useful insights into organizational culture, security concerns, and areas where the company may be vulnerable.

A more aggressive variant that is not analyzed in detail due to its high level of intrusiveness would be the conduct of fictitious interviews with current or former employees. With this, information about the target organization can be obtained, such as details about the work environment, internal structure, projects in development and possible areas of interest.

[3] https://obfuscator.io/

[4] https://www.guardsquare.com/proguard

5.5.1. **Subtechniques**

The collection of information about the target organization is carried out through several sub-techniques. Together they provide a complete and detailed view of your structure.

Subtechniques	Detail	Tools
Search for physical locations	Geolocation of the target's IP addresses to identify locations of servers, offices, and other facilities related to the organization. This can help reveal network infrastructure and potential vulnerabilities.	whois.domaintools, Robtex, Who.is, Viewdns, Shodan
Collection of Information About Related Companies	Search for information about the target and possible related companies to identify partnerships, subsidiaries and other business links that may be relevant to the investigation.	Crunchbase
Search in official bulletins	Review of official bulletins for legal and regulatory information about the organization, such as license records, penalties, fines, and other relevant data that may affect the company or reveal areas of interest.	Manually on official gazette websites, official journals, or public registries
Registration of owners	Investigation of the ownership and ownership of the target organization to identify the owners, managers, and other key people in the company. This can help you understand the structure and control of the organization.	Manually in public registers, business registers, government databases
Account balances	Obtaining financial information, including balance sheets and statements of the target organization, to assess financial health, detect potential problems or areas of interest, and understand the priorities and objectives of the company.	Manually on regulatory body websites, public financial records, annual reports
Organization Policy Information	Gathering information on internal policies, codes of conduct, and other related documents to understand the organization's standards and practices. This can help identify potential vulnerabilities and areas of interest.	Manually on the website of the target organization, search engines
Patent and Intellectual Property Information	Obtaining information on patents and intellectual property associated with the target organization to identify areas of research and development, key technologies, and potential competitive advantages.	Manually in patent databases, public registries, patent office websites and trademarks
Gathering organizational information through other open sources	Obtaining information from the organization, and from employees/roles that handle key information, through social networks and open sources to identify possible objectives and areas of interest. It can also help reveal organizational structure and employee relationships, business opening and closing hours, etc.	RocketReach, Lusha, LinkedIn searches, search engines

5.5.2. Mitigation measures

It is impossible to eliminate all the trace of information of an organization, especially when in many cases what is wanted is precisely that it is public and that it is widely disseminated. To mitigate the risks associated with collecting information about your organization, the important thing is to take information control measures, such as limiting the details available to the public on websites and in public records. In addition, it is essential to carry out security awareness training for employees, so that they understand the risks associated with sharing company information on social networks. Also, a regular security audit should be conducted to detect and address potential overexposures, including reviewing internal policies and intellectual property management.

5.6. T1598 Impersonation to obtain information

Impersonation is a social engineering attack in which the attacker seeks to obtain confidential information, through deception, which can be used later to carry out new attacks by posing as someone else. This type of attack can be targeted at particular individuals, companies, or industries.

Phishing can also use evasive techniques, such as deleting or manipulating emails, metadata, or headers.

Phishing is a technique increasingly used by cybercriminals due to its high success rate and low level of sophistication required for its execution. Despite being classified within the recognition techniques, impersonation is one of the most intrusive active techniques, since it leaves traces and evidence that could expose the attacker, revealing his presence and intentions.

5.6.1. Subtechniques

Information spoofing can be implemented through different variants, allowing attackers to adopt various strategies to obtain the desired information.

Subtechniques	Detail
Email spoofing	It is used to send emails that appear to come from a legitimate source in order to trick the recipient into revealing sensitive information or performing a harmful action. Links to fraudulent external sites and attachments with some kind of malicious *payload* are common.
Text message or instant messaging spoofing	It refers to the use of text messages (SMS) or *smishing* to trick victims into providing personal or financial information. The messages may include malicious links leading to fake websites that appear to be legitimate, or they may ask the victim to respond with sensitive information. More sophisticated examples may impersonate the phone number of companies or individuals.

Voice call spoofing	Phishing through a voice phone call (*vishing*) is a method of social engineering that uses psychological manipulation (such as urgency, threat, or sympathy) to obtain sensitive information from the victim.

5.6.2. **Mitigation measures**

To mitigate information spoofing, it is essential to implement multi-factor authentication and security policies. In the particular case of email, this involves enabling sender authentication (SPF, DKIM, DMARC*), spam* filters, blocking suspicious emails or message encryption. Ongoing training of employees in recognizing *phishing* tactics is also very important. In the case of voice call spoofing, it is crucial to provide training to employees so that they know how to act on suspicious calls.

5.7. T1597 Search for closed sources

It refers to the collection of information from resources and platforms that are not publicly available or that require a certain level of access and authorization to be consulted. These sources can include private databases, closed forums, private networks and groups, internal files, and documents of the organization, among others.

Unlike open sources (OSINT), closed sources may contain more sensitive and specific information, as they are not intended to be shared or accessible by the general public. Information gathered from closed sources can be valuable in gaining a more detailed view of the target organization and discovering vulnerabilities or areas of interest that are not available in open sources.

Access to closed sources can be difficult and, in some cases, require social engineering techniques, such as phishing or establishing trusting relationships with employees or members of the targeted organization. It may also require the use of access credentials, invitations to private groups or the exploitation of security vulnerabilities to access information.

There is the possibility of searching intelligence sources and threats, such as the following, where we can obtain information about the target, information regarding employees or information from systems.

5.7.1. Subtechniques

Under this category you can find various subtechniques depending on the type of information required and the level of access allowed.

Subtechniques	Detail	Tools
Search in engines specialized in data leaks	It employs specialized data leakage intelligence tools, based on input parameters such as email, domain, IP, CIDR, and Bitcoin address. In all kinds of sources, including Tor network.	Intelligence X, Spiderfoot
Private messaging groups	Participation in private messaging groups, such as those in encrypted messaging apps, where information related to vulnerabilities, data breaches, and other security issues is shared and discussed.	Messaging software (Telegram, Signal, WhatsApp, etc.)
Networks and communities of the *Deep* Web or *Dark Web*	Exploration of networks and communities on the Deep Web or Dark Web, where closed sources of information, stolen data and other illicit activities related to cybersecurity can be found.	Specific browsers such as Tor, forums, and markets on the Dark Web (requires technical knowledge and caution when browsing)

5.7.2. Mitigation measures

Mitigation measures again include controlling exposed information and monitoring data leaks.

5.8. T1596 Search open Access technical databases

This technique focuses on the collection of technical and specific information of a target organization through databases and resources that are freely accessible on the Internet. These databases may include patent registrations, technical documents, standards and regulations, product specifications, among others. The information obtained through this technique can provide deeper insight into the products, technologies, and processes used by the target organization, as well as its collaborations and alliances with other organizations. The information collected through databases may include technical details about the products and services offered by the organization, the technologies and processes used to manufacture or develop the products, registered patents, applicable rules, and regulations, among other relevant aspects.

5.8.1. Subtechniques

Each sub-technique allows attackers to gain a more detailed understanding of the technologies, products, and processes implemented by the target organization.

Subtechniques	Detail	Tools
Patent database search	Consultation of detailed information on registered patents, including descriptions of technologies, inventors, and patent holders.	USPTO, EPO, WIPO
Technical document repositories	Access to technical documents, project or product presentations, reports and publications related to various areas of knowledge and technologies of the organization.	arXiv, IEEE Xplore, Google Scholar, ResearchGate, Scribd
Websites of regulatory and standards bodies	Obtaining information on standards, regulations, and technical specifications applicable to products and technologies of the organization.	ISO, IEC, FCC standards
Access to vulnerability and *exploit* databases	Access to databases containing information about known vulnerabilities and *exploits*, including technical details and code examples, about technologies used, or developed by the organization.	National Vulnerability Database (NVD), Exploit Database (EDB), Common Vulnerabilities and Exposures (CVE)

5.8.2. Mitigation measures

Mitigation strategies focus on limiting the public exposure of detailed information and keeping the organization's technology environment up-to-date and secure. Document repositories should be reviewed to prevent the publication of unnecessary details that could be exploited by attackers. The organization should also actively monitor databases for vulnerabilities and *exploits* and apply patches or security updates as they become available to keep the IT infrastructure secure and resilient.

