## Document of Consultations and Tools for Pentesting, OSINT and Hacking

## Phases of Pentesting

The pentesting process consists of the following phases:

### 1. Recognition

The objective of this phase is to obtain information about the objective of pentesting. Data is collected to better understand the target and used to identify potential vulnerabilities. Reconnaissance includes techniques such as searching for information on the Internet, scanning ports, and enumerating services.

#### Popular tools:

* Nmap: Network port scanner. (<https://nmap.org/>)
* Smap: A direct replacement for Nmap powered by shodan.io<https://github.com/s0md3v/Smap>
* Recon-ng: Information collection framework. (<https://github.com/lanmaster53/recon-ng>)
* Shodan: Search engine for devices connected to the internet. (<https://www.shodan.io/>)
* theHarvester: Tool for collecting information from email, subdomains and IP addresses. (<https://github.com/laramies/theHarvester>)
* Maltego: Open source intelligence platform for the collection and analysis of information. (<https://www.maltego.com/>)
* SpiderFoot: Open source intelligence tool for collecting and analyzing information. (<https://www.spiderfoot.net/>)
* Shodan: Search engine for Internet-connected devices, including servers, routers, cameras, and other IoT devices. (<https://www.shodan.io/>)
* Censys: Security search engine that allows you to search for information from devices connected to the Internet, such as web servers, IoT devices, etc. (<https://censys.io/>)
* EyeWitness: Open source tool that captures screenshots of websites and stores them in a file for later analysis. (<https://github.com/FortyNorthSecurity/EyeWitness>)
* EasyG: Script I use to automate some information gathering tasks for my easyg/easyg.rb at [main · seeu-inspace/easyg (github.com](https://github.com/seeu-inspace/easyg/blob/main/easyg.rb)) hacking process.
* Gh0st: [Gh0st3xp101t/Gh0st automatic recognition tool (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**: A subdomain enumeration tool written in Python that uses various sources to find subdomains associated with a specific domain.
* Repository: <https://github.com/nsonaniya2010/SubDomainizer>
* **NmapAutomator**: A port scanning automation script written in Bash that uses Nmap to perform port scans and generate reports.
* Repository: <https://github.com/21y4d/nmapAutomator>
* **DNSRecon**: A DNS enumeration tool written in Python that uses different techniques to find DNS records and associated subdomains.
* Repository: <https://github.com/darkoperator/dnsrecon>
* **Photon**: A website information extraction tool written in Python that searches for sensitive information such as emails, usernames, files, and subdomains.
* Repository: <https://github.com/s0md3v/Photon>
* **Sn1per**: A threat intelligence and network awareness tool written in Bash that uses various techniques to gather information about specific targets.
* Repository: <https://github.com/1N3/Sn1per>
* **Sherlock**: A social media profile search tool written in Python that uses usernames to search for social media profiles.
* Repository: <https://github.com/sherlock-project/sherlock>
* **Fierce**: A DNS enumeration tool written in Perl that uses different techniques to find DNS records and associated subdomains.
* Repository: <https://github.com/mschwager/fierce>
* **Jigsaw**: An organization information gathering tool written in Python that uses different sources to find information about the organization, such as email addresses and domain names.
* Repository: <https://github.com/yassineaboukir/jigsaw>
* **Sublist3r**: A subdomain enumeration tool written in Python that uses different sources to find subdomains associated with a specific domain.
* Repository: <https://github.com/aboul3la/Sublist3r>
* Katana: Google Dorks Hacking <https://github.com/projectdiscovery/katana>

### 2. Vulnerability analysis

This phase analyzes the vulnerabilities found during the recognition phase. The results of the vulnerability analysis are used to plan and execute attacks.

#### Popular tools:

* Nessus: Vulnerability scanning tool. (<https://www.tenable.com/products/nessus>)
* OpenVAS: Vulnerability management system. (<https://www.openvas.org/>)
* Nikto: Web vulnerability scanner. (<https://cirt.net/Nikto2>)
* Lynis: Linux system security audit tool. (<https://cisofy.com/lynis/>)
* OWASP ZAP: Web application security analysis tool. (<https://www.zaproxy.org/>
* Metasploit Framework: Exploitation framework that also includes a vulnerability database. (<https://www.metasploit.com/>)
* Vega: Open source vulnerability scanner that focuses on web application security and detection of common vulnerabilities. (<https://subgraph.com/vega/>)
* OpenSCAP: Open source toolset that provides a platform for implementing security policies and assessing system security. (<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: A high-speed port scanning tool written in C that uses multiple threads to perform port scans in seconds. Repository: <https://github.com/robertdavidgraham/masscan>

### 3. Exploitation

In this phase, an attempt is made to exploit the vulnerabilities found in the previous phase. The goal is to gain access to the system or application.

#### Popular tools:

* Metasploit: Exploitation framework. (<https://www.metasploit.com/>)
* Burp Suite: Penetration testing tool for web applications. (<https://portswigger.net/burp>)
* SQLMap: Automated SQL injection tool. (<http://sqlmap.org/>)
* BeEF: Browser-based exploit framework for web application attacks. (<https://beefproject.com/>)
* SQLMate: Automated SQL injection tool and database enumeration. (<https://github.com/UltimateHackers/sqlmate>)
* Exploit Database: Collection of open source public exploits for a wide variety of software and systems. (<https://www.exploit-db.com/>)
* Mangrove: Es a tool that manipulates aspects of compiled executables (.exe or DLLs) to avoid detection of EDRs<https://github.com/optiv/Mangle>
* SET (Social-Engineer Toolkit): Social engineering framework that includes phishing, reverse engineering, and vulnerability exploitation modules. (<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>: A tool that allows the injection of malicious updates into vulnerable applications, in order to compromise the user's system.
* Pycrypter: Python Based Crypter That Can Bypass Any Kinds Of Antivirus Products<https://github.com/machine1337/pycrypt>
* BloodHound: a tool for analyzing and visualizing networks on Windows systems written in JavaScript and Python that allows you to visualize and analyze the structure of a network, as well as the relationships between the different nodes. Repository: <https://github.com/BloodHoundAD/BloodHound>
* Armitage: is a graphical user interface tool for Metasploit Framework, which allows you to visualize and explore network targets and launch attacks against them. Repository: <https://github.com/rsmudge/armitage>
* linWinPwn: Es a bash script that automates a series of Active Directory enumeration and vulnerability checks<https://github.com/lefayjey/linWinPwn>
* Bettercap: It is a network hijacking tool that allows you to intercept network traffic, perform MITM (man-in-the-middle) attacks and analyze network traffic. Repository: <https://github.com/bettercap/bettercap>
* Freeze: Eis a payload toolkit to avoid EDR using suspended processes, direct syscalls, and alternative execution methods<https://github.com/optiv/Freeze>
* PseudoHash: Password list generator that focuses on keywords mutated by commonly used password creation patterns [https://github.com/t3l3machus/psudohash](https://github.com/t3l3machus/psudohash%20)
* Exploit Finder: <https://sploitus.com/>

### 4. Post-Exploitation

#### Privilege escalation

Once access has been obtained, a way to increase privileges on the system or application is sought. The goal is to gain access to critical information or additional functionality.

##### Popular tools:

* PowerUp: PowerShell module for enumeration and privilege escalation. (<https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc>)
* WinPwnage: UAC bypass, elevation, and persistence methods<https://github.com/rootm0s/WinPwnage>
* JAWS: Privilege escalation tool for Windows systems. (<https://github.com/411Hall/JAWS>)
* Mimikatz: Windows Credential Extraction and Privilege Escalation Tool. (<https://github.com/gentilkiwi/mimikatz>)
* Privilege Escalation Awesome Scripts SUITE (PEASS): Set of scripts and tools for privilege escalation on Windows and Linux systems. (<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite>)
* LinEnum: Open source tool that automates the enumeration of information and the detection of vulnerabilities in Linux systems. (<https://github.com/rebootuser/LinEnum>)
* Windows-Exploit-Suggester: Open source tool that helps in identifying potential Windows vulnerabilities by comparing the version of Windows with a database of known vulnerabilities. (<https://github.com/GDSSecurity/Windows-Exploit-Suggester>)
* Pupy: Open source tool that allows privilege escalation and remote control of Windows, Linux, and OS X systems. (<https://github.com/n1nj4sec/pupy>)
* SudoKiller: Open source tool that looks for privilege escalation vulnerabilities in Linux systems using sudo. (<https://github.com/TH3xACE/SudoKiller>)
* [swisskyrepo](https://github.com/swisskyrepo)/**[PayloadsAllTheThings](https://github.com/swisskyrepo/PayloadsAllTheThings)**: Github repository with Pentest tips in which there are numerous privilege escalation methods on Linux and Windows.
* [Privilege Escalation - CSbyGB - Pentips (gitbook.io): Pentesting notes](https://csbygb.gitbook.io/pentips/windows/privesc), in which in addition to privilege escalations there are notes and tips for all phases of a Pentesting.
* ExploitLeakedHandle : A utility that identifies identifiers in unprivileged processes that may have been inherited from a privileged parent process and attempts to leverage them for local privilege escalation. <https://github.com/0x00Check/ExploitLeakedHandle>
* CrackMapExec: A post-exploitation tool on Windows and Linux systems written in Python that allows you to execute remote commands, escalate privileges and gain persistent access on compromised systems. Repository: <https://github.com/byt3bl33d3r/CrackMapExec>

#### Lateral movement

The lateral movement phase focuses on propagating access to other systems within the compromised network.

* BloodHound: Active Directory path discovery and relationship analysis tool. (<https://github.com/BloodHoundAD/BloodHound>)
* CrackMapExec: Pentesting tool that automates the lateral propagation of exploits in Windows networks and the search for vulnerabilities. (<https://github.com/byt3bl33d3r/CrackMapExec>)
* Metasploit Framework: Metasploit allows lateral propagation using the compromised systems as a pivot. (<https://github.com/rapid7/metasploit-framework>)

#### Data exfiltration

The data exfiltration phase involves extracting information from compromised systems and transferring it outside the compromised network.

* FTP: File transfer protocol that allows users to transfer files between systems. Repository: <https://github.com/madler/ftp>
* HTTPS: Secure Hypertext Transfer Protocol that allows users to securely transfer information over the Internet. Repository: <https://github.com/curl/curl>
* SCP: Secure copy protocol used to securely transfer files between systems. Repository: <https://github.com/openssh/openssh-portable>
* SFTP: Secure file transfer protocol used to securely transfer files between systems. Repository: <https://github.com/libssh2/libssh2>
* Netcat: A network utility that allows users to read and write data to network connections using TCP or UDP. It is a very versatile tool that can be used for covertly transferring files and data. The Netcat repository is located in <https://github.com/diegocr/netcat>.
* Steghide: Steganography tool that allows you to hide files in images and other audio and video files. It is a very useful tool for covert data exfiltration and can be used on both Linux and Windows systems. The Steghide repository is located in <https://github.com/StefanoDeVuono/steghide>.
* Hping: Network tool that allows the creation of custom network packets and the sending of fake network traffic. It is a very useful tool for data exfiltration through covert channels and can be used to evade detection of security systems. The Hping repository is located in <https://github.com/antirez/hping>.
* Powershell Empire: Post-exploit framework that allows attackers to remotely control compromised systems and covertly exfiltrate data. It is a tool widely used in large-scale attacks and can be used on Windows and Linux systems. The Powershell Empire repository is located in <https://github.com/EmpireProject/Empire>.
* Metasploit: Exploitation framework that allows attackers to exploit vulnerabilities in target systems and covertly exfiltrate data. It is a widely used tool in data exfiltration and can be used on Windows and Linux systems. The Metasploit repository is located in <https://github.com/rapid7/metasploit-framework>.
* Cain & Abel: [https://github.com/xenomuta/cain](https://github.com/xenomuta/cain%20) - a password recovery tool.
* Mimikatz - <https://github.com/gentilkiwi/mimikatz> - a tool that allows the extraction of passwords, hashes and other sensitive data from Windows systems.
* Reply - <https://github.com/lgandx/Responder> - a tool that allows the capture of hashes of passwords sent through protocols such as SMB and HTTP.
* PowerSploit - <https://github.com/PowerShellMafia/PowerSploit> - a set of PowerShell modules that allow the extraction of sensitive data from Windows systems, as well as the execution of commands and scripts on the compromised machine.
* Empire - <https://github.com/BC-SECURITY/Empire> - a post-exploit framework for Windows and Linux systems that allows remote command execution, sensitive data extraction and persistence on the compromised system.
* John the Ripper - <https://github.com/openwall/john> - a password cracking tool that allows the extraction of hash passwords and their subsequent decryption.
* LaZagne - <https://github.com/AlessandroZ/LaZagne> - a tool that allows the extraction of passwords from applications and operating systems, including Windows, Linux, macOS and web applications.
* Binwalk - <https://github.com/ReFirmLabs/binwalk> - a tool that allows the extraction of hidden data in binary files, such as firmware from embedded devices.
* Volatility - <https://github.com/volatilityfoundation/volatility> - a tool that allows the extraction of RAM information from compromised systems, including processes, open files and cached passwords.
* Empire - <https://github.com/BC-SECURITY/Empire>: A PowerShell post-exploitation framework that enables remote execution of commands on compromised systems, sensitive data extraction and network pivoting.
* CrackMapExec - <https://github.com/byt3bl33d3r/CrackMapExec>: A tool that allows the execution of commands and the extraction of credentials on Windows systems and Active Directory.
* LaZagne - <https://github.com/AlessandroZ/LaZagne>: A tool that allows the recovery of passwords stored on the system, including web browsers, email clients and others.
* Metasploit Framework - [https://github.com/rapid7/metasploit-framework](https://github.com/rapid7/metasploit-framework%20) - an offensive hacking framework that includes numerous modules and tools for carrying out attacks and post-exploiting systems.
* DumpsterDiver - <https://github.com/securing/DumpsterDiver>: A tool that allows searching for sensitive data in deleted files and folders on Unix and Windows systems.
* EvilGrade - <https://github.com/infobyte/evilgrade>: A tool that allows the injection of malicious updates into vulnerable applications, in order to compromise the user's system.
* Postenum - <https://github.com/mbad/host-exploit-1>: A tool that automates the enumeration of information and the extraction of sensitive data on Unix systems, in order to facilitate post-exploitation.
* ADRecon: [https://github.com/sense-of-security/ADRecon](https://github.com/sense-of-security/ADRecon%20) - an Active Directory enumeration and recognition tool that can extract valuable information, such as plaintext passwords and password hashes.
* Steganography: Technique used to hide information within images, audio or video files for later retrieval. Popular tools include OpenStego, Steghide and OutGuess.

### 5. Maintenance of access

Once privileges have been accessed and scaled, a way is sought to maintain long-term access. The goal is to maintain access and control the system or application.

#### Popular tools:

* Netcat: Network utility for file transfer and remote control of a system. (<http://netcat.sourceforge.net/>)
* Meterpreter: Metasploit payload used to maintain access and control. (<https://www.offensive-security.com/metasploit-unle>ashed/meterpreter-payloads/)
* Covenant: Post-exploitation framework for maintaining access and controlling Windows systems. (<https://github.com/cobbr/Covenant>)
* Merlin: Es a cross-platform post-exploit HTTP/2 command and control agent written in 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: Post-exploitation tool for remote control of Windows, Linux and macOS systems. (<https://github.com/n1nj4sec/pupy>)
* PowerSploit: Open source toolset that focuses on performing attacks and post-exploitation on Windows systems. (<https://github.com/PowerShellMafia/PowerSploit>)
* Empire: Post-exploitation framework that allows remote control of systems and execution of commands on Windows and Linux systems. (<https://github.com/BC-SECURITY/Empire>)
* Socat: Open source networking tool that allows the creation of secure and flexible network connections. (<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>

Free options to create a remote server and redirect connections through it. Here are some of these options:

* Ngrok: It is a free tool that allows you to create secure tunnels from a public address to a local server. In this way, connections can be securely routed through ngrok and accessed from anywhere. Ngrok is available for Windows, Mac and Linux. To use ngrok, you just need to download it from their website, register and follow the instructions.
* Serveo: It is another free tool that allows you to create secure tunnels and redirect connections to a local server. Like ngrok, serveo is easy to use and available for Windows, Mac, and Linux. To use serveo, you just need to open an SSH connection and redirect traffic through it.
* LocalXpose: It is a free tool that allows you to create secure tunnels and redirect traffic to a local server. LocalXpose is easy to use and available for Windows, Mac, and Linux. To use LocalXpose, you just need to download it from their website, register and follow the instructions.
* Pagekite: It is another free tool that allows you to create secure tunnels and redirect connections to a local server. Pagekite is easy to use and available for Windows, Mac, and Linux. To use Pagekite, you just need to download it from their website, register and follow the instructions.

Some options to create a server for free are:

* Heroku: It is a web hosting service that allows users to host web applications for free. Users can create a free account on Heroku, upload their app, and run it on a free server.
* Amazon Web Services (AWS) Free Tier: AWS offers a free tier of service that allows users to build and run applications in the cloud for free. The free tier includes services such as Amazon EC2 (virtual server), Amazon S3 (cloud storage), Amazon RDS (cloud database), and more.
* Google Cloud Platform (GCP) Free Tier: GCP also offers a free tier of service that allows users to build and run cloud applications for free. The free tier includes services such as Google Compute Engine (virtual server), Google Cloud Storage (cloud storage), Google Cloud SQL (cloud database), among others.
* DigitalOcean: It is a web hosting service that allows users to create virtual servers (droplets) in the cloud easily and quickly. DigitalOcean offers a free plan that includes a server with 1GB of RAM, 25GB of SSD storage, and 1TB of data transfer.

## Footprint Coverage

During this phase, attempts are made to cover the tracks and erase any evidence of the attack.

* CCleaner: Closed-source cleanup utility that removes temporary files, logs, and other unnecessary data from the system. (<https://www.ccleaner.com/>)
* Shred: Open source command line tool that overwrites files with random data to securely erase them. (<https://www.gnu.org/software/coreutils/manual/html_node/shred-invocation.html>)
* BleachBit: Open source cleanup utility that removes temporary files, logs, and other unnecessary data from the system. (<https://www.bleachbit.org/>)
* Timestomp: Tool that allows you to modify the timestamps of the files to hide the date and time of creation, modification and access.
* Metasploit Meterpreter: Metasploit module that allows you to delete files and clean the registry of the compromised system.
* Syslog-ng: is an event logging tool that allows filtering, classifying, and routing logs. It can be used to clear logs or to send them to a remote server.
* Logrotate: is a tool that allows you to rotate, compress and delete old log files. It can be configured to delete records after a certain period of time or size.
* Modification of log files: You can manually modify the logs to erase any evidence of the attack.

## Anonymity

Being anonymous online and during an attack is critical to protecting your identity and avoiding being tracked by authorities. Some ways to achieve anonymity are:

* Virtual Private Networks (VPNs): VPNs encrypt internet traffic, preventing internet service providers (ISPs) or any other entity from intercepting information and tracing its origin.
* Anonymous browsers: Browsers such as Tor, I2P, and Freenet use onion routing and cryptography to ensure user privacy and hide their IP address.
* Use of proxies: Proxies act as intermediaries between the user and the server, which hides the user's IP address and allows you to browse anonymously, tor, Privoxy and Squid.
* Data obfuscation: Data obfuscation can help prevent pattern detection and hide information. Data obfuscation tools, such as Obfsproxy and Shadowsocks, can help hide information and activities online.
* Tails: It is an operating system that runs from a USB or DVD, designed to preserve privacy and anonymity. All internet connections are routed through the TOR network, and system memory is cleared when you turn it off.

## Tools for Web Application Pentesting

In addition to the tools mentioned above, here are some of the best and most popular tools for web application pentesting:

* Burp Suite: Web application security testing framework that includes a variety of tools, including an interception proxy, vulnerability scanner, and custom attack intruder. (<https://portswigger.net/burp>)
* OWASP ZAP: Open source web application security testing framework that includes a variety of tools, including an interception proxy, vulnerability scanner, and custom attack intruder. (<https://www.zaproxy.org/>)
* Sqlmap: Open source tool that focuses on the detection and exploitation of SQL injection vulnerabilities in web applications. (<http://sqlmap.org/>)
* SstiMap: SSTI Autodiscover Tool with https://github.com/vladko312/SSTImap Interactive Interface
* Web-Scanner v3.0: WEB scanner that aims to get all possible information such as IP, CMS, Users, possible emails, URL performance, Open Ports, Subdirectories. <https://github.com/ShadowVMX/Web-Scanner>
* w3af: Open source tool that focuses on the detection and exploitation of web application vulnerabilities. (<http://w3af.org/>)
* Nikto: Open source scanning tool that focuses on finding common vulnerabilities in web servers and web applications. (<https://cirt.net/Nikto2>)
* Flan: Vulnerability Scanner [cloudflare/flan: A pretty sweet vulnerability scanner (github.com)](https://github.com/cloudflare/flan).
* Vega: Open source scanning tool that focuses on finding vulnerabilities in web applications. (<https://subgraph.com/vega/>)
* Arachni: Open source scanning tool that focuses on finding vulnerabilities in web applications. (<https://www.arachni-scanner.com/>)
* Skipfish: Open source scanning tool that focuses on finding vulnerabilities in web applications. (<https://code.google.com/archive/p/skipfish/>)
* Nmap: Open source scanning tool used to identify hosts and services on a network. It can also be used to find vulnerabilities in scanned systems. (<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**: vulnerability scanning tool in web applications. [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: Plugin-based vulnerability scanner used for massive-scale low-cost error detection [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: A web scanning tool written in Perl that uses different techniques to find vulnerabilities in web applications, such as SQL injection, cross-site scripting (XSS), and local file inclusion (LFI). Repository: <https://github.com/Uniscan/uniscan>
* Wapiti: A web scanning tool written in Python that uses different techniques to find vulnerabilities in web applications, such as SQL injection, XSS, and LFI. Repository: <https://github.com/wapiti-scanner/wapiti>
* CMSmap: A web application scanning tool written in Python that detects the CMS used by a web application and looks for CMS-specific vulnerabilities. Repository: <https://github.com/Dionach/CMSmap>
* Droopescan – A web application scanning tool written in Python that detects the CMS used by a web application and looks for CMS-specific vulnerabilities. Repository: <https://github.com/droope/droopescan>
* Skipfish: A web application scanning tool written in C that uses different techniques to find vulnerabilities in web applications, such as SQL injection, XSS, and LFI. Repository: <https://github.com/spinkham/skipfish>
* ZAP: A web application scanning tool written in Java that can detect and exploit vulnerabilities in web applications, such as SQL, XSS, and LFI injection. Repository: <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: A subdomain enumeration tool written in Go that uses different sources to find subdomains associated with a specific domain. Repository: <https://github.com/OWASP/Amass>
* EyeWitness: A screenshot tool written in Python that takes screenshots of websites and web applications and saves them as images. Repository: <https://github.com/FortyNorthSecurity/EyeWitness>
* Subfinder: A subdomain enumeration tool written in Go that uses different sources to find subdomains associated with a specific domain. Repository: <https://github.com/projectdiscovery/subfinder>
* Aquatone: A web application scanning tool written in Go that performs a port scan and takes screenshots of websites and web applications. Repository: <https://github.com/michenriksen/aquatone>
* Webtech: A web technology recognition tool written in Python that detects technologies used in a web application, such as CMS, frameworks, and libraries. Repository: <https://github.com/ShielderSec/webtech>
* Wappalyzer: A web technology recognition tool written in JavaScript that detects technologies used in a web application, such as CMS, frameworks, and libraries. Repository: <https://github.com/AliasIO/Wappalyzer>
* SpiderFoot: A threat intelligence tool written in Python that collects information about a target using different sources, such as search engines, public databases, and social media. Repository: <https://github.com/smicallef/spiderfoot>
* Dirsearch: A directory and file enumeration tool in a web application written in Python that uses a list of keywords to search for possible paths and files. Repository: <https://github.com/maurosoria/dirsearch>
* Gobuster: A directory and file enumeration tool in a web application written in Go that uses a list of keywords to search for possible paths and files. Repository: <https://github.com/OJ/gobuster>
* wfuzz: A directory and file enumeration tool in a web application written in Python that uses a list of keywords to search for possible paths and files. Repository: <https://github.com/xmendez/wfuzz>
* Parameth: A parameter enumeration tool in a web application written in Python that looks for possible input parameters in a web application. Repository: <https://github.com/maK-/parameth>
* Sublist3r: A subdomain enumeration tool in a web application written in Python that uses different sources to find subdomains associated with a specific domain. Repository:<https://github.com/aboul3la/Sublist3r>
* Shellshock Scanner: is a Bash tool that allows you to search for Shellshock vulnerabilities in web servers. It can be used to find vulnerable servers and launch command injection attacks. Repository: <https://github.com/nccgroup/shocker>
* SQLiv: is a Python tool for exploring SQL injections. It is capable of detecting SQL injections in different types of databases and can be used to launch SQL injection attacks. Repository: <https://github.com/Hadesy2k/sqliv>
* Checklist: [Web Application Penetration Testing Checklist - GBHackers](https://gbhackers.com/web-application-penetration-testing-checklist-a-detailed-cheat-sheet/)
* Repository with many tools: <https://github.com/kurogai/WebHackersWeapons>
* [URL and website scanner - urlscan.io](https://urlscan.io/)

## Trojan Creation Tools

Here are some of the most popular tools for creating Trojans:

* Metasploit Framework: Penetration testing framework that includes a variety of tools, including payload generators and exploits, that can be used to create Trojans. (<https://www.metasploit.com/>)
* Veil-Evasion: Open source tool that allows the generation of Trojans that avoid detection by antivirus systems. (<https://github.com/Veil-Framework/Veil-Evasion>)
* Empire: Open source tool that allows the creation of Trojans that allow remote control of compromised systems. (<https://github.com/BC-SECURITY/Empire>)
* Pupy: Open source tool that allows privilege escalation and remote control of Windows, Linux, and OS X systems. (<https://github.com/n1nj4sec/pupy>)
* Covenant: Open source tool that allows the creation of Trojans that allow remote control of compromised systems. (<https://github.com/cobbr/Covenant>)
* TheFatRat: Open source tool that allows the generation of cross-platform Trojans with various functionalities, such as screenshot, keylogging, webcam capture, among others. (<https://github.com/Screetsec/TheFatRat>)
* Venom: Open source tool that allows the generation of Trojans that avoid detection by antivirus systems, through the injection of payloads into legitimate files. (<https://github.com/r00t-3xp10it/venom>)
* AndroRAT: Open source tool that allows the creation of Trojans for Android devices, which allow remote control of the infected device. (<https://github.com/wszf/androrat>)
* EvilOSX: Open source tool that allows the creation of Trojans for Mac OS X devices, which allow remote control of the infected device. (<https://github.com/Marten4n6/EvilOSX>)
* QuasarRAT: Open source tool that allows the creation of Trojans for Windows systems, which allow remote control of the infected system. (<https://github.com/quasar/QuasarRAT>)
* Empire: Open source tool that allows the creation of Trojans for Windows and Linux systems, which allow remote control of the infected system. It has various features such as screen capture, keylogger, webcam capture, among others. (<https://github.com/BC-SECURITY/Empire>)
* Koadic: Open source tool that allows the creation of Trojans for Windows systems, which allow remote control of the infected system. It has various features such as screen capture, keylogger, webcam capture, among others. (<https://github.com/zerosum0x0/koadic>)
* Gcat: Open source tool that allows the creation of Trojans for Mac OS X and Linux systems, which allow remote control of the infected system. (<https://github.com/byt3bl33d3r/gcat>)
* Metasploit Framework: Open source tool that allows the creation of Trojans and other types of exploits for various platforms, which allow remote control of the infected system. It has a wide variety of functionalities and modules that allow the exploitation of various vulnerabilities. (<https://github.com/rapid7/metasploit-framework>)
* Veil Framework: Open source tool that allows the creation of Trojans and other types of exploits for various platforms, which allow remote control of the infected system. It has several functionalities to evade detection by antivirus systems. (<https://github.com/Veil-Framework/Veil>)

## Social Engineering Tools

Here are some social engineering tools that can be used in penetration testing:

* Mip22: Advanced Pishing tool <https://github.com/makdosx/mip22>
* SET (Social-Engineer Toolkit): Open source tool that allows the automation of various social engineering techniques, such as phishing, social media deception, among others. (<https://github.com/trustedsec/social-engineer-toolkit>)
* BeEF (Browser Exploitation Framework): Open source tool that allows the exploration of vulnerabilities in web browsers through social engineering techniques, such as remote control of web browsers and obtaining information from users. (<https://github.com/beefproject/beef>)
* Evilginx2: Open source tool that allows the creation of malicious proxy servers that allow the obtaining of credentials and other sensitive information through phishing techniques and deception in online authentication. (<https://github.com/kgretzky/evilginx2>)
* Gophish: Open source tool that allows the automation of phishing campaigns, from the creation of emails to the tracking of user interaction with them. (<https://github.com/gophish/gophish>)
* SETOOLKIT: Open source tool that allows the automation of various social engineering techniques, such as phishing, social media hoax, among others. It is an alternative to SET and focuses on phishing via SMS. (<https://github.com/SocialEngineeringTools/SEToolkit>)
* SocialFish: Open source tool that allows the automation of phishing attacks on social networks, with a focus on Facebook, Instagram, Google, among others. (<https://github.com/UndeadSec/SocialFish>)
* PhishLulz: Social engineering tool that allows the creation of emails and personalized phishing pages to trick victims and obtain information from them. (<https://github.com/dylanari/phishlulz>)
* ReelPhish: Social engineering tool that allows the creation of personalized phishing pages to capture information from victims. (<https://github.com/fireeye/ReelPhish>)
* HiddenEye: Social engineering tool that allows the creation of personalized phishing pages to capture information from victims, with a focus on creating fake login pages. (<https://github.com/DarkSecDevelopers/HiddenEye>)
* King Phisher: Open source tool that enables the creation and automation of custom phishing campaigns, including the creation of phishing emails and the simulation of malicious websites. (<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: Pishing Campaign Framework<https://github.com/Optane002/ZPhisher>

## OSINT Tools for Social Networks

Below are some OSINT tools for obtaining information from social networks such as Facebook, Instagram, and Twitter:

* Facebook Graph Search: Facebook search tool that allows advanced searches on the platform, such as searching for publications, photos, videos, among others. (<https://www.facebook.com/about/graphsearch>)
* Maigret: Collect a dossier about a person by username from thousands of sites<https://github.com/soxoj/maigret>
* NetBootCamp: Tool that allows you to search for information on different social networks, such as Facebook, Twitter, LinkedIn, among others. (<https://netbootcamp.org/>)
* Sherlock: Open source tool that allows you to search for information on different social networks, such as Facebook, Instagram, Twitter, LinkedIn, among others. (<https://github.com/sherlock-project/sherlock>)
* StalkScan: Search tool that allows you to search for information on public Facebook profiles, such as publications, photos, videos, among others. (<https://stalkscan.com/>)
* Twint: OSINT tool that allows you to search for information on Twitter, such as searching for publications, tweets, followers, among others. (<https://github.com/twintproject/twint>)
* Instalooter: OSINT tool that allows you to download photos and videos from public Instagram profiles. (<https://github.com/althonos/InstaLooter>)
* Social Mapper: This OSINT tool automates the process of searching and tracking targets on different social networks, including Facebook, Instagram, Twitter, LinkedIn, among others. (<https://github.com/SpiderLabs/social_mapper>)
* FacebookOSINT: This OSINT tool focuses exclusively on searching for Facebook information, and allows you to search by name, email, phone, date of birth, location and other criteria. (<https://github.com/lockfale/FacebookOSINT>)
* InstaInsane: This OSINT tool for Instagram allows the massive download of photos, videos and other content, as well as the search for hashtags and locations. (<https://github.com/thelinuxchoice/instainsane>)
* TweetDeck: This Twitter tool allows you to customize the display of tweets, searches, mentions and hashtags on a single screen, which facilitates the monitoring and analysis of information in real time. (<https://tweetdeck.twitter.com/>)
* GramSpider: This OSINT tool for Instagram allows you to search for users, posts, hashtags and comments, and download photos and videos in bulk. (<https://github.com/Naategh/GramSpider>)
* TweetBeaver: This OSINT tool for Twitter allows you to search for tweets and users based on different criteria, such as keywords, location and date, and export the results in different formats. (<https://github.com/NoxHarmonium/tweetbeaver>)
* Creepy: OSINT tool that allows the collection of information on social networks such as Facebook, Twitter, Instagram, among others. (<https://github.com/ilektrojohn/creepy>)
* FaceDominator: OSINT tool that allows the management and automation of Facebook accounts, as well as the collection of information from public profiles. (<https://facedominator.com/>)
* Instalooter: OSINT tool that allows the download of images and videos from Instagram, as well as the search and collection of information from public profiles. (<https://github.com/althonos/InstaLooter>)
* Tinfoleak: OSINT tool for Twitter that allows the collection of account and tweet information, as well as the generation of detailed reports. (<https://github.com/vaguileradiaz/tinfoleak>)
* FBI (Facebook Information): OSINT's tool that allows investigators to collect information from Facebook profiles, including contact information and recent activity. (<https://github.com/xHak9x/fbi>)
* Instalooter: OSINT tool that allows researchers to download photos, videos and other media from Instagram. (<https://github.com/althonos/InstaLooter>)

## OSINT tools for emails

Here are some OSINT tools that can be used to get information from emails:

* Hunter.io: This OSINT tool allows you to search for email addresses, and provides information about the company, the position of the email owner and other email addresses that may be related to the target. (<https://hunter.io/>)
* The Harvester: This OSINT tool allows you to collect public information from different sources, including emails, subdomains, hosts and IP addresses, using different search engines. (<https://github.com/laramies/theHarvester>)
* Shodan: This OSINT tool allows you to search for devices connected to the Internet, including email servers, routers and other devices that may be related to the target. (<https://www.shodan.io/>)
* Infoga: This OSINT tool automates the search for email information, including verifying their existence, searching for related domains, and enumerating subdomains. (<https://github.com/m4ll0k/Infoga>)
* HaveIBeenPwned: OSINT web service that allows the verification of whether an email account has been compromised in any known security breach. (<https://haveibeenpwned.com/>)
* EmailRep.io: This OSINT tool provides information about an email's reputation, including its likelihood of being spam, its history of abuse, and the existence of related malware. (<https://emailrep.io/>)
* Metagoofil: This OSINT tool allows you to search for information related to an email, including attachments, links and metadata. (<https://github.com/laramies/metagoofil>)
* Maltego: This OSINT tool allows you to collect information about a target using data mining and network visualization techniques. Maltego can also be used to search for email information, including listing subdomains, searching for social media profiles, and identifying other related contacts. (<https://www.maltego.com/>)
* Pipl: This OSINT tool allows you to search for information about people using different search criteria, including email. Pipl may provide information about physical address, social media activity, IP address, and other details about the target. (<https://pipl.com/>)
* Intel Techniques: This OSINT tool provides a wealth of resources and techniques for searching for information online, including tools for searching for email information, identifying social media profiles, searching for phone numbers, and other relevant information. (<https://inteltechniques.com/>)
* SocialCatfish: This OSINT tool allows you to search for information about people using different search criteria, including email. SocialCatfish can provide information about criminal history, property records, social media activity, and other details about the target. (<https://socialcatfish.com/>)
* Sherlock: This OSINT tool allows you to search for social network profiles based on a username or email address. Sherlock can search different social media platforms, including Instagram, Twitter, TikTok, Snapchat, and others. (<https://github.com/sherlock-project/sherlock>)

## Facial Recognition Tools

Here are some facial recognition tools that can be used in a pentesting or security testing context:

* OpenCV: This is an open-source computer vision library that can be used to develop facial recognition applications. OpenCV includes algorithms for detecting faces and recognizing facial patterns, as well as training and adjusting facial recognition models. (<https://opencv.org/>)
* DeepFaceLab: This is an open source tool for deep face learning. DeepFaceLab uses neural networks to perform tasks such as facial recognition, age classification, and face transfer. The tool also features a graphical user interface (GUI) for ease of use. (<https://github.com/iperov/DeepFaceLab>)
* Dlib: This is an open source library for image processing and machine learning. Dlib includes tools for face detection, facial landmarks tracking, and face comparison for facial recognition. (<http://dlib.net/>)
* Face\_recognition: This is an open source library for facial recognition. Face\_recognition uses the DLIB deep learning library to detect and recognize faces in images and videos. The library also features an easy-to-use Python API. (<https://github.com/ageitgey/face_recognition>)
* OpenBR: This is an open-source biometric recognition library that includes tools for face identification and verification, as well as for the identification of other biometric features such as fingerprints and irises. OpenBR can be used on a variety of operating systems, including Windows, Linux, and MacOS. (<http://openbiometrics.org/>)
* FaceNet: Deep learning framework for facial recognition that allows the creation of custom models. (<https://github.com/davidsandberg/facenet>)
* Facial recognition API: Facial recognition API that allows developers to add facial recognition capabilities to their applications. (<https://azure.microsoft.com/en-us/services/cognitive-services/face/>)
* Rekognition: Amazon's facial recognition service that allows developers to add facial recognition capabilities to their applications. (<https://aws.amazon.com/rekognition/>)

## OSINT Tools for Photographs

Here are some OSINT tools that can be used to get information from photographs:

* Google Images: With Google's image search feature, a reverse search of an image can be performed to find other instances of the same image online. This can be useful for finding information about the image, such as its origin or any other information associated with it.
* TinEye: TinEye is a reverse image search tool similar to Google Images. It can help find other places online where the image has been posted and provide information about its origin and use.
* ExifTool: This is a command-line tool that can read and write metadata information to image files. Metadata information may include details such as the location and date the photograph was taken, the camera used to take the picture, and other technical details.
* FotoForensics: This tool allows you to analyze the authenticity of an image by analyzing its metadata and the characteristics of the image. It can also detect if the image has been manipulated or edited in any way.
* Social Catfish: This tool allows you to perform a reverse image search on multiple social media platforms to find user profiles associated with the image.
* Sherlock: This is a tool from OSINT that allows you to search for a username on various social networks and online websites. If an image of the user is provided, the tool can also perform a reverse image lookup to find other online profiles associated with the same image.
* Yandex Images: Yandex Images is an image search engine similar to Google Images, which can help find other instances of an image online and provide information about its origin and use.
* ImageIdentify: This tool uses Google's image recognition technology to identify objects, people, and places in an image, which can provide additional information about the image and its content.
* ImageForensics: ImageForensics is a tool that allows you to analyze an image to detect if it has been manipulated or altered in any way. It can also provide information about the camera used to take the image, the date and location it was taken, and other technical details.
* WolframAlpha: WolframAlpha is a computational knowledge engine that can provide information about an image based on its content. For example, if an image of a famous monument or building is uploaded, WolframAlpha can provide information about its history, architecture, and location.
* PimEyes: PimEyes is a reverse image search tool that focuses on finding images of faces. It can help find online profiles associated with a specific face and provide information about the person.
* StalkScan: StalkScan is a tool that allows you to obtain information from public Facebook profiles using the profile URL. You can provide information about the person, such as their posts, photos, friends, and other online activities.

## Social Media Hacking

Popular tools:

* Social-Engineer Toolkit (SET): It is an open source tool that is used to carry out social engineering attacks. SET can be used to send phishing emails, create fake websites for phishing, and perform other types of social engineering attacks.
* BeEF: It is a penetration testing tool that is used to test the security of web browsers. BeEF allows security testers to perform XSS (Cross-site scripting) attacks and other types of attacks on the victim's browser.
* Burp Suite: It is a penetration testing tool that is used to test the security of web applications. Burp Suite can be used to find vulnerabilities in login pages and other parts of web applications, which could allow an attacker to gain access to a social media account.
* Hydra: It is a brute force tool that is used to guess passwords. Hydra can be used to test the security of social media accounts, guessing common passwords or using password dictionaries.
* Metasploit: It is a penetration testing framework that is used to find and exploit vulnerabilities in systems and applications. Metasploit can be used to find vulnerabilities in social media applications and exploit them to gain access to the account.
* SSLstrip: It is a tool that can be used to intercept web traffic between the user and the server of the social network, allowing an attacker to see and modify the information that is exchanged.
* Wireshark: It is a network analysis tool that allows security testers to view and analyze network traffic in real time. Wireshark can be used to detect vulnerabilities in an organization's network, which could allow an attacker to gain access to a social media account.
* Nmap: A port scanning tool used to discover open services and ports on a system. Nmap can be used to identify vulnerabilities in an organization's system, which could allow an attacker to gain access to a social media account.
* John the Ripper: It is a brute force tool that is used to guess passwords. John the Ripper can be used to test the password strength of social media accounts.
* InstaHack: Instagram account hacking tool that uses brute force to guess passwords. (<https://github.com/avramit/instahack>)
* FaceNiff: Facebook account hacking tool that intercepts network traffic and allows you to capture login credentials. (<https://faceniff.ponury.net/>)
* TwitterSniper: Twitter account hacking tool that uses brute force techniques to guess passwords. (<https://github.com/NullArray/TwitterSniper>)
* PhishingFrenzy: Phishing tool that allows attackers to create and personalize phishing emails to trick users into obtaining their login credentials. (<https://github.com/pentestgeek/phishing-frenzy>)
* SocialFish: Phishing tool that allows attackers to create and customize fake login pages to obtain users' login credentials. (<https://github.com/UndeadSec/SocialFish>)

## Hack WIFI

WiFi Network Hacking:

Types of WiFi network attacks:

* Rogue Access Point - Fraudulent Access Point - An attack in which a fake access point is created to trick users into connecting and can be monitored or tampered with.
* Evil Twin - Evil Double: An attack in which a fake hotspot with the same name as a legitimate hotspot is created to trick users into connecting and can be monitored or tampered with.
* Deauthentication Attack: An attack in which unauthentication packets are sent to a device or access point to interrupt the connection and possibly force a new authentication that can be intercepted.
* Fake Access Point – Fake Access Point – An attack in which a fake access point is created that mimics a legitimate access point to trick users into connecting and can be monitored or tampered with.
* WEP/WPA Key Cracking: An attack in which you attempt to decrypt the WEP/WPA encryption key to gain access to the network.
* Packet Sniffing: An attack in which packets of data transmitted on the network are captured and analyzed to obtain sensitive information.
* Man-in-the-Middle - Man in the middle: An attack in which an attacker intercepts and manipulates communication between two devices to obtain sensitive information.
* Eavesdropping - Listening: An attack in which an attacker intercepts and listens for wireless communication between two devices to obtain sensitive information.
* Wireless Bridging - Wireless Bridge: An attack in which an attacker establishes an unauthorized wireless connection between two devices to gain access to the network.
* Chop-Chop: This technique consists of deauthenticating a user from a Wi-Fi network and then capturing an encrypted packet containing information about the key. A statistical analysis technique is then used to decrypt the key from the information contained in the packet.
* Beacon Flooding: This technique involves sending a large number of polling packets to a Wi-Fi network, which can cause the network to overload and stop working properly.
* Wireless Jamming: In this type of attack, a device is used to emit radio frequency signals that interfere with the Wi-Fi signal, which can cause network users to disconnect or the network to stop working properly.

Tools:

* 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: A penetration testing tool for wireless routers that uses known exploits. (<https://github.com/threat9/routersploit>)
* Mind map: [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)

## Forensics

Forensics and reverse engineering tools along with their repositories:

* Volatility: Framework for forensic memory analysis. (<https://github.com/volatilityfoundation/volatility>)
* Wireshark: Network protocol analyzer. (<https://github.com/wireshark/wireshark>)
* Autopsy: Digital forensic analysis platform. (<https://github.com/sleuthkit/autopsy>)
* IDA Pro: Binary code disassembler and debugger. (<https://www.hex-rays.com/products/ida/>)
* OllyDbg: Binary code debugger. (<http://www.ollydbg.de/>)
* Ghidra: Open source reverse engineering tool. (<https://github.com/NationalSecurityAgency/ghidra>)
* Radare2: Framework for reverse engineering and binary analysis. (<https://github.com/radareorg/radare2>)
* Capstone: Framework for disassembling binary code. (<https://github.com/aquynh/capstone>)
* Hopper: Disassembler and debugger of binary code. (<https://www.hopperapp.com/>)
* Frida: Instrumentation and dynamic application debugging framework. (<https://github.com/frida/frida>)
* Recuva: Deleted File Recovery [Download Recuva | Recover deleted files, free! (ccleaner.com)](https://www.ccleaner.com/es-es/recuva) .
* EmailAnalyzer: Youcan analyze your suspicious emails. You can extract headers, links, and hashes from the .eml file<https://github.com/keraattin/EmailAnalyzer>
* FtkImager: Mounting Drive Images for Analysis [FTK Imager - Exterro](https://www.exterro.com/ftk-imager)
* EnCase: Digital forensics software used by researchers and computer security professionals to acquire, analyze, and present digital evidence. (<https://www.guidancesoftware.com/>)
* Autopsy: Open source digital forensics platform that includes image analysis, data recovery, and event log analysis tools. (<https://www.sleuthkit.org/autopsy/>)
* FTK Imager: Free forensic analysis tool used to acquire and analyze images of hard drives and storage devices. (<https://accessdata.com/products-services/forensic-toolkit-ftk>)
* Oxygen Forensic Detective: Forensic analysis tool that allows security investigators to examine mobile devices, applications, and data stored in the cloud. (<https://www.oxygen-forensic.com/>)
* Scalpel: File recovery tool used to extract files from damaged or corrupted file systems. (<https://github.com/sleuthkit/scalpel>)
* OSForensics: Forensic analysis platform that includes tools to examine file systems, partitions, logs and image files. (<https://www.osforensics.com/>)
* Ghiro: Digital forensic analysis tool that allows investigators to examine images and files to extract important information. (<https://github.com/Ghirensics/ghiro>)
* BitPim: Forensic analysis tool used to examine mobile devices and extract important information such as contacts, text messages, and call logs. (<https://github.com/bitpim/bitpim>)
* Wireshark: Open source network traffic analysis tool that allows users to capture and analyze network packets in real time. Provides tools for filtering and visualizing network traffic. (<https://www.wireshark.org/>)
* Osticket: Open source ticket management tool used in security incident analysis. It allows users to create, assign and track tickets related to security incidents. (<https://osticket.com/>)
* OSSEC: Open source intrusion detection system used to monitor systems and networks for suspicious activity. Provides real-time alerts on potential security threats. (<https://www.ossec.net/>)
* Bro: Open source network analytics platform used to monitor and analyze network traffic in real time. It provides tools to detect patterns of behavior and security threats. (<https://www.bro.org/>)
* RegRipper: Windows registry analysis tool used to extract important information from the operating system registry. It provides a wide variety of plugins to analyze different areas of the registry. (<https://github.com/keydet89/RegRipper3.0>)
* Bulk Extractor: Forensic data analysis tool used to extract information from files and hard drives. It provides tools to extract email addresses, phone numbers, and other types of information. (<https://github.com/simsong/bulk_extractor>)

## Malware Analysis

Malware analysis tools:

* Malwarebytes: A malware scanning tool that can detect and remove malicious software threats. (<https://www.malwarebytes.com/>)
* VirusTotal: A malware scanning web service that scans suspicious files for threats and provides detailed reports on the scan. (<https://www.virustotal.com/>)
* Yara: Malware analysis tool that allows security analysts to write rules to identify specific malware and malicious behavior. (<https://virustotal.github.io/yara/>)
* Cuckoo Sandbox: Malware analysis platform that runs malware in an isolated environment and captures malicious activity for analysis. (<https://cuckoosandbox.org/>)
* REMnux: Linux distribution specialized in malware analysis that includes tools to examine and disassemble malicious code. (<https://remnux.org/>)
* Sysinternals Suite: Collection of malware analysis tools for Windows systems, including tools to monitor processes, examine files and log system activity. (<https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>)
* IDA Pro: Reverse engineering tool used to examine and disassemble malware code and other programs. (<https://www.hex-rays.com/products/ida/>)
* Wireshark: Network traffic analysis tool that allows security analysts to examine network traffic and detect patterns of malicious behavior. (<https://www.wireshark.org/>)
* Cuckoo Sandbox: is an open source malware analysis tool that allows you to simulate a malware execution environment and analyze its behavior. Repository: <https://github.com/cuckoosandbox/cuckoo>
* Yara: is a malware analysis tool that allows you to look for patterns in the code of a file and thus identify if it is malicious. Repository: <https://github.com/VirusTotal/yara>
* REMnux: is a Linux distribution specialized in malware analysis. It includes a wide variety of malware analysis tools and allows the execution of these tools in an isolated environment to prevent the spread of malware. Repository: <https://github.com/REMnux/remnux-distro>
* Volatility Framework: is a memory analysis tool that allows you to analyze the memory of a system in search of evidence of malware or intrusions. Repository: <https://github.com/volatilityfoundation/volatility>
* Sandfly Security: is a malware analysis tool that focuses on detecting and responding to advanced persistent threats on Linux and Windows systems. Repository: <https://github.com/sandflysecurity/sandfly>
* Any.Run is an online service that allows you to scan malicious files and URLs for malware and other security threats. You can access the Any.Run website on <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 is a tool for monitoring and logging file system and registry changes, for example, made by an installer <https://github.com/skydive241/Regshot-Advanced>
* [Best Malware Analysis Tools List in 2023 - GBHackers](https://gbhackers.com/malware-analysis-tools/)

**Creating Malicious Files**

Malicious file creation tools:

* Metasploit Framework: is a penetration testing tool that can be used to create malicious files to exploit vulnerabilities in software. The official repository is located in [**https://github.com/rapid7/metasploit-framework**](https://github.com/rapid7/metasploit-framework).
* Social-Engineer Toolkit (SET): is a social engineering tool that can be used to create malicious files, such as Microsoft Office documents or PDFs, that include payloads to exploit vulnerabilities or execute commands on the target system. SET also provides predefined templates for creating phishing emails and malicious web pages. The official repository is located in **<https://github.com/trustedsec/social-engineer-toolkit>**.
* PowerShell Empire: is a post-exploitation tool that can be used to create malicious payloads to be delivered via malicious files. It is compatible with Windows, Linux, and macOS and offers a wide range of features, such as persistence, privilege escalation, and data exfiltration. The official repository is located in [**https://github.com/PowerShellEmpire/Empire**](https://github.com/PowerShellEmpire/Empire).
* Office Exploit Builder: This is a tool used to create malicious Microsoft Office files that contain zero-day exploits. It offers an easy-to-use graphical user interface and allows users to customize payload options and the way the file is delivered. The official repository is not available as it is a commercial tool.
* Veil-Evasion: is a tool that allows users to create malicious payloads that evade antivirus detection. It can be used to create malicious files in different formats such as Microsoft Office documents, PDF files, and executable files. The official repository is located in [**https://github.com/Veil-Framework/Veil**](https://github.com/Veil-Framework/Veil).
* Phantom Evasion: This is a free malware creation tool that allows users to create custom Trojans and other malicious payloads. It includes options to obfuscate code, avoid antivirus detection, and generate different malicious file formats, such as .exe files and Microsoft Office documents. The official repository is located at [**https://github.com/oddcod3/Phantom-Evasion**](https://github.com/oddcod3/Phantom-Evasion).
* PDFTools: It is a free and open source tool that allows the creation of malicious PDF files. It allows you to insert malicious scripts into PDF files, which can be used to execute commands on the target system. [**https://github.com/galkan/ptftools**](https://github.com/galkan/ptftools)
* Unicorn: tool that allows the creation of payloads to be delivered through malicious files and that avoids the detection of antivirus. [**https://github.com/trustedsec/unicorn/**](https://github.com/trustedsec/unicorn/)
* APKTool: Reverse engineering tool for Android apps that can be used to manipulate and create malicious apps. [**https://github.com/iBotPeaches/Apktool/**](https://github.com/iBotPeaches/Apktool/)
* Jupyter Notebook: Data analysis tool that can be used to create malware for machine learning and artificial intelligence. [**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)
* Zero-day attacks: Investigative techniques can also be used to identify and exploit new vulnerabilities in third-party software. For example, fuzzing tools can be used to send large amounts of unexpected input to an app and see how it reacts. If a vulnerability is found, a malicious file can develop that exploits it

**Pentesting in Mobile Applications**

Pentesting tools on mobile devices:

* Drozer: is a penetration testing tool for Android mobile applications. It allows you to explore and exploit vulnerabilities in Android mobile applications and is very useful for conducting mobile penetration tests. Repository: <https://github.com/FSecureLABS/drozer>
* Drodijack: This Trojan for Android is one of the most complete. With it we will be able to have remote access to the entire infected device, from the agenda, calls and SMS to the microphone and cameras of the smartphone <https://github.com/Pericena/Droidjack>
* Fridump: <https://github.com/Nightbringer21/fridump> - a script that allows memory extraction of applications on Android devices using Frida.
* AndroBugs\_Framework: <https://github.com/AndroBugs/AndroBugs_Framework> - a script that uses various tools to perform security analysis on Android applications.
* ADB-Toolkit: <https://github.com/ASHWIN990/ADB-Toolkit> - a set of scripts that automates various tasks related to the use of ADB (Android Debug Bridge) on Android devices.
* APK-Downloader: <https://github.com/ndossougbe/apk-downloader> - a script that allows downloading apps from the Google Play Store without the need for a Google account.
* dex2jar: <https://github.com/pxb1988/dex2jar> - a script that converts Android DEX files into JAR format files.
* Drozer: <https://github.com/FSecureLABS/drozer> - a security framework for Android that allows penetration testing on mobile applications.
* apktool: <https://github.com/iBotPeaches/Apktool> - a script that allows reverse engineering of Android applications to obtain resources and source code.
* Genymotion-ARM-Translation: <https://github.com/m9rco/Genymotion_ARM_Translation> - a script that allows the execution of ARM applications on the Genymotion Android emulation platform.
* Android-SSL-Trust-Killer: <https://github.com/iSECPartners/android-ssl-bypass> - a script that disables SSL validation in Android applications for penetration testing.
* Ssl-kill-switch2: <https://github.com/nabla-c0d3/ssl-kill-switch2> - a script that allows the disabling of SSL validation in iOS applications for penetration testing.
* Mobile-Security-Framework-MobSF: <https://github.com/MobSF/Mobile-Security-Framework-MobSF> - a mobile security framework for iOS and Android that enables static and dynamic analysis of mobile applications.
* Needle: <https://github.com/mwrlabs/needle> - a mobile app penetration testing framework for iOS that allows interaction with the app through a console.
* iNalyzer: <https://github.com/iSECPartners/iNalyzer> - a security analysis tool for iOS that allows the extraction of information and resources from mobile applications.
* Apk.sh: Freverse-engineering Android apps, automating some repetitive tasks like extracting, decoding, rebuilding, and patching an APK<https://github.com/ax/apk.sh>
* Objection: <https://github.com/sensepost/objection> - a penetration testing tool for iOS and Android mobile apps that allows interaction with the app through a console.
* AppMon: <https://github.com/dpnishant/appmon> - a security analysis tool for Android mobile applications that allows the extraction of information and resources from the application.
* AppUse: <https://github.com/appuse/appuse> - an emulation platform for penetration testing on Android mobile applications.
* APKiD: <https://github.com/rednaga/APKiD> - a tool that performs static analysis of Android applications for the identification of components and libraries used in the application.
* Bypass: <https://github.com/freedomofdevelopers/bypass> - a tool that allows the evasion of the security of iOS applications for penetration testing.
* SSLyze: <https://github.com/nabla-c0d3/sslyze> - a network security analysis tool that allows the identification of SSL/TLS vulnerabilities in mobile applications.
* EvilAP\_Defender: <https://github.com/PabloMansanet/EvilAP_Defender> - an Evil Access Points (APs) detection tool that can be used to intercept data from mobile devices.
* Hopper: <https://www.hopperapp.com/> - a reverse engineering tool for iOS and Android that allows the decompilation and analysis of mobile applications.
* Burp Suite Mobile Assistant: <https://portswigger.net/burp/documentation/desktop/tools/mobile-assistant> - a tool that allows the interception and manipulation of HTTP/S traffic between mobile applications and servers.
* DroidBox: <https://github.com/pjlantz/droidbox> - a dynamic analysis tool for Android applications that allows behavioral tracking and vulnerability identification.
* Xposed Framework: <https://github.com/rovo89/Xposed> - an Android modification framework that allows code injection into mobile applications.
* Androguard: <https://github.com/androguard/androguard> - a static analysis tool for Android applications that allows the extraction of information and resources.
* Cydia Impactor: <https://cydiaimpactor.com/> - a tool that allows the installation of IPA applications on iOS devices without the need for an Apple developer account.
* Metasploit Framework: A penetration testing framework that has an extensive set of modules for penetration testing on systems and applications, including mobile applications. Repository: <https://github.com/rapid7/metasploit-framework>
* AndroRAT: a remote access tool for Android devices that allows full control of the device and the possibility of injecting malicious code into applications. Repository: <https://github.com/wszf/AndroRAT>
* Evil-Droid - a tool that allows the creation of malicious applications for Android devices with the ability to inject malicious code and perform malicious actions. Repository: <https://github.com/M4sc3r4n0/Evil-Droid>
* TheFatRat: a tool that allows the creation of backdoors and payloads for Android devices, with the ability to execute malicious code and take full control of the device. Repository: <https://github.com/Screetsec/TheFatRat>
* Apktool - a reverse engineering tool that allows the decompilation and disassembly of Android applications for the modification and creation of malicious versions. Repository: <https://github.com/iBotPeaches/Apktool>
* Frida: a code injection framework that allows the modification and analysis of mobile applications at runtime, both on Android and iOS. Repository: <https://github.com/frida/frida>
* Xposed Framework: A code injection framework for Android devices that allows modification of the system and applications, including the injection of malicious code. Repository: <https://github.com/rovo89/Xposed>
* Objection: A penetration testing tool for mobile applications that allows interaction with the application through a console, including the injection of malicious code. Repository: <https://github.com/sensepost/objection>
* Appium: A test automation tool for mobile applications that allows the injection of malicious code into automated tests. Repository: <https://github.com/appium/appium>
* Inspeckage: a tool that allows dynamic analysis of Android applications, injecting malicious code at runtime and monitoring application communication attempts. Repository: <https://github.com/ac-pm/Inspeckage>
* Pen-Andro: Script to automate the installation of applications, frida server and move the Burpsuite certificate to the root folder<https://github.com/raoshaab/Pen-Andro>
* Xposed Framework: An Android application modification framework that allows the injection of malicious code into the application and the modification of its behavior at runtime. Repository: <https://github.com/rovo89/Xposed>
* Cain & Abel: [https://github.com/xenomuta/cain](https://github.com/xenomuta/cain%20) - a password recovery tool that can also be used for the exploitation of mobile devices through brute force attacks.

**Metadata Extraction**

Metadata extraction tools:

* FOCUS: Tool to find metadata and hidden information in <https://github.com/ElevenPaths/FOCA> documents
* Exiftool: A command-line tool written in Perl that allows you to read and write metadata to files of different formats, including images, audio files, and documents. Repository: <https://github.com/exiftool/exiftool>
* Exifread: a Python library that allows you to read and analyze metadata in images. Repository: <https://github.com/ianare/exif-py>
* Exiv2: A C++ library that allows you to read and write metadata to images and other files. Repository: <https://github.com/Exiv2/exiv2>
* Metadata-Extractor: A Java library that allows you to read metadata in different types of files, including images, audio files, and documents. Repository: <https://github.com/drewnoakes/metadata-extractor>
* ImageMagick: a command-line tool written in C that allows you to manipulate images of different formats and extract information from metadata. Repository: <https://github.com/ImageMagick/ImageMagick>
* Matroska: A C++ library that allows you to read and write metadata to video and audio files in Matroska format. Repository: <https://github.com/Matroska-Org/libmatroska>
* FFmpeg: a command-line tool written in C that allows you to manipulate video and audio files of different formats and extract metadata information. Repository: <https://github.com/FFmpeg/FFmpeg>
* PyExifTool: a Python library that allows you to read and write metadata in files of different formats, including images, audio files and documents. Repository: <https://github.com/smarnach/pyexiftool>
* PDFMiner: a Python library that allows you to extract text and metadata from PDF files. Repository: <https://github.com/pdfminer/pdfminer.six>
* LibTiff: A C library that allows you to read and write metadata to images in TIFF format. Repository: <https://gitlab.com/libtiff/libtiff>

**Extracting Sensitive Data from GitHub Repositories**

GitHub repository data extraction tools:

* GitDumper: a tool created by @arthaud takes a public Git repository and downloads all its history, including files, change history, passwords, tokens, among others. Repository: <https://github.com/arthaud/git-dumper>
* Gitleaks: A tool created by @zricethezav that scans Git repositories and looks for sensitive data such as passwords, tokens, SSH keys, and more. Repository: <https://github.com/zricethezav/gitleaks>
* TruffleHog: A tool created by @dxa4481 that recursively searches Git history to find passwords and other sensitive data. Repository: <https://github.com/dxa4481/truffleHog>
* Gitrob: A tool created by @michenriksen that scans public Git repositories and finds sensitive information, such as tokens, SSH keys, usernames, and emails. Repository: <https://github.com/michenriksen/gitrob>
* DumpsterDiver: A tool created by @securitywithoutborders that searches Git repositories for sensitive information, such as passwords, SSH keys, tokens, and usernames. Repository: <https://github.com/securitywithoutborders/dumpsterdiver>

**Repositories of Interest**

* [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 with Ettercap for HTTP/HTTPS – Strip that pounds ...](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)
* Document very similar to this.  [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) Publication | 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/)