## Documento de Consultas y Herramientas para Pentesting, OSINT y Hacking

## Fases del Pentesting

El proceso de pentesting consta de las siguientes fases:

### 1. Reconocimiento

El objetivo de esta fase es obtener información sobre el objetivo del pentesting. Se recopilan datos para comprender mejor el objetivo y se utilizan para identificar vulnerabilidades potenciales. El reconocimiento incluye técnicas como la búsqueda de información en internet, el escaneo de puertos y la enumeración de servicios.

#### Herramientas populares:

* Nmap: Escáner de puertos de red. (<https://nmap.org/>)
* Smap: un reemplazo directo para Nmap impulsado por shodan.io <https://github.com/s0md3v/Smap>
* Recon-ng: Framework de recolección de información. (<https://github.com/lanmaster53/recon-ng>)
* Shodan: Motor de búsqueda de dispositivos conectados a internet. (<https://www.shodan.io/>)
* theHarvester: Herramienta de recolección de información de correo electrónico, subdominios y direcciones IP. (<https://github.com/laramies/theHarvester>)
* Maltego: Plataforma de inteligencia de código abierto para la recopilación y el análisis de información. (<https://www.maltego.com/>)
* SpiderFoot: Herramienta de inteligencia de código abierto para la recopilación y el análisis de información. (<https://www.spiderfoot.net/>)
* Shodan: Motor de búsqueda de dispositivos conectados a Internet, incluidos servidores, routers, cámaras y otros dispositivos IoT. (<https://www.shodan.io/>)
* Censys: Motor de búsqueda de seguridad que permite buscar información de dispositivos conectados a Internet, como servidores web, dispositivos IoT, etc. (<https://censys.io/>)
* EyeWitness: Herramienta de código abierto que captura capturas de pantalla de sitios web y las almacena en un archivo para su posterior análisis. (<https://github.com/FortyNorthSecurity/EyeWitness>)
* EasyG: Script que utilizo para automatizar algunas tareas de recopilación de información para mi proceso de piratería [easyg/easyg.rb at main · seeu-inspace/easyg (github.com)](https://github.com/seeu-inspace/easyg/blob/main/easyg.rb).
* Gh0st: Herramienta de reconocimiento automático [Gh0st3xp101t/Gh0st (github.com)](https://github.com/Gh0st3xp101t/Gh0st).
* Osmedeus: Framework para reconocimiento automático [j3ssie/osmedeus: A Workflow Engine for Offensive Security (github.com)](https://github.com/j3ssie/osmedeus).
* Censys: <https://github.com/censys/censys-python>
* Awesome OSINT: A curated list of amazingly awesome open source intelligence tools and resources [jivoi/awesome-osint: A curated list of amazingly awesome OSINT (github.com)](https://github.com/jivoi/awesome-osint).
* Flashlight: Automated Information Gathering Tool for Penetration Testers <https://github.com/galkan/flashlight>
* Framework de OSINT: [OSINT-US - start.me](https://start.me/p/GEQXv7/osint-us)
* **SubDomainizer**: una herramienta de enumeración de subdominios escrita en Python que utiliza diversas fuentes para encontrar subdominios asociados con un dominio específico.
* Repositorio: <https://github.com/nsonaniya2010/SubDomainizer>
* **NmapAutomator**: un script de automatización de escaneo de puertos escrito en Bash que utiliza Nmap para realizar escaneos de puertos y generar informes.
* Repositorio: <https://github.com/21y4d/nmapAutomator>
* **DNSRecon**: una herramienta de enumeración de DNS escrita en Python que utiliza diferentes técnicas para encontrar registros DNS y subdominios asociados.
* Repositorio: <https://github.com/darkoperator/dnsrecon>
* **Photon**: una herramienta de extracción de información de sitios web escrita en Python que busca información sensible como correos electrónicos, nombres de usuarios, archivos y subdominios.
* Repositorio: <https://github.com/s0md3v/Photon>
* **Sn1per**: una herramienta de inteligencia de amenazas y reconocimiento de red escrita en Bash que utiliza diversas técnicas para recopilar información sobre objetivos específicos.
* Repositorio: <https://github.com/1N3/Sn1per>
* **Sherlock**: una herramienta de búsqueda de perfiles de redes sociales escrita en Python que utiliza nombres de usuario para buscar perfiles de redes sociales.
* Repositorio: <https://github.com/sherlock-project/sherlock>
* **Fierce**: una herramienta de enumeración de DNS escrita en Perl que utiliza diferentes técnicas para encontrar registros DNS y subdominios asociados.
* Repositorio: <https://github.com/mschwager/fierce>
* **Jigsaw**: una herramienta de recopilación de información de la organización escrita en Python que utiliza diferentes fuentes para encontrar información sobre la organización, como direcciones de correo electrónico y nombres de dominio.
* Repositorio: <https://github.com/yassineaboukir/jigsaw>
* **Sublist3r**: una herramienta de enumeración de subdominios escrita en Python que utiliza diferentes fuentes para encontrar subdominios asociados con un dominio específico.
* Repositorio: <https://github.com/aboul3la/Sublist3r>
* Katana: Google Dorks Hacking <https://github.com/projectdiscovery/katana>

### 2. Análisis de vulnerabilidades

En esta fase se analizan las vulnerabilidades encontradas durante la fase de reconocimiento. Los resultados del análisis de vulnerabilidades se utilizan para planificar y ejecutar los ataques.

#### Herramientas populares:

* Nessus: Herramienta de escaneo de vulnerabilidades. (<https://www.tenable.com/products/nessus>)
* OpenVAS: Sistema de gestión de vulnerabilidades. (<https://www.openvas.org/>)
* Nikto: Escáner de vulnerabilidades web. (<https://cirt.net/Nikto2>)
* Lynis: Herramienta de auditoría de seguridad de sistemas Linux. (<https://cisofy.com/lynis/>)
* OWASP ZAP: Herramienta de análisis de seguridad de aplicaciones web. (<https://www.zaproxy.org/>
* Metasploit Framework: Marco de explotación que también incluye una base de datos de vulnerabilidades. (<https://www.metasploit.com/>)
* Vega: Escáner de vulnerabilidades de código abierto que se enfoca en la seguridad de aplicaciones web y la detección de vulnerabilidades comunes. (<https://subgraph.com/vega/>)
* OpenSCAP: Conjunto de herramientas de código abierto que proporciona una plataforma para la implementación de políticas de seguridad y la evaluación de la seguridad de sistemas. (<https://www.open-scap.org/>)
* Nuclei: Automate Network Vulnerability Scans [Index - Nuclei - Community Powered Vulnerability Scanner (projectdiscovery.io)](https://nuclei.projectdiscovery.io/nuclei/get-started/) / [xm1k3/cent: Community edition nuclei templates, a simple tool that allows you to organize all the Nuclei templates offered by the community in one place (github.com)](https://github.com/xm1k3/cent)
* Masscan: una herramienta de escaneo de puertos de alta velocidad escrita en C que utiliza múltiples subprocesos para realizar escaneos de puertos en segundos. Repositorio: <https://github.com/robertdavidgraham/masscan>

### 3. Explotación

En esta fase se intenta explotar las vulnerabilidades encontradas en la fase anterior. El objetivo es obtener acceso al sistema o aplicación.

#### Herramientas populares:

* Metasploit: Framework de explotación. (<https://www.metasploit.com/>)
* Burp Suite: Herramienta de pruebas de penetración para aplicaciones web. (<https://portswigger.net/burp>)
* SQLMap: Herramienta de inyección SQL automatizada. (<http://sqlmap.org/>)
* BeEF: Marco de explotación basado en el navegador para ataques a aplicaciones web. (<https://beefproject.com/>)
* SQLMate: Herramienta de inyección SQL automatizada y enumeración de bases de datos. (<https://github.com/UltimateHackers/sqlmate>)
* Exploit Database: Recopilación de exploits públicos de código abierto para una amplia variedad de software y sistemas. (<https://www.exploit-db.com/>)
* Mangle: Es una herramienta que manipula aspectos de ejecutables compilados (.exe o DLL) para evitar la detección de EDRs <https://github.com/optiv/Mangle>
* SET (Social-Engineer Toolkit): Marco de ingeniería social que incluye módulos de phishing, ingeniería inversa y explotación de vulnerabilidades. (<https://github.com/trustedsec/social-engineer-toolkit>)
* Getsploit: Herramienta de descarga de exploits [vulnersCom/getsploit: Command line utility for searching and downloading exploits (github.com)](https://github.com/vulnersCom/getsploit)
* WinRM: The ultimate WinRM shell for hacking/pentesting [Hackplayers/evil-winrm: The ultimate WinRM shell for hacking/pentesting (github.com)](https://github.com/Hackplayers/evil-winrm)
* Sn1per: Pentesting toolkit [1N3/Sn1per: Attack Surface Management Platform | Sn1perSecurity LLC (github.com)](https://github.com/1N3/Sn1per)
* EvilGrade - <https://github.com/infobyte/evilgrade>: Una herramienta que permite la inyección de actualizaciones maliciosas en aplicaciones vulnerables, con el fin de comprometer el sistema del usuario.
* Pycrypter: Python Based Crypter That Can Bypass Any Kinds Of Antivirus Products <https://github.com/machine1337/pycrypt>
* BloodHound: una herramienta de análisis y visualización de redes en sistemas Windows escrita en JavaScript y Python que permite visualizar y analizar la estructura de una red, así como las relaciones entre los diferentes nodos. Repositorio: <https://github.com/BloodHoundAD/BloodHound>
* Armitage: es una herramienta de interfaz gráfica de usuario para Metasploit Framework, que permite visualizar y explorar los objetivos de la red y lanzar ataques contra ellos. Repositorio: <https://github.com/rsmudge/armitage>
* linWinPwn: Es un script bash que automatiza una serie de comprobaciones de enumeración y vulnerabilidad de Active Directory <https://github.com/lefayjey/linWinPwn>
* Bettercap: Es una herramienta de secuestro de red que permite interceptar el tráfico de red, realizar ataques MITM (man-in-the-middle) y analizar el tráfico de red. Repositorio: <https://github.com/bettercap/bettercap>
* Freeze: Es un kit de herramientas de carga útil para evitar EDR utilizando procesos suspendidos, syscalls directos y métodos de ejecución alternativos <https://github.com/optiv/Freeze>
* PseudoHash: Generador de listas de contraseñas que se centra en palabras clave mutadas por patrones de creación de contraseñas de uso común [https://github.com/t3l3machus/psudohash](https://github.com/t3l3machus/psudohash%20)
* Buscador de Exploits: <https://sploitus.com/>

### 4. Post-Explotación

#### Escalada de privilegios

Una vez que se ha obtenido acceso, se busca una manera de aumentar los privilegios en el sistema o aplicación. El objetivo es obtener acceso a información crítica o funcionalidad adicional.

##### Herramientas populares:

* PowerUp: Módulo de PowerShell para la enumeración y la escalada de privilegios. (<https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc>)
* WinPwnage: Métodos de omisión de UAC, elevación y persistencia <https://github.com/rootm0s/WinPwnage>
* JAWS: Herramienta de escalada de privilegios para sistemas Windows. (<https://github.com/411Hall/JAWS>)
* Mimikatz: Herramienta de extracción de credenciales de Windows y escalada de privilegios. (<https://github.com/gentilkiwi/mimikatz>)
* Privilege Escalation Awesome Scripts SUITE (PEASS): Conjunto de scripts y herramientas para la escalada de privilegios en sistemas Windows y Linux. (<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite>)
* LinEnum: Herramienta de código abierto que automatiza la enumeración de información y la detección de vulnerabilidades en sistemas Linux. (<https://github.com/rebootuser/LinEnum>)
* Windows-Exploit-Suggester: Herramienta de código abierto que ayuda en la identificación de posibles vulnerabilidades de Windows mediante la comparación de la versión de Windows con una base de datos de vulnerabilidades conocidas. (<https://github.com/GDSSecurity/Windows-Exploit-Suggester>)
* Pupy: Herramienta de código abierto que permite la escalada de privilegios y la toma de control remoto de sistemas Windows, Linux y OS X. (<https://github.com/n1nj4sec/pupy>)
* SudoKiller: Herramienta de código abierto que busca vulnerabilidades de escalada de privilegios en sistemas Linux que utilizan sudo. (<https://github.com/TH3xACE/SudoKiller>)
* [swisskyrepo](https://github.com/swisskyrepo)/**[PayloadsAllTheThings](https://github.com/swisskyrepo/PayloadsAllTheThings)**: Repositorio de Github con Pentest tips en los que se encuentran numerosos métodos de escalada de privilegios en Linux y Windows.
* [Privilege Escalation - CSbyGB - Pentips (gitbook.io)](https://csbygb.gitbook.io/pentips/windows/privesc): Notas de Pentesting, en las que además de escaladas de privilegios hay notas y tips para todas las fases de un Pentesting.
* ExploitLeakedHandle: Es una utilidad que identifica identificadores en procesos sin privilegios que pueden haberse heredado de un proceso padre con privilegios e intenta aprovecharlos para la escalada de privilegios locales. <https://github.com/0x00Check/ExploitLeakedHandle>
* CrackMapExec: una herramienta de post-explotación en sistemas Windows y Linux escrita en Python que permite ejecutar comandos remotos, escalar privilegios y obtener acceso persistente en sistemas comprometidos. Repositorio: <https://github.com/byt3bl33d3r/CrackMapExec>

#### Movimiento lateral

La fase de movimiento lateral se centra en la propagación del acceso a otros sistemas dentro de la red comprometida.

* BloodHound: Herramienta de análisis de relaciones y descubrimiento de rutas de acceso en Active Directory. (<https://github.com/BloodHoundAD/BloodHound>)
* CrackMapExec: Herramienta de pentesting que automatiza la propagación lateral de exploits en redes Windows y la búsqueda de vulnerabilidades. (<https://github.com/byt3bl33d3r/CrackMapExec>)
* Metasploit Framework: Metasploit permite la propagación lateral utilizando los sistemas comprometidos como pivot. (<https://github.com/rapid7/metasploit-framework>)

#### Exfiltración de datos

La fase de exfiltración de datos implica la extracción de información de los sistemas comprometidos y su transferencia fuera de la red comprometida.

* FTP: Protocolo de transferencia de archivos que permite a los usuarios transferir archivos entre sistemas. Repositorio: <https://github.com/madler/ftp>
* HTTPS: Protocolo de transferencia de hipertexto seguro que permite a los usuarios transferir información de forma segura a través de Internet. Repositorio: <https://github.com/curl/curl>
* SCP: Protocolo de copia segura que se utiliza para transferir archivos entre sistemas de forma segura. Repositorio: <https://github.com/openssh/openssh-portable>
* SFTP: Protocolo de transferencia de archivos seguros que se utiliza para transferir archivos de forma segura entre sistemas. Repositorio: <https://github.com/libssh2/libssh2>
* Netcat: Utilidad de red que permite a los usuarios leer y escribir datos en conexiones de red utilizando TCP o UDP. Es una herramienta muy versátil que se puede utilizar para la transferencia de archivos y datos de forma encubierta. El repositorio de Netcat se encuentra en <https://github.com/diegocr/netcat>.
* Steghide: Herramienta de esteganografía que permite ocultar archivos en imágenes y otros archivos de audio y video. Es una herramienta muy útil para la exfiltración de datos de forma encubierta y puede ser utilizada tanto en sistemas Linux como en Windows. El repositorio de Steghide se encuentra en <https://github.com/StefanoDeVuono/steghide>.
* Hping: Herramienta de red que permite la creación de paquetes de red personalizados y el envío de tráfico de red falso. Es una herramienta muy útil para la exfiltración de datos a través de canales encubiertos y puede ser utilizada para evadir la detección de sistemas de seguridad. El repositorio de Hping se encuentra en <https://github.com/antirez/hping>.
* Powershell Empire: Framework de post-explotación que permite a los atacantes controlar sistemas comprometidos de forma remota y exfiltrar datos de forma encubierta. Es una herramienta muy utilizada en ataques a gran escala y puede ser utilizada en sistemas Windows y Linux. El repositorio de Powershell Empire se encuentra en <https://github.com/EmpireProject/Empire>.
* Metasploit: Framework de explotación que permite a los atacantes aprovechar vulnerabilidades en sistemas objetivo y exfiltrar datos de forma encubierta. Es una herramienta muy utilizada en la exfiltración de datos y puede ser utilizada en sistemas Windows y Linux. El repositorio de Metasploit se encuentra en <https://github.com/rapid7/metasploit-framework>.
* Cain & Abel: [https://github.com/xenomuta/cain](https://github.com/xenomuta/cain%20) - una herramienta de recuperación de contraseñas.
* Mimikatz - <https://github.com/gentilkiwi/mimikatz> - una herramienta que permite la extracción de contraseñas, hashes y otros datos sensibles de sistemas Windows.
* Responder - <https://github.com/lgandx/Responder> - una herramienta que permite la captura de hashes de contraseñas enviados a través de protocolos como SMB y HTTP.
* PowerSploit - <https://github.com/PowerShellMafia/PowerSploit> - un conjunto de módulos de PowerShell que permiten la extracción de datos sensibles de sistemas Windows, así como la ejecución de comandos y scripts en la máquina comprometida.
* Empire - <https://github.com/BC-SECURITY/Empire> - un framework de post-explotación para sistemas Windows y Linux que permite la ejecución remota de comandos, la extracción de datos sensibles y la persistencia en el sistema comprometido.
* John the Ripper - <https://github.com/openwall/john> - una herramienta de cracking de contraseñas que permite la extracción de contraseñas de hashes y su posterior descifrado.
* LaZagne - <https://github.com/AlessandroZ/LaZagne> - una herramienta que permite la extracción de contraseñas de aplicaciones y sistemas operativos, incluyendo Windows, Linux, macOS y aplicaciones web.
* Binwalk - <https://github.com/ReFirmLabs/binwalk> - una herramienta que permite la extracción de datos ocultos en archivos binarios, como firmware de dispositivos embebidos.
* Volatility - <https://github.com/volatilityfoundation/volatility> - una herramienta que permite la extracción de información de memoria RAM de sistemas comprometidos, incluyendo procesos, archivos abiertos y contraseñas en caché.
* Empire - <https://github.com/BC-SECURITY/Empire>: Un framework de post-explotación de PowerShell que permite la ejecución remota de comandos en sistemas comprometidos, la extracción de datos sensibles y el pivoteo de red.
* CrackMapExec - <https://github.com/byt3bl33d3r/CrackMapExec>: Una herramienta que permite la ejecución de comandos y la extracción de credenciales en sistemas Windows y Active Directory.
* LaZagne - <https://github.com/AlessandroZ/LaZagne>: Una herramienta que permite la recuperación de contraseñas almacenadas en el sistema, incluyendo navegadores web, clientes de correo electrónico y otros.
* Metasploit Framework - [https://github.com/rapid7/metasploit-framework](https://github.com/rapid7/metasploit-framework%20) - un framework de hacking ofensivo que incluye numerosos módulos y herramientas para la realización de ataques y la post-explotación de sistemas.
* DumpsterDiver - <https://github.com/securing/DumpsterDiver>: Una herramienta que permite la búsqueda de datos sensibles en archivos y carpetas eliminadas en sistemas Unix y Windows.
* EvilGrade - <https://github.com/infobyte/evilgrade>: Una herramienta que permite la inyección de actualizaciones maliciosas en aplicaciones vulnerables, con el fin de comprometer el sistema del usuario.
* Postenum - <https://github.com/mbad/host-exploit-1>: Una herramienta que automatiza la enumeración de información y la extracción de datos sensibles en sistemas Unix, con el fin de facilitar la post-explotación.
* ADRecon: [https://github.com/sense-of-security/ADRecon](https://github.com/sense-of-security/ADRecon%20) - una herramienta de reconocimiento y enumeración de Active Directory que puede extraer información valiosa, como contraseñas en texto plano y hashes de contraseña.
* Steganography: Técnica que se utiliza para ocultar información dentro de imágenes, audio o archivos de vídeo para su posterior recuperación. Herramientas populares incluyen OpenStego, Steghide y OutGuess.

### 5. Mantenimiento de acceso

Una vez que se ha obtenido acceso y escalado los privilegios, se busca una manera de mantener el acceso a largo plazo. El objetivo es mantener el acceso y controlar el sistema o aplicación.

#### Herramientas populares:

* Netcat: Utilidad de red para la transferencia de archivos y el control remoto de un sistema. (<http://netcat.sourceforge.net/>)
* Meterpreter: Carga útil de Metasploit utilizada para mantener el acceso y el control. (<https://www.offensive-security.com/metasploit-unle>ashed/meterpreter-payloads/)
* Covenant: Marco de postexplotación para mantener el acceso y controlar sistemas Windows. (<https://github.com/cobbr/Covenant>)
* Merlin: Es un servidor y agente de comando y control HTTP / 2 post-explotación multiplataforma escrito en golang. <https://github.com/Ne0nd0g/merlin>
* PowershellBackdoor: Reverse backdoor written in PowerShell and obfuscated with Python. <https://github.com/Drew-Alleman/powershell-backdoor-generator>
* Pupy: Herramienta de postexplotación para el control remoto de sistemas Windows, Linux y macOS. (<https://github.com/n1nj4sec/pupy>)
* PowerSploit: Conjunto de herramientas de código abierto que se enfoca en la realización de ataques y la post-explotación en sistemas Windows. (<https://github.com/PowerShellMafia/PowerSploit>)
* Empire: Marco de post-explotación que permite el control remoto de sistemas y la ejecución de comandos en sistemas Windows y Linux. (<https://github.com/BC-SECURITY/Empire>)
* Socat: Herramienta de red de código abierto que permite la creación de conexiones de red seguras y flexibles. (<http://www.dest-unreach.org/socat/>)
* Cobalt Strike: <https://github.com/cobaltstrike> / [PayloadsAllTheThings](https://github.com/swisskyrepo/PayloadsAllTheThings)/[Methodology and Resources](https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Methodology%20and%20Resources)/Cobalt Strike - Cheatsheet.md
* Weevely: <https://github.com/epinna/weevely3>
* Villain:Villain is a Windows & Linux backdoor generator and multi-session handler that allows users to connect with sibling servers (other machines running Villain) and share their backdoor sessions, handy for working as a team [t3l3machus](https://github.com/t3l3machus)/[Villain](https://github.com/t3l3machus/Villain).
* Hoaxshell: hoaxshell is a Windows reverse shell payload generator and handler <https://github.com/t3l3machus/hoaxshell>

Opciones gratuitas para crear un servidor remoto y redirigir las conexiones a través de él. A continuación, se mencionan algunas de estas opciones:

* Ngrok: Es una herramienta gratuita que permite crear túneles seguros desde una dirección pública a un servidor local. De esta forma, se pueden redirigir las conexiones de manera segura a través de ngrok y acceder a ellas desde cualquier lugar. Ngrok está disponible para Windows, Mac y Linux. Para usar ngrok, solo necesitas descargarlo desde su sitio web, registrarte y seguir las instrucciones.
* Serveo: Es otra herramienta gratuita que permite crear túneles seguros y redirigir las conexiones a un servidor local. Al igual que ngrok, serveo es fácil de usar y está disponible para Windows, Mac y Linux. Para utilizar serveo, solo necesitas abrir una conexión SSH y redirigir el tráfico a través de ella.
* LocalXpose: Es una herramienta gratuita que permite crear túneles seguros y redirigir el tráfico a un servidor local. LocalXpose es fácil de usar y está disponible para Windows, Mac y Linux. Para utilizar LocalXpose, solo necesitas descargarlo desde su sitio web, registrarte y seguir las instrucciones.
* Pagekite: Es otra herramienta gratuita que permite crear túneles seguros y redirigir las conexiones a un servidor local. Pagekite es fácil de usar y está disponible para Windows, Mac y Linux. Para utilizar Pagekite, solo necesitas descargarlo desde su sitio web, registrarte y seguir las instrucciones.

Algunas opciones para crear un servidor de forma gratuita son:

* Heroku: Es un servicio de alojamiento web que permite a los usuarios alojar aplicaciones web de forma gratuita. Los usuarios pueden crear una cuenta gratuita en Heroku, subir su aplicación y ejecutarla en un servidor gratuito.
* Amazon Web Services (AWS) Free Tier: AWS ofrece una capa gratuita de servicio que permite a los usuarios crear y ejecutar aplicaciones en la nube de forma gratuita. La capa gratuita incluye servicios como Amazon EC2 (servidor virtual), Amazon S3 (almacenamiento en la nube), Amazon RDS (base de datos en la nube), entre otros.
* Google Cloud Platform (GCP) Free Tier: GCP también ofrece una capa gratuita de servicio que permite a los usuarios crear y ejecutar aplicaciones en la nube de forma gratuita. La capa gratuita incluye servicios como Google Compute Engine (servidor virtual), Google Cloud Storage (almacenamiento en la nube), Google Cloud SQL (base de datos en la nube), entre otros.
* DigitalOcean: Es un servicio de alojamiento web que permite a los usuarios crear servidores virtuales (droplets) en la nube de forma sencilla y rápida. DigitalOcean ofrece un plan gratuito que incluye un servidor con 1 GB de RAM, 25 GB de almacenamiento SSD y 1 TB de transferencia de datos.

## Cobertura de las Huellas

Durante esta fase, se intenta cubrir las huellas y borrar cualquier evidencia del ataque.

* CCleaner: Utilidad de limpieza de código cerrado que elimina archivos temporales, registros y otros datos innecesarios del sistema. (<https://www.ccleaner.com/>)
* Shred: Herramienta de línea de comando de código abierto que sobrescribe archivos con datos aleatorios para borrarlos de forma segura. (<https://www.gnu.org/software/coreutils/manual/html_node/shred-invocation.html>)
* BleachBit: Utilidad de limpieza de código abierto que elimina archivos temporales, registros y otros datos innecesarios del sistema. (<https://www.bleachbit.org/>)
* Timestomp: Herramienta que permite modificar las marcas de tiempo (timestamps) de los archivos para ocultar la fecha y hora de creación, modificación y acceso.
* Metasploit Meterpreter: Módulo de Metasploit que permite borrar archivos y limpiar el registro del sistema comprometido.
* Syslog-ng: es una herramienta de registro de eventos que permite filtrar, clasificar y enrutar registros. Se puede utilizar para borrar los registros o para enviarlos a un servidor remoto.
* Logrotate: es una herramienta que permite rotar, comprimir y eliminar los archivos de registro antiguos. Se puede configurar para eliminar los registros después de un cierto período de tiempo o tamaño.
* Modificación de archivos de registro: se puede modificar manualmente los registros para borrar cualquier evidencia del ataque.

## Anonimato

Ser anónimo en internet y durante un ataque es fundamental para proteger la identidad y evitar ser rastreado por las autoridades. Algunas formas de lograr anonimato son:

* Redes privadas virtuales (VPN): Las VPN encriptan el tráfico de internet, lo que impide que los proveedores de servicios de internet (ISP) o cualquier otra entidad intercepte la información y rastree su origen.
* Navegadores anónimos: Los navegadores como Tor, I2P y Freenet utilizan enrutamiento en cebolla y criptografía para asegurar la privacidad del usuario y ocultar su dirección IP.
* Uso de proxies: Los proxies actúan como intermediarios entre el usuario y el servidor, lo que oculta la dirección IP del usuario y le permite navegar de forma anónima, tor, Privoxy y Squid.
* Ofuscación de datos: La ofuscación de datos puede ayudar a evitar la detección de patrones y ocultar información. Las herramientas de ofuscación de datos, como Obfsproxy y Shadowsocks, pueden ayudar a ocultar la información y las actividades en línea.
* Tails: Es un sistema operativo que se ejecuta desde un USB o DVD, diseñado para preservar la privacidad y el anonimato. Todas las conexiones a internet se enrutan a través de la red TOR, y la memoria del sistema se limpia al apagarlo.

## Herramientas para Pentesting de Aplicaciones Web

Además de las herramientas mencionadas anteriormente, estas son algunas de las mejores y más populares herramientas para pentesting de aplicaciones web:

* Burp Suite: Marco de prueba de seguridad de aplicaciones web que incluye una variedad de herramientas, incluyendo un proxy de interceptación, un escáner de vulnerabilidades y un intruso de ataque personalizado. (<https://portswigger.net/burp>)
* OWASP ZAP: Marco de prueba de seguridad de aplicaciones web de código abierto que incluye una variedad de herramientas, incluyendo un proxy de interceptación, un escáner de vulnerabilidades y un intruso de ataque personalizado. (<https://www.zaproxy.org/>)
* Sqlmap: Herramienta de código abierto que se enfoca en la detección y explotación de vulnerabilidades de inyección SQL en aplicaciones web. (<http://sqlmap.org/>)
* SstiMap: Herramienta de detección automática de SSTI con interfaz interactiva <https://github.com/vladko312/SSTImap>
* Web-Scanner v3.0: Escaner WEB que tiene como objetivo sacar toda la información posible como IP, CMS, Usuarios, posibles correos, rendimiento de la URL, Puertos Abiertos, Subdirectorios. <https://github.com/ShadowVMX/Web-Scanner>
* w3af: Herramienta de código abierto que se enfoca en la detección y explotación de vulnerabilidades de aplicaciones web. (<http://w3af.org/>)
* Nikto: Herramienta de escaneo de código abierto que se enfoca en encontrar vulnerabilidades comunes en servidores web y aplicaciones web. (<https://cirt.net/Nikto2>)
* Flan: Vulnerability Scanner [cloudflare/flan: A pretty sweet vulnerability scanner (github.com)](https://github.com/cloudflare/flan).
* Vega: Herramienta de escaneo de código abierto que se enfoca en encontrar vulnerabilidades en aplicaciones web. (<https://subgraph.com/vega/>)
* Arachni: Herramienta de escaneo de código abierto que se enfoca en encontrar vulnerabilidades en aplicaciones web. (<https://www.arachni-scanner.com/>)
* Skipfish: Herramienta de escaneo de código abierto que se enfoca en encontrar vulnerabilidades en aplicaciones web. (<https://code.google.com/archive/p/skipfish/>)
* Nmap: Herramienta de escaneo de código abierto que se utiliza para identificar hosts y servicios en una red. También puede ser utilizado para encontrar vulnerabilidades en los sistemas escaneados. (<https://nmap.org/>)
* Arachni: Arachni - Web Application Security Scanner Framework [Arachni/arachni: Web Application Security Scanner Framework (github.com)](https://github.com/Arachni/arachni).
* **Acunetix**: herramienta de escaneo de vulnerabilidades en aplicaciones web. [Acunetix.com](https://www.acunetix.com/)
* DamnWebScanner: [swisskyrepo](https://github.com/swisskyrepo)/**[DamnWebScanner](https://github.com/swisskyrepo/DamnWebScanner)**
* Kraken: Webshell modular multilingüe [kraken-ng/Kraken: Kraken, a modular multi-language webshell coded by @secu\_x11 (github.com)](https://github.com/kraken-ng/Kraken).
* Jaeles: The Swiss Army knife for automated Web Application Testing [Jaeles Project (github.com)](https://github.com/jaeles-project).
* Retire: Scan a web app or node app for use of vulnerable JavaScript libraries and/or Node.JS modules [RetireJS/retire.js: scanner detecting the use of JavaScript libraries with known vulnerabilities. Can also generate an SBOM of the libraries it finds. (github.com)](https://github.com/retirejs/retire.js/).
* Findsploit: scanner de exploit en bases de datos local y online [1N3/Findsploit: Find exploits in local and online databases instantly (github.com)](https://github.com/1N3/findsploit).
* BlackWidow: Python based web application spider to gather subdomains, URL's, dynamic parameters, email addresses and phone numbers from a target website. This project also includes Inject-X fuzzer to scan dynamic URL's for common OWASP vulnerabilities [1N3](https://github.com/1N3)/**[BlackWidow](https://github.com/1N3/BlackWidow)**.
* BlackSlashPoweredScanner: Find known and unknown classes of server-side injection vulnerabilities [PortSwigger/backslash-powered-scanner: Finds unknown classes of injection vulnerabilities (github.com)](https://github.com/PortSwigger/backslash-powered-scanner).
* Eagle: Escáner de vulnerabilidades basado en complementos con soporte de subprocesos utilizado para la detección de errores de bajo costo a escala masiva [BitTheByte/Eagle: Multithreaded Plugin based vulnerability scanner for mass detection of web-based applications vulnerabilities (github.com)](https://github.com/BitTheByte/Eagle).
* Cariddi: Take a list of domains, crawl urls and scan for endpoints, secrets, api keys, file extensions, tokens and more [edoardottt/cariddi: Take a list of domains, crawl urls and scan for endpoints, secrets, api keys, file extensions, tokens and more (github.com)](https://github.com/edoardottt/cariddi).
* Scilla: Information Gathering tool - DNS / Subdomains / Ports / Directories enumeration [edoardottt/scilla: Information Gathering tool - DNS / Subdomains / Ports / Directories enumeration (github.com)](https://github.com/edoardottt/scilla).
* Uniscan: una herramienta de escaneo web escrita en Perl que utiliza diferentes técnicas para encontrar vulnerabilidades en aplicaciones web, como inyección de SQL, cross-site scripting (XSS) y local file inclusion (LFI). Repositorio: <https://github.com/Uniscan/uniscan>
* Wapiti: una herramienta de escaneo web escrita en Python que utiliza diferentes técnicas para encontrar vulnerabilidades en aplicaciones web, como inyección de SQL, XSS y LFI. Repositorio: <https://github.com/wapiti-scanner/wapiti>
* CMSmap: una herramienta de escaneo de aplicaciones web escrita en Python que detecta el CMS utilizado por una aplicación web y busca vulnerabilidades específicas de CMS. Repositorio: <https://github.com/Dionach/CMSmap>
* Droopescan: una herramienta de escaneo de aplicaciones web escrita en Python que detecta el CMS utilizado por una aplicación web y busca vulnerabilidades específicas de CMS. Repositorio: <https://github.com/droope/droopescan>
* Skipfish: una herramienta de escaneo de aplicaciones web escrita en C que utiliza diferentes técnicas para encontrar vulnerabilidades en aplicaciones web, como inyección de SQL, XSS y LFI. Repositorio: <https://github.com/spinkham/skipfish>
* ZAP: una herramienta de escaneo de aplicaciones web escrita en Java que puede detectar y explotar vulnerabilidades en aplicaciones web, como inyección de SQL, XSS y LFI. Repositorio: <https://github.com/zaproxy/zaproxy>
* Checklist: [Web Application Penetration Testing Checklist - GBHackers](https://gbhackers.com/web-application-penetration-testing-checklist-a-detailed-cheat-sheet/)
* Amass: una herramienta de enumeración de subdominios escrita en Go que utiliza diferentes fuentes para encontrar subdominios asociados con un dominio específico. Repositorio: <https://github.com/OWASP/Amass>
* EyeWitness: una herramienta de captura de pantallas escrita en Python que toma capturas de pantalla de sitios web y aplicaciones web y las guarda como imágenes. Repositorio: <https://github.com/FortyNorthSecurity/EyeWitness>
* Subfinder: una herramienta de enumeración de subdominios escrita en Go que utiliza diferentes fuentes para encontrar subdominios asociados con un dominio específico. Repositorio: <https://github.com/projectdiscovery/subfinder>
* Aquatone: una herramienta de escaneo de aplicaciones web escrita en Go que realiza un escaneo de puertos y toma capturas de pantalla de sitios web y aplicaciones web. Repositorio: <https://github.com/michenriksen/aquatone>
* Webtech: una herramienta de reconocimiento de tecnologías web escrita en Python que detecta tecnologías utilizadas en una aplicación web, como CMS, frameworks y librerías. Repositorio: <https://github.com/ShielderSec/webtech>
* Wappalyzer: una herramienta de reconocimiento de tecnologías web escrita en JavaScript que detecta tecnologías utilizadas en una aplicación web, como CMS, frameworks y librerías. Repositorio: <https://github.com/AliasIO/Wappalyzer>
* SpiderFoot: una herramienta de inteligencia de amenazas escrita en Python que recopila información sobre un objetivo utilizando diferentes fuentes, como motores de búsqueda, bases de datos públicas y redes sociales. Repositorio: <https://github.com/smicallef/spiderfoot>
* Dirsearch: una herramienta de enumeración de directorios y archivos en una aplicación web escrita en Python que utiliza una lista de palabras clave para buscar posibles rutas y archivos. Repositorio: <https://github.com/maurosoria/dirsearch>
* Gobuster: una herramienta de enumeración de directorios y archivos en una aplicación web escrita en Go que utiliza una lista de palabras clave para buscar posibles rutas y archivos. Repositorio: <https://github.com/OJ/gobuster>
* wfuzz: una herramienta de enumeración de directorios y archivos en una aplicación web escrita en Python que utiliza una lista de palabras clave para buscar posibles rutas y archivos. Repositorio: <https://github.com/xmendez/wfuzz>
* Parameth: una herramienta de enumeración de parámetros en una aplicación web escrita en Python que busca posibles parámetros de entrada en una aplicación web. Repositorio: <https://github.com/maK-/parameth>
* Sublist3r: una herramienta de enumeración de subdominios en una aplicación web escrita en Python que utiliza diferentes fuentes para encontrar subdominios asociados con un dominio específico. Repositorio: <https://github.com/aboul3la/Sublist3r>
* Shellshock Scanner: es una herramienta de Bash que permite buscar vulnerabilidades de Shellshock en servidores web. Puede ser utilizado para encontrar servidores vulnerables y lanzar ataques de inyección de comandos. Repositorio: <https://github.com/nccgroup/shocker>
* SQLiv: es una herramienta de Python para la exploración de inyecciones de SQL. Es capaz de detectar inyecciones de SQL en diferentes tipos de bases de datos y puede ser utilizado para lanzar ataques de inyección de SQL. Repositorio: <https://github.com/Hadesy2k/sqliv>
* Checklist: [Web Application Penetration Testing Checklist - GBHackers](https://gbhackers.com/web-application-penetration-testing-checklist-a-detailed-cheat-sheet/)
* Repositorio con cantidad de herramientas: <https://github.com/kurogai/WebHackersWeapons>
* [URL and website scanner - urlscan.io](https://urlscan.io/)

## Herramientas de Creación de Troyanos

Estas son algunas de las herramientas más populares para la creación de troyanos:

* Metasploit Framework: Marco de pruebas de penetración que incluye una variedad de herramientas, incluyendo generadores de payloads y exploits, que se pueden utilizar para crear troyanos. (<https://www.metasploit.com/>)
* Veil-Evasion: Herramienta de código abierto que permite la generación de troyanos que evitan la detección por parte de los sistemas antivirus. (<https://github.com/Veil-Framework/Veil-Evasion>)
* Empire: Herramienta de código abierto que permite la creación de troyanos que permiten la toma de control remoto de sistemas comprometidos. (<https://github.com/BC-SECURITY/Empire>)
* Pupy: Herramienta de código abierto que permite la escalada de privilegios y la toma de control remoto de sistemas Windows, Linux y OS X. (<https://github.com/n1nj4sec/pupy>)
* Covenant: Herramienta de código abierto que permite la creación de troyanos que permiten la toma de control remoto de sistemas comprometidos. (<https://github.com/cobbr/Covenant>)
* TheFatRat: Herramienta de código abierto que permite la generación de troyanos multiplataforma con diversas funcionalidades, como captura de pantalla, registro de teclas, captura de webcam, entre otras. (<https://github.com/Screetsec/TheFatRat>)
* Venom: Herramienta de código abierto que permite la generación de troyanos que evitan la detección por parte de los sistemas antivirus, a través de la inyección de payloads en archivos legítimos. (<https://github.com/r00t-3xp10it/venom>)
* AndroRAT: Herramienta de código abierto que permite la creación de troyanos para dispositivos Android, que permiten el control remoto del dispositivo infectado. (<https://github.com/wszf/androrat>)
* EvilOSX: Herramienta de código abierto que permite la creación de troyanos para dispositivos Mac OS X, que permiten el control remoto del dispositivo infectado. (<https://github.com/Marten4n6/EvilOSX>)
* QuasarRAT: Herramienta de código abierto que permite la creación de troyanos para sistemas Windows, que permiten el control remoto del sistema infectado. (<https://github.com/quasar/QuasarRAT>)
* Empire: Herramienta de código abierto que permite la creación de troyanos para sistemas Windows y Linux, que permiten el control remoto del sistema infectado. Cuenta con diversas funcionalidades como captura de pantalla, registro de teclas, captura de webcam, entre otras. (<https://github.com/BC-SECURITY/Empire>)
* Koadic: Herramienta de código abierto que permite la creación de troyanos para sistemas Windows, que permiten el control remoto del sistema infectado. Cuenta con diversas funcionalidades como captura de pantalla, registro de teclas, captura de webcam, entre otras. (<https://github.com/zerosum0x0/koadic>)
* Gcat: Herramienta de código abierto que permite la creación de troyanos para sistemas Mac OS X y Linux, que permiten el control remoto del sistema infectado. (<https://github.com/byt3bl33d3r/gcat>)
* Metasploit Framework: Herramienta de código abierto que permite la creación de troyanos y otros tipos de exploits para diversas plataformas, que permiten el control remoto del sistema infectado. Cuenta con una amplia variedad de funcionalidades y módulos que permiten la explotación de diversas vulnerabilidades. (<https://github.com/rapid7/metasploit-framework>)
* Veil Framework: Herramienta de código abierto que permite la creación de troyanos y otros tipos de exploits para diversas plataformas, que permiten el control remoto del sistema infectado. Cuenta con diversas funcionalidades para evadir la detección por parte de los sistemas antivirus. (<https://github.com/Veil-Framework/Veil>)

## Herramientas de Ingeniería Social

A continuación, se incluyen algunas herramientas de ingeniería social que pueden ser utilizadas en pruebas de penetración:

* Mip22: Advanced Pishing tool <https://github.com/makdosx/mip22>
* SET (Social-Engineer Toolkit): Herramienta de código abierto que permite la automatización de diversas técnicas de ingeniería social, como phishing, engaño en redes sociales, entre otras. (<https://github.com/trustedsec/social-engineer-toolkit>)
* BeEF (Browser Exploitation Framework): Herramienta de código abierto que permite la exploración de vulnerabilidades en navegadores web a través de técnicas de ingeniería social, como el control remoto de navegadores web y la obtención de información de los usuarios. (<https://github.com/beefproject/beef>)
* Evilginx2: Herramienta de código abierto que permite la creación de servidores proxy maliciosos que permiten la obtención de credenciales y otra información sensible a través de técnicas de phishing y engaño en la autenticación en línea. (<https://github.com/kgretzky/evilginx2>)
* Gophish: Herramienta de código abierto que permite la automatización de campañas de phishing, desde la creación de correos electrónicos hasta el seguimiento de la interacción de los usuarios con los mismos. (<https://github.com/gophish/gophish>)
* SETOOLKIT: Herramienta de código abierto que permite la automatización de diversas técnicas de ingeniería social, como phishing, engaño en redes sociales, entre otras. Es una alternativa a SET y se enfoca en el phishing a través de SMS. (<https://github.com/SocialEngineeringTools/SEToolkit>)
* SocialFish: Herramienta de código abierto que permite la automatización de ataques de phishing en redes sociales, con un enfoque en Facebook, Instagram, Google, entre otros. (<https://github.com/UndeadSec/SocialFish>)
* PhishLulz: Herramienta de ingeniería social que permite la creación de correos electrónicos y páginas de phishing personalizadas para engañar a las víctimas y obtener información de ellas. (<https://github.com/dylanari/phishlulz>)
* ReelPhish: Herramienta de ingeniería social que permite la creación de páginas de phishing personalizadas para capturar información de las víctimas. (<https://github.com/fireeye/ReelPhish>)
* HiddenEye: Herramienta de ingeniería social que permite la creación de páginas de phishing personalizadas para capturar información de las víctimas, con un enfoque en la creación de páginas falsas de inicio de sesión. (<https://github.com/DarkSecDevelopers/HiddenEye>)
* King Phisher: Herramienta de código abierto que permite la creación y automatización de campañas de phishing personalizadas, incluyendo la creación de correos electrónicos de phishing y la simulación de sitios web maliciosos. (<https://github.com/securestate/king-phisher>).
* Phisher: Tool designed for performing various social engineering attacks using PHP Apache & Ngrok <https://github.com/Yezz123-Archive/Phisher>.
* Zpisher: Framework de campañas de pishing <https://github.com/Optane002/ZPhisher>

## Herramientas OSINT para Redes Sociales

A continuación, se presentan algunas herramientas de OSINT para obtener información de redes sociales como Facebook, Instagram y Twitter:

* Facebook Graph Search: Herramienta de búsqueda de Facebook que permite realizar búsquedas avanzadas en la plataforma, como por ejemplo buscar publicaciones, fotos, vídeos, entre otros. (<https://www.facebook.com/about/graphsearch>)
* Maigret: Recopilar un dossier sobre una persona por nombre de usuario de miles de sitios <https://github.com/soxoj/maigret>
* NetBootCamp: Herramienta que permite buscar información en diferentes redes sociales, como Facebook, Twitter, LinkedIn, entre otros. (<https://netbootcamp.org/>)
* Sherlock: Herramienta de código abierto que permite buscar información en diferentes redes sociales, como Facebook, Instagram, Twitter, LinkedIn, entre otros. (<https://github.com/sherlock-project/sherlock>)
* StalkScan: Herramienta de búsqueda que permite buscar información en perfiles públicos de Facebook, como publicaciones, fotos, vídeos, entre otros. (<https://stalkscan.com/>)
* Twint: Herramienta de OSINT que permite buscar información en Twitter, como por ejemplo buscar publicaciones, tweets, seguidores, entre otros. (<https://github.com/twintproject/twint>)
* Instalooter: Herramienta de OSINT que permite descargar fotos y vídeos de perfiles públicos de Instagram. (<https://github.com/althonos/InstaLooter>)
* Social Mapper: Esta herramienta de OSINT automatiza el proceso de búsqueda y seguimiento de objetivos en diferentes redes sociales, incluyendo Facebook, Instagram, Twitter, LinkedIn, entre otros. (<https://github.com/SpiderLabs/social_mapper>)
* FacebookOSINT: Esta herramienta de OSINT se centra exclusivamente en la búsqueda de información de Facebook, y permite buscar por nombre, correo electrónico, teléfono, fecha de nacimiento, ubicación y otros criterios. (<https://github.com/lockfale/FacebookOSINT>)
* InstaInsane: Esta herramienta de OSINT para Instagram permite la descarga masiva de fotos, vídeos y otros contenidos, así como la búsqueda de hashtags y localizaciones. (<https://github.com/thelinuxchoice/instainsane>)
* TweetDeck: Esta herramienta de Twitter permite personalizar la visualización de tweets, búsquedas, menciones y hashtags en una sola pantalla, lo que facilita el monitoreo y análisis de información en tiempo real. (<https://tweetdeck.twitter.com/>)
* GramSpider: Esta herramienta de OSINT para Instagram permite buscar usuarios, publicaciones, hashtags y comentarios, y descargar fotos y vídeos en masa. (<https://github.com/Naategh/GramSpider>)
* TweetBeaver: Esta herramienta de OSINT para Twitter permite buscar tweets y usuarios en función de diferentes criterios, como palabras clave, ubicación y fecha, y exportar los resultados en diferentes formatos. (<https://github.com/NoxHarmonium/tweetbeaver>)
* Creepy: Herramienta de OSINT que permite la recopilación de información en redes sociales como Facebook, Twitter, Instagram, entre otras. (<https://github.com/ilektrojohn/creepy>)
* FaceDominator: Herramienta de OSINT que permite la gestión y automatización de cuentas en Facebook, así como la recopilación de información de perfiles públicos. (<https://facedominator.com/>)
* Instalooter: Herramienta de OSINT que permite la descarga de imágenes y vídeos de Instagram, así como la búsqueda y recopilación de información de perfiles públicos. (<https://github.com/althonos/InstaLooter>)
* Tinfoleak: Herramienta de OSINT para Twitter que permite la recopilación de información de cuentas y tweets, así como la generación de informes detallados. (<https://github.com/vaguileradiaz/tinfoleak>)
* FBI (Facebook Information): Herramienta de OSINT que permite a los investigadores recopilar información de perfiles de Facebook, incluyendo la información de contacto y la actividad reciente. (<https://github.com/xHak9x/fbi>)
* Instalooter: Herramienta de OSINT que permite a los investigadores descargar fotos, videos y otros medios de Instagram. (<https://github.com/althonos/InstaLooter>)

## Herramientas OSINT para correos electrónicos

Aquí hay algunas herramientas de OSINT que se pueden utilizar para obtener información a partir de correos electrónicos:

* Hunter.io: Esta herramienta de OSINT permite buscar direcciones de correo electrónico, y proporciona información sobre la empresa, la posición del titular del correo electrónico y otras direcciones de correo electrónico que pueden estar relacionadas con el objetivo. (<https://hunter.io/>)
* The Harvester: Esta herramienta de OSINT permite recopilar información pública de diferentes fuentes, incluyendo correos electrónicos, subdominios, hosts y direcciones IP, utilizando diferentes motores de búsqueda. (<https://github.com/laramies/theHarvester>)
* Shodan: Esta herramienta de OSINT permite buscar dispositivos conectados a Internet, incluyendo servidores de correo electrónico, routers y otros dispositivos que puedan estar relacionados con el objetivo. (<https://www.shodan.io/>)
* Infoga: Esta herramienta de OSINT automatiza la búsqueda de información de correos electrónicos, incluyendo la verificación de su existencia, la búsqueda de dominios relacionados y la enumeración de subdominios. (<https://github.com/m4ll0k/Infoga>)
* HaveIBeenPwned: Servicio web de OSINT que permite la verificación de si una cuenta de correo electrónico ha sido comprometida en alguna brecha de seguridad conocida. (<https://haveibeenpwned.com/>)
* EmailRep.io: Esta herramienta de OSINT proporciona información sobre la reputación de un correo electrónico, incluyendo su probabilidad de ser spam, su historial de abuso y la existencia de malware relacionado. (<https://emailrep.io/>)
* Metagoofil: Esta herramienta de OSINT permite buscar información relacionada con un correo electrónico, incluyendo archivos adjuntos, enlaces y metadatos. (<https://github.com/laramies/metagoofil>)
* Maltego: Esta herramienta de OSINT permite recopilar información sobre un objetivo utilizando técnicas de minería de datos y visualización de redes. Maltego también puede utilizarse para buscar información de correos electrónicos, incluyendo la enumeración de subdominios, la búsqueda de perfiles de redes sociales y la identificación de otros contactos relacionados. (<https://www.maltego.com/>)
* Pipl: Esta herramienta de OSINT permite buscar información de personas utilizando diferentes criterios de búsqueda, incluyendo el correo electrónico. Pipl puede proporcionar información sobre la dirección física, la actividad en redes sociales, la dirección IP y otros detalles sobre el objetivo. (<https://pipl.com/>)
* Intel Techniques: Esta herramienta de OSINT proporciona una gran cantidad de recursos y técnicas para buscar información en línea, incluyendo herramientas para buscar información de correos electrónicos, identificar perfiles de redes sociales, buscar números de teléfono y otra información relevante. (<https://inteltechniques.com/>)
* SocialCatfish: Esta herramienta de OSINT permite buscar información de personas utilizando diferentes criterios de búsqueda, incluyendo el correo electrónico. SocialCatfish puede proporcionar información sobre el historial criminal, los registros de propiedad, la actividad en redes sociales y otros detalles sobre el objetivo. (<https://socialcatfish.com/>)
* Sherlock: Esta herramienta de OSINT permite buscar perfiles de redes sociales a partir de un nombre de usuario o dirección de correo electrónico. Sherlock puede buscar en diferentes plataformas de redes sociales, incluyendo Instagram, Twitter, TikTok, Snapchat y otros. (<https://github.com/sherlock-project/sherlock>)

## Herramientas de Reconocimiento Facial

Aquí hay algunas herramientas de reconocimiento facial que se pueden utilizar en un contexto de pentesting o pruebas de seguridad:

* OpenCV: Esta es una biblioteca de visión por computadora de código abierto que se puede utilizar para desarrollar aplicaciones de reconocimiento facial. OpenCV incluye algoritmos para detectar rostros y reconocer patrones faciales, así como para entrenar y ajustar modelos de reconocimiento facial. (<https://opencv.org/>)
* DeepFaceLab: Esta es una herramienta de código abierto para el aprendizaje profundo de caras. DeepFaceLab utiliza redes neuronales para realizar tareas como el reconocimiento facial, la clasificación de edad y la transferencia de caras. La herramienta también cuenta con una interfaz gráfica de usuario (GUI) para facilitar su uso. (<https://github.com/iperov/DeepFaceLab>)
* Dlib: Esta es una biblioteca de código abierto para el procesamiento de imágenes y el aprendizaje automático. Dlib incluye herramientas para la detección de rostros, el seguimiento de puntos de referencia faciales y la comparación de rostros para el reconocimiento facial. (<http://dlib.net/>)
* Face\_recognition: Esta es una biblioteca de código abierto para el reconocimiento facial. Face\_recognition utiliza la biblioteca de aprendizaje profundo dlib para detectar y reconocer rostros en imágenes y videos. La biblioteca también cuenta con una API Python fácil de usar. (<https://github.com/ageitgey/face_recognition>)
* OpenBR: Esta es una biblioteca de reconocimiento biométrico de código abierto que incluye herramientas para la identificación y verificación de rostros, así como para la identificación de otras características biométricas como huellas dactilares y iris. OpenBR se puede utilizar en una variedad de sistemas operativos, incluyendo Windows, Linux y MacOS. (<http://openbiometrics.org/>)
* FaceNet: Framework de aprendizaje profundo para reconocimiento facial que permite la creación de modelos personalizados. (<https://github.com/davidsandberg/facenet>)
* Facial recognition API: API de reconocimiento facial que permite a los desarrolladores agregar capacidades de reconocimiento facial a sus aplicaciones. (<https://azure.microsoft.com/en-us/services/cognitive-services/face/>)
* Rekognition: Servicio de reconocimiento facial de Amazon que permite a los desarrolladores agregar capacidades de reconocimiento facial a sus aplicaciones. (<https://aws.amazon.com/rekognition/>)

## Herramientas OSINT para Fotografías

Aquí hay algunas herramientas de OSINT que se pueden utilizar para obtener información a partir de fotografías:

* Google Images: Con la función de búsqueda de imágenes de Google, se puede realizar una búsqueda inversa de una imagen para encontrar otras instancias de la misma imagen en línea. Esto puede ser útil para encontrar información sobre la imagen, como su origen o cualquier otra información asociada con ella.
* TinEye: TinEye es una herramienta de búsqueda de imágenes inversa similar a Google Images. Puede ayudar a encontrar otros lugares en línea donde se ha publicado la imagen y proporcionar información sobre su origen y uso.
* ExifTool: Esta es una herramienta de línea de comandos que puede leer y escribir información de metadatos en archivos de imagen. La información de metadatos puede incluir detalles como la ubicación y la fecha en que se tomó la fotografía, la cámara utilizada para tomarla y otros detalles técnicos.
* FotoForensics: Esta herramienta permite analizar la autenticidad de una imagen mediante el análisis de sus metadatos y las características de la imagen. También puede detectar si la imagen ha sido manipulada o editada de alguna manera.
* Social Catfish: Esta herramienta permite realizar una búsqueda de imagen inversa en múltiples plataformas de redes sociales para encontrar perfiles de usuario asociados con la imagen.
* Sherlock: Esta es una herramienta de OSINT que permite buscar un nombre de usuario en varias redes sociales y sitios web en línea. Si se proporciona una imagen del usuario, la herramienta también puede realizar una búsqueda inversa de la imagen para encontrar otros perfiles en línea asociados con la misma imagen.
* Yandex Images: Yandex Images es un motor de búsqueda de imágenes similar a Google Images, que puede ayudar a encontrar otras instancias de una imagen en línea y proporcionar información sobre su origen y uso.
* ImageIdentify: Esta herramienta utiliza la tecnología de reconocimiento de imagen de Google para identificar objetos, personas y lugares en una imagen, lo que puede proporcionar información adicional sobre la imagen y su contenido.
* ImageForensics: ImageForensics es una herramienta que permite analizar una imagen para detectar si ha sido manipulada o alterada de alguna manera. También puede proporcionar información sobre la cámara utilizada para tomar la imagen, la fecha y la ubicación en que se tomó, y otros detalles técnicos.
* WolframAlpha: WolframAlpha es un motor de conocimiento computacional que puede proporcionar información sobre una imagen en función de su contenido. Por ejemplo, si se carga una imagen de un monumento o edificio famoso, WolframAlpha puede proporcionar información sobre su historia, arquitectura y ubicación.
* PimEyes: PimEyes es una herramienta de búsqueda de imágenes inversa que se centra en encontrar imágenes de caras. Puede ayudar a encontrar perfiles en línea asociados con una cara específica y proporcionar información sobre la persona.
* StalkScan: StalkScan es una herramienta que permite obtener información de los perfiles de Facebook públicos utilizando la URL del perfil. Puede proporcionar información sobre la persona, como sus publicaciones, fotos, amigos y otras actividades en línea.

## Hacking de Redes Sociales

Herramientas populares:

* Social-Engineer Toolkit (SET): Es una herramienta de código abierto que se utiliza para llevar a cabo ataques de ingeniería social. El SET puede utilizarse para enviar correos electrónicos de phishing, crear sitios web falsos para el phishing y realizar otros tipos de ataques de ingeniería social.
* BeEF: Es una herramienta de prueba de penetración que se utiliza para probar la seguridad de los navegadores web. BeEF permite a los probadores de seguridad realizar ataques de XSS (Cross-site scripting) y otros tipos de ataques en el navegador de la víctima.
* Burp Suite: Es una herramienta de prueba de penetración que se utiliza para probar la seguridad de las aplicaciones web. Burp Suite puede ser utilizado para encontrar vulnerabilidades en las páginas de inicio de sesión y otras partes de las aplicaciones web, lo que podría permitir a un atacante obtener acceso a una cuenta de redes sociales.
* Hydra: Es una herramienta de fuerza bruta que se utiliza para adivinar contraseñas. Hydra puede ser utilizado para probar la seguridad de las cuentas de redes sociales, adivinando contraseñas comunes o utilizando diccionarios de contraseñas.
* Metasploit: Es un marco de prueba de penetración que se utiliza para encontrar y explotar vulnerabilidades en sistemas y aplicaciones. Metasploit puede ser utilizado para encontrar vulnerabilidades en las aplicaciones de redes sociales y explotarlas para obtener acceso a la cuenta.
* SSLstrip: Es una herramienta que puede ser utilizada para interceptar el tráfico web entre el usuario y el servidor de la red social, permitiendo a un atacante ver y modificar la información que se intercambia.
* Wireshark: Es una herramienta de análisis de red que permite a los probadores de seguridad ver y analizar el tráfico de red en tiempo real. Wireshark puede ser utilizado para detectar vulnerabilidades en la red de una organización, lo que podría permitir a un atacante obtener acceso a una cuenta de redes sociales.
* Nmap: Es una herramienta de escaneo de puertos que se utiliza para descubrir servicios y puertos abiertos en un sistema. Nmap puede ser utilizado para identificar vulnerabilidades en el sistema de una organización, lo que podría permitir a un atacante obtener acceso a una cuenta de redes sociales.
* John the Ripper: Es una herramienta de fuerza bruta que se utiliza para adivinar contraseñas. John the Ripper puede ser utilizado para probar la seguridad de las contraseñas de las cuentas de redes sociales.
* InstaHack: Herramienta de hacking de cuentas de Instagram que utiliza fuerza bruta para adivinar contraseñas. (<https://github.com/avramit/instahack>)
* FaceNiff: Herramienta de hacking de cuentas de Facebook que intercepta el tráfico de red y permite capturar las credenciales de inicio de sesión. (<https://faceniff.ponury.net/>)
* TwitterSniper: Herramienta de hacking de cuentas de Twitter que utiliza técnicas de fuerza bruta para adivinar contraseñas. (<https://github.com/NullArray/TwitterSniper>)
* PhishingFrenzy: Herramienta de phishing que permite a los atacantes crear y personalizar correos electrónicos de phishing para engañar a los usuarios y obtener sus credenciales de inicio de sesión. (<https://github.com/pentestgeek/phishing-frenzy>)
* SocialFish: Herramienta de phishing que permite a los atacantes crear y personalizar páginas de inicio de sesión falsas para obtener las credenciales de inicio de sesión de los usuarios. (<https://github.com/UndeadSec/SocialFish>)

## Hack WIFI

Hacking de Redes WiFi:

Tipos de ataque de redes WiFi:

* Rogue Access Point - Punto de acceso fraudulento: un ataque en el que se crea un punto de acceso falso para engañar a los usuarios para que se conecten y puedan ser monitoreados o manipulados.
* Evil Twin - Doble malvado: un ataque en el que se crea un punto de acceso falso con el mismo nombre que un punto de acceso legítimo para engañar a los usuarios para que se conecten y puedan ser monitoreados o manipulados.
* Deauthentication Attack - Ataque de desautenticación: un ataque en el que se envían paquetes de desautenticación a un dispositivo o punto de acceso para interrumpir la conexión y posiblemente forzar una nueva autenticación que pueda ser interceptada.
* Fake Access Point - Punto de acceso falso: un ataque en el que se crea un punto de acceso falso que imita a un punto de acceso legítimo para engañar a los usuarios para que se conecten y puedan ser monitoreados o manipulados.
* WEP/WPA Key Cracking - Descifrado de clave WEP/WPA: un ataque en el que se intenta descifrar la clave de cifrado WEP/WPA para obtener acceso a la red.
* Packet Sniffing - Captura de paquetes: un ataque en el que se capturan y analizan los paquetes de datos transmitidos en la red para obtener información confidencial.
* Man-in-the-Middle - Hombre en el medio: un ataque en el que un atacante intercepta y manipula la comunicación entre dos dispositivos para obtener información confidencial.
* Eavesdropping - Escuchando: un ataque en el que un atacante intercepta y escucha la comunicación inalámbrica entre dos dispositivos para obtener información confidencial.
* Wireless Bridging - Puente inalámbrico: un ataque en el que un atacante establece una conexión inalámbrica no autorizada entre dos dispositivos para obtener acceso a la red.
* Chop-Chop: Esta técnica consiste en desautenticar a un usuario de una red Wi-Fi para luego capturar un paquete cifrado que contenga información sobre la clave. Luego, se utiliza una técnica de análisis estadístico para descifrar la clave a partir de la información contenida en el paquete.
* Beacon Flooding: Esta técnica consiste en enviar una gran cantidad de paquetes de sondeo a una red Wi-Fi, lo que puede causar que la red se sobrecargue y deje de funcionar correctamente.
* Wireless Jamming: En este tipo de ataque, se utiliza un dispositivo para emitir señales de radiofrecuencia que interfieren con la señal Wi-Fi, lo que puede causar que los usuarios de la red se desconecten o que la red deje de funcionar correctamente.

Herramientas:

* Aircrack-ng - <https://github.com/aircrack-ng/aircrack-ng>
* Reaver - <https://github.com/t6x/reaver-wps-fork-t6x>
* Fern WiFi Cracker - <https://github.com/savio-code/fern-wifi-cracker>
* Kismet - <https://www.kismetwireless.org/>
* Wireshark - <https://github.com/wireshark/wireshark>
* Wifite - <https://github.com/derv82/wifite2>
* FruityWifi - <https://github.com/xtr4nge/FruityWifi>
* Fluxion - <https://github.com/FluxionNetwork/fluxion>
* Airgeddon - <https://github.com/v1s1t0r1sh3r3/airgeddon>
* Wifiphisher - <https://github.com/wifiphisher/wifiphisher>
* Pixiewps - <https://github.com/wiire-a/pixiewps>
* Aircrack-ng - <https://github.com/aircrack-ng/aircrack-ng>
* Fern WiFi Cracker - <https://github.com/savio-code/fern-wifi-cracker>
* Kismet - <https://www.kismetwireless.net/>
* Reaver - <https://github.com/t6x/reaver-wps-fork-t6x>
* Ghost Phisher - <https://github.com/savio-code/ghost-phisher>
* Wireshark - <https://www.wireshark.org/>
* Infernal Twin - <https://github.com/entropy1337/infernal-twin>
* Bully - <https://github.com/aanarchyy/bully>
* Bettercap: [https://github.com/bettercap/bettercap](https://github.com/bettercap/bettercap)).
* RouterSploit: una herramienta de pruebas de penetración para routers inalámbricos que utiliza exploits conocidos. (<https://github.com/threat9/routersploit>)
* Mindmap: [c4s73r/NetworkNightmare: Network Pentesting Mindmap by Caster (github.com)](https://github.com/c4s73r/NetworkNightmare)
* Checklist: [Wireless Penetration Testing Checklist - A Detailed Cheat Sheet (gbhackers.com)](https://gbhackers.com/wireless-penetration-testing-checklist-a-detailed-cheat-sheet/)
* Herramienta de aprendizaje: [The HakCat WiFi Nugget is a beginner’s guide to wireless mischief - The Verge](https://www.theverge.com/23438967/hakcat-wifi-nugget-hacking-open-source-hak5)

## Análisis Forense

Herramientas de análisis forense e ingeniería inversa junto con sus repositorios:

* Volatility: Framework para análisis de memoria forense. (<https://github.com/volatilityfoundation/volatility>)
* Wireshark: Analizador de protocolos de red. (<https://github.com/wireshark/wireshark>)
* Autopsy: Plataforma de análisis forense digital. (<https://github.com/sleuthkit/autopsy>)
* IDA Pro: Desensamblador y depurador de código binario. (<https://www.hex-rays.com/products/ida/>)
* OllyDbg: Depurador de código binario. (<http://www.ollydbg.de/>)
* Ghidra: Herramienta de ingeniería inversa de código abierto. (<https://github.com/NationalSecurityAgency/ghidra>)
* Radare2: Marco de trabajo para ingeniería inversa y análisis binario. (<https://github.com/radareorg/radare2>)
* Capstone: Marco de trabajo para desensamblar código binario. (<https://github.com/aquynh/capstone>)
* Hopper: Desensamblador y depurador de código binario. (<https://www.hopperapp.com/>)
* Frida: Marco de trabajo de instrumentación y depuración dinámica de aplicaciones. (<https://github.com/frida/frida>)
* Recuva: Recuperador de archivos borrados [Download Recuva | Recover deleted files, free! (ccleaner.com)](https://www.ccleaner.com/es-es/recuva).
* EmailAnalyzer: Puede analizar sus correos electrónicos sospechosos. Puede extraer encabezados, vínculos y hashes del archivo .eml <https://github.com/keraattin/EmailAnalyzer>
* FtkImager: Montar imágenes de unidades para su análisis [FTK Imager - Exterro](https://www.exterro.com/ftk-imager)
* EnCase: Software de análisis forense digital utilizado por investigadores y profesionales de seguridad informática para adquirir, analizar y presentar evidencia digital. (<https://www.guidancesoftware.com/>)
* Autopsy: Plataforma de análisis forense digital de código abierto que incluye herramientas de análisis de imágenes, recuperación de datos y análisis de registro de eventos. (<https://www.sleuthkit.org/autopsy/>)
* FTK Imager: Herramienta gratuita de análisis forense utilizada para adquirir y analizar imágenes de discos duros y dispositivos de almacenamiento. (<https://accessdata.com/products-services/forensic-toolkit-ftk>)
* Oxygen Forensic Detective: Herramienta de análisis forense que permite a los investigadores de seguridad examinar dispositivos móviles, aplicaciones y datos almacenados en la nube. (<https://www.oxygen-forensic.com/>)
* Scalpel: Herramienta de recuperación de archivos que se utiliza para extraer archivos de sistemas de archivos dañados o corruptos. (<https://github.com/sleuthkit/scalpel>)
* OSForensics: Plataforma de análisis forense que incluye herramientas para examinar sistemas de archivos, particiones, registros y archivos de imagen. (<https://www.osforensics.com/>)
* Ghiro: Herramienta de análisis forense digital que permite a los investigadores examinar imágenes y archivos para extraer información importante. (<https://github.com/Ghirensics/ghiro>)
* BitPim: Herramienta de análisis forense utilizada para examinar dispositivos móviles y extraer información importante como contactos, mensajes de texto y registros de llamadas. (<https://github.com/bitpim/bitpim>)
* Wireshark: Herramienta de análisis de tráfico de red de código abierto que permite a los usuarios capturar y analizar paquetes de red en tiempo real. Proporciona herramientas para filtrar y visualizar el tráfico de red. (<https://www.wireshark.org/>)
* Osticket: Herramienta de gestión de tickets de código abierto utilizada en el análisis de incidentes de seguridad. Permite a los usuarios crear, asignar y rastrear tickets relacionados con incidentes de seguridad. (<https://osticket.com/>)
* OSSEC: Sistema de detección de intrusos de código abierto utilizado para monitorear sistemas y redes en busca de actividades sospechosas. Proporciona alertas en tiempo real sobre posibles amenazas de seguridad. (<https://www.ossec.net/>)
* Bro: Plataforma de análisis de red de código abierto utilizada para monitorear y analizar el tráfico de red en tiempo real. Proporciona herramientas para detectar patrones de comportamiento y amenazas de seguridad. (<https://www.bro.org/>)
* RegRipper: Herramienta de análisis de registro de Windows utilizada para extraer información importante del registro del sistema operativo. Proporciona una amplia variedad de plugins para analizar diferentes áreas del registro. (<https://github.com/keydet89/RegRipper3.0>)
* Bulk Extractor: Herramienta de análisis de datos forenses utilizada para extraer información de archivos y discos duros. Proporciona herramientas para extraer direcciones de correo electrónico, números de teléfono y otros tipos de información. (<https://github.com/simsong/bulk_extractor>)

## Análisis de Malware

Herramientas de análisis de malware:

* Malwarebytes: Herramienta de análisis de malware que puede detectar y eliminar amenazas de software malintencionado. (<https://www.malwarebytes.com/>)
* VirusTotal: Servicio web de análisis de malware que escanea archivos sospechosos en busca de amenazas y proporciona informes detallados sobre el análisis. (<https://www.virustotal.com/>)
* Yara: Herramienta de análisis de malware que permite a los analistas de seguridad escribir reglas para identificar malware específico y comportamientos maliciosos. (<https://virustotal.github.io/yara/>)
* Cuckoo Sandbox: Plataforma de análisis de malware que ejecuta malware en un entorno aislado y captura la actividad maliciosa para su análisis. (<https://cuckoosandbox.org/>)
* REMnux: Distribución de Linux especializada en análisis de malware que incluye herramientas para examinar y desensamblar código malicioso. (<https://remnux.org/>)
* Sysinternals Suite: Colección de herramientas de análisis de malware para sistemas Windows, incluyendo herramientas para monitorear procesos, examinar archivos y registrar la actividad del sistema. (<https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>)
* IDA Pro: Herramienta de ingeniería inversa utilizada para examinar y desensamblar código de malware y otros programas. (<https://www.hex-rays.com/products/ida/>)
* Wireshark: Herramienta de análisis de tráfico de red que permite a los analistas de seguridad examinar el tráfico de red y detectar patrones de comportamiento malicioso. (<https://www.wireshark.org/>)
* Cuckoo Sandbox: es una herramienta de análisis de malware de código abierto que permite simular un entorno de ejecución de malware y analizar su comportamiento. Repositorio: <https://github.com/cuckoosandbox/cuckoo>
* Yara: es una herramienta de análisis de malware que permite buscar patrones en el código de un archivo y así identificar si es malicioso. Repositorio: <https://github.com/VirusTotal/yara>
* REMnux: es una distribución de Linux especializada en análisis de malware. Incluye una amplia variedad de herramientas de análisis de malware y permite la ejecución de estas herramientas en un entorno aislado para evitar la propagación del malware. Repositorio: <https://github.com/REMnux/remnux-distro>
* Volatility Framework: es una herramienta de análisis de memoria que permite analizar la memoria de un sistema en busca de evidencia de malware o intrusiones. Repositorio: <https://github.com/volatilityfoundation/volatility>
* Sandfly Security: es una herramienta de análisis de malware que se centra en detectar y responder a amenazas persistentes avanzadas en sistemas Linux y Windows. Repositorio: <https://github.com/sandflysecurity/sandfly>
* Any.Run es un servicio en línea que permite analizar archivos maliciosos y URLs en busca de malware y otras amenazas de seguridad. Puedes acceder al sitio web de Any.Run en <https://app.any.run/>
* PeStudio: Análisis estático de Malware [petoolse/petools: PE Tools - Portable executable (PE) manipulation toolkit (github.com)](https://github.com/petoolse/petools)
* Regshot advanced: Regshot advanced es una herramienta para monitorear y registrar cambios en el sistema de archivos y el registro, por ejemplo, realizados por un instalador <https://github.com/skydive241/Regshot-Advanced>
* [Best Malware Analysis Tools List in 2023 - GBHackers](https://gbhackers.com/malware-analysis-tools/)

**Creación de Archivos Maliciosos**

Herramientas de creación de archivos maliciosos:

* Metasploit Framework: es una herramienta de pruebas de penetración que se puede utilizar para crear archivos maliciosos para explotar vulnerabilidades en el software. El repositorio oficial se encuentra en [**https://github.com/rapid7/metasploit-framework**](https://github.com/rapid7/metasploit-framework).
* Social-Engineer Toolkit (SET): es una herramienta de ingeniería social que puede usarse para crear archivos maliciosos, como documentos de Microsoft Office o PDF, que incluyen payloads para explotar vulnerabilidades o ejecutar comandos en el sistema objetivo. SET también proporciona plantillas predefinidas para crear correos electrónicos de phishing y páginas web maliciosas. El repositorio oficial se encuentra en [**https://github.com/trustedsec/social-engineer-toolkit**](https://github.com/trustedsec/social-engineer-toolkit).
* PowerShell Empire: es una herramienta de post-explotación que se puede utilizar para crear payloads maliciosos para ser entregados a través de archivos maliciosos. Es compatible con Windows, Linux y macOS y ofrece una amplia gama de funciones, como persistencia, escalada de privilegios y exfiltración de datos. El repositorio oficial se encuentra en [**https://github.com/PowerShellEmpire/Empire**](https://github.com/PowerShellEmpire/Empire).
* Office Exploit Builder: es una herramienta que se utiliza para crear archivos de Microsoft Office maliciosos que contienen exploits de día cero. Ofrece una interfaz gráfica de usuario fácil de usar y permite a los usuarios personalizar las opciones de payload y la forma en que se entrega el archivo. El repositorio oficial no está disponible ya que se trata de una herramienta comercial.
* Veil-Evasion: es una herramienta que permite a los usuarios crear payloads maliciosos que evaden la detección de antivirus. Puede utilizarse para crear archivos maliciosos en diferentes formatos, como documentos de Microsoft Office, archivos PDF y archivos ejecutables. El repositorio oficial se encuentra en [**https://github.com/Veil-Framework/Veil**](https://github.com/Veil-Framework/Veil).
* Phantom Evasion: Esta es una herramienta gratuita de creación de malware que permite a los usuarios crear troyanos personalizados y otras cargas útiles maliciosas. Incluye opciones para ofuscar el código, evitar la detección de antivirus y generar diferentes formatos de archivos maliciosos, como archivos .exe y documentos de Microsoft Office. El repositorio oficial se encuentra en [**https://github.com/oddcod3/Phantom-Evasion**](https://github.com/oddcod3/Phantom-Evasion).
* PDFTools: Es una herramienta gratuita y de código abierto que permite la creación de archivos PDF maliciosos. Permite insertar scripts maliciosos en los archivos PDF, los cuales pueden ser utilizados para ejecutar comandos en el sistema objetivo. [**https://github.com/galkan/ptftools**](https://github.com/galkan/ptftools)
* Unicorn:herramienta que permite la creación de payloads para ser entregados a través de archivos maliciosos y que evita la detección de antivirus. [**https://github.com/trustedsec/unicorn/**](https://github.com/trustedsec/unicorn/)
* APKTool:herramienta de ingeniería inversa para aplicaciones Android que se puede utilizar para manipular y crear aplicaciones maliciosas. [**https://github.com/iBotPeaches/Apktool/**](https://github.com/iBotPeaches/Apktool/)
* Jupyter Notebook: herramienta de análisis de datos que se puede utilizar para crear malware para el aprendizaje automático y la inteligencia artificial. [**https://github.com/jupyter/notebook/**](https://github.com/jupyter/notebook/)
* <https://pa.linkedin.com/posts/cristivlad_github-jonaslejonmalicious-pdf-generate-activity-7026575045871239169-RKFK>
* [jonaslejon/malicious-pdf: 💀 Generate a bunch of malicious pdf files with phone-home functionality. Can be used with Burp Collaborator or Interact.sh (github.com)](https://github.com/jonaslejon/malicious-pdf)
* Ataques de día cero: También se pueden utilizar técnicas de investigación para identificar y explotar nuevas vulnerabilidades en software de terceros. Por ejemplo, se pueden utilizar herramientas de fuzzing para enviar grandes cantidades de entradas inesperadas a una aplicación y ver cómo reacciona. Si se encuentra una vulnerabilidad, se puede desarrollar un archivo malicioso que la explote

**Pentesting en Aplicaciones Móviles**

Herramientas de pentesting en dispositivos móviles:

* Drozer: es una herramienta de pruebas de penetración para aplicaciones móviles Android. Permite explorar y explotar vulnerabilidades en aplicaciones móviles Android y es muy útil para la realización de pruebas de penetración móviles. Repositorio: <https://github.com/FSecureLABS/drozer>
* Drodijack: Este troyano para Android es uno de los más completos. Con él vamos a poder tener acceso a remoto a todo el dispositivo infectado, desde la agenda, las llamadas y los SMS hasta el micrófono y las cámaras del smartphone <https://github.com/Pericena/Droidjack>
* Fridump: <https://github.com/Nightbringer21/fridump> - un script que permite la extracción de memoria de aplicaciones en dispositivos Android utilizando Frida.
* AndroBugs\_Framework: <https://github.com/AndroBugs/AndroBugs_Framework> - un script que utiliza diversas herramientas para realizar análisis de seguridad en aplicaciones Android.
* ADB-Toolkit: <https://github.com/ASHWIN990/ADB-Toolkit> - un conjunto de scripts que automatiza varias tareas relacionadas con el uso de ADB (Android Debug Bridge) en dispositivos Android.
* APK-Downloader: <https://github.com/ndossougbe/apk-downloader> - un script que permite la descarga de aplicaciones de Google Play Store sin la necesidad de una cuenta de Google.
* dex2jar: <https://github.com/pxb1988/dex2jar> - un script que convierte archivos de Android DEX en archivos de formato JAR.
* Drozer: <https://github.com/FSecureLABS/drozer> - un framework de seguridad para Android que permite la realización de pruebas de penetración en aplicaciones móviles.
* apktool: <https://github.com/iBotPeaches/Apktool> - un script que permite la ingeniería inversa de aplicaciones Android para la obtención de recursos y código fuente.
* Genymotion-ARM-Translation: <https://github.com/m9rco/Genymotion_ARM_Translation> - un script que permite la ejecución de aplicaciones ARM en la plataforma de emulación de Android Genymotion.
* Android-SSL-Trust-Killer: <https://github.com/iSECPartners/android-ssl-bypass> - un script que deshabilita la validación SSL en aplicaciones Android para la realización de pruebas de penetración.
* Ssl-kill-switch2: <https://github.com/nabla-c0d3/ssl-kill-switch2> - un script que permite la desactivación de la validación SSL en aplicaciones iOS para la realización de pruebas de penetración.
* Mobile-Security-Framework-MobSF: <https://github.com/MobSF/Mobile-Security-Framework-MobSF> - un framework de seguridad móvil para iOS y Android que permite el análisis estático y dinámico de aplicaciones móviles.
* Needle: <https://github.com/mwrlabs/needle> - un framework de pruebas de penetración en aplicaciones móviles para iOS que permite la interacción con la aplicación a través de una consola.
* iNalyzer: <https://github.com/iSECPartners/iNalyzer> - una herramienta de análisis de seguridad para iOS que permite la extracción de información y recursos de aplicaciones móviles.
* Apk.sh: Facilita la ingeniería inversa de las aplicaciones de Android, automatizando algunas tareas repetitivas como extraer, decodificar, reconstruir y parchear un APK <https://github.com/ax/apk.sh>
* Objection: <https://github.com/sensepost/objection> - una herramienta de pruebas de penetración para aplicaciones móviles iOS y Android que permite la interacción con la aplicación a través de una consola.
* AppMon: <https://github.com/dpnishant/appmon> - una herramienta de análisis de seguridad para aplicaciones móviles Android que permite la extracción de información y recursos de la aplicación.
* AppUse: <https://github.com/appuse/appuse> - una plataforma de emulación para pruebas de penetración en aplicaciones móviles Android.
* APKiD: <https://github.com/rednaga/APKiD> - una herramienta que realiza análisis estático de aplicaciones Android para la identificación de componentes y bibliotecas utilizadas en la aplicación.
* Bypass: <https://github.com/freedomofdevelopers/bypass> - una herramienta que permite la evasión de la seguridad de aplicaciones iOS para la realización de pruebas de penetración.
* SSLyze: <https://github.com/nabla-c0d3/sslyze> - una herramienta de análisis de seguridad de red que permite la identificación de vulnerabilidades SSL/TLS en aplicaciones móviles.
* EvilAP\_Defender: <https://github.com/PabloMansanet/EvilAP_Defender> - una herramienta de detección de Evil Access Points (APs) que pueden ser utilizados para interceptar datos de dispositivos móviles.
* Hopper: <https://www.hopperapp.com/> - una herramienta de ingeniería inversa para iOS y Android que permite la descompilación y análisis de aplicaciones móviles.
* Burp Suite Mobile Assistant: <https://portswigger.net/burp/documentation/desktop/tools/mobile-assistant> - una herramienta que permite la intercepción y manipulación de tráfico HTTP/S entre aplicaciones móviles y servidores.
* DroidBox: <https://github.com/pjlantz/droidbox> - una herramienta de análisis dinámico para aplicaciones Android que permite el seguimiento de comportamiento y la identificación de vulnerabilidades.
* Xposed Framework: <https://github.com/rovo89/Xposed> - un framework de modificación de Android que permite la inyección de código en aplicaciones móviles.
* Androguard: <https://github.com/androguard/androguard> - una herramienta de análisis estático para aplicaciones Android que permite la extracción de información y recursos.
* Cydia Impactor: <https://cydiaimpactor.com/> - una herramienta que permite la instalación de aplicaciones IPA en dispositivos iOS sin necesidad de una cuenta de desarrollador de Apple.
* Metasploit Framework: un framework de pruebas de penetración que cuenta con un amplio conjunto de módulos para realizar pruebas de penetración en sistemas y aplicaciones, incluyendo aplicaciones móviles. Repositorio: <https://github.com/rapid7/metasploit-framework>
* AndroRAT: una herramienta de acceso remoto para dispositivos Android que permite el control total del dispositivo y la posibilidad de inyectar código malicioso en aplicaciones. Repositorio: <https://github.com/wszf/AndroRAT>
* Evil-Droid: una herramienta que permite la creación de aplicaciones maliciosas para dispositivos Android con la capacidad de inyectar código malicioso y realizar acciones malintencionadas. Repositorio: <https://github.com/M4sc3r4n0/Evil-Droid>
* TheFatRat: una herramienta que permite la creación de backdoors y payloads para dispositivos Android, con la capacidad de ejecutar código malicioso y tomar el control total del dispositivo. Repositorio: <https://github.com/Screetsec/TheFatRat>
* Apktool: una herramienta de ingeniería inversa que permite la decompilación y desensamblado de aplicaciones Android para la modificación y creación de versiones maliciosas. Repositorio: <https://github.com/iBotPeaches/Apktool>
* Frida: un framework de inyección de código que permite la modificación y análisis de aplicaciones móviles en tiempo de ejecución, tanto en Android como en iOS. Repositorio: <https://github.com/frida/frida>
* Xposed Framework: un framework de inyección de código para dispositivos Android que permite la modificación del sistema y aplicaciones, incluyendo la inyección de código malicioso. Repositorio: <https://github.com/rovo89/Xposed>
* Objection: una herramienta de pruebas de penetración para aplicaciones móviles que permite la interacción con la aplicación a través de una consola, incluyendo la inyección de código malicioso. Repositorio: <https://github.com/sensepost/objection>
* Appium: una herramienta de automatización de pruebas para aplicaciones móviles que permite la inyección de código malicioso en las pruebas automatizadas. Repositorio: <https://github.com/appium/appium>
* Inspeckage: una herramienta que permite realizar análisis dinámicos de aplicaciones Android, inyectando código malicioso en tiempo de ejecución y monitorizando los intentos de comunicación de la aplicación. Repositorio: <https://github.com/ac-pm/Inspeckage>
* Pen-Andro: Script para automatizar la instalación de aplicaciones, frida server y mover el certificado Burpsuite a la carpeta raíz <https://github.com/raoshaab/Pen-Andro>
* Xposed Framework: un framework de modificación de aplicaciones Android que permite la inyección de código malicioso en la aplicación y la modificación de su comportamiento en tiempo de ejecución. Repositorio: <https://github.com/rovo89/Xposed>
* Cain & Abel: [https://github.com/xenomuta/cain](https://github.com/xenomuta/cain%20) - una herramienta de recuperación de contraseñas que también puede utilizarse para la explotación de dispositivos móviles a través de ataques de fuerza bruta.

**Extracción de Metadatos**

Herramientas de extracción de metadatos:

* FOCA: Herramienta para encontrar metadatos e información oculta en los documentos <https://github.com/ElevenPaths/FOCA>
* Exiftool: una herramienta de línea de comandos escrita en Perl que permite leer y escribir metadatos en archivos de diferentes formatos, incluyendo imágenes, archivos de audio y documentos. Repositorio: <https://github.com/exiftool/exiftool>
* Exifread: una biblioteca de Python que permite leer y analizar metadatos en imágenes. Repositorio: <https://github.com/ianare/exif-py>
* Exiv2: una biblioteca de C++ que permite leer y escribir metadatos en imágenes y otros archivos. Repositorio: <https://github.com/Exiv2/exiv2>
* Metadata-Extractor: una biblioteca de Java que permite leer metadatos en diferentes tipos de archivos, incluyendo imágenes, archivos de audio y documentos. Repositorio: <https://github.com/drewnoakes/metadata-extractor>
* ImageMagick: una herramienta de línea de comandos escrita en C que permite manipular imágenes de diferentes formatos y extraer información de metadatos. Repositorio: <https://github.com/ImageMagick/ImageMagick>
* Matroska: una biblioteca de C++ que permite leer y escribir metadatos en archivos de video y audio en formato Matroska. Repositorio: <https://github.com/Matroska-Org/libmatroska>
* FFmpeg: una herramienta de línea de comandos escrita en C que permite manipular archivos de video y audio de diferentes formatos y extraer información de metadatos. Repositorio: <https://github.com/FFmpeg/FFmpeg>
* PyExifTool: una biblioteca de Python que permite leer y escribir metadatos en archivos de diferentes formatos, incluyendo imágenes, archivos de audio y documentos. Repositorio: <https://github.com/smarnach/pyexiftool>
* PDFMiner: una biblioteca de Python que permite extraer texto y metadatos de archivos PDF. Repositorio: <https://github.com/pdfminer/pdfminer.six>
* LibTiff: una biblioteca de C que permite leer y escribir metadatos en imágenes en formato TIFF. Repositorio: <https://gitlab.com/libtiff/libtiff>

**Extracción de Datos Sensibles de Repositorios de GitHub**

Herramientas de extracción de datos de repositorios GitHub:

* GitDumper: una herramienta creada por @arthaud toma un repositorio de Git público y descarga todo su historial, incluyendo los archivos, historial de cambios, contraseñas, tokens, entre otros. Repositorio: <https://github.com/arthaud/git-dumper>
* Gitleaks: una herramienta creada por @zricethezav que realiza un escaneo de repositorios de Git y busca datos confidenciales como contraseñas, tokens, claves SSH y más. Repositorio: <https://github.com/zricethezav/gitleaks>
* TruffleHog: una herramienta creada por @dxa4481 que busca de forma recursiva en el historial de Git para encontrar contraseñas y otros datos confidenciales. Repositorio: <https://github.com/dxa4481/truffleHog>
* Gitrob: una herramienta creada por @michenriksen que escanea repositorios de Git públicos y encuentra información confidencial, como tokens, claves SSH, nombres de usuarios y correos electrónicos. Repositorio: <https://github.com/michenriksen/gitrob>
* DumpsterDiver: una herramienta creada por @securitywithoutborders que busca en los repositorios de Git información confidencial, como contraseñas, claves SSH, tokens y nombres de usuarios. Repositorio: <https://github.com/securitywithoutborders/dumpsterdiver>

**Repositorios de Interés**

* [swisskyrepo (Swissky) (github.com)](https://github.com/swisskyrepo)
* [Welcome to CSbyGB's Pentips - CSbyGB - Pentips (gitbook.io)](https://csbygb.gitbook.io/pentips/cs-by-gb-pentips/readme)
* [nemesida-waf/waf-bypass: Check your WAF before an attacker does this one (github.com)](https://github.com/nemesida-waf/waf-bypass)
* [100 Best Free Red Team Tools in 2023 - Cyber Security News](https://cybersecuritynews.com/red-team-tools/)
* [10 Best Penetration Testing Phases & Life cycle - 2023 Guide (cybersecuritynews.com)](https://cybersecuritynews.com/penetration-testing-phases/)
* [S3cur3Th1sSh1t (S3cur3Th1sSh1t) / Repositories (github.com)](https://github.com/S3cur3Th1sSh1t?tab=repositories)
* [Shell Code Injector with AES Encryption - EDR Bypass – San3ncrypt3d Inc. – Making cybersecurity a habit & Privacy a Goal](https://san3ncrypt3d.com/2022/03/24/AESInj/)
* [Penetration testing reports: A powerful template and guide (hackthebox.com)](https://www.hackthebox.com/blog/penetration-testing-reports-template-and-guide)
* [ihebski/A-Red-Teamer-diaries: RedTeam/Pentest notes and experiments tested on several infrastructures related to professional engagements. (github.com)](https://github.com/ihebski/A-Red-Teamer-diaries)
* [seeu-inspace/easyg: Here I gather all the resources about hacking that I find interesting (github.com)](https://github.com/seeu-inspace/easyg)
* [1N3 (1N3) / Repositories (github.com)](https://github.com/1N3?tab=repositories)
* [edoardottt (vrenzolaverace) (github.com)](https://github.com/edoardottt)
* [t3l3machus (t3l3machus) / Repositories (github.com)](https://github.com/t3l3machus?tab=repositories)
* [Man In The Middle con Ettercap para HTTP/HTTPS – Tira que libras …](https://blog.tiraquelibras.com/?p=444)
* [gentilkiwi (Benjamin DELPY) (github.com)](https://github.com/gentilkiwi)
* Hacktronian: Pentesting tools [thehackingsage/hacktronian: Tools for Pentesting (github.com)](https://github.com/thehackingsage/hacktronian)
* [jivoi (EK\_) (github.com)](https://github.com/jivoi)
* [wwong99 (Valimar) (github.com)](https://github.com/wwong99)
* Documento muy similar a este. [S3cur3Th1sSh1t/Pentest-Tools (github.com)](https://github.com/S3cur3Th1sSh1t/Pentest-Tools)
* [CyberForce (github.com)](https://github.com/post-cyberlabs)
* [CSbyGB/pentips: CSbyGB PenTips Gitbook (github.com)](https://github.com/CSbyGB/pentips)
* [CSbyGB (C.S. by G.B.) (github.com)](https://github.com/CSbyGB)
* [galkan (Gokhan ALKAN) (github.com)](https://github.com/galkan)
* [GTFOBins](https://gtfobins.github.io/)
* [Best Malware Analysis Tools List in 2023 - GBHackers](https://gbhackers.com/malware-analysis-tools/)
* [10 Best Cyber Attack Simulation Tools For Organization Security 2022 (cybersecuritynews.com)](https://cybersecuritynews.com/cyber-attack-simulation-tools/)
* Documento similar a este. [100 Best Free Red Team Tools in 2023 - Cyber Security News (ampproject.org)](https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/free-red-teaming-tools/?amp)
* [Black-box Penetration Testing - How To Perform External in Organization (ampproject.org)](https://gbhackers-com.cdn.ampproject.org/c/s/gbhackers.com/external-black-box-penetration-testing/amp/)
* [10 Best Free Forensic Investigation Tools 2022 - Cyber Security Tools (ampproject.org)](https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/free-forensic-investigation-tools/?amp)
* [10 Best Free Web Application Pentesting Tools 2022 (cybersecuritynews.com)](https://cybersecuritynews.com/web-application-pentesting-tools/?amp)
* [jhftss (Mickey Jin) (github.com)](https://github.com/jhftss)
* [s0md3v (Somdev Sangwan) (github.com)](https://github.com/s0md3v)
* [MazX0p (xMohamed) (github.com)](https://github.com/MazX0p)
* [(5) Publicación | LinkedIn](https://www.linkedin.com/posts/cristivlad_github-jonaslejonmalicious-pdf-generate-activity-7026575045871239169-RKFK/?originalSubdomain=pa)
* [Hackplayers (github.com)](https://github.com/Hackplayers)
* [MEGA](https://mega.nz/folder/DMxkyajI#-qgMzkrmoFBBsJ5dZxGrvA)
* [The Ultimate Google Dorking Cheat Sheet - 2023 (usersearch.org)](https://usersearch.org/updates/2023/02/05/the-ultimate-google-dorking-cheatsheet-2023/?amp=1)
* [Google Hacking Database (GHDB) - Google Dorks, OSINT, Recon (exploit-db.com)](https://www.exploit-db.com/google-hacking-database)
* [Drew-Alleman (Drew Alleman) (github.com)](https://github.com/Drew-Alleman)
* [kurogai (kurogai) / Repositories (github.com)](https://github.com/kurogai?tab=repositories)
* <https://github.com/xforcered/BokuLoader>
* [X-Force Red (github.com)](https://github.com/xforcered)
* [Daniel Kelley: Top 30 Cybersecurity Posts Swipe File (notion.site)](https://gold-marten-204.notion.site/2d292e0b941146ef858a125bf1cb0eb3?v=f04ea483a23b4119ad85592c6e8e961b)
* [ShadowVMX (ShadowVMX) / Repositories (github.com)](https://github.com/ShadowVMX?tab=repositories)
* [PracticalCyberSecurityResources/README.md at main · brcyrr/PracticalCyberSecurityResources (github.com)](https://github.com/brcyrr/PracticalCyberSecurityResources/blob/main/README.md)
* Documento similar a este. [A-poc/RedTeam-Tools: Tools and Techniques for Red Team / Penetration Testing (github.com)](https://github.com/A-poc/RedTeam-Tools)
* [A-poc (github.com)](https://github.com/A-poc)
* [Offensive OSINT | OSINT researcher doing cyber security art brut | Patreon](https://www.patreon.com/offensiveosint)
* [Most Important Network Penetration Testing Checklist - GBHackers - Latest Cyber Security News | Hacker News](https://gbhackers.com/network-penetration-testing-checklist-examples/amp/)
* [Tools | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/)
* [100 Best Ethical Hacking Tools - 2023 (New List) (gbhackers.com)](https://gbhackers.com/hacking-tools-list/amp/)
* [raoshaab (Devender) (github.com)](https://github.com/raoshaab?tab=repositories)
* [Active Directory Checklist - Attack & Defense Cheatsheet (cybersecuritynews.com)](https://cybersecuritynews.com/active-directory-checklist/)
* [lefayjey (github.com)](https://github.com/lefayjey)
* [50 Free Cyber Threat Intelligence Tools 2023 - GBHackers](https://gbhackers.com/cyber-threat-intelligence-tools/)
* [10 Best Free Forensic Investigation Tools 2022 - Cyber Security Tools (cybersecuritynews.com)](https://cybersecuritynews.com/free-forensic-investigation-tools/)
* [10 Best Free Web Application Pentesting Tools 2022 (cybersecuritynews.com)](https://cybersecuritynews.com/web-application-pentesting-tools/)