5.9. T1593 Find open domains/websites

This technique refers to the search and collection of information about domains and public websites related to a target organization. Its purpose is to obtain information about the organization's online presence, including details about the products, services, and technologies used by the organization, as well as contact and staff information.

Once websites and domains related to the organization have been identified, attackers can use web application scanning tools to look for vulnerabilities and weaknesses that can be exploited in later phases of an attack.

5.9.1. Subtechniques

We can find several sub-techniques that provide a more detailed view of the organization's digital presence, revealing potential vulnerabilities and areas of interest that could be exploited in future attacks.

Subtechniques	Detail	Tools
Search for domains and subdomains	Search for subdomains associated with the organization's primary domain.	Sublist3r, Recon-ng, Amass, Spiderfoot, search engines.
Searching for SSL certificates	Identification of SSL certificates associated with the organization.	SSLShopper, Censys, CRT.
DNS Information Lookup	Access to DNS records associated with the organization, including email records and mail servers.	Nslookup, Dig, Whois.
Search for public records	Search for public files hosted on your organization's web server, such as backup files, configuration files, and internal documents.	Search Engines, Dirb, Spiderfoot, Wfuzz

5.9.2. Mitigation measures

To minimize the associated risk, organizations can implement a number of measures. These include regular monitoring of domains and subdomains to detect any suspicious changes, proper management of SSL certificates to ensure communication and user privacy, tight control of DNS records to prevent exposure of sensitive information, and secure management of public files to prevent data leakage. The organization's security and privacy policies should be reviewed and updated regularly to reflect changes in infrastructure and emerging threats.

5.10. T1594 Search for victim-owned websites

This technique consists of the search and collection of information about websites or social profiles owned by the target organization that are publicly available on the Internet, with the aim of obtaining technical, organizational, and social information within the digital sites of the organization.

These sites may also have details that highlight the operations and business relationships of the organization's infrastructure and systems, including details about web applications, web servers, and network architecture.

Once the organization's websites have been identified, attackers can use web application scanning tools to look for vulnerabilities and weaknesses that can be exploited. Also, this technique can be used to identify missing patches and security updates.

5.10.1. **Subtechniques**

We can break this technique down into sub-techniques, each aimed at gathering information specific to the target organization's digital assets.

Subtechniques	Detail	Tools
Identifying subdomains	Identification of subdomains associated with the organization's primary domain.	Sublist3r, Recon-ng, Amass, search engines.
Vulnerability scanning	Identification of vulnerabilities in websites owned by the target organization.	Nikto, Burp Suite Scanner, OWASP ZAP, Acunetix, Nessus, Qualys, OpenVAS, Nmap, OpenSCAP.
Search for public records	Identification of public files hosted on your organization's web server, such as backup files, configuration files, and internal documents.	Search engines, Dirb, Wfuzz, HTTrack, Gobuster Fuzz, Spiderfoot, Intelligence X.
Metadata extraction	Extraction of metadata from files and documents hosted on the target organization's web server.	ExifTool, Metagoofil, FOCA.
DNS Information Lookup	Identification of DNS records associated with the organization, including email records and mail servers.	Nslookup, Dig, Whois.
Identification of technologies used	It focuses on identifying the technologies used on the target organization's websites. These technologies may include the operating system of the web server, the web server used, the CMS (content management system), programming language, *plugins*, *frameworks*, and other tools and *software*.	Wappalyzer, BuiltWith, WhatWeb, Nmap, Publicwww, Spyonweb, Whatweb
Website Browsing	Site exploration to reconstruct the map of your website allows: identification of pages and sections of the target website, analysis of the structure of the website and its architecture, identification of links and resources related to the website, identification of multimedia content and other files hosted on the website, identification of forms and web applications, and identification of authentication and restricted access areas.	Wfuzz, Burp Suite Spider, HTTrack, Gobuster, Builtwith.

Searching for information from website source code	Analyzing the source code (HTML, CSS, JavaScript, etc.), allows to identify *frameworks*, libraries, programming languages and possible vulnerabilities. In addition, comments and metadata can be found with sensitive information, specific settings and parameters that could be exploited, as well as the structure of the site and internal links that reveal hidden areas with valuable information.	Search Engine Cache, Wayback Machine
Social Media Search	The analysis of profiles of the target organization in social networks can be used to collect information about its activity, *partners,* or technologies. It is usually a place where organizations share their news. It can also be used to collect information about employees, which can help attackers create more effective *spear-phishing* attacks.	The social networks themselves
Open-source repositories	Exploration of open source and collaborative projects in which organizations and their employees can participate.	GitHub, GitLab, SourceForge

5.10.2. **Mitigation measures**

Organizations can implement regular monitoring of subdomains for suspicious activity, periodic vulnerability scans (and remediation), and secure management of public files to prevent exposure of sensitive information. In addition, they can implement appropriate controls to protect DNS information and practice metadata cleanup before publishing documents or files online. Finally, organizations should be aware of the information they share on social media and open-source repositories and should implement appropriate policies to control this disclosure.

6. Conclusion

Reconnaissance is a tactic used to gain a deep understanding of potential gaps or weaknesses in an organization's systems. It is a fundamental and critical step in any cyberattack or audit, as it provides the adversary with a clear view of the target organization, its infrastructure, and its personnel.

This detailed information, ranging from system architecture to the organization's security culture, can be used by the adversary to support and direct their efforts in other phases of their lifecycle. For example, with the data collected during reconnaissance, the actor can plan and execute an initial access to the organization's systems, using the identified weaknesses to gain a foothold. In addition, after achieving a commitment, you can use the information collected to define and prioritize your objectives, concentrating on the areas that present the greatest opportunity to achieve your ends, whether financial, espionage, service interruption, among others. **Recognition can also be an iterative process** to adjust and improve the strategy based on the information they obtain. For the actor, this may include identifying new vulnerabilities as the organization changes and evolves, seeking additional information can support more sophisticated attacks or improve defensive measures.

The reference to the ***MITRE*** **ATT&CK Enterprise matrix, in the context of reconnaissance techniques, suggests a structured approach to understanding and mitigating cyber threats**. This framework provides a catalog of tactics, techniques, and procedures (TTPs) used to get the maximum information from a target. In point 5 of this study, the techniques, and sub-techniques of recognition of MITRE ATT&CK have been detailed, providing a clear vision of how recognition can be carried out, and what tools they can use. For each technique, mitigation measures have been proposed to reduce their risk.

Reconnaissance techniques can be especially difficult to override or counter with preventative controls, as they rely on behaviors performed outside the reach of business defenses and controls. However, **mitigation actions can be proposed focused on minimizing the amount and sensitivity of data available to external parties**. Doing so can limit the amount of information attackers can collect, reducing the risk of it being used in future attacks. These measures include a variety of approaches, from implementing stricter security controls, or training staff to improve security awareness, to utilizing advanced detection and response tools.

There is no completely effective strategy to mitigate the risks associated with this tactic, so the most appropriate thing is to control the exposed information ensuring that the information that cybercriminals can obtain cannot be used against us, In addition, it is important to adopt a defense-in-depth approach that starts from **training** and **awareness** actions., involves multiple layers of security, considering security as an effort of all members of the organization.

7. Acronyms

- **ASN**: Autonomous System Number
- **ATT&CK**: Adversarial Tactics, Techniques, and Common Knowledge
- **CIDR**: Classless Inter-Domain Routing
- **CVE**: Common Vulnerabilities and Exposures
- **DKIM**: DomainKeys Identified Mail
- **DMARC**: Domain-based Message Authentication, Reporting & Conformance
- **DNS**: Domain Name System
- **DLP**: Data Loss Prevention
- **FCC**: Federal Communications Commisions
- **FIN**: Final (one bit of the TCP header used to terminate the session)
- **HTTP**: Hypertext Transfer Protocol
- **IEC**: International Electrotechnical Commission
- **ICMP**: Internet Control Message Protocol
- **IP**: Internet Protocol
- **ISO**: International Organization for Standardization
- **IT**: Information Technology
- **MX**: Mail eXchange record (a DNS record type)
- **NVD:** National Vulnerability Database
- **OSINT**: Open-Source INTelligence
- **SPF**: Sender Policy Framework
- **SSL**: Secure Sockets Layer
- **SYN**: Synchronize (a bit of the TCP header used to log on)
- **SMS**: Short Message Service
- **TCP**: Transmission Control Protocol
- **TTP**: Tactics, Techniques, and Procedures
- **TXT**: Text record (a DNS record type)
- **UDP**: User Datagram Protocol

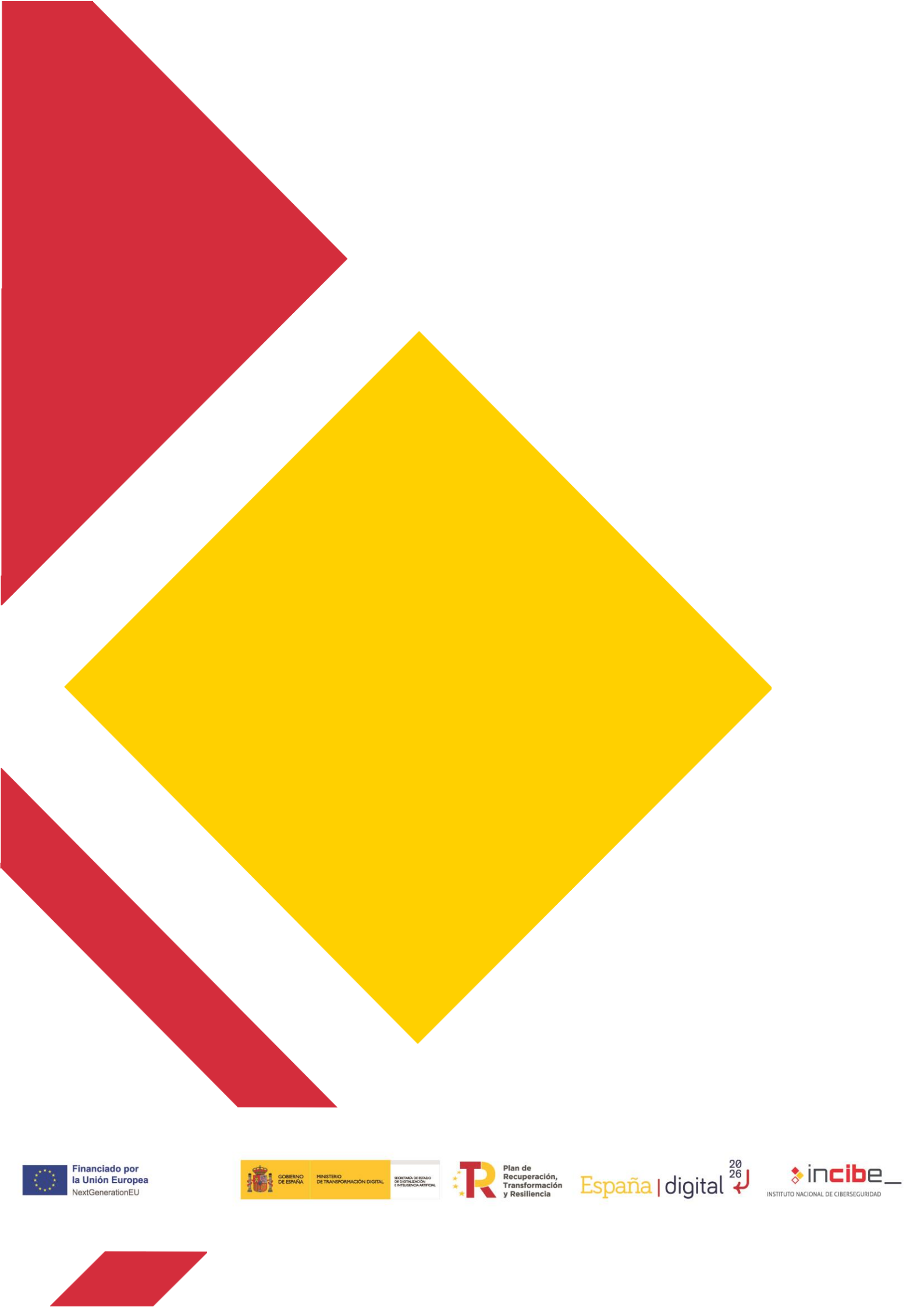
8. Bibliography

Reference	Title, author, date, and web link
[Ref.- 1]	Cyber Reconnaissance Techniques, Wojciech Mazurczyk y Luca Caviglione, Febrero 2021 URL: https://www.researchgate.net/publication/349589737
[Ref.- 2]	Survey and Taxonomy of Adversarial Reconnaissance Techniques, Shanto Roy y otros, ACM Computing Surveys, Diciembre 2022 URL: https://dl.acm.org/doi/pdf/10.1145/3538704
[Ref.- 3]	The not yet exploited goldmine of OSINT: Opportunities, J Pastor-Galindo y otros, IEEE Access, Enero 2020 URL: https://ieeexplore.ieee.org/iel7/6287639/8948470/08954668.pdf
[Ref.- 4]	Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise: Opportunities, Heather J. Williams y Ilana Blum, National Defense Research Institute, Enero 2018 URL: https://apps.dtic.mil/sti/pdfs/AD1053555.pdf
[Ref.- 5]	Best Practices for MITRE ATT&CK® Mapping, CISA, Enero 2023 URL: https://www.cisa.gov/sites/default/files/2023-01/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf

ANNEX 1: Tools

Tool	URL
Acunetix	https://www.acunetix.com/
Amass	https://github.com/owasp-amass/amass
arXiv	https://arxiv.org/
Assetfinder	https://github.com/tomnomnom/assetfinder
BuiltWith	https://builtwith.com/
Burp Suite	https://portswigger.net/burp
Censys	https://censys.io/
CRT	https://crt.sh/
Crunchbase	https://www.crunchbase.com/
DirBuster	https://github.com/KajanM/DirBuster
Dirb	https://www.kali.org/tools/dirb/
DirSearch	https://github.com/maurosoria/dirsearch
DNSRecon	https://github.com/darkoperator/dnsrecon
Whois.Domaintools	https://whois.domaintools.com/
EPO	https://www.epo.org/
ExifTool	https://exiftool.org/
Favihash	https://github.com/m4ll0k/BBTz/blob/master/favihash.py
FOCA	https://github.com/ElevenPaths/FOCA
FCC	https://www.fcc.gov/tags/technical-standards-0
Fping	https://github.com/schweikert/fping
Gobuster	https://github.com/OJ/gobuster
Google Scholar	https://scholar.google.es/
HTTrack	https://www.httrack.com/
Hunter	https://hunter.io/
Hurricane Electric BGP Toolkit	https://bgp.he.net/
Intelligence X	https://intelx.io/
Lusha	https://www.lusha.com/
Maltego	https://www.maltego.com/
Masscan	https://github.com/robertdavidgraham/masscan
Metagoofil	https://www.kali.org/tools/metagoofil/
Name2Email	https://name2email.com/
Nessus	https://es-la.tenable.com/products/nessus
Nikto	https://github.com/sullo/nikto
Nmap	https://nmap.org/
Nslookup	https://linux.die.net/man/1/nslookup
OpenSCAP	https://www.open-scap.org/
OpenVAS	https://openvas.org/
OwaspZap	https://www.zaproxy.org/
Pentestools	https://pentest-tools.com/information-gathering/find-subdomains-of-domain
p0f	https://www.kali.org/tools/p0f/
Qualys	https://www.qualys.com/
Recon-ng	https://github.com/lanmaster53/recon-ng
ResearchGate	https://www.researchgate.net/
Reverse DNS (DNS-recon)	https://github.com/darkoperator/dnsrecon
Reverse Whois	https://viewdns.info/reversewhois/

Robtex	https://www.robtex.com/
RocketReach	https://rocketreach.co/
Shodan	https://www.shodan.io/
SNMPenum	https://www.kali.org/tools/snmpenum/
SNMPwalk	http://www.net-snmp.org/
Spiderfoot	https://github.com/smicallef/spiderfoot
SpyOnWeb	https://api.spyonweb.com/
SSLShopper	https://www.sslshopper.com/ssl-checker.html
Subfinder	https://github.com/projectdiscovery/subfinder
Sublist3r	https://github.com/aboul3la/Sublist3r
TheHarvester	https://github.com/laramies/theHarvester
USPTO	https://www.uspto.gov/
VoilaNorbert	https://www.voilanorbert.com/email-finder/
Wappalyzer	https://www.wappalyzer.com/
WhatWeb	https://github.com/urbanadventurer/WhatWeb
WIPO	https://www.wipo.int/portal/en/index.html
Wfuzz	https://github.com/xmendez/wfuzz


Financiado por
la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO DE TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD