

Vista de navegador: [Recursos ciberseguridad](#).

Índice

- [Utilidades](#)
- [Aplicaciones](#)
- [VPNs seguros y con anonimidad](#)
- [Windows](#)
- [Linux](#)
- [Android](#)
- [Aplicaciones de seguridad para Android](#)
 - [CTFs](#)
- [Libros](#)
- [Exámenes](#)
- [Canales de YouTube](#)
- [Cursos](#)

Utilidades

- [ExplainShell](#) - Explicaciones de comandos de consola.
- [ShellCheck](#) - Encuentra bugs en tus scripts de bash.
- [ctf-katana](#) - Lista de herramientas y comandos que pueden ayudar con desafíos de CTF.
- [PayloadAllTheThings](#) - Lista de payloads y bypass de filtros para CTFs y Aplicaciones Web.
- [InternalAllTheThings](#) - Lista de payloads y bypass de filtros para Active Directory.
- [Book HackTricks](#) - Una lista enorme de técnicas, trucos y vulnerabilidades. También en [Español](#).
- [Cloud HackTricks](#) - Lista de vulnerabilidades para explotar servicios en la nube.
- [CyberChef](#) - Análisis de datos (Útil para Des/Encriptar).
- [Request Inspector](#) - Análisis de peticiones HTTP.
- [FactorDB](#) - Factorización en números primos de cualquier número.
- [IppSec Rocks](#) - Búsqueda en los cursos/videos de IppSec por palabras clave.
- [Cover Your Tracks](#) - Prueba tu navegador para ver qué tan protegido estas contra el rastreo.
- [Browser Leaks](#) - Prueba tu navegador para ver tu nivel de anonimidad.
- [Sploitus](#) - Búsqueda de exploits y herramientas de seguridad.
- [Wigle](#) - Lista de más de un millón de redes wifi en todo el mundo.
- [Censys](#) - Búsqueda de IPS y servicios.
- [Shodan](#) - Búsqueda de IPs y servicios. (Mi favorito)
- [FOFA](#) - Como Shodan pero chino (Literalmente chino).
- [Criminal IP](#) - Búsqueda de IPs y servicios.
- [ZoomEye](#) - Búsqueda de IPs y servicios.
- [GreyNoise](#) - Búsqueda de IPs y servicios.

- [Onyphe](#) - Búsqueda de IPs y servicios.
- [DB-IP](#) - Información sobre una IP.
- [Hunter](#) - Búsqueda de Emails de una compañía.
- [MobSFLive](#) - Análisis de APKs.
- [Browserling](#) - Sandbox en el navegador para probar links y aplicaciones.
- [Tria.ge](#) - Analizar muestras de malware.
- [MalAPI](#) - Listado de funciones utilizadas por malware.
- [Wappalyzer](#) - Identifica tecnologías en sitios web.
- [Leakpeek](#) - Búsqueda de contraseñas.
- [LeakCheck](#) - Busca de dónde ocurrieron las filtraciones.
- [HaveIBeenPwned](#) - Chequear si un Email ha sido comprometido.
- [Intelligence X](#) - Búsqueda de datos y contraseñas filtradas.
- [Canary Tokens](#) - Honey pots.
- [XSS Payloads](#) - Está caída pareciera.
- [Poastal](#) - Email Osint.
- [PentestMonkey](#) - Lista de herramientas, scripts e información.
- [C2 panels](#) - Paneles de control de malware.
- [C2 panels 2](#)
- [Dedigger](#) - Buscar en Google Drive archivos públicos.
- [Apkwash](#) - Evasión de antivirus para APKs generadas con msfvenom.
- [AbuseIP](#) - Chequear una IP o denunciar una.
- [DotGit](#) - Extensión para automatizar la búsqueda del directorio .git en el navegador.
- [HackTools](#) - Extensión para ayudarte con pentesting.
- [Urlscan](#) - Escanea una URL para ver qué puede contener.
- [AnyRun](#) - Ejecuta cualquier aplicación en el navegador con un sistema virtualizado.
- [VirusTotal](#) - Analiza aplicaciones y archivos con más de 70 antivirus.
- [Malwarewatch](#) - Repositorio de malware y software útil.
- [VxUnderground](#) - Repositorio de malware.
- [Privacytests](#) - Chequea los navegadores para ver cuál es más seguro.
- [Mefiltraron](#) - Busca si tus datos fueron filtrados con tu correo electrónico. (Poco exacto)
- [H8mail](#) - OSINT de correos electrónicos.
- [Breachdirectory](#) - Busca contraseñas expuestas de un usuario.
- [Bug Bounty Guide](#) - Tips, recursos, etc. para encontrar bugs y vulnerabilidades.
- [GuerrillaMail](#) - Envía mails "anónimamente".
- [Temp mail](#) - Genera mails temporales (Muchos están bloqueados para su uso en redes sociales).
- [Lyzem](#) - Busca en telegram por palabras clave.
- [LibGen](#) - Busca libros o artículos.
- [Cached View](#) - Ver página en caché.
- [Wayback Machine](#) - Ver versiones antiguas de páginas.
- [MITMonster](#) - Explicaciones de distintos tipos de ataques de Man In The Middle.
- [Nmap Formatter](#) - Convertir resultados de NMAP a otros formatos o gráficos.
- [CatPhish](#) - Genera dominios similares para ataques de phishing.

- [BLE Spam](#) - Ataque Bluetooth para spam de beacons.
 - [MHDDoS](#) - Herramienta para ataques DDoS.
 - [Free Media Heck Yeah](#) Colección de cosas gratis en internet.
 - [Kaspersky Virus Removal Tool](#) - Antivirus recomendado.
 - [JustDeleteMe](#) - Busca cómo eliminar tus datos de una página.
 - [JustGetMyData](#) - Solicita tu información en distintas páginas.
 - **Osint**
 - [Mi Nosis](#) - Busca informes crediticios por Nombre/DNI (También conseguís el DNI por el nombre).
 - [Dateas](#) - Busca cualquier persona por nombre, DNI, CUIT o CUIL.
-

Aplicaciones

- **General**
 - [Sectools](#) - Top 125 Aplicaciones de seguridad de la mano de los creadores de Nmap.
 - [RustScan](#) - Escaner de puertos moderno. (Alternativa rápida de Nmap).
 - [Red Teaming Toolkit](#) - Lista de herramientas comerciales y de código abierto para ayudar en operaciones Red Team.
 - [Web Hacker's Weapons](#) - Lista de herramientas usadas para hacking web.
 - [XssHunter Express](#) - Ayuda para conseguir ataques de Cross Site Scripting y te muestra si los exploits funcionaron.
 - [Sherlock Project](#) - OSINT para usuarios en múltiples páginas.
 - [GitTools](#) - Extracción de directorios .git.
 - [Ghauri](#) - Buena alternativa a sqlmap.
 - [Simple PHP WebShell](#) - Webshell en PHP para RCE.
 - [HTTPX](#) - Herramienta para hacer multiples peticiones de red.
 - [Subfinder](#) - Herramienta para enumeración pasiva de subdominios.
 - [CVEMap](#) - Herramienta para buscar en bases de datos de vulnerabilidades.
 - [Nuclei](#) - Herramienta para escanear vulnerabilidades.
 - [Nuclei Templates](#) - Lista de plantillas de nuclei para encontrar vulnerabilidades.
 - [ParamSpider](#)
 - [Nuclei Fuzzer](#)
 - [Ferox Buster](#) - Escáner de recursos recursivo.
- **Web3**
 - [Mythril](#) - Herramienta de análisis para smart contracts.
 - [DappTools](#) - Herramienta de CLI para Ethereum.
 - [Surya](#) - Herramienta para obtener información de un smart contract.
 - [Foundry](#) - Herramienta de CLI para Ethereum. [Click para más información.](#)

VPNs seguros y con anonimidad

- [Mullvad](#) - Para paranoicos.
- [Private Internet Access](#) - El más popular.
- [IVPN](#) - Alternativa más restringida a Mullvad.

- [NordVPN](#) - Con mejor puntuación.
-

Windows

- **Activación**
 - [MassGrave](#) - Métodos de activación de Windows y Office.
 - **Extraer contraseñas**
 - [Mimikatz](#) - Usuarios.
 - [LaZagne](#) - Navegadores.
 - **Shell**
 - [Evil-WinRM](#) - Consola remota para pentesting de windows.
 - **Escalada de privilegios**
 - [Windows Kernel Exploits](#) - Exploits del kernel de windows para ejecución de código con privilegios.
 - [Windows Exploit Suggester](#) - Provee una lista de vulnerabilidades que puede tener el sistema.
 - [WinPEAS](#) -Busca posibles caminos para escalar privilegios en sistemas Windows.
 - [Privesc Check](#) - Script para escalar privilegios.
 - [LOLBAS](#) - GTFOBins pero para Windows.
 - [WADComs](#) - Una lista de herramientas y sus comandos (Inspirado en LOLBAS y GTFOBins).
-

Linux

- **Escalada de privilegios**
 - [LinPEAS](#) - Busca posibles caminos para escalar privilegios en sistemas Linux/Unix/macOS.
 - [Unix Privesc Check](#) - Busca posibles caminos para escalar privilegios en sistemas Linux/Unix/macOS.
 - [Linux Priv Checker](#) - Busca posibles caminos para escalar privilegios en sistemas Linux/Unix/macOS.
 - [LinEnum](#) - Mi favorito junto a LinPEAS.
 - [PSpy](#) - Ver procesos, cron jobs y comandos de otros usuarios en tiempo real.
-

Android

- [Genymotion](#) - Emulador de android.

Aplicaciones de seguridad para Android

- [L4bsForAndroid](#) - Repositorio de aplicaciones de Seguridad para Android
- [Arc4i](#) - Aplicación para hacer ARP Spoof y bloquear personas del WiFi.
- [Fing](#) - Escáner de red.
- [Frida](#) - Herramienta para ingeniería inversa.

CTFs

- [HpAndro](#) - CTF de la aplicación de Android de HpAndro con vulnerabilidades fáciles([Instalar App](#)).
 - [Awesome Mobile CTF](#) - Repositorio con información sobre seguridad en dispositivos móviles.
-

Libros

- [Ethical Hacking Books](#) - PDFs de los libros de hacking más comunes y útiles.
- [Awesome Security Ebooks](#) - Lista de libros.
- [Repositorio elhacker](#) - Libros, tutoriales, isos, etc.
- [Repositorio AlbusSec](#) - Libros y payloads

Exámenes

- [Total OSCP guide](#) - Guía de estudio para el OSCP.

Canales de YouTube

- [lppSec](#) - Writeups de máquinas de HackTheBox.
 - [DarkSec](#) - Writeups para TryHackme.
-

Cursos

- **Web Security**
 - [Invicti Learn](#) - Cursos para vulnerabilidades web y cómo prevenirlas
- **Linux**
 - [Linux Journey](#) - Aprende Linux.
- **CTFs**
 - [Trail Of Bits](#) - Writeups de CTFs, explotación de binarios, seguridad forense, auditar sistemas.
- **Explotación de binarios**
 - [Nightmare](#) - Introducción a la explotación de binarios e ingeniería inversa.
 - [How2Heap](#) - Repositorio para aprender técnicas de heap exploitation.
- **Análisis**
 - [Shell storm](#) - Blog con datos sobre técnicas de deobfuscación, análisis binario, kernel.
- **Python**
 - [El libro de python](#) - Curso de Python gratuito.
- **Kotlin**
 - [Curso Kotlin](#) - Curso de Kotlin.
- **General**

- [Fuzzysecurity](#) - Explotación de Windows, Linux, análisis de malware, RFID.
 - [Hacksplaining](#) - Explicación de las vulnerabilidades más comunes en aplicaciones web.
 - [Cybrary](#) - Videos sobre ciberseguridad gratis.
 - [CTF101](#) - Guía con técnicas y metodologías para análisis forense, criptografía, explotación web, ingeniería inversa y explotación de binarios.
 - [PicoCTF](#) - Cursos de análisis forense, criptografía, explotación web, ingeniería inversa y explotación de binarios.
 - [LearnXinYMinutes](#) - Lista de lenguajes con documentación básica para entenderlos.
 - [Repositorio elhacker](#) - Libros, tutoriales, ISOs, etc.
 - **Web3**
 - [NotOnlyOwner](#) - Introducción a la seguridad y hacking en Ethereum.
 - [Learn web3 / smart-contract Hacking in 2023 step by step guide](#) - Guía para hackear smart contracts.
 - [Immunefi Web3 Security Library](#) - Información y tutoriales/herramientas sobre seguridad en web3
 - [Blocksec CTFs](#) - Lista de juegos, CTFs, writeups, etc.
 - **Learning paths**
 - [Web security learning path](#) - Mini curso de PortSwigger explicando vulnerabilidades web, con laboratorios para probarlas.
 - [Learning Paths TryHackMe](#) - "Cursos" de TryHackMe para aprender distintas vulnerabilidades y empezar en ciberseguridad.
-

Práctica

Writeups

- [Oxdeed](#) - Writeups de HackTheBox.
- [Oxdf](#) - Writeups para HackTheBox.
- [\[https://pentester.land/writeups/\]\(Pentester Land\)](https://pentester.land/writeups/) - Writeups de vulnerabilidades de programas de Bug Bounty.
- [Infosecmachines](#) - Writeups HackTheBox/VulnHub/Portswigger.
- [Infosecmachines Excel](#) - Excel con videos para HackTheBox/VulnHub/Portswigger.
- [Snowscan](#) - Writeups de HackTheBox.

Cheat Sheets

- [PayloadAllTheThings](#) - Lista de payloads y bypasses para distintas vulnerabilidades web.
- [OWASP Cheat Sheets Series](#) - Lista de vulnerabilidades web y cómo prevenirlas.
- [Invicti SQL Injection Cheat Sheet](#) - Lista de payloads para SQLI
- [One Liner Collections](#) - Lista de comandos de una linea.

Máquinas vulnerables / CTFs

- [HackTheBox](#) - VPN con máquinas vulnerables en la red. (De los más avanzados y realistas)
- [TryHackMe](#) - VPN con máquinas vulnerables en la red. (Más beginner friendly)
- [VulnHub](#) - Máquinas virtuales vulnerables.
- [PwnTillDawn](#) - VPN con máquinas vulnerables en la red.
- [OverTheWire](#) - Te conectas por SSH y empezás a hackear una máquina.
- [HackThisSite](#) - Más básico y fácil para empezar.

- [Pwnable](#) - Explotación de binarios.
- [Attack Defense](#) - Explicaciones y máquinas para atacar.
- [RootMe](#) - Páginas sin VPN, fáciles de hackear y relativamente realistas.
- [PortSwinger Web Security Academy](#) - Laboratorios para probar vulnerabilidades web.
- [Pwn College](#) - Plataforma educativa para practicar con CTFs.
- [PicoCTF](#) - CTFs amigables sobre explotación web, criptografía, explotación de binarios, análisis forense, ingeniería inversa, etc.
- [CTF Sites](#) - Lista de páginas de CTF.
- [Microcorruption](#) - Página para practicar explotación de binarios desde el navegador y de una forma realista.
- [Labs gf0s](#) - Retos de hacking fáciles.
- [Defend The Web](#) - Retos web.
- [Cryptohack](#) - Retos de criptografía.
- [Crackmes](#) - Retos de ingeniería inversa.
- [Ethernaut](#) - Retos de Web3.
- [Capture The Ether](#) - Retos de Web3.
- [Damn Vulnerable DeFi](#) - Retos de Web3.
- [DefiVulnLabs](#) - Retos de Web3

Programas de bug bounty

- [Hacker101](#)
- [BugCrowd](#)

Exámenes

- [TJNulls](#) - Preparación OSCP.

Otros

Listas

- [Other Awesome Lists](#)
- [Formación Ciberseguridad](#) - Repositorio público de recursos de formación en ciberseguridad (Gratis y de pago).
- [Osint](#)
- [Awesome Piracy](#) - Lista de links de piratería.
- [Awesome Reversing](#) - Información sobre Reverse Engineering.
- [Awesome GPT Agents](#) - Lista de agentes GPT para ciberseguridad.
- [Crypto Cat CTF](#) - Colección de información sobre ciberseguridad.
- [OSINT Discord Resources](#) - Lista de aplicaciones para hacer OSINT en discord.

Dark forums

- [Cracked.](#)
- [Nulled](#)

- [Black Hat World](#)

Denuncias

- [AntiphishingLA](#) - Denunciar páginas de phishing.
- [Phish Report](#) - Denunciar páginas de phishing.
- [Phish Tank](#) - Denunciar páginas de phishing.
- [Denunciar delitos informáticos](#)
- [Nollame](#) - Registre su número para evitar que lleguen llamadas publicitarias. [Link directo](#).
- [Lista Robinson](#) - Registre su número para evitar que lleguen llamadas publicitarias.
- [Safebrowsing Phishing](#) - Denunciar una página de phishing a Google.
- [Safebrowsing Malware](#) - Denunciar una página con malware a Google.
- [IC3 Delitos](#) - Reportar delitos informáticos al FBI.
- [IC3 Ransomware](#) - Reportar un ataque de ransomware.
- [Google imágenes no consentidas](#) - Solicitar la retirada de imágenes explícitas o íntimas no consentidas en Google.
- [Stop NCII](#) - Denunciar amenazas de compartir imágenes íntimas.
- [Departamento de seguridad nacional](#) - Reportar ataques de terrorismo o actividad sospechosa.
- [AbuseIP](#) - Denunciar una IP de abuso (intentos de ataque).

Ayuda

- [ID Ransomware](#) - Suba una nota de rescate o una muestra de archivo cifrado para identificar el ransomware que te infectó.
- [No More Ransom](#) - Obtén una herramienta de descifrado para el ransomware que te infectó.