TLP:CLEAR

España | digital 2026

Estudio de herramientas para la actividad de reconocimiento

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

TLP:CLEAR

septiembre 2023

INCIBE-CERT_ESTUDIO_DE_HERRAMIENTAS_DE_RECONOCIMIENTO_2023_v1.0

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/.

Índice

1. Sobre este estudio 5
2. Organización del documento 6
3. Introducción 7
4. La técnica de reconocimiento 8
5. Técnicas y herramientas 11
5.1. T1595 Escaneo activo 11
5.1.1. Subtécnicas 11
5.1.2. Medidas de mitigación 13
5.2. T1592 Recopilar información sobre los *hosts* del objetivo 13
5.2.1. Subtécnicas 13
5.2.2. Medidas de mitigación 14
5.3. T1589 Recoger información sobre la identidad del objetivo 15
5.3.1. Subtécnicas 15
5.3.2. Medidas de mitigación 16
5.4. T1590 Reunir información de la red del objetivo 16
5.4.1. Subtécnicas 16
5.4.2. Medidas de mitigación 19
5.5. T1591 Reunir información de la organización del objetivo 19
5.5.1. Subtécnicas 20
5.5.2. Medidas de mitigación 21
5.6. T1598 Suplantación para obtener información 21
5.6.1. Subtécnicas 21
5.6.2. Medidas de mitigación 22
5.7. T1597 Búsqueda de fuentes cerradas 22
5.7.1. Subtécnicas 23
5.7.2. Medidas de mitigación 23
5.8. T1596 Buscar en bases de datos técnicas de libre acceso 23
5.8.1. Subtécnicas 24
5.8.2. Medidas de mitigación 24
5.9. T1593 Buscar dominios/sitios web abiertos 25
5.9.1. Subtécnicas 25
5.9.2. Medidas de mitigación 25
5.10. T1594 Búsqueda de sitios web propiedad de las victimas 25
5.10.1. Subtécnicas 26
5.10.2. Medidas de mitigación 27

6. Conclusión 29
7. Acrónimos 30
8. Bibliografía 31
ANEXO 1: Herramientas 32

1. Sobre este estudio

La táctica de reconocimiento es un proceso fundamental en la ciberseguridad, que tiene como objetivo obtener información detallada sobre los sistemas y redes que se desea atacar o defender. En este sentido, el presente estudio se centra en esta táctica, su **aplicación** en distintos escenarios y las **medidas de mitigación** que pueden ser implementadas para prevenir posibles ataques.

La guía tiene un enfoque técnico, destinado a explicar todos los aspectos relacionados con la táctica de reconocimiento, tanto para usuarios que la desconocen, como para aquellos que desean mejorar las características de seguridad de sus sistemas y redes.

El orden de los contenidos está estructurado de manera que se comience con una explicación teórica general sobre los conceptos más importantes, para luego enfocarse en la explicación de técnicas y subtécnicas particulares, indicando alguna de las herramientas que se pueden emplear en cada caso.

En resumen, el objetivo de este estudio es proporcionar una guía detallada sobre la táctica de reconocimiento y su importancia en el ámbito de la ciberseguridad, con el objetivo principal de ayudar a las organizaciones a comprender mejor cómo los atacantes pueden recopilar información sobre ellas y sus sistemas, y cómo pueden mitigarse los riesgos asociados a esta táctica.

2. Organización del documento

Este estudio se centra en la táctica de reconocimiento, ampliamente utilizada en los ejercicios de Red Team y análisis de seguridad. Se comienza con la **3.- Introducción**, que establece el contexto y la importancia del reconocimiento en los ciberataques, destacando cómo los atacantes utilizan esta técnica para recopilar información que puede ser utilizada para planificar futuras operaciones.

Posteriormente, se enmarca la **4.- La técnica de reconocimiento** en el *framework* de referencia MITRE ATT&CK y sus TTP, centrándose específicamente en cómo recopilar información valiosa sobre el objetivo.

Una vez introducido y establecido el marco de referencia, se abordan las **5.- Técnicas y herramientas**, donde se desgranan las diferentes subtécnicas y herramientas posibles para llevarlas a cabo. Además, se proponen medidas de mitigación que las organizaciones pueden adoptar para reducir el riesgo asociado, que incluyen desde recomendaciones generales, hasta estrategias específicas que pueden utilizarse para detectar y prevenir el reconocimiento.

Finalmente, en la **6.- Conclusión**, se resumen los principales puntos del documento, proporcionando algunas recomendaciones sobre cómo pueden mejorar su seguridad ante la táctica del reconocimiento. Estas recomendaciones incluyen la importancia de limitar la cantidad y calidad de la información pública disponible, adoptar herramientas de detección y respuesta avanzadas y mejorar la formación y concienciación de los empleados.

3. Introducción

El reconocimiento ha sido una táctica fundamental a lo largo de la historia de la ciberseguridad, desde los primeros días de la informática y la seguridad de la red, cuando los primeros hackers exploraban sistemas por curiosidad, por reto personal o en busca de reconocimiento; hasta la actualidad, donde los expertos en seguridad buscan detectar vulnerabilidades en sus propios sistemas, para solucionarlas antes de que puedan ser aprovechadas por los atacantes.

El reconocimiento ha evolucionado con el paso del tiempo, hasta convertirse en una táctica muy sofisticada y estructurada, útil para entender los sistemas y las redes. De la misma forma, las herramientas utilizadas han ido mejorando y automatizando las tareas de escaneos de puertos, búsqueda de información en línea o pruebas de penetración.

A medida que los sistemas y las redes se volvieron más complejos, la importancia del reconocimiento creció. **Hoy en día, el reconocimiento es una fase crucial en el proceso de hacking ético y análisis de seguridad**, y se utiliza para descubrir vulnerabilidades, fallos de configuración, o datos sensibles expuestos sobre sistemas y redes en todas las industrias, desde las empresas privadas hasta los sistemas críticos de infraestructura o las agencias gubernamentales, y por supuesto, las personas.

Durante esta fase, se recopila información a través de diferentes técnicas y herramientas con el **objetivo obtener la mayor cantidad de información posible** sobre el sistema o red en cuestión, sin dañar la integridad del sistema**.** Una vez que se recopila la información necesaria, los expertos en seguridad pueden analizarla para identificar posibles debilidades que podrían ser explotadas. De esta manera, se pueden implementar medidas de protección para evitar posibles ataques o compromisos de seguridad.

Es importante destacar que la táctica de reconocimiento **no solo es utilizada por expertos en seguridad, sino también por atacantes malintencionados**. De hecho, es común que los ciberdelincuentes realicen un reconocimiento previo antes de lanzar un ataque para conocer las debilidades de la red o sistema objetivo. Por lo tanto, es esencial que las empresas y organizaciones estén al tanto de esta táctica y tomen medidas para protegerse.

4. La técnica de reconocimiento

Para la elaboración de este estudio, se ha tomado como referencia el marco MITRE ATT&CK, que brinda una base de conocimiento global sobre tácticas, técnicas y procedimientos (TTP) de los adversarios, es decir, las acciones ofensivas que pueden ser utilizadas contra los sistemas y que han sido recopiladas, clasificadas y categorizadas con una taxonomía en común, a partir de eventos observados en la vida real[1] . Esta herramienta proporciona información detallada acerca de más de 100 grupos de actores de amenazas. Por medio del uso de ATT&CK, es posible identificar y evaluar brechas defensivas, así como también las capacidades de las herramientas de seguridad. Este marco puede ser utilizado para ejecutar análisis de seguridad o de respuesta a incidentes, la búsqueda de amenazas, participación en actividades de *Red Team* o la validación de controles de mitigación, entre otras.

Las matrices MITRE ATT&CK son una representación visual del marco ATT&CK que se utiliza para proporcionar una vista contextualizada de las TTP durante el ciclo de vida del ataque. Aunque existen diferentes tipos de matrices, nos centraremos en la Enterprise[2],ya que es de interés para la mayor parte de las organizaciones, la cual cubre diferentes etapas del ciclo de vida de un ataque en el ámbito TIC, con objetivos específicos que los atacantes persiguen. Estos objetivos también se conocen como **tácticas**, y sirven para categorizar y organizar técnicas concretas. Entre ellas encontramos: el reconocimiento, el desarrollo de recursos, el acceso inicial, la ejecución, la persistencia, la escalada de privilegios, la evasión de la defensa, el acceso a credenciales, el descubrimiento, el movimiento lateral, la colección, el comando y control, la exfiltración y el impacto.

En el contexto de las **tácticas**, es importante entender la relación entre actores de amenaza, herramientas y técnicas. Los actores de amenaza son los individuos o grupos que llevan a cabo los ataques. Las **técnicas** son los métodos utilizados para llevarlos a cabo, y las **herramientas** son los programas o dispositivos utilizados en la práctica. La Figura 1 explica gráficamente esta relación.

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

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

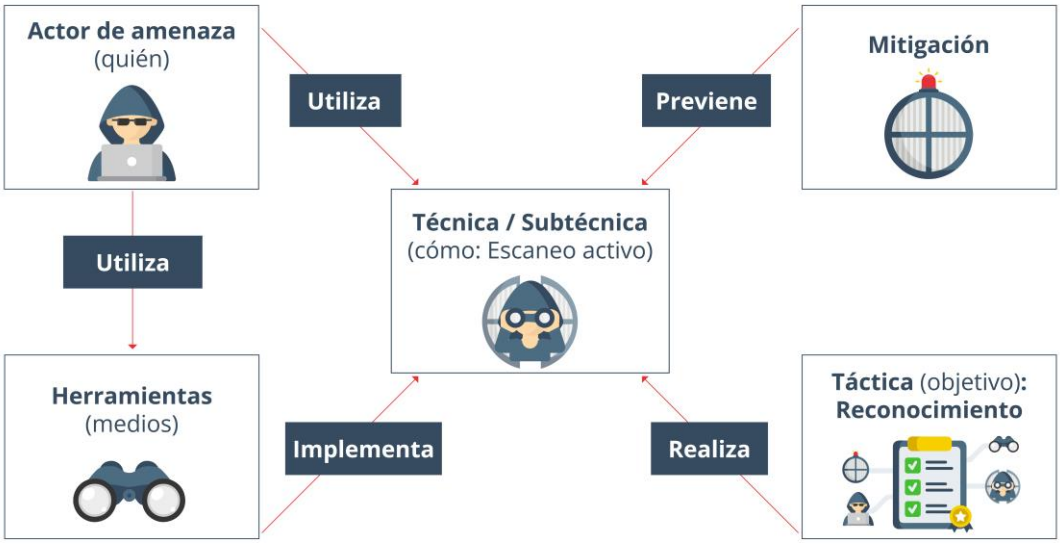


Figura 1 - Relación actor-técnica-herramienta

El **reconocimiento** es una de las tácticas más importantes durante la fase de planificación, debido a que proporciona a los atacantes información crucial para tomar decisiones y organizar la ejecución del ataque conforme a sus objetivos. Implica recopilar información sobre el objetivo de la red, como la topología de la red, los sistemas, los servicios que se ejecutan, las credenciales de usuario, etc., que permita a los atacantes identificar vulnerabilidades y puntos débiles del objetivo, para poder seleccionar y ejecutar ataques específicos con un mayor grado de éxito. Además, el reconocimiento también puede ayudar a los atacantes a evitar ser detectados ya que, si los atacantes conocen la estructura y las herramientas de seguridad utilizadas en la red, podrán adaptar sus ataques para eludir la detección por parte de los sistemas de seguridad de la red.

La matriz *Enterprise* establece 10 técnicas diferentes dentro del reconocimiento, algunas de estas técnicas incluyen el uso de herramientas de búsqueda de información pública, la exploración de servicios de red, la búsqueda de información en redes sociales y la recolección de información en correos electrónicos. **Es importante tener en cuenta que las técnicas de reconocimiento pueden ser utilizadas tanto por actores malintencionados, como por equipos de seguridad para evaluar la exposición y mejorar la postura de seguridad de una organización**. Por lo tanto, conocer estas técnicas y estar preparados es fundamental para prevenir y detectar posibles amenazas. A continuación, presentamos las técnicas de reconocimiento más representativas junto con sus identificadores:

- **T1595 Escaneo activo**: enviar paquetes a un sistema o red para obtener información sobre los servicios, puertos y sistemas operativos que se ejecutan en ellos.
- **T1592 Recopilar información sobre los hosts del objetivo**: buscar información sobre los *hosts* que forman parte de la infraestructura del objetivo, como direcciones IP, nombres de *host* y sistemas operativos.

- **T1589 Recoger información sobre la identidad del objetivo**: obtener información sobre los empleados y usuarios del objetivo, como nombres, direcciones de correo electrónico, números de teléfono y roles en la organización.
- **T1590 Reunir información de la red del objetivo**: recopilar información sobre la arquitectura y topología de la red del objetivo, incluyendo los dispositivos de red, los segmentos de red y los protocolos utilizados.
- **T1591 Reunir información de la organización del objetivo**: buscar información sobre la estructura organizativa, políticas y procedimientos del objetivo.
- **T1598 Suplantación de información**: utilizar técnicas para hacerse pasar por una entidad confiable y obtener información sobre el objetivo.
- **T1597 Búsqueda de fuentes cerradas**: buscar información en fuentes no públicas, como foros privados o redes de intercambio de información entre delincuentes.
- **T1596 Buscar en bases de datos técnicas de libre acceso**: utilizar herramientas de búsqueda y consultas en bases de datos de libre acceso para obtener información sobre el objetivo.
- **T1593 Buscar dominios/sitios web abiertos**: identificar y buscar información sobre dominios y sitios web que pertenecen al objetivo y que están disponibles públicamente.
- **T1594 Búsqueda de sitios web propiedad de las víctimas**: buscar sitios web que pertenecen a la organización del objetivo, y que están disponibles públicamente para obtener información sobre la infraestructura y los sistemas de la organización.

Estas técnicas de referencia serán de gran ayuda para clasificar diferentes herramientas existentes dentro del estado del arte.

5. Técnicas y herramientas

El reconocimiento es una etapa crucial en cualquier ejercicio de red *teaming* o *pentesting*. La mayor parte de sus técnicas se basan en **Open Source Intelligence (OSINT)**, una estrategia de recopilación de información que utiliza fuentes de información públicas y abiertas para obtener información sobre un objetivo como redes sociales, motores de búsqueda, bases de datos públicas y sitios web. La información obtenida puede incluir detalles sobre la infraestructura del objetivo, direcciones IP, nombres de dominio, correos electrónicos, nombres de usuarios, contraseñas, nombres de empleados, ubicaciones físicas, datos de contacto, información sobre productos y servicios, y cualquier otra información relevante que pueda ser útil para llevar a cabo una operación de seguridad.

Para llevar a cabo el reconocimiento de manera correcta, es necesario seguir las **reglas de compromiso** que establecen límites y condiciones en el uso de técnicas y herramientas. Estas reglas suelen incluir directrices sobre los sistemas que se pueden y no se pueden escanear, la hora del día en la que se pueden realizar pruebas, los datos que se pueden recopilar y la forma en que se pueden utilizar, entre otros aspectos.

En esta sección se describen algunas de las técnicas y herramientas de reconocimiento más comunes utilizadas en estos ejercicios, desde el escaneo de puertos hasta herramientas para la búsqueda de información sobre objetivos.

5.1. T1595 Escaneo activo

Se trata de la técnica utilizada para identificar los servicios y sistemas en una red, así como sus vulnerabilidades y configuraciones. Esta técnica implica enviar paquetes de red a los sistemas objetivo para obtener información sobre sus puertos abiertos, sistemas operativos, aplicaciones y versiones.

El nivel de intrusividad del escaneo activo puede variar dependiendo de la configuración de los sistemas objetivo y la cantidad de paquetes enviados, pero en general, es considerada más agresiva que el escaneo pasivo, ya que involucra enviar tráfico de red a los sistemas objetivo. Esta técnica puede ser detectada por herramientas de defensa, como los sistemas de detección de intrusiones y deja un rastro en forma de direcciones IP o información sobre la tecnología utilizada, lo que aumenta las posibilidades de descubrimiento del operativo del equipo de reconocimiento. Por esta razón, los *pentesters* o miembros del *Red Team*, deberán ser cautelosos al utilizar esta técnica, tomando medidas para pasar inadvertidos, como el uso de técnicas de ocultación de la dirección IP o el ajuste de la velocidad de escaneo.

5.1.1. Subtécnicas

Existen diversas subtécnicas de escaneo activo que se utilizan en la identificación de sistemas y servicios en una red. Algunas de las más utilizadas son:

Subtécnica	Detalle	Herramientas
Obtención de respuestas ICMP en un rango de IP o dominio	La obtención de respuestas ICMP (Internet Control Message Protocol) es una opción utilizada para determinar si un *host* está activo o en línea. Una de las formas más comunes de utilizar ICMP para la obtención de información es mediante el envío de paquetes "echo request" utilizando la herramienta Ping. Si el *host* objetivo está activo y en línea, responderá al paquete "echo request" con un paquete "echo reply". Si no se recibe una respuesta o si se recibe un mensaje de error ICMP, podría indicar que el *host* objetivo está inactivo, inaccesible o bloqueando el tráfico ICMP.	Ping, Fping, Traceroute
Escaneo de puertos TCP en un rango de IP o dominio	Se fundamenta en enviar paquetes TCP a un rango de puertos en un sistema objetivo para determinar si están abiertos o cerrados. Existen varios tipos de escaneos de puertos TCP, como SYN scan, Connect scan, FIN scan, Xmas scan y Null scan. Cada uno de estos métodos utiliza diferentes alternativas para interactuar con los puertos del sistema objetivo y determinar su estado.	Nmap, Masscan
Escaneo de puertos UDP en un rango de IP o dominio	Consiste en enviar paquetes UDP a un rango de puertos en un sistema objetivo para determinar si están abiertos o cerrados. Esta opción es más difícil de realizar que el escaneo de puertos TCP debido a que los sistemas pueden no enviar una respuesta si el puerto está cerrado, lo que hace que el escaneo sea más lento.	Nmap, Masscan
Escaneo de vulnerabilidades en un rango de IP o dominio	Se envían paquetes diseñados específicamente para reconocer vulnerabilidades existentes en los sistemas objetivo. Esta alternativa puede ser muy intrusiva y debe ser realizada con precaución, ya que puede ser detectada y bloqueada por los sistemas de defensa.	OpenVas, OwaspZap.
Escaneo mediante diccionario en un rango de IP o dominio	La idea es probar múltiples combinaciones de palabras o caracteres (tomadas normalmente de un diccionario) habituales en la infraestructura de red dentro de un rango de direcciones IP o en un dominio objetivo para identificar información sensible de la red.	DirBuster, Dirsearch, Gobuster

5.1.2. Medidas de mitigación

Es imposible eliminar por completo el riesgo de escaneo activo, ya que queda fuera del control de la organización. Sin embargo, se pueden implementar medidas para reducir la superficie de exposición, como limitar la apertura de puertos a los necesarios y modificar los puertos estándar utilizados por los servicios con el fin de dificultar su reconocimiento. Además, es posible detectar patrones de escaneo mediante el análisis de *logs* y activar reglas de bloqueo en el *firewall* para prevenir futuros intentos de escaneo. Con estas medidas, se puede reducir significativamente el riesgo y mejorar la seguridad de la red.

5.2. T1592 Recopilar información sobre los *hosts* del objetivo

Esta técnica se centra en obtener detalles sobre los sistemas, servicios y configuraciones de los sistemas. Es esencial para la identificación de posibles vulnerabilidades y ayuda a los profesionales de seguridad a planificar y llevar a cabo pruebas de seguridad de manera eficiente y eficaz. Puede ser tanto pasiva como activa, dependiendo del enfoque y las herramientas utilizadas.

- En el caso de un enfoque pasivo, se recolecta información sin interactuar directamente con los sistemas objetivo. Por ejemplo, se pueden utilizar motores de búsqueda especializados como Shodan para obtener información sobre direcciones IP, servicios y puertos abiertos en los sistemas objetivo sin enviarles tráfico de red. También, se puede recopilar información a través de la extracción de metadatos de documentos públicos, con el *software* con el que fueron creados, o su versión.
- Por otro lado, un enfoque activo implica interactuar directamente con los sistemas objetivo, enviándoles tráfico de red directamente. A diferencia del escaneo activo, se utiliza para obtener información más precisa relacionada con los *hosts*, como las versiones o arquitecturas de sus sistemas. Estos enfoques activos pueden ser más intrusivos y, por lo tanto, conllevan un mayor riesgo de ser detectados por los sistemas de defensa.

5.2.1. Subtécnicas

Existen diversas subtécnicas empleadas en la recopilación de información sobre los *hosts* del objetivo. Algunas de ellas son:

Subtécnica	Detalle	Herramientas
Búsqueda de información a partir de IP o dominios a través de indexadores	Permite obtener información sobre direcciones IP, como sus servicios y puertos abiertos, potenciales vulnerabilidades, ubicación física o datos del *hosting*. Todo ello a través de información que se muestran en la cabecera de la respuesta del servidor web a una solicitud de conexión.	Shodan, Censys

Extracción de metadatos	Esta opción se utiliza principalmente para encontrar metadatos e información oculta en los documentos que se escanean dentro del objetivo. Estos documentos pueden estar en páginas web y pueden descargarse y analizarse con herramientas específicas. Entre los metadatos, se puede descubrir información sobre los *hosts* como puede ser el dispositivo donde se elaboró el documento, rutas del espacio de usuario o el *software* utilizado por los mismos.	FOCA, ExifTool
Recolección de configuraciones en fuentes públicas	La recolección de configuraciones es una subtécnica utilizada por adversarios para obtener detalles sobre parámetros del sistema como información de las arquitecturas, zonas horarias, idiomas, etc. Por ejemplo, a través de la monitorización de foros públicos, perfiles de redes sociales y otros recursos en línea donde los usuarios objetivo puedan discutir sus configuraciones de sistema.	Motores de búsqueda, foros
Reconocimiento de sistemas operativos o *fingerprinting* en un rango de IP o dominio	Se basa en enviar paquetes a un sistema objetivo para determinar su sistema operativo, a partir de la respuesta recibida. Se puede obtener información sobre la versión y el tipo de sistema operativo que se está ejecutando. Un ejemplo es a través del parámetro `-O` de Nmap.	Nmap, p0f
Enumeración de servicios en un rango de IP o dominio	Mediante el envío de paquetes a un sistema objetivo, se determinan los servicios que se están ejecutando en él a partir de la respuesta recibida. Se puede obtener información sobre el tipo y la versión del servicio que se está ejecutando.	Nmap, OpenVas, Nessus, OwaspZap

5.2.2. **Medidas de mitigación**

La técnica, aunque no puede ser mitigada completamente, debido a que se basa en acciones llevadas a cabo fuera del alcance de los controles de seguridad empresariales, puede ser atenuada de manera efectiva a través de una serie de medidas proactivas. Las organizaciones deben minimizar la cantidad de datos técnicos y sensibles expuestos públicamente, lo que incluye restringir la información de metadatos en documentos y limitar la información del servidor en las cabeceras de respuesta. También es esencial mantener actualizados los sistemas operativos y las aplicaciones, aplicar regularmente parches de seguridad y emplear controles de seguridad robustos. En términos de información obtenida de foros públicos y redes sociales, una política de privacidad y seguridad sólida y bien

comunicada, puede ayudar a limitar la información que los empleados comparten públicamente.

5.3. T1589 Recoger información sobre la identidad del objetivo

Obtener la información sobre las identidades de individuos, grupos o sistemas dentro de una organización objetivo es de gran interés para los atacantes, para comprender mejor la estructura de la organización, las relaciones entre sus miembros, roles y responsabilidades. Esto permite planificar futuros ataques o crear campañas de ingeniería social mejor dirigidas, más convincentes y eficaces.

5.3.1. Subtécnicas

Podemos identificar algunas subtécnicas ligadas a la recogida de información sobre la identidad del objetivo, como, por ejemplo:

Técnica	Detalle	Herramientas
Búsqueda en motores generalistas	Utiliza operadores de búsqueda (*dorking*) para filtrar información en buscadores, permitiendo obtener datos como correos electrónicos, nombres de empleados y credenciales.	Motores de búsqueda, LinkedIn
Búsqueda en motores especializados en fugas de datos	Emplea herramientas de inteligencia especializadas de fuga de datos a partir de parámetros de entrada como correo electrónico, dominio, IP, CIDR, dirección de Bitcoin incluso en todo tipo de fuentes, incluyendo red Tor.	Intelligence X, Haveibeenpwned
Búsqueda de patrones de correo	Identifica patrones comunes en las direcciones de correo electrónico de una organización. También, ayuda a generar posibles direcciones de correo electrónico basadas en los nombres de empleados y la sintaxis identificada.	Email Permutator+, VoilaNorbert, Email Generator, Name2Email
Recopilación de correos y teléfonos	Búsqueda de datos personales como correos electrónicos profesionales y números de teléfono. Lo hace a través de dominios y redes sociales, especialmente LinkedIn.	theHarvester, Hunter, RocketReach, Lusha
Extracción de metadatos	Obtiene metadatos de documentos disponibles en sitios web del objetivo, incluyendo nombre de personas, roles, direcciones de correo de empleados. Estos pueden ser utilizadas en futuros ataques.	FOCA, ExifTool
Análisis de relaciones y conexiones	Uso de la minería de datos y el análisis de grafos para recopilar y visualizar información sobre entidades o personas específicas, como dominios, correos electrónicos y números de teléfono.	Maltego

5.3.2. Medidas de mitigación

Para mitigar los riesgos ligados a la sobreexposición de la identidad del objetivo, las organizaciones pueden adoptar prácticas como la formación y concienciación de los empleados en el uso seguro de las redes sociales y plataformas en línea. Se pueden implementar políticas y herramientas de monitoreo de DLP para contrarrestar la búsqueda en motores especializados en fugas de datos. Para prevenir la identificación de patrones que podrían servir para identificar a personas, se recomienda la ofuscación de la información, aplicando técnicas como:

- Anonimización de datos que implica eliminar o modificar información identificable.
- Enmascaramiento que reemplaza datos reales con falsos.
- despersonalización que altera los datos para que no puedan ser atribuidos a una entidad específica.
- Pseudonimización que sustituye los identificadores únicos con pseudónimos.

También se deben controlar los metadatos que poseen los documentos. Aunque estas técnicas pueden ser efectivas, no son infalibles y deben complementarse con políticas robustas de seguridad de la información.

5.4. T1590 Reunir información de la red del objetivo

Esta técnica se centra en obtener información detallada sobre los activos y la infraestructura de red de una organización objetivo para comprender mejor su entorno de red y potenciales vulnerabilidades. La recopilación de datos incluye la identificación de dominios, subdominios, servidores virtuales, direcciones IP y bloques de IP asignados a la organización. El propósito principal de esta técnica es descubrir posibles puntos de entrada en la red del objetivo, lo que puede ser de gran valor para los atacantes en sus esfuerzos por comprometer y explotar sistemas.

Para lograr esto, los atacantes utilizan diversos métodos y herramientas. Entre las más comunes encontramos algunas como identificar dominios y subdominios a través de búsquedas inversas de DNS y consultas Whois, emplear rastreadores para descubrir sitios web gestionados por el mismo equipo o empresa, buscar el *favicon* con el objetivo de identificar subdominios relacionados, enumerar activos existentes (como servidores, bases de datos y otros recursos), investigar servidores virtuales para descubrir debilidades en dominios alojados en la misma máquina, determinar bloques de direcciones IP y números de sistema autónomo (ASN) asignados a la organización, explorar rangos de IP para identificar activos adicionales en la misma red objetivo, y generar inteligencia tratando de reconstruir la topología de red del objetivo.

5.4.1. Subtécnicas

La técnica de recopilación de información de la red del objetivo se lleva a cabo mediante varias subtécnicas que permiten una exploración exhaustiva y detallada de la red objetivo.

Subtécnica	Detalle	Herramientas
Búsqueda de dominios y subdominios	Realizar búsquedas inversas de DNS a partir de los rangos de IP obtenidos del objetivo, con el fin de identificar posibles dominios y subdominios asociados a esas direcciones IP. A través del DNS se puede encontrar información valiosa, incluyendo servidores de nombres registrados, registros de subdominios, servidores de correo electrónico y otros *hosts* del objetivo. También, pueden identificar el uso de proveedores de nube y SaaS de terceros a través de los registros DNS como MX y TXT (por ejemplo, SPF).	Reverse DNS de DNSRecon, Hurricane Electric BGP Toolkit
	A través de la búsqueda inversa de Whois, es posible obtener información relacionada con un dominio principal, como el nombre de la organización, direcciones de correo electrónico, direcciones físicas, o incluso otros dominios y subdominios asociados a ese dominio principal	Reverse Whois de ViewDNS
	Identificar posibles sitios gestionados por el mismo equipo o compañía a través de la búsqueda de las tecnologías utilizadas en el sitio objetivo. También, se puede identificar a terceros que tienen una fuerte vinculación con la organización objetivo.	Rastreadores como: BuiltWith, PublicWWW, SpyOnWeb
	la búsqueda del *favicon* consiste en buscar el icono que aparece en la pestaña del navegador al visitar un sitio web, con el fin de identificar posibles subdominios asociados al objetivo.	Favihash
	Aplicar técnicas de dorking para filtrar con mayor precisión dominios o subdominios. Por ejemplo, utilizando el nombre del objetivo entre comillas dobles, con el fin de identificar posibles dominios y subdominios asociados al objetivo. Otra opción es añadir alguna frase identificativa, como el *copyright* que se incluye al final de muchos sitios web.	Motores de búsqueda
	La obtención de dominios con fecha cercana de expiración puede suponer una vulnerabilidad, ya que una vez que el dominio expire, puede ser registrado por otra persona. Para obtener esta información, se pueden utilizar servicios de WHOIS	Whois, Reverse Whois de ViewDNS

	Enumeración de activos basada en la recolección de información sobre los activos existentes, incluyendo dominios, subdominios, direcciones IP, servidores, bases de datos y otros recursos. La enumeración puede ser pasiva a través de la consulta de fuentes abiertas o activa, basada en la consulta por diccionario y *fuzzing*.	DnsRecon, Assetfinder, Subfinder, Amass, CRT, buscador de dominios de pentestools, Gobuster DNS
Virtual Hosts	El virtual *host*, o servidor virtual, es una forma de alojamiento web que permite que varias páginas web puedan funcionar en una misma máquina. Es muchas ocasiones, es posible encontrar debilidades no en el dominio objetivo, sino en el dominio más débil alojado en su mismo servidor. Con las técnicas de *dorking* se puede obtener una lista de sitios web alojados en una dirección IP específica y detectar dominios alojados en la misma dirección IP que el objetivo.	Motores de búsqueda
Listas de IP	La búsqueda de IP y ASN consiste en determinar el bloque de direcciones IP asignado a una determinada compañía, así como su Autonomous System Number (ASN). Esta información puede ser útil para identificar otros activos que pertenezcan a la misma organización o que estén ubicados en la misma red. Al conocer el rango de direcciones IP utilizado por una compañía, es posible realizar búsquedas más específicas y efectivas a la hora de detectar nuevos activos.	IPV4 info, Hurricane Electric BGP Toolkit, Amass
	Realizar búsquedas a través de la organización o rango de red implica buscar activos adicionales que pueden estar en la misma red objetivo. Esto se logra mediante el uso de herramientas de escaneo de rango de IP. Se puede encontrar información sobre las redes y subredes que pertenecen a la organización en cuestión, lo que ayuda a identificar posibles objetivos. Por otro lado, buscar a través de un rango de IP específico puede ayudar a descubrir nuevos dispositivos o servidores que forman parte de la misma red objetivo. De esta manera, se pueden identificar nuevos objetivos que pueden ser explotados.	Shodan, Censys

Topologías de red	El reconocimiento de topologías de red es una actividad en la que se intenta descubrir y mapear la estructura y el diseño de una red. Esta información puede ser útil para inferir en la arquitectura de red del sistema objetivo y determinar la naturaleza de *routers*, *switches* y otros dispositivos de electrónica de red.	Traceroute, Nmap, SNMPwalk, SNMPenum

5.4.2. Medidas de mitigación

Mitigar la recopilación de información de la red del objetivo implica una serie de estrategias interrelacionadas. Primero, se puede mejorar la privacidad del DNS y los datos de registro utilizando servicios de DNS Proxy para ocultar la IP real de los servidores. Los servicios de privacidad de Whois pueden reemplazar la información de contacto en el registro de Whois por la de una empresa de protección de privacidad. Para complicar el seguimiento de los activos en línea, se puede configurar el sistema para cambiar automáticamente de dominio o subdominio en intervalos regulares. Además, es crucial asegurar que las cabeceras HTTP y la información del *favicon* no revelen las tecnologías utilizadas ni los detalles de la infraestructura del sitio web. También, existen herramientas como JavaScript Obfuscator[3] o ProGuard[4] para Java que pueden ayudar a ofuscar el código fuente del sitio web. Igualmente, es importante gestionar eficazmente la información web y los metadatos para frustrar las técnicas de *dorking* y mantener un registro actualizado de los dominios con el fin de evitar que caigan en manos equivocadas. Limitar la exposición de detalles técnicos y gestionar adecuadamente los permisos de acceso para los *hosts* virtuales también son medidas fundamentales. Por último, la segmentación, la configuración de un *firewall* correcta y el uso de listas de control de acceso para limitar quién puede acceder a qué parte de la red, pueden proteger la información sobre la topología de la red.

5.5. T1591 Reunir información de la organización del objetivo

La técnica se centra en recopilar datos valiosos sobre la estructura organizativa, empleados estratégicos, políticas y procesos de una organización objetivo. Esta información es útil para los atacantes, ya que les permite comprender mejor el entorno empresarial y las dinámicas internas, lo que puede ser utilizado para adaptar y refinar sus ataques de manera más efectiva. Para llevar a cabo esta técnica, los atacantes utilizan diversos métodos y herramientas, como investigar el sitio web de la empresa objetivo y analizar sus comunicaciones públicas obuscar noticias y publicaciones en redes sociales para identificar empleados clave, roles y estructuras organizativas. También, pueden realizar búsquedas de información sobre la organización en bases de datos y registros públicos, como datos de registro de empresas y patentes.

Además, los atacantes pueden emplear métodos que incluyen la monitorización de las redes sociales y foros en línea para identificar discusiones y comentarios relacionados con la empresa objetivo, sus empleados y sus productos. Esto puede proporcionar información

[3] https://obfuscator.io/

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

útil sobre la cultura organizativa, las preocupaciones de seguridad y las áreas donde la empresa puede ser vulnerable.

Una variante más agresiva y que no se analiza en detalle por su alto nivel de intrusividad sería la realización de entrevistas ficticias a empleados actuales o antiguos. Con esto, se puede obtener información sobre la organización objetivo, como detalles sobre el entorno laboral, estructura interna, proyectos en desarrollo y posibles áreas de interés.

5.5.1. **Subtécnicas**

La recopilación de información sobre la organización objetivo se lleva a cabo a través de varias subtécnicas. Juntas proporcionan una visión completa y detallada de su estructura.

Subtécnica	Detalle	Herramientas
Búsqueda de ubicaciones físicas	Geolocalización de direcciones IP del objetivo para identificar ubicaciones de servidores, oficinas y otras instalaciones relacionadas con la organización. Esto puede ayudar a revelar la infraestructura de red y posibles vulnerabilidades.	whois.domaintools, Robtex, Who.is, Viewdns, Shodan
Recopilación de información sobre compañías relacionadas	Búsqueda de información sobre el objetivo y posibles compañías relacionadas para identificar asociaciones, subsidiarias y otros vínculos comerciales que puedan ser relevantes en la investigación.	Crunchbase
Búsqueda en boletines oficiales	Revisión de boletines oficiales para obtener información legal y regulatoria sobre la organización, como registros de licencias, sanciones, multas y otros datos relevantes que puedan afectar a la empresa o revelar áreas de interés.	De forma manual en sitios web de boletines oficiales, diarios oficiales o registros públicos
Registro de propietarios	Investigación de la titularidad y propiedad de la organización objetivo para identificar a los propietarios, directivos y otras personas clave en la empresa. Esto puede ayudar a entender la estructura y control de la organización.	De forma manual en registros públicos, registros mercantiles, bases de datos gubernamentales
Balances de cuentas	Obtención de información financiera, incluidos balances y estados de cuenta de la organización objetivo, para evaluar la salud financiera, detectar posibles problemas o áreas de interés, y comprender las prioridades y objetivos de la empresa.	De forma manual en sitios web de organismos reguladores, registros financieros públicos, informes anuales
Información de políticas de la organización	Recopilación de información sobre políticas internas, códigos de conducta y otros documentos relacionados para comprender las normas y prácticas de la organización. Esto puede ayudar a identificar posibles vulnerabilidades y áreas de interés.	De forma manual en el sitio web de la organización objetivo, motores de búsqueda

Información de patentes y propiedad intelectual	Obtención de información sobre patentes y propiedad intelectual asociadas con la organización objetivo para identificar áreas de investigación y desarrollo, tecnologías clave y posibles ventajas competitivas.	De forma manual en bases de datos de patentes, registros públicos, sitios web de oficinas de patentes y marcas registradas
Recopilación de información de la organización a través de otras fuentes abiertas	Obtención de información de la organización, y de empleados/roles que manejen información clave, a través de redes sociales y fuentes abiertas para identificar posibles objetivos y áreas de interés. También, puede ayudar a revelar la estructura organizativa y las relaciones entre empleados, horario de apertura y cierre de negocios, etc.	RocketReach, Lusha, búsquedas en LinkedIn, motores de búsqueda

5.5.2. **Medidas de mitigación**

Es imposible eliminar todo el rastro de información de una organización, máxime cuando en muchos casos lo que se quiere es justamente que sea pública y que se difunda ampliamente. Para mitigar los riesgos asociados a la recopilación de información sobre la organización, lo importante es tomar medidas de control de la información, como limitar los detalles disponibles al público en sitios web y en registros públicos. Además, es esencial llevar a cabo formación de concienciación sobre seguridad para los empleados, para que entiendan los riesgos asociados a la hora de compartir información de la empresa en las redes sociales. También, se debe realizar una auditoría de seguridad regular para detectar y abordar posibles sobreexposiciones, incluyendo la revisión de las políticas internas y la gestión de la propiedad intelectual.

5.6. T1598 Suplantación para obtener información

La suplantación es un ataque de tipo ingeniería social en el que el atacante busca obtener información confidencial, mediante el engaño, que puede ser utilizada posteriormente para llevar a cabo nuevos ataques haciéndose pasar por otra persona. Este tipo de ataque puede ser dirigido a individuos, empresas o industrias en particular.

El *phishing* también puede utilizar técnicas evasivas, como la eliminación o manipulación de correos electrónicos, metadatos o cabeceras.

El *phishing* es una técnica cada vez más utilizada por los ciberdelincuentes debido a su alta tasa de éxito y bajo nivel de sofisticación requerido para su ejecución. Pese a ser catalogada dentro de las técnicas de reconocimiento, la suplantación es una de las técnicas activas más intrusivas, ya que deja rastro y evidencias que podrían exponer al atacante, revelando su presencia e intenciones.

5.6.1. **Subtécnicas**

La suplantación de información puede implementarse a través de diferentes variantes, permitiendo a los atacantes adoptar diversas estrategias para obtener la información deseada.

Subtécnica	Detalle
Suplantación de correo electrónico	Se utiliza para enviar correos electrónicos que parecen provenir de una fuente legítima con el fin de engañar al destinatario para que revele información confidencial o realice una acción dañina. Los enlaces a sitios externos fraudulentos y los ficheros adjuntos con algún tipo de *payload* (o carga) maliciosa suelen ser habituales.
Suplantación de mensaje de texto o mensajería instantánea	Se refiere al uso de mensajes de texto (SMS) o *smishing* para engañar a las víctimas para que proporcionen información personal o financiera. Los mensajes pueden incluir enlaces maliciosos que llevan a sitios web falsos que parecen ser legítimos, o pueden pedir a la víctima que responda con información confidencial. Los ejemplos más sofisticados pueden hacer suplantación del número telefónico de compañías o personas.
Suplantación de llamada de voz	La suplantación de identidad a través de una llamada telefónica de voz (*vishing*) es un método de ingeniería social que utiliza la manipulación psicológica (como la urgencia, la amenaza o la simpatía) para obtener información confidencial de la víctima.

5.6.2. Medidas de mitigación

Para mitigar la suplantación de información, es esencial implementar la autenticación de múltiple factor y políticas de seguridad. En el caso particular del correo electrónico, esto implica habilitar la autenticación del remitente (SPF, DKIM, DMARC), filtros de *spam*, bloqueo de correos sospechosos o cifrado de mensajes. La formación continua de empleados en el reconocimiento de tácticas de *phishing* es también muy importante. En el caso de la suplantación de llamadas de voz, es crucial proporcionar formación a los empleados para que sepan cómo actuar ante llamadas sospechosas.

5.7. T1597 Búsqueda de fuentes cerradas

Se refiere a la recopilación de información de recursos y plataformas que no están disponibles públicamente o que requieren cierto nivel de acceso y autorización para ser consultadas. Estas fuentes pueden incluir bases de datos privadas, foros cerrados, redes y grupos privados, archivos y documentos internos de la organización, entre otros.

A diferencia de las fuentes abiertas (OSINT), las fuentes cerradas pueden contener información más sensible y específica, ya que no están destinadas a ser compartidas o accesibles por el público en general. La información recopilada de fuentes cerradas puede ser valiosa para obtener una visión más detallada de la organización objetivo y descubrir vulnerabilidades o áreas de interés que no están disponibles en fuentes abiertas.

El acceso a fuentes cerradas puede ser difícil y, en algunos casos, requerir técnicas de ingeniería social, como la suplantación de identidad o el establecimiento de relaciones de confianza con empleados o miembros de la organización objetivo. También, puede requerir

el uso de credenciales de acceso, invitaciones a grupos privados o la explotación de vulnerabilidades de seguridad para acceder a la información.

Existe la posibilidad de realizar búsquedas en fuentes de inteligencia y en amenazas, como las siguientes, donde podemos obtener información sobre el objetivo, información referentea los empleados o información de sistemas.

5.7.1. Subtécnicas

Bajo esta categoría se pueden encontrar diversas subtécnicas en función del tipo de información requerida y el nivel de acceso permitido.

Subtécnica	Detalle	Herramientas
Búsqueda en motores especializados en fugas de datos	Emplea herramientas de inteligencia especializadas de fuga de datos, a partir de parámetros de entrada como correo electrónico, dominio, IP, CIDR y dirección de Bitcoin. En todo tipo de fuentes, incluyendo red Tor.	Intelligence X, Spiderfoot
Grupos de mensajería privada	Participación en grupos de mensajería privada, como aquellos en aplicaciones de mensajería cifrada, donde se comparte y se discute información relacionada con vulnerabilidades, violaciones de datos y otros temas de seguridad.	Software de mensajería (Telegram, Signal, WhatsApp, etc.)
Redes y comunidades de la *Deep Web* o *Dark Web*	Exploración de redes y comunidades en la Deep Web o Dark Web, donde se pueden encontrar fuentes cerradas de información, datos robados y otras actividades ilícitas relacionadas con la ciberseguridad.	Navegadores específicos como Tor, foros y mercados en la Dark Web (requiere conocimientos técnicos y precaución al navegar)

5.7.2. Medidas de mitigación

Las medidas de mitigación incluyen nuevamente el control de la información expuesta y la monitorización de fugas de datos

5.8. T1596 Buscar en bases de datos técnicas de libre acceso

Esta técnica se enfoca en la recopilación de información técnica y específica de una organización objetivo a través de bases de datos y recursos que son de acceso libre en Internet. Estas bases de datos pueden incluir registros de patentes, documentos técnicos, normas y regulaciones, especificaciones de productos, entre otros. La información obtenida a través de esta técnica puede proporcionar una visión más profunda de los productos, tecnologías y procesos utilizados por la organización objetivo, así como de sus colaboraciones y alianzas con otras organizaciones. La información recopilada a través de bases de datos puede incluir detalles técnicos sobre los productos y servicios ofrecidos por la organización, las tecnologías y procesos utilizados para fabricar o desarrollar los

productos, las patentes registradas, las normas y regulaciones aplicables, entre otros aspectos relevantes.

5.8.1. **Subtécnicas**

Cada subtécnica permite a los atacantes obtener un entendimiento más detallado de las tecnologías, productos y procesos implementados por la organización objetivo.

Subtécnica	Detalle	Herramientas
Búsqueda en bases de datos de patentes	Consulta de información detallada sobre patentes registradas, incluyendo descripciones de tecnologías, inventores y titulares de patentes.	USPTO, EPO, WIPO
Repositorios de documentos técnicos	Acceso a documentos técnicos, presentaciones de proyectos o productos, informes y publicaciones relacionadas con diversas áreas de conocimiento y tecnologías de la organización.	arXiv, IEEE Xplore, Google Scholar, ResearchGate, Scribd
Sitios web de organismos reguladores y de normalización	Obtención de información sobre normas, regulaciones y especificaciones técnicas aplicables a productos y tecnologías de la organización.	Estándares ISO, IEC, FCC
Acceso a bases de datos de vulnerabilidades y *exploits*	Acceso a bases de datos que contienen información sobre vulnerabilidades y *exploits* conocidos, incluyendo detalles técnicos y ejemplos de código, sobre tecnologías utilizadas, o desarrolladas por la organización.	National Vulnerability Database (NVD), Exploit Database (EDB), Common Vulnerabilities and Exposures (CVE)

5.8.2. **Medidas de mitigación**

Las estrategias de mitigación se centran en limitar la exposición pública de información detallada y mantener actualizado y seguro el entorno tecnológico de la organización. Se deben revisar los repositorios de documentos para evitar la publicación de detalles innecesarios que puedan ser aprovechados por los atacantes. La organización también debe monitorear activamente las bases de datos de vulnerabilidades y *exploits*, y aplicar parches o actualizaciones de seguridad a medida que se dispongan para mantener la infraestructura de TI segura y resistente.

5.9. T1593 Buscar dominios/sitios web abiertos

Esta técnica se refiere a la búsqueda y recopilación de información sobre dominios y sitios web públicos relacionados con una organización objetivo. Su objetivo es obtener información sobre la presencia en línea de la organización, incluyendo detalles sobre los productos, servicios y tecnologías utilizados por la organización, así como información de contacto y del personal.

Una vez que se han identificado los sitios web y dominios relacionados con la organización, los atacantes pueden utilizar herramientas de exploración de aplicaciones web para buscar vulnerabilidades y debilidades que puedan ser explotadas en fases posteriores de un ataque.

5.9.1. Subtécnicas

Podemos encontrar varias subtécnicas que proporcionan una visión más detallada de la presencia digital de la organización, revelando potenciales vulnerabilidades y áreas de interés que podrían ser explotadas en futuros ataques.

Subtécnica	Detalle	Herramientas
Búsqueda de dominios y subdominios	Búsqueda de subdominios asociados con el dominio principal de la organización.	Sublist3r, Recon-ng, Amass, Spiderfoot, motores de búsqueda.
Búsqueda de certificados SSL	Identificación de certificados SSL asociados con la organización.	SSLShopper, Censys, CRT.
Búsqueda de información DNS	Acceso a registros DNS asociados con la organización, incluyendo registros de correo electrónico y servidores de correo.	Nslookup, Dig, Whois.
Búsqueda de archivos públicos	Búsqueda de archivos públicos alojados en el servidor web de la organización, como archivos de copias de seguridad, archivos de configuración y documentos internos.	Motores de búsqueda, Dirb, Spiderfoot, Wfuzz

5.9.2. Medidas de mitigación

Para minimizar el riesgo asociado, las organizaciones pueden implementar una serie de medidas. Estas incluyen la monitorización regular de dominios y subdominios para detectar cualquier cambio sospechoso, la administración adecuada de los certificados SSL para asegurar la comunicación y la privacidad del usuario, el control estricto de los registros DNS para prevenir la exposición de información sensible y la gestión segura de los archivos públicos para evitar la fuga de datos. Las políticas de seguridad y privacidad de la organización deben ser revisadas y actualizadas regularmente para reflejar los cambios en la infraestructura y las amenazas emergentes

5.10. T1594 Búsqueda de sitios web propiedad de las victimas

Esta técnica consiste en la búsqueda y recopilación de información sobre sitios web o perfiles sociales propiedad de la organización objetivo que están disponibles públicamente en Internet, con el objetivo de obtener información técnica, organizativa y social dentro de los sitios digitales de la organización.

Estos sitios también pueden tener detalles que resaltan las operaciones y relaciones comerciales la infraestructura y los sistemas de la organización, incluyendo detalles sobre las aplicaciones web, los servidores web y la arquitectura de la red.

Una vez que se han identificado los sitios web de la organización, los atacantes pueden utilizar herramientas de exploración de aplicaciones web para buscar vulnerabilidades y debilidades que puedan ser explotadas. También, se puede utilizar esta técnica para identificar falta de parches y actualizaciones de seguridad.

5.10.1. **Subtécnicas**

Podemos desglosar esta técnica en subtécnicas, cada una dirigida a recopilar información específica de los activos digitales de la organización objetivo.

Subtécnica	Detalle	Herramientas
Identificación de subdominios	Identificación de subdominios asociados con el dominio principal de la organización.	Sublist3r, Recon-ng, Amass, motores de búsqueda.
Escaneo de vulnerabilidades	Identificación de vulnerabilidades en los sitios web propiedad de la organización objetivo.	Nikto, Burp Suite Scanner, OWASP ZAP, Acunetix, Nessus, Qualys, OpenVAS, Nmap, OpenSCAP.
Búsqueda de archivos públicos	Identificación de archivos públicos alojados en el servidor web de la organización, como archivos de copias de seguridad, archivos de configuración y documentos internos.	Motores de búsqueda, Dirb, Wfuzz, HTTrack, Gobuster Fuzz, Spiderfoot, Intelligence X.
Extracción de metadatos	Extracción de metadatos de archivos y documentos alojados en el servidor web de la organización objetivo.	ExifTool, Metagoofil, FOCA.
Búsqueda de información DNS	Identificación de registros DNS asociados con la organización, incluyendo registros de correo electrónico y servidores de correo.	Nslookup, Dig, Whois.
Identificación de tecnologías utilizadas	Se enfoca en identificar las tecnologías utilizadas en los sitios web de la organización objetivo. Estas tecnologías pueden incluir el sistema operativo del servidor web, el servidor web utilizado, el CMS (sistema de gestión de contenidos), lenguaje de programación, *plugins*, *frameworks*, y otras herramientas y *software*.	Wappalyzer, BuiltWith, WhatWeb, Nmap, Publicwww, Spyonweb, Whatweb

Exploración del sitio web	La exploración del sitio para reconstruir el mapa de su web permite: identificación de páginas y secciones del sitio web objetivo, análisis de la estructura del sitio web y su arquitectura, identificación de enlaces y recursos relacionados con el sitio web, identificación de contenido multimedia y otros archivos alojados en el sitio web, identificación de formularios y aplicaciones web, e identificación de áreas de autenticación y acceso restringido.	Wfuzz, Burp Suite Spider, HTTrack, Gobuster, Builtwith.
Búsqueda de información a partir de código fuente del sitio web	Analizar el código fuente (HTML, CSS, JavaScript, etc.), permite identificar *frameworks*, librerías, lenguajes de programación y posibles vulnerabilidades. Además, se pueden encontrar comentarios y metadatos con información sensible, configuraciones y parámetros específicos que podrían ser explotados, así como la estructura del sitio y enlaces internos que revelen áreas ocultas con información valiosa.	Caché de motores de búsqueda, Wayback Machine
Búsqueda en redes sociales	El análisis de perfiles de la organización objetivo en redes sociales puede ser utilizado para recopilar información sobre su actividad, *partners* o tecnologías. Suele ser un sitio donde las organizaciones comparten sus actualidades. También, puede ser utilizado para recopilar información sobre empleados, lo que puede ayudar a los atacantes a crear ataques de *spear-phishing* (ataques de *phishing* personalizados) más efectivos.	Las propias redes sociales
Repositorios de código abierto	Exploración de proyectos de código abierto y colaborativo en los que las organizaciones y sus empleados pueden participar.	GitHub, GitLab, SourceForge

5.10.2. **Medidas de mitigación**

Las organizaciones pueden implementar la monitorización regular de los subdominios para detectar cualquier actividad sospechosa, la realización de escaneos periódicos de vulnerabilidades (y su remediación), y la gestión segura de los archivos públicos para evitar la exposición de información sensible. Además, pueden implementar controles adecuados

para proteger la información del DNS y practicar la limpieza de metadatos antes de publicar documentos o archivos en línea. Finalmente, las organizaciones deben ser conscientes de la información que comparten en las redes sociales y en los repositorios de código abierto, y deben implementar políticas adecuadas para controlar esta divulgación.

6. Conclusión

El reconocimiento es una táctica que se utiliza para obtener una comprensión profunda de las posibles brechas o debilidades en los sistemas de una organización. Es un paso fundamental y crítico en cualquier ciberataque o auditoría, ya que proporciona al adversario una visión clara de la organización objetivo, su infraestructura, y su personal.

Esta información detallada, que abarca desde la arquitectura del sistema hasta la cultura de seguridad de la organización, puede ser utilizada por el adversario para apoyar y dirigir sus esfuerzos en otras fases de su ciclo de vida. Por ejemplo, con los datos recopilados durante el reconocimiento, el actor puede planificar y ejecutar un acceso inicial a los sistemas de la organización, utilizando las debilidades identificadas para obtener un punto de apoyo. Además, después de lograr un compromiso, puede utilizar la información recolectada para definir y priorizar sus objetivos, concentrándose en las áreas que presentan la mayor oportunidad para lograr sus fines, ya sean financieros, de espionaje, de interrupción del servicio, entre otros. **El reconocimiento también puede ser un proceso iterativo** para ajustar y mejorar la estrategia en función de la información que van obteniendo. Para el actor, esto puede incluir la identificación de nuevas vulnerabilidades a medida que la organización cambia y evoluciona, la búsqueda de información adicional puede apoyar ataques más sofisticados o mejorar las medidas defensivas.

La referencia a **la matriz *Enterprise* de MITRE ATT&CK, en el contexto de las técnicas de reconocimiento, sugiere un enfoque estructurado para entender y mitigar las ciberamenazas**. Este marco proporciona un catálogo de tácticas, técnicas y procedimientos (TTP) utilizados para obtener la máxima información de un objetivo. En el punto 5 de este estudio se han detallado las técnicas y subtécnicas de reconocimiento de MITRE ATT&CK, proporcionando una visión clara de cómo se puede llevar a cabo el reconocimiento, y qué herramientas pueden emplear. Para cada técnica se han propuesto medidas de mitigación para reducir su riesgo.

Las técnicas de reconocimiento pueden ser especialmente difíciles de anular o contrarrestar con controles preventivos, ya que se basan en comportamientos realizados fuera del alcance de las defensas y controles empresariales. Sin embargo, **pueden proponerse acciones de mitigación centradas en minimizar la cantidad y la sensibilidad de los datos disponibles para las partes externas**. Al hacerlo, se puede limitar la cantidad de información que los atacantes pueden recopilar, lo que reduce el riesgo de que se utilice en futuros ataques. Estas medidas incluyen una variedad de enfoques, desde la implementación de controles de seguridad más estrictos, o la capacitación del personal para mejorar la conciencia de seguridad, hasta la utilización de herramientas de detección y respuesta avanzadas.

No hay una estrategia completamente efectiva para mitigar los riesgos asociados a esta táctica, por lo que lo más apropiado es controlar la información expuesta asegurando que la información que pueden obtener los ciberdelincuentes no pueda ser utilizada en nuestra contra, Además, es importante adoptar un enfoque de defensa en profundidad que partiendo de acciones **formativas** y de **concienciación**, implique múltiples capas de seguridad, considerando la seguridad como un esfuerzo de todos los miembros de la organización.

7. Acrónimos

- **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 (un bit del encabezado TCP usado para terminar la sesión)
- **HTTP**: Hypertext Transfer Protocol
- **IEC**: International Electrotechnical Commission
- **ICMP**: Internet Control Message Protocol
- **IP**: Internet Protocol
- **ISO**: International Organization for Standardization
- **MX**: Mail eXchange record (un tipo de registro DNS)
- **NVD:** National Vulnerability Database
- **OSINT**: Open Source INTelligence
- **SPF**: Sender Policy Framework
- **SSL**: Secure Sockets Layer
- **SYN**: Synchronize (un bit del encabezado TCP usado para iniciar la sesión)
- **SMS**: Short Message Service
- **TCP**: Transmission Control Protocol
- **TI**: Tecnologías de la Información
- **TTP**: Tactics, Techniques, and Procedures
- **TXT**: Text record (un tipo de registro DNS)
- **UDP**: User Datagram Protocol

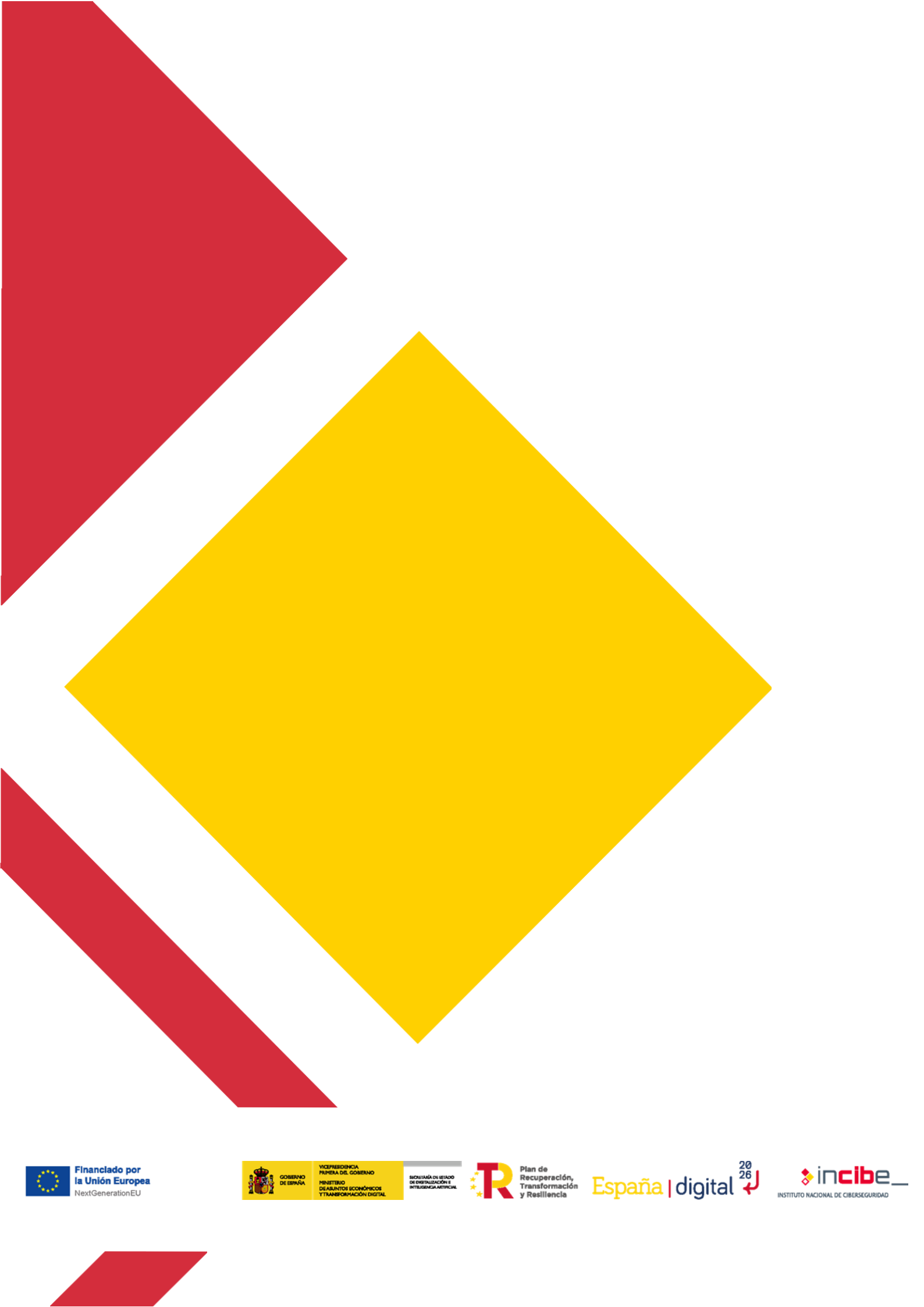
8. Bibliografía

Referencia	Título, autor, fecha y enlace web
[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

ANEXO 1: Herramientas

Herramienta	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
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD