--------------------------------------

PDF para aprender hacking (si no entiendes el hacking mira este PDF y luego usa estas herramientas

<https://acrobat.adobe.com/link/track?uri=urn:aaid:scds:US:26a5fa7c-e683-392d-bc23-f5232176b9a0>

--------------------------------------

Creador: ruben

Redes sociales

Instagram: g3\_ruben.\_.fnl\_

twitch: g3zeusomg

Youtube: dekwik 58

PSN: g3\_piton-52

Discord: ٴ😈🟡🔴🟢𖥡␃ ا𓂺13padا#0666

Twitter: g3ruben

Mi server: <https://discord.gg/ErwXcRgqvJ>

--------------------------------------

Redes de amigos (promoción)

--------------------------------------

Jump

Discord: Deleted User 52kasl3as#9176

--------------------------------------

No me hago responsable de ningún uso mal dado ningún pero vamos osea ningún uso mal dado (mi recomendacion) no usar los programas por seguridad (todo el que usé estas herramientas es consecuencia de la persona que las a usado) (algunas herramientas estarán borradas o enlaces por que serían programas de hacking muy peligrosos o por que serán muy antiguas y ya estaran borradas y eso no quiere decir que el word no sirva para nada estarán borradas por que algunas plataformas de subidas de archivos no permiten esas cosas o lo que mencione antes)

--------------------------------------

Este word en total cuesta más de 300€ pero lo vendo por 40€

--------------------------------------

Herramienta de ingeniería social [Acceso a cámara web, micrófono, grabador de contraseñas del sistema operativo y buscador de ubicación] con ngrok.

1: [https://github.com/ultrasecurity/Storm-Breaker](http://htps://github.com/ultrasecurity/Storm-Breaker)

--------------------------------------

Phishing personalizado

1: <https://github.com/swagkarna/tilapia>

--------------------------------------

Phishing

1: <https://github.com/tony23x/Predator-Phish>

2: <https://github.com/iinc0gnit0/BlackPhish>

3: <https://github.com/TermuxHackz/anonphisher>

4: <https://github.com/Bhaviktutorials/shark>

5: <https://github.com/Cesar-Hack-Gray/SocialSploit>

6: <https://github.com/htr-tech/zphisher>

7: <https://github.com/xHak9x/SocialPhish>

8: <https://github.com/Ignitetch/AdvPhishing>

9: <https://github.com/KasRoudra/PyPhisher>

10: <https://github.com/tony23x/Predator-Phish>

11: <https://github.com/noob-hackers/Mrphish>

12: <https://github.com/noob-hackers/sneakphish>

?: <https://github.com/The-Burning/blackeye-im>

?: <https://github.com/Ignitetch/Zomato-Phishing>

!: <https://github.com/jimywork/Modlishka>

?: https://github.com/error404-notfound/ScorpFishV2

--------------------------------------

Phishing lite

1: <https://github.com/swagkarna/LitePhish>

--------------------------------------

Wifi phishing

1: <https://github.com/parzibyte/firmware-upgrade-es>

--------------------------------------

Ocultar página de phishing con una página normal

1: https://github.com/jaykali/maskphish

--------------------------------------

Clone cualquier sitio web con solo un simple script de python

1: <https://github.com/swagkarna/WebCloner>

--------------------------------------

CredSniper es un marco de phishing escrito con el micro-marco de Python Flask y la plantilla Jinja2 que admite la captura de tokens 2FA.

1: <https://github.com/ustayready/CredSniper>

--------------------------------------

Generador de capa inversa

1: <https://github.com/chrispetrou/shellback>

--------------------------------------

Dominio inverso a IP

1: <https://github.com/AzhariKun/domain-to-ip>

--------------------------------------

🕵️‍♂️ Investigue las cuentas de Google con correos electrónicos.

1: https://github.com/mxrch/GHunt

--------------------------------------

Wi-Fi sploit es un descifrador de contraseñas para una página de administración de un enrutador Wi-Fi.

1: <https://github.com/kevinadhiguna/wifi-sploit>

--------------------------------------

CVE-2021-3449 Exploit de denegación de servicio de OpenSSL 👨🏻‍💻

1: <https://github.com/terorie/cve-2021-3449>

--------------------------------------

smartrecon es un poderoso script de shell para automatizar el reconocimiento y encontrar vulnerabilidades comunes para el cazador de errores

1: <https://github.com/kh4sh3i/smartrecon>

--------------------------------------

Herramienta de fuzzing, enumeración y explotación de inclusión de archivos y cruce de directorios.

1: <https://github.com/chrispetrou/FDsploit>

--------------------------------------

Herramienta para usar The Browser Exploitation Framework fuera de LAN, con diferentes opciones para hackear

1: <https://github.com/tony23x/beef-for-cerberus>

--------------------------------------

Sifter es un escáner de osint, reconocimiento y vulnerabilidad. Combina una plétora de herramientas dentro de diferentes conjuntos de módulos para realizar rápidamente tareas de reconocimiento, verificar el firewall de la red, enumerar hosts remotos y locales, y buscar las vulnerabilidades 'azules' dentro de microsft y, si no están parcheadas, explotarlas. Utiliza herramientas como blackwidow y konan para nosotros...

1: <https://github.com/5l1v3r1/sifter>

--------------------------------------

ChatSecure es un cliente de chat cifrado gratuito y de código abierto para iOS que admite el cifrado OTR y OMEMO sobre XMPP.

1: <https://github.com/ChatSecure/ChatSecure-iOS>

--------------------------------------

ES - Generador de cuentas de la plataforma Lampyre | PT - Administrador de cuentas de la plataforma Lampyre

1: <https://github.com/0moura/LAC>

--------------------------------------

Raspar y Descargar de dados no google

1: https://github.com/0moura/DSD

--------------------------------------

Encuentra nombres de usuario en más de 75 redes sociales

1: <https://github.com/xHak9x/finduser>

--------------------------------------

Una herramienta OSINT para recopilar información sobre números de teléfono

1: <https://github.com/spider863644/PhoneNumber-OSINT>

--------------------------------------

Ping2death es un ddos ​​para enviar paquetes sobre un usuario. Tiene una cantidad personalizada de paquetes

1: <https://github.com/spider863644/Ping2death>

--------------------------------------

Mailer es un script de python3 que se utiliza para enviar phishing selectivo al correo electrónico de destino... Fue creado por Spider Anongreyhat

1: <https://github.com/spider863644/Mailer>

--------------------------------------

Un cliente SQL moderno, rápido e impulsado por la productividad con un enfoque en UX.

1: <https://github.com/antares-sql/antares>

--------------------------------------

¡Un sitio web que proporciona información para instalar roms personalizadas o para instalar una recuperación personalizada o para rootear el dispositivo!

1: <https://github.com/KasRoudra/kascust>

--------------------------------------

¡Hackear a la NASA! (xd de seguro es falso xd)

1: <https://github.com/KasRoudra/nasahack>

--------------------------------------

Esta es la herramienta de pishing de Facebook

1: <https://github.com/BD8KR3M/bos-p>

--------------------------------------

InfoG is an information gathering tool. You can find ip addresses, phone number details and much more.

1: <https://github.com/Tech-Sec/InfoG>

--------------------------------------

Herramienta Doxing Sofisticada

1: <https://github.com/noob-coder123/Garuda>

Apt install Git -y

Git clone <https://github.com/noob-coder123/Garuda>

Cd Garuda

Pip install -r requirements.txt

Python3 setup.py

--------------------------------------

Speye es una herramienta avanzada de doxing, compatible con Windows, Termux y Linux.

1: <https://github.com/noob-coder123/speye>

--------------------------------------

Esta es una herramienta de spam, para obtener clientes potenciales.

1: <https://github.com/Crevils/mailextract>

--------------------------------------

Sin descripción del programa

1: <https://github.com/Crevils/hackingram>

--------------------------------------

UserBot avanzado de Telegram. [Python][Teletón]

1: <https://github.com/Crevils/TeleBot>

--------------------------------------

La última herramienta de reconocimiento web que necesitará

1: <https://github.com/thewhiteh4t/FinalRecon>

--------------------------------------

WHATSAPP-BANEO

1: <https://github.com/Hacking-pch/WHATSAPP-BANEO>

++++++++++++++++++++++++++++++

Comandos para suspender número

$apt update && apt upgrade

$apt install git

$git clone

<https://github.com/Hacking-pch/WHATSAPP-BANEO/blob/master/README.md>

$cd WHATSAPP-BANEO

$chmod +x \*WHATSAPP-BANEO.sh

$bash BANEO.sh

++++++++++++++++++++++++++++++

banear números que no sean +52 que pide el programa (solo tienes que modificar el Código osea buscas donde ponga +52 en el Código y lo cambias a +34 o del país que eres hay un video en YT explicando lo como se hace y yo editaría el Código con pluma)

--------------------------------------

Herramienta OSINT para encontrar contraseñas de direcciones de correo electrónico comprometidas

1: <https://github.com/thewhiteh4t/pwnedOrNot>

--------------------------------------

Herramienta OSINT para encontrar perfiles por nombre de usuario

1: <https://github.com/thewhiteh4t/nexfil>

--------------------------------------

Detecta y extrae imágenes de la cadena de bloques Goerli Testnet

1: <https://github.com/thewhiteh4t/goerli-image-hunt>

--------------------------------------

Marco de explotación para ataques HID basados ​​en ATtiny85

1: <https://github.com/thewhiteh4t/flashsploit>

--------------------------------------

Un simple spammer para WhatsApp hecho en vbscript solo para windows

1: <https://github.com/Euronymou5/WhatsApp-nuker>

--------------------------------------

Xepor, un marco de enrutamiento web para ingenieros inversos e investigadores de seguridad, trae lo mejor de mitmproxy y Flask

1: <https://github.com/xepor/xepor>

--------------------------------------

Un simple script de shell para cambiar los valores gamma de visualización

1: <https://github.com/thewhiteh4t/gammachanger>

--------------------------------------

Potentes miembros de Telegram que extraen y agregan kit de herramientas

1: <https://github.com/noob-coder123/Genisys>

--------------------------------------

mx-takeover enfoca los registros DNS MX y detecta los registros MX mal configurados.

1: <https://github.com/musana/mx-takeover>

--------------------------------------

SSH generation keys

1: <https://docs.github.com/es/authentication/connecting-to-github-with-ssh/generating-a-new-ssh-key-and-adding-it-to-the-ssh-agent>

--------------------------------------

Phonia Toolkit es uno de los kits de herramientas más avanzados para escanear números de teléfono utilizando solo recursos gratuitos. El objetivo es recopilar primero información estándar como país, área, operador y tipo de línea en cualquier número de teléfono internacional con muy buena precisión.

1: <https://github.com/coredamage/phonia>

--------------------------------------

Es una herramienta de discordia dedicada que envía continuamente una gran cantidad de mensajes al canal de discordia a través de Discord Webhook.

1: <https://github.com/KMKINGMAN/Discord-WebHook-Spammer>

--------------------------------------

[ Fuzzer web ultrarrápido en Rust ]

1: <https://github.com/iinc0gnit0/RBust>

--------------------------------------

Una biblioteca de Python para proporcionar funciones para manejar, analizar y validar números estándar.

1: <https://github.com/arthurdejong/python-stdnum>

--------------------------------------

Una herramienta de comprobación de sitios web para webmasters

1: https://github.com/arthurdejong/webcheck

--------------------------------------

🐔Kit de herramientas para analizar, validar, manipular, comparar y mostrar fechas, horas y zonas horarias en Swift.

1: <https://github.com/malcommac/SwiftDate>

--------------------------------------

Tool-X es un instalador de herramientas de hackeo de Kali Linux. Tool-X desarrollado para termux y otros sistemas basados ​​en Linux. Con Tool-X, puede instalar casi más de 370 herramientas de piratería en la aplicación Termux y otras distribuciones basadas en Linux.

1: <https://github.com/rajkumardusad/Tool-X>

--------------------------------------

Instalar automáticamente todas las herramientas de Kali Linux

1: https://github.com/LionSec/katoolin

--------------------------------------

Un módulo de autenticación de solicitudes para el borrador del estándar RFC de la firma HTTP IETF

1: <https://github.com/pyauth/requests-http-signature>

--------------------------------------

🐙Obtenga diariamente 400-500 seguidores reales👽[BadRobo] es el mejor bot de Instagram disponible ahora con todas las funciones. ¡Nuestro BOT no violó ninguna de las reglas de Instagram, por lo que no tiene que preocuparse por obtener ACTION BLOCK!

1: <https://github.com/jaleelx98/Bad-Robo>

--------------------------------------

Herramienta OSINT para encontrar correo electrónico por nombre y apellido

1: <https://github.com/mishakorzik/MailFinder>

--------------------------------------

Hombre eficiente y avanzado en el marco medio.

1: <https://github.com/LionSec/xerosploit>

--------------------------------------

La herramienta realiza el ataque y la defensa del gemelo malvado.

1: <https://github.com/vection/Evil-Twin-tool>

--------------------------------------

Herramienta DarkFly V.4.0

1: <https://github.com/Ranginang67/DarkFly-Tool>

--------------------------------------

🔥Herramientas de pentest de Firecrack: ataque aleatorio de piratería de Facebook, desfiguración, buscador de administradores, Bing dorking:

1: <https://github.com/Ranginang67/Firecrack>

--------------------------------------

AOXdeface desfigura automáticamente muchos sitios web a la vez

1: <https://github.com/Ranginang67/AOXdeface>

--------------------------------------

🔍Crypton: herramientas linux Pentester, pruebas de penetración y piratería ética

1: https://github.com/Ranginang67/Crypton

--------------------------------------

MyServer es su propio servidor web localhost. Puede configurar servidores PHP, Apache, Nginx y MySQL en sus dispositivos Android o Linux como Ubuntu, etc. MyServer está desarrollado para terminales Android como Termux o GNURoot Debian terminal.

1: <https://github.com/rajkumardusad/MyServer>

--------------------------------------

Biblioteca de contraseñas de un solo uso de Ruby

1: <https://github.com/mdp/rotp>

--------------------------------------

El shell WinRM definitivo para hacking/pentesting

1: <https://github.com/Hackplayers/evil-winrm>

--------------------------------------

Un script bash para anonimizar la IP pública utilizada para navegar por Internet, administrar la conexión a la red TOR y a diferentes proveedores de VPN (OpenVPN)

1: <https://github.com/Hackplayers/4nonimizer>

--------------------------------------

Prueba de concepto de vulnerabilidad de suplantación de direcciones de Chrome para HTTPS. (Original de David Leo.)

1: <https://github.com/musalbas/address-spoofing-poc>

--------------------------------------

Generador de cuentas.

1: <https://github.com/v-Cx/aio-generator>

--------------------------------------

Penetration Testers Framework (PTF) es una forma de soporte modular para herramientas actualizadas.

1: <https://github.com/trustedsec/ptf#the-pentesters-framework-ptf>

--------------------------------------

Unicorn es una herramienta simple para usar un ataque de degradación de PowerShell e inyectar shellcode directamente en la memoria. Basado en los ataques powershell de Matthew Graeber y la técnica de derivación powershell presentada por David Kennedy (TrustedSec) y Josh Kelly en Defcon 18.

1: <https://github.com/trustedsec/unicorn>

--------------------------------------

Una herramienta simple para generar navegación web falsa y mitigar el seguimiento

1: <https://github.com/davideolgiati/PartyLoud>

--------------------------------------

Herramienta de prueba de seguridad para identificar si se puede acceder a una lista de archivos de registro comunes, que pueden usarse para el envenenamiento de registros, desde una vulnerabilidad de inclusión de archivos local conocida.

1: <https://github.com/B2dfir/LinuxPoisonableLogFinder>

--------------------------------------

Rastreador de ubicación DNS ESP32

1: <https://github.com/mdp/ESP32_DNS_Tracker>

--------------------------------------

Recopilar o buscar sitios web que son vulnerables a la inyección de sql (herramientas GUI)

1: <https://github.com/Ranginang67/WSS>

--------------------------------------

Configure y recupere mensajes de estado por cuenta con este simple contrato inteligente.

1: <https://github.com/near-examples/rust-status-message>

--------------------------------------

Herramientas OSINT para la Dark Web

1: <https://github.com/apurvsinghgautam/dark-web-osint-tools>

--------------------------------------

DaProfiler le permite obtener correos electrónicos, redes sociales, direcciones, trabajos y más en su objetivo utilizando técnicas de web scraping y google dorking, con sede solo en Francia. La particularidad de este programa es su capacidad para encontrar las direcciones de correo electrónico de su objetivo.

1: <https://github.com/daprofiler/DaProfiler>

--------------------------------------

LD\_PRELOAD rootkit

1: <https://github.com/mav8557/Father>

--------------------------------------

⚡Descifrar cifrados automáticamente sin conocer la clave o el cifrado, decodificar codificaciones y descifrar hashes⚡

1: <https://github.com/Ciphey/Ciphey>

--------------------------------------

BackDoor para controlar sitios basados ​​en php.

1: <https://github.com/yasserbdj96/hiphp>

--------------------------------------

Marco PyBotNet, control remoto de alto nivel

1: <https://github.com/onionj/pybotnet>

--------------------------------------

¡RATata es una RAT de python simple para configurar y usar!

1: <https://github.com/loTus04/RATata>

--------------------------------------

Le permite recuperar información sobre perfiles de Linkedin, empresas de Linkedin y búsqueda de empresas/personas de Linkedin.

1: <https://github.com/megadose/nqntnqnqmb>

--------------------------------------

holehe le permite verificar si el correo se usa en diferentes sitios como twitter, instagram y recuperará información en sitios con la función de contraseña olvidada.

1: <https://github.com/megadose/holehe>

--------------------------------------

ADB para piratas informáticos (:

1: <https://github.com/jxroot/adbwebkit>

--------------------------------------

Mobile Security Framework (MobSF) es una aplicación móvil todo en uno automatizada (Android/iOS/Windows) para pruebas de penetración, análisis de malware y marco de evaluación de seguridad capaz de realizar análisis estáticos y dinámicos.

1: <https://github.com/MobSF/Mobile-Security-Framework-MobSF>

--------------------------------------

Herramientas de DirAttack, archivo de búsqueda o directorio en el sitio web

1: <https://github.com/Ranginang67/DirAttack>

--------------------------------------

M-tonto, google tonteando con mdork

1: <https://github.com/Ranginang67/M-dork>

--------------------------------------

Pagodo (Passive Google Dork) – Automatice el raspado y la búsqueda de la base de datos de Google Hacking

1: <https://github.com/opsdisk/pagodo>

--------------------------------------

ScanT3r - Herramienta de automatización de recompensas de errores basada en módulos

1: https://github.com/knassar702/scant3r

--------------------------------------

Evildork apuntando a tu prometida👁️

1: <https://github.com/Fricciolosa-Red-Team/evildork>

--------------------------------------

DiNA puede buscar y reconocer patrones en secuencias de ADN.

1: <https://github.com/epsylon/DiaNA>

--------------------------------------

Orb es una herramienta de huella masiva.

1: <https://github.com/epsylon/orbrb>

--------------------------------------

Un script de shell tiene como objetivo lanzar automáticamente más de 50 herramientas de escaneo web en línea en el navegador contra un dominio de destino en 10 oleadas

1: <https://github.com/AhmedConstant/lazyGrandma>

--------------------------------------

Herramienta para adivinar el dominio de un correo electrónico en base a un parcial

1: <https://github.com/drooling/email-guesser>

--------------------------------------

Una herramienta OSINT de correo electrónico escrita en python3

1: <https://github.com/drooling/email-osint>

--------------------------------------

Número de teléfono Herramienta OSINT hecha en python3 (saca nombre del propietario del numero)

1: <https://github.com/drooling/phosint>

--------------------------------------

Herramienta gráfica de penetración de intranet Viper (serpiente de colores)

1: <https://github.com/FunnyWolf/Viper>

--------------------------------------

Omitir el firewall para el reenvío de tráfico mediante webshell Una herramienta fuera de la red que utiliza webshell para el reenvío de tráfico

1: <https://github.com/FunnyWolf/pystinger>

--------------------------------------

Generación automática de exploits (AEG) y captura remota de banderas para problemas de CTF explotables

1: <https://github.com/ChrisTheCoolHut/Zeratool>

--------------------------------------

Un webshell que puede eludir parte de la seguridad del sistema.

1: <https://github.com/saraiva/Gel4y-Mini-Shell-Backdoor>

--------------------------------------

Otra versión de katana pero más automatizada y menos estable. el propósito de esta pequeña herramienta es ejecutar un reconocimiento pasivo basado en Google contra su alcance.

1: <https://github.com/TebbaaX/GRecon>

--------------------------------------

Herramienta de Python que le brinda la capacidad de ejecutar consultas avanzadas de Google (conocidas como Google Dorks - Google Dorking)

1: <https://github.com/TebbaaX/Katana>

--------------------------------------

Dorothy es una herramienta para probar el monitoreo y detección de seguridad para entornos Okta

1: <https://github.com/elastic/dorothy>

--------------------------------------

BAT es una herramienta para ayudar a todos a proteger sus servidores web.

1: <https://github.com/AveCaesarMorituriTeSalutant/BAT_CORE>

--------------------------------------

Herramienta automatizada de explotación de inyección de comandos de sistema operativo todo en uno.

1: <https://github.com/commixproject/commix>

--------------------------------------

Encuentre inyecciones de encabezado de host y realice ataques de encabezado de host con otro tipo de errores como envenenamiento de caché web

1: <https://github.com/mr-medi/HostPanic>

--------------------------------------

Recopile información sobre un dominio y utilícela para planificar un vector de ataque

1: <https://github.com/mr-medi/phpRecon>

--------------------------------------

Subbuscador de llamadas con un clic + ksubdominio + httpx poderosa combinación de descubrimiento de nombre de dominio -> verificación de nombre de dominio -> obtener título de nombre de dominio, tamaño de respuesta de código de estado y finalmente guardar el resultado, simplificar la operación comando operación electrica

1: <https://github.com/Mr-xn/subdomain_shell>

--------------------------------------

Sistema de automatización basado en reglas YARA para detectar ataques de red a nivel de byte

1: <https://github.com/karthikgenius/YaraCapper>

--------------------------------------

ODAT: herramienta de ataque a la base de datos de Oracle

1: <https://github.com/quentinhardy/odat>

--------------------------------------

Un paquete Zeek para detectar el tráfico de red de comando y control (C2) del túnel ICMP del malware Pingback.

1: <https://github.com/corelight/pingback>

--------------------------------------

Encuentre expresiones regulares que son vulnerables a ReDoS (Denegación de servicio de expresiones regulares)

1: <https://github.com/doyensec/regexploit>

--------------------------------------

Un analizador de encabezados HTTP humilde, rápido y orientado a la seguridad

1: <https://github.com/rfc-st/humble>

--------------------------------------

Cobra puede robar información del sistema del sistema de Windows y luego enviarla a un correo electrónico de su elección

1: <https://github.com/SxNade/Cobra>

--------------------------------------

Verifique si los nombres de usuario de tiktok están disponibles o tomados

1: <https://github.com/drooling/tiktok-checker>

--------------------------------------

(No se que es a lo mejor en un futuro tiene utilidad por eso lo guardo en el word)

1: <https://github.com/juanluidos/OsintSpector>

--------------------------------------

ETWProcessMon2 es para monitorear procesos/subprocesos/memoria/cargas de imágenes/TCPIP a través de ETW + detección para inyección remota de subprocesos y detección de carga útil mediante eventos VirtualMemAlloc (en memoria), etc.

1: <https://github.com/DamonMohammadbagher/ETWProcessMon2>

--------------------------------------

MikrotikSploit es un script que busca y explota las vulnerabilidades de la red Mikrotik

1: <https://github.com/0x802/MikrotikSploit>

--------------------------------------

Meterpreter Reverse shell sobre la red TOR usando servicios ocultos

1: <https://github.com/CalfCrusher/Poiana>

--------------------------------------

capturas de paquetes de ataques ddos ​​del mundo real

1: <https://github.com/StopDDoS/packet-captures>

--------------------------------------

Esta herramienta solo tiene fines educativos: Layer-7 o HTTP FLOODER

1: <https://github.com/NumeXx/Layer-7-Flooder>

--------------------------------------

Instagram Story View Bot Unencrypted Story Views es una herramienta útil que permite que miles de personas vean tus publicaciones. Es completamente gratis, la fuente es visible para que cualquiera la modifique Escriba su nombre de usuario, espere a que el bot automatice la tarea.

1: <https://github.com/5l1v3r1/Instagram-Story-Views>

--------------------------------------

Bot de Instagram para la interacción automatizada de Instagram usando un dispositivo Android a través de ADB

1: <https://github.com/alexal1/Insomniac>

--------------------------------------

Certonid es una autoridad de certificación SSH sin servidor

1: <https://github.com/certonid/certonid>

--------------------------------------

⬆️ ☠️ 🔥Privesc automático de Linux a través de la explotación de la fruta madura, por ejemplo, gtfobins, pwnkit, tubería sucia, +w docker.sock

1: <https://github.com/liamg/traitor>

--------------------------------------

Una interfaz de usuario de depuración hacky para piratas informáticos

1: <https://github.com/snare/voltron>

--------------------------------------

Sistema de clasificación de secuencias taxonómicas de Kraken

1: <https://github.com/DerrickWood/kraken>

--------------------------------------

Base de datos actualizada cada hora de exploits e informes de explotación

1: <https://github.com/gmatuz/inthewilddb>

--------------------------------------

SMBeagle: herramienta de auditoría de archivos compartidos.

1: <https://github.com/punk-security/smbeagle>

--------------------------------------

My Personal Nvim Config – Web Dev Ready – Minimalista – Ligero – Escrito en Pure Lua

1: <https://github.com/c99tn/vMass>

--------------------------------------

Evadir Windows Defender y AMSI con firmas actualizadas.

Probado Windows 11 Pro.

1: <https://github.com/HernanRodriguez1/MimikatzFUD>

--------------------------------------

Este script permite encontrar vulnerabilidades XSS con núcleos, aprovechando este recurso en su máxima capacidad de análisis.

1: <https://github.com/HernanRodriguez1/Bypass-AMSI>

--------------------------------------

Este script permite encontrar vulnerabilidades de MySQLi Basado en Errores con núcleos, aprovechando este recurso en su máxima capacidad de análisis.

1: <https://github.com/HernanRodriguez1/ScanReflectedXSS>

--------------------------------------

Compilación: Rubeus 1.4.2 (x64 x32)

Probado: Microsoft Windows 11 Pro – 10.0.22000 N/D Compilación 22000

1: <https://github.com/HernanRodriguez1/ScanMySQLiErrorBased-Nuclei>

--------------------------------------

Este script está basado en el de Nishang, gracias por compartir

1: <https://github.com/HernanRodriguez1/1nv0k3-Rvb3us2>

--------------------------------------

Este script permite encontrar vulnerabilidades XSS con núcleos, aprovechando este recurso en su máxima capacidad de análisis.

1: <https://github.com/HernanRodriguez1/RevershellTCP_BypassAMSI>

--------------------------------------

Este script permite encontrar vulnerabilidades XSS con núcleos, aprovechando este recurso en su máxima capacidad de análisis.

1: <https://github.com/HernanRodriguez1/ScanReflectedXSS>

--------------------------------------

Observador simple basado en cli, detecta transferencias USDT de ballenas y genera los detalles de tx, funciona con cualquier token ERC-20.

1: <https://github.com/c99tn/USDT-whales-watcher>

--------------------------------------

Urraca secreta - Herramienta de detección de secretos

1: <https://github.com/punk-security/secret-magpie-cli>

--------------------------------------

Repositorio pwnspoof

1: <https://github.com/punk-security/pwnspoof>

--------------------------------------

Colección de técnicas de inyección de shellcode empaquetadas en un archivo DLL armado D/Invoke

1: <https://github.com/snovvcrash/DInjector>

--------------------------------------

Seguimiento del historial de eventos USB en GNU/Linux

1: <https://github.com/snovvcrash/usbrip>

--------------------------------------

Script de Python con tecnología de Selenium para automatizar la búsqueda de aplicaciones web vulnerables.

1: <https://github.com/NullArray/DorkNet>

--------------------------------------

Explotador masivo automatizado

1: <https://github.com/NullArray/AutoSploit>

--------------------------------------

Instalador de paquete/paquete de inteligencia y reconocimiento.

1: <https://github.com/NullArray/IntRec-Pack>

--------------------------------------

Un script Bash que descarga y descomprime scripts que ayudarán con la escalada de privilegios en un sistema Linux.

1: <https://github.com/NullArray/RootHelper>

--------------------------------------

Detección de dominios phishing y usurpación de dominios. Admite permutaciones como ataque homógrafo, typosquatting y bitsquatting.

1: <https://github.com/atenreiro/opensquat>

--------------------------------------

Obtener códigos de estado HTTP para una lista de URL

1: <https://github.com/c0brabaghdad1/list-urls-to-http-status-codes>

--------------------------------------

robar contraseñas guardadas de Chrome "indetectables"

1: <https://github.com/De3vil/steal_ps>

--------------------------------------

SteaLinG es un marco de prueba de penetración de código abierto diseñado para la ingeniería social

1: <https://github.com/De3vil/SteaLinG>

--------------------------------------

AV evadiendo OSX Backdoor y Crypter Framework

1: <https://github.com/SubGlitch1/OSRipper>

--------------------------------------

Un simple script para verificar los privilegios incluidos en su token de acceso

1: <https://github.com/stark0de/tokenpriv>

--------------------------------------

Sencilla herramienta para buscar en tiempo real posibles fugas de información en los logs de una app Android

1: <https://github.com/stark0de/logcat-strings>

--------------------------------------

Esta herramienta es útil para encontrar una cadena en particular en una lista de URL usando las capacidades de OCR (reconocimiento óptico de caracteres) de tesseract.

1: <https://github.com/stark0de/ocr-recon>

--------------------------------------

Herramienta de descubrimiento y explotación de inclusión de archivos locales

1: <https://github.com/hansmach1ne/lfimap>

--------------------------------------

El destino es la botnet IRC, que se utiliza principalmente para lanzar ataques de denegación de servicio. Propagación mediante exploración aleatoria o de alcance en el puerto SSH y HTTP predeterminado.

1: <https://github.com/boz3r/Fatebot>

--------------------------------------

50+ Gadgets (20 Más que ysoserial). JNDI-Injection-Exploit-Plus es una herramienta para generar enlaces JNDI viables y proporcionar servicios en segundo plano iniciando el servidor RMI, el servidor LDAP y el servidor HTTP.

1: <https://github.com/cckuailong/JNDI-Injection-Exploit-Plus>

--------------------------------------

PowerHuntShares es un script de auditoría diseñado para inventariar, analizar e informar privilegios excesivos configurados en dominios de Active Directory.

1: <https://github.com/NetSPI/PowerHuntShares>

--------------------------------------

Paracosme es un exploit de corrupción de memoria remota con un clic cero que compromete ICONICS Genesis64.

1: <https://github.com/0vercl0k/paracosme>

--------------------------------------

PowerUpSQL: un kit de herramientas de PowerShell para atacar SQL Server

1: <https://github.com/NetSPI/PowerUpSQL>

--------------------------------------

Nginxpwner es una herramienta simple para buscar errores de configuración y vulnerabilidades comunes de Nginx.

1: <https://github.com/stark0de/nginxpwner>

--------------------------------------

📧Un ejemplo del uso de un formulario HTML (por ejemplo: "Contáctenos" en un sitio web) para enviar correo electrónico sin un servidor backend (usando un script de Google) perfecto para sitios web estáticos que necesitan recopilar datos.

1: <https://github.com/dwyl/learn-to-send-email-via-google-script-html-no-server>

--------------------------------------

¡25 honeypots diferentes en un solo paquete pypi! (dns, ftp, httpproxy, http, https, imap, mysql, pop3, postgres, redis, smb, smtp, socks5, ssh, telnet, vnc, mssql, elastic, ldap, ntp, memcache, snmp, oracle, sorbo e irc)

1: <https://github.com/qeeqbox/honeypots>

--------------------------------------

Obtenga acceso a la pantalla del usuario y la cámara web con esta herramienta.

1: <https://github.com/juuleeh/python-rat>

--------------------------------------

AlphaWeb XE, el servidor web integrado que se ejecuta en AlphaCom XE, tiene una vulnerabilidad que permite cargar archivos PHP que conducen a RCE una vez que la autenticación es exitosa:

1: <https://ricardojoserf.github.io/CVE-2021-40845/>

--------------------------------------

Un script para probar las credenciales contra los Servicios de federación de Active Directory (ADFS), lo que permite la difusión de contraseñas o ataques de fuerza bruta.

1: <https://github.com/ricardojoserf/adfsbrute>

--------------------------------------

🍁¿Lo mejor? ProxyScrapper

1: <https://github.com/Its-Vichy/ProxyHeast>

--------------------------------------

Una herramienta de análisis estático para asegurar el código Go

1: <https://github.com/praetorian-inc/gokart>

--------------------------------------

Una herramienta de rastreo de paquetes de red desarrollada en Python 3.

1: <https://github.com/EONRaider/Packet-Sniffer>

--------------------------------------

AERoot es una herramienta de línea de comandos que le permite otorgar privilegios de raíz sobre la marcha a cualquier proceso que se ejecute en el emulador de Android con AVD de Google Play.

1: <https://github.com/quarkslab/AERoot>

--------------------------------------

Trojan Rat Builder(310), Ransomware Builder(7), Crypter(72), Miner(9), Worm(8), Botnet(25), Virus Builder(9), Binder(25), Exploit(7), Keylogger & Stealer(40), Proxy Tool(9), Spoofer(11), Programa falso y Virus de muestra(64),Otros y herramientas(16). Alrededor de 610 herramientas, que puedes usar para Hackear.

1: <https://github.com/hktkqwe123/All-Hacking-Tools>

--------------------------------------

Kit de herramientas de monitoreo y captura de DNS pasivo

1: <https://github.com/mosajjal/dnsmonster>

--------------------------------------

Túnel de DNS cifrado de extremo a extremo y marco C2

1: <https://github.com/mosajjal/dnspot>

--------------------------------------

Cambia tu dirección IP

1: <https://github.com/shubhamg0sai/ip_changer>

--------------------------------------

Analice, extraiga y visualice funciones, artefactos e IoC de archivos y volcados de memoria (Windows, Linux, Android, iPhone, Blackberry, archivos binarios de macOS, correos electrónicos y más)

1: <https://github.com/qeeqbox/analyzer>

--------------------------------------

API, CLI y aplicación web para analizar y encontrar el perfil de una persona en 1000 redes sociales \ sitios web

1: <https://github.com/qeeqbox/social-analyzer>

--------------------------------------

Automatizador de comercio para el intercambio de criptomonedas.

1: <https://github.com/dallyshalla/tropix>

--------------------------------------

Herramienta para generar listas de palabras inteligentes y potentes

1: <https://github.com/r3nt0n/bopscrk>

--------------------------------------

Herramienta de automatización de ataques DDoS a través de la red Tor

1: <https://github.com/r3nt0n/torDDoS>

--------------------------------------

SDK de veredicto como servicio: analice archivos en busca de contenido malicioso

1: <https://github.com/GDATASoftwareAG/vaas>--------------------------------------

Atasco de WiFi. Desconecta a cualquiera de cualquier wifi o punto de acceso. Envía un paquete diseñado para desconectar al usuario de WiFi.

1: <https://github.com/tusharkeshav/wifi-jam>

--------------------------------------

Discordia, Twitter, cookies de Instagram y capturador de fichas

1: <https://github.com/h4x0r-project/CookedGrabber>

--------------------------------------

🔍Un editor hexadecimal para ingenieros inversos, programadores y personas que valoran sus retinas cuando trabajan a las 3 de la mañana.

1: <https://github.com/WerWolv/ImHex>

--------------------------------------

Implementación de PyTorch del aprendizaje de representación de similitud de región (ReSim)

1: <https://github.com/Tete-Xiao/ReSim>

--------------------------------------

Software de ingeniería inversa utilizando un simulador de sistema completo

1: <https://github.com/mfthomps/RESim>

--------------------------------------

Google se vuelve loco para obtener fácilmente algunos tokens de bots de Discord

1: <https://github.com/Traumatism/get-discord-bots-tokens-with-google>

--------------------------------------

Herramienta OSINT de Python personalizable para recopilar información y engañar a las personas

1: <https://github.com/kl3sshydra/UltraCyberStalk>

--------------------------------------

Plataforma de ingeniería inversa gratuita y de código abierto impulsada por rizin

1: <https://github.com/rizinorg/cutter>

--------------------------------------

Una herramienta de cazadores de errores para encontrar muchas vulnerabilidades usando Google dorks

1: <https://github.com/gokulapap/bugdork>

--------------------------------------

Rastreador en línea de Whatsapp📲[Obtener la notificación🔔e historia📜de en línea]

1: <https://github.com/rizwansoaib/whatsapp-monitor>

--------------------------------------

Sitio web intencionalmente vulnerable para LFI y envenenamiento/contaminación de registros.

1: <https://github.com/F3dai/log-poison>

--------------------------------------

Herramienta de administración remota para Windows

1: <https://github.com/quasar/Quasar>

--------------------------------------

👻RAT (troyano de acceso remoto) – Botnet silencioso – Acceso remoto completo a la línea de comandos – Descarga y ejecución de programas – Propagación de virus y malware

1: <https://github.com/AHXR/ghost>

--------------------------------------

API REST vulnerable con las 10 principales vulnerabilidades de OWASP para pruebas de seguridad

1: <https://github.com/erev0s/VAmPI>

--------------------------------------

Escanear cifrados SSH

1: <https://github.com/evict/SSHScan>

--------------------------------------

Vaf es un fuzzer web multiplataforma muy avanzado y rápido escrito en nim

1: <https://github.com/d4rckh/vaf>

--------------------------------------

Morpheus – Automatización de Ettercap TCP/IP (herramienta de secuestro MITM)

1: <https://github.com/r00t-3xp10it/morpheus>

--------------------------------------

Página cautiva configurable para servicios WiFi públicos/privados que brinda inicio de sesión, registro, inicio de sesión social, verificación por SMS, cambio de contraseña, restablecimiento de contraseña, cambio de número de teléfono y más.

1: <https://github.com/openwisp/openwisp-wifi-login-pages>

--------------------------------------

HackingPro - ¡Hackea como un profesional!

1: <https://github.com/Anlominus/HacKingPro>

--------------------------------------

Obtiene la conexión más fuerte e inicia sesión en Jarvis

1: <https://github.com/arstevens/BluetoothLogin>

--------------------------------------

Curso de pruebas de penetración oscp por s4vitar

1: <https://gist.github.com/s4vitar/b88fefd5d9fbbdcc5f30729f7e06826e>

--------------------------------------

Preparación para el OSWP (by s4vitar)

1: <https://gist.github.com/s4vitar/3b42532d7d78bafc824fb28a95c8a5eb>

--------------------------------------

Herramienta de seguridad cibernética para piratear conexiones inalámbricas utilizando herramientas Kali integradas. Admite todos los valores (WEP, WPS, WPA, WPA2/TKIP/IES)

1: <https://github.com/ankit0183/Wifi-Hacking>

--------------------------------------

Esta herramienta configurará su puerta trasera/rootkits cuando la puerta trasera ya esté configurada, ocultará su proceso específico, su sesión será ilimitada en Metasploit y será transparente. Incluso cuando mató, se volverá a ejecutar. Siempre hay un proceso que mientras ejecuta otro proceso, por lo que podemos suponer que este proceso es imparable como un fantasma en el caparazón.

1: <https://github.com/screetsec/Vegile>

--------------------------------------

Solucionador de cadenas ofuscadas FLARE: extraiga automáticamente cadenas ofuscadas del malware.

1: <https://github.com/mandiant/flare-floss>

--------------------------------------

Complete Mandiant Offensive VM (Commando VM), una distribución de máquina virtual de pentesting basada en Windows totalmente personalizable. [comandovm@fireeye.com](mailto:comandovm@fireeye.com)

1: <https://github.com/mandiant/commando-vm>

--------------------------------------

La herramienta de código abierto del equipo FLARE para identificar capacidades en archivos ejecutables.

1: <https://github.com/mandiant/capa>

--------------------------------------

La navaja suiza a juego con el patrón

1: <https://github.com/VirusTotal/yara>

--------------------------------------

Seguimiento de dispositivos WiFi con la intensidad de la señal recibida

1: <https://github.com/90N45-d3v/dBmonster>

--------------------------------------

Una demostración de dbmon ejecutándose en las ramas idempotent-rerender de Ember y HTMLBars

1: <https://github.com/wycats/dbmonster>

--------------------------------------

Automatización de rastreo de red con Bettercap como AP no autorizado o como cliente en su red

1: <https://github.com/90N45-d3v/BetterSniff>

--------------------------------------

Una aplicación sencilla que te permite visualizar dónde has estado

1: <https://github.com/globalpolicy/PhoneMapper>

--------------------------------------

Una secuencia de comandos de Python para verificar si un artículo está en stock principalmente para Amazon, pero también se puede adaptar a otros sitios.

1: <https://github.com/zer0mania/amazon-stock-notifier>

--------------------------------------

Un simple script de utilidad que deja de seguir a todos los usuarios en Github que no se preocupan lo suficiente como para seguirte.

1: <https://github.com/arnavb/github_unfollower.py>

--------------------------------------

Dorothy es una herramienta para probar el monitoreo y detección de seguridad para entornos Okta

1: <https://github.com/elastic/dorothy>

--------------------------------------

Aplicación de comunicación de malla inalámbrica independiente de Internet

1: <https://github.com/qaul/qaul.net>

--------------------------------------

Firmware ESP8266 para realizar ataques de desautenticación con facilidad.

1: <https://github.com/samdenty/Wi-PWN>

--------------------------------------

Un cliente Rust HTTP fácil y potente

1: <https://github.com/seanmonstar/reqwest>

--------------------------------------

Visualice la intensidad de la señal Wi-Fi en un área geográfica

1: <https://github.com/ecoAPM/WiFiSurveyor>

--------------------------------------

Un complemento de Firefox para investigaciones OSINT

1: <https://github.com/vincenzocaputo/FoxyRecon>

--------------------------------------

Escanee activos de acceso público en su entorno de nube de AWS

1: <https://github.com/9rnt/poro>

--------------------------------------

Kit de herramientas de monitoreo y captura de DNS pasivo

1: <https://github.com/mosajjal/dnsmonster>

--------------------------------------

Túnel de DNS cifrado de extremo a extremo y marco C2

1: <https://github.com/mosajjal/dnspot>

--------------------------------------

PVR y guía de episodios que descarga y administra todos tus programas de TV

1: <https://github.com/midgetspy/Sick-Beard>

--------------------------------------

Un módulo de Python para eludir la página anti-bot de Cloudflare.

1: <https://github.com/VeNoMouS/cloudscraper>

--------------------------------------

Interfaz fácil de usar para la API de TheTVDB.com en Python

1: <https://github.com/dbr/tvdb_api>

--------------------------------------

AndroBugs Framework es un escáner de vulnerabilidades de Android eficiente que ayuda a los desarrolladores o investigadores de seguridad a encontrar posibles vulnerabilidades de seguridad en las aplicaciones de Android.

1: <https://github.com/androbugs2/androbugs2>

--------------------------------------

Una herramienta de línea de comandos para detectar vulnerabilidades en las dependencias de Python y realizar instalaciones seguras de paquetes

1: <https://github.com/ochronasec/ochrona-cli>

--------------------------------------

Alerta diaria cuando se registra un nuevo nombre de dominio y contiene sus palabras clave

1: <https://github.com/pixelbubble/DomainAlerting>

--------------------------------------

Scrape Pastebin API para recopilar pegados diarios, configurar una lista de palabras y recibir alertas por correo electrónico cuando tenga una coincidencia.

1: <https://github.com/pixelbubble/PasteMonitor>

--------------------------------------

Un analizador push para el protocolo HTTP 1.x en Rust.

1: <https://github.com/seanmonstar/httparse>

--------------------------------------

Encuestas Wi-Fi: conducción, conjuntos de datos, estadísticas, herramientas y más.

1: <https://github.com/domienschepers/wifi-surveying>

--------------------------------------

Mininode es una herramienta CLI para reducir la superficie de ataque de las aplicaciones Node.js mediante el uso de análisis estático.

1: <https://github.com/wspr-ncsu/mininode>

--------------------------------------

Realice ataques MiTM avanzados en sitios web con facilidad💉

1: <https://github.com/samdenty/injectify>

--------------------------------------

Panel para la botnet HTTP UBoat

1: <https://github.com/UBoat-Botnet/UBoat-Panel>

--------------------------------------

Herramienta simple para inundación de SMS usando muchas api

1: <https://github.com/youhacker55/SMSFlooder>

--------------------------------------

Shreder es una poderosa herramienta de fuerza bruta de contraseñas de protocolo SSH de subprocesos múltiples.

1: <https://github.com/entysec/shreder>

--------------------------------------

Scrape Pastebin API para recopilar pegados diarios, configurar una lista de palabras y recibir alertas por correo electrónico cuando tenga una coincidencia.

1: <https://github.com/pixelbubble/PasteMonitor>

--------------------------------------

Alerta diaria cuando se registra un nuevo nombre de dominio y contiene sus palabras clave

1: <https://github.com/pixelbubble/DomainAlerting>

--------------------------------------

ProtOSINT es un script de Python que lo ayuda a investigar las cuentas de Protonmail y las direcciones IP de ProtonVPN

1: <https://github.com/pixelbubble/ProtOSINT>

--------------------------------------

Módulos para recibir y transmitir streams ADAT

1: <https://github.com/xcore/sc_adat>

--------------------------------------

ADAT es una pequeña herramienta que se utiliza para ayudar a los jugadores de CTF y a los probadores de penetración con comandos fáciles de ejecutar en un controlador de dominio de Active Directory. Esta herramienta se utiliza mejor utilizando un conjunto de credenciales conocidas contra el host.

1: <https://github.com/The-Viper-One/ActiveDirectoryAttackTool>

--------------------------------------

Un shell inverso para Linux. Escrito en Python3.

1: <https://github.com/Keyj33k/ReverseShell>

--------------------------------------

Hunter-Toolkit, un asistente confiable para probadores de penetración.

1: <https://github.com/Keyj33k/Hunter-Toolkit>

--------------------------------------

ToRat es una herramienta de administración remota escrita en Go que utiliza Tor como mecanismo de transporte y RPC para la comunicación.

1: <https://github.com/lu4p/ToRat>

--------------------------------------

RomBuster es una herramienta de explotación de enrutadores que permite revelar la contraseña de administrador del enrutador de red.

1: <https://github.com/EntySec/RomBuster>

--------------------------------------

ReconPal: Aprovechando la PNL para Infosec

1: <https://github.com/pentesteracademy/reconpal>

--------------------------------------

VoIPShark es una plataforma de análisis de VoIP de código abierto que permitirá a las personas analizar el tráfico de VoIP en vivo o almacenado, descifrar fácilmente el flujo SRTP cifrado, realizar análisis de macros, generar un resumen específico para el tráfico/nodos de VoIP y exportar llamadas/SMS/DTMF en un archivo popular fácil de usar. Formatos.

1: <https://github.com/pentesteracademy/voipshark>

--------------------------------------

PA Toolkit es una colección de complementos de análisis de tráfico centrados en la seguridad

1: <https://github.com/pentesteracademy/patoolkit>

--------------------------------------

una extensión de eructo para la generación dinámica de carga útil para detectar fallas de inyección (RCE, LFI, SQLi), crea sesiones de usuario basadas en matriz de acceso para detectar problemas de autenticación/autorización y convierte las solicitudes Http a Javascript para una mayor explotación de XSS y más.

1: <https://github.com/volkandindar/agartha>

--------------------------------------

PowerShell Pass The Hash Utils

1: <https://github.com/Kevin-Robertson/Invoke-TheHash>

--------------------------------------

Prowler es una herramienta de seguridad de código abierto para realizar evaluaciones de mejores prácticas de seguridad, auditorías, respuesta a incidentes, monitoreo continuo, fortalecimiento y preparación forense de AWS. Contiene más de 240 controles que cubren CIS, PCI-DSS, ISO27001, GDPR, HIPAA, FFIEC, SOC2, AWS FTR, ENS y marcos de seguridad personalizados.

1: <https://github.com/prowler-cloud/prowler>

--------------------------------------

RIPPL es una herramienta que abusa de un modo de usuario solo para manipular procesos PPL en Windows

1: <https://github.com/last-byte/RIPPL>

--------------------------------------

La mejor herramienta de reconocimiento de Internet de las cosas/Sistemas de control industrial.

1: <https://github.com/woj-ciech/Kamerka-GUI>

--------------------------------------

Una plataforma para construir proxies para eludir las restricciones de la red.

1: <https://github.com/v2fly/v2ray-core>

--------------------------------------

Shell inverso de TCP asíncrono de PowerShell

1: <https://github.com/JoelGMSec/PSAsyncShell>

--------------------------------------

Company Passwords Profiler (también conocido como ComPP) ayuda a crear una lista de palabras de fuerza bruta para una empresa objetivo.

1: <https://github.com/sec-it/ComPP>

--------------------------------------

ShellCheck, una herramienta de análisis estático para scripts de shell

1: <https://github.com/koalaman/shellcheck>

--------------------------------------

Un deofuscador de Javascript

1: <https://github.com/PerimeterX/Restringer>

--------------------------------------

Visualización de datos para equipos azules

1: <https://github.com/WithSecureLabs/detectree>

--------------------------------------

Navaja suiza Webserver en Golang. Manténgase simple como Python SimpleHTTPServer pero con muchas características

1: <https://github.com/nodauf/Swego>

--------------------------------------

Marco de explotación de la nube

1: <https://github.com/teamssix/cf>

--------------------------------------

modDetective es una pequeña herramienta de Python que cronifica los archivos según el tiempo de modificación para investigar la actividad reciente del sistema.

1: <https://github.com/itsKindred/modDetective>

--------------------------------------

Servidor ssh vinculado estáticamente con funcionalidad de shell inverso para CTF y similares

1: <https://github.com/Fahrj/reverse-ssh>

--------------------------------------

Una sencilla utilidad de PowerShell que se utiliza para pasar a redes internas a través de un host de Windows comprometido.

1: <https://github.com/itsKindred/winPortPush>

--------------------------------------

¡Supervise la creación, la eliminación y los cambios en los objetos LDAP en vivo durante su pentest o administración del sistema!

1: <https://github.com/p0dalirius/LDAPmonitor>

--------------------------------------

Un rootkit independiente de Python 3 para Windows 10/Linux que utiliza Tor.

1: <https://github.com/emcruise/tor-rootkit>

--------------------------------------

Herramienta en Bash para realizar una enumeración básica y extraer la información más relevante de un Directorio Activo vía rpcclient.

1: <https://github.com/m4lal0/RPCrecon>

--------------------------------------

Herramienta de ingeniería social (Creador de puerta trasera con Reverse Shell para Windows/Android) con Ngrok.

1: <https://github.com/m4lal0/backdoorPhish>

--------------------------------------

NO USE ESTO EN CLASE NI PARA INTERRUMPIR LA CLASE OK!!!!

1: <https://github.com/lockness-Ko/google-meet-trolling-toolkit>

--------------------------------------

¡Realice una investigación forense de dominios sospechosos, sitios web y otras cosas peligrosas sin temor a ser infectado! Un sistema operativo en vivo y una imagen acoplable para ocultarse al enrutar todo su tráfico a través de TOR

1: <https://github.com/lockness-ko/wot>

--------------------------------------

firewall sin estado con reglas similares a yara en python

1: <https://github.com/coraltk/pkt>

--------------------------------------

Zero-attacker es una herramienta de piratería multipropósito con más de 24 herramientas como token-gen, ddos ​​y más (código público en algún momento)

1: <https://github.com/AsjadOooO/Zero-attacker>

--------------------------------------

Zero-attacker es una herramienta de piratería multipropósito con más de 24 herramientas como token-gen, ddos ​​y más (código público en algún momento)

1: <https://github.com/AsjadOooO/Zero-attacker>

--------------------------------------

Escáner web de próxima generación

1: <https://github.com/urbanadventurer/WhatWeb>

--------------------------------------

bingip2hosts es un web scraper de Bing.com que descubre sitios web por dirección IP

1: <https://github.com/urbanadventurer/bing-ip2hosts>

--------------------------------------

Un complemento OWASP ZAPROXY que permite probar las vulnerabilidades de las aplicaciones web mediante la grabación de secuencias complejas de varios pasos. Puede probar aplicaciones que necesitan acceder a páginas en un orden específico, como carritos de compras o registro de información de miembros.

1: <https://github.com/gdgd009xcd/AutoMacroBuilderForZAP>

--------------------------------------

Shells de PHP que funcionan en Linux OS, macOS y Windows OS.

1: <https://github.com/ivan-sincek/php-reverse-shell>

--------------------------------------

Omita los códigos de estado de respuesta HTTP 4xx y más. Basado en PycURL.

1: <https://github.com/ivan-sincek/forbidden>

--------------------------------------

Encuentre inyecciones de encabezado de host y realice ataques de encabezado de host con otro tipo de errores como envenenamiento de caché web

1: <https://github.com/mr-medi/HostPanic>

--------------------------------------

Recopile información sobre un dominio y utilícela para planificar un vector de ataque

1: <https://github.com/mr-medi/phpRecon>

--------------------------------------

Un conjunto de herramientas para el reconocimiento web, es rápido y fácil de usar.

1: <https://github.com/whoamisec75/httpsuite>

--------------------------------------

Métodos de derivación 403/401 + Automatización Bash + Su apoyo😉

1: <https://github.com/Dheerajmadhukar/4-ZERO-3>

--------------------------------------

DetectionLabELK es una bifurcación de DetectionLab con pila ELK en lugar de Splunk.

1: <https://github.com/cyberdefenders/DetectionLabELK>

--------------------------------------

Herramienta para encontrar la IP real detrás de CDN/WAF como cloudflare usando reconocimiento pasivo recuperando el hash de favicon. Para el mismo valor hash, se buscan todas las IP, PUERTOS y Certificados SSL/TLS posibles para validar el objetivo dentro del alcance.

1: <https://github.com/Dheerajmadhukar/Lilly>

--------------------------------------

Laboratorios forenses digitales prácticos y gratuitos para estudiantes y profesores

1: <https://github.com/frankwxu/digital-forensics-lab>

--------------------------------------

Conjunto de herramientas para auditar sistemas VoIP basados ​​en SIP

1: <https://github.com/Pepelux/sippts>

--------------------------------------

ClusterFuzzLite: fuzzing continuo simple que se ejecuta en CI.

1: <https://github.com/google/clusterfuzzlite>

--------------------------------------

La forma más fácil y segura de acceder a la infraestructura.

1: <https://github.com/gravitational/teleport>

--------------------------------------

AD Enum es una herramienta de pentesting que permite encontrar errores de configuración a través del protocolo LDAP y explotar algunas de esas debilidades con kerberos.

1: <https://github.com/SecuProject/ADenum>

--------------------------------------

Este es un PoC para eludir UAC mediante el secuestro de DLL y el abuso de la verificación de "Directorios de confianza".

1: <https://github.com/SecuProject/DLLHijackingScanner>

--------------------------------------

Snap Scraper permite a los usuarios descargar medios cargados en Snap Map de Snapchat utilizando un conjunto de coordenadas de latitud y longitud.

1: <https://github.com/rhematt/Snap-Scraper>

--------------------------------------

Ataques previos a la conexión, obtención de acceso y ataques posteriores a la conexión en WEP, WPA y WPA2.🛰✔️

1: <https://github.com/JulienFink/WiFi-Project>

--------------------------------------

Whoami proporciona privacidad mejorada, anonimato para las distribuciones de Linux basadas en Debian y Arch

1: <https://github.com/owerdogan/whoami-project>

--------------------------------------

Herramienta de enumeración de nombres de usuario y rociado de contraseñas dirigida a Microsoft O365.

1: <https://github.com/0xZDH/o365spray>

--------------------------------------

Oculte su carga útil en un archivo .jpg

1: <https://github.com/Tsuyoken/ImgBackdoor>

--------------------------------------

Plataforma de análisis de similitud de malware IoT

1: <https://github.com/mucoze/Umay>

--------------------------------------

¡TREVORspray es un rociador de contraseñas modular con subprocesos, proxy inteligente, módulos de botín y más!

1: <https://github.com/blacklanternsecurity/TREVORspray>

--------------------------------------

WSOB es una herramienta de Python creada para explotar la nueva vulnerabilidad en WSO2 asignada como CVE-2022-29464.

1: <https://github.com/oppsec/WSOB>

--------------------------------------

🦁Juumla es una herramienta de Python creada para identificar la versión de Joomla, buscar vulnerabilidades y buscar archivos de configuración o de copia de seguridad.

1: <https://github.com/oppsec/juumla>

--------------------------------------

🕵️Pinkerton es un rastreador de archivos JavaScript y un buscador de secretos desarrollado en Python

1: <https://github.com/oppsec/Pinkerton>

--------------------------------------

[DEPRECATED]Un nuevo motor de detección de inyección de SQL creado sobre tokenización de SQL y análisis de sintaxis.

1: <https://github.com/chaitin/sqlchop>

--------------------------------------

herramientas de veinmind

1: <https://github.com/chaitin/veinmind-tools>

--------------------------------------

Jarbou3 es una herramienta rat codificada en python con C&C que puede aceptar múltiples conexiones de clientes

1: <https://github.com/youhacker55/jarbou3>

--------------------------------------

Herramientas inversas y dormidas

1: <https://github.com/tegal1337/Akuma>

--------------------------------------

Una extensión del navegador que cifra sus comunicaciones con muchos sitios web que ofrecen HTTPS pero aún permiten conexiones sin cifrar.

1: <https://github.com/EFForg/https-everywhere>

--------------------------------------

✉️Script de Python que genera una nueva cuenta de Gmail con credenciales aleatorias

1: <https://github.com/stav121/gmail-generator>

--------------------------------------

Desofusque las cargas útiles de Log4Shell con facilidad.

1: <https://github.com/ox-eye/Ox4Shell>

--------------------------------------

ORM para TypeScript y JavaScript (ES7, ES6, ES5). Admite bases de datos MySQL, PostgreSQL, MariaDB, SQLite, MS SQL Server, Oracle, SAP Hana, WebSQL. Funciona en las plataformas NodeJS, Browser, Ionic, Cordova y Electron.

1: <https://github.com/typeorm/typeorm>

--------------------------------------

Omisión de UAC al abusar de RPC y objetos de depuración.

1: <https://github.com/Kudaes/Elevator>

--------------------------------------

Invoque dinámicamente código no administrado arbitrario.

1: <https://github.com/Kudaes/DInvoke_rs>

--------------------------------------

\*\* DESCATALOGADO \*\* Framework C2 que utiliza el Servicio de transferencia inteligente en segundo plano (BITS) como protocolo de comunicación y Direct Syscalls + Dinvoke para la evasión de conexión en modo usuario de EDR.

1: <https://github.com/Kudaes/LOLBITS>

--------------------------------------

PoC por vulnerabilidad en Renault ZOE Keyless System(CVE-2022-38766)

1: <https://github.com/AUTOCRYPT-IVS-VnV/CVE-2022-38766>

--------------------------------------

web analytics

1: <https://github.com/watchdog2000/cve-2022-24637_open-web-analytics-info-disclosure-to-rce>

--------------------------------------

Un framework C2/post-explotación multiplataforma.

1: <https://github.com/b23r0/Heroinn>

--------------------------------------

Herramienta de descubrimiento y explotación de inclusión de archivos locales

1: <https://github.com/hansmach1ne/lfimap>

--------------------------------------

Analizador de seguridad de configuración para dispositivos de red. Pynipper-ng es una evolución de nipper-ng, actualizado y traducido a python. [versión ALFA]

1: <https://github.com/syn-4ck/pynipper-ng>

--------------------------------------

Genera listas de hosts en vivo y URL para la orientación, automatizando el uso de MassDNS, Masscan y nmap para filtrar hosts inalcanzables y recopilar información de servicio.

1: <https://github.com/allyomalley/LiveTargetsFinder>

--------------------------------------

Comprobador de disponibilidad de Tor Relay, para usarlo como puente en países con censura

1: <https://github.com/ValdikSS/tor-relay-scanner>

--------------------------------------

GoodbyeDPI: utilidad de elusión de inspección profunda de paquetes (para Windows)

1: <https://github.com/ValdikSS/GoodbyeDPI>

--------------------------------------

Herramienta para enviar automáticamente por correo electrónico los resultados de sus secuencias de comandos de Python a su bandeja de entrada como texto o como un archivo adjunto, almacenando la contraseña de la cuenta de correo electrónico del remitente de forma segura en el llavero.

1: <https://github.com/allyomalley/MailBot>

--------------------------------------

Un práctico servicio de DNS escrito en Go para ayudar en la detección de varios tipos de vulnerabilidades ciegas. Supervisa el servidor de un pentester en busca de interacciones de DNS fuera de banda y envía notificaciones de búsqueda a través de Slack.

1: <https://github.com/allyomalley/dnsobserver>

--------------------------------------

Desofuscador para la aplicación de Android

1: <https://github.com/Gyoonus/deoptfuscator>

--------------------------------------

TLS-Anvil, un conjunto de pruebas TLS totalmente automatizado para clientes y servidores.

1: <https://github.com/tls-attacker/TLS-Anvil>

--------------------------------------

GoSniper es una herramienta DoS/DDoS.

1: <https://github.com/Discordmodsbers/GoSniper>

--------------------------------------

Administrador y monitor avanzados para Apache Tomcat, bifurcado de Lambda Probe

1: <https://github.com/psi-probe/psi-probe>

--------------------------------------

Sonda: esta es una herramienta especial para el cazador de errores para el proceso de reconocimiento automatizado sin problemas.

1: <https://github.com/whoami-anoint/Probe>

--------------------------------------

👀¡Intercepte solicitudes pasivamente de DHCP desde su propia red!👀

1: <https://github.com/vincenzogianfelice/DHCPEyes>

--------------------------------------

Una forma muy sencilla de averiguar qué suites de cifrado SSL son compatibles con un objetivo.

1: <https://github.com/mozilla/cipherscan>

--------------------------------------

Hackers Hunter: busque y rastree las cuentas de CTF Players & Bug Hunters, etc. por nombre de usuario en la mayoría de los lugares donde puede encontrarlos🔎 🕵️

1: <https://github.com/c0brabaghdad1/Hackers-Hunter>

--------------------------------------

Configuración incorrecta de DNS: S0x4 - Escáner de secuencias de comandos del mismo sitio

1: <https://github.com/c0brabaghdad1/S0x4>

--------------------------------------

Analizador WiFi y Bluetooth basado en GUI de última generación para Linux

1: <https://github.com/ghostop14/sparrow-wifi>

--------------------------------------

Una herramienta generadora de alcance para Burp Suite y ZAP

1: <https://github.com/root4loot/rescope>

--------------------------------------

WireBug es un conjunto de herramientas para pruebas de penetración de voz sobre IP

1: <https://github.com/SySS-Research/WireBug>

--------------------------------------

HRShell es un shell inverso HTTPS/HTTP construido con matraz. Es un servidor C2 avanzado con muchas características y capacidades.

1: <https://github.com/chrispetrou/HRShell>

--------------------------------------

Herramienta de fuzzing, enumeración y explotación de inclusión de archivos y cruce de directorios.

1: https://github.com/chrispetrou/FDsploit

--------------------------------------

Salsa Tools - ShellReverse TCP/UDP/ICMP/DNS/SSL/BINDTCP/Shellcode/SILENTTRINITY y AV bypass, parcheado AMSI

1: <https://github.com/Hackplayers/Salsa-tools>

--------------------------------------

El shell WinRM definitivo para hacking/pentesting

1: <https://github.com/Hackplayers/evil-winrm>

--------------------------------------

Omisión de autenticación para <https://github.com/patrickfuller/camp>

1: <https://github.com/ehtec/camp-exploit>

--------------------------------------

AMSI omite el enganche de NtCreateSection 1: <https://github.com/waawaa/AMSI_Rubeus_bypass>

--------------------------------------

Scan a range of IPv4 addresses easily.

1: <https://github.com/Keyj33k/Ovax-IPsweep-Java>

--------------------------------------

DDos Ripper un servidor de ataque Distributable Denied-of-Service (DDOS) que corta los objetivos o la infraestructura circundante en una avalancha de tráfico de Internet

1: <https://github.com/palahsu/DDoS-Ripper>

--------------------------------------

DOM Clobbering Wiki, pruebas de navegador y generación de carga útil

1: <https://github.com/SoheilKhodayari/DOMClobbering>

--------------------------------------

DOMPurify: un desinfectante XSS ultrarrápido, súper tolerante y solo DOM para HTML, MathML y ​​SVG. DOMPurify funciona con un valor predeterminado seguro, pero ofrece muchas opciones de configuración y ganchos. Manifestación:

1: <https://github.com/cure53/DOMPurify>

--------------------------------------

HStreamDB es una base de datos de transmisión nativa de la nube de código abierto para IoT y más. Modernice su pila de datos para aplicaciones en tiempo real.

1: <https://github.com/hstreamdb/hstream>

--------------------------------------

Elkeid es un proyecto de solución de detección de intrusos basado en host nativo de la nube para proporcionar detección de amenazas y audición de comportamiento de próxima generación con una arquitectura moderna.

1: <https://github.com/bytedance/elkeid>

--------------------------------------

Una aplicación de chat entre pares sin servidor, descentralizada y efímera

1: <https://github.com/jeremyckahn/chitchatter>

--------------------------------------

Una secuencia de comandos que monitorea y extrae las URL solicitadas y los clientes conectados al servicio mediante la explotación de instancias de estado del servidor Apache accesibles públicamente.

1: <https://github.com/mazen160/server-status_PWN>

--------------------------------------

Una secuencia de comandos que monitorea y extrae las URL solicitadas y los clientes conectados al servicio mediante la explotación de instancias de estado del servidor Apache accesibles públicamente.

1: <https://github.com/mazen160/server-status_PWN>

--------------------------------------

BFAC (verificador de artefactos de archivos de respaldo): una herramienta automatizada que busca artefactos de respaldo que puedan revelar el código fuente de la aplicación web.

1: <https://github.com/mazen160/bfac>

--------------------------------------

Explotación F5 BIG-IP RCE (CVE-2022-1388)

1: <https://github.com/alt3kx/CVE-2022-1388_PoC>

--------------------------------------

Dataiku REST-API por defecto el software permite el acceso anónimo a la funcionalidad que permite a un atacante conocer usuarios válidos.

1: <https://github.com/alt3kx/CVE-2018-10732>

--------------------------------------

Herramienta de pulverización de contraseñas de Microsoft Exchange con soporte de proxy.

1: <https://github.com/iomoath/PyExchangePasswordSpray>

--------------------------------------

Dos method

1: <https://github.com/0x44F/blazingfast-dos-updated>

--------------------------------------

Proyecto rastreador Darkweb

1: <https://github.com/JarryShaw/darc>

--------------------------------------

Kit de análisis PCAP multimotor de Python.

1: <https://github.com/JarryShaw/PyPCAPKit>

--------------------------------------

Compilador de backport para expresiones de asignación de Python 3.8 (walrus).

1: <https://github.com/pybpc/walrus>

--------------------------------------

Sandman es una puerta trasera basada en NTP para compromisos de equipos rojos en redes reforzadas.

1: <https://github.com/Idov31/Sandman>

--------------------------------------

MrKaplan es una herramienta destinada a ayudar a los miembros del equipo rojo a mantenerse ocultos eliminando las pruebas de ejecución.

1: <https://github.com/Idov31/MrKaplan>

--------------------------------------

Una herramienta de automatización simple para detectar vulnerabilidades lfi, rce y ssti

1: <https://github.com/aniqfakhrul/lazyParam>

--------------------------------------

FarsightADes un script de PowerShell que tiene como objetivo ayudar a descubrir mecanismos de persistencia

1: <https://github.com/Qazeer/FarsightAD>

--------------------------------------

Una PoC para agregar NtContinue a la lista permitida de CFG para que Ekko funcione en un proceso protegido por CFG

1: <https://github.com/IcebreakerSecurity/Ekko_CFG_Bypass>

--------------------------------------

Exploit for the Unauthenticated RCE in Open Web Analytics (OWA) <1.7.4. This work is based on

1: <https://github.com/JacobEbben/CVE-2022-24637>

--------------------------------------

Un PoC para controlar remotamente máquinas Windows a través de Websockets.

1: <https://github.com/ps1337/reinschauer>

--------------------------------------

Kit de herramientas de análisis de seguridad para protocolos de automóviles patentados

1: <https://github.com/schutzwerk/CANalyzat0r>

--------------------------------------

holehe le permite verificar si el correo se usa en diferentes sitios como twitter, instagram y recuperará información en sitios con la función de contraseña olvidada.

1: <https://github.com/megadose/holehe>

--------------------------------------

Biblioteca de Python y CLI para consultar con precisión el nombre de usuario y el uso de correo electrónico en plataformas en línea

1: <https://github.com/iojw/socialscan>

--------------------------------------

Generación automática de exploits (AEG) y captura remota de banderas para problemas de CTF explotables

1: <https://github.com/ChrisTheCoolHut/Zeratool>

--------------------------------------

Erebus es una herramienta rápida para el análisis de vulnerabilidades basado en parámetros que utiliza un motor de plantillas basado en Yaml como núcleos.

1: <https://github.com/ethicalhackingplayground/erebus>

--------------------------------------

TProx es un rápido detector de cruce de ruta de proxy inverso y fuerza bruta de directorio.

1: <https://github.com/ethicalhackingplayground/tprox>

--------------------------------------

Erebus es una herramienta rápida para el análisis de vulnerabilidades basado en parámetros que utiliza un motor de plantillas basado en Yaml como núcleos.

1: <https://github.com/ethicalhackingplayground/erebus>

--------------------------------------

Un webshell que puede eludir parte de la seguridad del sistema.

1: <https://github.com/22XploiterCrew-Team/Gel4y-Mini-Shell-Backdoor>

--------------------------------------

Wpushell es una herramienta que se utiliza para cargar un shell de puerta trasera en un sitio que utiliza un sistema de gestión de contenido de WordPress con un proceso simple y rápido.

1: <https://github.com/22XploiterCrew-Team/Wpushell>

--------------------------------------

Pwny es una implementación de una carga útil avanzada de código nativo HatSploit, diseñada para la portabilidad, la capacidad de integración y la baja utilización de recursos.

1: <https://github.com/EntySec/Pwny>

--------------------------------------

Shreder es una poderosa herramienta de fuerza bruta de contraseñas de protocolo SSH de subprocesos múltiples.

1: <https://github.com/EntySec/Shreder>

--------------------------------------

Marco y bibliotecas de ataque GoldenSAML

1: <https://github.com/secureworks/whiskeysamlandfriends>

--------------------------------------

Una herramienta de seguridad para detectar modificaciones de PDF sospechosas que se encuentran comúnmente en BEC

1: <https://github.com/secureworks/pdfxpose>

--------------------------------------

Una herramienta para implementar y detectar el uso de tokens de miel de Active Directory

1: <https://github.com/secureworks/dcept>

--------------------------------------

un compilador de captura de paquetes de red

1: <https://github.com/secureworks/flowsynth>

Herramienta para marcar puertos eBPF

1: <https://github.com/eeriedusk/knockles>

--------------------------------------

RomBuster es una herramienta de explotación de enrutadores que permite revelar la contraseña de administrador del enrutador de red.

1: <https://github.com/EntySec/RomBuster>

--------------------------------------

Una herramienta de exploración de penetración de dominio que facilita la automatización con un solo clic, la recopilación de información integral y la exploración de vulnerabilidades de escalada de privilegios de dominio.

1: <https://github.com/lele8/mscan>

--------------------------------------

Secuencia de comandos de explotación de ZeroLogon, recuperación con un solo clic del hash de la máquina del controlador de dominio

1: <https://github.com/lele8/CVE-2020-1472>

--------------------------------------

analizador de red web

1: <https://github.com/shade234sherif/NETPHY>

--------------------------------------

CVE-2022-36200 PoC

1: <https://github.com/afaq1337/CVE-2022-36200>

--------------------------------------

MOTOR DE CORREO ANÓNIMO

1: <https://github.com/shade234sherif/MAILER>

--------------------------------------

Erlik - Servicio de jabón vulnerable

1: <https://github.com/anil-yelken/Vulnerable-Soap-Service>

--------------------------------------

Abusar del mecanismo del inspector de node.js para obligar a cualquier proceso basado en node.js/electron/v8 a ejecutar código javascript arbitrario.

1: <https://github.com/evilsocket/jscythe>

--------------------------------------

Un escáner de malware multiplataforma minimalista con monitoreo del sistema de archivos en tiempo real sin bloqueo utilizando reglas YARA.

1: <https://github.com/evilsocket/sauron>

--------------------------------------

🧠 🔎 🤖Kitsune es una red neuronal artificial diseñada para detectar y correlacionar perfiles de Twitter con comportamientos similares.

1: <https://github.com/evilsocket/kitsune>

--------------------------------------

XRay es una herramienta para reconocimiento, mapeo y recopilación OSINT de redes públicas.

1: <https://github.com/evilsocket/xray>

--------------------------------------

OpenSnitch es un puerto GNU/Linux del cortafuegos de aplicaciones Little Snitch

1: <https://github.com/evilsocket/opensnitch>

--------------------------------------

(⌐■\_■) - Aprendizaje de refuerzo profundo que instrumenta bettercap para pwning WiFi.

1: <https://github.com/evilsocket/pwnagotchi>

--------------------------------------

interfaz de usuario web de bettercap

1: <https://github.com/bettercap/ui>

--------------------------------------

La navaja suiza para reconocimiento de redes 802.11, BLE, IPv4 e IPv6 y ataques MITM.

1: <https://github.com/bettercap/bettercap>

--------------------------------------

Herramienta #OSINT para encontrar repositorios de Github extrayendo registros de confirmación en tiempo real desde la API de eventos de Github

1: <https://github.com/robhax/commit-stream>

--------------------------------------

Citrix ADC (NetScaler) Honeypot. Admite la detección de CVE-2019-19781 e intentos de inicio de sesión

1: <https://github.com/robhax/citrix-honeypot>

--------------------------------------

Conjunto de Mindmaps que proporciona una descripción detallada de las diferentes capacidades de auditoría de #Microsoft para Windows, Exchange, Azure,…

1: <https://github.com/mdecrevoisier/Microsoft-eventlog-mindmap>

--------------------------------------

Una herramienta de QoL para ofuscar el shellcode. En el futuro será posible encadenar métodos de codificación/cifrado/compresión.

1: <https://github.com/iilegacyyii/Shellcrypt>

--------------------------------------

La principal fuente de verdad que impulsa la automatización de redes. Código abierto bajo Apache 2. Demostración pública

1: <https://github.com/netbox-community/netbox>

--------------------------------------

Omitir la contraseña de Windows y Bitlocker

1: <https://github.com/Push3AX/GrabAccess>

--------------------------------------

un registro RMI de Java malvado.

1: <https://github.com/hakivvi/ermi>

--------------------------------------

Sugerencia de vulnerabilidades de Windows: próxima generación

1: <https://github.com/bitsadmin/wesng>

--------------------------------------

Koppeling x Metatwin x LazySign

1: <https://github.com/jfmaes/Invoke-DLLClone>

--------------------------------------

Herramienta para generar listas de palabras inteligentes y potentes

1: <https://github.com/r3nt0n/bopscrk>

--------------------------------------

La navaja suiza de la piratería. Todos los scripts y herramientas necesarios integrados en una CLI portátil y personalizable.

1: <https://github.com/troopek/TropX>

--------------------------------------

Marco de botnet con arquitectura modular y extensible, programador de tareas, sesiones en vivo de shell remotas y una interfaz retro que hace que su uso sea divertido. Por ahora, incluye keylogger, DDoS y ataques de fuerza bruta. El proyecto aún está en fase de desarrollo, agradezco cualquier contribución 1: <https://github.com/r3nt0n/zombiegang>

--------------------------------------

APIKit: kit de herramientas de API de descubrimiento, escaneo y auditoría, todo en uno.

1: <https://github.com/API-Security/APIKit>

--------------------------------------

Athena es una distribución basada en Arch Linux centrada en la ciberseguridad. ¡Aprende, practica y disfruta con cualquier herramienta de hackeo!

1: <https://github.com/Athena-OS/athena-iso>

--------------------------------------

🛡️⚔️¡Proteja su aplicación web del ataque DDOS o Dead Ping + VERIFICACIÓN DE CAPTCHA en una línea!

1: <https://github.com/Sanix-Darker/AntiDDOS-system>

--------------------------------------

Extensión de Burp Suite útil para verificar la seguridad OAUTHv2 y OpenID

1: <https://github.com/akabe1/OAUTHScan>

--------------------------------------

Una herramienta simple que podría ser útil para inspeccionar la seguridad UPnP

1: <https://github.com/akabe1/upnp-hunter>

--------------------------------------

Script de Python que recopila información SSL/TLS de los hosts

1: <https://github.com/narbehaj/ssl-checker>

--------------------------------------

Día N de QNAP (probablemente no CVE-2020-2509)

1: <https://github.com/jbaines-r7/overkill>

--------------------------------------

(Obsoleto) Exportador de lista de seguidores/seguidores de Instagram usando Python Flask

1: <https://github.com/narbehaj/instagram-status>

--------------------------------------

TerraformGoat es la herramienta de implementación de múltiples nubes "Vulnerable by Design" de selefra research lab.

1: <https://github.com/selefra/TerraformGoat>

--------------------------------------

GO Anti-Kill Shellcode Loader ofusca el cifrado AES

1: <https://github.com/HZzz2/go-shellcode-loader>

--------------------------------------

Script de fuerza bruta multiproceso SSH basado en Python y versión dual del módulo Metasploit

1: <https://github.com/HZzz2/SSH_Bruteforce>

--------------------------------------

La forma más fácil de ejecutar WireGuard VPN + interfaz de usuario de administración basada en la web.

1: <https://github.com/WeeJeWel/wg-easy>

--------------------------------------

Omisión de UAC, Elevate, Métodos de persistencia

1: <https://github.com/rootm0s/WinPwnage>

--------------------------------------

Repositorio de cursos para PowerShell for Pentesters Course

1: <https://github.com/dievus/PowerShellForPentesters>

--------------------------------------

Esto podría haber sido una frase ingeniosa, pero adivina qué. Es una pequeña herramienta Go que enumera las CVE de tendencia de cvetrends.com

1: <https://github.com/tr3ss/gofetch>

--------------------------------------

Varios métodos de ejecución de shellcode

1: <https://github.com/Kr0ff/WinMalDev>

--------------------------------------

Una herramienta para la gestión de secretos, el cifrado como servicio y la gestión de acceso privilegiado

1: <https://github.com/hashicorp/vault>

--------------------------------------

Un scrapper de PasteBin que no depende de la API de scrape de PasteBin

1: <https://github.com/Kr0ff/Pasta>

--------------------------------------

Conecte, asegure, controle y observe los servicios.

1: <https://github.com/istio/istio>

--------------------------------------

Packer es una herramienta para crear imágenes de máquinas idénticas para múltiples plataformas a partir de una configuración de fuente única.

1: <https://github.com/hashicorp/packer>

--------------------------------------

Llamada al sistema directa e indirecta de un único código auxiliar con resolución de SSN en tiempo de ejecución para Windows.

1: <https://github.com/janoglezcampos/c_syscalls>

--------------------------------------

Un archivador nativo de código abierto silencioso (oculto) gratuito - Incluye la omisión de Windows Defender – EyeBinder

1: <https://github.com/TeamDarkAnon/EyeBinder>

--------------------------------------

Massayo es una pequeña biblioteca Rust de prueba de concepto que elimina los ganchos AV/EDR en un sistema DLL determinado

1: <https://github.com/thiagopeixoto/massayo>

--------------------------------------

Herramienta de administración remota [RAT para Android] Sin reenvío de puertos

1: <https://github.com/TeamDarkAnon/xhunter>

--------------------------------------

Un exploit confiable + redacción para elevar los privilegios a la raíz. (Probado en Ubuntu 22.04)

1: <https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit>

--------------------------------------

Este proyecto fue construido por pentesters para pentesters.

1: <https://github.com/redeye-framework/Redeye>

--------------------------------------

CVE-2022-36946 pánico del kernel de Linux en netfilter\_queue

1: <https://github.com/Pwnzer0tt1/CVE-2022-36946>

--------------------------------------

Desarrollo de exploits: exploits armados y prueba de concepto (PoC)

1: <https://github.com/VoidSec/Exploit-Development>

--------------------------------------

marco canbus h4xing rápido y sucio

1: <https://github.com/shipcod3/canTot>

--------------------------------------

Una metodología rápida para probar/hackear aplicaciones SAP para n00bz y cazarrecompensas de errores

1: <https://github.com/shipcod3/mySapAdventures>

--------------------------------------

Proxy de Socks4a que aprovecha PIC, Websockets y ofuscación estática en el nivel de ensamblaje

1: <https://github.com/codewhitesec/Lastenzug>

--------------------------------------

Biblioteca de Python y CLI para consultar con precisión el nombre de usuario y el uso de correo electrónico en plataformas en línea

1: <https://github.com/iojw/socialscan>

--------------------------------------

Análisis de sentimiento en tiempo real y visualización de Twitter

1: <https://github.com/iojw/bluebird>

--------------------------------------

SkyPilot es un marco para ejecutar fácilmente cargas de trabajo de aprendizaje automático en cualquier nube a través de una interfaz unificada.

1: <https://github.com/skypilot-org/skypilot>

--------------------------------------

Generación automática de exploits (AEG) y captura remota de banderas para problemas de CTF explotables

1: <https://github.com/ChrisTheCoolHut/Zeratool>

--------------------------------------

Erebus es una herramienta rápida para el análisis de vulnerabilidades basado en parámetros que utiliza un motor de plantillas basado en Yaml como núcleos.

1: <https://github.com/ethicalhackingplayground/erebus>

--------------------------------------

Uso de la herramienta PIN de Intel para resolver problemas de CTF

1: <https://github.com/ChrisTheCoolHut/PinCTF>

--------------------------------------

Descubrimiento de vulnerabilidades en el firmware a través de análisis concolic y agrupación de funciones.

1: <https://github.com/ChrisTheCoolHut/Firmware_Slap>

--------------------------------------

Herramienta para generar listas de palabras inteligentes y potentes

1: <https://github.com/r3nt0n/bopscrk>

--------------------------------------

Script de Python que recopila información SSL/TLS de los hosts

1: <https://github.com/narbehaj/ssl-checker>

--------------------------------------

Exportación y vinculación de funciones automáticas para fuzzing de archivos binarios entre arquitecturas.

1: <https://github.com/ChrisTheCoolHut/Easy-Pickings>

--------------------------------------

Día N de QNAP (probablemente no CVE-2020-2509)

1: <https://github.com/jbaines-r7/overkill>

--------------------------------------

Repositorio de cursos para PowerShell for Pentesters Course

1: <https://github.com/dievus/PowerShellForPentesters>

--------------------------------------

Una herramienta para la gestión de secretos, el cifrado como servicio y la gestión de acceso privilegiado

1: <https://github.com/hashicorp/vault>

--------------------------------------

Script súper organizado y flexible para enviar campañas de phishing

1: <https://github.com/KINGSABRI/goCabrito>

--------------------------------------

Packer es una herramienta para crear imágenes de máquinas idénticas para múltiples plataformas a partir de una configuración de fuente única.

1: <https://github.com/hashicorp/packer>

--------------------------------------

Consul es una solución distribuida, de alta disponibilidad y consciente del centro de datos para conectar y configurar aplicaciones a través de una infraestructura dinámica y distribuida.

1: <https://github.com/hashicorp/consul>

--------------------------------------

Nomad es un orquestador de cargas de trabajo fácil de usar, flexible y eficaz que puede implementar una combinación de aplicaciones de microservicios, lotes, en contenedores y no en contenedores. Nomad es fácil de operar y escalar y tiene integraciones nativas de Consul y Vault.

1: <https://github.com/hashicorp/nomad>

--------------------------------------

Comprobador de disponibilidad de Tor Relay, para usarlo como puente en países con censura

1: <https://github.com/ValdikSS/tor-relay-scanner>

--------------------------------------

GoodbyeDPI: utilidad de elusión de inspección profunda de paquetes (para Windows)

1: <https://github.com/ValdikSS/GoodbyeDPI>

--------------------------------------

Genera listas de hosts en vivo y URL para la orientación, automatizando el uso de MassDNS, Masscan y nmap para filtrar hosts inalcanzables y recopilar información de servicio.

1: <https://github.com/allyomalley/LiveTargetsFinder>

--------------------------------------

TLS-Anvil, un conjunto de pruebas TLS totalmente automatizado para clientes y servidores.

1: <https://github.com/tls-attacker/TLS-Anvil>

--------------------------------------

PwnFox es una extensión de Firefox/Burp que proporciona herramientas útiles para su auditoría de seguridad.

1: <https://github.com/yeswehack/PwnFox>

--------------------------------------

🤒Un rastreador de tráfico de red alternativo y moderno.

1: <https://github.com/chenjiandongx/sniffer>

--------------------------------------

Mango es un programa Powershell interactivo para el usuario para buscar posibles vectores de escalada de privilegios en Windows

1: <https://github.com/SxNade/Mango>

--------------------------------------

Mufasa es un potente extractor de comentarios, mufasa puede eliminar automáticamente los comentarios de la página principal, los archivos Javascript y CSS utilizados por un sitio web.

1: <https://github.com/SxNade/Mufasa>

--------------------------------------

“GIFShell”: cadena de ataque encubierta y C2 que utilizan GIF de Microsoft Teams

1: <https://medium.com/@bobbyrsec/gifshell-covert-attack-chain-and-c2-utilizing-microsoft-teams-gifs-1618c4e64ed7>

--------------------------------------

Una secuencia de comandos de python para obligar automáticamente a un servidor de Windows a autenticarse en una máquina arbitraria a través de 9 métodos.

1: <https://github.com/p0dalirius/Coercer>

--------------------------------------

Una versión azucarada de RottenPotatoNG, con un poco de jugo, es decir, otra herramienta de escalamiento de privilegios locales, de cuentas de servicio de Windows a NT AUTHORITY\SYSTEM.

1: <https://github.com/ohpe/juicy-potato>

--------------------------------------

Muraena es un proxy inverso casi transparente destinado a automatizar las actividades de phishing y posteriores al phishing.

1: <https://github.com/muraenateam/muraena>

--------------------------------------

Automatización de la escalada de privilegios locales de papa jugosa para los probadores de penetración.

1: <https://github.com/TsukiCTF/Lovely-Potato>

--------------------------------------

Escalada de privilegios de Windows

1: <https://github.com/k4sth4/Juicy-Potato>

--------------------------------------

🔍Un editor hexadecimal para ingenieros inversos, programadores y personas que valoran sus retinas cuando trabajan a las 3 de la mañana.

1: <https://github.com/WerWolv/ImHex>

--------------------------------------

VECTR es una herramienta que facilita el seguimiento de las actividades de prueba de su equipo rojo y azul para medir las capacidades de detección y prevención en diferentes escenarios de ataque.

1: <https://github.com/SecurityRiskAdvisors/VECTR>

--------------------------------------

Colección de herramientas que reflejan la dimensión de la red en los datos de Bloodhound

1: <https://github.com/zeronetworks/BloodHound-Tools>

--------------------------------------

Prueba de concepto para CVE-2021-31166, un HTTP.sys remoto use-after-free activado de forma remota.

1: <https://github.com/0vercl0k/CVE-2021-31166>

--------------------------------------

Script de prueba para CVE-2020-1472 para RPC/TCP y RPC/SMB

1: <https://github.com/zeronetworks/zerologon>

--------------------------------------

Discord, Twitter, cookies de Instagram y capturador de fichas. Agarrando de todos los navegadores web!

1: <https://github.com/mouadessalim/CookedGrabber>

--------------------------------------

¡Utiliza la función de inicio de sesión QR de Discord para crear un código QR escaneable de Token Logger!

1: <https://github.com/9P9/Discord-QR-Token-Logger>

--------------------------------------

este es un módulo de python que contiene funciones y clases que se utilizan para probar la seguridad de las aplicaciones web/de red. ¡Está codificado en Python puro y es una herramienta muy inteligente! Puede detectar fácilmente: XSS (recogido/almacenado), RCE (código remoto/ejecución de comandos), SSTI, SSRF, errores de configuración de CORS, carga de archivos, CSRF, recorrido de ruta,... Además,…

1: <https://github.com/AlaBouali/bane>

--------------------------------------

Recopile parámetros vulnerables XSS de todo el dominio.

1: <https://github.com/thenurhabib/collector>

--------------------------------------

MainCoon es un marco de reconocimiento automatizado destinado a recopilar información durante las pruebas de penetración de aplicaciones web.

1: <https://github.com/thenurhabib/maincoon>

--------------------------------------

Transforme los registros de auditoría de Linux para el uso de SIEM

1: <https://github.com/threathunters-io/laurel>

--------------------------------------

Interfaz oficial de línea de comandos para la API de IPinfo (geolocalización de IP y otros tipos de datos de IP)

1: <https://github.com/ipinfo/cli>

--------------------------------------

Rastreador web simple y rápido diseñado para el descubrimiento fácil y rápido de puntos finales y activos dentro de una aplicación web

1: <https://github.com/hakluke/hakrawler>

--------------------------------------

Cree un directorio activo vulnerable que le permita probar la mayoría de los ataques de directorio activo en un laboratorio local

1: <https://github.com/WazeHell/vulnerable-AD>

--------------------------------------

Chalumeau es una herramienta de volcado de credenciales automatizada, ampliable y personalizable basada en powershell y python.

1: <https://github.com/cyberstruggle/chalumeau>

--------------------------------------

Servidor HTTP que sirve scripts/cargas de Powershell ofuscados

1: <https://github.com/WazeHell/LightMe>

--------------------------------------

Cree un directorio activo vulnerable que le permita probar la mayoría de los ataques de directorio activo en un laboratorio local

1: <https://github.com/WazeHell/vulnerable-AD>

--------------------------------------

Haz combinaciones de rutas URL usando una lista de palabras

1: <https://github.com/trickest/mkpath>

--------------------------------------

Ejecutores sigilosos de shellcode🐺

1: <https://github.com/kymb0/Stealth_shellcode_runners>

--------------------------------------

Ladrón en tan solo 3 líneas con envío a Telegram.

1: <https://github.com/FallenAstaroth/stink>

--------------------------------------

Marco de botnet con arquitectura modular y extensible, programador de tareas, sesiones en vivo de shell remotas y una interfaz retro que hace que su uso sea divertido. Por ahora, incluye keylogger, DDoS y ataques de fuerza bruta. El proyecto aún está en fase de desarrollo, agradezco cualquier contribución.

1: <https://github.com/r3nt0n/zombiegang>

--------------------------------------

🐸Identifica cualquier cosa. pyWhat le permite identificar fácilmente correos electrónicos, direcciones IP y más. ¡Aliméntalo con un archivo .pcap o algún texto y te dirá qué es!🧙‍♀️

1: <https://github.com/bee-san/pyWhat>

--------------------------------------

🚩🐺¡Generador de shell para CTF!

1: <https://github.com/cr-0w/inumaki>

--------------------------------------

⚡Descifrar cifrados automáticamente sin conocer la clave o el cifrado, decodificar codificaciones y descifrar hashes⚡

1: <https://github.com/Ciphey/Ciphey>

--------------------------------------

🦝💰generador de nombre de usuario para CTFs!

1: <https://github.com/cr-0w/thievius>

--------------------------------------

😃Python para la carga útil de implementación masiva en servidores de Microsoft Exchange afectados por ProxyLogon (CVE-2021-26857, CVE-2021-26855, CVE-2021-27065)

1: <https://github.com/cryptolakk/ProxyLogon-Mass-RCE>

--------------------------------------

Explotación de ejecución remota de código para CVE-2022-36804 (BitBucket Server y DataCenter).

1: <https://github.com/cryptolakk/CVE-2022-36804-RCE>

--------------------------------------

Plantilla de CMake para una aplicación/bootkit básico de EFI. Esta biblioteca es solo de encabezado, ¡no hay tiempo de ejecución de EDK2!).

1: <https://github.com/mrexodia/EfiCMake>

--------------------------------------

DuckySploit V3 Roblox Nivel 7 Ejecutor Gratis

1: <https://github.com/Omnis9/DuckySploit-V3>

--------------------------------------

League of Legends Evolut Client Hack v7.0 - ¡Incluye SkinChanger, AutoBan, Scripts para campeones + 50 MÁS!

1: <https://github.com/Omnis9/League-of-Legends-Evolut-Client-Hack-v7.0>

--------------------------------------

Invision Apex Legends Private Cheat - AimBot + ESP + FOV diferente + Habilidades ilimitadas + ¡50 MÁS!

1: <https://github.com/Omnis9/InvisioN-ApexLegends-PrivateCheat-V2.0>

--------------------------------------

Xloop CSGO Private CHEAT - INCLUYE AIMBOT, WALLHACK + ESP + SOFTAIM + MÁS DE 100 CARACTERÍSTICAS

1: <https://github.com/Omnis9/Xloop-CSGO-PrivateCheat>

--------------------------------------

Call Of Duty: WarZone HWID Spoofer (DESBÁRQUESE USTED MISMO, TRABAJANDO EN EL PARCHE DEL JUEGO ACTUALMENTE)

1: <https://github.com/Omnis9/COD-Warzone-Spoofer>

--------------------------------------

Chameleon proporciona un mejor descubrimiento de contenido mediante el uso del conjunto de huellas digitales de tecnología de wappalyzer junto con listas de palabras personalizadas adaptadas a cada tecnología detectada.

1: <https://github.com/iustin24/chameleon>

--------------------------------------

Una colección de scripts de explotación de prueba de concepto escritos por el equipo de STAR Labs para varios CVE que descubrieron o encontraron otros.

1: <https://github.com/star-sg/CVE>

--------------------------------------

Identifique rutas de escalada de privilegios dentro y entre diferentes nubes

1: <https://github.com/carlospolop/PurplePanda>

--------------------------------------

Una implementación de PoC para una técnica de evasión para finalizar el subproceso actual y restaurarlo antes de reanudar la ejecución, al tiempo que implementa cambios de protección de página sin ejecución.

1: <https://github.com/janoglezcampos/DeathSleep>

--------------------------------------

Terminator Framework Console, Framework de explotación para Pentesters y Ethical Hackers, con módulos propios y publicados por el usuario

1: <https://github.com/optionalg/Terminator>

--------------------------------------

Una herramienta profesional de hacking ético.

1: <https://github.com/legly/SamSploit>

--------------------------------------

¡Comprueba si tu proveedor te está bloqueando!

1: <https://github.com/Peco602/findwall>

--------------------------------------

Una herramienta de cambio automático de IP de Tor. Este programa puede cambiar automáticamente nuestra identidad/IP de Tor. Funciona al 100%.

1: <https://github.com/r3k4t/AutoTorIP>

--------------------------------------

Una colección de scripts ZAP proporcionados por la comunidad. ¡Las solicitudes de incorporación de cambios son muy bienvenidas!

1: <https://github.com/zaproxy/community-scripts>

--------------------------------------

Extensión de detección de cumplimiento de autorización automática para burp suite escrita en Jython desarrollada por Barak Tawily para facilitar el trabajo de seguridad de la aplicación y permitirles realizar pruebas de autorización automáticas

1: <https://github.com/Quitten/Autorize>

--------------------------------------

¡Bienvenidos! Esta es una utilidad que se puede compilar con Visual Studio 2019 (o posterior). El objetivo de este programa es crear una sesión SMB falsa.

1: <https://github.com/Sq00ky/SMB-Session-Spoofing>

--------------------------------------

Avance más profundamente en las redes al descubrir hosts y puertos, utilizando una máquina comprometida a través de SSH

1: <https://github.com/Xeonrx/Puwr>

--------------------------------------

⭐ ⭐tcpdump distribuido para entornos nativos de la nube⭐ ⭐

1: <https://github.com/deepfence/PacketStreamer>

--------------------------------------

Transforma el flujo UDP en flujos TCP (falsos) que pueden atravesar firewalls/NAT de capa 3 y capa 4 (NAPT).

1: <https://github.com/dndx/phantun>

--------------------------------------

ExeSpy es un visor PE multiplataforma para archivos EXE y DLL

1: <https://github.com/andyjsmith/Exe-Spy>

--------------------------------------

Integración de monitoreo de Shodan para TheHive.

1: <https://github.com/KaanSK/shomon>

--------------------------------------

Analizador WiFi y Bluetooth basado en GUI de próxima generación para Linux

1: <https://github.com/ghostop14/sparrow-wifi>

--------------------------------------

redirector ligero de http escrito en nim

1: <https://github.com/d4rckh/http-redirector>

--------------------------------------

WebView2 le permite iniciar con una carpeta de datos de usuario (UDF)

1: <https://github.com/mrd0x/WebView2-Cookie-Stealer>

--------------------------------------

Automatice las tareas comunes del Protocolo de depuración de Chrome para ayudar a depurar aplicaciones web desde la línea de comandos y monitorear e interceptar activamente las solicitudes y respuestas HTTP.

1: <https://github.com/pownjs/cdb>

--------------------------------------

Ingeniería inversa ninja en paquetes Android APK

1: <https://github.com/rovellipaolo/NinjaDroid>

--------------------------------------

Servidor ssh vinculado estáticamente con funcionalidad de shell inverso para CTF y similares

1: <https://github.com/Fahrj/reverse-ssh>

--------------------------------------

Un script agresor para Cobalt Strike para consultar los mensajes GetLastError de Windows

1: <https://github.com/Henkru/cs-get-last-error>

--------------------------------------

Un laboratorio de omisión de captcha en PHP

1: <https://github.com/D3Ext/Captcha-Bypassing>

--------------------------------------

Su compañero de MitM para la retransmisión de ataques con adquisición de DNS de DHCPv6, así como suplantación de identidad de mDNS, LLMNR y NetBIOS-NS.

1: <https://github.com/RedTeamPentesting/pretender>

--------------------------------------

Herramienta de código abierto para hacer cumplir las mejores prácticas de privacidad y seguridad en Windows y macOS, porque la privacidad es sexy🍑🍆

1: <https://github.com/undergroundwires/privacy.sexy>

--------------------------------------

Similar a Petitpotam, el servicio netdfs está habilitado en Windows Server y entornos AD, y el método RPC abusado permite que los procesos privilegiados accedan a canalizaciones maliciosas para su explotación.

1: <https://github.com/crisprss/magicNetdefs>

--------------------------------------

Una herramienta de acceso remoto oculta e indetectable escrita en C++ y servidor en Python3.

1: <https://github.com/ryanwe1ss/Windows-Backdoor>

--------------------------------------

Este es un script de python que explota wget cuando se configura con un bit SUID y sobrescribe la contraseña de root.

1: <https://github.com/CopernicusPY/wget-root>

--------------------------------------

RunAsWinTcb utiliza un exploit de usuario para ejecutar una DLL con un nivel de protección de WinTcb-Light.

1: <https://github.com/tastypepperoni/RunAsWinTcb>

--------------------------------------

Una aplicación de seguimiento de objetivos y toma de notas multiplataforma para probadores de penetración.

1: <https://github.com/ehrishirajsharma/SwiftnessX>

--------------------------------------

Exploración de puertos combinada con la velocidad de Masscan y las funciones de exploración de Nmap.

1: <https://github.com/capt-meelo/MassMap>

--------------------------------------

Omisión de autenticación por Capture Replay (Dingtian-DT-R002)

1: <https://github.com/9lyph/CVE-2022-29593>

--------------------------------------

Implementación de Mimikatz en Python puro

1: <https://github.com/skelsec/pypykatz>

--------------------------------------

Entorno de depuración del kernel de Linux totalmente dockerizado

1: <https://github.com/0xricksanchez/like-dbg>

--------------------------------------

Evasión AV/EDR a través de llamadas directas al sistema.

1: <https://github.com/jthuraisamy/SysWhispers2>

--------------------------------------

La bifurcación Iceman de Proxmark3 / RFID / NFC lector, escritor, sniffer y emulador

1: <https://github.com/RfidResearchGroup/proxmark3>

--------------------------------------

El análisis de resultados XML de Nmap y la correlación CPE de NVD para buscar CVE.

1: <https://github.com/CoolerVoid/Vision2>

--------------------------------------

Vulnerabilidad de divulgación de nombre de host interno

1: <https://github.com/Vulnmachines/Zoho_CVE-2022-23779>

--------------------------------------

IPTV-Link-Scraper raspa los enlaces de IPTV de https://streamtest.in/ y los guarda como archivo m3u.

1: <https://github.com/henry-richard7/IPTV-Link-Scraper>

--------------------------------------

Este programa de Python obtiene la dirección IP durante la sesión en línea de GTA V en línea

1: <https://github.com/henry-richard7/GTA-V-Online-IP-Grabber>

--------------------------------------

Stego es una herramienta de esteganografía gratuita y de código abierto que le permite ocultar su mensaje secreto en una imagen o archivo de audio. No notará ningún cambio en la imagen o el archivo de audio. Sin embargo, su mensaje secreto estará dentro de la imagen original o el archivo de audio.

1: <https://github.com/W1LDN16H7/StegoCracker>

--------------------------------------

Escáner de vulnerabilidades de carga de archivos y herramienta de explotación.

1: <https://github.com/almandin/fuxploider>

--------------------------------------

LeakScraper es un conjunto eficiente de herramientas para procesar y visualizar archivos de texto de gran tamaño que contienen credenciales. Estas herramientas están diseñadas para ayudar a los evaluadores de penetración y a los equipos de red a hacer OSINT mediante la recopilación de credenciales que pertenecen a su objetivo.

1: <https://github.com/Acceis/leakScraper>

--------------------------------------

Doxea información pública de un número de teléfono

1: <https://github.com/Alcatraz2033/Phone-dox>

--------------------------------------

Herramienta simple para monitorear el secuestro de DNS

1: <https://github.com/mdjunior/pharming>

--------------------------------------

PowerUpSQL: un kit de herramientas de PowerShell para atacar SQL Server

1: <https://github.com/NetSPI/PowerUpSQL>

--------------------------------------

Catspin rota la dirección IP de las solicitudes HTTP, lo que hace que los bloques basados ​​en IP o las medidas de ralentización sean ineficaces. Se basa en AWS API Gateway y se implementa a través de AWS Cloudformation.

1: <https://github.com/rootcathacking/catspin>

--------------------------------------

Repositorio pwnspoof

1: <https://github.com/punk-security/pwnspoof>

--------------------------------------

AGREGAR (Servicios de dominio de Active Directory)

1: <https://github.com/DavidGeeraerts/ADDS_Tool>

--------------------------------------

Kit de herramientas de monitoreo y captura de DNS pasivo

1: <https://github.com/mosajjal/dnsmonster>

--------------------------------------

Un marco de prueba de penetración modular

1: <https://github.com/fsociety-team/fsociety>

--------------------------------------

Cavar más profundo....

1: <https://github.com/Velocidex/velociraptor>

--------------------------------------

Túnel de DNS cifrado de extremo a extremo y marco C2

1: <https://github.com/mosajjal/dnspot>

--------------------------------------

Un asistente multiplataforma para crear documentos maliciosos de MS Office. Puede ocultar macros de VBA, pisotear el código de VBA (a través de P-Code) y confundir las herramientas de análisis de macros. Se ejecuta en Linux, OSX y Windows.

1: <https://github.com/outflanknl/EvilClippy>

--------------------------------------

Servidor de comando y control (C2) con puerta trasera que actúa como troyano de administración remota (RAT) escrito en Python3

1: <https://github.com/safesploit/PythonRAT>

--------------------------------------

El destino es la botnet IRC, que se utiliza principalmente para lanzar ataques de denegación de servicio. Propagación mediante exploración aleatoria o de alcance en el puerto SSH y HTTP predeterminado.

1: <https://github.com/boz3r/Fatebot>

--------------------------------------

Capturador completamente no detectado (toma billeteras, contraseñas, cookies, modifica el cliente de discordia, etc.)

1: <https://github.com/doener2323/doenerium>

--------------------------------------

Herramienta de prueba de penetración para juegos desarrollados en el motor de juegos Roblox.

1: <https://github.com/Upbolt/Hydroxide>

--------------------------------------

Doogle es un motor de búsqueda y un rastreador web que puede buscar sitios web e imágenes indexados.

1: <https://github.com/safesploit/Doogle>

--------------------------------------

Herramienta de enumeración de LinkedIn para extraer nombres de empleados válidos de una organización a través del raspado de motores de búsqueda

1: <https://github.com/m8sec/CrossLinked>

--------------------------------------

SIEM de Red Team: herramienta para Red Teams utilizada para rastrear y generar alarmas sobre las actividades de Blue Team, así como una mejor usabilidad en operaciones a largo plazo.

1: <https://github.com/outflanknl/RedELK>

--------------------------------------

⚔️Armas de piratas informáticos web / Una colección de herramientas geniales utilizadas por piratas informáticos web. Feliz piratería, feliz caza de errores

1: <https://github.com/hahwul/WebHackersWeapons>

--------------------------------------

PacketSifter es una herramienta/secuencia de comandos que está diseñada para ayudar a los analistas a filtrar una captura de paquetes (pcap) para encontrar tráfico notable. Packetsifter acepta un pcap como argumento y genera varios archivos.

1: <https://github.com/packetsifter/packetsifterTool>

--------------------------------------

Utilidad rápida de Python que escribí para convertir las solicitudes HTTP de Burp Suite en perfiles Cobalt Strike Maleable C2

1: <https://github.com/CodeXTF2/Burp2Malleable>

--------------------------------------

Obtenga dominios / subdominios relacionados mirando las ID de Google Analytics

1: <https://github.com/Josue87/AnalyticsRelationships>

--------------------------------------

dnsReaper: ¡herramienta de adquisición de subdominios para atacantes, cazarrecompensas de errores y el equipo azul!

1: <https://github.com/punk-security/dnsReaper>

--------------------------------------

HomePwn - Navaja suiza para pentesting de dispositivos IoT

1: <https://github.com/Telefonica/HomePWN>

--------------------------------------

Oculte su carga útil en DNS

1: <https://github.com/mhaskar/DNSStager>

--------------------------------------

Lookyloo es una interfaz web que permite a los usuarios capturar la página de un sitio web y luego mostrar un árbol de dominios que se llaman entre sí.

1: <https://github.com/Lookyloo/lookyloo>

--------------------------------------

Detección de dominios phishing y usurpación de dominios. Admite permutaciones como ataque homógrafo, typosquatting y bitsquatting.

1: <https://github.com/atenreiro/opensquat>

--------------------------------------

Obtener información sobre un documento público de Google.

1: <https://github.com/Malfrats/xeuledoc>

--------------------------------------

pivotool en piratería ética, como era de esperar, es una herramienta simple escrita en bash que podría ayudarlo en la fase posterior a la explotación para pasar a otros sistemas.

1: <https://github.com/artusec/pivotool>

--------------------------------------

Una sencilla aplicación de Android que registra sms en un servidor remoto

1: <https://github.com/ajibigad/sms-logger>

--------------------------------------

Colector de solicitudes HTTP para probar webhooks, notificaciones, clientes REST y más...

1: <https://github.com/darklynx/request-baskets>

--------------------------------------

Tome notas y clasifique los problemas durante una auditoría de código fuente.

1: <https://github.com/belane/CodeAuditor>

--------------------------------------

Una utilidad de inventario robusta y multiplataforma que genera un código QR que contiene las especificaciones del hardware del sistema.

1: <https://github.com/microsoft/InQRy>

--------------------------------------

Una elegante herramienta de monitoreo autohospedada

1: <https://github.com/louislam/uptime-kuma>

--------------------------------------

Una poderosa herramienta de penetración para automatizar tareas de penetración, como escalada de privilegios locales, enumeración, exfiltración y más... Use o cree módulos de automatización para acelerar su vida de seguridad cibernética

1: <https://github.com/Skiller9090/Lucifer>

--------------------------------------

Un servidor web para demostrar la inyección HTML (muy) básica

1: <https://github.com/rdsk-ur/html-injection>

--------------------------------------

dnsx es un conjunto de herramientas de DNS rápido y multipropósito que permite ejecutar múltiples consultas de DNS de su elección con una lista de resoluciones proporcionadas por el usuario.

1: <https://github.com/projectdiscovery/dnsx>

--------------------------------------

CrackQL es una utilidad de fuerza bruta y fuzzing de contraseñas de GraphQL.

1: <https://github.com/nicholasaleks/CrackQL>

--------------------------------------

KIZAGAN es una puerta trasera de la computadora Python y puede tomar fotos de la cámara, capturas de pantalla, obtener

1: sonidos del micrófono... etc.

<https://github.com/st4inl3s5/kizagan>

--------------------------------------

Una colección de módulos de PowerShell diseñados para la recopilación de artefactos y el reconocimiento de puntos finales basados ​​en Windows.

1: <https://github.com/TonyPhipps/Meerkat>

--------------------------------------

Un programa de Python para realizar la reconstrucción del espacio recíproco a partir de mediciones de rayos X de un solo cristal.

1: <https://github.com/aglie/meerkat>

--------------------------------------

Estructuras de datos flexibles para conjuntos de datos complejos de aprendizaje automático.

1: <https://github.com/robustness-gym/meerkat>

--------------------------------------

Un webshell que puede eludir parte de la seguridad del sistema.

1: <https://github.com/22XploiterCrew-Team/Gel4y-Mini-Shell-Backdoor>

--------------------------------------

Wpushell es una herramienta que se utiliza para cargar un shell de puerta trasera en un sitio que utiliza un sistema de gestión de contenido de WordPress con un proceso simple y rápido.

1: <https://github.com/22XploiterCrew-Team/Wpushell>

--------------------------------------

Automatización de pruebas EDR con referencia a MITRE ATTACK a través de Cobalt Strike [Purple Team].

1: <https://github.com/TH3xACE/EDR-Test>

--------------------------------------

Automatización de pruebas EDR con referencia a MITRE ATTACK a través de Cobalt Strike [Purple Team].

1: <https://github.com/TH3xACE/EDR-Test>

--------------------------------------

Esta herramienta tiene como objetivo automatizar la identificación del servicio potencial que se ejecuta detrás de los puertos identificados manualmente, ya sea mediante un escaneo manual o servicios que se ejecutan localmente. La herramienta es útil cuando nmap o cualquier herramienta de escaneo no está disponible y en la situación en la que realizó un escaneo manual de puertos y luego desea identificar los servicios que se ejecutan...

1: <https://github.com/TH3xACE/OFFPORT_KILLER>

--------------------------------------

Arañador de caja de arena

1: <https://github.com/PayloadSecurity/Sandbox_Scryer>

--------------------------------------

Physmem2profit se puede utilizar para crear un minivolcado del proceso LSASS de un host de destino mediante el análisis de la memoria física de forma remota

1: <https://github.com/WithSecureLabs/physmem2profit>

--------------------------------------

Marco CTF y biblioteca de desarrollo de exploits

1: <https://github.com/Gallopsled/pwntools>

--------------------------------------

Android Debug Bridge (adb) era vulnerable a ataques transversales de directorio que podrían haber sido montados por demonios adb no autorizados/comprometidos durante una operación de extracción de adb.

1: <https://github.com/irsl/CVE-2022-20128>

--------------------------------------

PoC de C# para la investigación de técnicas de ejecución de procesos de Windows

1: <https://github.com/daem0nc0re/TangledWinExec>

--------------------------------------

Una herramienta para generar certificados de firma de codigo falso o firma certificados reales

1: <https://github.com/Tylous/Limelighter>

--------------------------------------

Ataques automatizados de inicio de sesión de fuerza bruta contra redes EAP.

1: <https://github.com/Tylous/Auto_EAP>

--------------------------------------

Sudo-Stealer es un programa \*nix para robar contraseñas de Sudo haciéndose pasar por el software Sudo original.

1: <https://github.com/Genaro-Chris/Sudo-Stealer>

--------------------------------------

CVE-2022-36946 pánico del kernel de Linux en netfilter\_queue

1: <https://github.com/Pwnzer0tt1/CVE-2022-36946>

--------------------------------------

Firegex es un cortafuegos de aplicaciones creado para las competiciones CTF Attack-Defence por Pwnzer0tt1

1: <https://github.com/Pwnzer0tt1/firegex>

--------------------------------------

Desarrollo de exploits: exploits armados y prueba de concepto (PoC)

1: <https://github.com/VoidSec/Exploit-Development>

--------------------------------------

marco canbus h4xing rápido y sucio

1: <https://github.com/shipcod3/canTot>

--------------------------------------

Compruebe si su VPN filtra su dirección IP a través de la tecnología WebRTC

1: <https://github.com/VoidSec/WebRTC-Leak>

--------------------------------------

Driver Buddy Reloaded es un complemento IDA Pro Python que ayuda a automatizar algunas tediosas tareas de ingeniería inversa de los controladores del kernel de Windows

1: <https://github.com/VoidSec/DriverBuddyReloaded>

--------------------------------------

Endurecimiento de dispositivos móviles Android

1: <https://github.com/A-YATTA/AMDH>

--------------------------------------

Proxy de Socks4a que aprovecha PIC, Websockets y ofuscación estática en el nivel de ensamblaje

1: <https://github.com/codewhitesec/Lastenzug>

--------------------------------------

Esta secuencia de comandos se desarrolló para realizar un seguimiento del progreso de los informes (captura de pantalla, comandos y resultados) durante el compromiso de pentest y OSCP.

1: <https://github.com/TH3xACE/SCREEN_KILLER>

--------------------------------------

Una herramienta para identificar y explotar las configuraciones incorrectas y las vulnerabilidades de las reglas de Sudo dentro de Sudo para la escalada de privilegios de Linux.

1: <https://github.com/TH3xACE/SUDO_KILLER>

--------------------------------------

Un kit de herramientas de validación y escaneo masivo totalmente automatizado, confiable y súper rápido para la vulnerabilidad Log4J RCE CVE-2021-44228.

1: <https://github.com/0xInfection/LogMePwn>

--------------------------------------

Updog es un reemplazo para SimpleHTTPServer de Python. Permite cargar y descargar a través de HTTP/S, puede configurar certificados SSL ad hoc y usar la autenticación básica de http.

1: <https://github.com/sc0tfree/updog>

--------------------------------------

Una secuencia de comandos de python para obligar automáticamente a un servidor de Windows a autenticarse en una máquina arbitraria a través de 9 métodos.

1: <https://github.com/p0dalirius/Coercer>

--------------------------------------

¡Supervise la creación, la eliminación y los cambios en los objetos LDAP en vivo durante su pentest o administración del sistema!

1: <https://github.com/p0dalirius/LDAPmonitor>

--------------------------------------

Mangle es una herramienta que manipula aspectos de ejecutables compilados (.exe o DLL) para evitar la detección de EDR

1: <https://github.com/optiv/Mangle>

--------------------------------------

Este script fue desarrollado para ayudar en la campaña SpearPhishing durante las operaciones del Equipo Rojo. Se puede usar para generar nombres aleatorios según el país de origen, el sexo y qué tan común puede ser la combinación de apellido y nombre.

1: <https://github.com/TH3xACE/genAvatar>

--------------------------------------

❄️PcapXray: una herramienta forense de red: para visualizar una captura de paquetes fuera de línea como un diagrama de red que incluye la identificación del dispositivo, resalta la comunicación importante y la extracción de archivos

1: <https://github.com/Srinivas11789/PcapXray>

--------------------------------------

Enmascarar enlace

1: <https://github.com/Alcatraz2033/evil-link>

--------------------------------------

Api no oficial de exploits.shodan.io no se necesita clave de api

1: <https://github.com/System00-Security/Explapi>

--------------------------------------

Aplicación de Android para agregar registros de llamadas falsas y eliminar automáticamente su número de teléfono secreto inmediatamente después de finalizar la llamada.

1: <https://github.com/rgajendran/CallMask>

--------------------------------------

personalice su shell con pocos comandos para linux, los comandos son diferentes y para termux, los comandos son diferentes. Y apóyanos en nuestro trabajo.

1: <https://github.com/errorteam07/shell-edit>

--------------------------------------

automatiza las técnicas utilizadas para eludir las restricciones de control de acceso en las páginas de destino. Esta herramienta seguirá desarrollándose, las contribuciones son bienvenidas.

1: <https://github.com/yunemse48/403bypasser>

--------------------------------------

Escáner avanzado de búsqueda de idiotas y exploits masivos

1: <https://github.com/AlisamTechnology/ATSCAN>

--------------------------------------

Salamandra es una herramienta para encontrar micrófonos espía que utilizan radiofrecuencia para transmitir. Utiliza SDR.

1: <https://github.com/eldraco/Salamandra>

--------------------------------------

Todo en una herramienta para facilitar su piratería.

1: <https://github.com/ManasHarsh/Cobra>

--------------------------------------

darm: rastreador de red inteligente para las masas darm es un intento de crear una aplicación muy fácil de usar que rastreará y reportará información sobre las actividades que suceden en una red en vivo. El objetivo principal es educar al público para que tome conciencia de la seguridad de sus comunicaciones. leandrinux está desarrollando darm como un proyecto...

1: <https://github.com/eldraco/darm>

--------------------------------------

Ataque de red Ataque wifi Ataque vlan Ataque arp Ataque Mac Ataque revelado etc../

1: <https://github.com/Matrix07ksa/EvilNet>

--------------------------------------

Un escáner basado en complementos que ayuda a los investigadores de seguridad a identificar problemas con varios CMS, principalmente Drupal y Silverstripe.

1: <https://github.com/SamJoan/droopescan>

--------------------------------------

Biblioteca de Android para acceder a los registros de llamadas del dispositivo

1: <https://github.com/wickerlabs/calllogs>

--------------------------------------

Herramienta para escanear especialmente dispositivos cercanos y ejecutar un comando dado en su propio sistema mientras el dispositivo de destino está dentro del alcance.

1: <https://github.com/souravbaghz/RadareEye>

--------------------------------------

Una herramienta basada en Python para explotar y administrar dispositivos Android a través de ADB

1: <https://github.com/mesquidar/adbsploit>

--------------------------------------

Sistema de detección de tráfico malicioso

1: <https://github.com/stamparm/maltrail>

--------------------------------------

El kit de herramientas de inyección CAN

1: <https://github.com/souravbaghz/Carpunk>

--------------------------------------

escáner de vulnerabilidades de sitios web para termux

1: <https://github.com/TechnicalMujeeb/TM-scanner>

--------------------------------------

Infoooze es una herramienta de inteligencia de código abierto (OSINT) en NodeJs. Proporciona varios módulos que permiten búsquedas eficientes.

1: <https://github.com/7ORP3DO/infoooze>

--------------------------------------

Creador de puertas traseras

1: <https://github.com/KobaWare/Deepsploit>

--------------------------------------

Complemento IDA de depuración de viajes en el tiempo

1: <https://github.com/airbus-cert/ttddbg>

--------------------------------------

El hipervisor UEFI de investigación que admite el arranque de un sistema operativo.

1: <https://github.com/tandasat/MiniVisorPkg>

--------------------------------------

Idioma intermedio de traducción de máquina virtual

1: https://github.com/vtil-project/VTIL-Core

--------------------------------------

Anomalia es un complemento para nfsen que detecta anomalías en las conexiones TCP en función del análisis de flujo.

1: <https://github.com/mdjunior/anomalia>

--------------------------------------

(aquí ningun programa por que a ver tenía un programa que podia controlar las sirenas de Ucrania hackeando su radiofrecuencia y en el programa enseñaba su radiofrecuencia y todo pero lo perdí por razones desconocidas y estoy haciendo omenaje a ese programa perdido 😔)

1: (enlace perdido😔)

--------------------------------------

Bash script que automatiza la enumeración de dominios y servidores DNS en la recopilación de información activa.

1: <https://github.com/dabasanta/DNSExplorer>

--------------------------------------

Un complemento independiente para GnuPG

1: <https://github.com/RichardRMatthews/VSHG>

--------------------------------------

Nmap2acl es una herramienta que hace que los resultados del analizador de un escaneo nmap se conviertan en diferentes tipos de reglas para firewalls. Su función es hacer que el control del perímetro de la red sea eficiente y menos costoso.

1: https://github.com/mdjunior/nmap2acl

--------------------------------------

Herramienta de administración remota de Android

1: <https://github.com/bmshifat/TecSpy>

--------------------------------------

Una API NMAP es una API para la disponibilidad de resultados encontrados por NMAP y ferramentas similares (que compartilhem o mesmo format of saída).

1: <https://github.com/mdjunior/nmap-api>

--------------------------------------

Proyecto muy sencillo para monitorizar pasivamente tu marca frente a respuestas maliciosas

1: <https://github.com/byhardest/dnspharming>

--------------------------------------

un marco de verificación poc de código abierto ligero, flexible y novedoso

1: https://github.com/cckuailong/pocsploit

--------------------------------------

Herramienta criptográfica para pentest y ctf: intente descifrar datos utilizando múltiples algoritmos y modos de encadenamiento de bloques. Útil para una revisión rápida de texto cifrado desconocido y diccionario

1: <https://github.com/Acceis/crypto_identifier>

--------------------------------------

Herramientas de seguridad, escáneres, código de explotación

1: <https://github.com/cudeso/security-tools>

--------------------------------------

Herramienta de ingeniería social para múltiples propósitos, como localizar la ubicación del objetivo, acceder a la cámara web, capturar contraseñas del sistema operativo…

1: https://github.com/IHosseini083/SuperLink

--------------------------------------

Marco para ataques de puntos de acceso Wi-Fi no autorizados

1: <https://github.com/P0cL4bs/WiFi-Pumpkin-deprecated>

--------------------------------------

T-XPLOITER es un programa Perl para detectar e (incluso) explotar sitios web. ¿Por qué el nombre es T-XPLOITER? T significa Triple, XPLOITER significa Explotador. Este programa tiene 3 características y funciones para detectar e (incluso) explotar sitios web, solo échale un vistazo :).

1: <https://github.com/mfazrinizar/T-XPLOITER>

--------------------------------------

Una aplicación de Android de uso gratuito OTP & Call flooding con capacidad de envío ilimitada.

1: <https://github.com/utsanjan/Tsunami-Bomber-Android>

--------------------------------------

Programa CLI que recopila información de los perfiles de usuario de Facebook a través de Selenium.

1: <https://github.com/Godofcoffe/FisherMan>

--------------------------------------

OffensivePH: use el antiguo controlador Process Hacker para omitir varios controles de acceso en modo de usuario

1: <https://github.com/RedSection/OffensivePH>

--------------------------------------

Escanee redes en busca de servidores HTTP, haga cosas cuando los encuentre.

1: <https://github.com/atarantini/httpscan>

--------------------------------------

Escanee redes en busca de servidores SSH con nombre de usuario y contraseña predeterminados

1: <https://github.com/atarantini/sshdefaultscan>

--------------------------------------

Pruebe de forma remota la seguridad de la contraseña del software de blogs de WordPress

1: <https://github.com/atarantini/wpbf>

--------------------------------------

Herramientas de investigación y reconocimiento de Android

1: <https://github.com/jonathandata1/tyr>

--------------------------------------

Ejecución remota de código V1 para iOS 15 enviado a través de airdrop después de que el dispositivo se conectó a un host confiable

1: <https://github.com/jonathandata1/ios_15_rce>

--------------------------------------

Kit de herramientas de ataques de VLAN

1: <https://github.com/in9uz/VLANPWN>

--------------------------------------

Cómo descifrar manualmente la contraseña hash MD5 de los protocolos FHRP.

1: <https://github.com/in9uz/FHRPAuthBypass>

--------------------------------------

Algunas herramientas para realizar ataques a la red.

1: <https://github.com/in9uz/NetworkExploitation>

--------------------------------------

Herramientas para realizar ataques en dominios EIGRP

1: <https://github.com/in9uz/EIGRPWN>

--------------------------------------

Exploits de secuestro de raíz STP y RSTP

1: <https://github.com/in9uz/Grit>

--------------------------------------

Agresor y controlador de persistencia de Zoom

1: <https://github.com/aahmad097/ZoomPersistence>

--------------------------------------

Proyecto para la identificación de ejecutables y DLL vulnerables al secuestro de DLL basado en variables de entorno.

1: <https://github.com/wietze/windows-dll-env-hijacking>

--------------------------------------

Proyecto para identificar ejecutables y DLL vulnerables al secuestro de DLL de ruta relativa.

1: <https://github.com/wietze/windows-dll-hijacking>

--------------------------------------

Proyecto para rastrear oportunidades de secuestro de DLL divulgadas públicamente.

1: <https://github.com/wietze/HijackLibs>

--------------------------------------

Escáner web pasivo con buscador de archivos de copia de seguridad, detector de tecnologías (servidor, waf, ...) capacidades...

1: <https://github.com/w00dyl3g/BurpFeeder>

--------------------------------------

Un marco de prueba negativo, DoLTEst, para encontrar errores que no cumplen con los estándares en las implementaciones del protocolo LTE de los UE

1: <https://github.com/SysSec-KAIST/DoLTEst>

--------------------------------------

Herramienta de análisis de vulnerabilidad de firmware IoT basada en análisis de similitud de código binario (BCSA)

1: <https://github.com/SysSec-KAIST/FirmKit>

--------------------------------------

Una herramienta para SigOver, ataque de ensombrecimiento de señales en las señales de transmisión LTE en el dominio físico.

1: <https://github.com/SysSec-KAIST/sigover_injector>

--------------------------------------

CrossC2 desarrollado en base al marco Cobalt Strike se puede utilizar para el control de otros sistemas multiplataforma. CrossC2Kit proporciona algunas interfaces para que los usuarios llamen para manipular la sesión de CrossC2 Beacon, lo que amplía la funcionalidad de Cobalt Strikeforce

1: <https://github.com/CrossC2/CrossC2Kit>

--------------------------------------

CVE-2021-3560-Polkit-Privilege-Esclation Poc

1: <https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Esclation>

--------------------------------------

Herramienta de omisión de autenticación nps, use esta herramienta para acceder a la página de fondo de la consola web en el navegador, u obtenga calcetines5 y proxy http en lotes

1: <https://github.com/carr0t2/nps-auth-bypass>

--------------------------------------

Organizó 16 tipos de pruebas anti-kill de api basadas en go, 8 tipos de pruebas de cifrado, pruebas anti-sandbox, compilación, ofuscación, empaquetado, modificación de recursos y tecnologías anti-kill, y recopiló algunas herramientas de datos.

1: <https://github.com/TideSec/GoBypassAV>

--------------------------------------

Extraiga las contraseñas de Wi-Fi de Windows a la URL remota

1: <https://github.com/hmaverickadams/Windows-WiFi-Extractor>

--------------------------------------

Cavar más profundo.

1: <https://github.com/Velocidex/velociraptor>

--------------------------------------

Un proxy TCP que usa HTTP: llegue a SSH detrás de un proxy inverso Nginx

1: <https://github.com/julianbuettner/tcp-over-http>

--------------------------------------

Herramienta para buscar y extraer credenciales de archivos de configuración de teléfonos alojados en CUCM

1: <https://github.com/llt4l/iCULeak.py>

--------------------------------------

Herramienta simple para descargar y analizar automáticamente los archivos de configuración de los sistemas telefónicos de Cisco en busca de credenciales SSH.

1: <https://github.com/trustedsec/SeeYouCM-Thief>

--------------------------------------

El objetivo de esta extensión de Burp Suite es la extracción, correlación y presentación estructurada flexible y dinámica de la información del proyecto Burp Suite, así como la modificación sobre la marcha flexible y dinámica de las solicitudes HTTP salientes o entrantes mediante scripts de Python. Por lo tanto, Turbo Data Miner ayudará a obtener una mejor y más rápida

1: <https://github.com/chopicalqui/TurboDataMiner>

--------------------------------------

Extensión de eructo SAML2

1: <https://github.com/CompassSecurity/SAMLRaider>

--------------------------------------

Extensión de Burp Suite: active acciones y modifique el tráfico de solicitudes y respuestas HTTP mediante reglas configurables

1: <https://github.com/synfron/ReshaperForBurp>

--------------------------------------

AD Enum es una herramienta de pentesting que permite encontrar errores de configuración a través del protocolo LDAP y explotar algunas de esas debilidades con kerberos.

1: <https://github.com/SecuProject/ADenum>

--------------------------------------

Herramienta para la enumeración y el abuso de los servicios de certificados de Active Directory

1: <https://github.com/ly4k/Certipy>

--------------------------------------

Módulo de Powershell que pueden utilizar Blue Teams, Incident Responders y System Administrators para buscar persistencias implantadas en máquinas Windows.

1: <https://github.com/last-byte/PersistenceSniper>

--------------------------------------

Durante mis compromisos de respuesta a incidentes, me di cuenta de que descargar datos volátiles siempre se hace mal (o al menos de una manera diferente a la mejor). Además, los datos nunca tienen el mismo formato, lo que hace que el análisis sea más difícil (si no imposible) de automatizar.

1: <https://github.com/gtworek/VolatileDataCollector>

--------------------------------------

Es una herramienta para automatizar el proceso de reconocimiento web, lo que facilita la recopilación de información sobre su objetivo.

1: <https://github.com/Cyber-Guy1/BlackDragon>

--------------------------------------

Mi secuencia de comandos de enumeración de subdominio. Es único en la forma en que está construido.

1: <https://github.com/iamthefrogy/frogy>

--------------------------------------

Mara es un husmeador de pty/tty de usuario

1: <https://github.com/io-tl/Mara>

--------------------------------------

Notify es un paquete de asistencia basado en Go que le permite transmitir el resultado de varias herramientas (o leer de un archivo) y publicarlo en una variedad de plataformas compatibles.

1: <https://github.com/projectdiscovery/notify>

--------------------------------------

Esta herramienta le permitirá suplantar las direcciones de retorno de sus funciones, así como las funciones del sistema.

1: <https://github.com/Barracudach/CallStack-Spoofer>

--------------------------------------

Enumere silenciosamente un dominio de Active Directory a través de LDAP analizando usuarios, administradores, grupos, etc.

1: <https://github.com/layer8secure/SilentHound>

--------------------------------------

Una herramienta para sincronizar un directorio (AD, LDAP, Azure, G Suite, Okta) con una organización.

1: <https://github.com/bitwarden/directory-connector>

--------------------------------------

Análisis de dominios de AD en busca de riesgos de seguridad relacionados con cuentas de usuario

1: <https://github.com/ST1LLY/dc-sonar>

--------------------------------------

Realizar un ataque de suplantación de identidad arp en C

1: <https://github.com/avan-pra/arpmess>

--------------------------------------

Herramienta de detección automática de SSTI con interfaz interactiva

1: <https://github.com/vladko312/SSTImap>

--------------------------------------

Daemon DNS pasivo-recursivo

1: <https://github.com/korc/PR-DNSd>

--------------------------------------

Proxy TCP para simular una latencia de red variable pero predecible🌐⏳

1: <https://github.com/kffl/speedbump>

--------------------------------------

Una secuencia de comandos de python para buscar vulnerabilidades del servidor Apache Tomcat.

1: <https://github.com/p0dalirius/ApacheTomcatScanner>

--------------------------------------

Herramienta de administración remota para Windows

1: <https://github.com/quasar/Quasar>

--------------------------------------

Una herramienta para extraer, modificar y crear paquetes binarios ASDM (CVE-2022-20829)

1: <https://github.com/jbaines-r7/theway>

--------------------------------------

Este repositorio contiene los materiales para la charla "Explorando la superficie de ataque oculta de los dispositivos OEM IoT

1: <https://github.com/infobyte/cve-2022-27255>

--------------------------------------

Herramienta pasiva de búsqueda de nombre de host, dominio e IP para no robots

1: <https://github.com/pirxthepilot/wtfis>

--------------------------------------

Contenedor de taller DEFCON 30 Mainframe buffer overlow

1: <https://github.com/mainframed/DC30_Workshop>

--------------------------------------

Rastreador de ID de usuario y contraseña de sesión de TSO sin cifrar TN3270 de mainframe

1: <https://github.com/mainframed/MFSniffer>

--------------------------------------

Utilidad de Python rápida que escribí para convertir las solicitudes HTTP de Burp Suite en perfiles Cobalt Strike Maleable C2

1: <https://github.com/CodeXTF2/Burp2Malleable>

--------------------------------------

Tiene como objetivo identificar balizas durmientes

1: <https://github.com/thefLink/Hunt-Sleeping-Beacons>

Una técnica avanzada de evasión en memoria que fluctúa la protección de la memoria del shellcode entre RW/NoAccess y RX y luego cifra/descifra su contenido

1: <https://github.com/mgeeky/ShellcodeFluctuation>

--------------------------------------

Este es un proyecto simple hecho para evadir <https://github.com/thefLink/Hunt-Sleeping-Beacons> mediante el uso de una espera ocupada en lugar de la llamada Sleep() integrada de beacon. La mayor parte de la estructura, por ejemplo, Sleep hook, shellcode exec, etc., se toman de

<https://github.com/mgeeky/ShellcodeFluctuation> de mgeeky.

1: <https://github.com/CodeXTF2/BusySleepBeacon>

--------------------------------------

Proxy de Socks4a que aprovecha PIC, Websockets y ofuscación estática en el nivel de ensamblaje

1: <https://github.com/codewhitesec/Lastenzug>

--------------------------------------

A DTrace en la reimplementación de Windows

1: <https://github.com/mandiant/STrace>

--------------------------------------

La herramienta de código abierto del equipo FLARE para identificar capacidades en archivos ejecutables.

1: <https://github.com/mandiant/capa>

--------------------------------------

buscar directorios NTLM

1: <https://github.com/nyxgeek/ntlmscan>

--------------------------------------

localizar y atacar Lync/Skype for Business

1: <https://github.com/nyxgeek/lyncsmash>

--------------------------------------

Una demostración que muestra cómo reutilizar ejecutables, cuentas de servicio y servicios en la nube confiables de Microsoft para potenciar una operación de malware

1: <https://github.com/mbrg/power-pwn>

--------------------------------------

recuperar información a través de O365 y AzureAD con una credencial válida

1: <https://github.com/nyxgeek/o365recon>

--------------------------------------

Zombie Ant Farm: herramientas primitivas y ofensivas para la evasión de EDR de Linux.

1: <https://github.com/dsnezhkov/zombieant>

--------------------------------------

Kit de herramientas de ataque de gestión de código fuente

1: <https://github.com/h4wkst3r/SCMKit>

--------------------------------------

Sistema de inyector de carga util de acoplamiento seccional ELF

1: <https://github.com/dsnezhkov/elfpack>

--------------------------------------

Kit de herramientas de ofuscación de prueba de concepto para herramientas posteriores a la explotación de C#

1: <https://github.com/h4wkst3r/InvisibilityCloak>

--------------------------------------

Proyecto para rastrear oportunidades de secuestro de DLL divulgadas públicamente.

1: <https://github.com/wietze/HijackLibs>

--------------------------------------

Encuentre información confidencial utilizando idiotas de diferentes motores de búsqueda.

1: <https://github.com/R0X4R/Agnee>

--------------------------------------

Cuentagotas Stealth que ejecuta binarios remotos sin colocarlos en el disco. (Soporte HTTP3, soporte ICMP, pistas invisibles, multiplataforma,...)

1: <https://github.com/ariary/fileless-xec>

--------------------------------------

Binario de Golang para exfiltración de datos con protocolo ICMP (+ ICMP bindshell, http sobre túnel ICMP, ...)

1: <https://github.com/ariary/QueenSono>

--------------------------------------

Threatest es un marco Go para las reglas de detección de amenazas de prueba de extremo a extremo.

1: <https://github.com/datadog/threatest>

--------------------------------------

Omitir Malware Sandbox Evasion Ram check

1: <https://github.com/ZeroMemoryEx/Bypass-Sandbox-Evasion>

--------------------------------------

El marco de ataque de la sombra

1: <https://github.com/JoelGMSec/AutoRDPwn>

--------------------------------------

Descifrado de contraseñas de infraestructura cero

1: <https://github.com/JoelGMSec/Cloudtopolis>

--------------------------------------

Convierta solicitudes HTTP GET en consultas LDAP y devuelva resultados JSON.

1: <https://github.com/larsks/ldap2json>

--------------------------------------

ssb=fuerza bruta de subdominio simple

1: <https://github.com/R00tendo/ssb>

--------------------------------------

Escáner de seguridad cibernética completamente automatizado

1: <https://github.com/R00tendo/awacs-scanner>

--------------------------------------

Proteja sus servidores SIP de los malos actores.

1: <https://github.com/SentryPeer/SentryPeer>

--------------------------------------

Un repositorio de plantillas para la gestión de Internet-Draft

1: <https://github.com/martinthomson/internet-draft-template>

--------------------------------------

EDRSandBlastes una herramienta escrita Cque arma un controlador firmado vulnerable para eludir las detecciones EDR (notificar devoluciones de llamada de rutina, devoluciones de llamada de objetos y ETW TIproveedor) y LSASSprotecciones. También se implementan múltiples técnicas de desenganche de áreas de usuarios para evadir el monitoreo de las áreas de usuarios.

1: <https://github.com/wavestone-cdt/EDRSandblast>

--------------------------------------

Las operaciones del equipo rojo involucran habilidades diversas, duran varios meses y son políticamente delicadas; requieren mucho seguimiento, consolidación y cautela. El software de administración de operaciones del equipo rojo de Wavestone, Abaddon, ha sido diseñado para hacer que las operaciones del equipo rojo sean más rápidas, repetibles y sigilosas, al tiempo que incluye herramientas de valor agregado y brinda numerosas capacidades de generación de informes.

1: <https://github.com/wavestone-cdt/abaddon>

--------------------------------------

Cazador de contraseñas en la infame base de datos LDAP

1: <https://github.com/oldboy21/LDAP-Password-Hunter>

--------------------------------------

Gestión de postura de seguridad en la nube (CSPM)

1: <https://github.com/aquasecurity/cloudsploit>

--------------------------------------

una herramienta para ayudar a los pentesters a encontrar dulces deliciosos, por (Twitter: @g3ruben )

1: <https://github.com/SnaffCon/Snaffler>

--------------------------------------

Inyecta cargas útiles de php en imágenes jpeg

1: <https://github.com/dlegs/php-jpeg-injector>

--------------------------------------

Descargue fácilmente aplicaciones de Android en el Subsistema de Windows para Android en Windows 11

1: <https://github.com/infinitepower18/WSA-Sideloader>

--------------------------------------

Extrae las cookies de Chrome.

1: <https://github.com/m0rv4i/SharpCookieMonster>

--------------------------------------

Túneles HTTP(S)/WS(S)/TCP a localhost usando solo SSH.

1: <https://github.com/antoniomika/sish>

--------------------------------------

Script de trazado GeoIP escrito en Python para ayudar a los equipos de seguridad a dibujar informes visualizados a partir de direcciones IP

1: <https://github.com/op7ic/GeoIPPlotter>

--------------------------------------

Marco de pulverización de contraseñas

1: <https://github.com/aahmad097/Tritium>

--------------------------------------

domhttpx es un motor de búsqueda de Google con un kit de herramientas HTTP creado con python, puede facilitarle la búsqueda de muchas URL/IP a la vez con rapidez.

1: <https://github.com/naufalardhani/domhttpx>

--------------------------------------

Una herramienta fácil para restablecer la contraseña de cpanel cuando no puede cargar la puerta trasera al servidor. Esta herramienta será útil solo si la función de restablecimiento de contraseña en cpanel está activada.

1: <https://github.com/naufalardhani/cpanel-pass-reset>

--------------------------------------

RDP monster-in-the-middle (mitm) y biblioteca para Python con la capacidad de ver conexiones en vivo o después del hecho

1: <https://github.com/GoSecure/pyrdp>

--------------------------------------

Obtenga muchas rutas para muchos hosts, sin matar a los hosts

1: <https://github.com/tomnomnom/meg>

--------------------------------------

Tome una lista de dominios y sondee para trabajar con servidores HTTP y HTTPS

1: <https://github.com/tomnomnom/httprobe>

--------------------------------------

Una pequeña herramienta que hice para volcar la tabla de exportación de archivos PE. El caso de uso principal estaba diseñado para usarse dentro del proxy de DLL.

1: <https://github.com/iilegacyyii/ExportDumper>

--------------------------------------

Herramienta para ayudar a aquellos en Ucrania a encontrar rutas alternativas de evacuación de flixbus. Consulta la API de FlixBus (si hay documentación, hágamelo saber) para encontrar rutas desde cualquier ciudad a todas las ciudades en países específicos.

1: <https://github.com/iilegacyyii/FlixBus-Scraper>

--------------------------------------

Marcador GTPv1/GTPv2

1: <https://github.com/fasferraz/gtp_dialer>

--------------------------------------

La herramienta de código abierto del equipo FLARE para identificar capacidades en archivos ejecutables.

1: <https://github.com/mandiant/capa>

--------------------------------------

Marcador NWu IKEv2/IPSec para 5GC / N3IWF

1: <https://github.com/fasferraz/NWu-Non3GPP-5GC>

--------------------------------------

Chepy es un equivalente de python lib/cli de la increíble herramienta CyberChef.

1: <https://github.com/securisec/chepy>

--------------------------------------

un programa similar a edr que engancha algunas llamadas al sistema

1: <https://github.com/ORCx41/W0wS3cur1tyEDR>

--------------------------------------

Moderna red de bots P2P multiplataforma basada en HTTP sobre TOR que no se puede rastrear.

1: <https://github.com/ThrillQuks/Pitraix>

--------------------------------------

🦉🔎Una herramienta simple para auditar su infraestructura de AWS en busca de errores de configuración o posibles problemas de seguridad.

1: <https://github.com/StanGirard/YATAS>

--------------------------------------

Colección de consultas KQL

1: <https://github.com/reprise99/Sentinel-Queries>

--------------------------------------

SEO y auditoría de seguridad para sitios web. Rastreador de Lighthouse & Security Headers, Sitemap/Keywords/Images Extractor, Summarizer, etc...

1: <https://github.com/StanGirard/seo-audits-toolkit>

--------------------------------------

Optik es un conjunto de herramientas de ejecución simbólica que ayudan a los fuzzers de contratos inteligentes

1: <https://github.com/crytic/optik>

--------------------------------------

PXEThief es un conjunto de herramientas que puede extraer contraseñas de la funcionalidad de implementación del sistema operativo en Microsoft Endpoint Configuration Manager.

1: <https://github.com/MWR-CyberSec/PXEThief>

--------------------------------------

Scripts de aprovisionamiento vagabundos para crear un entorno de red simulado para ejercicios de simulación

1: <https://github.com/MWR-CyberSec/tabletop-lab-creation>

--------------------------------------

ARRIBA Todo bugbounty pentesting CVE-2022- POC Exp RCE ejemplo de carga útil Cosas

1: <https://github.com/hktalent/TOP>

--------------------------------------

golang, penetración, ataque, herramienta auxiliar, tnb = árbol nueva abeja

1: <https://github.com/hktalent/goSqlite_gorm>

--------------------------------------

cómo detectar CVE-2020-2551 poc exploit python Weblogic RCE con IIOP

1: <https://github.com/hktalent/CVE-2020-2551>

--------------------------------------

Repositorio oficial vuls Scan: 15000+PoCs; 23 tipos de descifrado de contraseñas de aplicaciones; 7000+huellas dactilares web; 146 protocolos y más de 90000 reglas Escaneo de puertos; Fuzz, HW, increíble BugBounty ( ͡° ͜ʖ ͡°)…

1: <https://github.com/hktalent/scan4all>

--------------------------------------

rootkit LD\_PRELOAD

1: <https://github.com/mav8557/Father>

--------------------------------------

AVML - Adquirir memoria volátil para Linux

1: <https://github.com/microsoft/avml>

--------------------------------------

ParamFirstCheck identifica en una lista de URL aquellas que contienen un parámetro de los 25 principales de los parámetros más vulnerables para SQLi, LFI, RCE y Open redirect

1: <https://github.com/mathis2001/ParamFirstCheck>

--------------------------------------

Playwright es un marco para pruebas y automatización web. Permite probar Chromium, Firefox y WebKit con una sola API.

1: <https://github.com/microsoft/playwright>

--------------------------------------

Kit de herramientas para abusar de Kerberos PKU2U y NegoEx. Requiere impacket Se recomienda instalar impacket directamente desde git para tener la última versión disponible.

1: <https://github.com/morRubin/NegoExRelay>

--------------------------------------

Herramienta para realizar movimiento lateral entre dispositivos unidos AAD

1: <https://github.com/morRubin/AzureADJoinedMachinePTC>

--------------------------------------

Los defensores adaptan constantemente su seguridad para contrarrestar nuevas amenazas.

1: <https://github.com/BC-SECURITY/Beginners-Guide-to-Obfuscation>

--------------------------------------

Invoke-ZeroLogon permite a los atacantes hacerse pasar por cualquier computadora, incluido el propio controlador de dominio, y ejecutar llamadas a procedimientos remotos en su nombre.

1: <https://github.com/BC-SECURITY/Invoke-ZeroLogon>

--------------------------------------

Una colección de módulos de PowerShell diseñados para la recopilación de artefactos y el reconocimiento de puntos finales basados ​​en Windows.

1: <https://github.com/TonyPhipps/Meerkat>

--------------------------------------

Stego es una herramienta de esteganografía gratuita y de código abierto que le permite ocultar su mensaje secreto en una imagen o archivo de audio. No notará ningún cambio en la imagen o el archivo de audio. Sin embargo, su mensaje secreto estará dentro de la imagen original o el archivo de audio.

1: <https://github.com/W1LDN16H7/StegoCracker>

--------------------------------------

Cliente qBittorrent multifacético en Docker

1: <https://github.com/qBitMF/qBitMF>

--------------------------------------

Un escáner de malware multiplataforma minimalista con monitoreo del sistema de archivos en tiempo real sin bloqueo utilizando reglas YARA.

1: <https://github.com/evilsocket/sauron>

--------------------------------------

Reemplazo de GetModuleHandle y GetProcAddress como un Dios

1: <https://github.com/ORCx41/ApiHashing>

--------------------------------------

secureCodeBox (SCB): entrega segura continua lista para usar

1: <https://github.com/secureCodeBox/secureCodeBox>

--------------------------------------

Una herramienta de gestión de eventos e información de seguridad en tiempo real y de código abierto basada en tecnologías de big data, que proporciona un marco de análisis de seguridad avanzado y escalable.

1: <https://github.com/G-Research/siembol>

--------------------------------------

Matos es una herramienta de seguridad en la nube de código abierto para analizar la seguridad de la infraestructura de múltiples nubes.

1: <https://github.com/cloudmatos/Matos>

--------------------------------------

CloudBunny es una herramienta para capturar la IP real del servidor que utiliza un WAF como proxy o protección. En esta herramienta utilizamos tres motores de búsqueda para buscar información de dominio: Shodan, Censys y Zoomeye.

1: <https://github.com/Warflop/CloudBunny>

--------------------------------------

Una puerta trasera web PHP simple le permite recuperar el contenido del directorio/archivo y cargar archivos desde la máquina local o la URL remota.

1: <https://github.com/aqhmal/simple-php-web-backdoor>

--------------------------------------

Un envenenador de caché de DNS dirigido

1: <https://github.com/cr0mll/deserter>

--------------------------------------

Manejador de concha de Penélope

1: <https://github.com/brightio/penelope>

--------------------------------------

Una herramienta de ingeniería inversa Flutter/Dart

1: <https://github.com/rscloura/Doldrums>

--------------------------------------

Proyecto que contiene varias herramientas/scripts para recuperar las claves de sesión de OpenSSH utilizadas para cifrar/descifrar el tráfico SSH.

1: <https://github.com/fox-it/OpenSSH-Session-Key-Recovery>

--------------------------------------

Encuentra dominios y subdominios relacionados con un dominio dado

1: <https://github.com/tomnomnom/assetfinder>

--------------------------------------

Redirigir el tráfico TCP, UDP e ICMP (específico) a otro destino.

1: <https://github.com/jellever/StreamDivert>

--------------------------------------

Proyecto para descifrar y analizar el tráfico SSH

1: <https://github.com/fox-it/OpenSSH-Network-Parser>

--------------------------------------

LittleCorporal: AC# Generador de Maldoc Automatizado

1: <https://github.com/connormcgarr/LittleCorporal>

--------------------------------------

tgtdelegation es un Beacon Object File (BOF) para obtener un TGT utilizable a través del "truco de delegación de TGT"

1: <https://github.com/connormcgarr/tgtdelegation>

--------------------------------------

Un servidor HTTP simple para entregar y filtrar archivos/datos durante, por ejemplo, CTF.

1: <https://github.com/IngoKl/HTTPUploadExfil>

--------------------------------------

Envoltura de Multi-Packer que nos permite conectar en cadena varios packers, ofuscadores y otras armas orientadas al Red Team. Presentado con marca de agua de artefactos, colección de IOC y puerta trasera de PE. Lo alimentas con tu implante, hace muchas cosas furtivas y escupe un ejecutable ofuscado.

1: <https://github.com/mgeeky/ProtectMyTooling>

--------------------------------------

Una técnica avanzada de evasión en memoria que fluctúa la protección de la memoria del shellcode entre RW/NoAccess y RX y luego cifra/descifra su contenido

1: <https://github.com/mgeeky/ShellcodeFluctuation>

--------------------------------------

Cobalt Strike C2 Proxy inverso que evita Blue Teams, AV, EDR, escáneres a través de la inspección de paquetes y la correlación de perfil maleable

1: <https://github.com/mgeeky/RedWarden>

--------------------------------------

Un PoC que empaqueta las cargas útiles en contenedores de salida para evadir el indicador Mark-of-the-Web y demostrar los riesgos asociados con los formatos de archivo de contenedor. Compatible con: ZIP, 7zip, PDF, ISO, IMG, CAB, VHD, VHDX

1: <https://github.com/mgeeky/PackMyPayload>

--------------------------------------

Analice rápidamente y aplique ingeniería inversa a los paquetes de Android

1: <https://github.com/1N3/ReverseAPK>

--------------------------------------

Plataforma de gestión de superficie de ataque | Sn1perSecurity LLC

1: <https://github.com/1N3/Sn1per>

--------------------------------------

Navaja suiza Webserver en Golang. Manténgase simple como Python SimpleHTTPServer pero con muchas características

1: <https://github.com/nodauf/Swego>

--------------------------------------

Transferir archivo a través de Dns

1: <https://github.com/nodauf/ToDns>

--------------------------------------

Proxy [Buscador | Comprobador | Servidor]. HTTP(S) Y CALCETINES🎭

1: <https://github.com/constverum/ProxyBroker>

--------------------------------------

🔪Dumper & ripper para bots de Telegram por token

1: <https://github.com/soxoj/telegram-bot-dumper>

--------------------------------------

📖Recopile enlaces a perfiles por nombre de usuario a través de motores de búsqueda y analícelos con varios complementos

1: <https://github.com/soxoj/marple>

--------------------------------------

🕵️‍♂️Recopile un expediente sobre una persona por nombre de usuario de miles de sitios

1: <https://github.com/soxoj/maigret>

--------------------------------------

⛏️Extraiga información de cuentas de páginas personales en varios sitios para fines OSINT

1: <https://github.com/soxoj/socid-extractor>

--------------------------------------

Esta herramienta busca todos los formularios y entradas que se encuentran en una lista de URL. Este script extrae la información del código de la aplicación web.

1: <https://github.com/xtormin/formshunter>

--------------------------------------

Un kit de herramientas HTTP para la investigación de seguridad.

1: <https://github.com/dstotijn/hetty>

--------------------------------------

Un potente generador de capas inversas

1: <https://github.com/FlyfishSec/rcX>

--------------------------------------

cve2019\_2725, CNVD-C-2019-48814 Weblogic \_async exp de ejecución de comando remoto

1: <https://github.com/FlyfishSec/weblogic_rce>

--------------------------------------

rsGen es un generador de carga útil de Shell inverso para piratear.

1: <https://github.com/FlyfishSec/rsGen>

--------------------------------------

Convertidor de cargas útiles de RubberDucky sin procesar a la fuente Digispark Arduino IDE Sketch.

1: <https://github.com/mame82/duck2spark>

--------------------------------------

P4wnP1 - Canal encubierto WiFi - Agente de cliente (Prueba de concepto experimental) por MaMe82

1: <https://github.com/mame82/P4wnP1_WiFi_covert_channel_client>

--------------------------------------

Herramienta para buscar archivos secretos en servidores HTTP

1: <https://github.com/hannob/snallygaster>

--------------------------------------

Escáner de secuestro de aplicaciones para macOS

1: <https://github.com/bashexplode/boko>

--------------------------------------

kit de herramientas de phishing de token de un solo uso

1: <https://github.com/bashexplode/otu-plz>

--------------------------------------

Realice OSINT en objetivos externos usando Shodan

1: <https://github.com/stavinski/showdown>

--------------------------------------

Transforma el flujo UDP en flujos TCP (falsos) que pueden atravesar firewalls/NAT de capa 3 y capa 4 (NAPT).

1: <https://github.com/dndx/phantun>

--------------------------------------

Capacitación práctica en análisis forense de Windows

1: <https://github.com/bluecapesecurity/PWF>

--------------------------------------

Análisis forense del navegador web para Google Chrome/Chromium

1: <https://github.com/obsidianforensics/hindsight>

--------------------------------------

Ejecute captura de banderas y entrenamientos de seguridad con OWASP Juice Shop

1: <https://github.com/iteratec/multi-juicer>

--------------------------------------

Crear un dominio de Active Directory y hackearlo

1: <https://github.com/chryzsh/DarthSidious>

--------------------------------------

Una herramienta de administración y monitoreo remoto, construida con Django, Vue y Go.

1: <https://github.com/amidaware/tacticalrmm>

--------------------------------------

Esta herramienta brinda a desarrolladores, investigadores y empresas la capacidad de analizar paquetes de software de diferentes lenguajes de programación que están siendo o serán utilizados en sus códigos, brindándoles información que les permite saber con anticipación si esta librería cumple con los procesos. desarrollo seguro, si actualmente es compatible, posibles puertas traseras (malicio...

1: <https://github.com/TelefonicaTC2Tech/packagedna>

--------------------------------------

Una herramienta de pentesting de generador de tráfico turbo para generar tráfico aleatorio con direcciones MAC e IP aleatorias, además de números de secuencia aleatorios para una IP y un puerto en particular.

1: <https://github.com/mytechnotalent/turbo-attack>

--------------------------------------

Un motor de automatización de código abierto que puede realizar una automatización completa de front-end y back-end para extraer datos, además de la automatización de pruebas con la integración de Docker y Kubernetes.

1: <https://github.com/mytechnotalent/CortexaAI>

--------------------------------------

RedDrop es un servidor web rápido y fácil para capturar y procesar cargas útiles y archivos tar codificados y encriptados.

1: <https://github.com/cyberbutler/RedDrop>

--------------------------------------

Rem es un editor de código de terminal para uso personal que hace la mayoría de las cosas que hacen los editores de terminal, pero es una implementación muy básica.

1: <https://github.com/Hifumi1337/rem>

--------------------------------------

Us3r Unl0ck3d es un escáner de permisos creado para escanear la mayoría de los entornos Linux y Windows. Devuelve todos los archivos accesibles por el usuario actualmente conectado utilizando un patrón octal.

1: <https://github.com/Hifumi1337/us3r-unl0ck3d>

--------------------------------------

Aplicación con vulnerabilidad de inyección SQL y posible escalada de privilegios. Aplicación vulnerable gratuita para capacitación en pruebas de penetración / piratería ética.

1: <https://github.com/filipkarc/sqli-postgres-rce-privesc-hacking-playground>

--------------------------------------

CONSEJOS 2018

1: <https://github.com/Ridter/Intranet_Penetration_Tips>

--------------------------------------

Explotación de CVE-2021-42278 y CVE-2021-42287 para hacerse pasar por DA del usuario de dominio estándar

1: <https://github.com/Ridter/noPac>

--------------------------------------

Preparación para el examen de Especialista en Seguridad Cibernética con Diploma Federal Suizo

1: <https://github.com/phr85/swiss-cyber-defence>

--------------------------------------

Encuentre la instancia de Microsoft Exchange para un dominio determinado e identifique la versión exacta

1: <https://github.com/mhaskar/ExchangeFinder>

--------------------------------------

Oculte su carga útil en DNS

1: <https://github.com/mhaskar/DNSStager>

--------------------------------------

¡Guía de compilación completa para crear su propio lector RFID de cuello de cisne de largo alcance!

1: <https://github.com/sh0ckSec/RFID-Gooseneck>

--------------------------------------

zyxel\_ipc\_camera\_pwn

1: <https://github.com/hydrogen18/zyxel_ipc_camera_pwn>

--------------------------------------

Este proyecto va a diseñar un sitio web de citas de seguridad que es para hacer amigos. Los usuarios se registran y visitan el sitio web de citas para encontrar amigos adecuados y chatear con nuevos amigos.

1: <https://github.com/HKSSY/EIE3117_Dating_Website>

--------------------------------------

¡Este programa de python obtiene todas las contraseñas, tarjetas de crédito y marcadores guardados de los navegadores basados ​​en cromo compatibles con cromo 80 y superior!

1: <https://github.com/henry-richard7/Browser-password-stealer>

--------------------------------------

Programa AC# que obtiene la dirección IP de los jugadores en un lobby público de GTA Online.

1: <https://github.com/henry-richard7/Grand-Theft-Auto-Online-IP-Grabber>

--------------------------------------

Marco de evaluación de la seguridad de la plataforma

1: <https://github.com/chipsec/chipsec>

--------------------------------------

Una herramienta de piratería y Pentesting para Linux y Windows

1: <https://github.com/i-am-unbekannt/unbekannt-framework>

--------------------------------------

Conchas y contenedores instantáneos, fáciles y predecibles.

1: <https://github.com/jetpack-io/devbox>

--------------------------------------

Un túnel basado en reglas en Go.

1: <https://github.com/Dreamacro/clash>

--------------------------------------

puerto web de choque

1: <https://github.com/Dreamacro/clash-dashboard>

--------------------------------------

EDR de código abierto para Windows

1: <https://github.com/0xrawsec/whids>

--------------------------------------

EvilCrowRF-V2

1: <https://github.com/joelsernamoreno/EvilCrowRF-V2>

--------------------------------------

Analizador de seguridad de configuración para dispositivos de red. Pynipper-ng es una evolución de nipper-ng, actualizado y traducido a python. [versión ALFA]

1: <https://github.com/syn-4ck/pynipper-ng>

--------------------------------------

Un ejemplo de escucha TCP que se puede detener en Go

1: <https://github.com/hydrogen18/stoppableListener>

--------------------------------------

Una utilidad rápida y sucia para capturar y almacenar sondas WiFi.

1: <https://github.com/hydrogen18/probecap>

--------------------------------------

Drone Hacking Tool es una herramienta GUI que funciona con un adaptador WiFi USB y HackRF One para piratear drones.

1: https://github.com/HKSSY/Drone-Hacking-Tool

--------------------------------------

RediSea es un marco de comunicación de Redis (base de datos en memoria) que se utiliza para ver claves de Redis, volcar claves de Redis, volcar información clave sobre el servidor de Redis, análisis de bases de datos de Redis en tiempo real y mucho más.

1: <https://github.com/Hifumi1337/RediSea>

--------------------------------------

Una herramienta de detección de servicios y escáner de puertos que utiliza 1000 gorutinas a la vez para escanear la ip o fqdn de cualquier host con el único propósito de probar su propia red para asegurarse de que no haya servicios maliciosos en ejecución.

1: <https://github.com/mytechnotalent/turbo-scanner>

--------------------------------------

Un completo y GRATUITO tutorial de desarrollo de Python en línea PARA NIÑOS que utiliza una placa de desarrollo micro: bit oficial de la BBC que avanza paso a paso en el mundo de Python para microcontroladores.

1: <https://github.com/mytechnotalent/Python-For-Kids>

--------------------------------------

Un completo tutorial GRATUITO de ingeniería inversa que cubre las arquitecturas x86, x64, ARM de 32 bits y ARM de 64 bits.

1: https://github.com/mytechnotalent/Reverse-Engineering

--------------------------------------

Extraiga y visualice datos de URL utilizando Unfurl

1: <https://github.com/obsidianforensics/unfurl>

--------------------------------------

Buscador de cookies de sesión

1: <https://github.com/darklotuskdb/goSCF>

--------------------------------------

Kit de herramientas de explotación multipropósito Metasploit para Termux

1: <https://github.com/isuruwa/MSF-ANDRO>

--------------------------------------

Sistema detector de mascarillas construido con aprendizaje automático (Curso Procesamiento de Imágenes y Tesis).

1: <https://github.com/medpaf/face-mask-detector>

--------------------------------------

Manejador de shell invertido y enlazado elegante

1: <https://github.com/calebstewart/pwncat>

--------------------------------------

Una colección de vulnerabilidades del administrador de trabajos de impresión de Windows en contenedores con otras utilidades para una explotación práctica.

1: <https://github.com/BeetleChunks/SpoolSploit>

--------------------------------------

[TRABAJANDO EN V2, CON PROXIES, USER AGENT PERSONALIZADO... ¡MUCHO MEJOR!] DorkMe es una herramienta diseñada con el propósito de facilitar la búsqueda de vulnerabilidades con Google Dorks, como vulnerabilidades de SQL Injection.

1: <https://github.com/blueudp/DorkMe>

--------------------------------------

Deep Explorer es una herramienta (desarrollada en 1 día) hecha en python que tiene como finalidad la búsqueda de servicios ocultos en la red tor, utilizando Ahmia Browser y rastreando los enlaces obtenidos

1: <https://github.com/blueudp/Deep-Explorer>

--------------------------------------

Generador automático de carcasa inversa

1: <https://github.com/d4t4s3c/shelly>

--------------------------------------

Repetición automática de solicitudes HTTP con Burp Suite

1: <https://github.com/nccgroup/AutoRepeater>

--------------------------------------

Rastreador de IP real Cloudflare, Sucuri, Incapsula.

1: <https://github.com/mrh0wl/Cloudmare>

--------------------------------------

Shell inverso basado en SSH

1: <https://github.com/NHAS/reverse_ssh>

--------------------------------------

Cloudlist es una herramienta para enumerar activos de múltiples proveedores de nube.

1: <https://github.com/projectdiscovery/cloudlist>

--------------------------------------

Un servidor de recopilación de interacción OOB y una biblioteca de cliente

1: <https://github.com/projectdiscovery/interactsh>

--------------------------------------

Predecir la probabilidad de que se publique un exploit después de que se publique un CVE (mediante un algoritmo de aprendizaje automático)

1: <https://github.com/wisoffe/exploits-predict>

--------------------------------------

CVE-2022-40297 - Prueba de concepto: escalada de privilegios en Ubuntu Touch 16.04 - por PIN Bruteforce

1: <https://github.com/filipkarc/PoC-ubuntutouch-pin-privesc>

--------------------------------------

Voluntad dll.exe

1: <https://github.com/Ciyfly/microwaveo>

--------------------------------------

el mejor buscador de hazañas/referencias

1: <https://github.com/ARPSyndicate/xlocate>

--------------------------------------

toma de huellas dactilares de favicon

1: <https://github.com/ARPSyndicate/favinizer>

--------------------------------------

enumeración y escaneo automatizados de activos web

1: <https://github.com/ARPSyndicate/kenzer>

--------------------------------------

Módulo de PowerShell para exportar una copia local de todos los objetos y valores de configuración de Azure Active Directory.

1: <https://github.com/microsoft/azureadexporter>

--------------------------------------

MemoryRanger protege los datos y el código del kernel mediante la ejecución de controladores y el alojamiento de datos en enclaves de kernel aislados mediante funciones VT-x y EPT. MemoryRanger se ha presentado en BlackHat, HITB, CDFSL.

1: <https://github.com/IgorKorkin/MemoryRanger>

--------------------------------------

Una herramienta que escanea una lista de dominios dados y devuelve los códigos de estado para cada dominio en los puertos 80 y 443

1: <https://github.com/0xApt/subzer0>

--------------------------------------

BadBlood de @davidprowe , Secframe.com, llena un dominio de Microsoft Active Directory con una estructura y miles de objetos. La salida de la herramienta es un dominio similar a un dominio en el mundo real. Después de ejecutar BadBlood en un dominio, los analistas de seguridad y los ingenieros pueden practicar el uso de herramientas para comprender y prescribir la protección de Active...

1: <https://github.com/davidprowe/BadBlood>

--------------------------------------

Bóveda de fichas en memoria BOF para Cobalt Strike

1: <https://github.com/Henkru/cs-token-vault>

--------------------------------------

Una secuencia de comandos de Python para aprovechar las actualizaciones del paquete de software CVE-2022-36446 RCE (autenticado) en Webmin < 1.997.

1: <https://github.com/p0dalirius/CVE-2022-36446-Webmin-Software-Package-Updates-RCE>

--------------------------------------

Script de enumeración de escalada de privilegios para Windows

1: <https://github.com/itm4n/PrivescCheck>

--------------------------------------

Bug's feed es un portal alojado localmente donde puede buscar las últimas noticias, videos, CVE, vulnerabilidades...

1: <https://github.com/PwnedShell/Bugs-feed>

--------------------------------------

Rustcat (rcat): el escucha de puerto moderno y el shell inverso

1: <https://github.com/robiot/rustcat>

--------------------------------------

un exploit de ejecución remota de código de VMWare Workspace ONE Access

1: <https://github.com/sourceincite/hekate>

--------------------------------------

50+ Gadgets (20 Más que ysoserial). JNDI-Injection-Exploit-Plus es una herramienta para generar enlaces JNDI viables y proporcionar servicios en segundo plano iniciando el servidor RMI, el servidor LDAP y el servidor HTTP.

1: <https://github.com/cckuailong/JNDI-Injection-Exploit-Plus>

--------------------------------------

OpenWRT SDK para dispositivos GL.iNet

1: <https://github.com/gl-inet/sdk>

--------------------------------------

Cobalt Strike UDRL para la evasión del escáner de memoria.

1: <https://github.com/kyleavery/AceLdr>

--------------------------------------

Este repositorio cubre algunos métodos de ejecución de código y evasión AV para macros en documentos de Office

1: <https://github.com/S3cur3Th1sSh1t/OffensiveVBA>

--------------------------------------

el falsificador de cuentas invisible

1: <https://github.com/r4wd3r/Suborner>

--------------------------------------

descargar archivos a través de DoH, o descargar y ejecutar un shellcode

1: <https://github.com/darksh3llRU/dark-doh>

--------------------------------------

ParamChanger es una herramienta que le permite reemplazar los parámetros de una lista de URL por una carga útil ingresada como argumento

1: <https://github.com/mathis2001/ParamChanger>

--------------------------------------

Herramienta Python Recon pasiva simple para la enumeración de subdominios con crt.sh

1: <https://github.com/mathis2001/Cert4Recon>

--------------------------------------

LighTraversal es una herramienta diseñada para encontrar vulnerabilidades básicas de cruce de directorios

1: <https://github.com/mathis2001/LighTraversal>

--------------------------------------

ParamFirstCheck identifica en una lista de URL aquellas que contienen un parámetro de los 25 principales de los parámetros más vulnerables para SQLi, LFI, RCE y Open redirect

1: <https://github.com/mathis2001/ParamFirstCheck>

--------------------------------------

ParamChanger es una herramienta que le permite reemplazar los parámetros de una lista de URL por una carga útil ingresada como argumento

1: <https://github.com/mathis2001/ParamChanger>

--------------------------------------

Una colección de cargas útiles de Burpsuite Intruder, cargas útiles de BurpBounty, listas fuzz, cargas de archivos maliciosos y metodologías y listas de verificación de pentesting web.

1: <https://github.com/1N3/IntruderPayloads>

--------------------------------------

🛡️La capa de seguridad de seguridad de GraphQL que falta para los servidores Apollo GraphQL y Yoga/Envelop🛡️

1: <https://github.com/Escape-Technologies/graphql-armor>

--------------------------------------

un marco para fuzzers modulares y reutilizables

1: <https://github.com/AFLplusplus/libafl_paper_artifacts>

--------------------------------------

Shell inverso de Powershell usando el protocolo HTTP/S con omisión de AMSI y Proxy Aware

1: <https://github.com/3v4Si0N/HTTP-revshell>

--------------------------------------

Un desempaquetador y registrador automático para archivos de destino de DotNet Framework

1: <https://github.com/advanced-threat-research/DotDumper>

--------------------------------------

OFRAK: desempaquetar, modificar y reempaquetar binarios.

1: <https://github.com/redballoonsecurity/ofrak>

--------------------------------------

Contrabandista de solicitudes HTTP

1: <https://github.com/portswigger/http-request-smuggler>

--------------------------------------

Esquema OCSF

1: <https://github.com/ocsf/ocsf-schema>

--------------------------------------

Una secuencia de comandos de Python para aprovechar las actualizaciones del paquete de software CVE-2022-36446 RCE (autenticado) en Webmin < 1.997.

1: <https://github.com/p0dalirius/CVE-2022-36446-Webmin-Software-Package-Updates-RCE>

--------------------------------------

Detectar programa Bug Bounty

1: <https://github.com/xcapri/dProgBb>

--------------------------------------

Obtener nombre de usuario y contraseña de Chrome.

1: <https://github.com/justjavac/chrome_password.js>

--------------------------------------

AzureGoat: una maldita infraestructura vulnerable de Azure

1: <https://github.com/ine-labs/AzureGoat>

--------------------------------------

Escáner de vulnerabilidades rápido y personalizable basado en DSL simple basado en YAML.

1: <https://github.com/projectdiscovery/nuclei>

--------------------------------------

herramienta para generar listas de palabras o ampliar una existente mediante mutaciones.

1: <https://github.com/d4rckh/gorilla>

--------------------------------------

🌀Un generador de actividad sin sentido

1: <https://github.com/svenstaro/genact>

--------------------------------------

🌟¡Para cuando realmente solo quiera servir algunos archivos a través de HTTP ahora mismo!

1: <https://github.com/svenstaro/miniserve>

--------------------------------------

La herramienta de verificación🚀detrás de nuestra plataforma de análisis de seguridad a gran escala para detectar paquetes de código abierto maliciosos/riesgosos

1: <https://github.com/ossillate-inc/packj>

--------------------------------------

PowerHuntShares es un script de auditoría diseñado para inventariar, analizar e informar privilegios excesivos configurados en dominios de Active Directory.

1: <https://github.com/NetSPI/PowerHuntShares>

--------------------------------------

Baton Drop (CVE-2022-21894): Vulnerabilidad de omisión de la función de seguridad de arranque seguro

1: <https://github.com/Wack0/CVE-2022-21894>

--------------------------------------

Msmap es un generador de WebShell de memoria.

1: <https://github.com/hosch3n/msmap>

--------------------------------------

Herramienta de descubrimiento y explotación de inclusión de archivos locales

1: <https://github.com/hansmach1ne/lfimap>

--------------------------------------

Herramienta de prueba de penetración para juegos desarrollados en el motor de juegos Roblox.

1: <https://github.com/Upbolt/Hydroxide>

--------------------------------------

¡Un módulo de PowerShell que encuentra archivos, carpetas y su información de una manera realmente rápida y fácil!

1: <https://github.com/eizedev/PSItems>

--------------------------------------

Herramienta de detección de directorio/archivo, DNS y VHost escrita en Go

1: <https://github.com/OJ/gobuster>

--------------------------------------

DefectDojo es una herramienta de administración de vulnerabilidades y DevSecOps.

1: <https://github.com/DefectDojo/django-DefectDojo>

--------------------------------------

Scripts para hacer que los ataques de rociado de contraseñas contra Lync/S4B, OWA y O365 sean mucho más rápidos, menos dolorosos y más eficientes

1: <https://github.com/byt3bl33d3r/SprayingToolkit>

--------------------------------------

Herramienta de inventario web, toma capturas de pantalla de páginas web usando Pyppeteer (Chrome/Chromium sin interfaz gráfica) y proporciona algunas campanas y silbatos adicionales para hacer la vida más fácil.

1: <https://github.com/byt3bl33d3r/WitnessMe>

--------------------------------------

Cargador Syscall Shellcode (trabajo en curso)

1: <https://github.com/icyguider/Shhhloader>

--------------------------------------

Transfiera archivos hacia y desde un host de Windows a través de ICMP en entornos de red restringidos.

1: <https://github.com/icyguider/ICMP-TransferTools>

--------------------------------------

Pingtunnel es una herramienta que envía tráfico TCP/UDP sobre ICMP

1: <https://github.com/esrrhs/pingtunnel>

--------------------------------------

Avance más profundamente en las redes al descubrir hosts y puertos, utilizando una máquina comprometida a través de SSH

1: <https://github.com/Xeonrx/Puwr>

--------------------------------------

BlueHound es una herramienta de código abierto que ayuda a los equipos azules a identificar los problemas de seguridad que realmente importan.

1: <https://github.com/zeronetworks/BlueHound>

--------------------------------------

Elimine los servicios de EDR eliminando todos los identificadores abiertos del proceso de EDR.

1: <https://github.com/waawaa/breakcyserver>

--------------------------------------

CustomXMLPart como arma de PoC para ocultar el código de malware dentro de las estructuras de documentos de Office.

1: <https://github.com/mgeeky/CustomXMLPart>

--------------------------------------

Catspin rota la dirección IP de las solicitudes HTTP, lo que hace que los bloques basados ​​en IP o las medidas de ralentización sean ineficaces. Se basa en AWS API Gateway y se implementa a través de AWS Cloudformation.

1: <https://github.com/rootcathacking/catspin>

--------------------------------------

una herramienta para reducir la entropía de su carga útil, funciona agregando bytes nulos, en una secuencia ordenada: cada 10 bytes agrega 5 bytes nulos.

1: <https://gitlab.com/ORCA000/entropyfix>

--------------------------------------

Una implementación de agresor de ataque de cobalto encriptado .NET XOR para chisel para utilizar un proxy más rápido y capacidades avanzadas de socks5.

1: <https://github.com/m3rcer/Chisel-Strike>

--------------------------------------

Herramienta de informes de Pentesting

1: <https://github.com/micro-joan/BlackStone>

--------------------------------------

¡Un marco con módulos publicados como BlestSploit Framework, Exploits, Payloads, Posts y más!

1: <https://github.com/G00Dway/BlestSploit>

--------------------------------------

Airdiscovery, monitorea redes y realiza ataques de deauth usando Airdiscovery

1: <https://github.com/G00Dway/Airdiscovery>

--------------------------------------

AFlasher es un Flasher avanzado de Android, que muestra sus archivos de forma remota desde su computadora (USB, ADB)

1: <https://github.com/G00Dway/AFlasher>

--------------------------------------

Esta herramienta extrae números de tarjetas de crédito, NTLM (DCE-RPC, HTTP, SQL, LDAP, etc.), Kerberos (AS-REQ Pre-Auth etype 23), HTTP Basic, SNMP, POP, SMTP, FTP, IMAP, etc. archivo pcap o desde una interfaz en vivo.

1: <https://github.com/lgandx/PCredz>

--------------------------------------

Esta herramienta extrae números de tarjetas de crédito, NTLM (DCE-RPC, HTTP, SQL, LDAP, etc.), Kerberos (AS-REQ Pre-Auth etype 23), HTTP Basic, SNMP, POP, SMTP, FTP, IMAP, etc. archivo pcap o desde una interfaz en vivo.

1: <https://github.com/lgandx/PCredz>

--------------------------------------

Escáner de vulnerabilidades rápido y personalizable basado en DSL simple basado en YAML.

1: <https://github.com/projectdiscovery/nuclei>

--------------------------------------

Un repositorio de herramientas para pentesting de entornos restringidos y aislados.

1: <https://github.com/InfosecMatter/Minimalistic-offensive-security-tools>

--------------------------------------

Navaja suiza Herramienta proxy para captura, manipulación y reproducción de tráfico HTTP/HTTPS sobre la marcha.

1: <https://github.com/projectdiscovery/proxify>

--------------------------------------

Conjunto de datos de huellas dactilares alternativo de nnposter para el script Nmap http-default-accounts

1: <https://github.com/nnposter/nndefaccts>

--------------------------------------

Convierta PuTTY en una herramienta de fuerza bruta de inicio de sesión SSH.

1: <https://github.com/InfosecMatter/SSH-PuTTY-login-bruteforcer>

--------------------------------------

Uso de la herramienta cURL para OSINT (Inteligencia de código abierto)

1: <https://github.com/C3n7ral051nt4g3ncy/cURL_for_OSINT>

--------------------------------------

Exploit shell root para varios routers Xiaomi: 4A Gigabit, 4A 100M, 4, 4C, 3Gv2, 4Q, miWifi 3C...

1: <https://github.com/acecilia/OpenWRTInvasion>

--------------------------------------

EasyPen es un programa GUI que ayuda a los pentesters a recopilar información, escanear y explotar vulnerabilidades.

1: <https://github.com/lijiejie/EasyPen>

--------------------------------------

Cross Site "Scripter" (también conocido como XSSer) es un -marco- automático para detectar, explotar y reportar vulnerabilidades XSS en aplicaciones basadas en web.

1: <https://github.com/epsylon/xsser>

--------------------------------------

Escáner de paso débil HTTP

1: <https://github.com/lijiejie/htpwdScan>

--------------------------------------

Herramienta de registro DNS/HTTP optimizada para pentesters, más rápida y fácil de usar.

1: <https://github.com/lijiejie/eyes.sh>

--------------------------------------

Tracer es una herramienta OSINT que se puede utilizar para detectar en qué sitios web se está utilizando actualmente un nombre de usuario

1: <https://github.com/chr3st5an/tracer>

--------------------------------------

Ejecute procesos completos de pentesting combinando múltiples herramientas de piratería automáticamente

1: <https://github.com/pablosnt/rekono>

--------------------------------------

OpenArk es una herramienta anti-rookit (ARK) de código abierto para Windows.

1: <https://github.com/BlackINT3/OpenArk>

--------------------------------------

Herramienta RPC Monitor basada en Event Tracing para Windows

1: <https://github.com/cyberark/RPCMon>

--------------------------------------

Un Poc sobre el bloqueo de Procmon para que no supervise los eventos de la red

1: <https://github.com/ORCx41/EtwSessionHijacking>

--------------------------------------

usando el kct para ejecutar su shellcode al estilo apt

1: <https://github.com/ORCx41/KctHijackLib>

--------------------------------------

reducir la entropía de su carga útil

1: <https://github.com/ORCx41/EntropyFix>

--------------------------------------

Este repositorio contiene las herramientas que usamos en nuestra investigación sobre el chip Google Titan M.

1: <https://github.com/quarkslab/titanm>

--------------------------------------

Biblioteca de Python con CLI que permite volcar de forma remota las credenciales de usuario del dominio a través de un ADCS sin volcar la memoria del proceso LSASS

1: <https://github.com/Z4kSec/Masky>

--------------------------------------

QCSuper es una herramienta que se comunica con teléfonos y módems basados ​​en Qualcomm, lo que permite capturar tramas de radio 2G/3G/4G sin procesar, entre otras cosas.

1: <https://github.com/P1sec/QCSuper>

--------------------------------------

Clouditor es una herramienta para respaldar la garantía continua de la nube. Desarrollado por Fraunhofer AISEC.

1: <https://github.com/clouditor/clouditor>

--------------------------------------

Un ofuscador de Python que utiliza solicitudes HTTP y Hastebin.

1: <https://github.com/billythegoat356/Jawbreaker>

--------------------------------------

Una herramienta de Python3 que le permite ofuscar su secuencia de comandos y camuflar la ofuscación.

1: <https://github.com/billythegoat356/Specter>

--------------------------------------

Un capturador de tokens de Discord escrito en Python3, con una increíble ofuscación y protección anti-depuración.

1: <https://github.com/billythegoat356/Plague>

--------------------------------------

Herramientas y artículos técnicos que describen técnicas de ataque que se basan en ocultar la ejecución de código en Windows

1: <https://github.com/huntandhackett/concealed_code_execution>

--------------------------------------

¡Supervise la creación, la eliminación y los cambios en los objetos LDAP en vivo durante su pentest o administración del sistema!

1: <https://github.com/p0dalirius/LDAPmonitor>

--------------------------------------

Solitude es una herramienta de análisis de privacidad que permite a cualquiera realizar sus propias investigaciones de privacidad. Ya sea un novato curioso o un investigador más avanzado, Solitude hace que el proceso de evaluación de la privacidad del usuario dentro de una aplicación sea accesible para todos.

1: <https://github.com/nccgroup/Solitude>

--------------------------------------

Smuggler: una herramienta de prueba de desincronización/contrabando de solicitudes HTTP escrita en Python 3

1: <https://github.com/defparam/smuggler>

--------------------------------------

Kit de herramientas de reconocimiento, prueba, enumeración y eXploitation general de VPN

1: <https://github.com/klezVirus/vortex>

--------------------------------------

Escáner Pentesting popular en Python3.6 para SQLi/XSS/LFI/RFI y otras vulnerabilidades

1: <https://github.com/v3n0m-Scanner/V3n0M-Scanner>

--------------------------------------

SysWhispers on Steroids: evasión AV/EDR a través de llamadas directas al sistema.

1: <https://github.com/klezVirus/SysWhispers3>

--------------------------------------

Marco de evasión AV/EDR basado en plantillas

1: <https://github.com/klezVirus/inceptor>

--------------------------------------

Herramienta para automatizar la redirección abierta desde un sitio web.

1: <https://github.com/PishangShedappp/OPdirect>

--------------------------------------

Servidor SMTP falso que imprime correos electrónicos en la salida estándar

1: <https://github.com/soveran/mailcat>

--------------------------------------

Una bifurcación y sucesora de Sulley Fuzzing Framework

1: <https://github.com/jtpereyda/boofuzz>

--------------------------------------

Un escáner de host virtual que realiza búsquedas inversas, se puede usar con herramientas pivote, detecta escenarios generales, soluciona comodines, alias y páginas predeterminadas dinámicas.

1: <https://github.com/codingo/VHostScan>

--------------------------------------

Un DNS bruteforcer personalizado con subprocesos múltiples y manejo de resolutores defectuosos.

1: <https://github.com/codingo/fastsub>

--------------------------------------

Esta aplicación es un panel XSS avanzado, se utiliza para capturar sesiones con explotación XSS y <img src="grabber\_url">

1: <https://github.com/Inplex-sys/cookies-sniffer>

--------------------------------------

¡Un bypass uam de cloudflare en funcionamiento!

1: <https://github.com/Inplex-sys/cloudflare-uam-bypass>

--------------------------------------

Comparta archivos de forma segura y anónima, aloje sitios web y chatee con amigos usando la red Tor

1: <https://github.com/onionshare/onionshare>

--------------------------------------

Automatización de pruebas simplificada

1: <https://github.com/karatelabs/karate>

--------------------------------------

FazScan es un programa de Perl para realizar análisis de vulnerabilidades y pentesting |

1: <https://github.com/mfazrinizar/FazScan>

--------------------------------------

Potente kit de herramientas Discord OSINT escrito en Python

1: <https://github.com/darvester/darvester>

--------------------------------------

Un complemento de Firefox para investigaciones OSINT

1: <https://github.com/vincenzocaputo/FoxyRecon>

--------------------------------------

Srelay: el proxy SOCKS y Relay (importado de sourceforge)

1: <https://github.com/gco/srelay>

--------------------------------------

La retransmisión NTLM para Windows simplificada

1: <https://github.com/CCob/lsarelayx>

--------------------------------------

Necesito más información

1: <https://github.com/zeronetworks/rpcfirewall>

--------------------------------------

🥧HTTPie para Terminal: cliente HTTP de línea de comandos moderno y fácil de usar para la era API. Compatibilidad con JSON, colores, sesiones, descargas, complementos y más.

1: <https://github.com/httpie/httpie>

--------------------------------------

httpcat es una utilidad simple para construir solicitudes HTTP sin formato en la línea de comandos.

1: <https://github.com/httpie/httpcat>

--------------------------------------

Un cliente interactivo de prueba de API y HTTP de línea de comandos creado sobre HTTPie que incluye autocompletado, resaltado de sintaxis y más.

1: <https://github.com/httpie/http-prompt>

--------------------------------------

Ataques de Oracle de relleno de subprocesos múltiples contra cualquier servicio. Escrito en óxido.

1: <https://github.com/Kibouo/rustpad>

--------------------------------------

Un kit de herramientas HTTP para la investigación de seguridad.

1: <https://github.com/dstotijn/hetty>

--------------------------------------

⛤Generador Keylogger para Windows escrito en Python⛤

1: <https://github.com/FZGbzuw412/SATANKLGR>

--------------------------------------

SyntheticSun es un marco de monitoreo y automatización de seguridad de defensa en profundidad que utiliza inteligencia de amenazas, aprendizaje automático, servicios de seguridad de AWS administrados y tecnologías sin servidor para prevenir, detectar y responder continuamente a las amenazas.

1: <https://github.com/jonrau1/SyntheticSun>

--------------------------------------

Supervise continuamente su superficie de ataque de AWS y evalúe los servicios en busca de configuraciones que puedan provocar la degradación de la confidencialidad, la integridad o la disponibilidad. Todos los resultados se pueden exportar a Security Hub, JSON, CSV, bases de datos y más para una mayor agregación y análisis.

1: <https://github.com/jonrau1/ElectricEye>

--------------------------------------

Script para automatizar, cuando sea posible, el reconocimiento pasivo realizado en un sitio web previo a una evaluación.

1: <https://github.com/righettod/website-passive-reconnaissance>

--------------------------------------

Sugerencia de vulnerabilidades de Windows: próxima generación

1: <https://github.com/bitsadmin/wesng>

--------------------------------------

ReVBShell - Shell VBS inverso

1: <https://github.com/bitsadmin/revbshell>

--------------------------------------

Sugerencia de vulnerabilidades de Windows: próxima generación

1: <https://github.com/bitsadmin/wesng>

--------------------------------------

Carga útil de Meterpreter para todas las plataformas

1: <https://github.com/Err0r-ICA/Venomsploit>

--------------------------------------

Scrape Pastebin API para recopilar pegados diarios, configurar una lista de palabras y recibir alertas por correo electrónico cuando tenga una coincidencia.

1: <https://github.com/pixelbubble/PasteMonitor>

--------------------------------------

Script Bash para verificar si un dominio o una lista de dominios se pueden falsificar en función de los registros DMARC

1: <https://github.com/v4d1/SpoofThatMail>

--------------------------------------

🤖Huellas dactilares falsas para eludir los sistemas anti-bot. Simule las operaciones del mouse y el teclado para comportarse como una persona real.

1: <https://github.com/kkoooqq/fakebrowser>

--------------------------------------

Dispositivo real Android, teléfono en la nube, simulador para control grupal de múltiples dispositivos. Evite la detección del sistema anti-bot. Admite RPC, NAT transversal.

1: <https://github.com/kkoooqq/fake-android>

--------------------------------------

Marco Wi-Fi para crear pruebas de concepto, experimentos automatizados, conjuntos de pruebas, fuzzers y más.

1: <https://github.com/domienschepers/wifi-framework>

--------------------------------------

Una herramienta de escritorio de Windows que permite al usuario controlar activamente las conexiones Wi-Fi

1: <https://github.com/emoacht/Wifinian>

--------------------------------------

Generador de páginas HTML desfiguradas

1: <https://github.com/Err0r-ICA/DefGen>

--------------------------------------

Una herramienta avanzada para trabajar con tokens de acceso y política de seguridad de Windows.

1: <https://github.com/diversenok/TokenUniverse>

--------------------------------------

Flutter hace que sea fácil y rápido crear hermosas aplicaciones para dispositivos móviles y más allá

1: <https://github.com/flutter/flutter>

--------------------------------------

Marco de ingeniería inversa de Flutter

1: <https://github.com/Impact-I/reFlutter>

--------------------------------------

Analice las solicitudes HTTP para minimizar los riesgos de ataques de desincronización HTTP (precursor del contrabando/división de solicitudes HTTP).

1: <https://github.com/aws/http-desync-guardian>

--------------------------------------

Esta herramienta ayuda a detectar y explotar el contrabando de solicitudes HTTP en los casos en que se puede lograr a través de la conversión HTTP/2 -> HTTP/1.1 por parte del servidor frontend.

1: <https://github.com/neex/http2smugl>

--------------------------------------

Este es un pequeño conjunto de utilidades DNS de configuración cero para ayudar en la detección y explotación de vulnerabilidades relacionadas con SSRF. Proporciona una utilidad de reenlace de DNS fácil de usar, así como una forma de obtener registros de recursos resolubles con cualquier contenido dado.

1: <https://github.com/neex/1u.ms>

--------------------------------------

Puerta trasera de autenticación NTLM de Windows

1: <https://github.com/kindtime/nosferatu>

--------------------------------------

Este es un proyecto educativo que envía el registro de pulsaciones de teclas de la máquina de destino a un servidor en la nube mediante la creación de una puerta trasera.

1: <https://github.com/kesaralive/BitzLogger>

--------------------------------------

Esta secuencia de comandos de Python se puede usar para eludir las restricciones de origen de IP mediante encabezados HTTP.

1: <https://github.com/p0dalirius/ipsourcebypass>

--------------------------------------

El mejor script de ataque DDoS Python3, ataque (Cyber ​​/ DDos) con 56 métodos

1: <https://github.com/MatrixTM/MHDDoS>

--------------------------------------

Verifique que el asn se pueda usar para la modificación del encabezado de IP o no

1: <https://github.com/MatrixTM/IPHM-Checker>

--------------------------------------

Kit de herramientas AC# MS SQL diseñado para reconocimiento ofensivo y post-explotación.

1: <https://github.com/skahwah/SQLRecon>

--------------------------------------

Obtener y analizar certificados SSL

1: <https://github.com/skahwah/CheckCert>

--------------------------------------

Otro ofuscador de PHP

1: <https://github.com/Cvar1984/yapo>

--------------------------------------

Subprocesos múltiples OTP Spam Amp/Paralell

1: <https://github.com/Cvar1984/LiteOTP>

--------------------------------------

Un motor de búsqueda de texto completo con todas las funciones escrito en PHP

1: <https://github.com/teamtnt/tntsearch>

--------------------------------------

Nuke Discord Bot en Js (Beta ha llegado)

1: <https://github.com/17teen/Discord-Presser-Server-Nuker>

--------------------------------------

Verificador de números de DNI de Perú, solo mayores de edad.

1: <https://github.com/Monkey-hk4/dni-checker>

--------------------------------------

Androidqf (Android Quick Forensics) ayuda a recopilar rápidamente evidencia forense de dispositivos Android, para identificar posibles rastros de compromiso.

1: <https://github.com/botherder/androidqf>

--------------------------------------

Pcqf (PC Quick Forensics) ayuda a recopilar rápidamente evidencia forense de los sistemas Windows, Mac y Linux para identificar posibles rastros de compromiso.

1: <https://github.com/botherder/pcqf>

--------------------------------------

La Guía de prueba de seguridad móvil (MSTG) es un manual completo para la prueba de seguridad de aplicaciones móviles y la ingeniería inversa. Describe los procesos técnicos para verificar los controles enumerados en el Estándar de verificación de seguridad de aplicaciones móviles (MASVS) de OWASP.

1: <https://github.com/OWASP/owasp-mstg>

--------------------------------------

Ingeniería inversa WhatsApp Web.

1: <https://github.com/sigalor/whatsapp-web-reveng>

--------------------------------------

Explotar el desarrollo y la ingeniería inversa con GDB Made Easy

1: <https://github.com/pwndbg/pwndbg>

--------------------------------------

Una herramienta de geolocalización OSINT para Telegram que encuentra usuarios y grupos cercanos📡🌍🔍

1: <https://github.com/Alb-310/Geogramint>

--------------------------------------

Explotación de PoC de PrintNightmare (CVE-2021-34527)

1: <https://github.com/m8sec/CVE-2021-34527>

--------------------------------------

Pymeta buscará en la web archivos en un dominio para descargar y extraer metadatos. Esta técnica se puede utilizar para identificar: dominios, nombres de usuario, números de versión/software y convenciones de nomenclatura.

1: <https://github.com/m8sec/pymeta>

--------------------------------------

Pre2k es una herramienta para consultar la existencia de objetos informáticos anteriores a Windows 2000 que se pueden aprovechar para afianzarse en un dominio de destino.

1: <https://github.com/garrettfoster13/pre2k>

--------------------------------------

Script de enumeración de escalada de privilegios para Windows

1: <https://github.com/itm4n/PrivescCheck>

--------------------------------------

Cree una carga útil completamente inadvertida convirtiéndola en PDF. Sin macros.

1: <https://github.com/luci61/Exe-to-pdf>

--------------------------------------

Complemento Burp para almacenar en caché tokens de autenticación desde una URL de "autenticación" y luego agregarlos como encabezados en todas las solicitudes que van a un determinado alcance.

1: <https://github.com/nccgroup/jwt-reauth>

--------------------------------------

Whalescan es un escáner de vulnerabilidades para contenedores de Windows, que realiza varias comprobaciones comparativas, además de comprobar si hay CVE/paquetes vulnerables en el contenedor.

1: <https://github.com/nccgroup/whalescan>

--------------------------------------

Redpanda es una plataforma de transmisión de datos para desarrolladores. Compatible con la API de Kafka. 10 veces más rápido. Sin ZooKeeper. ¡Sin JVM!

1: <https://github.com/redpanda-data/redpanda>

--------------------------------------

Limpiar una lista de URL

1: <https://github.com/xnl-h4ck3r/urless>

--------------------------------------

🛡️¡Haga que sus servicios web sean seguros por defecto!

1: <https://github.com/bunkerity/bunkerweb>

--------------------------------------

Agente Swift 5 macOS

1: <https://github.com/MythicAgents/hermes>

--------------------------------------

Repositorio público para arnés de prueba atómica

1: <https://github.com/redcanaryco/AtomicTestHarnesses>

--------------------------------------

Pruebas de detección pequeñas y altamente portátiles basadas en ATT&CK de MITRE.

1: <https://github.com/redcanaryco/atomic-red-team>

--------------------------------------

yaranges un experimento centrado en el nuevo motor de análisis para YARA, que se basa en compilar el conjunto de reglas de YARA en código nativo

1: <https://github.com/avast/yarang>

--------------------------------------

Desofusque las cargas útiles de Log4Shell con facilidad.

1: <https://github.com/ox-eye/Ox4Shell>

--------------------------------------

Herramienta de enumeración de LinkedIn para extraer nombres de empleados válidos de una organización a través del raspado de motores de búsqueda

1: <https://github.com/m8sec/CrossLinked>

--------------------------------------

Realice la enumeración de subdominios a través de varias técnicas y obtenga resultados detallados para ayudar en pruebas adicionales.

1: <https://github.com/m8sec/subscraper>

--------------------------------------

Kit de herramientas de ataque de gestión de código fuente

1: <https://github.com/h4wkst3r/SCMKit>

--------------------------------------

Ejecute este raspador gratis

1: <https://github.com/vdrmota/Social-Media-and-Contact-Info-Extractor>

--------------------------------------

Escáner de vulnerabilidades sin agente para Linux, FreeBSD, Container, WordPress, bibliotecas de lenguajes de programación, dispositivos de red

1: <https://github.com/future-architect/vuls>

--------------------------------------

Busque y busque rápidamente a través de los registros de eventos de Windows

1: <https://github.com/WithSecureLabs/chainsaw>

--------------------------------------

Una aplicación de kit de herramientas de investigación NFC para Android

1: <https://github.com/nfcgate/nfcgate>

--------------------------------------

DirtyCred es un concepto de explotación del kernel que intercambia las credenciales del kernel sin privilegios

1: <https://github.com/markakd/DirtyCred>

--------------------------------------

La mejor herramienta para el phishing, el futuro del phishing

1: <https://github.com/bhikandeshmukh/shark>

--------------------------------------

Rastreador de ubicación GPS preciso (teléfonos Android, IOS, Windows).

1: <https://github.com/bhikandeshmukh/MapEye>

--------------------------------------

Un sistema de detección de intrusos basado en aprendizaje automático

1: <https://github.com/PoCInnovation/SmartShark>

--------------------------------------

Un marco Ruby diseñado para ayudar en las pruebas de penetración de los sistemas WordPress.

1: <https://github.com/rastating/wordpress-exploit-framework>

--------------------------------------

¡Mi marco más avanzado hasta ahora!

1: <https://github.com/samyoyo/Trity-1>

--------------------------------------

Herramienta de ataque mongoDB basada en python2.7.x (consulte NoSQLMap)

1: h[ttps://github.com/sixwha1e/MongoAttack](http://ttps://github.com/sixwha1e/MongoAttack)

--------------------------------------

Herramienta OSINT en Twitter e Instagram.

1: <https://github.com/xadhrit/terra>

--------------------------------------

Capturas de paquetes de ataques ddos ​​del mundo real

1: <https://github.com/StopDDoS/packet-captures>

--------------------------------------

FUZZBUNCH – Herramientas de seguridad de la NSA

1: https://github.com/exploitx3/FUZZBUNCH

--------------------------------------

Una RAT malvada (herramienta de administración remota) para macOS / OS X.

1: <https://github.com/Marten4n6/EvilOSX>

--------------------------------------

Un visor de imágenes de investigación médica de JavaScript puro.

1: <https://github.com/rii-mango/Papaya>

--------------------------------------

Matos es una herramienta de seguridad en la nube de código abierto para analizar la seguridad de la infraestructura de múltiples nubes.

1: <https://github.com/cloudmatos/Matos>

--------------------------------------

Kit de herramientas de software de inspección profunda de paquetes de código abierto

1: <https://github.com/ntop/nDPI>

--------------------------------------

Monitoreo de tráfico de red de seguridad y tráfico basado en web

1: <https://github.com/ntop/ntopng>

--------------------------------------

Marco OSINT avanzado de Github

1: https://github.com/rly0nheart/octosuite

--------------------------------------

Herramienta para descifrar hashes de contraseñas como MD5, SHA1, SHA256, PDF encriptado, archivo comprimido encriptado y muchos otros hashes de contraseñas🤘🤘

1: <https://github.com/ASHWIN990/JTRE>

--------------------------------------

Herramienta de inyección NoSQL para omitir formularios de inicio de sesión y extraer nombres de usuario/contraseñas mediante expresiones regulares.

1: <https://github.com/eversinc33/Papaya>

--------------------------------------

Hunter - Asistente de Pentesting: recopilación de información y más.

1: <https://github.com/Keyj33k/Hunter-Toolkit>

--------------------------------------

Un shell inverso para Linux. Escrito en Python3.

1: <https://github.com/Keyj33k/ReverseShell>

--------------------------------------

Escáner de seguridad WPScan WordPress. Escrito para profesionales de seguridad y mantenedores de blogs para probar la seguridad de sus sitios web de WordPress.

1: <https://github.com/wpscanteam/wpscan>

--------------------------------------

Una herramienta de explotación POST-XSS.

1: <https://github.com/t3l3machus/toxssin>

--------------------------------------

Herramienta de automatización de flujo de trabajo basada en nodos con licencia de código justo, gratuita y abierta. Automatice fácilmente las tareas en diferentes servicios.

1: <https://github.com/n8n-io/n8n>

--------------------------------------

Cloudsplaining es una herramienta de evaluación de seguridad de AWS IAM que identifica violaciones de privilegios mínimos y genera un informe con prioridad de riesgo.

1: <https://github.com/salesforce/cloudsplaining>

--------------------------------------

JA3 es un estándar para crear huellas digitales de clientes SSL de una manera fácil de producir y compartir.

1: <https://github.com/salesforce/ja3>

--------------------------------------

⚡Potente, personalizable y fácil de usar Instagram dm bot. ¡Con TUI y GUI de Electron.js! Uso de Selenium webdriver y archivos de configuración de Yaml. (WIP)

1: <https://github.com/hbollon/IGopher>

--------------------------------------

Merlion: un marco de aprendizaje automático para la inteligencia de series temporales

1: <https://github.com/salesforce/Merlion>

--------------------------------------

PasteExploit es un generador de comandos malicioso para sistemas Windows y Linux escrito en Python

1: <https://github.com/trhacknon/PasteExploit>

--------------------------------------

Ejecute exploits interactivos de Android en Linux.

1: <https://github.com/sundaysec/Andspoilt>

--------------------------------------

PEASS - Suite de scripts impresionantes de escalada de privilegios (con colores)

1: <https://github.com/carlospolop/PEASS-ng>

--------------------------------------

Analizador WiFi y Bluetooth basado en GUI de próxima generación para Linux

1: <https://github.com/ghostop14/sparrow-wifi>

--------------------------------------

Optiva-marco🔎Escáner de aplicaciones web🕵️

1: https://github.com/joker25000/Optiva-Framework

--------------------------------------

Esta es una herramienta simple de reconocimiento de nombre de usuario. Puede buscar un nombre de usuario en más de 200 plataformas de redes sociales diferentes.

1: <https://github.com/vijaysahuofficial/UserReCon>

--------------------------------------

Script para generar paquetes debian maliciosos (troyanos debain).

1: <https://github.com/ChaitanyaHaritash/kimi>

--------------------------------------

Herramienta de Google dorking

1: <https://github.com/rly0nheart/oxdork>

--------------------------------------

💀Subdominio – Buscando Subdominio Del sitio

1: <https://github.com/joker25000/subdomain>

--------------------------------------

🕵️‍♂️Marco ofensivo de Google.

1: <https://github.com/mxrch/GHunt>

--------------------------------------

Rastreador increíblemente rápido diseñado para OSINT.

1: <https://github.com/s0md3v/Photon>

--------------------------------------

🛡️¡Haga que sus servicios web sean seguros por defecto!

1: <https://github.com/bunkerity/bunkerweb>

--------------------------------------

The spy's job es una Herramienta enfocada al OSINT la cual cuenta con los mejores métodos para recolectar Información sobre algo o alguien. Como todas las Herramientas creadas por XDeadHackerX una de las mejores cualidades es la automatización de todos los procesos. [NO ME HAGO RESPONSABLE DEL MAL USO DE ESTA HERRAMIENTA]

1: <https://github.com/XDeadHackerX/The_spy_job>

--------------------------------------

DongTai es un producto de prueba de seguridad de aplicaciones interactivas (IAST) que admite la detección de vulnerabilidades OWASP WEB TOP 10, vulnerabilidades relacionadas con solicitudes múltiples (incluidas vulnerabilidades lógicas, vulnerabilidades de acceso no autorizado, etc.), vulnerabilidades de componentes de terceros, etc.

1: <https://github.com/HXSecurity/DongTai>

--------------------------------------

Potente herramienta y gema de análisis de parámetros y escaneo XSS

1: <https://github.com/hahwul/XSpear>

--------------------------------------

🔑Authz0 es una herramienta de prueba de autorización automatizada. El acceso no autorizado se puede identificar en función de las URL y las funciones y credenciales.

1: <https://github.com/hahwul/authz0>

--------------------------------------

Automatización para pruebas internas de penetración de Windows / AD-Security

1: <https://github.com/S3cur3Th1sSh1t/WinPwn>

--------------------------------------

Omisión de UAC, Elevate, Métodos de persistencia

1: <https://github.com/rootm0s/WinPwnage>

--------------------------------------

UIAccess UAC Bypass mediante duplicación de tokens y eventos de teclado

1: <https://github.com/rootm0s/UUB>

--------------------------------------

Bustr es una utilidad creada para descubrir si se ha conectado/emparejado con el sistema algún nuevo dispositivo USB, almacenamiento, teléfono o Bluetooth.

1: <https://github.com/rootm0s/Bustr>

--------------------------------------

Servidores de escalamiento y scripts para escalamiento privado

1: <https://github.com/Shiva108/escalationserver>

--------------------------------------

encuentre los parámetros que se pueden usar para encontrar SSRF o carga de recursos fuera de banda

1: <https://github.com/knassar702/lorsrf>

--------------------------------------

TRIFECTA es un script por lotes que le permite buscar una frase o palabras clave con 12 motores de búsqueda diferentes, ya sea de forma individual o simultánea.

1: <https://github.com/V1XX-1/TRIFECTA-Search-Tool>

--------------------------------------

Otro corredor de shellcode🦀 🐚

1: <https://github.com/b1tg/rs_shellcode>

--------------------------------------

evilginx2 + gophish

1: <https://github.com/fin3ss3g0d/evilgophish>

--------------------------------------

Esta extensión debería agregar una serie de características funcionales y de interfaz de usuario a Burp Suite para facilitar el trabajo.

1: <https://github.com/mdsecresearch/BurpSuiteSharpener>

--------------------------------------

CPH:SEC WAES: Web Auto Enum & Scanner: enumera automáticamente los sitios web y volca los archivos como resultado

1: <https://github.com/Shiva108/WAES>

--------------------------------------

Bandit es una herramienta diseñada para encontrar problemas de seguridad comunes en el código de Python.

1: <https://github.com/PyCQA/bandit>

--------------------------------------

Bandit es un servidor HTTP Elixir puro para aplicaciones Plug

1: <https://github.com/mtrudel/bandit>

--------------------------------------

Un exploit de escalada de privilegios en Steam Client

1: <https://github.com/alexanderbittner/steam-privesc>

--------------------------------------

explotación de mantenimiento azul

1: <https://github.com/NAXG/cve_2019_0708_bluekeep_rce>

--------------------------------------

Herramienta ofensiva para escanear y explotar vulnerabilidades en Microsoft Windows sobre el protocolo Samba (SMB) utilizando Metasploit Framework.

1: <https://github.com/d4t4s3c/SMBploit>

--------------------------------------

Extensión para Burp Suite que utiliza AWS API Gateway para cambiar su IP en cada solicitud.

1: <https://github.com/mrhacker51/BurpSuiteBypassWAF>

--------------------------------------

Keylogger es un keylogger 100% invisible no solo para los usuarios, sino también indetectable por el software antivirus. Registrador de teclas Blackcat Supervisa todas las pulsaciones de teclas, clics del mouse. Tiene un proceso separado que continúa capturando la captura de pantalla del sistema y enviándola al servidor ftp en un tiempo dado.

1: <https://github.com/ajayrandhawa/Keylogger>

--------------------------------------

Crypter - Generador basado en Python3 y ransomware compilado en ejecutable de Windows usando PyInstaller

1: <https://github.com/sithis993/Crypter>

--------------------------------------

Shell inverso en archivo de acceso directo (.lnk)

1: <https://github.com/jaivikpatel147/badlnk>

--------------------------------------

Generador de carga útil FUD win32 msfvenom

1: <https://github.com/jermainlaforce/catchyou>

--------------------------------------

Marco de prueba de penetración MODBUS

1: <https://github.com/0x0mar/smod>

--------------------------------------

Un interceptor de tráfico y paquetes de red para Linux. Spoof ARP & Wiretap A Network.

1: <https://github.com/MandConsultingGroup/Espionage>

--------------------------------------

Una herramienta de Python para verificar la vulnerabilidad de adquisición de subdominios

1: <https://github.com/r3curs1v3-pr0xy/sub404>

--------------------------------------

Shell de Gmail, para que los piratas informáticos ejecuten comandos a través de gmail

1: <https://github.com/RiadhBenlamine/gmail-shell>

--------------------------------------

Servicio de alojamiento de archivos autoimplementable para equipos rojos, lo que permite cargar y compartir fácilmente cargas útiles a través de HTTP y WebDAV.

1: <https://github.com/kgretzky/pwndrop>

--------------------------------------

PENIOT: herramienta de prueba de penetración para IoT

1: <https://github.com/yakuza8/peniot>

--------------------------------------

¡Rubyfu, donde Ruby se vuelve malvado!

1: <https://github.com/rubyfu/RubyFu>

--------------------------------------

Un script de enumeración de Linux para Hack The Box

1: <https://github.com/SolomonSklash/htbenum>

--------------------------------------

Ransomware simple pero agudo

1: <https://github.com/r3nt0n/markransom>

--------------------------------------

marco de explotación posterior de Android ADB

1: <https://github.com/security007/sword>

--------------------------------------

Herramienta de automatización de ataques DDoS a través de la red Tor

1: <https://github.com/r3nt0n/torDDoS>

--------------------------------------

Marco de botnet con arquitectura modular y extensible, programador de tareas, sesiones en vivo de shell remotas y una interfaz retro que hace que su uso sea divertido. Por ahora, incluye keylogger, DDoS y ataques de fuerza bruta. El proyecto aún está en fase de desarrollo, agradezco cualquier contribución 1: <https://github.com/r3nt0n/zombiegang>

--------------------------------------

Esta es una combinación de una herramienta de hacking y cracking.

1: <https://github.com/Mayur-Debu/Kissing-Bug>

--------------------------------------

Arbitrium es un troyano de acceso remoto multiplataforma totalmente indetectable para controlar Android, Windows y Linux y no requiere excepciones de firewall ni reglas de reenvío de puertos.

1: <https://github.com/im-hanzou/Arbitrium-RAT>

--------------------------------------

EXOCET: herramienta de entrega de carga útil indetectable que evade AV

1: <https://github.com/tanc7/EXOCET-AV-Evasion>

--------------------------------------

HTTP fuzzer engine orientado a la seguridad

1: <https://github.com/htrgouvea/nozaki>

--------------------------------------

Un motor para hacer de la red Tor su puerta de enlace predeterminada

1: <https://github.com/htrgouvea/nipe>

--------------------------------------

[WIP] Un ecosistema de rastreadores para detectar: ​​fugas, exposición de datos confidenciales e intentos de exfiltración de datos

1: <https://github.com/htrgouvea/harpoon>

--------------------------------------

Generador de shell inverso alojado con un montón de funcionalidad. -- (Ideal para CTF)

1: <https://github.com/0dayCTF/reverse-shell-generator>

--------------------------------------

espiar las consultas de DNS que realiza tu ordenador

1: <https://github.com/jvns/dnspeep>

--------------------------------------

Escáner rápido de vulnerabilidades de configuración incorrecta de CORS🍻

1: <https://github.com/chenjj/CORScanner>

--------------------------------------

C2/marco posterior a la explotación

1: <https://github.com/loseys/BlackMamba>

--------------------------------------

Goblyn es una herramienta de Python enfocada a la enumeración y captura de metadatos de archivos de sitios web.

1: <https://github.com/loseys/Goblyn>

--------------------------------------

Un generador de criptomineros gratuito silencioso (oculto): admite ETH, ETC, XMR y muchos más.

1: <https://github.com/UnamSanctam/SilentCryptoMiner>

--------------------------------------

ContainerSSH: lanzamiento de contenedores bajo demanda

1: <https://github.com/ContainerSSH/ContainerSSH>

--------------------------------------

El uso de armas para archivos privilegiados escribe errores con el servicio PrintNotify

1: <https://github.com/sailay1996/SpoolTrigger>

--------------------------------------

Kit de herramientas de ataque de base de datos Oracle de Windows

1: <https://github.com/InitRoot/wodat>

--------------------------------------

El script enumerará el nombre de dominio mediante enumeración horizontal, búsqueda inversa. Cada dominio horizontal se enumerará verticalmente utilizando Sublist3r.

1: <https://github.com/InitRoot/fransRecon>

--------------------------------------

Una red socialista: encriptada, invigilable, no montizable y autónoma. La aplicación está escrita en Python. (¡Llamando a todos los programadores socialistas para pedir ayuda!)

1: <https://github.com/ComradOrg/Comrad>

--------------------------------------

Herramientas para Pentesting

1: <https://github.com/thehackingsage/hacktronian>

--------------------------------------

Taller de ataque y detección del equipo rojo de Azure

1: <https://github.com/mandiant/Azure_Workshop>

--------------------------------------

🌸Un buscador difuso de línea de comandos

1: <https://github.com/junegunn/fzf>

--------------------------------------

Escáner de red con detección de puerta trasera, otros recursos de Nmap y detección de protección de sincronización

1: <https://github.com/xadhrit/d9scan>

--------------------------------------

Ejecución de comando de shell de solicitud POST simple

1: <https://github.com/dmzhari/hidden-shell>

--------------------------------------

Marco de automatización de seguridad de aplicaciones web que reconoce el objetivo de varios activos para maximizar la superficie de ataque para profesionales de seguridad y cazadores de errores

1: <https://github.com/0xdekster/ReconNote>

--------------------------------------

Este kit de herramientas de desbordamiento de búfer funciona a través de protocolos FTP, SMTP, POP, HTTP y también salidas de archivos para listas de reproducción que explotan variables/comandos personalizados. Las cargas útiles se pueden generar a través de MSFVENOM o puede usar sus propios archivos ASM.

1: <https://github.com/danieljs777/fastoverflowtk>

--------------------------------------

Un escáner completo, preciso y completamente automatizado para encontrar log4j RCE CVE-2021-44228

1: <https://github.com/fullhunt/log4j-scan>

--------------------------------------

Este es el código fuente simple de C# para omitir casi "todos" los AVS (kaspersky v19, Eset v12 v13, Trend-Micro v16, Comodo y Windows Defender omitidos a través de este método Muy simple)

1: <https://github.com/DamonMohammadbagher/NativePayload_ReverseShell>

--------------------------------------

ETWProcessMon2 es para monitorear procesos/subprocesos/memoria/cargas de imágenes/TCPIP a través de ETW + detección para inyección remota de subprocesos y detección de carga útil mediante eventos VirtualMemAlloc (en memoria), etc.

1: <https://github.com/DamonMohammadbagher/ETWProcessMon2>

--------------------------------------

ETWNetMonv3 es un código C# simple para monitorear la conexión de red TCP a través de ETW y ETWProcessMon/2 es para monitorear procesos/subprocesos/memoria/cargas de imágenes/TCPIP a través de ETW + Detección para inyección remota de subprocesos y detección de carga mediante eventos VirtualMemAlloc (en memoria), etc.

1: <https://github.com/DamonMohammadbagher/ETWNetMonv3>

--------------------------------------

NativePayload\_TiACBT (inyección remota de subprocesos + método asincrónico de C# + técnica de funciones de devolución de llamada)

1: <https://github.com/DamonMohammadbagher/NativePayload_TiACBT>

--------------------------------------

Código C# para transferir cargas útiles de puerta trasera mediante tráfico ARP y omitir antivirus (lento)

1: <https://github.com/DamonMohammadbagher/NativePayload_ARP>

--------------------------------------

Código C# para transferir cargas útiles de puerta trasera mediante tráfico ICMPv4 y evitar antivirus

1: <https://github.com/DamonMohammadbagher/NativePayload_ICMP>

--------------------------------------

Marco de ataque de intermediario independiente utilizado para credenciales de inicio de sesión de phishing junto con cookies de sesión, lo que permite eludir la autenticación de 2 factores

1: <https://github.com/kgretzky/evilginx2>

--------------------------------------

Inyectar keylogger en página web

1: <https://github.com/pioneerhfy/keylogoverhttp>

--------------------------------------

Herramienta de hoja de trucos de Shell inverso

1: <https://github.com/0xR0/shellver>

--------------------------------------

Generador de contraseñas para BIOS

1: <https://github.com/bacher09/pwgen-for-bios>

--------------------------------------

Un marco forense de memoria avanzado

1: <https://github.com/volatilityfoundation/volatility>

--------------------------------------

Automatización OSINT para hackers.

1: <https://github.com/blacklanternsecurity/bbot>

--------------------------------------

Cree un shell inverso sobre la red Tor sin reenvío de puertos y con anonimato mejorado.

1: <https://github.com/pisoj/torsh>

--------------------------------------

Funciones que se pueden usar para obtener Reverse Shells con PowerShell

1: <https://github.com/tobor88/ReversePowerShell>

--------------------------------------

Una utilidad súper liviana para crear unidades USB de arranque.

1: <https://github.com/CYB3RMX/pyXuSB>

--------------------------------------

Herramienta de fuerza bruta de directorio simple escrita con python.

1: <https://github.com/CYB3RMX/d00r>

--------------------------------------

Herramienta de análisis de malware todo en uno.

1: <https://github.com/CYB3RMX/Qu1cksc0pe>

--------------------------------------

Una herramienta de ingeniería inversa Flutter/Dart

1: <https://github.com/rscloura/Doldrums>

--------------------------------------

Biblioteca de análisis de archivos Android DEX. Con esta librería go puede extraer metadatos de archivos de clase Java DEX (Dalvik).

1: <https://github.com/dutchcoders/godex>

--------------------------------------

Aprenda sobre piratería ética. Obtenga información sobre reconocimiento, piratería de Windows/Linux, tecnologías web de ataque y redes inalámbricas de pruebas de penetración. Recursos para aprender análisis de malware e ingeniería inversa.

1: <https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE>

--------------------------------------

Herramienta OSINT para encontrar información sobre un usuario de github (email2username, username2email, fecha de creación...)

1: <https://github.com/hippiiee/osgint>

--------------------------------------

Un marco de escaneo nmap/masscan distribuido completo con programación de escaneo, agrupación de motores, diferenciación de puerto de escaneo posterior y un cliente API para flujos de trabajo de automatización.

1: <https://github.com/rackerlabs/scantron>

--------------------------------------

pagodo (Passive Google Dork) - Automatice el raspado y la búsqueda de la base de datos de Google Hacking

1: <https://github.com/opsdisk/pagodo>

--------------------------------------

Genere correo electrónico, regístrese para cualquier cosa, obtenga la OTP/enlace

1: <https://github.com/s0md3v/ote>

--------------------------------------

Una herramienta OSINT CLI diseñada para realizar un seguimiento rápido de la reputación de IP y la búsqueda de ubicación geográfica para los analistas de seguridad.

1: <https://github.com/radioactivetobi/geo-recon>

--------------------------------------

Este script es simplemente un contenedor para NMAP y Masscan. Instálelos desde su administrador de paquetes favorito o instálelos desde la fuente.

1: <https://github.com/trustedsec/spoonmap>

--------------------------------------

Devploit v 1.1 Herramienta de recopilación de información

1: https://github.com/GhettoCole/Devploit

--------------------------------------

🏗DZGEN – Funciona con herramientas Kali Linux

1: <https://github.com/joker25000/DZGEN>

--------------------------------------

TorghostNG: haga que todo su tráfico de Internet sea anónimo con la red Tor. Reescrito de TorGhost con Python 3

1: <https://github.com/jermainlaforce/TorghostNG>

--------------------------------------

Generador de billetera Bitcoin automatizado que con mnemónicos y frases de contraseña direcciones de billetera de fuerza bruta

1: <https://github.com/adrijano/Bitcoin-wallet-cracker>

--------------------------------------

Herramienta ligera de enumeración de n

hombres de usuario que comprueba la disponibilidad de un nombre de usuario específico en más de 200 sitios web.

1: <https://github.com/rly0nheart/thorndyke>

--------------------------------------

NekRos es un ransomeware de código abierto, con características avanzadas, que se parece a Wannacry y tiene un servidor C&C que se puede usar para recuperar la CLAVE

1: <https://github.com/PushpenderIndia/nekros>

--------------------------------------

Log4jScanner es un escáner CVE relacionado con Log4j, diseñado para ayudar a los evaluadores de penetración a realizar pruebas de caja negra en subdominios determinados.

1: https://github.com/PushpenderIndia/Log4jScanner

--------------------------------------

Este es un proyecto de raspberry pi-pico, pico se convierte en un USB defectuoso al convertirlo en un teclado oculto usando el módulo de circuito python

1: <https://github.com/EnriqueStrange/Pi-Pico-BAD-USB>

--------------------------------------

Multi tool👍

1: <https://github.com/aniketstark/STARK3.0>

--------------------------------------

Una herramienta de automatización que escanea subdominios, toma de control de subdominios, luego filtra XSS, SSTI, SSRF y más parámetros de punto de inyección y escanea automáticamente en busca de algunas vulnerabilidades bajas.

1: <https://github.com/R0X4R/Garud>

--------------------------------------

🌐🔍Red Network Tool es una herramienta para la exploración de redes y la búsqueda de información.

1: <https://github.com/Red-company/RedNetwork_Tool>

--------------------------------------

🔫Red DDoS Tool es -LA MEJOR- herramienta para ataques DDoS.

1: <https://github.com/Red-company/RDDoS_Tool>

--------------------------------------

Pingtunnel es una herramienta que envía tráfico TCP/UDP sobre ICMP

1: <https://github.com/esrrhs/pingtunnel>

--------------------------------------

Detección de anomalías en gráficos dinámicos (que evolucionan en el tiempo) en tiempo real y en forma de transmisión. Detección de intrusiones (ataques DoS y DDoS), fraudes, anomalías de calificación falsa.

1: <https://github.com/Stream-AD/MIDAS>

--------------------------------------

diseño de FPGA (chip) de banda base WiFi IEEE 802.11 de código abierto: controlador, software

1: <https://github.com/open-sdr/openwifi>

--------------------------------------

Pequeño script de python para buscar vulnerabilidades comunes en el servidor SMTP.

1: <https://github.com/mrlew1s/BrokenSMTP>

--------------------------------------

Thanos es un Http Flooder que enviará un montón de solicitudes http-get a un servidor web

1: <https://github.com/loTus04/Thanos>

--------------------------------------

Escáner de vulnerabilidades de contrabando de solicitudes Http

1: <https://github.com/Sh1Yo/request_smuggler>

--------------------------------------

domhttpx es un motor de búsqueda de Google con un kit de herramientas HTTP creado con python, puede facilitarle la búsqueda de muchas URL/IP a la vez con rapidez.

1: <https://github.com/naufalardhani/domhttpx>

--------------------------------------

Automatice el escaneo y la enumeración de máquinas de forma externa mientras mantiene un control total sobre los escaneos dirigidos a los objetivos con la velocidad y la comodidad de Tmux. Ideal para máquinas tipo OSCP/HTB, así como para pruebas de penetración.

1: <https://github.com/CoolHandSquid/TmuxRecon>

--------------------------------------

Kit de herramientas multiplataforma para una exfiltración de comandos de shell DNS interactivos, al usar DNS-Cat podrá ejecutar comandos del sistema en modo shell sobre el protocolo DNS

1: <https://github.com/lawrenceamer/dns-black-cat>

--------------------------------------

Un sniffer para Bluetooth 5 y 4.x LE

1: <https://github.com/nccgroup/Sniffle>

--------------------------------------

Simulación de ataques automatizados en la nube, completa con casos de uso de detección.

1: <https://github.com/WithSecureLabs/leonidas>

--------------------------------------

Ataques previos a la conexión, obtención de acceso y ataques posteriores a la conexión en WEP, WPA y WPA2.🛰✔️

1: <https://github.com/JulienFink/WiFi-Project>

--------------------------------------

Nzyme es un sistema de defensa WiFi gratuito y abierto de última generación. Visite www.nzyme.org para obtener más información.

1: <https://github.com/lennartkoopmann/nzyme>

--------------------------------------

Use este bot para monitorear nuevos CVE que contengan palabras clave definidas y envíe alertas a Slack y/o Telegram.

1: <https://github.com/carlospolop/BotPEASS>

--------------------------------------

Un tráfico ilimitado del sitio web y un generador de vistas de YouTube

1: <https://github.com/ingramali/Bot>

--------------------------------------

Rastreador de ubicación GPS preciso (teléfonos Android, IOS, Windows).

1: <https://github.com/bhikandeshmukh/MapEye>

--------------------------------------

🤖El escáner de puertos moderno🤖

1: <https://github.com/RustScan/RustScan>

--------------------------------------

✔Una herramienta de hacking escrita en Python👽👾👩‍💻🔒🚀

1: <https://github.com/giovanni-iannaccone/ians>

--------------------------------------

Implementación automatizada de la infraestructura del equipo rojo mediante Docker

1: <https://github.com/khast3x/Redcloud>

--------------------------------------

Bombardeo GZip HTTP en Python para todos

1: <https://github.com/khast3x/flaskbomb>

--------------------------------------

Drone Hacking Tool es una herramienta GUI que funciona con un adaptador WiFi USB y HackRF One para piratear drones.

1: https://github.com/HKSSY/Drone-Hacking-Tool

--------------------------------------

Devils Eye es una herramienta OSINT que extrae enlaces de cebolla y descripciones que coinciden con la consulta de los usuarios de Darkweb, sin necesidad de utilizar Tor.

1: <https://github.com/rly0nheart/thedevilseye>

--------------------------------------

Air Script es una navaja suiza de pwning Wi-Fi que también tiene notificaciones de correo electrónico opcionales para cuando se han capturado apretones de manos.

1: <https://github.com/B3ND1X/air-script>

--------------------------------------

Extraiga la información del servidor y la dirección IP del navegador SSRF

1: <https://github.com/bbhunter/Priest>

--------------------------------------

XRay es una herramienta para reconocimiento, mapeo y recopilación OSINT de redes públicas.

1: <https://github.com/evilsocket/xray>

--------------------------------------

Vajra es un marco de piratería web automatizado basado en objetivos y alcance altamente personalizable para automatizar tareas de reconocimiento aburridas y los mismos escaneos para múltiples objetivos durante las pruebas de penetración de aplicaciones web.

1: <https://github.com/r3curs1v3-pr0xy/vajra>

--------------------------------------

Un marco de IOT genérico, abierto para todos los dispositivos de nodo rojo de usuario y para cualquier lógica personalizada avanzada, con algunas características únicas: rico en interfaces (MQTT, REST, DB), orientado a OO más la capacidad de integrar TODOS los dispositivos Tuya sin piratear.

1: <https://github.com/msillano/tuyaDAEMON>

--------------------------------------

Shellshock exploit + entorno vulnerable

1: <https://github.com/opsxcq/exploit-CVE-2014-6271>

--------------------------------------

Herramientas automáticas Bruteforce Login WordPress

1: <https://github.com/Kedjaw3n/WpCrack>

--------------------------------------

Una herramienta OSINT para buscar cuentas por nombre de usuario en redes sociales.

1: <https://github.com/p1ngul1n0/blackbird>

--------------------------------------

Una herramienta gratuita de código abierto para generar datos de usuario aleatorios. Como Lorem Ipsum, pero para las personas.

1: <https://github.com/rly0nheart/rug>

--------------------------------------

Herramienta Github OSINT que busca un nombre de usuario específico en github y devuelve la información de los usuarios

1: <https://github.com/rly0nheart/githunt>

--------------------------------------

Un bot de Reddit Lmgtfy (permítanme buscarlo en Google) que responde a las preguntas en subreddits específicos. Responderá a preguntas que contengan Quién es, Qué es, Dónde está, Cómo está, Qué es, etc.

1: <https://github.com/rly0nheart/lmgtfy>

--------------------------------------

MyServer es su propio servidor web localhost. Puede configurar servidores PHP, Apache, Nginx y MySQL en sus dispositivos Android o Linux como Ubuntu, etc. MyServer está desarrollado para terminales Android como Termux o GNURoot Debian terminal.

1: https://github.com/rajkumardusad/MyServer

--------------------------------------

Generador de contraseñas, es un programa que genera contraseñas aleatoriamente a partir de mayúsculas AZ, minúsculas z, números 0-9 y la contraseña siempre tiene 10 caracteres. Haciéndola 5 veces más segura que la contraseña promedio, las contraseñas generadas se pueden usar para cualquier propósito.

1: https://github.com/rly0nheart/password\_generator

--------------------------------------

Herramienta de rastreo web de Python

1: https://github.com/rly0nheart/tarantula

--------------------------------------

Herramienta de administración remota para Windows

1: https://github.com/quasar/Quasar

--------------------------------------

Una herramienta de código abierto que recupera información del Programa de personas buscadas del FBI, esto incluye listas de delincuentes buscados, víctimas no identificadas, etc.

1: <https://github.com/rly0nheart/fbi-mostwanted>

--------------------------------------

Thelordseye busca y devuelve información detallada sobre los dispositivos que están directamente conectados a Internet [IoT] (Smart TV, neveras, cámaras web, semáforos, etc.).

1: https://github.com/rly0nheart/thelordseye

--------------------------------------

Suite de reconocimiento y enumeración de nombres de usuario

1: <https://github.com/rly0nheart/osinteye>

--------------------------------------

Falsificar de quién es un SMS usando una API de SMS

1: <https://github.com/vpn/SMSSpoof>

--------------------------------------

Powershell Script para ayudar en la respuesta a incidentes y el análisis forense en vivo

1: <https://github.com/Johnng007/Live-Forensicator>

--------------------------------------

ADB para piratas informáticos (:

1: <https://github.com/jxroot/adbwebkit>

--------------------------------------

Un script bash que instalará automáticamente una lista de herramientas de búsqueda de errores que encuentro interesantes para reconocimiento, explotación, etc. (menos eructos) para Ubuntu/Debain.

1: <https://github.com/0xApt/awesome-bbht>

--------------------------------------

PacketWhisper: extraiga datos de forma sigilosa y elimine la atribución mediante consultas de DNS y esteganografía basada en texto. Evite los problemas asociados con los métodos típicos de exfiltración de DNS. Transfiera datos entre sistemas sin que los dispositivos de comunicación se conecten directamente entre sí o a un punto final común. No es necesario controlar un servidor de nombres DNS.

1: <https://github.com/TryCatchHCF/PacketWhisper>

--------------------------------------

SrchX Google dorks avanzados y otras herramientas.

1: <https://github.com/Blacksterhack/SrchX>

--------------------------------------

Fatrat: una suite de administración remota de Android basada en la nube, con tecnología de NodeJS

1: <https://github.com/evildevill/Fatrat>

--------------------------------------

Hackthebox tool para automatizar procesos desde la terminal.

1: <https://github.com/sergioab7/boxthehack>

--------------------------------------

Paquete blueranger para Kali Linux

1: <https://gitlab.com/kalilinux/packages/blueranger/>

--------------------------------------

Extractor de propiedades para aplicaciones de Android

1: <https://github.com/cryptax/droidlysis>

--------------------------------------

Simplificó el reconocimiento de sus subdominios bugbounty con Hunt3r, el marco de reconocimiento de aplicaciones web

1: <https://github.com/EasyRecon/Hunt3r>

--------------------------------------

Erlik - Servicio de jabón vulnerable

1: <https://github.com/anil-yelken/Vulnerable-Soap-Service>

--------------------------------------

pFuzz nos ayuda a eludir el firewall de aplicaciones web mediante el uso de diferentes métodos al mismo tiempo.

1: <https://github.com/RedSection/pFuzz>

--------------------------------------

Script de vigilancia para monitorear múltiples carpetas usando python y multiprocesamiento.

1: <https://github.com/IvanHanonoCozzetti/File-Watchdog>

--------------------------------------

OffensivePH: use el antiguo controlador Process Hacker para omitir varios controles de acceso en modo de usuario

1: <https://github.com/RedSection/OffensivePH>

--------------------------------------

Loki - IOC simple y escáner de respuesta a incidentes

1: <https://github.com/Neo23x0/Loki>

--------------------------------------

Motor de permutación de nombres de dominio para detectar ataques de phishing homógrafo, usurpación de errores tipográficos y suplantación de identidad de marca

1: <https://github.com/elceef/dnstwist>

--------------------------------------

Un conjunto de herramientas para hacer que un sistema parezca víctima de un ataque APT

1: <https://github.com/NextronSystems/APTSimulator>

--------------------------------------

Verificador de hash en línea para Virustotal y otros servicios

1: <https://github.com/Neo23x0/munin>

--------------------------------------

GoAccess es un analizador de registros web en tiempo real y un visor interactivo que se ejecuta en una terminal en sistemas \*nix o a través de su navegador.

1: <https://github.com/allinurl/goaccess>

--------------------------------------

Herramienta para automatizar ataques personalizados contra aplicaciones web. Completamente hecho en lenguaje C con pthreads, tiene un rendimiento rápido.

1: <https://github.com/CoolerVoid/0d1n>

--------------------------------------

Una herramienta de cambio automático de IP de Tor. Este programa puede cambiar automáticamente nuestra identidad/IP de Tor. Funciona al 100%.

1: <https://github.com/r3k4t/AutoTorIP>

--------------------------------------

Onionnux es una herramienta del sitio de cebolla (DEEPNET/DARKNET). Puede ayudar a identificar que el sitio de cebolla está activo o el nombre del servidor del sitio de cebolla.

1: <https://github.com/r3k4t/onionnux>

--------------------------------------

TORAPF es una herramienta de búsqueda de páginas de administración de la red Tor. Puede ayudar a obtener una página de administración de la red Tor.

1: <https://github.com/r3k4t/torapf>

--------------------------------------

DNSProb es una herramienta construida sobre retryabledns que le permite realizar múltiples consultas dns de su elección con una lista de resolutores proporcionados por el usuario.

1: <https://github.com/projectdiscovery/dnsprobe>

--------------------------------------

Sondeo del servidor web HTTP

1: <https://github.com/projectdiscovery/httpx-action>

--------------------------------------

Package retryablehttp proporciona una interfaz de cliente HTTP familiar con reintentos automáticos y retroceso exponencial

1: <https://github.com/projectdiscovery/retryablehttp-go>

--------------------------------------

Un escáner de puertos rápido integrado con un enfoque en la confiabilidad y la simplicidad. Diseñado para usarse en combinación con otras herramientas para el descubrimiento de superficies de ataque en bug bounties y pentests

1: <https://github.com/projectdiscovery/naabu>

--------------------------------------

Capturador de TLS rápido y configurable centrado en la recopilación de datos basada en TLS.

1: <https://github.com/projectdiscovery/tlsx>

--------------------------------------

Herramienta Recopilación de información e ingeniería social Escribir por [Python,JS,PHP]

1: <https://github.com/ultrasecurity/DarkSide>

--------------------------------------

Cloudlist es una herramienta para enumerar activos de múltiples proveedores de nube.

1: <https://github.com/projectdiscovery/cloudlist>

--------------------------------------

🕸️Herramienta de auditoría para encontrar vulnerabilidades comunes en el código fuente de PHP

1: <https://github.com/ecriminal/phpvuln>

--------------------------------------

Recupera contraseñas de capturas de pantalla pixeladas

1: <https://github.com/beurtschipper/Depix>

--------------------------------------

🏴‍☠️Sitios mal configurados de Pwn que ejecutan la API de carga de imágenes personalizadas de ShareX a través de un exploit encadenado

1: <https://github.com/ecriminal/PwnX.py>

--------------------------------------

🥧HTTPie para Terminal: cliente HTTP de línea de comandos moderno y fácil de usar para la era API. Compatibilidad con JSON, colores, sesiones, descargas, complementos y más.

1: <https://github.com/httpie/httpie>

--------------------------------------

Este kit de herramientas de desbordamiento de búfer funciona a través de protocolos FTP, SMTP, POP, HTTP y también salidas de archivos para listas de reproducción que explotan variables/comandos personalizados. Las cargas útiles se pueden generar a través de MSFVENOM o puede usar sus propios archivos ASM.

1: <https://github.com/danieljs777/fastoverflowtk>

--------------------------------------

Herramienta para marcar puertos eBPF

1: <https://github.com/eeriedusk/knockles>

--------------------------------------

Una comunicación autónoma asistida por UAV en un área remota de desastre utilizando el aprendizaje por imitación (clonación del comportamiento)

1: <https://github.com/AlirezaShamsoshoara/Imitation-Learning-Behavioral-Cloning-UAV-Assisted-Communication>

--------------------------------------

📧Un ejemplo del uso de un formulario HTML (por ejemplo: "Contáctenos" en un sitio web) para enviar correo electrónico sin un servidor backend (usando un script de Google) perfecto para sitios web estáticos que necesitan recopilar datos.

1: <https://github.com/dwyl/learn-to-send-email-via-google-script-html-no-server>

--------------------------------------

Herramienta para el reconocimiento basico de una pagina web.

1: <https://github.com/sergioab7/HackWeb>

--------------------------------------

Herramienta automatizada para enviar correos con phising

1: <https://github.com/sergioab7/phishboom>

--------------------------------------

Entropy Toolkit es un conjunto de herramientas para proporcionar ataques de cámaras web IP Netwave y GoAhead. Entropy Toolkit es un poderoso conjunto de herramientas para pruebas de penetración de cámaras web.

1: <https://github.com/evildevill/entropy>

--------------------------------------

Shell inverso de forma anónima a través de la red Tor utilizando servicios ocultos sin reenvío de puertos.

1: <https://github.com/samet-g/tornado>

--------------------------------------

¡Encuentra todas las cuentas de redes sociales con un nombre de usuario!

1: <https://github.com/BLINKING-IDIOT/Aliens_eye>

--------------------------------------

escáner web - explotación - recopilación de información

1: <https://github.com/jaxBCD/Zeebsploit>

--------------------------------------

Rastreador web sin cabeza para bugbounty y pruebas de penetración/redequipo

1: <https://github.com/jonaslejon/lolcrawler>

--------------------------------------

SuDOS es un inundador HTTP basado en proxy que se utiliza para bloquear sitios web desprotegidos de ataques DoS.

1: <https://github.com/optionalg/sudos>

--------------------------------------

Una implementación de agresor de ataque de cobalto encriptado .NET XOR para chisel para utilizar un proxy más rápido y capacidades avanzadas de socks5.

1: <https://github.com/m3rcer/Chisel-Strike>

--------------------------------------

Windows Feature Hunter

1: <https://github.com/ConsciousHacker/WFH>

--------------------------------------

EyeWitness está diseñado para tomar capturas de pantalla de sitios web, proporcionar información del encabezado del servidor e identificar las credenciales predeterminadas si es posible.

1: <https://github.com/FortyNorthSecurity/EyeWitness>

--------------------------------------

Herramienta para descubrir rutas de ataque de delegación restringida basada en recursos en entornos de Active Directory

1: <https://github.com/FatRodzianko/Get-RBCD-Threaded>

--------------------------------------

Generador de macros de Excel 4.0 (XLM) para inyectar archivos DLL y EXE en la memoria.

1: <https://github.com/FortyNorthSecurity/EXCELntDonut>

--------------------------------------

Encuentre y recupere de forma interactiva archivos eliminados o👉sobrescrito👈archivos desde tu terminal

1: <https://github.com/PabloLec/RecoverPy>

--------------------------------------

Registrador de Python y lector en vivo

1: <https://github.com/PabloLec/livelog>

--------------------------------------

✔️Estadísticas de socket detalladas y fáciles de usar con una interfaz de usuario de terminal.

1: <https://github.com/PabloLec/neoss>

--------------------------------------

Herramienta de evasión de limitación de velocidad de direcciones IPv4 e IPv6

1: <https://github.com/blechschmidt/freebind>

--------------------------------------

Probar el cifrado TLS/SSL en cualquier lugar y en cualquier puerto

1: <https://github.com/drwetter/testssl.sh>

--------------------------------------

Mi recorrido por el CTF desde 2015. Estadísticas, reseñas, fragmentos de código, notas, desafíos.

1: <https://github.com/bl4de/ctf>

--------------------------------------

Generador de saltos falsos de traceroute simple a través de la suplantación de IP

1: <https://github.com/blechschmidt/certbot-dns-local>

--------------------------------------

Un resolutor de código auxiliar de DNS de alto rendimiento para búsquedas masivas y reconocimiento (enumeración de subdominios)

1: <https://github.com/blechschmidt/massdns>

--------------------------------------

Generador de saltos falsos de traceroute simple a través de la suplantación de IP

1: <https://github.com/blechschmidt/fakeroute>

--------------------------------------

Monitor de URL dinámico

1: <https://github.com/alanEG/Gosna>

--------------------------------------

Muestra y controla tu dispositivo Android

1: <https://github.com/Genymobile/scrcpy>

--------------------------------------

Recursos de prueba SSRF (falsificación de solicitud del lado del servidor)

1: <https://github.com/cujanovic/SSRF-Testing>

--------------------------------------

¡Hacer a Recon Great de nuevo basado en Favicon.ico!

1: <https://github.com/devanshbatham/FavFreak>

--------------------------------------

Enumerador de deposito S3

1: <https://github.com/gdraperi/slurp-1>

--------------------------------------

fuzzuli es una herramienta de fuzzing de URL que tiene como objetivo encontrar archivos de copia de seguridad críticos mediante la creación de una lista de palabras dinámica basada en el dominio.

1: <https://github.com/musana/fuzzuli>

--------------------------------------

Rastree a los usuarios a través de las plataformas de redes sociales

1: <https://github.com/gdraperi/SocialPath>

--------------------------------------

Un script para extraer subdominios/correos electrónicos para un dominio dado usando un conjunto de datos de certificados SSL/TLS en Censys

1: <https://github.com/0xbharath/censys-enumeration>

--------------------------------------

Extensión BURP para registrar cada solicitud HTTP enviada a través de BURP y crear un registro de seguimiento de auditoría de una evaluación.

1: <https://github.com/righettod/log-requests-to-sqlite>

--------------------------------------

Comprobador HTTP rápido.

1: <https://github.com/Edu4rdSHL/fhc>

--------------------------------------

Script para automatizar, cuando sea posible, el reconocimiento pasivo realizado en un sitio web previo a una evaluación.

1: <https://github.com/righettod/website-passive-reconnaissance>

--------------------------------------

La solución más rápida y completa para el reconocimiento de dominios. Admite capturas de pantalla, escaneo de puertos, verificación de HTTP, importación de datos de otras herramientas, monitoreo de subdominios, alertas a través de Discord, Slack y Telegram, múltiples claves API para fuentes y mucho más.

1: <https://github.com/Findomain/Findomain>

--------------------------------------

Un escáner de puertos TCP SYN de alto rendimiento.

1: <https://github.com/resyncgg/armada>

--------------------------------------

Herramienta de búsqueda rápida CLI DNS

1: <https://github.com/zmap/zdns>

--------------------------------------

Análisis en tiempo real del tráfico HTTP con aprendizaje automático

1: <https://github.com/musana/Attackdet>

--------------------------------------

Una herramienta que le permite hacer de TOR su puerta de enlace predeterminada y enviar todas las conexiones a Internet bajo TOR (como proxy transparente) para aumentar la privacidad/anonimato sin código adicional innecesario.

1: <https://github.com/Edu4rdSHL/tor-router>

--------------------------------------

una herramienta para enumerar los registros de recursos de una zona DNS utilizando su cadena DNSSEC NSEC o NSEC3

1: <https://github.com/anonion0/nsec3map>

--------------------------------------

🔓 🔓Encuentre secretos y contraseñas en imágenes de contenedores y sistemas de archivos🔓 🔓

1: <https://github.com/deepfence/SecretScanner>

--------------------------------------

reNgine es un marco de reconocimiento automatizado para aplicaciones web con un enfoque en el proceso de reconocimiento optimizado altamente configurable a través de motores, correlación y organización de datos de reconocimiento, monitoreo continuo, respaldado por una base de datos y una interfaz de usuario simple pero intuitiva. reNgine facilita a los probadores de penetración recopilar reconocimiento con...

1: <https://github.com/yogeshojha/rengine>

--------------------------------------

Una lista seleccionada de blogs y herramientas increíbles sobre ataques de contrabando de solicitudes HTTP. ¡Siéntete libre de contribuir!🍻

1: <https://github.com/chenjj/Awesome-HTTPRequestSmuggling>

--------------------------------------

Una herramienta de prueba de suplantación de correo electrónico que tiene como objetivo eludir SPF/DKIM/DMARC y falsificar firmas DKIM.🍻

1: <https://github.com/chenjj/espoofer>

--------------------------------------

Servidor SSH y auditoría de clientes (banner, intercambio de claves, cifrado, mac, compresión, compatibilidad, seguridad, etc.)

1: <https://github.com/jtesta/ssh-audit>

--------------------------------------

Biblioteca de pirateo de memoria de Windows

1: <https://github.com/DarthTon/Blackbone>

--------------------------------------

⚡Cree avisos de UAC infinitos que obliguen a un usuario a ejecutar como administrador⚡

1: https://github.com/catzsec/ForceAdmin

--------------------------------------

DirBruter es una herramienta CLI basada en Python. Busca directorios/archivos ocultos o existentes utilizando el método de fuerza bruta. Básicamente funciona lanzando un ataque basado en diccionario contra un servidor web y analizando su respuesta.

1: <https://github.com/vijaysahuofficial/DirBruter>

--------------------------------------

Este es un script que informa cuentas de instagram específicas. Hasta que lo prohíban

1: <https://github.com/Crevils/InstaReport>

--------------------------------------

Ghost Eye Recopilación de información Footprinting Scanner y Lanzamiento de herramienta de reconocimiento. Ghost Eye es una herramienta de recopilación de información que hice en python 3. Para ejecutar Ghost Eye, solo necesita un dominio o ip. Ghost Eye puede funcionar con cualquier distribución de Linux si es compatible con Python 3. Autor: Jolanda de Koff

1: <https://github.com/BullsEye0/ghost_eye>

--------------------------------------

kit de herramientas de auditoría masiva de amplio rango

1: <https://github.com/utkusen/leviathan>

una herramienta para compartir archivos que le permite encontrar a la persona responsable en caso de fuga

1: <https://github.com/utkusen/wholeaked>

--------------------------------------

una herramienta de evaluación comparativa y estrés que puede enviar solicitudes HTTP sin procesar

1: <https://github.com/utkusen/reqstress>

--------------------------------------

Marco de ataque de intermediario independiente utilizado para credenciales de inicio de sesión de phishing junto con cookies de sesión, lo que permite eludir la autenticación de 2 factores

1: <https://github.com/kgretzky/evilginx2>

--------------------------------------

¡Un rastreador de respuesta sorprendentemente rápido para encontrar cosas jugosas en el código fuente!😎🔥

1: <https://github.com/ksharinarayanan/SourceWolf>

--------------------------------------

NFStream: un marco de análisis de datos de red flexible.

1: <https://github.com/nfstream/nfstream>

--------------------------------------

ShotDroid es una herramienta de pentesting para Android. Hay 3 herramientas que tienen sus respectivas funciones, obtener archivos del directorio de Android, almacenamiento interno y externo, Android Keylogger + Reverse Shell y tomar una foto de cámara web de la cara desde la cámara frontal del teléfono y la PC.

1: <https://github.com/kp300/shotdroid>

--------------------------------------

Un script para volcar archivos y carpetas de forma remota desde un recurso compartido SMB de Windows.

1: <https://github.com/p0dalirius/DumpSMBShare>

--------------------------------------

Genere JSON compatible con BloodHound a partir de registros escritos por ldapsearch BOF y pyldapsearch

1: <https://github.com/fortalice/bofhound>

--------------------------------------

Modificación de plantilla de certificado ADCS y enumeración de ACL

1: <https://github.com/fortalice/modifyCertTemplate>

--------------------------------------

Herramienta para emitir consultas LDAP manuales que ofrece salida compatible con bofhound

1: <https://github.com/fortalice/pyldapsearch>

--------------------------------------

Active Directory ACL Visualizer and Explorer: ¿quién es realmente el administrador del dominio?

1: <https://github.com/lkarlslund/Adalanche>

--------------------------------------

Protéjase contra la adquisición de subdominios

1: <https://github.com/ovotech/domain-protect>

--------------------------------------

Una herramienta web basada en aprendizaje profundo para pupilometría traslacional y en tiempo real

1: <https://github.com/fabiocarrara/meye>

--------------------------------------

Elimine las direcciones IP elásticas pendientes realizando un análisis de sus recursos en todas sus cuentas de AWS.

1: <https://github.com/assetnote/ghostbuster>

--------------------------------------

FrostByte es un proyecto POC que combina diferentes técnicas de evasión de defensa para construir mejores cargas útiles de redteam

1: <https://github.com/pwn1sher/frostbyte>

--------------------------------------

Un pequeño POC para hacer que el defensor sea inútil al eliminar sus privilegios de token y reducir la integridad del token.

1: <https://github.com/pwn1sher/KillDefender>

--------------------------------------

WMEye es una herramienta de explotación posterior que utiliza WMI Event Filter y MSBuild Execution para el movimiento lateral

1: <https://github.com/pwn1sher/WMEye>

--------------------------------------

Compruebe las instancias de AWS S3 para acceso de lectura/escritura/eliminación

1: <https://github.com/0xmoot/s3sec>

--------------------------------------

msImpersonate - Suplantación de cuenta de usuario escrita en Python3 puro

1: <https://github.com/dievus/msImpersonate>

--------------------------------------

Un motor de flujo de trabajo para seguridad ofensiva

1: <https://github.com/j3ssie/osmedeus>

--------------------------------------

Herramienta de enumeración DNS de MayorSec

1: <https://github.com/dievus/msdnsscan>

--------------------------------------

Herramienta de enumeración de usuarios Python3 o365

1: <https://github.com/dievus/Oh365UserFinder>

--------------------------------------

para la explotacion masiva

1: <https://github.com/jm33-m0/mec>

--------------------------------------

encontrar donde se toma una imagen

1: <https://github.com/jm33-m0/img2location>

--------------------------------------

Una utilidad de fuerza bruta de configuración Wi-Fi protegida fuera de línea

1: <https://github.com/wiire-a/pixiewps>

--------------------------------------

Explotación de HEVD y CVE

1: <https://github.com/ReJimp/Kernel_Exploit>

--------------------------------------

mift: un conjunto de herramientas forenses de imágenes móviles

1: <https://github.com/controlf/mift>

--------------------------------------

Paquete de complementos Flutter para varios servicios WiFi.

1: <https://github.com/flutternetwork/WiFiFlutter>

--------------------------------------

Una herramienta de análisis forense de paquetes de red para SSH

1: <https://github.com/benjeems/packetStrider>

--------------------------------------

HASSH es un estándar de huellas dactilares de red que se puede utilizar para identificar implementaciones específicas de SSH de cliente y servidor. Las huellas dactilares se pueden almacenar, buscar y compartir fácilmente en forma de una pequeña huella dactilar MD5.

1: <https://github.com/salesforce/hassh>

--------------------------------------

Generador de políticas de privilegios mínimos de IAMGenerador de políticas de privilegios mínimos de IAM

1: <https://github.com/salesforce/policy_sentry>

--------------------------------------

Merlion: un marco de aprendizaje automático para la inteligencia de series temporales

1: <https://github.com/salesforce/Merlion>

--------------------------------------

HTTP fuzzer engine orientado a la seguridad

1: <https://github.com/htrgouvea/nozaki>

--------------------------------------

Un motor para hacer de la red Tor su puerta de enlace predeterminada

1: <https://github.com/htrgouvea/nipe>

--------------------------------------

[WIP] Un ecosistema de rastreadores para detectar: ​​fugas, exposición de datos confidenciales e intentos de exfiltración de datos

1: <https://github.com/htrgouvea/harpoon>

--------------------------------------

Ashok es una herramienta OSINT Recon, también conocida como😍Cuchillo del ejército suizo.

1: <https://github.com/powerexploit/Ashok>

--------------------------------------

Fuerza bruta desde la salida de Nmap: intenta automáticamente las credenciales predeterminadas en los servicios encontrados.

1: <https://github.com/x90skysn3k/brutespray>

--------------------------------------

Complemento Plex que reproduce transmisiones en vivo (como IPTV) desde una lista de reproducción M3U

1: <https://github.com/Cigaras/IPTV.bundle>

--------------------------------------

La hoja de trucos sobre las vulnerabilidades de deserialización de Java

1: <https://github.com/GrrrDog/Java-Deserialization-Cheat-Sheet>

--------------------------------------

Algunos scripts para ataques al protocolo Tacacs+

1: <https://github.com/GrrrDog/TacoTaco>

--------------------------------------

Hoja de trucos de proxies inversos

1: <https://github.com/GrrrDog/weird_proxies>

--------------------------------------

Estamos lanzando una forma alternativa de elevar a SYSTEM cuando tiene SeTcbPrivilege

1: <https://gist.github.com/antonioCoco/19563adef860614b56d010d92e67d178>

--------------------------------------

Rootkit en modo usuario

1: <https://github.com/ZeroMemoryEx/URootkit>

--------------------------------------

tunele el tráfico de puerto a puerto a través de un canal ofuscado con cifrado AES-GCM.

1: <https://github.com/Potato-Industries/gohide>

--------------------------------------

Russia Wipers Dropper (REvil Ransomware incluido) (fines educativos)

1: <https://github.com/ZeroMemoryEx/U-Boat>

--------------------------------------

Llamada al sistema directa e indirecta de un único código auxiliar con resolución de SSN en tiempo de ejecución para Windows.

1: <https://github.com/janoglezcampos/rust_syscalls>

--------------------------------------

carcasa inversa portátil basada en dardos

1: <https://github.com/Potato-Industries/dartrs>

--------------------------------------

CVE-2022-31188 - OpenCV CVAT (herramienta de anotación de visión por computadora) SSRF

1: <https://github.com/emirpolatt/CVE-2022-31188>

--------------------------------------

Código hacky para extraer llamadas en DLL por función

1: <https://github.com/janoglezcampos/FindItByCalls>

--------------------------------------

Una implementación de PoC para una técnica de evasión para finalizar el subproceso actual y restaurarlo antes de reanudar la ejecución, al tiempo que implementa cambios de protección de página sin ejecución.

1: <https://github.com/janoglezcampos/DeathSleep>

--------------------------------------

Herramienta para eludir códigos de respuesta 40X.

1: <https://github.com/devploit/dontgo403>

--------------------------------------

Codificador para omitir los filtros WAF mediante operaciones XOR.

1: <https://github.com/devploit/XORpass>

--------------------------------------

Analizador de encabezado de correo electrónico

1: <https://github.com/cyberdefenders/email-header-analyzer>

--------------------------------------

Cargue su controlador como win32k.sys

1: <https://github.com/gmh5225/CallMeWin32kDriver>

--------------------------------------

Lista seleccionada por la comunidad de plantillas para el motor de núcleos para encontrar vulnerabilidades de seguridad.

1: <https://github.com/projectdiscovery/nuclei-templates>

--------------------------------------

Herramienta de depuración nativa de última generación

1: <https://github.com/HyperDbg/HyperDbg>

--------------------------------------

RAT-el es una herramienta de prueba de penetración de código abierto que le permite tomar el control de una máquina con Windows. Funciona en el modelo cliente-servidor, el servidor envía comandos y el cliente ejecuta los comandos y envía el resultado al servidor. El cliente es completamente indetectable por el software antivirus.

1: <https://github.com/FrenchCisco/RATel>

--------------------------------------

Un proxy inverso rápido para ayudarlo a exponer un servidor local detrás de un NAT o firewall a Internet.

1: <https://github.com/fatedier/frp>

--------------------------------------

Ro3b - Botnet HTTP de banca avanzada

1: <https://github.com/mathio3/Ro3b-HTTP-botnet>

--------------------------------------

Explotación de XSHOCK Shellshock

1: <https://github.com/capture0x/XSHOCK>

--------------------------------------

Shodan Eye Esta herramienta recopila toda la información sobre todos los dispositivos conectados directamente a Internet utilizando las palabras clave especificadas que ingresa. Autora: Jolanda de Koff

1: <https://github.com/BullsEye0/shodan-eye>

--------------------------------------

Twitter Eye es una herramienta de recopilación de información de Twitter Con Twitter Eye, puede buscar con varias palabras clave y nombres de usuario en Twitter. Luego, los datos que obtiene se guardan en un archivo .csv. Autora: Jolanda de Koff

1: <https://github.com/BullsEye0/twitter-eye>

--------------------------------------

Elimina la información de los seguidores de Instagram.

1: https://github.com/Crevils/instascraper

--------------------------------------

Se construyo un sistema de reconocimiento de voz que permite al usuario identificarse por medio de su voz para entrar a una aplicación.

1: <https://github.com/jonatan-parra/sistema-de-reconocimiento-de-voz>

--------------------------------------

Cambiador aleatorio de Mac y nombre de host

1: https://github.com/andrei-zgirvaci/hide-me

--------------------------------------

Este repositorio contiene herramientas de seguridad de código abierto (OST) de vanguardia para un equipo rojo y un cazador de amenazas.

1: <https://github.com/infosecn1nja/Red-Teaming-Toolkit>

--------------------------------------

Administrador de paquetes para piratas informáticos creado por piratas informáticos

1: <https://github.com/Ekultek/HacApt>

--------------------------------------

🏴‍☠️herramientas (versión py3) del libro Black Hat Python🏴‍☠️

1: https://github.com/edoardottt/black-hat-python3-code

--------------------------------------

Herramienta OSINT para encontrar correos electrónicos violados, bases de datos, pastas e información relevante

1: https://github.com/Ekultek/WhatBreach

--------------------------------------

Xteam All in one Instagram, Android, phishing osint y herramienta de piratería wifi disponible

1: <https://github.com/xploitstech/Xteam>

--------------------------------------

La mejor herramienta para aumentar los seguidores de Instagram

1: <https://github.com/xploitstech/xploits>

--------------------------------------

Un marco OSINT actualizado semanalmente, con el que puede buscar objetivos precisos, con muchas funciones como búsqueda de personas, búsqueda de delincuentes o escaneo de redes sociales con correo electrónico/teléfono y cambiador de ip

1: <https://github.com/DR34M-M4K3R/GhostRecon>

--------------------------------------

Una herramienta para realizar fuerza bruta previa a la autenticación de Kerberos

1: <https://github.com/ropnop/kerbrute>

--------------------------------------

RDPloit: un simple comprobador de vulnerabilidades de seguridad para el protocolo de escritorio remoto

1: <https://github.com/souravbaghz/RDPloit>

--------------------------------------

Proxy de calcetines y servidor de calcetines inverso usando powershell.

1: <https://github.com/p3nt4/Invoke-SocksProxy>

--------------------------------------

Herramienta de auditoría de seguridad de múltiples nubes

1: <https://github.com/nccgroup/ScoutSuite>

--------------------------------------

Caja de herramientas de análisis de recurrencia y redes complejas unificadas

1: <https://github.com/pik-copan/pyunicorn>

--------------------------------------

Simple .net Web BruteForcer para fines educativos y de pentesting

1: <https://github.com/m4ndingo/.net-WebBruteForcer>

--------------------------------------

Herramienta de búsqueda de rangos de direcciones IP en la nube + enumeración de subdominios DNS + Transparencia de certificados

1: <https://github.com/iknowjason/edge>

--------------------------------------

Herramienta de prueba de penetración de red VoIP Hopper: ¡saltar de una VLAN a la siguiente! Una herramienta de seguridad de prueba de penetración de infraestructura de red. Una herramienta para probar la (in)seguridad de VLANS. Puede imitar el comportamiento de los teléfonos IP para comprender mejor los riesgos comerciales dentro de una infraestructura de red de telefonía IP. VoIP Hopper está incluido en Kali Linux…

1: <https://github.com/iknowjason/voiphopper>

--------------------------------------

Merlin es un servidor y agente de comando y control HTTP/2 posterior a la explotación multiplataforma escrito en golang.

1: <https://github.com/Ne0nd0g/merlin>

--------------------------------------

Un marco de comando y control (C2) HTTP(S) basado en Flask con una interfaz web. Agentes maleables escritos en Go y scripts escritos en bash.

1: <https://github.com/AshleyNikr/Bifrost>

--------------------------------------

BuffMate es una herramienta de desbordamiento de búfer de Perl

1: <https://github.com/stevcoll/buffmate>

--------------------------------------

FileDozer es una herramienta de búsqueda y procesamiento de archivos Perl

1: <https://github.com/stevcoll/filedozer>

--------------------------------------

Auditoría de código fuente de Python y análisis estático a gran escala

1: <https://github.com/SourceCode-AI/aura>

--------------------------------------

Una herramienta para levantar (¡y derribar!) una infraestructura en la nube intencionalmente insegura

1: <https://github.com/nccgroup/sadcloud>

--------------------------------------

Ejecución y persistencia de código en SERVICIO DE RED Servicio de FAX

1: <https://github.com/hackerhouse-opensource/NoFaxGiven>

--------------------------------------

Forzar la autenticación de máquinas Windows a través de MS-EVEN

1: <https://github.com/evilashz/CheeseOunce>

--------------------------------------

Herramientas para mantener el acceso a los sistemas y demostraciones de prueba de concepto.

1: <https://github.com/hackerhouse-opensource/backdoors>

--------------------------------------

Marco de mando y control

1: <https://github.com/skylerknecht/connect>

--------------------------------------

Una herramienta para ayudar a consultar AD a través del protocolo LDAP

1: <https://github.com/tomcarver16/ADSearch>

--------------------------------------

iPhone 11 emulado en QEMU

1: <https://github.com/TrungNguyen1909/qemu-t8030>

--------------------------------------

Aplicación para administrar redes multidominio basadas en Active Directory

1: <https://github.com/sysadminanywhere/sysadmin>

--------------------------------------

Utilidad de prueba de penetración y herramienta de evaluación antivirus.

1: <https://github.com/ivan-sincek/invoker>

--------------------------------------

Omita los códigos de estado de respuesta HTTP 4xx y más. Basado en PycURL.

1: <https://github.com/ivan-sincek/forbidden>

--------------------------------------

API simple para almacenar todas las solicitudes XSS entrantes.

1: <https://github.com/ivan-sincek/xss-catcher>

--------------------------------------

Un marco de comando y control (C2) HTTP(S) basado en Flask con una interfaz web. Implantes personalizados EXE/DLL de Windows escritos en C++. Sólo para uso educativo.

1: <https://github.com/JrM2628/httpworker>

--------------------------------------

Un fuzzer de plugin de WordPress de prueba de concepto

1: <https://github.com/kazet/wpgarlic>

--------------------------------------

Canadian Furious Beaver es una herramienta para monitorear el controlador IRP en los controladores de Windows y facilitar el proceso de análisis, reproducción y fuzzing de los controladores de Windows en busca de vulnerabilidades.

1: <https://github.com/hugsy/CFB>

--------------------------------------

Plantillas de navegador en el navegador (BITB)

1: <https://github.com/mrd0x/BITB>

--------------------------------------

EvilSelenium es una herramienta que convierte a Selenium en un arma para atacar navegadores basados ​​en Chromium.

1: <https://github.com/mrd0x/EvilSelenium>

--------------------------------------

Una biblioteca de Python para utilizar el gran grupo de direcciones IP de AWS API Gateway como un proxy para generar direcciones IP pseudo-infinitas para web scraping y fuerza bruta.

1: <https://github.com/Ge0rg3/requests-ip-rotator>

--------------------------------------

Whoami proporciona privacidad mejorada, anonimato para las distribuciones de Linux basadas en Debian y Arch

1: <https://github.com/owerdogan/whoami-project>

--------------------------------------

🐚ᴠʟᴀɴɢ ʀᴇᴠᴇʀsᴇ sʜᴇʟʟ🐚

1: <https://github.com/Lexxrt/vShell>

--------------------------------------

Proxy PowerShell SOCKS con capacidades de proxy inverso

1: <https://github.com/get-get-get-get/PowerProxy>

--------------------------------------

Plataforma de phishing lista para usar

1: <https://github.com/JoelGMSec/EvilnoVNC>

--------------------------------------

El marco de ataque de la sombra

1: <https://github.com/JoelGMSec/AutoRDPwn>

--------------------------------------

(Sim)ulate (Ba)zar Cargador

1: <https://github.com/OccamsXor/sim-ba>

--------------------------------------

Técnicas de abuso de Win32 y Kernel para pentesters

1: <https://github.com/matthieu-hackwitharts/Win32_Offensive_Cheatsheet>

--------------------------------------

Siofra es una herramienta diseñada para identificar y explotar vulnerabilidades de secuestro de DLL

1: <https://github.com/Cybereason/siofra>

--------------------------------------

Utilice la vulnerabilidad de Log4Shell para vacunar a un servidor víctima contra Log4Shell

1: <https://github.com/Cybereason/Logout4Shell>

--------------------------------------

IPSweep con configuración adicional de exploración de puertos

1: <https://github.com/amaitou/DarkSpy>

--------------------------------------

BlackHeart es un script de Python simple para generar scripts de PowerShell que demuestran la obtención de shell inverso sin restricciones de Microsoft Defender. (PARA FINES EDUCATIVOS!!)

1: <https://github.com/CYB3RMX/BlackHeart>

--------------------------------------

Manejador de concha de Penélope

1: <https://github.com/brightio/penelope>

--------------------------------------

Funciones que se pueden usar para obtener Reverse Shells con PowerShell

1: <https://github.com/tobor88/ReversePowerShell>

--------------------------------------

HardeningKitty: comprueba y fortalece la configuración de Windows

1: <https://github.com/scipag/HardeningKitty>

--------------------------------------

Escanee pasivamente en busca de dispositivos Bluetooth Low Energy e intente tomar sus huellas digitales

1: <https://github.com/scipag/btle-sniffer>

--------------------------------------

Huella digital avanzada del servidor web para Nmap

1: <https://github.com/scipag/httprecon-nse>

--------------------------------------

Ataques HTTP3 (CVE-2022-30592)

1: <https://github.com/efchatz/HTTP3-attacks>

--------------------------------------

reducir la entropía de su carga útil

1: <https://github.com/ORCx41/EntropyFix>

--------------------------------------

Proteja sus servidores SIP de los malos actores.

1: <https://github.com/SentryPeer/SentryPeer>

--------------------------------------

DongTai es un producto de prueba de seguridad de aplicaciones interactivas (IAST) que admite la detección de vulnerabilidades OWASP WEB TOP 10, vulnerabilidades relacionadas con solicitudes múltiples (incluidas vulnerabilidades lógicas, vulnerabilidades de acceso no autorizado, etc.), vulnerabilidades de componentes de terceros, etc.

1: <https://github.com/HXSecurity/DongTai>

--------------------------------------

Sistema de detección de comportamiento de phishing de voz en AOSP

1: <https://github.com/WSP-LAB/hearmeout>

--------------------------------------

Biblioteca de pirateo de memoria de Windows

1: <https://github.com/DarthTon/Blackbone>

--------------------------------------

HiddenCPG: Detección de clones vulnerables a gran escala mediante isomorfismo de subgráficos de gráficos de propiedades de código

1: <https://github.com/WSP-LAB/HiddenCPG>

--------------------------------------

Oracle WebLogic CVE-2022-21371

1: <https://github.com/Vulnmachines/Oracle-WebLogic-CVE-2022-21371>

--------------------------------------

Rootkit fileless ring 3 con instalador y persistencia que oculta procesos, archivos, conexiones de red, etc.

1: <https://github.com/bytecode77/r77-rootkit>

--------------------------------------

Al obtener las WindowsAPI credenciales de usuario y guardarlas en un archivo

1: <https://github.com/Rvn0xsy/GetWindowsCredentials>

--------------------------------------

Rootkit fileless ring 3 con instalador y persistencia que oculta procesos, archivos, conexiones de red, etc.

1: <https://github.com/bytecode77/r77-rootkit>

--------------------------------------

MATE es un conjunto de herramientas para el análisis de programas interactivos con un enfoque en la búsqueda de errores en el código C y C++ utilizando gráficos de propiedades de código.

1: <https://github.com/GaloisInc/MATE>

--------------------------------------

Un escáner de aplicaciones web basado en Python para recopilar OSINT y fuzz para vulnerabilidades OWASP en un sitio web de destino.

1: <https://github.com/1N3/BlackWidow>

--------------------------------------

Una colección de cargas útiles de Burpsuite Intruder, cargas útiles de BurpBounty, listas fuzz, cargas de archivos maliciosos y metodologías y listas de verificación de pentesting web.

1: <https://github.com/1N3/IntruderPayloads>

--------------------------------------

Esta herramienta le ayudará a encontrar la información de USERNAME. Antes, hay muchas herramientas que solo muestran que el NOMBRE DE USUARIO se usa en ese sitio web, pero no muestran el nombre, el número de teléfono, la foto de perfil, la dirección, los seguidores, etc. Esto es diferente de otras herramientas. Esta herramienta mostrará toda la información disponible PÚBLICAMENTE en el sitio web

1: <https://github.com/uosint-project/uosint>

--------------------------------------

Esta es una herramienta completa que contiene la caja para la competencia Capture The Flag. Sobre todo he insertado todas las herramientas necesarias. Algunas personas tienen problemas para instalar herramientas para las etapas iniciales.

1: <https://github.com/arhaxor21/Flagy>

--------------------------------------

IoT resistente y Honeypot de tecnología operativa

1: <https://github.com/aau-network-security/riotpot>

--------------------------------------

Rastreador web con perspectiva de usuario que utiliza el protocolo de depuración de Chromium

1: <https://github.com/aau-network-security/kraaler>

--------------------------------------

Kit de herramientas de enriquecimiento de dominio $ pip install richkit

1: <https://github.com/aau-network-security/richkit>

--------------------------------------

Reenvíe puertos tcp locales o remotos a través de canalizaciones SMB.

1: <https://github.com/p3nt4/Invoke-Piper>

--------------------------------------

¡El mejor espía WiFi disponible para alquilar! Hecho para piratas informáticos, para piratas informáticos

1: <https://github.com/DeaDHackS/WiFiSpy>

--------------------------------------

Un programa de trabajo que le permite no ser expulsado de un servidor por inactividad.

1: <https://github.com/DR34M-M4K3R/Anti-AFK-kick-for-all-games>

--------------------------------------

DNA-RECON { Herramienta automática de reconocimiento web }

1: <https://github.com/CYBERNIKUNJ/DNA-RECON>

--------------------------------------

💻Una herramienta de administración remota de la consola de Windows escrita en Go & Intel x86 Assembly. Admite shell remoto y captura de pantalla.

1: <https://github.com/Zhuagenborn/Goasm-RAT>

--------------------------------------

Un backdoor con multitud de funcionalidades.

1: <https://github.com/thatcherclough/BetterBackdoor>

--------------------------------------

Ataque de red Ataque wifi Ataque vlan Ataque arp Ataque Mac Ataque revelado etc../

1: <https://github.com/Matrix07ksa/EvilNet>

--------------------------------------

Brute\_Force\_Attack Gmail Hotmail Twitter Facebook Netflix

1: <https://github.com/Matrix07ksa/Brute_Force>

--------------------------------------

OBSERVA

1: <https://github.com/b4rc0d37/Observa>

--------------------------------------

MARCO REBELDE v.2 . SERVIDOR HTTP PARA PHISHING

1: <https://github.com/AngelSecurityTeam/RevoltShing>

--------------------------------------

💉Una herramienta de inyección de biblioteca de enlace dinámico de Windows escrita en C++20. Puede inyectar una biblioteca de enlaces dinámicos en un proceso en ejecución por el título de su ventana o crear un nuevo proceso con una inyección.

1: <https://github.com/Zhuagenborn/Dll-Injector>

--------------------------------------

Volcar DPAPI credz de forma remota

1: <https://github.com/login-securite/DonPAPI>

--------------------------------------

Entropy Toolkit es un conjunto de herramientas para proporcionar ataques de cámaras web IP Netwave y GoAhead. Entropy Toolkit es un poderoso conjunto de herramientas para pruebas de penetración de cámaras web.

1: <https://github.com/evildevill/entropy>

--------------------------------------

HaCkeRWaSi es una herramienta de recopilación de información (OSINT) que tiene como objetivo realizar investigaciones sobre una persona francesa, suiza, luxemburguesa o belga. Proporciona varios módulos que permiten búsquedas eficientes. HaCkeRWaSi no requiere una clave API o ID de inicio de sesión. puede ejecutar esta herramienta en puerto de comando Linux y Termux SO Esta herramienta es solo para fines educativos

1: <https://github.com/evildevill/Hackerwasi>

--------------------------------------

Devil es una herramienta que está hecha básicamente para Facebook para hackear cuentas objetivo, BruteForce Attack, capturar cuentas de amigos, yahoo chacker, herramienta de recopilación de información de Facebook Friend, reacciones de me gusta automáticas y mucho más. Espero que disfrutes esta herramienta. No soy responsable si tú usar esta herramienta para cualquier propósito ilegal

1: <https://github.com/evildevill/Devil>

--------------------------------------

extensión spoofer and payload generator

1: <https://github.com/thelinuxchoice/lizard>

--------------------------------------

SharpDPAPI es un puerto C# de alguna funcionalidad DPAPI de Mimikatz.

1: https://github.com/ghostpack/sharpdpapi

--------------------------------------

Una herramienta de reconocimiento que permite buscar URL que están expuestas a través de servicios más cortos

1: <https://github.com/utkusen/urlhunter>

--------------------------------------

Escáner de DNS/red/puerto peligrosamente rápido

1: <https://github.com/Esc4iCEscEsc/skanuvaty>

--------------------------------------

CamOver es una herramienta de explotación de cámara que permite revelar la contraseña de administrador de la cámara de red.

1: <https://github.com/EntySec/CamOver>

--------------------------------------

Clona rápidamente un sitio web e inicia un servidor HTTP para robar información con httphish.py🐍

1: <https://github.com/miguelangelramirez/httphish>

--------------------------------------

Configure su propio servidor OpenVPN en Debian, Ubuntu, Fedora, CentOS o Arch Linux.

1: <https://github.com/angristan/openvpn-install>

--------------------------------------

Panel DDoS de capa 7 con Cloudflare Bypass (UAM, CAPTCHA, BFM, etc.)

1: <https://github.com/firstapostle/Blood>

--------------------------------------

Script OSINT simple para encontrar perfiles de Instagram por nombre y correo electrónico/teléfono

1: <https://github.com/blackeko/yesitsme>

--------------------------------------

DaProfiler le permite crear un perfil en su objetivo basado únicamente en Francia. La particularidad de este programa es su capacidad para encontrar las direcciones de correo electrónico de su objetivo.

1: <https://github.com/dalunacrobate/DaProfiler>

--------------------------------------

BioIG es un módulo que le permite extraer información personal de una biografía de perfil de Instagram, como: religión, pasatiempos, origen étnico, correos electrónicos, Paypal.me/, Snapchat, Twitter, mejores amigos, edad, ubicación, relación amorosa, fecha de relación amorosa, Facebooks, Signo Astrológico, Sexualidad.

1: <https://github.com/dalunacrobate/BioIG>

--------------------------------------

Snap Scraper permite a los usuarios descargar medios cargados en Snap Map de Snapchat utilizando un conjunto de coordenadas de latitud y longitud.

1: <https://github.com/rhematt/Snap-Scraper>

--------------------------------------

Esta es una herramienta de inteligencia de código abierto y se usa para recopilar información sobre las redes sociales y también se usa para averiguar si el nombre de usuario se encuentra en alguno de los sitios web. Se usa para encontrar la ubicación GPS de una imagen y también verifica si el correo electrónico se encuentra o no.

1: <https://github.com/Ramalingasamy012/SocialRecon>

--------------------------------------

Script para modificar una distro Parrot OS con las herramientas OSINT más populares

1: <https://github.com/Dimaslg/osintBOX>

--------------------------------------

Marco OSINT para Skype

1: <https://github.com/8C/SkypeSearch>

--------------------------------------

Infosint es una herramienta de inteligencia de código abierto que se utiliza para rastrear la dirección IP y generar mapas de calor y puede encontrar cuentas de redes sociales usando imágenes.

1: <https://github.com/Ramalingasamy012/Infosint>

--------------------------------------

Rastreador web simple, pero inteligente, de subprocesos múltiples para recopilar aleatoriamente grandes listas de nombres de dominio únicos.

1: <https://github.com/kgretzky/dcrawl>

--------------------------------------

Marco de ataque de intermediario independiente utilizado para credenciales de inicio de sesión de phishing junto con cookies de sesión, lo que permite eludir la autenticación de 2 factores

1: <https://github.com/kgretzky/evilginx2>

--------------------------------------

Plataforma de automatización y generación de informes VAPT (evaluación de vulnerabilidades y pruebas de penetración).

1: <https://github.com/reconmap/reconmap>

--------------------------------------

Una herramienta de Python utilizada para automatizar la ejecución de las siguientes herramientas: Nmap, Nikto y Dirsearch, pero también para automatizar la generación de informes durante una prueba de penetración web.

1: https://github.com/Anteste/WebMap

--------------------------------------

Generador de accesos directos maliciosos para recopilar hashes NTLM de recursos compartidos de archivos inseguros.

1: <https://github.com/dievus/lnkbomb>

--------------------------------------

Ignorante le permite verificar si un número de teléfono se usa en diferentes sitios como Snapchat, Instagram.

1: <https://github.com/megadose/ignorant>

--------------------------------------

🇮🇳 🤖Es fácil de usar el trabajo de botnet de Android sin reenvío de puertos, vps y Android Studio

1: https://github.com/ScRiPt1337/Teardroid-phprat

--------------------------------------

Holehe le permite verificar si el correo se usa en diferentes sitios como twitter, instagram y recuperará información en sitios con la función de contraseña olvidada.

1: <https://github.com/megadose/holehe>

--------------------------------------

Toutatis es una herramienta que te permite extraer información de cuentas de instagram como correos electrónicos, números de teléfono y más

1: https://github.com/megadose/toutatis

--------------------------------------

Puredns es una herramienta rápida de resolución de dominios y fuerza bruta de subdominios que puede filtrar con precisión los subdominios comodín y las entradas envenenadas de DNS.

1: <https://github.com/d3mondev/puredns>

--------------------------------------

Robar imágenes de víctimas, ubicación exacta, información del dispositivo y mucho más

1: <https://github.com/swagkarna/nivistealer>

--------------------------------------

HostHunter una herramienta de reconocimiento para descubrir nombres de host utilizando técnicas OSINT.

1: <https://github.com/SpiderLabs/HostHunter>

--------------------------------------

Totalmente en desarrollo! Un conjunto de herramientas que reúne herramientas de prueba de penetración, como herramientas inalámbricas, herramientas web, herramientas para descifrar contraseñas, etc.

1: <https://github.com/MyMeepSQL/OmegaPSToolkit>

--------------------------------------

Inyector de puerta trasera de complemento de Minecraft

1: <https://github.com/VoxelHax/OpenBukloit>

--------------------------------------

Escáner de seguridad cibernética completamente automatizado

1: <https://github.com/R00tendo/awacs-scanner>

--------------------------------------

Doxea información pública de un número de teléfono

1: <https://github.com/Alcatraz2033/Phone-dox>

--------------------------------------

Automatización de scripts bash de Linux para metasploit

1: <https://github.com/rand0m1ze/ezsploit>

--------------------------------------

Obtener historial de google chrome

1: <https://github.com/De3vil/Get_History>

--------------------------------------

Robar contraseñas guardadas de Chrome “indetectables”

1: <https://github.com/de3vil/steal_ps>

--------------------------------------

Herramienta de ingeniería social

1: https://github.com/Gameye98/santet-online

--------------------------------------

Una herramienta de reconocimiento que encuentra datos confidenciales dentro de las capturas de pantalla cargadas en prnt.sc

1: https://github.com/utkusen/shotlooter

--------------------------------------

Rastrea el sitio web y encuentra enlaces de redes sociales rotos que pueden ser secuestrados

1: <https://github.com/utkusen/socialhunter>

--------------------------------------

Responder es un envenenador LLMNR, NBT-NS y MDNS, con un servidor de autenticación no autorizado HTTP/SMB/MSSQL/FTP/LDAP integrado que admite NTLMv1/NTLMv2/LMv2, seguridad extendida NTLMSSP y autenticación HTTP básica.

1: <https://github.com/SpiderLabs/Responder>

--------------------------------------

Herramienta de ataque WPA/WPA2 PSK automatizada

1: <https://github.com/MS-WEB-BN/h4rpy>

--------------------------------------

Una herramienta avanzada para el reconocimiento de correo electrónico

1: <https://github.com/sham00n/buster>

--------------------------------------

Enlaces para el equipo OSINT

1: <https://github.com/IVMachiavelli/OSINT_Team_Links>

--------------------------------------

ReconPi: una herramienta de reconocimiento liviana que realiza un escaneo extenso con las últimas herramientas.

1: https://github.com/x1mdev/ReconPi

--------------------------------------

Generador y verificador de código Nitro de Discord. Genera códigos Nitro Classic y Boost. Uso de proxy HTTPS (Autoscraper)

1: <https://github.com/lnxcz/nitro-generator>

--------------------------------------

Discord Nitro, Sorteo y francotirador Privnote! Hecho con Python

1: <https://github.com/lnxcz/discord-sniper>

--------------------------------------

Herramienta para crear puertas traseras

1: <https://github.com/KobaWare/Deepsploit>

--------------------------------------

Discord Invite Generator And Checker. Uso de proxy HTTPS (Autoscraper)

1: <https://github.com/lnxcz/invite-generator>

--------------------------------------

Visualizador de estado personalizado de Discord. Puede agregar reproducción, transmisión, visualización y escucha.

1: <https://github.com/lnxcz/custom-status>

--------------------------------------

Selfbot.py – Un selfbot de python discord que es fácil de instalar – Escrito usando discord.py

1: <https://github.com/cgrok/selfbot.py>

--------------------------------------

Autopsy® es una plataforma forense digital y una interfaz gráfica para The Sleuth Kit® y otras herramientas forenses digitales. Puede ser utilizado por examinadores policiales, militares y corporativos para investigar lo que sucedió en una computadora. Incluso puede usarlo para recuperar fotos de la tarjeta de memoria de su cámara.

1: <https://github.com/sleuthkit/autopsy>

--------------------------------------

Enlaces para el equipo osint

1: <https://github.com/IVMachiavelli/OSINT_Team_Links>

--------------------------------------

Gorecon es una herramienta de reconocimiento todo en uno, también conocida como navaja suiza para reconocimiento, una herramienta que todo pentester/bughunter podría querer considerar en su arsenal.

1: <https://github.com/devanshbatham/Gorecon>

--------------------------------------

Escáner de vulnerabilidades de cámaras web | Herramienta de escaneo de vulnerabilidades de cámaras web

1: <https://github.com/jorhelp/Ingram>

--------------------------------------

Automatización de rastreo de red con Bettercap como AP no autorizado o como cliente en su red

1: <https://github.com/90N45-d3v/BetterSniff>

--------------------------------------

Seguimiento de dispositivos WiFi con la intensidad de la señal recibida

1: <https://github.com/90N45-d3v/dBmonster>

--------------------------------------

Sandman es una puerta trasera basada en NTP para compromisos de equipos rojos en redes reforzadas.

1: <https://github.com/Idov31/Sandman>

--------------------------------------

Moderna red de bots punto a punto multiplataforma automodificable sobre TOR

1: <https://github.com/ThrillQuks/Pitraix>

--------------------------------------

Extraiga la información del servidor y la dirección IP del navegador SSRF

1: <https://github.com/bbhunter/Priest>

--------------------------------------

HazProne es un marco de Pentesting en la nube que emula escenarios del mundo real mediante la implementación de recursos de AWS Vulnerable-By-Demand que le permiten pentestear vulnerabilidades internas y, por lo tanto, obtener una mejor comprensión de lo que podría salir mal y por qué.

1: <https://github.com/stafordtituss/HazProne>

--------------------------------------

Un marco C2 consciente de proxy utilizado para ayudar a los equipos rojos con la post-explotación y el movimiento lateral.

1: <https://github.com/nettitude/PoshC2>

--------------------------------------

HTTP/HTTPS tunelizable proxy socks4a escrito en C# e implementable a través de PowerShell

1: <https://github.com/nettitude/SharpSocks>

--------------------------------------

OpenThread lanzado por Google es una implementación de código abierto del protocolo de red Thread

1: <https://github.com/openthread/openthread>

--------------------------------------

Herramientas para realizar ataques en dominios EIGRP

1: <https://github.com/in9uz/EIGRPWN>

--------------------------------------

WPRecon, es una herramienta para el reconocimiento de vulnerabilidades e información de blackbox para wordpress.

1: <https://github.com/blackcrw/wprecon>

--------------------------------------

ReconNess es una plataforma para permitir el reconocimiento continuo (CR) donde puede configurar una canalización de herramientas de #recon (Agentes) y activarlo según el cronograma o los eventos.

1: <https://github.com/reconness/reconness>

--------------------------------------

Rock-On es una herramienta de reconocimiento todo en uno que solo obtendrá una sola entrada del nombre de dominio y hará todo el trabajo solo.

1: <https://github.com/SilverPoision/Rock-ON>

--------------------------------------

JF⚡can - Escaneo de puertos y descubrimiento de servicios súper rápidos usando Masscan y Nmap. Escanee grandes redes con Masscan y use las capacidades de secuencias de comandos de Nmap para descubrir información sobre los servicios. Generar informe.

1: <https://github.com/nullt3r/jfscan>

--------------------------------------

Una herramienta de seguridad para enumerar WebSockets

1: <https://github.com/PalindromeLabs/STEWS>

--------------------------------------

Trato de suplantación de identidad XLL

1: <https://github.com/Octoberfest7/XLL_Phishing>

--------------------------------------

👀¡Intercepte solicitudes pasivamente de DHCP desde su propia red!👀

1: <https://github.com/vincenzogianfelice/DHCPEyes>

--------------------------------------

RAVEN es un marco flexible y polivalente de análisis probabilístico de riesgos, validación y cuantificación de incertidumbres, optimización de parámetros, reducción de modelos y descubrimiento de conocimiento de datos.

1: <https://github.com/idaholab/raven>

--------------------------------------

KubeClarity es una herramienta para la detección y gestión de listas de materiales de software (SBOM) y vulnerabilidades de imágenes de contenedores y sistemas de archivos.

1: <https://github.com/openclarity/kubeclarity>

--------------------------------------

Malcolm es un conjunto de herramientas de análisis de tráfico de red potente y fácil de implementar para artefactos de captura de paquetes completos (archivos PCAP) y registros Zeek.

1: <https://github.com/cisagov/Malcolm>

--------------------------------------

Una herramienta de automatización que escanea subdominios, toma de control de subdominios, luego filtra XSS, SSTI, SSRF y más parámetros de punto de inyección y escanea automáticamente en busca de algunas vulnerabilidades bajas.

1: <https://github.com/R0X4R/Garud>

--------------------------------------

Un escáner basado en Python usa shodan-internetdb para escanear la IP.

1: <https://github.com/R0X4R/snetra>

--------------------------------------

Venom: un proxy multisalto para probadores de penetración

1: <https://github.com/Dliv3/Venom>

--------------------------------------

EV: Evasión de IDS mediante manipulación de paquetes

1: <https://github.com/TomAPU/ev>

--------------------------------------

Detectar eructos

1: <https://github.com/TomAPU/checkburp>

--------------------------------------

Shell inverso de forma anónima a través de la red Tor utilizando servicios ocultos sin reenvío de puertos.

1: <https://github.com/samet-g/tornado>

--------------------------------------

Automatización externa avanzada en programas de recompensas por errores al ejecutar el mejor conjunto de herramientas para realizar escaneos y descubrir vulnerabilidades.

1: <https://github.com/samet-g/bugradar>

--------------------------------------

Una herramienta orientada a Python para eliminar el enlace del grupo de WhatsApp usando Google Dork. Elimina los enlaces del grupo de Whatsapp de los resultados de Google y brinda enlaces que funcionan.

1: <https://github.com/riz4d/WaGpScraper>

--------------------------------------

Dome - Herramienta de enumeración de subdominios. Rápido y confiable script en python que realiza escaneo activo y/o pasivo para obtener subdominios y buscar puertos abiertos.

1: <https://github.com/v4d1/Dome>

--------------------------------------

El marco web HTTP/2 Go más rápido. Fácil de aprender. Desarrollo rápido con Code you control. Relación costo-rendimiento imbatible🍃 🚀 | gracias |

1: <https://github.com/kataras/iris>

--------------------------------------

Muxie es un multiplexor HTTP moderno, rápido y ligero para Go. Totalmente compatible con la interfaz http.Handler. Escrito para todos.

1: https://github.com/kataras/muxie

--------------------------------------

Recsech es una herramienta para hacer Footprinting y Reconocimiento en la red de destino. Recsech recopila información como información de DNS, subdominios, HoneySpot detectado, adquisiciones de subdominios, reconocimiento en Github y mucho más que puede ver en Funciones en herramientas.

1: <https://github.com/radenvodka/Recsech>

--------------------------------------

datos de reconocimiento para programas públicos de recompensas por errores (actualizaciones irregulares)

1: <https://github.com/ARPSyndicate/bug-bounty-recon-dataset>

--------------------------------------

Paquete para crear enlaces con backlinks automáticos

1: <https://github.com/toshism/org-super-links>

--------------------------------------

Herramienta para desbloquear el cargador de arranque y habilitar el acceso raíz en teléfonos con Windows

1: <https://github.com/ReneLergner/WPinternals>

--------------------------------------

HellPot es un portal de sufrimiento interminable destinado a castigar a los bots HTTP rebeldes.

1: <https://github.com/yunginnanet/HellPot>

--------------------------------------

KcpNatProxy es un proxy inverso para ayudarlo a exponer un servidor TCP/UDP local detrás de un NAT o un firewall en Internet.

1: <https://github.com/yigolden/KcpNatProxy>

--------------------------------------

Una herramienta de Python puro para encontrar y comparar ataques de typo-squatting, bytesqatting, phishing y suplantación de marca

1: <https://github.com/f8al/DNSrazzle>

--------------------------------------

¡25 honeypots diferentes en un solo paquete pypi! (dns, ftp, httpproxy, http, https, imap, mysql, pop3, postgres, redis, smb, smtp, socks5, ssh, telnet, vnc, mssql, elastic, ldap, ntp, memcache, snmp, oracle, sorbo e irc )

1: <https://github.com/qeeqbox/honeypots>

--------------------------------------

19 Honeypots personalizables para monitorear el tráfico de red, las actividades de los bots y las credenciales de nombre de usuario/contraseña (DNS, HTTP Proxy, HTTP, HTTPS, SSH, POP3, IMAP, STMP, RDP, VNC, SMB, SOCKS5, Redis, TELNET, Postgres, MySQL, MSSQL , Elástico y ldap)

1: <https://github.com/qeeqbox/chameleon>

--------------------------------------

Herramienta rápida, multiproceso, eficiente y fácil de usar para el bombardeo de correo/spam. Envío de correos a través de servicios de cartero alojados por diferentes proveedores.

1: <https://github.com/juzeon/fast-mail-bomber>

--------------------------------------

Encuentra ID de ubicación de Instagram cerca de una latitud y longitud específicas.

1: <https://github.com/bellingcat/instagram-location-search>

--------------------------------------

Un envenenador de caché de DNS dirigido

1: <https://github.com/cr0mll/deserter>

--------------------------------------

E-ntel es una herramienta que recopila información de cuentas de correo electrónico (ip, nombre de host, país,...) de diferentes fuentes públicas (motores de búsqueda, servidores de claves pgp y shodan) y verifica si los correos electrónicos se filtraron utilizando la API de correos electrónicos pirateados. Es una herramienta realmente simple, pero muy efectiva para las primeras etapas de una prueba de penetración o simplemente para conocer la visibilidad de su empresa en…

1: <https://github.com/CybernetiX-S3C/E-ntel>

--------------------------------------

Herramienta que limita el ancho de banda de los dispositivos en la misma red sin acceso.

1: <https://github.com/bitbrute/evillimiter-windows>

--------------------------------------

herramienta de piratería

1: <https://github.com/programmingAthlete/BruteSniffing_Fisher>

--------------------------------------

📡Convierta un nombre de host en una IP y una IP en un nombre de host, realice un WHOIS, obtenga toda la información de una IP o un nombre de host.

1: <https://github.com/loutrerusse/RusseIP>

--------------------------------------

Herramientas de creación/inyección de carga de imagen

1: https://github.com/chinarulezzz/pixload

--------------------------------------

Herramienta de administración remota de Android impulsada por Electron Framework con compatibilidad con Java 11 | los problemas duplicados del problema n. ° 72 darán como resultado que el usuario publique el problema, ¡prohibido!

1: <https://github.com/Morsmalleo/AhMyth>

--------------------------------------

Herramienta de amplificación DDoS

1: <https://github.com/OffensivePython/Saddam>

--------------------------------------

Nscan: Escáner rápido de Internet

1: <https://github.com/OffensivePython/Nscan>

--------------------------------------

Apkatshu es una herramienta para extraer URL, correos electrónicos, direcciones IP y datos interesantes de archivos APK

1: <https://github.com/0xPwny/Apkatshu>

--------------------------------------

Forzado Man-In-The-Middle HTTPs-Evitar proxy inverso

1: <https://github.com/m4n3dw0lf/sslkill>

--------------------------------------

Script PHP para robar cookies, capturar IP e información del dispositivo.

1: <https://github.com/4xx404/CookieCatch>

--------------------------------------

Arissploit Framework es una base de datos de exploits, virus y herramientas para pruebas de penetración desarrollada por Entynetproject y diseñada por DJ Mobley.

1: <https://github.com/attackgithub/arissploit>

--------------------------------------

Una herramienta OSINT de Instagram para recopilar todas las ubicaciones geoetiquetadas disponibles en un perfil de Instagram para trazarlas en un mapa y volcarlas en un JSON.

1: <https://github.com/bernsteining/instaloctrack>

--------------------------------------

Raspador TikTok. Descargue publicaciones de video, recopile metadatos de usuario/tendencia/hashtag/música, firme URL, etc.

1: <https://github.com/drawrowfly/tiktok-scraper>

--------------------------------------

Omega Framework es un marco de post-explotación de PHP, con el objetivo de proporcionar una conexión sigilosa similar a un shell a través de HTTP entre el cliente y el servidor web utilizando solo una carga útil de PHP simple. Es un marco poderoso capaz de mantener el acceso a un servidor web comprometido con fines de escalada de privilegios.

1: <https://github.com/BelalAbdelWahab/omega>

--------------------------------------

Herramienta de rastreo web de Python

1: <https://github.com/rly0nheart/tarantula>

--------------------------------------

Utilidad de Python rápida que escribí para convertir las solicitudes HTTP de Burp Suite en perfiles Cobalt Strike Maleable C2

1: <https://github.com/CodeXTF2/Burp2Malleable>

--------------------------------------

Packer Fuzzer es un escáner rápido y eficiente para la detección de seguridad de sitios web construidos por un paquete de módulos javascript como Webpack.

1: <https://github.com/rtcatc/Packer-Fuzzer>

--------------------------------------

¡Ultra DDos en un script de python en línea ddos!

1: <https://github.com/mishakorzik/Ultra-DDos>

--------------------------------------

Script simple que verifica un dominio para protecciones de correo electrónico

1: <https://github.com/BishopFox/spoofcheck>

--------------------------------------

Enumeración de subdominios y marcadores de mapa

1: <https://github.com/le4f/dnsmaper>

--------------------------------------

PenBox: un marco de prueba de penetración: la herramienta con todas las herramientas, el repositorio del pirata informático

1: <https://github.com/x3omdax/PenBox>

--------------------------------------

El objetivo del proyecto es crear un bot que pueda jugar Agar.io

1: <https://github.com/Apostolique/Agar.io-bot>

--------------------------------------

Herramientas de evasión AV de Python

1: <https://github.com/G1ft3dC0d3/MsfMania>

--------------------------------------

detectar el capturador/ladrón de fichas de discordia

1: <https://github.com/Traumatism/Discord-Malware-Detector>

--------------------------------------

un escáner de subdominios moderno

1: <https://github.com/Traumatism/subdah>

--------------------------------------

Un marco semiautomático osint/recon.

1: <https://github.com/Traumatism/Smog>

--------------------------------------

Osint

1: <https://github.com/Traumatism/Stick>

--------------------------------------

Herramienta de búsqueda simple de Google Dorks

1: <https://github.com/six2dez/dorks_hunter>

--------------------------------------

Script Bash para verificar si un dominio o una lista de dominios se pueden falsificar en función de los registros DMARC

1: <https://github.com/v4d1/spoofthatmail>

--------------------------------------

Dome – Herramienta de enumeración de subdominios. Rápido y confiable script en python que realiza escaneo activo y/o pasivo para obtener subdominios y buscar puertos abiertos.

1: https://github.com/v4d1/Dome

--------------------------------------

Cobalt Strike es una herramienta comercial de acceso remoto con todas las funciones que se anuncia a sí misma como “software de simulación de adversarios diseñado para ejecutar ataques dirigidos y emular las acciones posteriores a la explotación de actores de amenazas avanzados”. Las capacidades interactivas posteriores a la explotación de Cobalt Strike cubren la gama completa de tácticas ATT&CK, todas ejecutadas dentro de un único…

1: <https://github.com/trewisscotch/CobaltStr4.4>

--------------------------------------

SMS anonimos

1: <https://github.com/MasterS00/smscat>

Apt -y install python

Apt -y install python-pip

Apt -y install git

Git clone <https://github.com/MasterS00/smscat>

Cd smscat

Bash install.sh

Python3 setup.py

--------------------------------------

plataforma de radio de software de bajo costo

1: <https://github.com/greatscottgadgets/hackrf>

--------------------------------------

Escáner avanzado de búsqueda de idiotas y exploits masivos

1: <https://github.com/AlisamTechnology/ATSCAN>

--------------------------------------

una multiherramienta USB + marco Amaranth HDL para monitorear, piratear y desarrollar dispositivos USB

1: <https://github.com/greatscottgadgets/luna>

--------------------------------------

Script para generar una aplicación de Android que puede secuestrar sesiones autenticadas en cookies

1: <https://github.com/Ro9ueAdmin/EvilApp>

--------------------------------------

Lockphish es la primera herramienta (04/07/2020) para ataques de phishing en la pantalla de bloqueo, diseñada para capturar las credenciales de Windows, el PIN de Android y el código de acceso de iPhone usando un enlace https.

1: <https://github.com/jaykali/lockphish>

--------------------------------------

PHISHLET [EVILGINX2] La configuración de los sitios de phishing está escrita en el lenguaje yaml. Este es un largo desarrollo de mi colección en el que he estado trabajando durante los últimos 3 meses debido a los cambios en las reglas de seguridad del sitio en scripts particulares para eludir la seguridad de CloudFlare.🙌Les presento mi colección de los sitios: 1Password / Binance /…

1: <https://github.com/trewisscotch/PHISHLET-EVILGINX2->

--------------------------------------

Herramienta para automatizar la explotación de la vulnerabilidad del puente android degubg

1: <https://github.com/DrH3X/Android-debug-bridge->

--------------------------------------

Programa, creado para facilitar el uso de los comandos populares adb y fastboot

1: <https://github.com/fast-geek/Android-Tool>

--------------------------------------

📃Guión para el envío conveniente de documentación para cualquier curso en la plataforma Yandex Academy

1: <https://github.com/fast-geek/YandexLyceumDocs>

--------------------------------------

BirWell / CoinEx / eTorox / Venus / ProBit Global / Poloniex / Gemini / Gate.io / Binance / Bitfinex / Blockchain / Cex.io / Coinbase / Dashlane / Enpass / Enterprise WebAccountManager / Exmo / FTX Trading / Google / Huobi / Keeper / Korbit / Kraken / Multicontraseña / O365 / Yahoo / Canadianbitcoins.com / Liquid.com / Litebit.com / Netcoins.com /…

1: <https://github.com/trewisscotch/Modlishka-Templates>

--------------------------------------

Sitio que recopila palabras y billeteras secretas, y luego lo agregaremos y enviaremos datos a los telegramas. Después de recibir las palabras y direcciones secretas de las billeteras criptográficas, puede restaurarlas y venderlas o venderlas.

1: <https://github.com/trewisscotch/DeFi-phishing->

--------------------------------------

Una colección de scripts, herramientas. Y configuraciones para varios sistemas operativos y aplicaciones, todos gratuitos o de código abierto, para ayudar en la defensa improvisada de Blue-Team bajo una amenaza activa.

1: <https://github.com/simeononsecurity/Blue-Team-Tools>

--------------------------------------

Una colección de increíbles recursos, herramientas y otras cosas brillantes para las pruebas de penetración.

1: <https://github.com/enaqx/awesome-pentest>

--------------------------------------

Inyecte una biblioteca compartida (es decir, código arbitrario) en un proceso de Linux en vivo, sin ptrace

1: <https://github.com/DavidBuchanan314/dlinject>

--------------------------------------

Escáner de red Golang con descubrimiento arp y analizador propio

1: https://github.com/luijait/GONET-Scanner

--------------------------------------

Recursos del equipo azul

1: <https://github.com/rosonsec/BlueTeam>

--------------------------------------

Exploits públicos y modificaciones

1: https://github.com/rosonsec/Exploits

--------------------------------------

SharpDoor es un RDPWrap alternativo escrito en C# para permitir múltiples sesiones de RDP (Escritorio remoto) al parchear el archivo termsrv.dll.

1: <https://github.com/infosecn1nja/SharpDoor>

--------------------------------------

𝙷𝚎𝚢!! 𝙷𝚘𝚕𝚊👋, 𝚎𝚜 𝚞𝚗 𝚐𝚞𝚜𝚝𝚘 𝚝𝚎𝚗𝚎𝚛𝚝𝚎 𝚊𝚚𝚞𝚒́ 𝚎𝚗 𝚎𝚜𝚝𝚎 𝚛𝚎𝚙𝚘𝚜𝚒𝚝𝚘𝚛𝚒𝚘 ¿𝙼𝚎 𝚛𝚎𝚐𝚊𝚕𝚊𝚜 𝚞𝚗𝚊⭐?, 𝚎𝚜𝚝𝚎 𝚎𝚜 𝚃𝚑𝚎 𝙼𝚢𝚜𝚝𝚒𝚌 - 𝙱𝚘𝚝, 𝚞𝚗 𝙱𝚘𝚝 𝚙𝚊𝚛𝚊 𝚆𝚑𝚊𝚝𝚜𝙰𝚙𝚙 𝚏𝚞𝚗𝚌𝚒𝚘𝚗𝚊𝚕 𝚌𝚘𝚗 𝚕𝚊 𝚟𝚎𝚛𝚜𝚒𝚘𝚗 𝚖𝚞𝚕𝚝𝚒 -𝚍𝚎𝚟𝚒𝚌𝚎 (𝚋𝚎𝚝𝚊), 𝚎𝚜𝚙𝚎𝚛𝚘 𝚝𝚎 𝚐𝚞𝚜𝚝𝚎: 𝙳

1: <https://github.com/BrunoSobrino/TheMystic-Bot-MD>

--------------------------------------

Red Team Toolkit es una aplicación web ofensiva Django de código abierto que mantiene unidas las útiles herramientas ofensivas utilizadas en el equipo rojo.

1: https://github.com/signorrayan/RedTeam\_toolkit

--------------------------------------

Herramienta automatizada para crackear redes WiFi con protección WPA2 y WPS.

1: <https://github.com/R3LI4NT/Wifi-Hack>

--------------------------------------

[Script] Cifrar y descifrar mensajes con python.

1: <https://github.com/R3LI4NT/Crypt-Zer0>

--------------------------------------

Una herramienta profesional de hacking ético.

1: <https://github.com/SamOBoy97/SamSploit>

--------------------------------------

Herramienta de informe de errores de Laravel

1: <https://github.com/LaraBug/LaraBug>

--------------------------------------

Configuración de malware y extracción de carga útil

1: <https://github.com/kevoreilly/CAPEv2>

--------------------------------------

QCSuper es una herramienta que se comunica con teléfonos y módems basados ​​en Qualcomm, lo que permite capturar tramas de radio 2G/3G/4G sin procesar, entre otras cosas.

1: <https://github.com/P1sec/QCSuper>

--------------------------------------

AttackSurfaceMapper es una herramienta que tiene como objetivo automatizar el proceso de reconocimiento.

1: <https://github.com/superhedgy/AttackSurfaceMapper>

--------------------------------------

OBTENGA todas las direcciones IP de cualquier empresa que utilice ASN

1: <https://github.com/mrrobot1o1/asnips>

--------------------------------------

TorGhost es un script de anonimización. TorGhost redirige todo el tráfico de Internet a través del proxy SOCKS5 tor. Las solicitudes de DNS también se redireccionan a través de tor, lo que evita la fuga de DNS. Los scripts también deshabilitan los paquetes no seguros que salen del sistema. Algunos paquetes como la solicitud de ping pueden comprometer su identidad.

1: <https://github.com/SusmithKrishnan/torghost>

--------------------------------------

🔐Lockigest: ¿por qué tendría que ingresar una contraseña para desbloquear su pantalla innumerables veces al día? Lockigest es una idea simple que resuelve esto. Bloqueará su pantalla solo si no se sigue un patrón predefinido dentro de un tiempo determinado.

1: <https://github.com/elmsec/lockigest>

--------------------------------------

Un controlador de devolución de llamada de inyección ciego XXE. Utiliza HTTP y FTP para extraer información. Escrito originalmente en Ruby por ONsec-Lab.

1: <https://github.com/TheTwitchy/xxer>

--------------------------------------

Una herramienta para la búsqueda de errores o pentesting para sitios web que tienen repositorios .git abiertos disponibles en público

1: <https://github.com/HightechSec/git-scanner>

--------------------------------------

Una herramienta para realizar varias técnicas OSINT, agregar todos los datos sin procesar, visualizarlos en un tablero y facilitar las alertas y el monitoreo de los datos.

1: <https://github.com/dvopsway/datasploit>

--------------------------------------

MARA es un marco de análisis e ingeniería inversa de aplicaciones móviles. Es un conjunto de herramientas que reúne herramientas de análisis e ingeniería inversa de aplicaciones móviles de uso común para ayudar a probar aplicaciones móviles contra las amenazas de seguridad móvil OWASP.

1: <https://github.com/xtiankisutsa/MARA_Framework>

--------------------------------------

Herramienta de rastreo pasivo para capturar y visualizar datos de ubicación WiFi revelados por dispositivos iOS

1: <https://github.com/hubert3/iSniff-GPS>

--------------------------------------

Esta herramienta extrae números de tarjetas de crédito, NTLM (DCE-RPC, HTTP, SQL, LDAP, etc.), Kerberos (AS-REQ Pre-Auth etype 23), HTTP Basic, SNMP, POP, SMTP, FTP, IMAP, etc. de un archivo pcap o desde una interfaz en vivo.

1: <https://github.com/lgandx/PCredz>

--------------------------------------

El motor de recopilación de información simplista | Encuentre información avanzada sobre un nombre de usuario, sitio web, número de teléfono, etc.

1: <https://github.com/MandConsultingGroup/Scylla>

--------------------------------------

Un interceptor de tráfico y paquetes de red para Linux. Spoof ARP & Wiretap A Network.

1: <https://github.com/MandConsultingGroup/Espionage>

--------------------------------------

Un marco como un metasploit que contiene una variedad de módulos para pentesting o piratería ética. Este repositorio se actualizará y se agregarán nuevos módulos de vez en cuando.

1: <https://github.com/Cyber-Dioxide/Cyber-Sploit>

--------------------------------------

Una interfaz de línea de comandos de explotación XSS y un generador de carga útil.

1: <https://github.com/t3l3machus/toxssin>

--------------------------------------

Un shell inverso de Windows no convencional, actualmente no detectado por Microsoft Defender y varias otras soluciones antivirus, basado únicamente en el tráfico de http(s).

1: <https://github.com/t3l3machus/hoaxshell>

--------------------------------------

Generador de listas de contraseñas que se enfoca en palabras clave mutadas por patrones de creación de contraseñas de uso común

1: <https://github.com/t3l3machus/psudohash>

--------------------------------------

Reciba alertas por correo electrónico sobre

inicios de sesión ssh exitosos basados ​​en una lista blanca de IP predefinida O una lista blanca de origen de país de IP predefinida (usando mailgun)

1: <https://github.com/t3l3machus/ssh-log-alert>

--------------------------------------

Escáner de captura de pantalla basado en electrones

1: <https://github.com/moloch--/electric-scan>

--------------------------------------

Marco de emulación del adversario

1: <https://github.com/BishopFox/sliver>

--------------------------------------

Escala web NoSQL idempotente Cloud-Native Big-Data Serverless Búsqueda de credenciales de texto sin formato

1: <https://github.com/moloch--/leakdb>

--------------------------------------

Conéctese como si no hubiera un firewall. De forma segura.

1: <https://github.com/hackerschoice/gsocket>

--------------------------------------

oletools: herramientas de Python para analizar archivos MS OLE2 (almacenamiento estructurado, formato binario de archivo compuesto) y documentos de MS Office, para análisis de malware, análisis forense y depuración.

1: <https://github.com/decalage2/oletools>

--------------------------------------

ExeFilter es una herramienta y un marco de código abierto para filtrar formatos de archivo en correos electrónicos, páginas web o archivos. Detecta muchos formatos de archivo comunes y puede eliminar contenido activo (scripts, macros, etc.) de acuerdo con una política configurable.

1: <https://github.com/decalage2/exefilter>

--------------------------------------

Balbuzard es un paquete de herramientas de análisis de malware en python para extraer patrones de interés de archivos sospechosos (direcciones IP, nombres de dominio, encabezados de archivos conocidos, cadenas interesantes, etc.). También puede descifrar la ofuscación de malware como XOR, ROL, etc. mediante fuerza bruta y verificando esos patrones.

1: <https://github.com/decalage2/balbuzard>

--------------------------------------

ACHE es un rastreador web para la búsqueda de dominios específicos.

1: <https://github.com/VIDA-NYU/ache>

--------------------------------------

ReproZip es una herramienta que simplifica el proceso de creación de experimentos reproducibles a partir de ejecuciones de línea de comandos, un denominador común de uso frecuente en la ciencia computacional.

1: <https://github.com/VIDA-NYU/reprozip>

--------------------------------------

Herramienta de descubrimiento y explotación de inclusión de archivos locales

1: <https://github.com/hansmach1ne/lfimap>

--------------------------------------

cheat le permite crear y ver hojas de trucos interactivas en la línea de comandos. Fue diseñado para ayudar a recordar a los administradores del sistema \*nix las opciones para los comandos que usan con frecuencia, pero no con la frecuencia suficiente para recordar.

1: <https://github.com/cheat/cheat>

--------------------------------------

Compruebe a qué proveedores de CDN pertenece una lista de IP

1: <https://github.com/six2dez/ipcdn>

--------------------------------------

Una herramienta de prueba de suplantación de correo electrónico que tiene como objetivo eludir SPF/DKIM/DMARC y falsificar firmas DKIM.🍻

1: <https://github.com/chenjj/espoofer>

--------------------------------------

Escáner rápido de vulnerabilidades de configuración incorrecta de CORS🍻

1: <https://github.com/chenjj/CORScanner>

--------------------------------------

herramientas de pentesting de aplicaciones web para docker

1: <https://github.com/diwsec/pentdocks>

--------------------------------------

Un marco como un metasploit que contiene una variedad de módulos para pentesting o piratería ética. Este repositorio se actualizará y se agregarán nuevos módulos de vez en cuando.

1: <https://github.com/Cyber-Dioxide/Cyber-Sploit>

--------------------------------------

Marco de piratería de Windows usando Reverse Shell

1: <https://github.com/canarddu38/DUCKSPLOIT>

--------------------------------------

Un explorador de cobertura para ingenieros inversos

1: <https://github.com/gaasedelen/lighthouse>

--------------------------------------

Una herramienta para encontrar CNAME de subdominios y verificar la vulnerabilidad de clickjacking.

1: <https://github.com/secretguard/web-recon>

--------------------------------------

💀Genere un montón de archivos pdf maliciosos con la funcionalidad de teléfono en casa. Se puede usar con Burp Collaborator o Interact.sh

1: <https://github.com/jonaslejon/malicious-pdf>

--------------------------------------

GetProcAddressByHash/remap/full dll unhooking/Tartaru's Gate/Spoofing Gate/universal/Perun's Fart/Spoofing-Gate/EGG/RecycledGate/syswhisper/RefleXXion golang implementación

1: <https://github.com/timwhitez/Doge-Gabh>

--------------------------------------

Un exploit de vulnerabilidad xdebug 2.5.5 automatizado

1: <https://github.com/D3Ext/XDEBUG-Exploit>

--------------------------------------

Generador de informes Pentest

1: <https://github.com/pwndoc/pwndoc>

--------------------------------------

Prowler es una herramienta de seguridad de código abierto para realizar evaluaciones de mejores prácticas de seguridad, auditorías, respuesta a incidentes, monitoreo continuo, fortalecimiento y preparación forense de AWS. Contiene más de 240 controles que cubren CIS, PCI-DSS, ISO27001, GDPR, HIPAA, FFIEC, SOC2, AWS FTR, ENS y marcos de seguridad personalizados.

1: <https://github.com/prowler-cloud/prowler>

--------------------------------------

ShellCheck, una herramienta de análisis estático para scripts de shell

1: <https://github.com/koalaman/shellcheck>

--------------------------------------

Merlin es un servidor y agente de comando y control HTTP/2 posterior a la explotación multiplataforma escrito en golang.

1: <https://github.com/Ne0nd0g/merlin>

--------------------------------------

Ataque de delegación restringida basado en recursos de Kerberos desde el exterior mediante Impacket

1: <https://github.com/tothi/rbcd-attack>

--------------------------------------

Una herramienta para generar IP o IP más puerto en lotes de acuerdo con el segmento de IP, puerto o archivo especificado. Según el segmento de IP, puerto o archivo especificado, IP generado por lotes o IP más herramientas de puerto.

1: <https://github.com/nanaao/IPGenerater>

--------------------------------------

Herramienta de seguridad para el reconocimiento y recopilación de información en un sitio web. (pitón 3.x)

1: <https://github.com/c0dejump/HawkScan>

--------------------------------------

Herramienta de Reconocimiento en una cámara web.

1: <https://github.com/c0dejump/camcheckr>

--------------------------------------

WAF\_RateLimitBypass

1: <https://github.com/c0dejump/WAF_RLB>

--------------------------------------

Envoltura de Multi-Packer que nos permite conectar en cadena varios packers, ofuscadores y otras armas orientadas al Red Team. Presentado con marca de agua de artefactos, colección de IOC y puerta trasera de PE. Lo alimentas con tu implante, hace muchas cosas furtivas y escupe un ejecutable ofuscado.

1: <https://github.com/mgeeky/ProtectMyTooling>

--------------------------------------

Una implementación de PoC para suplantar pilas de llamadas arbitrarias al realizar llamadas al sistema (por ejemplo, tomar un identificador a través de NtOpenProcess)

1: <https://github.com/WithSecureLabs/CallStackSpoofer>

--------------------------------------

Malwoverview es una herramienta de primera respuesta utilizada para la búsqueda de amenazas y ofrece información de inteligencia de Virus Total, Hybrid Analysis, URLHaus, Polyswarm, Malshare, Alien Vault, Malpedia, Malware Bazaar, ThreatFox, Triage y es capaz de escanear dispositivos Android contra VT.

1: <https://github.com/alexandreborges/malwoverview>

--------------------------------------

Astra es una herramienta para encontrar URL y secretos dentro de una página web/archivos

1: <https://github.com/Sachin-v3rma/Astra>

--------------------------------------

Herramienta de prueba de penetración de pwning y despliegue WAR automático de Apache Tomcat.

1: <https://github.com/mgeeky/tomcatWarDeployer>

--------------------------------------

API REST de ingeniería inversa automática a través de la captura de tráfico

1: <https://github.com/alufers/mitmproxy2swagger>

--------------------------------------

GoReplay es una herramienta de código abierto para capturar y reproducir tráfico HTTP en vivo en un entorno de prueba para probar continuamente su sistema con datos reales. Se puede utilizar para aumentar la confianza en las implementaciones de código, los cambios de configuración y los cambios de infraestructura.

1: <https://github.com/buger/goreplay>

--------------------------------------

Framework de ingeniería inversa en Python

1: <https://github.com/cea-sec/miasm>

--------------------------------------

Herramienta y marco para leer de forma segura dispositivos de almacenamiento masivo USB que no son de confianza.

1: <https://github.com/cea-sec/usbsas>

--------------------------------------

La solución más rápida y completa para el reconocimiento de dominios. Admite capturas de pantalla, escaneo de puertos, verificación de HTTP, importación de datos de otras herramientas, monitoreo de subdominios, alertas a través de Discord, Slack y Telegram, múltiples claves API para fuentes y mucho más.

1: <https://github.com/Findomain/Findomain>

--------------------------------------

GEF (características mejoradas de GDB): una experiencia moderna para GDB con capacidades avanzadas de depuración para desarrolladores de exploits e ingenieros inversos en Linux

1: <https://github.com/hugsy/gef>

--------------------------------------

Herramienta de detección automática de SSTI con interfaz interactiva

1: <https://github.com/vladko312/SSTImap>

--------------------------------------

Omita las restricciones del firewall del proxy DNS de Cisco Umbrella

1: <https://github.com/plinioseniore/cisco-umbrella-bypass>

--------------------------------------

Una herramienta para descifrar una contraseña wifi con la ayuda de una lista de palabras. Esto puede llevar mucho tiempo para descifrar un wifi dependiendo de la cantidad de contraseñas que contenga su lista de palabras. También es más lento en comparación con el descifrado de cuentas de redes sociales. Me he esforzado lo suficiente para hacerlo lo más rápido posible.

1: <https://github.com/Cyber-Dioxide/Wifi-Brute>

--------------------------------------

Esta herramienta generará un virus que solo puede destruir la computadora con Windows. También puede configurar la ejecución automática en la unidad USB

1: <https://github.com/Cyber-Dioxide/Virus-Builder>

--------------------------------------

Redes HTTP elegantes en Swift

1: <https://github.com/Alamofire/Alamofire>

--------------------------------------

Una herramienta para generar direcciones IP válidas de 55 países. Estas ip se pueden usar para OpenBullet.

1: <https://github.com/Cyber-Dioxide/IP-Grabber>

--------------------------------------

Generador de accesos directos maliciosos para recopilar hashes NTLM de recursos compartidos de archivos inseguros.

1: <https://github.com/dievus/lnkbomb>

--------------------------------------

Desbloquee los enrutadores Wi-Fi WPA/WPA2 con Airodump-ng y Aircrack-ng/Hashcat

1: <https://github.com/brannondorsey/wifi-cracking>

--------------------------------------

Un servidor DNS “malicioso” para ejecutar ataques de DNS Rebinding sobre la marcha (instancia pública que se ejecuta en rebind.network:53)

1: https://github.com/brannondorsey/whonow

--------------------------------------

Un generador de correo electrónico simple que utiliza idiotas en Bing para generar correos electrónicos desde perfiles de LinkedIn.

1: <https://github.com/navisecdelta/EmailGen>

--------------------------------------

Reconocimiento Automático de Matrículas de Tráfico para Android

1: <https://github.com/gonpuga/ANPR>

--------------------------------------

Reconocimiento de placas vehiculares con tecnicas de procesamiento de imágenes digitales en MATLAB

1: https://github.com/sebas932/P\_Final

--------------------------------------

Profesional Inalámbrico de Seguridad Ofensiva

1: <https://github.com/vdb-sander/OSWP>

--------------------------------------

Un kit de herramientas de JavaScript de front-end para crear ataques de reenlace de DNS.

1: https://github.com/brannondorsey/dns-rebind-toolkit

--------------------------------------

Permite el inicio de sesión automático a través de un punto de acceso MEO Wifi punto de acceso MEO Wifi Premium

1: <https://github.com/ravemir/meo-wifi-login>

--------------------------------------

herramienta de reconocimiento simple para ayudarlo a buscar vulnerabilidades en el servidor web

1: <https://github.com/root-x-krypt0n-x/s1c0n>

--------------------------------------

Rastreador web simple y rápido diseñado para el descubrimiento fácil y rápido de puntos finales y activos dentro de una aplicación web

1: <https://github.com/hakluke/hakrawler>

--------------------------------------

Herramienta para descubrir el host de origen detrás de un proxy inverso. ¡Útil para evitar los WAF en la nube!

1: <https://github.com/hakluke/hakoriginfinder>

--------------------------------------

hakip2host toma una lista de direcciones IP a través de stdin, luego realiza una serie de comprobaciones para devolver los nombres de dominio asociados.

1: <https://github.com/hakluke/hakip2host>

--------------------------------------

Extraiga el dominio raíz, el nombre del subdominio y el tld de una URL mediante la lista de sufijos públicos.

1: <https://github.com/joeguo/tldextract>

--------------------------------------

Herramienta pequeña y rápida para realizar búsquedas DNS inversas en masa.

1: <https://github.com/hakluke/hakrevdns>

--------------------------------------

Extraer dominios/subdominios de URLs en masa

1: <https://github.com/hakluke/haktldextract>

--------------------------------------

Algunas herramientas para automatizar el reconocimiento – 003random

1: <https://github.com/003random/003Recon>

--------------------------------------

Herramienta de rastreo de resolución de DNS

1: <https://github.com/rs/dnstrace>

--------------------------------------

FUD metasploit Persistencia RAT

1: <https://github.com/youhacker55/PayGen>

--------------------------------------

Un robot de Telegram puede clonar medios de cualquier chat a su propio chat.

1: <https://github.com/m4mallu/clonebot>

--------------------------------------

DaProfiler es una herramienta OSINT que le permite recopilar cierta información sobre usted para rectificar mediante solicitudes de rgpd los rastros que haya dejado en la red. De hecho, DaProfiler puede recuperar: direcciones, cuentas de redes sociales, direcciones de correo electrónico, número de teléfono fijo/móvil, trabajos. Sobre un tema específico en un tiempo limitado. DaProfiler está diseñado…

1: <https://github.com/daprofiler/DaProfiler>

--------------------------------------

Script de omisión de firewall basado en registros de historial de DNS. Este script buscará registros de historial de DNS A y verificará si el servidor responde para ese dominio. Práctico para los cazadores de recompensas.

1: <https://github.com/vincentcox/bypass-firewalls-by-DNS-history>

--------------------------------------

Un dispositivo simple para atacar un sitio web o servidor (script de Python de Termux)

1: <https://github.com/pembriahmad/DDOS>

--------------------------------------

Thanos es un Http Flooder que necesitará un montón de solicitudes http-get a un servidor web

1: <https://github.com/loTus04/Thanos>

--------------------------------------

Raspe todos los medios de una cuenta de OnlyFans - Actualizado regularmente

1: <https://github.com/DIGITALCRIMINAL/OnlyFans>

--------------------------------------

Clonador de ID de Facebook, facebook-clone, Facebook-Id-Cracker, Facebook Password Cracker

1: <https://github.com/5l1v3r1/Azim0.6>

--------------------------------------

sonarbyte es un escáner de subdominio simple y rápido escrito en go para extraer el subdominio de la base de datos DNS de Rapid7 usando la API de omnisint.

1: <https://github.com/channyein1337/sonarbyte>

--------------------------------------

Azur3Alph4 es un módulo de PowerShell que automatiza las tareas del equipo rojo para operaciones en el objetivo. Este módulo se ubica en una posición posterior a la infracción (RCE logrado).

1: <https://github.com/hyd3sec/Azur3Alph4>

--------------------------------------

Big-Papa es un ladrón de cookies remoto que luego se puede usar para secuestrar sesiones y omitir la autenticación de 2 factores

1: <https://github.com/SxNade/Big-Papa>

--------------------------------------

Una herramienta para aumentar los privilegios en una red de directorio activo mediante la coerción de la autenticación de las cuentas de la máquina y la retransmisión al servicio de certificados.

1: <https://github.com/bats3c/ADCSPwn>

--------------------------------------

Buscar en la API del bot TrashPanda OSINT para verificar si su correo electrónico/dominio o contraseña se filtró o no

1: <https://github.com/rndinfosecguy/TrashSearch>

--------------------------------------

Servicio de vigilancia del registro de Internet

1: <https://github.com/SecurityRiskAdvisors/SHADOWSTAR>

--------------------------------------

menú de herramientas de piratería!

1: <https://github.com/mrprogrammer2938/20>

--------------------------------------

😎rxback - filtrador de back-end del sitio web l33t. Buscador de registros DNS, comparador Shodan

1: <https://github.com/5l1v3r1/rxback>

--------------------------------------

QUESTER es una herramienta Web Pentesting & Bug Bounty Recon que consulta URLs/Subdominios de la lista dada de URLs o subdominios.

1: <https://github.com/febinrev/quester>

--------------------------------------

Auditoría automatizada, métricas de rendimiento y mejores prácticas para la web.

1: <https://github.com/GoogleChrome/lighthouse>

--------------------------------------

Validación de mejores prácticas en sus clústeres de Kubernetes

1: <https://github.com/FairwindsOps/polaris>

--------------------------------------

SEO y auditoría de seguridad para sitios web. Rastreador de Lighthouse & Security Headers, Sitemap/Keywords/Images Extractor, Summarizer, etc...

1: <https://github.com/StanGirard/seo-audits-toolkit>

--------------------------------------

Optik es un conjunto de herramientas de ejecución simbólica que ayudan a los fuzzers de contratos inteligentes

1: <https://github.com/crytic/optik>

--------------------------------------

Sondee y descubra el nombre de la ruta HTTP utilizando la metodología de fuerza bruta y filtrado por palabra específica o 2 palabras a la vez

1: <https://github.com/xchopath/pathprober>

--------------------------------------

😎Extensión de Chrome para obtener el ID de correo electrónico de un usuario, incluso si no lo han hecho público en su perfil de GitHub

1: <https://github.com/prabhakar267/github-email-extractor>

--------------------------------------

Con esta herramienta, puede capturar todas las contraseñas WiFi almacenadas en una computadora con Windows y enviarlas por correo electrónico a su cuenta de correo electrónico.

1: <https://github.com/Vedant-Bhalgama/Dr0pFi>

--------------------------------------

Escáner de vulnerabilidades de contrabando de solicitudes Http

1: <https://github.com/Sh1Yo/request_smuggler>

--------------------------------------

Una herramienta simple para auditar su infraestructura de AWS en busca de errores de configuración o posibles problemas de seguridad.

1: <https://github.com/StanGirard/YATAS>

--------------------------------------

🕵️‍♂️Recopile un expediente sobre una persona por nombre de usuario de miles de sitios

1: <https://github.com/soxoj/maigret>

--------------------------------------

simulación baliza de ataque de cobalto paquete en linea. Paquete de conexión de baliza de ataque de cobalto de simulación.

1: <https://github.com/burpheart/CS_mock>

--------------------------------------

PortFU es un escáner de puertos ultrarrápido que puede escanear toda la gama de puertos 65535 en solo 50-55 segundos en un host de destino

1: <https://github.com/SxNade/PortFU>

--------------------------------------

SECMON es una herramienta basada en la web para la automatización de la vigilancia de la seguridad de la información y la gestión de vulnerabilidades con una interfaz web.

1: https://github.com/Guezone/SECMON

--------------------------------------

BlackNet - ¡Un completo buscador de cebollas en tu terminal!

1: <https://github.com/5l1v3r1/blacknet-3>

--------------------------------------

Herramienta de autenticación wifi

1: <https://github.com/CyberTitus/Wifi-Deauth-Tool>

--------------------------------------

MadSpam es una herramienta de Spammer que se utiliza para enviar spam. Esta herramienta es muy fácil de usar.

1: <https://github.com/mrmadbhai/MadSpam>

--------------------------------------

MadCam es una herramienta que puede capturar tomas de cámara de la cámara frontal del teléfono objetivo o de la cámara web de la PC con solo enviar un enlace.

1: https://github.com/mrmadbhai/MadCam

--------------------------------------

Rastree a los usuarios a través de la plataforma de redes sociales

1: <https://github.com/woj-ciech/SocialPath>

--------------------------------------

extraiga proxies de más de 5 fuentes diferentes y compruebe cuáles siguen vivos

1: <https://github.com/iw4p/proxy-scraper>

--------------------------------------

Encuentre vulnerabilidades en bases de datos locales y en línea al instante

1: <https://github.com/1N3/Findsploit>

--------------------------------------

Descubra la superficie de ataque y priorice los riesgos con nuestra plataforma continua de gestión de superficie de ataque (ASM): Sn1per Professional #pentest #redteam #bugbounty

1: <https://github.com/1N3/Sn1per>

--------------------------------------

Script pirateado para introducir direcciones URL en el mapa del sitio de Burp

1: <https://github.com/ZephrFish/BurpFeed>

--------------------------------------

Snoop es una herramienta de inteligencia basada en datos abiertos (mundo OSINT)

1: <https://github.com/snooppr/snoop>

--------------------------------------

API simple que puede usar para proteger su webhook de discordia para que no se elimine ni se envíe spam. Ratelimits solicitudes no autorizadas y acepta json, incrustaciones de discordia y archivos.

1: <https://github.com/429565000161264517609635766710319130884/Discord-Webhook-Protector>

--------------------------------------

AntiAnalysis (VirtualBox, SandBox, Debugger, VirusTotal, Any.Run) Obtenga información del sistema (versión, CPU, GPU, RAM, IP, BSSID, ubicación, métricas de pantalla, aplicaciones instaladas) Navegadores basados ​​en Chromium (contraseñas, tarjetas de crédito, cookies, historial , autorelleno, marcadores) Navegadores basados ​​en Firefox (archivos db, cookies, historial, marcadores) Internet explorer/Edge (contraseñas...

1: <https://github.com/tom3454/Discord-Stealer-College-Project>

--------------------------------------

Tor2web es un software proxy HTTP que permite el acceso a los servicios ocultos de Tor por medio de navegadores web comunes

1: <https://github.com/tor2web/Tor2web>

--------------------------------------

🕵️OSINT Herramientas para la recopilación de información y acciones forenses🕵️

1: <https://github.com/danieldurnea/FBI-tools>

--------------------------------------

Archivo DDOS de RootSec (Escáneres, BotNets (Mirai y QBot Premium & Normal y más), Exploits, Métodos, Sniffers)

1: <https://github.com/R00tS3c/DDOS-RootSec>

--------------------------------------

Repositorio oficial de herramientas de seguridad de Black Hat Arsenal

1: <https://github.com/toolswatch/blackhat-arsenal-tools>

--------------------------------------

Vulnerabilidad de inyección SQL autenticada en el complemento de Wordpress "NEX Forms"

1: <https://github.com/ehtec/nex-forms-exploit>

--------------------------------------

AGREGAR (Servicios de dominio de Active Directory)

1: <https://github.com/DavidGeeraerts/ADDS_Tool>

--------------------------------------

Una herramienta de descubrimiento de contenido rápida, simple y recursiva escrita en Rust.

1: <https://github.com/epi052/feroxbuster>

--------------------------------------

¡Un marco con módulos publicados como BlestSploit Framework, Exploits, Payloads, Posts y más!

1: <https://github.com/G00Dway/BlestSploit>

--------------------------------------

Durante la fase de explotación de una prueba de penetración o un compromiso de piratería ética, en última instancia, deberá intentar hacer que el código se ejecute en las computadoras del sistema de destino. Ya sea que se logre mediante correos electrónicos de phishing, entregando una carga útil a través de un exploit o ingeniería social, la ejecución de código en las computadoras de destino es parte de la mayoría de las pruebas de penetración. Eso significa que tu…

1: <https://github.com/RoseSecurity/Anti-Virus-Evading-Payloads>

--------------------------------------

VECTR es una herramienta que facilita el seguimiento de las actividades de prueba de su equipo rojo y azul para medir las capacidades de detección y prevención en diferentes escenarios de ataque.

1: <https://github.com/SecurityRiskAdvisors/VECTR>

--------------------------------------

Mapeo detallado de la superficie de ataque y descubrimiento de activos

1: <https://github.com/OWASP/Amass>

--------------------------------------

¡Un método sobre cómo hacer un registrador de imágenes de un clic!

1: <https://github.com/FLUORESCENTXX/One-Click-Image-Logger>

--------------------------------------

EvilPIP👿Módulo malicioso con Discord Logger y Socket Reverse Shell

1: <https://github.com/codeuk/EvilPIP>

--------------------------------------

Herramienta de búsqueda de violación de contraseña y OSINT de correo electrónico, localmente o usando servicios premium. Admite la búsqueda de correo electrónico relacionado

1: <https://github.com/khast3x/h8mail>

--------------------------------------

Generador de pines WPS escrito en Python 3

1: <https://github.com/drygdryg/wpspin>

--------------------------------------

Muestra y controla tu dispositivo Android

1: <https://github.com/Genymobile/scrcpy>

--------------------------------------

Gnirehtet proporciona tethering inverso para Android

1: <https://github.com/Genymobile/gnirehtet>

--------------------------------------

W3b0s1nt (WebOSINT) es una herramienta/secuencia de comandos de Python para la recopilación pasiva de inteligencia de dominio.

1: <https://github.com/C3n7ral051nt4g3ncy/webosint>

--------------------------------------

Su compañero de MitM para la retransmisión de ataques con adquisición de DNS de DHCPv6, así como suplantación de identidad de mDNS, LLMNR y NetBIOS-NS.

1: <https://github.com/RedTeamPentesting/pretender>

--------------------------------------

Endurecimiento de dispositivos móviles Android

1: <https://github.com/A-YATTA/AMDH>

--------------------------------------

🛡️⚔️¡Proteja su aplicación web del ataque DDOS o Dead Ping + VERIFICACIÓN DE CAPTCHA en una línea!

1: https://github.com/Sanix-Darker/AntiDDOS-system

--------------------------------------

🔒Shutdown 2017 Malware (Worm – Ransomware – Rogue Security Software) – Incluye AHXR-ScreenLock (Creador de bloqueo de pantalla – Elimina el Administrador de tareas + Bloquea la computadora + Adjunta ejecutable)

1: <https://github.com/AHXR/Trojan.Win32.Lockdown>

--------------------------------------

Automatización OSINT para hackers.

1: <https://github.com/blacklanternsecurity/bbot>

--------------------------------------

¡TREVORspray es un rociador de contraseñas modular con subprocesos, proxy inteligente, módulos de botín y más!

1 <https://github.com/blacklanternsecurity/TREVORspray>

--------------------------------------

Un proxy SOCKS escrito en Python que aleatoriza su dirección IP de origen. ¡Rodee sus paquetes malignos a través de túneles SSH o déles miles de millones de direcciones de origen únicas!

1: <https://github.com/blacklanternsecurity/TREVORproxy>

--------------------------------------

BLURtooth: Explotación de la derivación de clave de transporte cruzado en Bluetooth Classic y Bluetooth Low Energy [CVE-2020-15802] [CVE-2022-20361]

1: <https://github.com/francozappa/blur>

--------------------------------------

Ataques de suplantación de identidad por Bluetooth (BIAS) [CVE 2020-10135]

1: <https://github.com/francozappa/bias>

--------------------------------------

SECMON es una herramienta basada en la web para la automatización de la vigilancia de la seguridad de la información y la gestión de vulnerabilidades con una interfaz web.

1: <https://github.com/Guezone/SECMON>

--------------------------------------

Tiuku es una herramienta para escanear varios tipos de sistemas y entornos en busca de información relacionada con la seguridad y mostrar los resultados en una interfaz de usuario basada en navegador.

1: <https://github.com/ncsc-fi/tiuku>

--------------------------------------

🖖Escáner de red rápido, moderno y fácil de usar

1: <https://github.com/v-byte-cpu/sx>

--------------------------------------

domhttpx es un motor de búsqueda de Google con un kit de herramientas HTTP creado con python, puede facilitarle la búsqueda de muchas URL/IP a la vez con rapidez.

1: <https://github.com/naufalardhani/domhttpx>

--------------------------------------

Una herramienta fácil para restablecer la contraseña de cpanel cuando no puede cargar la puerta trasera al servidor. Esta herramienta será útil solo si la función de restablecimiento de contraseña en cpanel está activada.

1: <https://github.com/naufalardhani/cpanel-pass-reset>

--------------------------------------

El kit de herramientas de penetración WiFi

1: <https://github.com/MA24th/WiFiHunter>

--------------------------------------

CamOver es una herramienta de explotación de cámara que permite revelar la contraseña de administrador de la cámara de red.

1: <https://github.com/EntySec/CamOver>

--------------------------------------

Manipulación de verbos HTTP y enumeración de métodos

1: <https://github.com/ShutdownRepo/httpmethods>

--------------------------------------

Generador de billetera Bitcoin automatizado que con mnemónicos y frases de contraseña direcciones de billetera de fuerza bruta

1: <https://github.com/adrijano/Bitcoin-wallet-cracker>

--------------------------------------

Archivo DDOS (Escáneres, BotNets (Mirai y QBot Premium & Normal y más), Exploits, Métodos, Sniffers)

1: <https://github.com/1ucif3r/DDOS-th31ucif3r>

--------------------------------------

XMap es un escáner de red rápido diseñado para realizar escaneos de investigación de redes IPv6 e IPv4 en toda Internet.

1: <https://github.com/idealeer/xmap>

--------------------------------------

Exfiltrador de datos DNS simple y personalizable

1: <https://github.com/JoelGMSec/Invoke-DNSteal>

--------------------------------------

TinyCheck le permite capturar fácilmente las comunicaciones de la red desde un teléfono inteligente o cualquier dispositivo que pueda asociarse a un punto de acceso Wi-Fi para analizarlas rápidamente. Esto se puede usar para verificar si alguna comunicación sospechosa o maliciosa está saliendo desde un teléfono inteligente, mediante el uso de heurísticas o indicadores de compromiso (IoC) específicos. en orden…

1: <https://github.com/KasperskyLab/TinyCheck>

--------------------------------------

¡Convierta su teléfono Android en cualquier dispositivo USB que desee! USB Gadget Tool le permite crear y activar roles de dispositivos USB, como un mouse o un teclado.🛠🛡📱

1: <https://github.com/tejado/android-usb-gadget>

--------------------------------------

Ejecución del código del kernel de Windows x64 a través del modo de usuario, llamada al sistema arbitraria, demostración de IOCTL vulnerables

1: <https://github.com/kkent030315/anycall>

--------------------------------------

Verificador de ADN

1: <https://github.com/Its-Vichy/Open-ADN>

--------------------------------------

🔐Generador de contraseñas múltiples: caracteres únicos, secuencias únicas, números, mayúsculas, minúsculas, símbolos, generador múltiple

1: <https://github.com/AHXR/eyepassgen>

--------------------------------------

-----à RAFELß---- Android Rat escrito en Java con WebPanel para controlar a las víctimas… Hackear dispositivos Android

1: <https://github.com/swagkarna/Rafel-Rat>

--------------------------------------

TechNowHorse es un generador RAT (troyano de administrador remoto) para sistemas Windows/Linux escrito en Python 3.

1: <https://github.com/PushpenderIndia/technowhorse>

--------------------------------------

Detección de intrusiones HTTP en tiempo real

1: <https://github.com/kitabisa/teler>

--------------------------------------

DNSTake: una herramienta rápida para comprobar las zonas DNS alojadas que faltan y que pueden llevar a la adquisición de subdominios

1: <https://github.com/pwnesia/dnstake>

--------------------------------------

Una herramienta de python fácil de usar para realizar dns recon

1: <https://github.com/D3Ext/SDomDiscover>

--------------------------------------

Herramienta Python Pentester: agregue/cree complementos fácilmente, disponible en la herramienta y el módulo de línea de comandos.

1: <https://github.com/HarryLudemann/Ngoto>

--------------------------------------

Herramienta de evasión antivirus para ejecutables .NET/Native (x64)

1: <https://github.com/ch2sh/Crybat>

--------------------------------------

Robe el token de Discord directamente de la memoria y omita cualquier tipo de protección de token

1: <https://github.com/ZeroMemoryEx/DeadLight>

--------------------------------------

Rustcat (rcat): el escucha de puerto moderno y el shell inverso

1: <https://github.com/robiot/rustcat>

--------------------------------------

Russia Wipers Dropper (REvil Ransomware incluido) (fines educativos)

1: <https://github.com/ZeroMemoryEx/U-Boat>

--------------------------------------

Omitir Malware Sandbox Evasion Ram check

1: <https://github.com/ZeroMemoryEx/Bypass-Sandbox-Evasion>

--------------------------------------

El sistema de faro de reconocimiento de activos ARL (Asset Reconnaissance Lighthouse) está diseñado para detectar rápidamente activos de Internet asociados con objetivos y crear una base de datos básica de información de activos. Ayude al equipo de seguridad o al probador de penetración de la Parte A a realizar un reconocimiento y recuperación efectivos de los activos, y descubra los puntos débiles existentes y las superficies de ataque.

1: <https://github.com/TophantTechnology/ARL>

--------------------------------------

Script de shell simple para reconocimiento de dominio automatizado con algunas herramientas

1: <https://github.com/JoshuaMart/AutoRecon>

--------------------------------------

Decodificar todas las bases - Decodificador de esquema base

1: <https://github.com/mufeedvh/basecrack>

--------------------------------------

MagicRecon es un poderoso shell script para maximizar el proceso de reconocimiento y recolección de datos de un objetivo y encontrar vulnerabilidades comunes, todo esto guardando los resultados obtenidos de forma organizada en directorios y con varios formatos.

1: <https://github.com/robotshell/magicRecon>

--------------------------------------

⡷⠂𝚔𝚊𝚛𝚖𝚊 𝚟𝟸⠐⢾ es un Reconocimiento Automatizado de Inteligencia Pasiva de Código Abierto (OSINT) (marco)

1: <https://github.com/Dheerajmadhukar/karma_v2>

--------------------------------------

Armas de hackers móviles / Una colección de herramientas geniales utilizadas por hackers móviles. Feliz piratería, feliz caza de errores

1: <https://github.com/hahwul/MobileHackersWeapons>

--------------------------------------

Un escáner de host virtual que realiza búsquedas inversas, se puede usar con herramientas pivote, detecta escenarios generales, soluciona comodines, alias y páginas predeterminadas dinámicas.

1: <https://github.com/codingo>

--------------------------------------

una herramienta de reconocimiento que permite buscar URL que están expuestas a través de servicios más cortos

1: <https://github.com/utkusen/urlhunter>

--------------------------------------

Escaneo de archivos APK para URI, puntos finales y secretos.

1: <https://github.com/dwisiswant0/apkleaks>

--------------------------------------

Sudomy es una herramienta de enumeración de subdominios para recopilar subdominios y analizar dominios que realizan reconocimiento automatizado (recon) para la búsqueda de errores/pentesting

1: <https://github.com/screetsec/Sudomy>

--------------------------------------

Burp Bounty (cheque de escaneo constructor en BApp Store) es una extensión de Burp Suite que permite, de forma rápida y sencilla, mejorar el escáner activo y pasivo mediante reglas personalizadas a través de una interfaz gráfica muy intuitiva.

1: <https://github.com/wagiro/BurpBounty>

--------------------------------------

gitGraber: monitoriza GitHub para buscar y encontrar datos sensibles en tiempo real para diferentes servicios online como: Google, Amazon, Paypal, Github, Mailgun, Facebook, Twitter, Heroku, Stripe...

1: <https://github.com/hisxo/gitGraber>

--------------------------------------

POC para replicar la vulnerabilidad completa RCE de Office 'Follina' con fines de prueba (infectar word para hackear ordenador pd: también se puede hacer con evil word evil PDF evilexcel y etc esta vulnerabilidad lleva existiendo desde hace mucho tiempo atrás desde como una actualización de word o desde inicios de word)

1: <https://github.com/chvancooten/follina.py>

--------------------------------------

pagodo (Pasivo Google Dork) - Automatice el raspado y la búsqueda de la base de datos de Google Hacking

1: <https://github.com/opsdisk/pagodo>

--------------------------------------

una herramienta de reconocimiento que encuentra datos confidenciales dentro de las capturas de pantalla cargadas en prnt.sc

1: <https://github.com/utkusen/shotlooter>

--------------------------------------

rastrea el sitio web y encuentra enlaces de redes sociales rotos que pueden ser secuestrados

1: <https://github.com/utkusen/socialhunter>

--------------------------------------

Herramientas para la caza de errores

1: <https://github.com/thehackingsage/bughunter>

--------------------------------------

Un marco Ruby diseñado para ayudar en las pruebas de penetración de los sistemas WordPress.

1: <https://github.com/rastating/wordpress-exploit-framework>

--------------------------------------

KratosKnife es una BOTNET avanzada escrita en Python 3 para el sistema operativo Windows. Viene con muchas funciones avanzadas, como métodos de detección de VM y persistencia, carpeta integrada, etc.

1: <https://github.com/PushpenderIndia/KratosKnife>

--------------------------------------

Web analizador

1: <https://github.com/lukejharmon/netphy/>

--------------------------------------

🧛🐲

1: <https://github.com/cr-0w/drakali>

--------------------------------------

🚩🐺¡Generador de shell para CTF!

1: https://github.com/cr-0w/inumaki

--------------------------------------

🙀Icon Changer, File Pumper y Extension Spoofer: modifique rápidamente los archivos ejecutables

1: <https://github.com/AHXR/maskedkitty>

--------------------------------------

👽Programa para el control remoto de computadoras con Windows a través del bot de Telegram. Escrito en C#

1: <https://github.com/LimerBoy/ToxicEye>

--------------------------------------

RAT-el es una herramienta de prueba de penetración de código abierto que le permite tomar el control de una máquina con Windows. Funciona en el modelo cliente-servidor, el servidor envía comandos y el cliente ejecuta los comandos y envía el resultado al servidor. El cliente es completamente indetectable por el software antivirus.

1: <https://github.com/FrenchCisco/RATel>

--------------------------------------

“Socialx” es una herramienta troyana de ingeniería social y acceso remoto. Puede generar fud backdoor e incrustar cualquier archivo que desee dentro del archivo exe.

1: <https://github.com/AzizKpln/Social_X>

--------------------------------------

Esta herramienta brinda información sobre el número de teléfono que ingresó.

1: <https://github.com/AzizKpln/Moriarty-Project>

--------------------------------------

DKMC - No mates a mi gato - Herramienta maliciosa de evasión de carga útil

1: https://github.com/Mr-Un1k0d3r/DKMC

--------------------------------------

NekRos es un ransomeware de código abierto, con características avanzadas, que se parece a Wannacry y tiene un servidor C&C que se puede usar para recuperar la CLAVE

1: <https://github.com/PushpenderIndia/nekros>

--------------------------------------

chat web a través de WebSockets/WebRTC que permite enviar mensajes/videollamadas/compartir pantalla

1: <https://github.com/akoidan/pychat>

--------------------------------------

APOLOGEE es un script de Python y un módulo de Metasploit que enumera un directorio oculto en los controladores de automatización Siemens APOGEE PXC BACnet (todas las versiones anteriores a la V3.5) y los controladores de automatización TALON TC BACnet (todas las versiones anteriores a la V3.5). Con un CVSS 7.5, este exploit permite que un atacante realice una omisión de autenticación utilizando una alternativa...

1: <https://github.com/RoseSecurity/APOLOGEE>

--------------------------------------

Descifrar la clave privada de Ethereum y la dirección generada desde el hexadecimal y verificar la dirección de datos enriquecidos [Rápido]

1: <https://github.com/Pymmdrza/EthKeyClear>

--------------------------------------

Atacar y descifrar la clave privada AIO (TODO en UNO) Todas las criptomonedas de las palabras [HACK]

1: <https://github.com/Pymmdrza/AttackAIO_Crypto>

--------------------------------------

Búsqueda de todos los tipos de direcciones de Bitcoin con base de datos verificada de alta velocidad

1: <https://github.com/Pymmdrza/BitcoinXPowerHunter>

--------------------------------------

Una aplicación especial de DOS para detener sitios web de agresión prorrusos. ¡Apoye a Ucrania!

1: <https://github.com/erkexzcx/stoppropaganda>

--------------------------------------

✨Spark es una herramienta de administración remota (RAT) basada en la web, multiplataforma y con todas las funciones escrita en Go que le permite controlar todos sus dispositivos en cualquier lugar. Chispa

1: <https://github.com/XZB-1248/Spark>

--------------------------------------

Kit de herramientas del equipo rojo: una lista seleccionada de herramientas que se usan comúnmente en el campo para la seguridad física, el equipo rojo y la entrada táctica encubierta.

1: <https://github.com/DavidProbinsky/RedTeam-Physical-Tools>

--------------------------------------

PROTOCOLO SIMPLE DE TRANSFERENCIA DE CORREO (SMTP) CHECKER V3

1: <https://github.com/0xSojalSec/-Smtp-cracker-v3>

--------------------------------------

Herramienta de administración remota de Saqwel permite administrar computadoras Windows remotas a través de una red.

1: <https://github.com/saqwel/srat>

--------------------------------------

Cliente DNS sobre HTTPS / DNS sobre Tor / DNSCrypt, firewall y rastreador de conexión para Android.

1: <https://github.com/celzero/rethink-app>

--------------------------------------

Hackear cámaras de circuito cerrado de televisión (esto sirve parpara hackear cámaras de television aunque buscaré algo mejor que esto estad atentos al word y a mis redes sociales para saber si encontré algo sobre esto)

1: <https://github.com/yan4ikyt/webhack>

--------------------------------------

Shell inverso de forma anónima a través de la red Tor utilizando servicios ocultos sin reenvío de puertos.

1: <https://github.com/samet-g/tornado>

--------------------------------------

Herramienta de implementación automatizada del entorno del equipo rojo/azul | Herramienta de implementación de automatización del entorno del equipo rojo/azul

1: <https://github.com/ffffffff0x/f8x>

--------------------------------------

Otra herramienta más para la clonación de cuentas de Facebook.

1: <https://github.com/mkdirlove/fact.py>

--------------------------------------

Protección de la información y recursos OSINT | OSINT (OSINT)

1: <https://github.com/ffffffff0x/Digital-Privacy>

--------------------------------------

Una herramienta de monitoreo de Android solo para no rooteados (Termux)

1: <https://github.com/Hackerscolonyofficial/HCORat>

--------------------------------------

Raspados: [HTTP, HTTPS, SOCKS4 y SOCKS5] || "Omite" y raspa los proxies pagados

1: <https://github.com/WTSTiNy/DeCryPt_ProxyScraper_v1>

--------------------------------------

Automatice el bot seguidor de TikTok, como bot, comparta bot, vea bot y más usando selenio (zefoy.com es una página de seguidores en tiktok este repositorio lo hace automatizado aunque no se si es real o no por que la página tiene un captcha así que si queréis probarlo aquí osea lo dejo)

1: <https://github.com/useragents/Zefoy-TikTok-Automator>

--------------------------------------

Herramienta para descubrir el host de origen detrás de un proxy inverso. ¡Útil para evitar los WAF en la nube!

1: <https://github.com/hakluke/hakoriginfinder>

--------------------------------------

Google se vuelve loco para obtener fácilmente algunos tokens de bots de Discord

1: <https://github.com/Traumatism/get-discord-bots-tokens-with-google>

--------------------------------------

Un ofuscador de Python que utiliza solicitudes HTTP y Hastebin.

1: <https://github.com/billythegoat356/Jawbreaker>

--------------------------------------

detectar el capturador/ladrón de fichas de discordia

1: <https://github.com/Traumatism/Discord-Malware-Detector>

--------------------------------------

Un marco semiautomático osint/recon.

1: <https://github.com/Traumatism/Smog>

--------------------------------------

Un capturador de tokens de Discord escrito en Python3, con una increíble ofuscación y protección anti-depuración.

1: <https://github.com/billythegoat356/Plague>

--------------------------------------

Root: acceda a los privilegios de root en termux sin rootear el dispositivo Android

1: <https://github.com/adarshaddee/root>

--------------------------------------

Una herramienta automatizada que puede rastrear, llenar formularios, activar páginas de error/depuración y "saquear" secretos del código de sitios orientado al cliente simultáneamente.

1: <https://github.com/redhuntlabs/HTTPLoot>

--------------------------------------

pagodo (Passive Google Dork) - Automatice el raspado y la búsqueda de la base de datos de Google Hacking

1: <https://github.com/opsdisk/pagodo>

--------------------------------------

Stunner es una herramienta para probar y explotar STUN, TURN y TURN sobre servidores TCP.

1: <https://github.com/firefart/stunner>

--------------------------------------

DNSTake: una herramienta rápida para comprobar las zonas DNS alojadas que faltan y que pueden llevar a la adquisición de subdominios

1: <https://github.com/pwnesia/dnstake>

--------------------------------------

Esta secuencia de comandos de Python se puede usar para eludir las restricciones de origen de IP mediante encabezados HTTP.

1: <https://github.com/p0dalirius/ipsourcebypass>

--------------------------------------

Shell inverso de forma anónima a través de la red Tor utilizando servicios ocultos sin reenvío de puertos.

1: <https://github.com/samet-g/tornado>

--------------------------------------

Automatización externa avanzada en programas de recompensas por errores al ejecutar el mejor conjunto de herramientas para realizar escaneos y descubrir vulnerabilidades.

1: <https://github.com/samet-g/bugradar>

--------------------------------------

Una herramienta de automatización que escanea subdominios, toma de control de subdominios, luego filtra XSS, SSTI, SSRF y más parámetros de punto de inyección y escanea automáticamente en busca de algunas vulnerabilidades bajas.

1: <https://github.com/R0X4R/Garud>

--------------------------------------

G3nius-Tools Sploit es una herramienta de explotación de servidor, cliente, red y señal poderosamente fácil de usar. Tenemos soporte en línea y actualizaciones.

1: <https://github.com/witblack/G3nius-Tools-Sploit>

--------------------------------------

ShoLister es una herramienta que recopila todos los subdominios disponibles para nombres de host específicos u organizaciones de Shodan. La herramienta está diseñada para ser utilizada por Penetration Tester y Bug Bounty Hunters.

1: <https://github.com/eslam3kl/ShoLister>

--------------------------------------

Script Pyhton para eludir las respuestas HTTP 40X. Funciones: manipulación de verbos, encabezados, #bugbountytips, agentes de usuario, extensiones, credenciales predeterminadas y fuzzing.

1: <https://github.com/lobuhi/byp4xx>

--------------------------------------

Una forma un poco menos hacker de interceptar y modificar protocolos que no son HTTP a través de Burp y otros.

1: <https://github.com/cyberark/MITM_Intercept>

--------------------------------------

📝urlRecon - Herramienta de recopilación o reconocimiento de información para URL -> Recupera \* Información Whois del dominio \* Detalles DNS del dominio \* Huella digital del servidor \* Geolocalización IP del servidor

1: <https://github.com/Srinivas11789/urlRecon>

--------------------------------------

❄️PcapXray: una herramienta forense de red: para visualizar una captura de paquetes fuera de línea como un diagrama de red que incluye la identificación del dispositivo, resalta la comunicación importante y la extracción de archivos

1: <https://github.com/Srinivas11789/PcapXray>

--------------------------------------

Una biblioteca de Python para utilizar el gran grupo de direcciones IP de AWS API Gateway como un proxy para generar direcciones IP pseudo-infinitas para web scraping y fuerza bruta.

1: <https://github.com/Ge0rg3/requests-ip-rotator>

--------------------------------------

Encontrar XSS durante el reconocimiento

1: <https://github.com/ferreiraklet/airixss>

--------------------------------------

Verificar si existe el correo electrónico

1: <https://github.com/4w4k3/KnockMail>

--------------------------------------

Obtenga rápidamente su contraseña de WiFi y, si es necesario, genere un código QR de su WiFi para permitir que los teléfonos se conecten fácilmente

1: <https://github.com/sdushantha/wifi-password>

--------------------------------------

Smuggler: una herramienta de prueba de desincronización/contrabando de solicitudes HTTP escrita en Python 3

1: <https://github.com/defparam/smuggler>

--------------------------------------

CloudScraper: Herramienta para enumerar objetivos en busca de recursos en la nube. S3 Buckets, Azure Blobs, Digital Ocean Storage Space.

1: <https://github.com/jordanpotti/CloudScraper>

--------------------------------------

Una vulnerabilidad de omisión de autenticación de dos factores (2FA) en "Simple 2FA Plugin for Moodle" de LMS Doctor

1: <https://github.com/FlaviuPopescu/CVE-2022-28601>

--------------------------------------

Script rápido y de subprocesos múltiples para reclamar automáticamente el nombre de usuario objetivo, incluida la omisión de 14 días

1: <https://github.com/useragents/Instagram-Username-Auto-Claimer>

--------------------------------------

Herramienta de búsqueda de rangos de direcciones IP en la nube + enumeración de subdominios DNS + Transparencia de certificados

1: <https://github.com/iknowjason/edge>

--------------------------------------

Una herramienta avanzada para escanear cientos de IP en segundos para CVE, puertos abiertos y tecnologías web.

1: <https://github.com/machine1337/fast-scan>

--------------------------------------

Hackfruit es una herramienta de búsqueda fácil que encuentra herramientas de piratería, comandos y hojas de trucos. Ayuda al aprendizaje y la capacitación en ciberseguridad, CTF, recompensas por errores, piratería ética.

1: <https://github.com/hideckies/hackfruit>

--------------------------------------

Navaja suiza Herramienta proxy para captura, manipulación y reproducción de tráfico HTTP/HTTPS sobre la marcha.

1: <https://github.com/projectdiscovery/proxify>

--------------------------------------

Onex es un administrador de paquetes para piratas informáticos. Onex administra más de 400 herramientas de piratería que se pueden instalar con un solo clic.

1: <https://github.com/rajkumardusad/onex>

--------------------------------------

Una forma un poco menos hacker de interceptar y modificar protocolos que no son HTTP a través de Burp y otros.

1: <https://github.com/cyberark/MITM_Intercept>

--------------------------------------

Herramienta de ingeniería social para múltiples propósitos, como localizar la ubicación del objetivo, acceder a la cámara web, capturar contraseñas del sistema operativo...

1: <https://github.com/IHosseini083/SuperLink>

--------------------------------------

Hoja de referencia de ataques web

1: <https://github.com/riramar/Web-Attack-Cheat-Sheet>

--------------------------------------

Un potente generador de capas inversas

1: <https://github.com/FlyfishSec/rcX>

--------------------------------------

DarkTor es un script de anonimización que redirige todo el tráfico de Internet a través del proxy tor SOCKS5.

1: <https://github.com/D4RK-4RMY/DarkTor>

--------------------------------------

DARKARMY Hacking Tools Pack: un marco de prueba de penetración.

1: <https://github.com/D4RK-4RMY/DARKARMY>

--------------------------------------

La herramienta DDWPasteRecon lo ayudará a identificar fugas de código, archivos confidenciales, contraseñas de texto sin formato, hash de contraseñas. También permite que los miembros de SOC y Blue Team obtengan conocimiento de la situación de la exposición web de la organización en los sitios de pegado. Utiliza la indexación de sitios web de Google para obtener inteligencia específica de la organización. Los equipos azul y SOC pueden...

1: <https://github.com/Viralmaniar/DDWPasteRecon>

--------------------------------------

Monitor de red sin root, firewall y dumper PCAP para Android

1: <https://github.com/emanuele-f/PCAPdroid>

--------------------------------------

sshDump es la carga útil de BashBunny que aprovecha las claves privadas ssh sin cifrar almacenadas en el directorio de inicio y las saquea.

1: <https://github.com/drapl0n/sshDump>

--------------------------------------

Vernet - Analizador de red y herramienta de monitoreo

1: <https://github.com/git-elliot/vernet>

--------------------------------------

💳Comprobador de tarjetas de crédito (CC Checker) y Mass SK Checker & Generator💳

1: <https://github.com/rimurx/DemonLordV2>

--------------------------------------

Esta secuencia de comandos de Python se puede usar para eludir las restricciones de origen de IP mediante encabezados HTTP.

1: <https://github.com/p0dalirius/ipsourcebypass>

--------------------------------------

Kit de herramientas de ataques de VLAN

1: <https://github.com/in9uz/VLANPWN>

--------------------------------------

Una herramienta OSINT para obtener el número de teléfono de un objetivo con solo tener su dirección de correo electrónico

1: <https://github.com/martinvigo/email2phonenumber>

--------------------------------------

Puerta trasera oxidada+spyware💣 🚪

1: <https://github.com/talbor49/spyware>

--------------------------------------

Herramienta de reconocimiento de automatización que funciona con alcances grandes y medianos. Realiza más de 20 tareas y recupera todos los resultados en archivos separados.

1: <https://github.com/eslam3kl/3klcon>

--------------------------------------

FreeRADIUS: un servidor de políticas multiprotocolo.

1: <https://github.com/FreeRADIUS/freeradius-server>

--------------------------------------

Interfaces web modulares rápidas Bruteforcer

1: <https://github.com/koutto/web-brutator>

--------------------------------------

Jok3r v3 BETA 2 - Marco de automatización de red y Web Pentest

1: https://github.com/koutto/jok3r

--------------------------------------

Una aplicación gratuita, segura y de código abierto para Android para administrar sus tokens de verificación en dos pasos.

1: <https://github.com/beemdevelopment/Aegis>

--------------------------------------

🔑 One Time Password (OTP) / 2FA for Node.js and Browser – Supports HOTP, TOTP and Google Authenticator

1: <https://github.com/yeojz/otplib>

--------------------------------------

Marco de recopilación de información

1: <https://github.com/gotr00t0day/IGF>

--------------------------------------

La clásica biblioteca de envío de correo electrónico para PHP

1: <https://github.com/PHPMailer/PHPMailer>

--------------------------------------

Administrador de dependencias para PHP

1: https://github.com/composer/composer

--------------------------------------

Una navaja suiza para pentesting de redes.

1: https://github.com/byt3bl33d3r/CrackMapExec

--------------------------------------

Un paquete de aleteo que lo ayudará a generar campos de código PIN con hermosos diseños y animaciones. Puede ser útil para entradas de código PIN o OTP🤓🤓

1: https://github.com/adar2378/pin\_code\_fields

--------------------------------------

🔐Una biblioteca PHP para generar contraseñas de un solo uso según RFC 4226 (HOTP) y RFC 6238 (TOTP)

1: https://github.com/Spomky-Labs/otphp

--------------------------------------

(Windows/Linux/Mac) Herramienta de administración remota

1: <https://github.com/muneebwanee/WinRAT>

--------------------------------------

OSS-Fuzz: fuzzing continuo para software de código abierto.

1: <https://github.com/google/oss-fuzz>

--------------------------------------

Proyecto de muestra para demostrar scrapy con python-telegram-bot

1: https://github.com/v1k45/scrapygram

--------------------------------------

GG Dorking es una herramienta para generar GitHub y Google dorking para pentesters y cazarrecompensas de errores.

1: <https://github.com/eslam3kl/GG-Dorking>

--------------------------------------

Bot de Telegram que usa python scrapy para encontrar los mejores hilos de reddit

1: <https://github.com/tiagoReichert/reddit-crawler>

--------------------------------------

Herramienta de recuperación de contraseña para sistemas operativos de Microsoft. Permite una fácil recuperación de varios tipos de contraseñas olfateando la red, descifrando contraseñas encriptadas usando ataques de diccionario, fuerza bruta y criptoanálisis, grabando conversaciones de VoIP, decodificando contraseñas codificadas, recuperando claves de redes inalámbricas, revelando casillas de contraseñas, descubriendo...

1: <https://github.com/xchwarze/Cain>

--------------------------------------

penSIPS es una implementación GPL de un servidor SIP multifuncional que tiene como objetivo ofrecer una solución técnica de alto nivel (rendimiento, seguridad y calidad) para ser utilizada en plataformas de servidores SIP profesionales.

1: <https://github.com/OpenSIPS/opensips>

--------------------------------------

Aimbot + Esp + Spoofer / C++

1: <https://github.com/SarnaxLii/Valorant-External>

--------------------------------------

Esto cambiará el S/N y el ID de hardware.

1: <https://github.com/SarnaxLii/HWID-Spoofer>

--------------------------------------

Suplantador de Valorant 2021 – 2022

1: <https://github.com/SarnaxLii/Valorant-Spoofer>

--------------------------------------

Omisión de ScriptHook para Fivem/omisión de ID de hardware solo para nvdia

1: <https://github.com/SarnaxLii/Fivem-Clean>

--------------------------------------

Una sencilla utilidad de auditoría para macOS

1: <https://github.com/santoru/filewatcher>

--------------------------------------

Una herramienta básica para comprobar los encabezados de seguridad de un sitio web

1: <https://github.com/santoru/shcheck>

--------------------------------------

El proxy inverso faltante para ssh scp

1: <https://github.com/tg123/sshpiper>

--------------------------------------

Permite a los usuarios de WhatsApp extraer su clave de cifrado y bases de datos en dispositivos Android no rooteados.

1: https://github.com/EliteAndroidApps/WhatsApp-Key-DB-Extractor

--------------------------------------

Una secuencia de comandos de Python que recopila todas las direcciones IP válidas de todos los archivos de texto de un directorio y las compara con la base de datos Whois, los relés TOR y la ubicación

1: <https://github.com/ciprianster/osips>

--------------------------------------

Ingeniería inversa y pentesting para aplicaciones Android

1: <https://github.com/androguard/androguard>

--------------------------------------

Araña de raspado web de Instagram construida con Python Scrapy

1: <https://github.com/ian-kerins/instagram-python-scrapy-spider>

--------------------------------------

Python Scrapy spider que extrae todos los productos de Amazon de una búsqueda de palabras clave

1: <https://github.com/ian-kerins/amazon-python-scrapy-scraper>

--------------------------------------

Raspa las fotos y videos de un usuario de instagram

1: <https://github.com/arc298/instagram-scraper>

--------------------------------------

Raspa medios, me gusta, seguidores, etiquetas y todos los metadatos. Inspirado en instagram-php-scraper,bot

1: <https://github.com/realsirjoe/instagram-scraper>

--------------------------------------

Bug bounty extrae todos los datos del subdominio, herramientas de piratas informáticos

1: <https://github.com/jonathandata1/cyfon>

--------------------------------------

Sistema de gestión de flujo de trabajo Pegasus: automatice, recupere y depure cálculos científicos.

1: <https://github.com/pegasus-isi/pegasus>

--------------------------------------

Scrapy spider para página de facebook

1: <https://github.com/opplieam/Facebook_page_crawler>

--------------------------------------

Mira un ojo en su sistema. Una alternativa top/htop para sistemas operativos GNU/Linux, BSD, Mac OS y Windows.

1: https://github.com/nicolargo/glances

--------------------------------------

Pegasus\_spyware descompilado

1: <https://github.com/jonathandata1/pegasus_spyware>

--------------------------------------

Rastreador web paralelo (Python)

1: <https://github.com/opplieam/Oppomus>

--------------------------------------

Un protocolo descentralizado de préstamos y participación construido sobre el ecosistema de Polkadot.

1: <https://github.com/parallel-finance/parallel>

--------------------------------------

Ruby: procesamiento paralelo simplificado y rápido

1: https://github.com/grosser/parallel

--------------------------------------

Cable BadUSB basado en microcontrolador Attiny85 con línea de datos habilitada.

1: https://github.com/joelsernamoreno/EvilCrow-Cable

--------------------------------------

Explorer es una herramienta muy útil que te ayudará en la fase de reconocimiento en la búsqueda de Bug Bounty o Web Pentesting. Puede realizar muchas cosas individualmente o todos juntos.

1: <https://github.com/eslam3kl/Explorer>

--------------------------------------

GRIM ES UNA HERRAMIENTA DE RECOGIDA DE INFORMACIÓN Y PROBADOR DE VULNERABILIDAD, PUEDE UTILIZARLA EN CUALQUIER SITIO WEB PARA OBTENER SU INFORMACIÓN

1: <https://github.com/nandydark/grim>

--------------------------------------

Scrapy, un marco rápido de raspado y rastreo web de alto nivel para Python.

1: https://github.com/scrapy/scrapy

--------------------------------------

Obtén los enlaces de descarga, ya sea de un único archivo o una carpeta entera.

1: <https://github.com/DtxdF/mediafire2links>

--------------------------------------

Shell reversa usando el protocolo sdc

1: <https://github.com/DtxdF/reverse-shell-sdc>

--------------------------------------

Parsel le permite extraer datos de documentos XML/HTML usando selectores XPath o CSS

1: <https://github.com/scrapy/parsel>

--------------------------------------

Un web scraper inteligente, automático, rápido y ligero para Python

1: <https://github.com/alirezamika/autoscraper>

--------------------------------------

viewgen es una herramienta de ViewState capaz de generar cargas útiles firmadas y cifradas con claves de validación filtradas

1: https://github.com/0xacb/viewgen

--------------------------------------

Escanea numeros de telefono, descubre de que pais es y quien manifesto el numero

1: <https://github.com/xKatooo/PhoneScan>

--------------------------------------

Una herramienta para mostrar la informacion importante de un numero telefonico aceptando hasta 232 paises

1: https://github.com/DtxdF/Rifap

--------------------------------------

Es una red social que permite interactuar en un contexto de prestación y consumo de servicios a domicilio.

1: <https://github.com/andgerald/Social-Network.2>

--------------------------------------

WhatScriptApp es un programa que nos ayuda a hacer spam masivo, el proyecto lo realizó mas que todo para marketing digital cuando quieres enviar un anuncio a cada usuario de la empresa o un cliente. También puedes usar para hacer ataques masivos que hoy en día hay legiones que se encargan de atacar a grupos inapropiados.

1: <https://github.com/Pericena/WhatScriptApp>

--------------------------------------

Este troyano para Android es uno de los más completos. Con él vamos a poder tener acceso a remoto a todo el dispositivo infectado, desde la agenda, las llamadas y los SMS hasta el micrófono y las cámaras del smartphone. Todo.

1: https://github.com/Pericena/Droidjack

--------------------------------------

Aquí encontrarás 5 binarios para WhatsApp

Apt update && apt upgrade -y

Pkg install git -y

Git clone <https://github.com/Predator-james/WhatsLag.git>

Cd WhatsLag

Bash WhatsLag.sh

--------------------------------------

Herramienta OSINT que usa páginas web para hacer el trabajo correcto, no nos hacemos responsables de el mal uso que le den a la herramienta…

1: <https://github.com/Predator-james/TecniSearch>

--------------------------------------

XERXES la herramienta Ddos más potente.

1: <https://github.com/Scorpio28-Oficial/XERXES>

--------------------------------------

Herramienta que sirve para mandar un ataque de spam SMS.

1: <https://github.com/Monkey-hk4/CelBoom>

--------------------------------------

Verificar usuarios de movistar con nºDNI

1: <https://github.com/Monkey-hk4/checker-movistar>

--------------------------------------

Herramienta para enviar spam de correos electrónicos a cualquier persona con su correo.

1: <https://github.com/Monkey-hk4/zombie>

--------------------------------------

Checker de números de DNI de Perú, solo mayores de edad.

1: https://github.com/Monkey-hk4/dni-checker

--------------------------------------

Herramienta de raspado de grupo de telegramas. Obtener toda la información sobre los miembros del grupo

1: https://github.com/th3unkn0n/TeleGram-Scraper

--------------------------------------

Útil para investigaciones forenses digitales o huellas iniciales de pentest de caja negra.

1: https://github.com/am0nt31r0/OSINT-Search

--------------------------------------

MagicRecon es un poderoso shell script para maximizar el proceso de reconocimiento y recolección de datos de un objetivo y encontrar vulnerabilidades comunes, todo esto guardando los resultados obtenidos de forma organizada en directorios y con varios formatos.

1: <https://github.com/robotshell/magicRecon>

--------------------------------------

Reescritura del popular auditor de redes inalámbricas, “wifite”

1: https://github.com/derv82/wifite2

--------------------------------------

RobotScraper es una herramienta simple escrita en Python para verificar cada una de las rutas que se encuentran en el archivo robots.txt y qué código de respuesta HTTP devuelven.

1: <https://github.com/robotshell/robotScraper>

--------------------------------------

Encuentre kits de phishing que utilizan los archivos y la imagen de su marca/organización.

1: <https://github.com/t4d/PhishingKitHunter>

--------------------------------------

🌰Un inspector de URL de cebolla para inspeccionar enlaces web profundos.

1: <https://github.com/k4m4/onioff>

--------------------------------------

¡Una utilidad multiplataforma basada en Python para la recopilación de información y la automatización de pruebas de penetración!

1: <https://github.com/Anon-Exploiter/SiteBroker>

--------------------------------------

Un script de python independiente que utiliza los módulos integrados de python para enumerar los binarios SUID, separar los binarios predeterminados de los binarios personalizados, compararlos con los contenedores en el repositorio de GTFO Bin y explotarlos automáticamente, ¡todo con colores! ( ͡~ ͜ʖ ͡°)

1: <https://github.com/Anon-Exploiter/SUID3NUM>

--------------------------------------

La mejor lista sobre hacking ético Si estás interesado en aprender más sobre seguridad informática y Hacking Ético aquí te dejo esta impresionante Lista.

1: <https://github.com/teamghsoftware/herramientas_hacking>

--------------------------------------

MARA es una aplicación móvil Framework de análisis e ingeniería inversa. Es una herramienta que reúne herramientas de ingeniería inversa y análisis de aplicaciones móviles utilizadas, para ayudar a probar aplicaciones móviles contra las amenazas de ciberseguridad móvil de OWASP. Su objetivo es hacer esta tarea más fácil y más amigab…

1: https://github.com/teamghsoftware/-MARA

--------------------------------------

StalkPhish: el acosador de kits de phishing, que recolecta kits de phishing para investigaciones.

1: https://github.com/t4d/StalkPhish

--------------------------------------

Detección de dominios phishing y usurpación de dominios. Admite permutaciones como ataque homógrafo, typosquatting y bitsquatting.

1: https://github.com/atenreiro/opensquat

--------------------------------------

DorkScraper es una sencilla herramienta escrita en Python para extraer todas las urls que aparecen al utilizar Google Dork.

1: <https://github.com/robotshell/dorkSraper>

--------------------------------------

QRLJacking o Quick Response Code Login Jacking es un vector de ataque simple pero desagradable que afecta a todas las aplicaciones que se basa en la función “Iniciar sesión con código QR” como una forma segura de iniciar sesión en cuentas cuyo objetivo es secuestrar la sesión de los usuarios por parte de los atacantes.

1: https://github.com/orgs/OWASP/QRLjacking

--------------------------------------

ORHound es una herramienta escrita en Python cuya función principal es encontrar posibles Open Redirects en un objetivo utilizando Google D

1: https://github.com/robotshell/ORHound

--------------------------------------

3klector es una herramienta Recon de automatización que recopila información sobre Adquisiciones y ASN relacionadas con la empresa Big Scope.

1: https://github.com/eslam3kl/3klector

--------------------------------------

Herramienta rápida para extraer todos los subdominios del sitio web crt.sh. La salida será sub.sub.sub.subdomain.com con técnicas de búsqueda estándar y avanzada

1: https://github.com/eslam3kl/crtfinder

--------------------------------------

Un módulo de python para enviar sms gratis y encontrar detalles del número de teléfono móvil a través del sitio web Way2sms.

1: <https://github.com/bhattsameer/numspy>

--------------------------------------

Cracker de hash con hash de detección automática

1: <https://github.com/CiKu370/hasher>

--------------------------------------

Una lista de herramientas de análisis forense gratuitas y abiertas y otros recursos

1: <https://github.com/mesquidar/ForensicsTools>

--------------------------------------

EVIL (Exploiting software VIa natural Language) es un enfoque para generar automáticamente exploits de software en lenguaje ensamblador/Python a partir de descripciones en lenguaje natural. El enfoque aprovecha las técnicas de traducción automática neuronal (NMT) y un conjunto de datos que desarrollamos para este trabajo.

1: <https://github.com/dessertlab/EVIL>

--------------------------------------

OhNo – El malvado generador de imágenes y metamanipulador

1: <https://github.com/Hood3dRob1n/OhNo>

--------------------------------------

Un generador de billetera bitcoin automatizado que genera direcciones de billetera aleatorias con clave privada asociada y verifica su saldo en tiempo real.

1: https://github.com/ay-bros-inc/btc-hack

--------------------------------------

Una herramienta de administración remota para dispositivos Android

1: <https://github.com/globalpolicy/PhoneMonitor>

--------------------------------------

Proyecto para automatizacion de analisis forense basico en Windows

1: <https://github.com/AlDr0id/Analisis-Forense>

--------------------------------------

Se trata de un análisis forense de un caso real, que por medio de una imagen, se obtiene una serie de datos que ayudan a una investigación.

1: <https://github.com/SVelizDonoso/forense-autopsy>

--------------------------------------

TakeTV permite descubrir dispositivos de red DLNA/UPnP y ayuda a reproducir archivos multimedia en los televisores inteligentes desde nuestra terminal en Linux.

1: <https://github.com/SVelizDonoso/taketv>

--------------------------------------

Hotspot con portal cautivo para conectar a Internet a través de redes sociales. Incluye panel de administración.

1: https://github.com/rockscripts/Zona-Wifi-Social

--------------------------------------

Escáner de cadenas en Swift puro (compatible con Unicode)

1: https://github.com/malcommac/SwiftScanner

--------------------------------------

🛰CoreLocation Made Easy: rastreador de ubicación eficiente y fácil, ubicación de IP, gecoder, geovalla, autocompletar, alcance de balizas, transmisión y monitoreo de visitas

1: <https://github.com/malcommac/SwiftLocation>

--------------------------------------

Obtenga seguidores ilimitados en Instagram de forma gratuita. Bot de CyberGhost

1: <https://github.com/MrHarshArora/Instapie>

--------------------------------------

🔎raspador de proxy y agente de usuario

1: <https://github.com/ebankoff/scraper>

--------------------------------------

Bloquee WhatsApp usando la ventana de Termux KaliLinux, WhatsApp Crasher, Estado del bloqueo, Hack WhatsApp Termux, Cómo bloquear WhatsApp

1: https://github.com/Elliot290/WhatsApp-Crasher

--------------------------------------

Generador de datos falsos completamente válidos

1: <https://github.com/JoelGMSec/FakeDataGen>

--------------------------------------

El marco de ataque de la sombra

1: <https://github.com/JoelGMSec/AutoRDPwn>

--------------------------------------

📧📡Enviar spam a miles de puntos de acceso WiFi con SSID personalizados

1: https://github.com/125K/WiFi-Spam

--------------------------------------

AntiSpy es un kit de herramientas anti-virus y rootkits gratuito pero poderoso. Le ofrece la capacidad con los privilegios más altos para detectar, analizar y restaurar varias modificaciones y ganchos del kernel. Con su ayuda, puede detectar y neutralizar fácilmente los malwares ocultos de los detectores normales.

1: <https://github.com/mohuihui/antispy>

--------------------------------------

Vulnerabilidad🕷️un Bot inteligente, Shell puede lograr la inyección automática y ayudar a los investigadores a detectar vulnerabilidades de seguridad del sistema CMS. Puede realizar una rápida detección de seguridad de CMS, recopilación de información (incluido el nombre del subdominio, la dirección IP, la información del país, la información de la organización y la zona horaria, etc.) y el escaneo de vulnerabilidades.

1: <https://github.com/anouarbensaad/vulnx>

--------------------------------------

⚡Desactivar un punto de acceso WiFi específico o un canal completo

1: <https://github.com/125K/PwrDeauther>

--------------------------------------

Herramienta avanzada de evasión AV de Android escrita en Python 3 que puede incrustar/vincular APK de meterpreter a cualquier APK legítimo

1: <https://github.com/PushpenderIndia/apkinfector>

--------------------------------------

Asistir a shells TCP inversos en tareas posteriores a la exploración

1: <https://github.com/r00t-3xp10it/redpill>

--------------------------------------

Packer Fuzzer es un escáner rápido y eficiente para la detección de seguridad de sitios web construidos por un paquete de módulos javascript como Webpack.

1: <https://github.com/rtcatc/Packer-Fuzzer>

--------------------------------------

Un tutorial de fuzzing paso a paso. Una iniciativa del laboratorio de seguridad de GitHub

1: <https://github.com/antonio-morales/Fuzzing101>

--------------------------------------

Un Android RAT multifuncional basado en Telegram sin reenvío de puertos.

1: <https://github.com/shivaya-dav/DogeRat>

--------------------------------------

Generador de listas de contraseñas que se enfoca en palabras clave mutadas por patrones de creación de contraseñas de uso común

1: <https://github.com/t3l3machus/psudohash>

--------------------------------------

Un rápido escáner de vulnerabilidades XSS basado en DOM con simplicidad.

1: <https://github.com/dwisiswant0/findom-xss>

--------------------------------------

Esta es una combinación de una herramienta de hacking y cracking.

1: <https://github.com/Mayur-Debu/Kissing-Bug>

--------------------------------------

Potentes miembros de Telegram que extraen y agregan kit de herramientas

1: <https://github.com/noob-coder123/Genisys>

--------------------------------------

Una herramienta para analizar el flujo de la red durante las competiciones de captura de bandera de ataque/defensa

1: <https://github.com/eciavatta/caronte>

--------------------------------------

venom - generador/compilador/manejador de shellcode C2

1: <https://github.com/r00t-3xp10it/venom>

--------------------------------------

R3C0Nizer es el primer marco de reconocimiento B-Tier de una aplicación web basada en menús y basada en CLI.

1: <https://github.com/Anon-Artist/R3C0Nizer>

--------------------------------------

🔑Portal cautivo WiFi para ESP8266 para contraseñas WiFi de phishing

1: <https://github.com/125K/ESP8266-Captive-Portal>

--------------------------------------

Herramienta de creación de exploits con Metasploit Framework como núcleo.

1: <https://github.com/n0obit4/friendzone>

--------------------------------------

GoReplay es una herramienta de código abierto para capturar y reproducir tráfico HTTP en vivo en un entorno de prueba para probar continuamente su sistema con datos reales. Se puede utilizar para aumentar la confianza en las implementaciones de código, los cambios de configuración y los cambios de infraestructura.

1: <https://github.com/buger/goreplay>

--------------------------------------

Cargador de shellcode evasivo para eludir la detección de inyección basada en eventos (PoC)

1: <https://github.com/xuanxuan0/DripLoader>

--------------------------------------

💻Controla tu PC de forma remota

1: <https://github.com/125K/IR_Remote_PC>

--------------------------------------

Marcador de precios en tiempo real para Bitcoin a través de nombres SSID wifi

1: https://github.com/shesek/bitcoin-ssid-ticker

--------------------------------------

Marcador de precios en tiempo real para Bitcoin a través de nombres SSID wifi

1: <https://github.com/shesek/bitcoin-ssid-ticker>

--------------------------------------

Herramienta de auditoría y ataque basada en SIP

1: https://github.com/meliht/Mr.SIP

--------------------------------------

Scanner de wifis

1: <https://github.com/alexxy/netdiscover>

--------------------------------------

Generador de saltos falsos de traceroute simple a través de la suplantación de IP

1: https://github.com/blechschmidt/fakeroute

--------------------------------------

Herramienta de defensa DDoS basada en SIP

1: <https://github.com/meliht/SIP-DD>

--------------------------------------

Herramienta de red, reconocimiento y seguridad ofensiva para sistemas Linux.

1: https://github.com/JamesonArcher/hawk

--------------------------------------

Envío de ping icmp con una IP falsificada usando un socket sin procesar de Unix

1: https://github.com/Subangkar/ICMP-Ping-Spoofing

--------------------------------------

Complemento de autenticador de DNS agnóstico del registrador de dominio para certbot

1: https://github.com/blechschmidt/certbot-dns-local

--------------------------------------

Demuestra un ataque DDOS synflood con sockets sin procesar (para distribuciones tipo Ubuntu y Debian)

1: https://github.com/rootVIII/gosynflood

--------------------------------------

Rastreo y falsificación de paquetes🗃️

1: <https://github.com/adamalston/Packet-Sniffing-and-Spoofing>

--------------------------------------

Herramienta de envenenamiento ARP escrita en python con interfaz de línea de comandos para agregar y eliminar objetivos sobre la marcha

1: https://github.com/ickerwx/arpspoof

--------------------------------------

Escáner IPv4 masivo, encuentre y analice dispositivos conectados a Internet en minutos, cree su propio motor de búsqueda de IoT en casa.

1: <https://github.com/alechilczenko/pwndora>

--------------------------------------

Herramienta de seguridad para detectar ataques de envenenamiento ARP

1: https://github.com/Ash-Shaun/ARPShield

--------------------------------------

Herramienta Osint basada en namechk.com para verificar nombres de usuario en más de 100 sitios web, foros y redes sociales.

1: <https://github.com/TheRipperJhon/namechk>

--------------------------------------

Un kit de herramientas HTTP para la investigación de seguridad.

1: <https://github.com/dstotijn/hetty>

--------------------------------------

Escáner Pentesting popular en Python3.6 para SQLi/XSS/LFI/RFI y otras vulnerabilidades

1: https://github.com/v3n0m-Scanner/V3n0M-Scanner

--------------------------------------

Herramienta para buscar archivos secretos en servidores HTTP

1: <https://github.com/hannob/snallygaster>

--------------------------------------

Repositorio oficial de herramientas de seguridad de Black Hat Arsenal

1: https://github.com/toolswatch/blackhat-arsenal-tools

--------------------------------------

Como tener wifi gratis.

1: <https://github.com/kylemcdonald/FreeWifi>

--------------------------------------

🔗GUI de suplantación de MAC de capa de enlace para macOS

1: <https://github.com/halo/LinkLiar>

--------------------------------------

Una extensión del navegador para bloquear el acceso al sitio web mediante la coincidencia de nombre de host

1: <https://github.com/ray-lothian/Block-Site>

--------------------------------------

Una extensión de navegador falsificador de User-Agent que es altamente configurable

1: https://github.com/ray-lothian/UserAgent-Switcher

--------------------------------------

🔧Cree VPN para macOS mediante programación (L2TP y Cisco)

1: <https://github.com/halo/macosvpn>

--------------------------------------

Aplicación MacOS 10.15 / 11.0 para falsificar la ubicación de su dispositivo iOS / iPadOS o iPhoneSimulator. WatchOS y TvOS son parcialmente compatibles.

1: <https://github.com/Schlaubischlump/LocationSimulator>

--------------------------------------

Un paquete shairport-metadata-reader escrito en Python, que admite la lectura de metadatos del archivo de tubería, el servidor UDP y el servidor MQTT si está configurado.

1: <https://github.com/Schlaubischlump/shairport-metadatareader-python>

--------------------------------------

Sencilla Herramienta la cual usa 2 tipos de técnicas para Desconectar a dispositivos conectados a una red por tiempo ilimitado. Herramienta desarrollada en Español e Inglés. [Para los Ataques a otras redes Wifi es necesario de una Tarjeta de Red que soporte Modo Monitor] [NO ME HAGO RESPONSABLE DEL MAL USO DE ESTA HERRAMIENTA]

1: <https://github.com/XDeadHackerX/Inhibitor>

--------------------------------------

Controlador RTL8812AU/21AU y RTL8814AU con modo monitor e inyección de fotogramas

1: https://github.com/astsam/rtl8812au

--------------------------------------

🤖Huellas dactilares falsas para eludir los sistemas anti-bot. Simule las operaciones del mouse y el teclado para comportarse como una persona real.

1: https://github.com/kkoooqq/fakebrowser

--------------------------------------

Puede obtener cc de escuchar codificado por cyber kallan

1: <https://github.com/cyberkallan/cardershub>

--------------------------------------

Dispositivo real Android, teléfono en la nube, simulador para control grupal de múltiples dispositivos. Evite la detección del sistema anti-bot. Admite RPC, NAT transversal.

1: <https://github.com/kkoooqq/fake-android>

-------------------------------------- ͓̗̹͔͙̗̗̣͇̪͚̞̞͕̹̯͚̼̠ͮͫ̇̎ͧ̐

Suplantar el número de serie de la unidad de disco duro/unidad de disco de Windows 10 desde el kernel sin enganchar

1: <https://github.com/Alex3434/wmi-static-spoofer>

--------------------------------------

Oculte su carga útil en un archivo .jpg

1: <https://github.com/Tsuyoken/ImgBackdoor>

--------------------------------------

El uso de Xposed Framework permitirá que su dispositivo aparezca como una aplicación completamente diferente a aplicaciones específicas para eludir las restricciones.

1: <https://github.com/pbombnz/Spoof-My-Device>

--------------------------------------

Espia trafico de la red NETSPY.sh ( hackingyseguridad.com )

1: <https://github.com/hackingyseguridad/netspy>

--------------------------------------

Magicspoofing es un script de Python que verifica y prueba los registros DNS SPF/DMARC e intenta falsificar un dominio con un sistema de correo de retransmisión abierto.

1: <https://github.com/magichk/magicspoofing>

--------------------------------------

[Descontinuado] Transforme su carga útil en powerpoint falso (.ppt)

1: https://github.com/Tsuyoken/MSBackdoor

--------------------------------------

Bash script que descarga juegos de PS4 a través de una conexión FTP a través de la red. Para obtener el mejor rendimiento de descarga, utilice esta carga útil de FTP: <https://github.com/hippie68/ps4-ftp> .

1: https://github.com/hippie68/ftpdump

--------------------------------------

Este es el jailbreak de PS4 de sleirsgoevy para el firmware 7.02/7.5x, actualizado con características adicionales y más cargas útiles.

1: https://github.com/hippie68/hippie68.github.io

--------------------------------------

arpspoof para macOS: intercepta paquetes en una LAN conmutada

https://github.com/YeautyYE/arpspoof

--------------------------------------

Hash Cracker, base de datos MD5 y herramientas de fuerza bruta

1: https://github.com/4xx404/BrutoNova

--------------------------------------

Wsvuls: el escáner de vulnerabilidades del sitio web detecta problemas [software de servidor desactualizado y encabezados HTTP inseguros.]

1: <https://github.com/anouarbensaad/wsvuls>

--------------------------------------

EXOCET: herramienta de entrega de carga útil indetectable que evade AV

1: <https://github.com/tanc7/EXOCET-AV-Evasion>

--------------------------------------

Esta herramienta es para detectar todo lo que hace NMAP si alguien quiere hackearlo y exponer el escaneo desde donde por DIRECCIÓN IP y la hora exacta para el análisis y convertirlo automáticamente en archivos de registro.

1: <https://github.com/anouarbensaad/nmapvision>

--------------------------------------

Bot de discordia de NotSoSuper

1: <https://github.com/NotSoSuper/NotSoBot>

--------------------------------------

reconFTW es una herramienta diseñada para realizar un reconocimiento automatizado en un dominio de destino ejecutando el mejor conjunto de herramientas para realizar escaneos y descubrir vulnerabilidades

1: <https://github.com/six2dez/reconftw>

--------------------------------------

Almacén de datos NoSQL utilizando el marco seastar, compatible con Apache Cassandra

1: <https://github.com/scylladb/scylla>

--------------------------------------

DARKARMY Hacking Tools Pack: un marco de prueba de penetración.

1: <https://github.com/D4RK-4RMY/DARKARMY>

--------------------------------------

Un HexEditor con todas las funciones compatible con Linux/Windows/M

1: <https://github.com/echo-devim/fhex>

--------------------------------------

Interfaces web modulares rápidas Bruteforcer

1: <https://github.com/koutto/web-brutator>

--------------------------------------

Pwnspoff

1: <https://github.com/punk-security/pwnspoof>

--------------------------------------

¡Tu práctica navaja suiza Cyber ​​Dandy!

1: <https://github.com/spicesouls/spicescript2>

--------------------------------------

Herramienta de fuerza bruta X🔓WordPress, Joomla, DruPal, OpenCart, Magento

1: <https://github.com/Moham3dRiahi/XBruteForcer>

--------------------------------------

Una herramienta de reconocimiento pasivo para el descubrimiento de URL conocidas: recopila una lista de URL de forma pasiva utilizando varias fuentes en línea.

1: <https://github.com/signedsecurity/sigurlfind3r>

--------------------------------------

Sigs3scann3r es una herramienta para escanear los permisos de depósito de AWS S3 y volcar el contenido del depósito cuando corresponda.

1: <https://github.com/signedsecurity/sigs3scann3r>

--------------------------------------

Un generador de ladrones de tokens AIO y un enumerador de tokens

1: <https://github.com/spicesouls/disenum>

--------------------------------------

Obtenga la dirección IP en la llamada de audio del otro lado en Telegram.

1: <https://github.com/n0a/telegram-get-remote-ip>

--------------------------------------

Clonar sitios web automáticamente y parchearlos con PHP para crear páginas de phishing

1: <https://github.com/andpalmier/makephish>

--------------------------------------

MagicRecon es un poderoso shell script para maximizar el proceso de reconocimiento y recolección de datos de un objetivo y encontrar vulnerabilidades comunes, todo esto guardando los resultados obtenidos de forma organizada en directorios y con varios formatos.

1: <https://github.com/robotshell/magicRecon>

--------------------------------------

Script de PowerShell del equipo rojo

1: <https://github.com/securethelogs/RedRabbit>

--------------------------------------

Herramienta de pirateo de Instagram todo en uno disponible (recopilación de información de Insta, fuerza bruta de Insta, autorreportador automático de cuenta de Insta)

1: <https://github.com/IncredibleHacker/insta-hack>

--------------------------------------

PassLock es una aplicación simple que utiliza una base de datos local para manejar una lista de usuarios de credenciales de servicio.

1: <https://github.com/mastrHyperion98/PassLock>

--------------------------------------

DorkScraper es una sencilla herramienta escrita en Python para extraer todas las urls que aparecen al utilizar Google Dork.

1: <https://github.com/robotshell/dorkSraper>

--------------------------------------

Script Bash para CTF que automatiza la enumeración básica

1: <https://github.com/zAbuQasem/zBuster>

--------------------------------------

Una herramienta para la explotación persistente de XSS con un enfoque para navegadores web móviles

1: <https://github.com/echo-devim/xbackdoor>

--------------------------------------

Una RAT multifuncional multiplataforma (Windows/Linux/Mac).

1: <https://github.com/hash3liZer/SillyRAT>

--------------------------------------

Una herramienta inalámbrica (WPA/WPA2) Pentest/Cracking. Captura y descifra el apretón de manos de 4 vías y la clave PMKID. Además, admite un modo de desautenticación/jammer para pruebas de esfuerzo.

1: <https://github.com/hash3liZer/WiFiBroot>

--------------------------------------

Herramienta avanzada de evasión AV de Android escrita en Python 3 que puede incrustar/vincular APK de meterpreter a cualquier APK legítimo

1: <https://github.com/PushpenderIndia/apkinfector>

--------------------------------------

MgToLs mas de 80 herramientas de hacking para la gran mayoria de ataques.

1: <https://github.com/NePtYx2018/MgToLs>

--------------------------------------

Simular root en Termux

1: <https://github.com/Darkmux/RootTH>

--------------------------------------

💤Saque los dispositivos de su red realizando un ataque ARP Spoof.

1: <https://github.com/k4m4/kickthemout>

--------------------------------------

Una herramienta OSINT para obtener el número de teléfono de un objetivo con solo tener su dirección de correo electrónico

1: https://github.com/martinvigo/email2phonenumber

--------------------------------------

CLAYS HACKER NINGUN SISTEMA ES SEGURO

1: https://github.com/CLAYSHACKER/virus-apk-

--------------------------------------

Saca tarjeta de credito a full

1: https://github.com/RealHackRH593/CC-MundoRH

--------------------------------------

ADB-Toolkit V2 para trucos ADB fáciles con muchas ventajas en uno. ¡DISFRUTAR!

1: <https://github.com/ASHWIN990/ADB-Toolkit>

--------------------------------------

Herramienta para descifrar hashes de contraseñas como MD5, SHA1, SHA256, PDF encriptado, archivo comprimido encriptado y muchos otros hashes de contraseñas🤘🤘

1: <https://github.com/ASHWIN990/JTRE>

--------------------------------------

Aplicación de Pishing con Facebook e Ing Social con enlaces de WhatsApp

1: <https://github.com/krootca/kface.git>

--------------------------------------

Un script de pirateo fácil de manejar, SSH Forcebrute, FTP Forcebrute y muchas otras características

1: <https://github.com/Coroxx/TheSmartool>

--------------------------------------

Esta herramienta para simular ataques de servidor http en Python que registra HackerIP y todo el seguimiento que hace en un archivo de registro y luego en una base de datos.

1: <https://github.com/anouarbensaad/honeypot-iot>

--------------------------------------

CyberScan: kit de herramientas forenses de la red

1: <https://github.com/medbenali/CyberScan>

--------------------------------------

RomBuster es una herramienta de explotación de enrutadores que permite revelar la contraseña de administrador del enrutador de red.

1: <https://github.com/EntySec/RomBuster>

--------------------------------------

Página para obtener la ubicación de su víctima mediante GPS usando ing. Social

1: <https://github.com/tony23x/geo>

--------------------------------------

Plataforma modular de pruebas de penetración que le permite escribir, probar y ejecutar código de explotación.

1: <https://github.com/EntySec/HatSploit>

--------------------------------------

Evilgrade es un marco modular que permite al usuario aprovechar las implementaciones de actualización deficientes mediante la inyección de actualizaciones falsas.

1: https://github.com/infobyte/evilgrade

--------------------------------------

Geolocalizacion en tiempo real

1: <https://github.com/devatens/geo-localiza>

--------------------------------------

Spoilerwall presenta un concepto completamente nuevo en el campo del fortalecimiento de redes. ¡Evite ser escaneado estropeando películas en todos sus puertos!

1: <https://github.com/infobyte/spoilerwall>

--------------------------------------

Marco de explotación de Wi-Fi

1: <https://github.com/D3Ext/WEF>

--------------------------------------

Escáner CMS: escanee sitios web de Wordpress, Drupal, Joomla, vBulletin en busca de problemas de seguridad

1: <https://github.com/ajinabraham/CMSScan>

--------------------------------------

Avisos, archivos de prueba de concepto y exploits que @pedrib ha hecho públicos

1: <https://github.com/pedrib/PoC>

--------------------------------------

Genera código shell independiente de posición x86, x64 o AMD64+x86 que carga ensamblajes .NET, archivos PE y otras cargas útiles de Windows desde la memoria y las ejecuta con parámetros

1: <https://github.com/TheWover/donut>

--------------------------------------

Plataforma colaborativa de gestión de vulnerabilidades y pruebas de penetración

1: <https://github.com/infobyte/faraday>

--------------------------------------

Una biblioteca para generar datos falsos como nombres, direcciones y números de teléfono.

1: <https://github.com/faker-ruby/faker>

--------------------------------------

Faker es una biblioteca PHP que genera datos falsos para ti

1: <https://github.com/fzaninotto/Faker>

--------------------------------------

aplicación de prueba de concepto para mostrar cómo cargar y descifrar la base de datos de respaldo de WhatsApp

1: <https://github.com/taufderl/whatsapp-sniffer-android-poc>

--------------------------------------

📡Herramienta de sobrecarga DDOS (capa 7)

1: <https://github.com/7zx/overload>

--------------------------------------

Una herramienta de automatización avanzada para Web-Recon desarrollada para sistemas Linux

1: <https://github.com/Cyber-Guy1/BlackDragon>

--------------------------------------

Una herramienta de automatización para instalar las herramientas más populares para bug bounty o pentesting.

1: <https://github.com/DonatoReis/arno>

--------------------------------------

Generador de informes Pentest

1: <https://github.com/pwndoc/pwndoc>

--------------------------------------

Una herramienta para generar cargas útiles de shell inverso sobre la marcha.

1: <https://github.com/octetsplicer/LAZYPARIAH>

--------------------------------------

Herramienta en Bash para realizar una enumeración básica y extraer la información más relevante de un Directorio Activo vía rpcclient.

1: <https://github.com/m4lal0/RPCrecon>

--------------------------------------

GeoTrackerIP es una herramienta que analiza y recopila información de una dirección IP o dominio, por ejemplo: Ubicación Geográfica, ISP(Proveedor de Servicios de Internet), Ciudad, País, entre otros.

1: <https://github.com/jric2002/GeoTrackerIP>

--------------------------------------

Herramienta de acceso remoto escrita en C#

1: <https://github.com/arsium/EagleMonitorRAT>

--------------------------------------

🔓Ataque de oráculo de relleno contra PKCS7🔓

1: <https://github.com/mpgn/Padding-oracle-attack>

--------------------------------------

Script de ingeniería inversa para cargas útiles de Android Rat

1: <https://github.com/Max-IQ/Horus-Eye>

--------------------------------------

👽Programa para el control remoto de computadoras con Windows a través del bot de Telegram. Escrito en C#

1: <https://github.com/LimerBoy/ToxicEye>

--------------------------------------

Una herramienta para construir un troyano de acceso remoto.

1: <https://github.com/AdolfMacro/eyerat>

--------------------------------------

Este repositorio contiene todos los documentos relacionados con ISA. Este curso trata sobre seguridad y garantía de la información y los conceptos necesarios para asegurar el ciberespacio. Introduce modelos de seguridad, políticas de aseguramiento, políticas y procedimientos de seguridad y tecnología. Ayuda a comprender la necesidad de aseguramiento de la información, identificar la seguridad…

1: <https://github.com/cmoulika009/Information_Security_Assurance>

--------------------------------------

CarDataSnatch le permite encontrar rápidamente información sobre un automóvil en el Reino Unido utilizando una placa de matrícula válida. Tome una imagen del automóvil en cuestión junto con una multitud de otros datos. Compare los datos de dos autos para un análisis rápido y fácil.

1: <https://github.com/kylekirkby/CarDataSnatch>

--------------------------------------

El es un script bash que se ha creado para enrutar el tráfico desde la computadora de una víctima a la computadora de los atacantes. Esto es excelente para la recolección de credenciales. La configuración de burp suite se puede encontrar en la sección de comentarios del script bash o en el archivo Léame.

1: <https://github.com/Silas-Stone/burp-arp-spoof>

--------------------------------------

ExeSpy es un visor PE multiplataforma para archivos EXE y DLL

1: <https://github.com/andyjsmith/Exe-Spy>

--------------------------------------

Pruebas de penetración en servidores SSH usando fuerza bruta o ataques de diccionario. Escrito en Python.

1: <https://github.com/matricali/brutekra>

--------------------------------------

CVE-2021-4034 1day (whoami root)

1: <https://github.com/berdav/CVE-2021-4034>

--------------------------------------

Herramienta de fuerza bruta

1: <https://github.com/Aaron-Akhtar/Jupiter>

--------------------------------------

Herramienta de Python que envía las capturas de pantalla del dispositivo de la víctima.

1: <https://github.com/sanskarbansal/Python_Spy_Tool>

--------------------------------------

Ataque de diccionario al portal de usuario NIT Kurukshetra (Cyberoam). Un script de nodejs para adivinar la contraseña de cyberoam para cualquier nombre de usuario dado.

1: <https://github.com/varunon9/Dictionary-Attack-Cyberoam>

--------------------------------------

Script basico para extraer datos de una ip

1: <https://github.com/b4rc0d37/IP-GEO>

--------------------------------------

Generador y cambiador de direcciones MAC

1: https://github.com/waseem-sajjad/MACMasterTool

--------------------------------------

Servidor HTTP para phishing en python

1: <https://github.com/evait-security/weeman>

$ apt update

$ apt upgrade

$ apt install git

$ apt install python2

$ git clone <https://github.com/evait-security/weeman>

$ cd weeman

$ chmod +x \*

Uso :

$ python2 weeman.py

$ set url <http://target.com>

$ set action\_url <http://target.com>

$ run

--------------------------------------

::////

1: <https://github.com/cr4shcod3/pureblood>

--------------------------------------

Dropper de carga útil multiplataforma

1: <https://github.com/UndeadSec/Enigma>

--------------------------------------

Dark-Fb Sin inicio de sesión 100% seguro

1: https://github.com/BOT-033/Sensei

--------------------------------------

Script de Python que se crea para descifrar archivos rar protegidos con contraseña

1: <https://github.com/TermuxHackz/Crack-rar>

--------------------------------------

phonesploit

1: https://github.com/mishab-ka/PhoneSploit

--------------------------------------

Una sesión de herramientas Secuestro y ladrón Código de acceso local Telegram Windows

1: <https://github.com/ultrasecurity/TeleKiller>

--------------------------------------

El script LAZY te hará la vida más fácil y, por supuesto, más rápida.

1: https://github.com/arismelachroinos/lscrip

--------------------------------------

El bot de Discord más rápido que asalta, destruye y piratea servidores de Discord

1: <https://github.com/KMKINGMAN/Raid-Bot-TS>

--------------------------------------

Organiza los canales de sugerencias en los servidores, donde el administrador puede especificar los canales de sugerencias, y las personas pueden enviar la propuesta a través de uno de los comandos del bot, y aparte de esto, el administrador puede simplemente eliminar y responder a las sugerencias

1: <https://github.com/KMKINGMAN/Suggestion-bot>

--------------------------------------

Cliente API RabbitMQ HTTP en G

1: <https://github.com/michaelklishin/rabbit-hole>

--------------------------------------

Virus()

1: https://github.com/ArroKM/VIRTEX

--------------------------------------

Es un bot de Discord cuyo objetivo es facilitar a los propietarios de servidores la creación de una aplicación llamada Staff/Mode.

1: <https://github.com/KMKINGMAN/Application-Bot>

--------------------------------------

Hackeo de Whatsapp

1: <https://github.com/Bl4ckDr460n/HxWhatsApp.git>

Cd HxWhatsApp

$ chmod +x HxWhatsApp.py

$ python2 HxWhatsApp.py

--------------------------------------

Es un bot que envía informes sobre personas que roban sus derechos de Códigos y dicen que son programadores, etc.

1: <https://github.com/KMKINGMAN/AntiCopyPaster>

--------------------------------------

Las mejores aplicaciones de virus y la herramienta de creación de mensajes VIRUS

1: https://github.com/Devil-Tigers/TigerVirus

--------------------------------------

Es una herramienta de discordia que elimina/deshabilita Discord Webhook

1: <https://github.com/KMKINGMAN/Discord-webhook-disabler>

--------------------------------------

Una herramienta fácil de pentesting.

1: <https://github.com/kuburan/txtool>

--------------------------------------

Herramienta de recopilación de información del sitio web

1: https://github.com/Err0r-ICA/InfoWeb

--------------------------------------

Es una herramienta de discordia dedicada que envía continuamente una gran cantidad de mensajes al canal de discordia a través de Discord Webhook.

1: <https://github.com/KMKINGMAN/Discord-WebHook-Spammer>

--------------------------------------

Weather bot es un bot de discord simple que le muestra el clima en su área con un simple comando

1: <https://github.com/KMKINGMAN/Weather-Bot>

--------------------------------------

Script solo para Termux que automatiza la conexión a la base de datos de Metasploit sin errores

1: <https://github.com/tony23x/MSF-DB>

--------------------------------------

Una herramienta sencilla para rastrear IP programada en Python

1: <https://github.com/Euronymou5/Spyrod-v2>

--------------------------------------

Aceptador de solicitudes en Instagram

1: <https://github.com/anonymouslb/Auto-accept-Follow-request>

--------------------------------------

Una herramienta hecha para obtener el pip de python3 y python2

1: <https://github.com/Euronymou5/Get-pip>

--------------------------------------

Potente herramienta de ataque IP Stresser / DDoS

1: <https://github.com/iJoshoa/UnstableDDoS>

--------------------------------------

Decodificar todas las bases - Decodificador de esquema base

1: <https://github.com/mufeedvh/basecrack>

--------------------------------------

Es un marco lleno de muchas opciones y herramientas de piratería que usa directamente en el script, desde la fuerza bruta hasta la carga útil, lo que hace que sigo agregando más cosas. Ahora tengo otra herramienta llamada htkl-lite, su kit de herramientas para hackers no es tan grande y desordenado. Para ver las actualizaciones, consulte mi instagram @tuf\_unkn0wn o si hay algún problema, envíeme un mensaje en insta…

1: <https://github.com/unkn0wnh4ckr/hackers-tool-kit>

--------------------------------------

Publicaré actualizaciones en mi instagram @g3\_ruben.\_.fuenla\_: un marco de piratería con todo tipo de herramientas de fuerza bruta, recopilación de información, ataque dos, etc. Que usa directamente en el script. Lamentablemente, la fuerza bruta de Twitter no funciona.

1: <https://github.com/unkn0wnh4ckr/tufhub>

--------------------------------------

Un booter espeluznante para halloween, este script de python contiene una variedad de ataques DOS y alguna recopilación de información (EJECUTAR COMO ROOT)

1: <https://github.com/unkn0wnh4ckr/boOoter>

--------------------------------------

🦀Prueba de estrés DoS (Denegación de servicio) basada en UDP y herramienta de Denegación de servicio realizada en Rust.

1: <https://github.com/c3l3si4n/r-u-flooded>

--------------------------------------

Claramente diseñé esta herramienta con fines educativos y solo para comprender cómo se realizan los ataques de sockets y DDOS. ¡Eres responsable de tus propias acciones!

1: https://github.com/s1ralt/D.DDOS

--------------------------------------

Pugrecon es un script bash para el reconocimiento automático de vulnerabilidades comunes, configuraciones incorrectas y archivos en dominios.

1: <https://github.com/c3l3si4n/pugrecon>

--------------------------------------

Genera Discord Nitro Gift Link y verifica si es válido o no válido

1: https://github.com/s1ralt/D.NitroGen

--------------------------------------

Un booter falso para entretener a la galería

1: https://github.com/Sayrix/fake-booter

--------------------------------------

📍Verifique si una red Wi-Fi está ubicada en una ubicación geográfica razonable

1: https://github.com/rodrigobdz/geo-wifi

--------------------------------------

Proxychains ng (nueva generación): un precargador que engancha llamadas a sockets en programas vinculados dinámicamente y los redirige a través de uno o más proxies de calcetines/http. Continuación del proyecto de cadenas de proxy no mantenidas. La página de sf.net no está actualizada actualmente, use versiones de la página de lanzamiento de github en su lugar.

1: https://github.com/rofl0r/proxychains-ng

--------------------------------------

Kit de herramientas de piratería PCI Express DIY para Xilinx SP605

1: <https://github.com/EgeBalci/s6_pcie_microblaze>

--------------------------------------

Busque datos de geolocalización WiFi por BSSID y SSID en diferentes bases de datos públicas.

1: https://github.com/GONZOsint/geowifi

--------------------------------------

Eficaz herramienta capaz de inyectar un backdoor a casi cualquier aplicación Android actual

1: <https://github.com/yaxter/BACKDROID>

--------------------------------------

Herramienta OSINT para obtener información de un perfil de Github y Gitlab y encontrar las direcciones de correo electrónico de los usuarios filtradas en las confirmaciones.

1: <https://github.com/GONZOsint/gitrecon>

--------------------------------------

Kit de detección y explotación de CMS basado en la API de Whatcms.org

1: https://github.com/GONZOsint/WhatCMS

--------------------------------------

MacGeiger: una herramienta para rastrear la ubicación de puntos de acceso WIFI con sonido (similar a un contador Geiger)

1: <https://github.com/rofl0r/MacGeiger>

--------------------------------------

Herramienta Osint basada en namechk.com para verificar nombres de usuario en más de 100 sitios web, foros y redes sociales.

1: https://github.com/GONZOsint/Namechk

--------------------------------------

Mi secuencia de comandos de enumeración de subdominio. Es único en la forma en que está construido.

1: <https://github.com/iamthefrogy/frogy>

--------------------------------------

Kaumodaki es una herramienta que tiene una colección de todas las herramientas de piratería populares en un solo lugar.

1: <https://github.com/CybSec-NITW/kaumodaki>

--------------------------------------

Explotación de XSHOCK Shellshock

1: <https://github.com/capture0x/XSHOCK>

--------------------------------------

Token de discordia y capturador de IP

1: https://github.com/EbicHecker/DiscordTokenStealer

--------------------------------------

Extractor de correo con su idiota

1: <https://github.com/capture0x/mailExtractor>

--------------------------------------

Herramienta de piratería todo en uno para Linux y Android (Termux). Convierta su entorno Linux en una máquina de piratería. Los hackers son bienvenidos en nuestro blog.

1: <https://github.com/technicaldada/hackerpro.git>

--------------------------------------

Doxing es el proceso de obtención de información acerca de una persona a través de fuentes de internet, utilizando el ingenio y las habilidades de búsqueda. La palabra deriva de “document” en inglés y ing, que sería un gerundio en esa lengua : documentando o algo por el estilo pero queda mejor doxing

1: https://github.com/Pericena/Doxinfo

--------------------------------------

Herramienta diseñada para el e

1: https://github.com/Not-Risks/SpamMAIL-NR

--------------------------------------

XCTR Hacking Tools

1: https://github.com/capture0x/XCTR-Hacking-Tools/

--------------------------------------

Un poderoso kit de herramientas para hackers recopiló más de 10 categorías de escáneres de código abierto de Github

1: <https://github.com/We5ter/Scanners-Box>

--------------------------------------

Herramienta Avoidz para eludir la mayoría de los softwares AV

1: https://github.com/M4sc3r4n0/avoidz

--------------------------------------

La extensión Red Team todo en uno para Web Pentester🛠

1: <https://github.com/LasCC/Hack-Tools>

--------------------------------------

La mejor tabla de datos de JavaScript para crear aplicaciones empresariales. Admite React / Angular / Vue / JavaScript simple.

1: <https://github.com/ag-grid/ag-grid>

--------------------------------------

Potente fuzzer de directorio web mutable para aplicar fuerza bruta a archivos o directorios existentes y/o ocultos.

1: https://github.com/cytopia/urlbuster

--------------------------------------

Pwncat: netcat con esteroides con cortafuegos, evasión de IDS/IPS, shell de enlace e inversión, shell de autoinyección y magia de reenvío de puertos, y es completamente programable con Python (PSE)

1: https://github.com/cytopia/pwncat

--------------------------------------

Obtenga entradas de teclado, mouse, captura de pantalla, micrófono de la computadora de destino y envíelas a su correo.

1: <https://github.com/aydinnyunus/Keylogger>

--------------------------------------

Herramientas de Python para piratear USB

1: <https://github.com/Merimetso-Code/USB-Hacking>

--------------------------------------

Herramienta de piratería todo en uno para Linux y Android (Termux). Convierta su entorno Linux en una máquina de piratería. Los hackers son bienvenidos en nuestro blog.

1: https://github.com/jaykali/hackerpro

--------------------------------------

PacketWhisper: extraiga datos de forma sigilosa y elimine la atribución mediante consultas de DNS y esteganografía basada en texto. Evite los problemas asociados con los métodos típicos de exfiltración de DNS. Transfiera datos entre sistemas sin que los dispositivos de comunicación se conecten directamente entre sí o a un punto final común. No es necesario controlar un servidor de nombres DNS.

1: https://github.com/TryCatchHCF/PacketWhisper

--------------------------------------

Redes sociales y piratería de cámaras y virus de WhatsApp y bombardeo de SMS

1: <https://github.com/rixon-cochi/hacking-tool>

--------------------------------------

Un registrador de teclas USB habilitado para WiFi y una herramienta de inyección de pulsaciones de teclas

1: <https://github.com/justcallmekoko/USBKeylogger>

--------------------------------------

Web dorking por problema de la base de datos de piratería de Google [Exploit-DB]

1: <https://github.com/nalonal/ghdb>

--------------------------------------

Obtener información detallada sobre los archivos apk

1: <https://github.com/andpalmier/apkingo>

--------------------------------------

Contaminar kits de phishing con credenciales falsas

1: https://github.com/andpalmier/phishflood

--------------------------------------

MS17-010

1: https://github.com/worawit/MS17-010

--------------------------------------

Recursos de Word para phishing. Incluye la implementación de documentos de cebo y señuelo “Hacer clic en Habilitar contenido”.

1: <https://github.com/TheKevinWang/MacroPhishing>

--------------------------------------

Python Script para ayudar/automatizar los ejercicios de piratería WiFi.

1: https://github.com/ShineZex/WiCrackFi

--------------------------------------

Un inyector de registrador de teclas simple que le envía correos electrónicos frecuentes sobre los registros de las computadoras host.

1: <https://github.com/ahmedhamedaly/Key-Logger-Injector>

--------------------------------------

Hash brute

1: <https://github.com/king-hacking/MK_hash>

--------------------------------------

Dracnmap es un programa de código abierto que se utiliza para explotar la red y recopilar información con la ayuda de nmap. El comando Nmap viene con muchas opciones que pueden hacer que la utilidad sea más robusta y difícil de seguir para los nuevos usuarios. Por lo tanto, Dracnmap está diseñado para realizar un escaneo rápido con el motor de secuencias de comandos de nmap y nmap puede realizar va…

1: <https://github.com/Screetsec/Dracnmap>

--------------------------------------

🐰Gestión de fragmentos de comandos para piratas informáticos/cazadores de recompensas por errores. Con mascota

1: <https://github.com/hahwul/hack-pet>

--------------------------------------

Fb oscuro

1: <https://github.com/ezaID/darkfb>

--------------------------------------

Offensive Docker es una imagen con las herramientas ofensivas más utilizadas para crear un entorno fácil y rápido para lanzar evaluaciones a los objetivos.

1: <https://github.com/aaaguirrep/offensive-docker>

--------------------------------------

Windows payloads

1: <https://github.com/nccgroup/Winpayloads.git>

--------------------------------------

Este Script te ayudará a recopilar información sobre tu víctima o amigo.

1: <https://github.com/Deadshot0x7/007-TheBond>

--------------------------------------

Herramienta OSINT para extraer nombres y nombres de usuario de grandes listas de amigos en Facebook, sin límite de frecuencia.

1: <https://github.com/narkopolo/fb_friend_list_scraper>

--------------------------------------

Herramienta OSINT para encontrar correos electrónicos violados, bases de datos, pastas e información relevante

1: <https://github.com/Ekultek/WhatBreach>

--------------------------------------

Xepor, un marco de enrutamiento web para ingenieros inversos e investigadores de seguridad, trae lo mejor de mitmproxy y Flask

1: <https://github.com/xepor/xepor>

--------------------------------------

Agente Mythic C2 dirigido a hosts Linux y Windows escrito en Rust

1: https://github.com/MythicAgents/tetanus

--------------------------------------

Hackeo de redes sociales

1: <https://github.com/rixon-cochi/SMF>

--------------------------------------

¡El mejor espía WiFi disponible para alquilar! Hecho para piratas informáticos, para piratas informáticos

1: https://github.com/DeaDHackS/WiFiSpy

--------------------------------------

Herramienta de administración remota para OS Linux

1: https://github.com/king-hacking/SPY-KING

--------------------------------------

Plataforma de gestión de superficie de ataque | Sn1perSecurity LLC

1: https://github.com/1N3/Sn1per

--------------------------------------

Herramienta DDOS: para eliminar sitios web pequeños con HTTP FLOOD. Escáner de puertos: Para conocer los puertos abiertos de un sitio. FTP Password Cracker: para piratear el sistema de archivos de los sitios web. Banner Grabber: para ejecutar el servicio o el software en un puerto. (Después de conocer las vulnerabilidades del software que ejecuta Google). Web Spider: para recopilar aplicaciones web pirateadas en…

1: <https://github.com/ritvikb99/dark-fantasy-hack-tool>

--------------------------------------

Un token nuker de Discord Con un montón de opciones que arruinarán una cuenta realmente mal, también tiene un informe masivo incorporado, GroupChat Spammer y Token / Contraseña / Capturador de tarjetas de crédito ¡y mucho más!

1: <https://github.com/Rdimo/Hazard-Nuker>

--------------------------------------

Versión actualizada de https://github.com/Rdimo/Hazard-Token-Grabber ¡Esta tiene mucho más impacto y roba contraseñas, cookies, tokens, tarjetas de crédito, capturas de pantalla de IP y más de Google Chrome!

1: <https://github.com/Rdimo/Hazard-Token-Grabber-V2>

--------------------------------------

secuestrador de conexión tcp, reescritura de óxido de shijack

1: https://github.com/kpcyrd/rshijack

--------------------------------------

Una simple herramienta que utiliza Localhost.run para entunelar un puerto de localhost a un link donde las personas puedan entrar a el link

1: <https://github.com/Euronymou5/Entunelador>

--------------------------------------

Herramienta para generar virus programado en python

1: <https://github.com/Euronymou5/VenoM>

--------------------------------------

Ejecute exploits interactivos de Android en Linux.

1: <https://github.com/sundaysec/Andspoilt>

--------------------------------------

“Socialx” es una herramienta troyana de ingeniería social y acceso remoto. Puede generar fud backdoor e incrustar cualquier archivo que desee dentro del archivo exe. (hackear ordenador con pdf)

1: <https://github.com/AzizKpln/Social_X>

--------------------------------------

Esta herramienta brinda información sobre el número de teléfono que ingresó.

1: <https://github.com/AzizKpln/Moriarty-Project>

--------------------------------------

HERCULES es un generador de carga útil especial que puede pasar por alto los softwares antivirus.

1: <https://github.com/EgeBalci/HERCULES>

--------------------------------------

Todo lo necesario que un doxxer debe de tener siempre a mano

1: <https://github.com/Euronymou5/Doxxer-Toolkit>

--------------------------------------

Ratifique un dispositivo Windows usando Telegram.Bot API

1: <https://github.com/HworangeRival/Telegram_BotRat>

--------------------------------------

Osint gmail

1: <https://github.com/-mxrch/GHunt>

--------------------------------------

Autoliker Instagram bot

1: <https://github.com/numero69/likeThat>

--------------------------------------

Encuentra nombres de usuario en más de 75 redes sociales

1: https://github.com/wishihab/userrecon

--------------------------------------

XploitSPY es una herramienta de monitoreo / espionaje de Android

1: <https://github.com/XploitWizer-Community/XploitSPY>

--------------------------------------

⛔🛡️WeDefend – Supervise y proteja Windows del troyano de acceso remoto

1: <https://github.com/wishihab/WeDefend>

--------------------------------------

Herramienta para ayudar a explotar vulnerabilidades XXE

1: <https://github.com/luisfontes19/xxexploiter>

--------------------------------------

Herramienta para generar payloads csrf basados ​​en solicitudes vulnerables

1: <https://github.com/luisfontes19/CSRFER>

--------------------------------------

Las botnets Smishing se vuelven virales en Irán

1: <https://github.com/kh4sh3i/Smishing-Botnets>

--------------------------------------

Un repetidor WiFi completamente funcional (correctamente: un enrutador WiFi NAT)

1: <https://github.com/martin-ger/esp_wifi_repeater>

--------------------------------------

🔎Olfateando y analizando el protocolo mysql, redis, http, mongodb, etc.

1: <https://github.com/40t/go-sniffer>

--------------------------------------

El ChameleonMini es un emulador de tarjeta inteligente sin contacto versátil compatible con NFC. El ChameleonMini fue desarrollado por <https://kasper-oswald.de> . El dispositivo está disponible en <https://shop.kasper.it> . Para obtener más información, consulte la página de inicio <https://rawgit.com/emsec/ChameleonMini/master/Doc/Doxygen/html/_page__getting_started.html> o la Wi…

1: <https://github.com/emsec/ChameleonMini>

--------------------------------------

Escaneo de subdominio knock

1: <https://github.com/guelfoweb/knock>

--------------------------------------

Este es el bot de whatsapp para termux. Y no toques mi teléfono

1: https://github.com/affisjunianto/botwasapv4

--------------------------------------

Herramienta de phishing fácil de usar con 65 plantillas de sitios web. El autor no es responsable por cualquier mal uso.

1: <https://github.com/KasRoudra/PyPhisher>

--------------------------------------

Rastreador de paquetes multiproceso Seguro

1: https://github.com/kpcyrd/sniffglue

--------------------------------------

⛔ 🛡️WeDefend: controle y proteja Android del troyano de acceso remoto

1: <https://github.com/wishihab/WeDefend-Android>

--------------------------------------

Registrar y analizar solicitudes HTTP salientes

1: <https://github.com/aderyabin/sniffer>

--------------------------------------

Rastreador y transmisor de paquetes Bluetooth Low Energy (BLE) para estándar y no estándar (bit sin formato) basado en Software Defined Radio (SDR).

1: <https://github.com/JiaoXianjun/BTLE>

--------------------------------------

Una herramienta para la captura pasiva de datos y el reconocimiento de chips flash seriales. Se utiliza junto con un analizador lógico Saleae para reconstruir el contenido de la memoria flash y extraer información contextual sobre las operaciones del dispositivo.

1: https://github.com/alainiamburg/sniffROM

--------------------------------------

Trax | Escáner de vulnerabilidad XSS automatizado actualmente en desarrollo🐍PROYECTO HACKTOBERFEST 2019

1: <https://github.com/M4cs/traxss>

--------------------------------------

Servidores RIP; El robot nuclear más rápido que existe.

1: <https://github.com/TKperson/Nuking-Discord-Server-Bot-Nuke-Bot>

--------------------------------------

Tomando el token de Discord usando solo la consola de JavaScript.

1: <https://github.com/TKperson/jsConsole-discordTokenGrabber>

--------------------------------------

💣Guildbomb es un bot de discordia simple, que te muestra lo fácil que puede ser asaltar un servidor de discordia en un minuto, por lo que todos serán baneados, todos los emojis serán eliminados, todas las invitaciones serán eliminadas, todos los roles y todos los canales también.

1: https://github.com/ARealWant/Guildbomb-Discord-Bot

--------------------------------------

No permita que los desbordamientos de búfer desborden su mente

1: <https://github.com/gh0x0st/Buffer_Overflow>

--------------------------------------

Cyborg Nuker V4 | ¡El nuker más rápido disponible en discord gratis! ¡limpia los srvrs en solo unos segundos!

1: <https://github.com/Icognito777/Cyborg-Nuker-v4>

--------------------------------------

💀La primera herramienta de incursión de este tipo. Inyecte servidores Deadcord y raid directamente desde el cliente Discord.

1: <https://github.com/GalaxzyDev/Deadcord>

--------------------------------------

E4GL30S1NT – Herramienta sencilla de recopilación de información

1: https://github.com/C0MPL3XDEV/E4GL30S1NT

--------------------------------------

Discord Server Anti Nuke Tool para evitar que su servidor sea destruido. (V3 Beta disponible ahora)

1: https://github.com/17teen/Discord-Bladee-Server-Anti-Nuker

--------------------------------------

Crea tu bot discord raid en discord.js node.js

1: https://github.com/Walkoud/raidbotdiscord

--------------------------------------

Nuke Discord Bot en Js (Beta ha llegado)

1: https://github.com/17teen/Discord-Presser-Server-Nuker

--------------------------------------

Enumerar información de puntos finales web habilitados para la autenticación NTLM🔎

1: https://github.com/pwnfoo/NTLMRecon

--------------------------------------

Parámetros de minería de rincones oscuros de archivos web

1: https://github.com/devanshbatham/ParamSpider

--------------------------------------

Ingeniería inversa kahoot

1: <https://github.com/unixpickle/kahoot-hack>

--------------------------------------

El propósito de este script es automatizar el proceso de enumeración web y buscar exploits.

1: <https://github.com/V1n1v131r4/webdiscover>

--------------------------------------

Este repositorio es un espejo de <https://git.openwrt.org/openwrt/openwrt.git> Es solo para referencia y no está activo para registros. Continuaremos aceptando Pull Requests aquí. Se fusionarán a través de árboles de preparación y luego en openwrt.git.

1: <https://github.com/openwrt/openwrt>

--------------------------------------

Página de inicio: https://pyscript.net Ejemplos: <https://pyscript.net/examples>

1: https://github.com/pyscript/pyscript

--------------------------------------

Una sencilla herramienta de administración remota web para Windows escrita en Python, PHP y JavaScript

1: <https://github.com/cyberaz0r/WebRAT>

--------------------------------------

Exfiltrador de contenido de varias líneas fuera de banda XXE a través de DTD externo utilizando servidores HTTP y FTP autohospedados

1: <https://github.com/cyberaz0r/XXE-OOB-Exfiltrator>

--------------------------------------

Una herramienta que encuentra, enumera y explota cámaras Reolink.

1: <https://github.com/spicesouls/reosploit>

--------------------------------------

Generador de carga útil MSFVenom simple

1: <https://github.com/spicesouls/lemon>

--------------------------------------

Una aplicación de Android vulnerable que muestra ejemplos simples de vulnerabilidades en un estilo ctf.

1: <https://github.com/B3nac/InjuredAndroid>

--------------------------------------

Comprobador SMTP / Cracker SMTP mejorado con soporte de proxy, prueba de bandeja de entrada y muchas más funciones.

1: <https://github.com/DrPython3/MailRipV2>

--------------------------------------

Ejecute ataques PIN de WPS (Pixie Dust, fuerza bruta en línea, predicción de PIN) sin modo monitor con wpa\_supplicant

1: <https://github.com/swagkarna/OneShot>

--------------------------------------

HERRAMIENTA PROFESIONAL ORIENTADA A LA RECREACIÓN DE ESCENARIOS DE SITIOS WEB DE PHISHING

1: <https://github.com/AngelSecurityTeam/Recreator-Phishing>

--------------------------------------

MacGeiger: una herramienta para rastrear la ubicación de puntos de acceso WiFi con sonido (similar a un contador Geiger)

1: <https://github.com/rofl0r/MacGeiger>

--------------------------------------

Generador de código PIN WPS en línea experimental para algunos dispositivos Tenda

1: <https://github.com/drygdryg/TendaOnlinePIN>

--------------------------------------

Una suite de administración remota de Android basada en la nube, impulsada por NodeJS

1: <https://github.com/bmh1cker/BMHacker-Botnet>

--------------------------------------

L3MON – Suite de gestión remota de Android

1: <https://github.com/D3VL/L3MON>

--------------------------------------

Herramienta de recuperación de contraseña para sistemas operativos de Microsoft. Permite una fácil recuperación de varios tipos de contraseñas olfateando la red, descifrando contraseñas encriptadas usando ataques de diccionario, fuerza bruta y criptoanálisis, grabando conversaciones de VoIP, decodificando contraseñas codificadas, recuperando claves de redes inalámbricas, revelando casillas de contraseñas, descubriendo…

1: https://github.com/xchwarze/Cain

--------------------------------------

Un kit de herramientas WPA/WPS todo en uno

1: https://github.com/soxrok2212/PSKracker

--------------------------------------

Paquete de herramientas de auditoría de seguridad WiFi

1: https://github.com/aircrack-ng/aircrack-ng

--------------------------------------

Repositorio de descifrado de contraseñas de Brutus

1: https://github.com/LittleBigHack/Brutus-Password-Cracker

--------------------------------------

[ECCV2020] Un conjunto de datos anti-suplantación de identidad facial a gran escala

1: <https://github.com/Davidzhangyuanhan/CelebA-Spoof>

--------------------------------------

Una herramienta de fuzzing para el ataque de suplantación de identidad del remitente de correo electrónico.👻

1: <https://github.com/mo-xiaoxi/ESpoofing>

--------------------------------------

Una herramienta de extracción y descifrado y paquete y cifrado para typora.

1: <https://github.com/mo-xiaoxi/typoraCracker>

--------------------------------------

Kit de herramientas DNSSEC para Python

1: <https://github.com/mo-xiaoxi/pydnssec>

--------------------------------------

Iconos y extensiones de archivos falsos en Windows

1: <https://github.com/henriksb/ExtensionSpoofer>

--------------------------------------

Obtenga rápidamente todas las contraseñas predeterminadas para la mayoría de los enrutadores extrayendo todos los datos de routerpasswords.com

1: https://github.com/henriksb/RouterPassword-Lookup

--------------------------------------

Omita la protección contra bots de Coudflare con Cloudflare Workers

1: <https://github.com/mo-xiaoxi/cloudflare-bypass>

--------------------------------------

Google dorks

1: <https://github.com/BullsEye0/google_dork_list.git>

--------------------------------------

Este script creado en python3 esta hecho con fines educativos (spammer de mensajes pd: no se de que espamea mensajes exactamente lo siento)

1: https://github.com/error404-notfound/spammerpy

--------------------------------------

Interfaz web para navegar, buscar y filtrar envíos recientes de arxiv

1: <https://github.com/Davidzhangyuanhan/arxiv-sanity-preserver>

--------------------------------------

¡Hagamos un seguimiento de los kits de phishing para dar a la comunidad de investigación materia prima para estudiar!

1: <https://github.com/marcoramilli/PhishingKitTracker>

--------------------------------------

Monitoreo de control de malware

1: <https://github.com/marcoramilli/malcontrol>

--------------------------------------

Herramienta de detección de hash

1: https://github.com/marcoramilli/hashdetection

--------------------------------------

Emails de forma masiva

1: <https://github.com/error404-notfound/Zica-One-v2->

--------------------------------------

Una herramienta ampliable para recopilar, rastrear y monitorear sitios de cebolla en la red tor e indexar la información recopilada en Elasticsearch

1: <https://github.com/marcoramilli/OnionIngestor>

--------------------------------------

Fuzzer de aplicaciones web

1: https://github.com/xmendez/wfuzz

--------------------------------------

Bueno, esta es una renovación de la anterior, tiene la capacidad de cambiar completamente la información del token en Discord y bloquear la cuenta del usuario y otorgarle acceso a ella y omite 2FA…

1: <https://github.com/xCutieePiee/Discordapp-TokenGrabber>

--------------------------------------

MacGeiger: una herramienta para rastrear la ubicación de puntos de acceso WIFI con sonido (similar a un contador Geiger)

1: <https://github.com/rofl0r/MacGeiger>

--------------------------------------

Script para escaneo en red y detección automática de dispositivos para NetBox

1: <https://github.com/drygdryg/netbox-device-autodiscovery>

--------------------------------------

Encuentre exploits en la base de datos local y en línea

1: <https://github.com/Err0r-ICA/Searchsploit>

--------------------------------------

🎯Evite los ataques de RubberDucky (u otra inyección de pulsaciones de teclas)

1: <https://github.com/pmsosa/duckhunt>

--------------------------------------

El repositorio oficial de carga útil USB Rubber Ducky

1: <https://github.com/hak5/usbrubberducky-payloads>

--------------------------------------

Un exploit que encontre en discord

1: https://github.com/TheonlyIcebear/Discord-Image-Logger

--------------------------------------

Ha3Mrx Pentesting y piratería de seguridad

1: <https://github.com/Ha3MrX/Hacking>

--------------------------------------

Un pin bruteforcer para roblox

1: <https://github.com/TheonlyIcebear/Roblox-Pin-Bruteforcer>

--------------------------------------

TikTok Vista masiva y compartir Boting ~ parchado

1: <https://github.com/Wizz1337/TikTokMassBotting>

--------------------------------------

Secuencia de comandos de Python simple compatible con el perfil BurpBouty que lo ayuda a detectar la inyección SQL "basada en errores" mediante el envío de múltiples solicitudes con 14 cargas útiles y la verificación de 152 patrones de expresiones regulares para diferentes bases de datos.

1: <https://github.com/eslam3kl/SQLiDetector>

--------------------------------------

Herramienta de reconocimiento de automatización que funciona con alcances grandes y medianos. Realiza más de 20 tareas y recupera todos los resultados en archivos separados.

1: <https://github.com/eslam3kl/3klCon>

--------------------------------------

Controle múltiples nodos de Bettercap a través de la API REST

1: <https://github.com/MelroyB/PSBettercap>

--------------------------------------

Ataques de desbordamiento de búfer basados ​​en pila simplificados. BufferSploit es una herramienta basada en CLI semiautomática para realizar ataques de desbordamiento de búfer basados ​​en pila con facilidad.

1: <https://github.com/adithyan-ak/BufferSploit>

--------------------------------------

Airavat es un interceptor de métricas y un supervisor de trabajos para aplicaciones Spark. También cuenta con una interfaz de usuario interactiva que muestra todas las aplicaciones Spark en ejecución, trabajos y consultas SQL junto con sus métricas.

1: <https://github.com/alivcor/airavat>

--------------------------------------

Herramienta de exfiltración de DNS para enviar archivos sigilosamente a través de solicitudes de DNS.

1: <https://github.com/m57/dnsteal>

--------------------------------------

Herramienta reflexiva DDoS de Akamai: ataque el host de origen detrás de los hosts Akamai Edge y la protección DDoS que ofrecen los servicios de Akamai.

1: <https://github.com/m57/ARDT>

--------------------------------------

Un escáner de puerto simple y rápido para cuando no puede usar Nmap en un pentest.

1: <https://github.com/m57/piescan>

--------------------------------------

Checkpoint Firewall Ruleset Auditor (Para las exportaciones de HTML cuando no tiene los archivos de objeto)

1: <https://github.com/m57/myCVT>

--------------------------------------

Araña redes enteras para archivos jugosos que se encuentran en recursos compartidos SMB. Busque nombres de archivos o contenido de archivos: ¡regex compatible!

1: <https://github.com/blacklanternsecurity/MANSPIDER>

--------------------------------------

Un proxy SOCKS escrito en Python que aleatoriza su dirección IP de origen. ¡Reparta sus paquetes malignos a través de túneles SSH o deles miles de millones de direcciones de origen únicas!

1: <https://github.com/blacklanternsecurity/TREVORproxy>

--------------------------------------

Escáner Pentesting popular en Python3.6 para SQLi/XSS/LFI/RFI y otras vulnerabilidades

1: <https://github.com/v3n0m-Scanner/V3n0M-Scanner>

--------------------------------------

Vaf es un fuzzer web multiplataforma muy avanzado y rápido escrito en nim

1: <https://github.com/d4rckh/vaf>

--------------------------------------

Troyano de acceso remoto Discord

1: <https://github.com/ch2sh/DiscoShell>

--------------------------------------

Herramienta de análisis de red

1: <https://github.com/odedshimon/BruteShark>

--------------------------------------

Una RAT de Android multifuncional con panel web basado en GUI sin reenvío de puertos.

1: <https://github.com/Th30neAnd0nly/AIRAVAT>

--------------------------------------

Gosh: un marco conectable para crear programas de shell de comando

1: <https://github.com/vladimirvivien/gosh>

--------------------------------------

WebMap-Nmap Web Dashboard and Reporting

1: <https://github.com/SabyasachiRana/WebMap>

--------------------------------------

¡Discord nitro francotirador! Reclame automáticamente Nitro en su cuenta principal usando alts para que no sature su cuenta principal con servidores

1: <https://github.com/9P9/Nitro-Sniper-v2>

--------------------------------------

🔥🌌Este repositorio contiene recursos útiles para realizar investigaciones e investigaciones OSINT sobre cuentas, servidores y bots de Discord.🌌🔥

1: <https://github.com/atoncehussein/DiscordOSINT>

--------------------------------------

Un marco de análisis forense para enumerar artefactos de holgura que residen en el sistema operativo.

1: <https://github.com/adithyan-ak/Slacksploit>

--------------------------------------

Ataques de desbordamiento de búfer basados ​​en pila simplificados. BufferSploit es una herramienta basada en CLI semiautomática para realizar ataques de desbordamiento de búfer basados ​​en pila con facilidad.

1: <https://github.com/adithyan-ak/BufferSploit>

--------------------------------------

Explotador de vulnerabilidades de aplicaciones web (OLA) es básicamente un escáner de vulnerabilidades que busca vulnerabilidades de seguridad en aplicaciones web.

1: <https://github.com/adithyan-ak/WAVE>

--------------------------------------

¡Utiliza la función de inicio de sesión QR de Discord para crear un código QR escaneable de Token Logger

1: <https://github.com/9P9/Discord-QR-Token-Logger>

--------------------------------------

Creador de fichas de discordia🥵

1: https://github.com/dropout1337/Discord-Token-Creator

--------------------------------------

Devil es una herramienta que está hecha básicamente para Facebook para hackear cuentas objetivo, BruteForce Attack, capturar cuentas de amigos, yahoo chacker, herramienta de recopilación de información de Facebook Friend, reacciones de me gusta automáticas y mucho más. Espero que disfrutes esta herramienta. No soy responsable si tú usar esta herramienta para cualquier propósito ilegal

1: <https://github.com/evildevill/Devil>

--------------------------------------

Hidra en Termux

1: <https://github.com/isuruwa/T-HYDRA>

--------------------------------------

La piratería es tu arma J

1: <https://github.com/ASU-LAB/asu-v5>

--------------------------------------

Fuerza bruta de Gmail versión 1.0

1: <https://github.com/AL-AlamySploit/Gemail-BruteForce>

--------------------------------------

Hack de gmail de fuerza b

1: <https://github.com/0xfff0800/Brute-force-gmail>

--------------------------------------

Marco para BruteForce Media liek instagram; Facebook ; twitter escribir en pitón

1: <https://github.com/Sir-wolf/media_brute>

--------------------------------------

Brutal SSH: fuerza bruta de inicio de sesión de SSH, escaneo en busca de una versión vulnerable y exploit de 0 días (en desarrollo)

1: <https://github.com/d3vilbug/Brutal_SSH>

--------------------------------------

Herramienta OSINT para obtener información de un perfil de Github y Gitlab y encontrar las direcciones de correo electrónico de los usuarios filtradas en las confirmaciones.

1: <https://github.com/GONZOsint/gitrecon>

--------------------------------------

Busque datos de geolocalización WiFi por BSSID y SSID en diferentes bases de datos públicas.

1: https://github.com/GONZOsint/geowifi

--------------------------------------

Thefatrat una herramienta de explotación masiva: herramienta fácil para generar puertas traseras y herramienta fácil para publicar ataques de explotación como ataques de navegador, etc. Esta herramienta compila un malware con una carga útil popular y luego el malware compilado se puede ejecutar en Windows, Android, Mac. El malware que se creó con esta herramienta también tiene la capacidad de eludir la mayoría de los software AV…

1: <https://github.com/screetsec/TheFatRat>

--------------------------------------

Todo en una herramienta de pirateo de Facebook para noobz.

1: <https://github.com/mkdirlove/FBTOOL>

--------------------------------------

Es un sniffer de red de Python de línea de comandos que detecta paquetes de red sin procesar.

1: <https://github.com/tejeshreddymeka/Network-packet-Sniffer>

--------------------------------------

Herramienta de ataque DHCP👿

1: <https://github.com/jacopodl/dstar>

--------------------------------------

Una aplicación GUI de seguimiento de objetivos, toma de notas, listas de verificación y gestión de datos para Bug Hunter's y Pentesters.

1: <https://github.com/tarunkoyalwar/sandman>

--------------------------------------

Una herramienta generadora de shell multiplataforma flexible y escalable

1: <https://github.com/nozerobit/gshell>

--------------------------------------

Impresionante enumerador de nubes

1: <https://github.com/0xsha/CloudBrute>

--------------------------------------

Extractor de propiedades para aplicaciones de Android

1: <https://github.com/cryptax/droidlysis>

--------------------------------------

Herramienta de exfiltración de datos y comunicación encubierta

1: https://github.com/jacopodl/pulsar

--------------------------------------

Plataforma de gestión de superficie de ataque | Sn1perSecurity LLC

1: <https://github.com/1N3/Sn1per>

--------------------------------------

Encuentre vulnerabilidades en bases de datos locales y en línea al instante

1: <https://github.com/1N3/Findsploit>

--------------------------------------

Herramientas de piratería. Fortuna de IP, mapa web: escáner de vulnerabilidades web, rtsp brute+fuzz y más.

1: <https://github.com/fagci/h4ck>

--------------------------------------

Instale Kali Linux Tools y otros en su Linux.

1: <https://github.com/i386angel/kali-my-linux>

--------------------------------------

Bot de Telegram/Discord que obtiene información sobre los jugadores de Fortnite

1: https://github.com/abhinavk99/fortnite-bot

--------------------------------------

Ahora puedes descargar las herramientas más poderosas usando este simple script

1: <https://github.com/king-hacking/King-Hacking>

--------------------------------------

Herramienta que automatiza la generación de dispositivos autenticados para varias cuentas de epicgames.

1: <https://github.com/Luc1412/EasyDeviceAuth>

--------------------------------------

Sifter: centro de operaciones de pruebas de penetración para todo uso

1: <https://github.com/whiterabb17/sifter>

--------------------------------------

SpyCore - Escáner de archivos maliciosos de Windows (distribuciones)

1: https://github.com/whiterabb17/SpyCore

--------------------------------------

ATAQUE DE RED2

1: <https://github.com/sosrepos/netattack>

--------------------------------------

Exploit webmin

1: <https://github.com/N3utr0n-FHC/Webmin-Exploits>

--------------------------------------

VULNRΞPO: generador de informes de vulnerabilidad gratuito y repositorio cifrado de extremo a extremo. Plantillas completas de incidencias, CWE, CVE, MITRE ATT&CK, PCI DSS, cifrado AES, importación de incidencias Nmap/Nessus/Burp/OpenVAS, exportación Jira, informe TXT/HTML/PDF, archivos adjuntos, registro de cambios automático, estadísticas, gestión de vulnerabilidades, informe de seguridad constructor.

1: <https://github.com/kac89/vulnrepo>

--------------------------------------

Realice OSINT en objetivos externos usando Shodan

1: https://github.com/stavinski/showdown

--------------------------------------

Generador de payloads

1: <https://github.com/N3utr0n-FHC/GenPayloads>

--------------------------------------

Un escáner de puertos súper rápido y personalizable, basado en Masscan y NMap. Escanee redes enormes y use las capacidades de secuencias de comandos de NMap para descubrir información sobre los servicios. Generar informe sencillo.

1: <https://github.com/nullt3r/jfscan>

--------------------------------------

Enumere rápidamente subdominios y dominios usando rapiddns.io.

1: <https://github.com/nullt3r/rapiddns>

--------------------------------------

❄️PcapXray: una herramienta forense de red: para visualizar una captura de paquetes fuera de línea como un diagrama de red que incluye la identificación del dispositivo, resalta la comunicación importante y la extracción de archivos

1: <https://github.com/Srinivas11789/PcapXray>

--------------------------------------

Reverse/ Concha Shell Generator para sistemas multiplataforma

1: <https://github.com/sundaysec/pwn3rGenerator>

--------------------------------------

📝urlRecon – Herramienta de recopilación o reconocimiento de información para Urls -> Recupera \* Información Whois del dominio \* Detalles DNS del dominio \* Huella digital del servidor \* Geolocalización IP del servidor

1: <https://github.com/Srinivas11789/urlRecon>

--------------------------------------

Pantalla de inicio de sesión de Windows falsa para robar contraseñas

1: <https://github.com/bitsadmin/fakelogonscreen>

--------------------------------------

Potente herramienta para tomar instantáneas de la cámara frontal usando un enlace

1: <https://github.com/kinghacker0/WishFish>

--------------------------------------

Una herramienta que le permite buscar dispositivos Android vulnerables en todo el mundo y explotarlos.

1: <https://github.com/0x1CA3/AdbNet>

--------------------------------------

HostHunter una herramienta de reconocimiento para descubrir nombres de host utilizando técnicas OSINT.

1: <https://github.com/SpiderLabs/HostHunter/>

--------------------------------------

BruteSploit es una colección de métodos para listas de palabras automatizadas de generación, fuerza bruta y manipulación con shell interactivo. Eso se puede usar durante una prueba de penetración para enumerar y tal vez se puede usar en CTF para manipular, combinar, transformar y permutar algunas palabras o texto de archivo: p

1: <https://github.com/screetsec/BruteSploit>

--------------------------------------

Encuentra números de telefono

1: <https://github.com/UltimateHackers/infinity>

Cd infinity

Python infinity.py

--------------------------------------

Esta herramienta configurará su puerta trasera/rootkits cuando la puerta trasera ya esté configurada, ocultará su proceso específico, su sesión será ilimitada en Metasploit y será transparente. Incluso cuando mató, se volverá a ejecutar. Siempre hay un proceso que mientras ejecuta otro proceso, por lo que podemos suponer que este proceso es imparable como un fantasma en el caparazón.

1: <https://github.com/screetsec/Vegile>

--------------------------------------

Carga útil para adolescentes como un patito de goma, pero la sintaxis es diferente. Este dispositivo de interfaz humana (ataques HID). Penetración con Teensy. Brutal es un conjunto de herramientas para crear rápidamente varias cargas útiles, ataques de powershell, ataques de virus y escuchas de lanzamiento para un dispositivo de interfaz humana (Payload Teensy)

1: <https://github.com/screetsec/Brutal>

--------------------------------------

Ghost Eye Informationgathering Footprinting Scanner y Recon Tool Release. Ghost Eye es una herramienta de recopilación de información que hice en python 3. Para ejecutar Ghost Eye, solo necesita un dominio o ip. Ghost Eye puede funcionar con cualquier distribución de Linux si es compatible con Python 3. Autor: Jolanda de Koff

1: <https://github.com/BullsEye0/ghost_eye>

--------------------------------------

Shodan Eye Esta herramienta recopila toda la información sobre todos los dispositivos conectados directamente a Internet utilizando las palabras clave especificadas que ingresa. Autora: Jolanda de Koff

1: https://github.com/BullsEye0/shodan-eye

--------------------------------------

John the Ripper jumbo: descifrador avanzado de contraseñas fuera de línea, que admite cientos de tipos de cifrado y hash, y se ejecuta en muchos sistemas operativos, CPU, GPU e incluso algunos FPGA

1: https://github.com/openwall/john

--------------------------------------

CamOver es una herramienta de explotación de cámara que permite revelar la contraseña de administrador de la cámara de red.

1: https://github.com/EntySec/CamOver

--------------------------------------

CamRaptor es una herramienta que explota varias vulnerabilidades en cámaras DVR populares para obtener credenciales de cámara de red.

1: <https://github.com/EntySec/CamRaptor>

--------------------------------------

Herramienta de Python para suplantar la dirección IP

1: <https://github.com/akokare/My-IP-Spoofer>

--------------------------------------

Escáner de puerto abierto de Python usando sockets integrados

1: <https://github.com/akokare/Python-Port-Scanner>

--------------------------------------

Envío de ping icmp con una IP falsificada usando un socket sin procesar de Unix

1: https://github.com/Subangkar/ICMP-Ping-Spoofing

--------------------------------------

Un ejemplo de cómo falsificar direcciones IP en paquetes

1: https://github.com/pullrequestrfb/ip-spoof-example

--------------------------------------

Implementación de suplantación de identidad IP: ataque pitufo

1: <https://github.com/idobhh/IP-Spoofing>

--------------------------------------

El cifrado bífido alfanumérico que incluye cifrados y descifrados.

1: <https://github.com/ReinaldoDiasAbreu/BifidCipher>

--------------------------------------

📦Herramientas de ataques inalámbricos🕷️

1: <https://github.com/oanderoficial/wiresec>

--------------------------------------

Programa de Python que realiza reconocimiento de voz utilizando la biblioteca SpeechRecognition y pyttsx3 para texto a voz, junto con el navegador web para abrir el resultado en el navegador. El programa busca automáticamente Bitcoin, Mempool, Arbitrage, Cryptocurrency Quotes, etc. Uso de comandos de voz predefinidos.

1: <https://github.com/oanderoficial/reconhecimento-de-voz>

--------------------------------------

Framework diseñado para automatizar varios ataques a redes inalámbricas (el proyecto se presentó en la caja de herramientas de Pentester Academy TV en 2017).

1: <https://github.com/AresS31/wirespy.git>

--------------------------------------

Code Talker puede ser utilizado para criptografiar y descriptografiar mensajes utilizando uma chave previamente definida para el usuario. A chave debe ter apenas 4 caracteres numéricos.

1: <https://github.com/gushpat/code-talker>

--------------------------------------

Hoy hackearemos el panel de administración del sitio.

1: <https://github.com/mishakorzik/AdminHack>

--------------------------------------

Instalador automático de herramientas de hacking para Android [SOLO PARA TERMUX]

1: <https://github.com/AnonHackerr/toolss>

--------------------------------------

MÁS DE 300 HERRAMIENTAS EN 1 HERRAMIENTA

1: <https://github.com/TUANB4DUT/TOOLSINSTALLERV3>

--------------------------------------

🔎El marco de inteligencia de código abierto más avanzado (OSINT) para escanear direcciones IP, correos electrónicos, sitios web, organizaciones.

1: https://github.com/bhavsec/reconspider

--------------------------------------

ShotDroid es una herramienta de pentesting para Android. Hay 3 herramientas que tienen sus respectivas funciones, obtener archivos del directorio de Android, almacenamiento interno y externo, Android Keylogger + Reverse Shell y tomar una foto de cámara web de la cara desde la cámara frontal del teléfono y la PC.

1: <https://github.com/kp300/shotdroid>

--------------------------------------

Este script instala automáticamente cualquier paquete para pentest con herramientas actualizadas y un comando perezoso para ejecutar herramientas como lazynmap, instala otro y actualiza a nuevo instrumentos . Es compatible con la última versión de Kali (Rolling)

1: https://github.com/screetsec/LALIN

--------------------------------------

Consola de marco de prueba de drones

1: <https://github.com/dhondta/dronesploit>

--------------------------------------

Herramienta todo en uno para la recopilación de información, el análisis de vulnerabilidades y el rastreo. Una herramienta imprescindible para todos los probadores de penetración.

1: <https://github.com/Tuhinshubhra/RED_HAWK>

--------------------------------------

La herramienta realiza el ataque y la defensa del gemelo malvado.

1: <https://github.com/vection/Evil-Twin-tool>

--------------------------------------

Phishing avanzada con creacion propia de página por ejemplo <https://pavosgratis.com> (borraron el repositorio por el uso que se le pudiese dar por cierto puedes hacer cualquier página osea el programa accede a algún sitio de compró de dominios compra el dominio y lo transforma en página de phishing pd: no se si algúna persona ha guardado el Código fuente y implementado en otro programa)

1: <https://github.com/thelinuxchoice/formphish>

cd formphish

bash formphish.sh

--------------------------------------

)(.

1: <https://github.com/rebellionil/tornado>

--------------------------------------

Genere máscaras de destellos para imágenes RGB

1: https://github.com/HakaiInstitute/GlintMaskGenerator

--------------------------------------

Generación de carga útil

1: <https://github.com/Hackingvisionofficial/splotgen>

--------------------------------------

Una secuencia de comandos de Python para generar cargas útiles que pasa por alto todos los antivirus hasta el momento.

1: <https://github.com/stormshadow07/HackTheWorld>

--------------------------------------

Varias herramientas para trabajar con máscara y partes ocultas en Blender 2.8 en modo Sculpt

1: <https://github.com/Mysmallscripts/Mask-T>

--------------------------------------

Una herramienta para enmascarar sus datos a simple vista

1: <https://github.com/TryCatchHCF/Cloakify.git>

--------------------------------------

Marco C2 con todas las funciones que persiste silenciosamente en el servidor web con una puerta trasera PHP de una sola línea

1: <https://github.com/nil0x42/phpsploit>

--------------------------------------

Chimera es un script de ofuscación de PowerShell diseñado para eludir AMSI y las soluciones antivirus comerciales.

1: <https://github.com/tokyoneon/chimera>

--------------------------------------

PortForce: una herramienta de fuerza bruta de puerto personalizado para CTF y Pentest

1: https://github.com/jhalon/PortForce

--------------------------------------

WAFW00F permite identificar y tomar huellas dactilares de los productos de firewall de aplicaciones web (WAF) que protegen un sitio web.

1: <https://github.com/EnableSecurity/wafw00f>

--------------------------------------

Utilidad de línea de comandos para buscar y descargar exploits

1: <https://github.com/vulnersCom/getsploit>

--------------------------------------

EasySploit – Automatización de Metasploit (MÁS FÁCIL y MÁS RÁPIDO que NUNCA)

1: https://github.com/KALILINUXTRICKSYT/easysploit

--------------------------------------

El script LAZY te hará la vida más fácil y, por supuesto, más rápida.

1: <https://github.com/arismelachroinos/lscript>

--------------------------------------

Detección automática y explotación de CMS.

1: https://github.com/MrSqar-Ye/BadMod.git

--------------------------------------

🔐 Criptografia RSA

1: <https://github.com/araujogabriel77/Projeto-RSA>

--------------------------------------

Fuerza bruta de DNS de subdominio simple en Python

1: <https://github.com/araujogabriel77/dnsbrute>

--------------------------------------

Marco para ataques Man-In-The-Middle

1: <https://github.com/byt3bl33d3r/MITMf>

--------------------------------------

Una lista de payloads útiles y bypass para Web Application Security y Pentest/CTF

1: <https://github.com/swisskyrepo/PayloadsAllTheThings>

--------------------------------------

Acceda a ADB en navegadores (:

1: <https://github.com/jxroot/adbwebkit>

--------------------------------------

Pentesting Framework es un paquete de herramientas de prueba de penetración que incluye: seguridad, pentesting, piratería y muchas más.

1: https://github.com/abhackerofficial/pentesting-framework

--------------------------------------

Este Script te ayudará a recopilar información sobre tu víctima o amigo.

1: https://github.com/Deadshot0x7/007-TheBond

--------------------------------------

Este script lo ayudará a encontrar la información sobre el sitio web y a ayudar en las pruebas de penetración.

1: https://github.com/Deadshot0x7/Webspoilt

--------------------------------------

T-load

1: https://github.com/ExpertAnonymous/T-LOAD

--------------------------------------

MgToLs mas de 80 herramientas de hacking para la gran mayoria de ataques.

1: <https://github.com/NePtYx2018/MgToLs>

--------------------------------------

👶BabySploit Beginner Pentesting Toolkit/Framework escrito en Python🐍

1: <https://github.com/M4cs/BabySploit>

--------------------------------------

GPT-2 Discord Bot y pasos para entrenar algo como tú

1: <https://github.com/M4cs/yourAI>

--------------------------------------

Herramienta de recopilación de información

1: https://github.com/R3dy/jigsaw

--------------------------------------

Entorno Vagrant VirtualBox para realizar una prueba de penetración de red interna

1: https://github.com/R3dy/capsulecorp-pentest

--------------------------------------

Una herramienta que encuentra, enumera y explota cámaras Reolink.

1: https://github.com/spicesouls/reosploit

--------------------------------------

¡Tu práctica navaja suiza Cyber ​​Dandy!

1: https://github.com/spicesouls/spicescript2

--------------------------------------

Herramientas de piratería. Fortuna de IP, mapa web: escáner de vulnerabilidades web, rtsp brute+fuzz y más.

1: https://github.com/fagci/h4ck

--------------------------------------

💌Encuentra la dirección de correo electrónico de cualquier persona

1: https://github.com/krmbzds/guessmail

--------------------------------------

Bienvenido a la página donde encontrarás cada truco/técnica/lo que sea que he aprendido en CTFs, aplicaciones de la vida real, y leyendo investigaciones y noticias.

1: <https://github.com/carlospolop/hacktricks>

--------------------------------------

HTTP Header Spy le permite inspeccionar encabezados de solicitud-respuesta y cookies justo después de cargar la página sin clics adicionales.

1: https://github.com/Tuurlijk/HTTP-Header-Spy

--------------------------------------

Terminal Android SSH y aplicación de transferencia de archivos

1: <https://github.com/marcb1/droid-ssh>

--------------------------------------

Busque un shell de puerta trasera en el sitio web

1: <https://github.com/Rhi7/shell-scan>

--------------------------------------

Vuelca todos los correos electrónicos de tus amigos en Facebook

1: https://github.com/warifp/FacebookEmailDumpper

--------------------------------------

APKinspector es una poderosa herramienta GUI para que los analistas analicen las aplicaciones de Android.

1: <https://github.com/honeynet/apkinspector>

--------------------------------------

Una herramienta para obtener datos de Facebook, y algunos bots de Facebook, y herramientas adicionales que se encuentran en Facebook Toolkit ++.

1: <https://github.com/warifp/FacebookToolkit>

--------------------------------------

Kit de herramientas de detección de suplantación de identidad LLMNR/NBNS/mDNS

1: <https://github.com/Rushyo/VindicateTool>

--------------------------------------

Certbot es la herramienta de EFF para obtener certificados de Let’s Encrypt y (opcionalmente) habilitar automáticamente HTTPS en su servidor. También puede actuar como cliente de cualquier otra CA que utilice el protocolo ACME.

1: https://github.com/certbot/certbot

--------------------------------------

JPEXS Free Flash Descompilador

1: https://github.com/jindrapetrik/jpexs-decompiler

--------------------------------------

Spotify es un servicio de transmisión de música digital, hice varias herramientas para ti.

1: https://github.com/warifp/SpotifyToolkit

--------------------------------------

cSploit: el conjunto de herramientas profesional de seguridad de TI más completo y avanzado en Android.

1: <https://github.com/cSploit/android>

--------------------------------------

Generador de claves FaceNiff

1: https://github.com/ricardoteixas/faceniffkey

--------------------------------------

Herramienta de red hping

1: https://github.com/antirez/hping

--------------------------------------

Este programa comprueba localmente si hay signos de un rootkit. ‘Bifurcado’ para corregir falsos positivos para el rootkit SucKIT

1: https://github.com/Magentron/chkrootkit

--------------------------------------

Scripts para hacer que los ataques de rociado de contraseñas contra Lync/S4B, OWA y O365 sean mucho más rápidos, menos dolorosos y más eficientes

1: https://github.com/byt3bl33d3r/SprayingToolkit

--------------------------------------

Una herramienta basada en Python para explotar y administrar dispositivos Android a través de ADB

1: <https://github.com/mesquidar/adbsploit>

--------------------------------------

Cree un troyano de Android 100% FUD y omita todos los antivirus + Android Google Play Protector

1: <https://github.com/erfan4lx/Android-Trojan-FUD-Crypter>

--------------------------------------

Armas de hackers móviles / Una colección de herramientas geniales utilizadas por hackers móviles. Feliz piratería, feliz caza de errores

1: https://github.com/hahwul/MobileHackersWeapons

--------------------------------------

SPY BOMB es una herramienta utilizada para generar varias cargas útiles para Android, Windows, iOS, Mac y muchos más. Es una herramienta muy fácil de usar.

1: https://github.com/BYTEHACKING-CREATIVE/SPYBOMB

--------------------------------------

Ghost Framework es un marco de post-explotación de Android que explota el puente de depuración de Android para acceder de forma remota a un dispositivo Android.

1: https://github.com/EntySec/Ghost

--------------------------------------

Una herramienta bruta de dominio rápido

1: https://github.com/Q2h1Cg/dnsbrute

--------------------------------------

🔒Cliente para GnuPG – Criptografia Asimétrica (mejor criptografía programa)

1: <https://github.com/oanderoficial/AutoCrypto>

--------------------------------------

Herramienta de piratería todo en uno para Linux y Android (Termux). Convierta su entorno Linux en una máquina de piratería. Los hackers son bienvenidos en nuestro blog.

1: https://github.com/jaykali/hackerpro

--------------------------------------

Un exploit y una demostración sobre cómo explotar una vulnerabilidad XSS almacenada en <https://anonstress.com> .

1: <https://github.com/0x1CA3/AnonStress-Stored-XSS-Exploit>

--------------------------------------

# Solo un programa simple para falsificar el dispositivo enviando un enlace malicioso

1: <https://github.com/FajarTheGGman/PhoneSpoofing>

--------------------------------------

Nginx Block Bad Bots, Spam Referrer Blocker, Escáneres de vulnerabilidades, Agentes de usuario, Malware, Adware, Ransomware, Sitios maliciosos, con anti-DDOS, Bloqueo de detectores de temas de Wordpress y Fail2Ban Jail para reincidentes

1: <https://github.com/mitchellkrogza/nginx-ultimate-bad-bot-blocker>

--------------------------------------

Dominios de phishing, sitios web de urls y base de datos de amenazas. Usamos la herramienta de prueba PyFunceble para validar el estado de todos los dominios de phishing conocidos y proporcionamos estadísticas para revelar cuántos dominios únicos utilizados para phishing todavía están activos.

1: <https://github.com/mitchellkrogza/Phishing.Database>

--------------------------------------

🔥CHAOS es una herramienta de administración remota gratuita y de código abierto que permite generar binarios para controlar sistemas operativos remotos.

1: <https://github.com/tiagorlampert/CHAOS>

--------------------------------------

Verificador de cuenta multiherramienta 2020

1: <https://github.com/pwn0sec/PwnChecker>

--------------------------------------

Shalfa es una herramienta sencilla que te ayuda a extraer URL.

1: <https://github.com/pwn0sec/Pwnscan>

--------------------------------------

Multiherramienta avanzada de Discord creada por ig: g3\_ruben.\_.fuenla\_esta multiherramienta tiene muchas cosas avanzadas/de pago, ¡pero he hecho que la mía sea gratis! (GANG Nuker)

1: https://github.com/TT-Tutorials/GANG-Nuker

--------------------------------------

Un token nuker de discord Con un montón de opciones que arruinarán una cuenta realmente mal, también tiene un informe masivo incorporado, GroupChat Spammer y Token / Contraseña / Capturador de tarjetas de crédito ¡y mucho más!

1: https://github.com/Rdimo/Hazard-Nuker

--------------------------------------

👁️(s)AINT es un generador de spyware para sistemas Windows escrito en Java.

1: <https://github.com/tiagorlampert/sAINT>

--------------------------------------

⚡Esta aplicación proporciona una forma rápida y sencilla de verificar si su dispositivo Android está rooteado, con solo un clic.

1: <https://github.com/tiagorlampert/RootChecker>

--------------------------------------

Un spyware troyano sigiloso

1: <https://github.com/MinhasKamal/TrojanCockroach>

--------------------------------------

Troyano🐍(registrador de teclas, toma capturas de pantalla, abre tu cámara web)🔓

1: <https://github.com/HouariZegai/SpyGen>

--------------------------------------

¡Instala las herramientas y comienza a atacar, black-tool v5.0!⬛

1: <https://github.com/mrprogrammer2938/Black-Tool>

--------------------------------------

Black DataBase – Conector de base de datos

1: https://github.com/mrprogrammer2938/Black-Database

--------------------------------------

Pupy es una herramienta de administración remota y posexplotación de código abierto y multiplataforma (Windows, Linux, OSX, Android) escrita principalmente en python.

1: https://github.com/n1nj4sec/pupy

--------------------------------------

🎯Lista de cargas útiles de vulnerabilidades de Cross Site Scripting ( XSS )

1: https://github.com/payloadbox/xss-payload-list

--------------------------------------

Una herramienta que le permite buscar dispositivos Android vulnerables en todo el mundo y explotarlos.

1: https://github.com/0x1CA3/AdbNet

--------------------------------------

Hoja de trucos de DDoS y una herramienta DDoS de protocolo de enlace de tres vías falsificada de TCP

1: https://github.com/unregistered436/DDoS

--------------------------------------

HatVenom es una poderosa herramienta de generación de carga útil nativa de HatSploit que brinda soporte para todas las plataformas y arquitecturas comunes.

1: <https://github.com/EntySec/HatVenom>

--------------------------------------

La mejor herramienta para aumentar los seguidores de Instagram.

1: <https://github.com/termuxprofessor/insfollow>

--------------------------------------

Herramienta de recopilación de información escrita por Python.

1: <https://github.com/ultrasecurity/webkiller>

--------------------------------------

Twitter BruteForcer multihilo en Shell script

1: <https://github.com/Mehran/tweetshell>

--------------------------------------

Aplicación FW o Firewall Habilitar y Deshabilitar

1: <https://github.com/Pericena/Firewall>

--------------------------------------

El programa esta desarrollado en bat y en powershell su objetivo es extraer la contraseña he information de red que tiene un pc ya sea manualmente o automaticamente Solo las contraseñas guardadas de la pc ,puedes guardar el programa en un USB y ejecutarlo de ahí mismo. O usar diversas tecnicas de ingenieria social para poder obtener las claves…

1: <https://github.com/Pericena/HackWifi>

--------------------------------------

Vamos a realizar los primeros pasos para implementar un cortafuegos en un nodo de una red, aquel que se ejecuta en el propio equipo que trata de proteger, lo que a veces se denomina un cortafuegos personal.

1: https://github.com/MoralG/Cortafuego\_Personal

--------------------------------------

WhatScriptApp es un programa que nos ayuda a hacer spam masivo, el proyecto lo realizó mas que todo para marketing digital cuando quieres enviar un anuncio a cada usuario de la empresa o un cliente. También puedes usar para hacer ataques masivos que hoy en día hay legiones que se encargan de atacar a grupos inapropiados.

1: <https://github.com/Pericena/WhatScriptApp>

--------------------------------------

Hackear con pdf

<https://github.com/thelinuxchoice/evilpdf>

--------------------------------------

Diapositivas, documentos o cualquier cosa para REW-sploit

1: https://github.com/REW-sploit/REW-sploit\_docs

--------------------------------------

Creación rápida y fácil de explotación de backdoor office utilizando el paquete de metaploit del módulo, Microsoft Office, Open Office, ataque macro, desbordamiento de búfer

1: <https://github.com/screetsec/Microsploit>

--------------------------------------

Script de herramientas de piratería de Facebook súper rápido y fácil de usar

1: <https://github.com/fikrado/fikrado.py>

--------------------------------------

Herramienta OSINT de la Web Oscura

1: <https://github.com/DedSecInside/TorBot>

--------------------------------------

Herramientas para la caza de errores

1: <https://github.com/thehackingsage/bughunter>

--------------------------------------

Sable de luz

1: <https://github.com/thehackingsage/lightsaber>

--------------------------------------

Pentesting usando Android

1: <https://github.com/thehackingsage/hackdroid>

--------------------------------------

Brute.

1: <https://github.com/aprilahijriyan/w3brute.git>

--------------------------------------

Herramientas para Pentesting

1: <https://github.com/thehackingsage/hacktronian>

--------------------------------------

Shodan Eye Esta herramienta recopila toda la información sobre todos los dispositivos conectados directamente a Internet utilizando las palabras clave especificadas que ingresa. Autora: Jolanda de Koff

1: <https://github.com/BullsEye0/shodan-eye>

--------------------------------------

Una herramienta OSINT CLI diseñada para realizar un seguimiento rápido de la reputación de IP y la búsqueda de ubicación geográfica para los analistas de seguridad.

1: https://github.com/radioactivetobi/geo-recon

--------------------------------------

¡?

1: <https://github.com/thelinuxchoice/inshackle>

--------------------------------------

Ladon para Cobalt Strike & Cracked Download, Escáner de penetración de red grande, vulnerabilidad/exploit/detección/MS17010/contraseña/brute-force/psexec/atexec/sshexec/webshell/smbexec/netcat/osscan/netscan/struts2Poc/weblogicExp

1: <https://github.com/k8gege/Aggressor>

--------------------------------------

Escáner de penetración de red Ladon para PowerShell, vulnerabilidad/aprovechamiento/detección/MS17010/SmbGhost,Brute-Force SMB/IPC/WMI/NBT/SSH/FTP/MSSQL/MYSQL/ORACLE/VNC

1: <https://github.com/k8gege/PowerLadon>

--------------------------------------

Escáner Ladon para Python, Escáner de penetración de red grande y Cobalt Strike, vulnerabilidad/aprovechamiento/detección/MS17010/SmbGhost/CVE-2020-0796/CVE-2018-2894

1: <https://github.com/k8gege/PyLadon>

--------------------------------------

Envíe un bombardero de correo electrónico de forma anónima utilizando su cuenta de Yahoo o Gmail

1: <https://github.com/stormshadow07/Email-Bomb>

--------------------------------------

Pequeña puerta trasera usando cookie.

1: <https://github.com/jofpin/backcookie>

--------------------------------------

Generador en vivo

1: https://github.com/Scorpio28-Oficial/Live-Generator

--------------------------------------

Generador de enlaces a través de una URL

1: <https://github.com/drorganvidez/link-generator>

--------------------------------------

#Attaks-Ddos ataque de negación de servicio. Antes de usar esta herramienta primero debe encontrar la dirección IP de la víctima y escanear dónde está abierto el puerto #Note Esta herramienta es sólo como aprender para los ataques DOS & DDOS recuerden que sí, ddos son sólo una pequeña parte y muy pequeño del mundo de la piratería, así que no se …

1: <https://github.com/Scorpio28-Oficial/Attaks-Ddos>

--------------------------------------

Generar virus en Termux. Z Virus es una colección de virus ready made que se puede enviar a su víctima utilizando el enlace. Aquellos que no saben cómo usar VCRT, VBug o VBug Mapa.

1: https://github.com/Scorpio28-Oficial/zVirus-Gen

--------------------------------------

XERXES la herramienta Ddos más potente.

1: <https://github.com/Scorpio28-Oficial/XERXES>

--------------------------------------

Nunca jamás utilices la pixelación como técnica de redacción. (Despixelear fotos

1: <https://github.com/bishopfox/unredacter>

--------------------------------------

Conjunto de herramienta fundamentales para reversa/analisis/cracking

1: https://github.com/indetectables-net/toolkit

--------------------------------------

Banner-Login es una herramienta creada en bash, cuya función es un inicio de sesión para poder acceder a la terminal mediante un nombre de usuario (clave de acceso) y evitar el acceso de intrusos.

1: https://github.com/Scorpio28-Oficial/Banner-Login

--------------------------------------

Quack-Toolkit (proyecto entynet)

1: https://github.com/Scorpio28-Oficial/quack

--------------------------------------

Generador de certificados para eventos

1: https://github.com/horaciochacon/certificate-generator

--------------------------------------

Programa generador de números de cédula (DNI en otros paises) válidos en el pais, el fin es obtener un diccionario para ataques de fuerza bruta.

1: <https://github.com/daniel-alejandro-t/generadorcedulas>

--------------------------------------

Comandos de voz inaudibles

1: <https://github.com/USSLab/DolphinAttack>

--------------------------------------

Inyectar voces a micrófonos a través de condensadores

1: <https://github.com/USSLab/CapSpeaker>

--------------------------------------

Herramienta de red hping

1: <https://github.com/antirez/hping>

--------------------------------------

Proyecto upstream ← → Distribución downstream

1: <https://github.com/packit/packit>

--------------------------------------

Creador de carga útil de MSFvenom (MSFPC)

1: https://github.com/g0tmi1k/msfpc

--------------------------------------

Herramienta OSINT para encontrar contraseñas de direcciones de correo electrónico comprometidas

1: https://github.com/thewhiteh4t/pwnedOrNot

--------------------------------------

Investigación sobre vectores de amplificación UDP/TCP, payloads y mitigaciones contra su uso en ataques DDoS

1: https://github.com/Phenomite/AMP-Research

--------------------------------------

Herramienta de amplificación DRDoS UDP

1: https://github.com/daniel0x00/r2dr2-udp-drdos-tool

--------------------------------------

Una utilidad de creación e inyección de paquetes de red de línea de comandos

1: https://github.com/libnet/nemesis

--------------------------------------

Algunos buenos trucos para hacer clic en las cookies

1: https://github.com/JadeGrey/CookieClickerHacking

--------------------------------------

Carga automáticamente las cookies robadas de ChromePass

1: https://github.com/darkarp/autocookie

--------------------------------------

HHVM y Hack Cookies para facebook/hack-http-request-response-interfaces

1: https://github.com/ytake/hack-cookie

--------------------------------------

Suite EternalBlue rehecha en C/C++ que incluye: MS17-010 Exploit, detector de vulnerabilidad EternalBlue, detector DoublePulsar y DoublePulsar Shellcode & DLL uploader

1: https://github.com/bhassani/EternalBlueC

--------------------------------------

Crackear la pantalla de bloqueo de la interfaz, Metasploit y más piratería de Android/IOS

1: <https://github.com/tegal1337/CiLocks>

--------------------------------------

Exploit Exploits binarios de la base de datos ubicados en el directorio /sploits

1: https://github.com/offensive-security/exploitdb-bin-sploits

--------------------------------------

Rastreador de IP real Cloudflare, Sucuri, Incapsula.

1: https://github.com/mrh0wl/Cloudmare

--------------------------------------

Una secuencia de comandos de Python para generar cargas útiles que pasa por alto todos los antivirus hasta el momento.

1: https://github.com/stormshadow07/HackTheWorld

--------------------------------------

🔓Deshabilite la verificación SSL y la fijación en Android, en todo el sistema

1: https://github.com/ViRb3/TrustMeAlready

--------------------------------------

Una herramienta que detecta las vulnerabilidades de escalada de privilegios causadas por configuraciones incorrectas y actualizaciones faltantes en los sistemas operativos Windows.

1: https://github.com/hlldz/dazzleUP

--------------------------------------

Cargador, generador de cuentagotas con múltiples funciones para eludir las contramedidas del lado del cliente y del lado de la red.

1: <https://github.com/hlldz/SpookFlare>

--------------------------------------

IP-Biter: el marco de seguimiento de correo electrónico compatible con piratas informáticos (pero no solo)

1: <https://github.com/damianofalcioni/IP-Biter>

--------------------------------------

Trojan Rat Builder(310), Ransomware Builder(17), Crypter(72), Miner(9), Worm(8), Botnet(25), Virus Builder(9), Binder(25), Exploit(7), Keylogger & Stealer(40), Proxy Tool(9), Spoofer(11), Programa falso y Virus de muestra(64),Otros y herramientas(16). Alrededor de 𝟔𝟑𝟎 herramientas, que puedes usar para Hackear.

1: <https://github.com/HackerTBack-supporter/Hacking-Tools-Pack>

--------------------------------------

¡La gran herramienta es para instalar todas las herramientas de piratería y seguridad!

1: https://github.com/mrprogrammer2938/Big-Tool

--------------------------------------

Alfabeto de piratas informáticos. Letras Hacker para Diversão. Muto usado em Foros y Chats. Letras con fáciles entendimientos y con teclas de activación para activación y desactivación.

1: https://github.com/Romulo-Meirelles/Hacker-Alphabet-Letters

--------------------------------------

HackToolKit

1: <https://github.com/ByCh4n/BCHackTool>

--------------------------------------

Un spyware troyano sigiloso

1: https://github.com/MinhasKamal/TrojanCockroach

--------------------------------------

Un potente kit de herramientas para hackers recopiló más de 10 categorías de escáneres de código abierto de Github

1: https://github.com/We5ter/Scanners-Box

--------------------------------------

Generación de carga útil de Windows indetectable

1: <https://github.com/nccgroup/Winpayloads>

--------------------------------------

🔓Descifra hashes utilizando los servicios de ataque de tabla de búsqueda y arcoíris en línea, directamente desde tu terminal.

1: <https://github.com/k4m4/dcipher-cli>

--------------------------------------

Acelera los ataques de diccionario en hashes NETLMv1/MSCHAPv2 mediante el uso de una técnica híbrida de fuerza bruta parcial/tabla arcoíris

1: <https://github.com/tehrhart/challenger>

--------------------------------------

Escáner SQL rápido, Dorker, inyector Webshell PHP

1: <https://github.com/Cvar1984/sqlscan>

--------------------------------------

Herramientas de piratería

1: <https://github.com/B012ED/Deface>

--------------------------------------

Rastrear y monitorear direcciones MAC en su LAN

1: https://github.com/curtis86/mactrack

--------------------------------------

Hackear sitios web que son vulnerables a SQLI

1: https://github.com/navin-hariharan/WEB-DEFACE

--------------------------------------

Guía de pruebas de penetración basada en OWASP que incluye casos de prueba, recursos y ejemplos.

1: https://github.com/Voorivex/pentest-guide

--------------------------------------

Herramienta OSINT para encontrar correos electrónicos violados, bases de datos, pastas e información relevante

1: <https://github.com/Ekultek/WhatBreach>

--------------------------------------

Escanee en busca de cubos S3 abiertos y descargue el contenido

1: <https://github.com/sa7mon/S3Scanner>

--------------------------------------

Herramienta de reconocimiento todo en uno, rápida y sencilla

1: https://github.com/aufzayed/HydraRec

--------------------------------------

Una forma flexible de buscar direcciones IP para nombres de host y URL

1: https://github.com/pbnj/host-to-ip

--------------------------------------

Striker es un escáner de vulnerabilidades e información ofensiva.

1: https://github.com/s0md3v/Striker

--------------------------------------

Genere rápidamente direcciones URL protegidas con contraseña en Apache

1: https://github.com/curtis86/secure-share

--------------------------------------

Detectar y eludir los cortafuegos de aplicaciones web y los sistemas de protección

1: https://github.com/Ekultek/WhatWaf

--------------------------------------

Linux动态链接库的注入修改查找工具 Una herramienta para inyección, modificación y búsqueda de la biblioteca de enlaces dinámicos de Linux

1: https://github.com/esrrhs/hookso

--------------------------------------

Pingtunnel es una herramienta que envía tráfico TCP/UDP sobre ICMP

1: https://github.com/esrrhs/pingtunnel

--------------------------------------

Evitar los muros de pago para Firefox

1: <https://github.com/iamadamdev/bypass-paywalls-firefox>

--------------------------------------

Ensamblaje de herramientas K8 (penetración de red interna/herramienta de suministro/desbordamiento de distancia/uso de túnel de fuga/herramienta de dibujo/craqueo secreto/herramienta que no mata / EXPROIT / APT / 0DAY / STARCHODE / Payload / Priviledge / ByPassuac / OverFlow / WebShell / Pentest) Web Getshell Explotar (Struts2/Zimbra/Weblogic/Tomcat/Apache/Jboss/DotNetNuke/zabbix)

1: <https://github.com/k8gege/K8tools>

--------------------------------------

#Super-dracOS Dracos Linux es un sistema operativo de código abierto que proporciona pruebas de penetración. Equipado con una tonelada de herramientas de pentest que incluyen recopilación de información, análisis forense, análisis de malware, mantenimiento de acceso e ingeniería inversa.

1: https://github.com/screetsec/super-dracos

--------------------------------------

Carga útil para adolescentes como un patito de goma, pero la sintaxis es diferente. Este dispositivo de interfaz humana (ataques HID). Penetración con teensy

1: https://github.com/screetsec/Pateensy

--------------------------------------

Este script instala automáticamente cualquier paquete para pentest con herramientas actualizadas y un comando perezoso para ejecutar herramientas como lazynmap, instala otro y actualiza a nuevo instrumentos . Es compatible con la última versión de Kali (Rolling)

1: https://github.com/screetsec/LALIN

--------------------------------------

Dracnmap es un programa de código abierto que se utiliza para explotar la red y recopilar información con la ayuda de nmap. El comando Nmap viene con muchas opciones que pueden hacer que la utilidad sea más robusta y difícil de seguir para los nuevos usuarios. Por lo tanto, Dracnmap está diseñado para realizar un escaneo rápido con el motor de secuencias de comandos de nmap y nmap puede realizar va…

1: https://github.com/screetsec/Dracnmap

--------------------------------------

imR0T: envíe un mensaje rápido con cifrado de texto simple a su contacto de WhatsApp y proteja su texto cifrando y descifrando, básicamente en ROT13 con un nuevo algoritmo basado en cifrado múltiple en ASCII y sustitución de símbolos

1: <https://github.com/screetsec/imR0T>

--------------------------------------

Herramienta OSINT en Twitter e Instagram.

1: <https://github.com/xadhrit/terra>

--------------------------------------

Escáner de vulnerabilidades xss y herramienta de fuzzing de entrada.

1: <https://github.com/xadhrit/xira>

--------------------------------------

Escáner de red con detección de puerta trasera, otros recursos de Nmap y detección de protección de sincronización

1: <https://github.com/xadhrit/d9scan>

--------------------------------------

Depurador .NET y editor de ensamblados

1: <https://github.com/xadhrit/dnSpy/pulls>

--------------------------------------

ISeeYou es una herramienta de Bash y Javascript para encontrar la ubicación exacta de los usuarios durante los compromisos de ingeniería social o phishing. Usando las coordenadas de ubicación exactas, un atacante puede realizar un reconocimiento preliminar que lo ayudará a realizar más ataques dirigidos.

1: <https://github.com/Viralmaniar/I-See-You>

--------------------------------------

Passhunt es una herramienta simple para buscar credenciales predeterminadas para dispositivos de red, aplicaciones web y más. Busque a través de 523 proveedores y sus 2084 contraseñas predeterminadas.

1: <https://github.com/Viralmaniar/Passhunt>

--------------------------------------

La herramienta BigBountyRecon utiliza 58 técnicas diferentes utilizando varios tontos de Google y herramientas de código abierto para acelerar el proceso de reconocimiento inicial de la organización objetivo.

1: https://github.com/Viralmaniar/BigBountyRecon

--------------------------------------

Herramienta de Python que automatiza el proceso de investigación de Twitter OSiNT usando twint.

1: <https://github.com/falkensmz/tw1tter0s1nt>

--------------------------------------

Esta es una herramienta de código abierto para volcar los perfiles wifi y las contraseñas de texto claro de los puntos de acceso conectados en la máquina con Windows. Esta herramienta te ayudará en una prueba de penetración Wifi. Además, es útil al realizar compromisos de equipo rojo o de infraestructura interna.

1: <https://github.com/Viralmaniar/Wifi-Dumper>

--------------------------------------

Esta herramienta permite recuperar información de sesión RDP (mstsc) antigua en forma de archivos PNG rotos. Estos archivos PNG permiten a los miembros del Red Team extraer información jugosa, como contraseñas de LAPS o cualquier información confidencial en la pantalla. El miembro del Blue Team puede reconstruir archivos PNG para ver qué hizo un atacante en un host comprometido. Es extremadamente u…

1: <https://github.com/Viralmaniar/Remote-Desktop-Caching->

--------------------------------------

Kaumodaki es una herramienta que tiene una colección de todas las herramientas de piratería populares en un solo lugar.

1: <https://github.com/CybSec-NITW/kaumodaki>

--------------------------------------

Obtenga todas sus herramientas favoritas en un solo clic

1: https://github.com/Abdulrah33m/Cl0neMast3r

--------------------------------------

Una herramienta avanzada de raspado de Twitter y OSINT escrita en Python que no utiliza la API de Twitter, lo que le permite raspar los seguidores, seguidores, tweets y más de un usuario mientras evade la mayoría de las limitaciones de la API.

1: <https://github.com/twintproject/twint>

--------------------------------------

Herramienta para minería avanzada de contenido en Github

1: <https://github.com/UnkL4b/GitMiner>

--------------------------------------

La piratería es tu arma J

1: https://github.com/ASU-LAB/asu-v5

--------------------------------------

Capture, reaccione y comparta sus reacciones Usando ambas cámaras del móvil, una para capturar imágenes y la otra para registrar su reacción facial.

1: <https://github.com/xadhrit/reactions>

--------------------------------------

Mejor herramienta para hackear a través de windows 1: cmdhttps://github.com/edmark21/FishCracker

--------------------------------------

Un FortniteLauncher personalizado que puede evitar la fijación de SSL (y anti-trampas, más o menos).

1: <https://github.com/EZFNDEV/FortniteLauncher>

--------------------------------------

Omita la extensión del navegador web Paywalls para Chrome y Firefox.

1: <https://github.com/iamadamdev/bypass-paywalls-chrome>

--------------------------------------

Omitir 2FA Instagram

1: <https://github.com/afernandezb92/2FAInstagram>

--------------------------------------

Espia trafico de la red NETSPY.sh ( hackingyseguridad.com )

1: <https://github.com/hackingyseguridad/netspy>

--------------------------------------

Hackear el mundo usando Termux

1: https://github.com/sabri-zaki/EasY\_HaCk

--------------------------------------

🐱‍💻 Parche su aplicación de Android (apk) con un certificado autofirmado para rastrear el tráfico https.

1: https://github.com/rlxone/android-https-patcher

--------------------------------------

🌐¡Descubre cómo crear e implementar una extensión de Google Chrome para tu proyecto!

1: https://github.com/dwyl/learn-chrome-extensions

--------------------------------------

Inyector extremo

1: <https://github.com/master131/ExtremeInjector>

--------------------------------------

El marco del punto de acceso no autorizado

1: https://github.com/wifiphisher/wifiphisher

--------------------------------------

Marco general de autenticación de bastidores

1: https://github.com/wardencommunity/warden

--------------------------------------

La utilidad de recuperación de contraseña basada en GPGPU más rápida y avanzada del mundo

1: https://github.com/Rich5/oclHashcat

--------------------------------------

Una herramienta para sitio web de fuerza bruta y dirección de correo.

1: https://github.com/l1444/assbreak

--------------------------------------

Herramienta de fuerza bruta X🔓WordPress, Joomla, DruPal, OpenCart, Magento

1: https://github.com/Moham3dRiahi/XBruteForcer

--------------------------------------

Herramienta de piratería automatizada que encontrará bases de datos filtradas con una precisión del 97,1 % para obtener el correo y la contraseña juntos de cargas recientes de <https://pastebin.com> . Soporte de fuerza bruta para cuentas de spotify, cuentas de instagram, servidores ssh, clientes de microsoft rdp y cuentas de gmail

1: https://github.com/wuseman/EMAGNET

--------------------------------------

Un generador de diccionarios de piratas informáticos potente y útil para un ataque de fuerza bruta

1: https://github.com/LandGrey/pydictor

--------------------------------------

Herramientas de pentesting

1: <https://github.com/error404-notfound/ToolsE404>

--------------------------------------

Ghidra es un marco de ingeniería inversa de software (SER)

1: <https://github.com/error404-notfound/ghidra>

--------------------------------------

Recolector de metadatos

1: https://github.com/laramies/metagoofil

--------------------------------------

Recopilación de información – API hackertarget.com

1: https://github.com/error404-notfound/GatheTOOL

--------------------------------------

Phishing-Tool es un completo sistema de phishing. Te permite crear sitios web con el objetivo de obtener credenciales – serveo.net

1: <https://github.com/error404-notfound/RevoltShinG>

--------------------------------------

Una aplicación para iOS que te permite reproducir la misma canción al mismo tiempo en varios dispositivos.

1: <https://github.com/thatcherclough/Song-inSync>

--------------------------------------

FUD MSFVenom Payload Generador. CatchYou 2 es una bifurcación de CatchYou de TheLinuxChoice.

1: <https://github.com/SrMilton/CatchYou-2>

--------------------------------------

Whoami proporciona privacidad mejorada, anonimato para las distribuciones de Linux basadas en Debian y Arch

1: <https://github.com/owerdogan/whoami-project>

--------------------------------------

Marco de prueba de penetración automatizado – Escáner de vulnerabilidades de código abierto – Gestión de vulnerabilidades

1: <https://github.com/OWASP/Nettacker>

--------------------------------------

La utilidad de recuperación de contraseñas más rápida y avanzada del md5

1: https://github.com/hashcat/hashcat

--------------------------------------

Fuerza bruta SnapChat [SC API] ~ SnapWreck

1: <https://github.com/u0pattern/SnapBrute>

--------------------------------------

Marco de piratería

1: <https://github.com/b3-v3r/Hunner>

--------------------------------------

Recopilación de información Instagram.

1: <https://github.com/th3unkn0n/osi.ig>

--------------------------------------

Escáner de vulnerabilidades de inyección SQL hecho con Python

1: <https://github.com/americo/sqlifinder>

--------------------------------------

🐸Identifica cualquier cosa. pyWhat le permite identificar fácilmente correos electrónicos, direcciones IP y más. ¡Aliméntalo con un archivo .pcap o algún texto y te dirá qué es!🧙‍♀️.

1: <https://github.com/bee-san/pyWhat>

--------------------------------------

Una herramienta OSINT para buscar cuentas por nombre de usuario en 72 redes sociales.

1: <https://github.com/p1ngul1n0/blackbird>

--------------------------------------

Una aplicación de línea de comandos reddit OSINT.

1: https://github.com/georgehawkins0/reddittz

--------------------------------------

Controlador de Windows con interfaz de modo de usuario que puede ocultar procesos, sistemas de archivos y objetos de registro, proteger procesos, etc.

1: <https://github.com/JKornev/hidden>

--------------------------------------

Una herramienta para generar cargas útiles de shell inverso sobre la marcha.

1: https://github.com/octetsplicer/LAZYPARIAH

--------------------------------------

Doxing)/

1: <https://github.com/cyber1nj3ctor/Doxing>

--------------------------------------

Escáner de vulnerabilidades de carga de archivos y herramienta de explotación.

1: <https://github.com/almandin/fuxploider>

--------------------------------------

HERRAMIENTA DE PRUEBA DE PENETRACIÓN WEB💥

1: <https://github.com/Nabil-Official/N-WEB>

--------------------------------------

GENERAR DIRECCIONES DE CORREO TEMPORAL Y RECIBIR MENSAJES

1: <https://github.com/Nabil-Official/N-MAIL>

--------------------------------------

Un poderoso sistema Spider (Web Crawler) en Python.

1: https://github.com/binux/pyspider

--------------------------------------

¡UNA HERRAMIENTA PARA ENVIAR SMS ANÓNIMAMENTE!

1: https://github.com/Nabil-Official/N-ANOM

--------------------------------------

SEGUIMIENTO DE IP | IPPHISH | GENERADOR DE IP ALEATORIA

1: <https://github.com/Nabil-Official/N-TRACE>

--------------------------------------

Potente marco para ataques de puntos de acceso no autorizados.

1: <https://github.com/P0cL4bs/wifipumpkin3>

--------------------------------------

Plataforma de ataque de surf anti hombro (ASSAP)

1: https://github.com/assap-org/assap

--------------------------------------

📶Herramienta de punto de acceso no autorizado.

1: https://github.com/makdosx/wifi-agent

--------------------------------------

Una colección de herramientas de piratería, recursos y referencias para practicar la piratería ética.

1: <https://github.com/sundowndev/hacker-roadmap>

--------------------------------------

Es un autenticador gráfico que tiene como objetivo eliminar el ataque Shoulder Surfing, el ataque más vulnerable para la autenticación gráfica y otros ataques de contraseña basados ​​en texto. Elimina la necesidad de memorizar contraseñas textuales, lo que lo hace fácil de usar y seguro, al mismo tiempo.

1: <https://github.com/apurvashinde01/Image-based-Authenticator>

--------------------------------------

Prevención de ataques de Shoulder Surfing mediante técnicas criptográficas

1: https://github.com/RohanCK/Crypto

--------------------------------------

Listado completo y uso de las herramientas utilizadas para el hacking ético

1: https://github.com/hhhrrrttt222111/Ethical-Hacking-Tools

--------------------------------------

Obtener la ubicación exacta de un dispositivo, con un enlace.

1: <https://github.com/InformaticayHacking/jager>

--------------------------------------

Utilice DNS mal configurados y registros de bases de datos antiguos para encontrar direcciones IP ocultas detrás de la red CloudFlare

1: <https://github.com/m0rtem/CloudFail>

--------------------------------------

Herramienta de recopilación de información para un sitio web o dirección IP

1: https://github.com/bahatiphill/BillCipher

--------------------------------------

Implementación automatizada de la infraestructura del equipo rojo mediante Docker

1: <https://github.com/khast3x/Redcloud>

--------------------------------------

Dracnmap es un programa de código abierto que se utiliza para explotar la red y recopilar información con la ayuda de nmap. El comando Nmap viene con muchas opciones que pueden hacer que la utilidad sea más robusta y difícil de seguir para los nuevos usuarios. Por lo tanto, Dracnmap está diseñado para realizar un escaneo rápido con el motor de secuencias de comandos de nmap y nmap puede realizar va…

1: <https://github.com/screetsec/Dracnmap>

--------------------------------------

Genere registradores de teclas de correo electrónico de Gmail para Windows.

1: https://github.com/4w4k3/BeeLogger

--------------------------------------

Entorno Vagrant VirtualBox para realizar una prueba de penetración de red interna

1: <https://github.com/R3dy/capsulecorp-pentest>

--------------------------------------

Raspador de metadatos de tweets y analizador de actividad

1: <https://github.com/x0rz/tweets_analyzer>

--------------------------------------

Genere cargas útiles y controle máquinas remotas. [Interrumpido]

1: <https://github.com/4w4k3/Insanity-Framework>

--------------------------------------

Verificar si existe el correo electrónico

1: <https://github.com/4w4k3/KnockMail>

--------------------------------------

Sistema Android Malware (Análisis | Puntuación)

1: https://github.com/quark-engine/quark-engine

--------------------------------------

Un potente rastreador de navegador para escáneres de vulnerabilidades web

1: https://github.com/Qianlitp/crawlergo

--------------------------------------

Metagoofil es una herramienta de recopilación de información diseñada para extraer metadatos de documentos públicos (pdf,doc,xls,ppt,docx,pptx,xlsx) pertenecientes a una empresa objetivo.

1: <https://github.com/kurobeats/metagoofil>

--------------------------------------

Herramienta para obtener información y ubicación, de una dirección IP o Dominio.

1: https://github.com/InformaticayHacking/iphunter

--------------------------------------

El Nuevo Marco de Hackeo (Sniffing, Ataques de Red, Herramientas, Explotación, Clientes, Etc.)

1: <https://github.com/HackingEnVivo/KatanaFramework>

--------------------------------------

Programas para falsificar DNS y detectar este tipo de ataques

1: <https://github.com/shahzebp/dns_spoof_detect>

--------------------------------------

Controlador de Windows y XInput Wrapper para controladores Sony DualShock ¾

1: <https://github.com/nefarius/ScpToolkit>

--------------------------------------

[Fork-n-Go] Una página personal simple. Manifestación:

1: <https://github.com/jlord/hello>

--------------------------------------

Diablo ~ Herramientas de Hacking / Pentesting

1: https://github.com/Anlominus/Diablo

--------------------------------------

Aloje de forma segura sus propias cuentas de correo electrónico, ya que el correo electrónico se diseñó originalmente para funcionar.

1: <https://github.com/d3cod3/EndtoEndEncryptedMailServer>

--------------------------------------

🤣Una herramienta de informes pentest escrita en Python. Libérate de Microsoft Word.

1: https://github.com/blacklanternsecurity/writehat

--------------------------------------

Un script de Python de múltiples subprocesos diseñado para forzar directorios y nombres de archivos en servidores web.

1: <https://github.com/ytisf/BirDuster>

--------------------------------------

🎩servidor bastión SSH (y telnet) simple, divertido y transparente

1: <https://github.com/moul/sshportal>

--------------------------------------

Araña redes enteras para archivos jugosos que se encuentran en recursos compartidos SMB. Busque nombres de archivos o contenido de archivos: ¡regex compatible!

1: <https://github.com/blacklanternsecurity/MANSPIDER>

--------------------------------------

Un proxy SOCKS escrito en Python que aleatoriza su dirección IP de origen. ¡Rodee sus paquetes malignos a través de túneles SSH o déles miles de millones de direcciones de origen únicas!

1: <https://github.com/blacklanternsecurity/TREVORproxy>

--------------------------------------

CrowdSec: el IPS de código abierto y participativo capaz de analizar el comportamiento de los visitantes y proporcionar una respuesta adaptada a todo tipo de ataques. También aprovecha el poder de la multitud para generar una base de datos CTI global para proteger la red de usuarios.

1: <https://github.com/crowdsecurity/crowdsec>

--------------------------------------

Un CrowdSec Bouncer que sincroniza las decisiones tomadas por CrowdSec con el firewall de CloudFlare. Administra la configuración de múltiples usuarios, múltiples cuentas y múltiples zonas. Admite decisiones con alcance de IP, país y AS.

1: https://github.com/crowdsecurity/cs-cloudflare-bouncer

--------------------------------------

Caja de herramientas de incumplimiento

1: <https://github.com/decyphir/breach>

--------------------------------------

Con el objetivo de guiarlo a través de todas sus necesidades de participación preactiva | ¡OpSec nunca se vio tan débil!

1: <https://github.com/ItsJustShepherd/BREACH>

--------------------------------------

RedGuard es una herramienta de control de flujo frontal C2, puede evitar la verificación de equipos azules, AV y EDR.

1: https://github.com/wikiZ/RedGuard

--------------------------------------

🔍Una herramienta para rastrear solicitudes de sondeo inalámbrico sin cifrar de dispositivos.

1: <https://github.com/xdavidhu/probeSniffer>

--------------------------------------

Irparpayaña, Herramienta diseñada para sacar la mayor informacion de páginas web y crear payload de inyección (sacar metodos de internet ilimitado)

1: <https://github.com/HackeRStrategy/Irparpaya-a>

--------------------------------------

Actualizacion del generador de bin cc-genpro, con nuevas herramientas y mas sencillo de utilizar el generador de bin

1: <https://github.com/HackeRStrategy/cc-genpro1.2>

--------------------------------------

Captcha Intruder (CIntrud3r) es una herramienta automática de pentesting para eludir captchas.

1: <https://github.com/epsylon/cintruder>

--------------------------------------

FuzzSSH es una herramienta de software libre creada para detectar vulnerabilidades SSH (protocolo).

1: <https://github.com/epsylon/fuzzssh>

--------------------------------------

Orb es una herramienta de huella masiva.

1: <https://github.com/epsylon/orb>

--------------------------------------

¡Descifrado de contraseñas de archivos zip con el uso de la lista de contraseñas!

1: <https://github.com/The404Hacking/ZIP-Password-BruteForcer>

--------------------------------------

Número de whatsapp fuerza bruta. (Ab) utiliza la API web de WhatsApp.

1: <https://github.com/p4kl0nc4t/wabf>

--------------------------------------

Versión actualizada de <https://github.com/Rdimo/Hazard-Token-Grabber> ¡Esta tiene mucho más impacto y roba contraseñas de Google Chrome, cookies, tokens, tarjetas de crédito, capturas de pantalla de IP y más!

1: <https://github.com/Rdimo/Hazard-Token-Grabber-V2>

--------------------------------------

Herramienta de administración remota de Discord completamente escrita en Python3

1: <https://github.com/Sp00p64/DiscordRAT>

--------------------------------------

Herramienta de administración remota de Discord (versión mejorada)

1: <https://github.com/Rdimo/DiscordRAT>

--------------------------------------

Un exploit de spammer de correo electrónico de Discord que funciona anulando la verificación de un correo electrónico de tokens y luego solicitando que Discord lo verifique nuevamente varias veces, lo que lleva a que Discord envíe spam a ese correo electrónico con mensajes de verificación de correo electrónico.

1: <https://github.com/Rdimo/Discord-email-spammer-exploit>

--------------------------------------

Discord Auto bumper hecho en python, solo un simple auto bumper que hice porque estaba aburrido

1: https://github.com/Rdimo/Auto-Bumper

--------------------------------------

Un capturador de fichas/contraseñas de Discord que captura todas sus fichas, contraseñas, tarjetas de crédito y mucho más

1: https://github.com/Rdimo/Hazard-Token-Grabber

--------------------------------------

Grabadora de cámara web que captura un video de la víctima y luego lo carga y lo envía a su webhook

1: https://github.com/Rdimo/Webcam-recorder

--------------------------------------

Un script por lotes simple pero destructivo que deshabilitará Windows Defender, administrador de tareas, herramientas de registro, cmd, evitará la protección contra manipulaciones y mucho más

1: https://github.com/Rdimo/Defender-disabler

--------------------------------------

¡Un simple bot de Discord que se puede usar para generar cuentas, generar nitro, enviar seguidores de contracción también tiene enfriamiento en los comandos y puede incluir en la lista negra a los usuarios con mucha más personalización!

1: <https://github.com/Rdimo/GenBot>

--------------------------------------

Una colección de herramientas de piratería, recursos y referencias para practicar la piratería ética.

1: <https://github.com/sundowndev/hacker-roadmap>

--------------------------------------

Detecte, rastree y alerte sobre la desviación de la infraestructura

1: <https://github.com/snyk/driftctl>

--------------------------------------

Herramientas IP Para obtener rápidamente información sobre direcciones IP, páginas web y registros DNS.

1: <https://github.com/Manisso/Crips>

--------------------------------------

Marco de explotación de reenlace de DNS

1: https://github.com/FSecureLABS/dref

--------------------------------------

🔗Todos los recursos que pude encontrar para aprender Ethical Hacking y Penetration Testing.

1: https://github.com/husnainfareed/Awesome-Ethical-Hacking-Resources

--------------------------------------

Marco C2 con todas las funciones que persiste silenciosamente en el servidor web con una puerta trasera PHP de una sola línea

1: <https://github.com/nil0x42/phpsploit>

--------------------------------------

Paquete de herramientas de piratería fsociety: un marco de prueba de penetración

1: https://github.com/Manisso/fsociet

--------------------------------------

Un token nuker de discord Con un montón de opciones que arruinarán una cuenta realmente mal, también tiene un informe masivo incorporado, GroupChat Spammer y Token / Contraseña / Capturador de tarjetas de crédito ¡y mucho más!

1: https://github.com/Rdimo/Hazard-Nuker

--------------------------------------

Descargador de tablones de imágenes/booru muy personalizable con potentes funciones de nombres de archivos.

1: https://github.com/Bionus/imgbrd-grabber

--------------------------------------

Herramienta de prueba automática de Python.

1: https://github.com/jeffh/sniffer

--------------------------------------

Herramienta de fuerza bruta de actualización de DNS dinámico

1: https://github.com/mandatoryprogrammer/UPBRUTE

--------------------------------------

Increíble fuerza bruta de contraseñas para todos los juegos de xgenstudios. Pasa por alto todo y comprueba pws a una velocidad ridícula.

1: https://github.com/Michal2SAB/XGen-Password-Cracker

--------------------------------------

Anyform es una herramienta ligera de fuerza bruta.

1: <https://github.com/yak0d3/anyForm>

--------------------------------------

Cubre tus huellas durante la explotación de Linux dejando cero rastros en los registros del sistema y las marcas de tiempo del sistema de archivos.

1: https://github.com/mufeedvh/moonwalk

--------------------------------------

El motor de recopilación de información simplista | Encuentre información avanzada sobre un nombre de usuario, sitio web, número de teléfono, etc.

1: https://github.com/MandConsultingGroup/Scylla

--------------------------------------

Memenite – Fortnite Anti-cheat Bruteforcer, HWID Spoofer, Cleaner, Hardware Serials checker, Aimbot/ESP Cheat, FOV Changer

1: <https://github.com/disrupt-epic/memenite>

--------------------------------------

Un interceptor de tráfico y paquetes de red para Linux. Spoof ARP & Wiretap A Network.

1: https://github.com/MandConsultingGroup/Espionage

--------------------------------------

Cross Site “Scripter” (también conocido como XSSer) es un -marco- automático para detectar, explotar y reportar vulnerabilidades XSS en aplicaciones basadas en web.

1: https://github.com/epsylon/xsser

--------------------------------------

Herramienta para obtener información de una página web sacar dominios, host, enlaces…etc

1: https://github.com/HackeRStrategy/Tool-Web-RS

--------------------------------------

Una herramienta de phishing avanzada enfocada a hackear cuentas de facebook mediante phishing. Facehack te permite personalizar la página de inicio de sesión agregandole una imagen de fondo o agregarle un degradado. Tambien puedes agregarle una descripcion, titulo o imagen al link que te genera. Otra cosa que puedes hacer es agregar una URL personalizada …

1: https://github.com/HACKDRES2/Facehack

--------------------------------------

Con este script podras crear virus potentes en link ya no es necesario una apk para meterle virus a tu enemig@ ya solo con mandarle el link y ella/el lo abran valieron madr&

1: https://github.com/HACKDRES2/virus-link

--------------------------------------

Herramienta para obtener información de una página web sacar dominios, host, links…etc

1: https://github.com/HackeRStrategy/Tool-Web-RS

--------------------------------------

DiosOjo

1: https://gitlab.com/adrielgro/GodEye/

--------------------------------------

Pasarela de cifrado de correo electrónico

1: https://github.com/gpgmailencrypt/gpgmailencrypt

--------------------------------------

Envía correos electrónicos usando Gmail en formato encriptado

1: https://github.com/SinghCoder/secureMails

--------------------------------------

Herramienta de fuerza bruta del cubo de Amazon

1: https://github.com/FishermansEnemy/bucket\_finder

--------------------------------------

Kit de herramientas sociales para ataques de phishing (multiplataforma)

1: https://github.com/PowerScript/STP

--------------------------------------

Herramienta de Ingeniería Social Orientada a facebook

1: https://github.com/PowerScript/facebrok

--------------------------------------

Una bifurcación GPL del popular escáner de vulnerabilidades de wordpress WPScan

1: https://github.com/HackingEnVivo/vane

--------------------------------------

Rastreador de personas en Internet: Aprenda a rastrear el mundo, para evitar ser rastreado.

1: https://github.com/HackingEnVivo/trape

--------------------------------------

Esta programada totalmente por mi, su uso es muy sencillo, 5 opciones que te ayudarán a obtener información de un nick, ip, nombre y demás.

1: https://github.com/SerLink04/LinkDox

--------------------------------------

Una herramienta de inteligencia de código abierto de Instagram

1: <https://github.com/sc1341/InstagramOSINT>

--------------------------------------

Omitir SSL Pinning en la aplicación de Instagram para Android

1: https://github.com/u0pattern/Instagram\_SSL\_Pinning

--------------------------------------

Verificador de nombres de usuario Snapchat usando SC API

1: https://github.com/u0pattern/SnapCheck

--------------------------------------

[Verificador de correos electrónicos Twitter + Inicio de sesión API Twitter] – API REST Twitter

1: https://github.com/u0pattern/TwitterKit

--------------------------------------

Xray, Penetra Todo. También el mejor v2ray-core, con soporte XTLS. Configuración totalmente compatible.

1: https://github.com/XTLS/Xray-core

--------------------------------------

Herramientas y utilidades para facilitar el trabajo con la red ION y el uso de ION DID

1: https://github.com/decentralized-identity/ion-tools

--------------------------------------

Un programa de mensajería de texto SMS con interfaz de línea de comandos.

1: https://github.com/thatcherclough/CLImessage

--------------------------------------

Un backdoor con multitud de funcionalidades.

1: <https://github.com/thatcherclough/BetterBackdoor>

--------------------------------------

Botnet de Windows moderno y avanzado gratuito con un panel PHP agradable y seguro desarrollado con VB.NET.

1: <https://github.com/therealelyayo/BlackNET-2>

--------------------------------------

Es un marco lleno de muchas opciones y herramientas de piratería que usa directamente en el script, desde la fuerza bruta hasta la carga útil, lo que hace que sigo agregando más cosas. Ahora tengo otra herramienta llamada htkl-lite, su kit de herramientas para hackers no es tan grande y desordenado. Para ver las actualizaciones, consulte mi instagram @g3\_ruben.\_.fuenla\_ o si hay algún problema, envíeme un mensaje en insta…

1: https://github.com/unkn0wnh4ckr/hackers-tool-kit

--------------------------------------

Mail-in-a-Box ayuda a las personas a recuperar el control de su correo electrónico al definir un servidor SMTP+todo lo demás con un solo clic y fácil de implementar: un servidor de correo en una caja.

1: https://github.com/mail-in-a-box/mailinabox

--------------------------------------

[NUEVO]: VERIFICADOR del Protocolo simple de transferencia de correo (SMTP) – Herramienta CRACKER V2

1: https://github.com/ARON-TN/Smtp-cracker

--------------------------------------

💤Saque los dispositivos de su red realizando un ataque ARP Spoof.

1: <https://github.com/k4m4/kickthemout>

--------------------------------------

Una aplicación web para clasificar los departamentos de ciencias de la computación según sus resultados de investigación en lugares seleccionados y para encontrar profesores activos en una amplia gama de área.

1: <https://github.com/chenjj/CSrankings>

--------------------------------------

Escáner rápido de vulnerabilidades de configuración incorrecta de CORS🍻

1: <https://github.com/chenjj/CORScanner>

--------------------------------------

Este es un script bash de usos múltiples para sistemas Linux para auditar redes inalámbricas.

1: <https://github.com/v1s1t0r1sh3r3/airgeddon>

--------------------------------------

Escaneo, generación de informes y análisis automatizados y sencillos de vulnerabilidades

1: <https://github.com/seccubus/seccubus>

--------------------------------------

Orientación para las vulnerabilidades Spectre, Meltdown, Speculative Store Bypass, Rogue System Register Read, Lazy FP State Restore, Bounds Check Bypass Store, TLBleed y L1TF/Foreshadow, así como una guía general de seguridad de hardware y firmware. #nsacyber

1: <https://github.com/nsacyber/Hardware-and-Firmware-Security-Guidance>

--------------------------------------

VULNRΞPO: generador de informes de vulnerabilidad gratuito y repositorio cifrado de extremo a extremo. Plantillas completas de incidencias, CWE, CVE, MITRE ATT&CK, PCI DSS, cifrado AES, importación de incidencias Nmap/Nessus/Burp/OpenVAS, exportación Jira, informe TXT/HTML/PDF, archivos adjuntos, registro de cambios automático, estadísticas, gestión de vulnerabilidades, informe de seguridad constructor.

1: <https://github.com/kac89/vulnrepo>

--------------------------------------

Colección de exploits verificados del kernel de Linux

1: <https://github.com/jollheef/lpe>

--------------------------------------

Herramienta de desarrollo {módulo, explotación} kernel fuera del árbol

1: <https://github.com/jollheef/out-of-tree>

--------------------------------------

AutoIt HackTool, Shortcuts .lnk Generador de cargas útiles como LNK-KISSER.

1: <https://github.com/9aylas/Shortcut-Payload-Generator>

--------------------------------------

🔍Una herramienta Osint completa

1: https://github.com/Lucksi/Mr.Holmes

--------------------------------------

Kit de herramientas para la explotación manual del búfer, que cuenta con un fuzzer de socket de red básico, un generador y detector de patrones de desplazamiento, un identificador de caracteres incorrectos, un tallador de shellcode y un explotador de EIP estándar.

1: <https://github.com/ins1gn1a/WoollyMammoth>

--------------------------------------

Python – Gestión de base de datos Metasploit-Framework

1: <https://github.com/sectool/Python-Metasploit-Framework-Database-Management>

--------------------------------------

Onex es un administrador de paquetes para piratas informáticos. Onex administra más de 400 herramientas de piratería que se pueden instalar con un solo clic.

1: <https://github.com/rajkumardusad/onex>

--------------------------------------

Plataforma avanzada de pruebas de penetración ANDRAX para teléfonos inteligentes A

1: https://github.com/hail33/ANDRAX-Mobile-Pentest

--------------------------------------

Aplicación GUI Aircrack, Airodump, Aireplay, MDK3 y Reaver para Android

1: <https://github.com/chrisk44/Hijacker>

--------------------------------------

Acecha a tus amigos. Encuentre sus perfiles de Instagram, FB y Twitter mediante el reconocimiento de imágenes y la búsqueda inversa de imágenes.

1: <https://github.com/ThoughtfulDev/EagleEye>

--------------------------------------

Herramienta de piratería TODO EN UNO para piratas informáticos

1: <https://github.com/Z4nzu/hackingtool>

--------------------------------------

Herramienta de código abierto portátil, liviana y de alto rendimiento para escaneo SMBGhost masivo

1: <https://github.com/deepsecurity-pe/GoGhost>

--------------------------------------

Gusano cliente ssh

1: <https://github.com/hc0d3r/tea>

--------------------------------------

Volcar la contraseña del cliente mysql de la memoria

1: <https://github.com/hc0d3r/mysql-magic>

--------------------------------------

Script de PowerShell del equipo rojo

1: https://github.com/securethelogs/RedRabbit

--------------------------------------

dDumper es un escáner de vulnerabilidades de Drupal y un explotador automático.

1: <https://github.com/yak0d3/dDumper>

--------------------------------------

Herramienta de craqueo WiFi (usando Evil Twin Attack) con algunas modificaciones. (Solo para fines legales)

1: <https://github.com/thehackingsage/fluxion>

--------------------------------------

Herramientas de protección y ataques DoS y DDoS para Windows, Linux y Android (solo con fines educativos)

1: <https://github.com/thehackingsage/ddos>

--------------------------------------

Aplicación de Android para contraseñas WiFi de fuerza bruta sin necesidad de un dispositivo rooteado.

1: <https://github.com/faizann24/wifi-bruteforcer-fsecurify>

--------------------------------------

Herramienta de raspado de grupo de telegramas. Obtener toda la información sobre los miembros del grupo

1: https://github.com/th3unkn0n/TeleGram-Scraper

--------------------------------------

BitCracker es la primera herramienta de descifrado de contraseñas de código abierto para unidades de memoria cifradas con BitLocker

1: <https://github.com/e-ago/bitcracker>

--------------------------------------

Herramientas desempaquetadas de CQAcademy

1: <https://github.com/BlackDiverX/cqtools>

--------------------------------------

La extensión Red Team todo en uno para Web Pentester🛠

1: <https://github.com/LasCC/Hack-Tools>

--------------------------------------

uDork es un script escrito en Bash Scripting que utiliza técnicas avanzadas de búsqueda de Google para obtener información sensible en archivos o directorios, encontrar dispositivos IoT, detectar versiones de aplicaciones web, etc.

1: <https://github.com/m3n0sd0n4ld/uDork>

--------------------------------------

Troyano de acceso remoto para Windows via servidor de Telegram, controla y una una maquina infectada mediante un bot de Telegram – Python3

1: <https://github.com/Aaronmaiden666/RAT_via_Telegram_Windows>

--------------------------------------

Un Creador de Troyanos automatico.

1: https://github.com/KentMGR/Troyan-Maker

--------------------------------------

Herramientas de piratería para todos los sistemas operativos basados ​​en Debian

1: <https://github.com/thehackingsage/hacknix>

--------------------------------------

DISPOSITIVO DE SUEÑO PARA HACKERS

1: <https://github.com/thehackingsage/pwnphone>

--------------------------------------

🔓Herramienta de recopilación de información y enumeración de subdominios

1: <https://github.com/jonluca/Anubis>

--------------------------------------

Ocultar enlace de phishing: URL personalizada de Ngrok

1: <https://github.com/OnlineHacKing/Masking-URL>

--------------------------------------

Kit de herramientas de ingeniería inversa

1: https://github.com/mentebinaria/retoolkit

--------------------------------------

PUBG & BGMI Mobile Phishing Tool ID Hack Tool para piratería en línea

1: https://github.com/OnlineHacKing/PUBG\_BGMI-Phishing

--------------------------------------

SIGIT – Kit de herramientas de recopilación de información simple

1: https://github.com/termuxhackers-id/SIGIT

--------------------------------------

Herramientas para Pentesting

1: https://github.com/thehackingsage/hacktronian

--------------------------------------

Kit de herramientas Pentest

1: https://github.com/sectool/Python-Pentest-ToolKit

--------------------------------------

Este es un programa que instalará Metasploit-Framework y Armitage en cualquier distribución de Linux basada en Debian (también se puede adaptar para funcionar en Mac). Esto fue posible gracias a una combinación de mi propio código, el de darkoperator y un instalador nocturno de Metasploit de rapid7.

1: https://github.com/Matt-London/Install-Armitage-on-Linux

--------------------------------------

Herramienta de ataque X☣Escáner de vulnerabilidades de sitios web y explotador automático

1: https://github.com/reaperb0t/XAttacker

--------------------------------------

YAMAS: herramienta de metaanálisis para estudios GWAS

1: <https://github.com/cmeesters/yamas>

--------------------------------------

Herramienta de inyección SQL

1: <https://github.com/xxgrunge/sqlninja>

--------------------------------------

Herramientas del administrador de Android

1: <https://github.com/xxgrunge/QtADB>

--------------------------------------

No he encontrado una versión razonable del kit de explotación BlackHole sin las molestias de ionCube; así que aquí hay una solución para ese problema J Tenga en cuenta que estos archivos han sido decodificados y compartidos solo con fines educativos.

1: <https://github.com/CryptXor/BlackHole-ExploitKit-Decoded>

--------------------------------------

No he encontrado una versión razonable del kit de exploits CrimePack sin las molestias de ionCube; así que aquí hay una solución para ese problema J Tenga en cuenta que estos archivos han sido decodificados y compartidos solo con fines educativos.

1: <https://github.com/CryptXor/CrimePack-ExploitKit-Decoded>

--------------------------------------

DNS fantasma

1: https://github.com/reaperb0t/GhostDNS

--------------------------------------

Plataforma colaborativa de gestión de vulnerabilidades y pruebas de penetración

1: https://github.com/infobyte/faraday

--------------------------------------

Pequeña herramienta python3 para verificar vulnerabilidades comunes en servidores SMTP

1: <https://github.com/xFreed0m/SMTPTester>

--------------------------------------

Una herramienta avanzada para el reconocimiento de correo electrónico

1: https://github.com/sham00n/buster

--------------------------------------

Script para aplicar un proxy transparente a través de Tor con nftables o iptables y, opcionalmente, puede falsificar una MAC aleatoria, hora local, ip, nombre de host.

1: <https://github.com/szorfein/paranoid-ninja>

--------------------------------------

(Privacidad de metadatos de red) Falsificador de dirección MAC con combo adicional (opciones): nombre de host + falsificador de señal - \*¡sin desconexiones!\* Cambio de privacidad con Brand Mimics: ejecutar como comando o una nueva identidad aleatoria opcional en cada arranque; incluye banderas para cambiar continuamente tiempos aleatorios/cambiar direcciones OUI válidas + Aleatorizador de nombre de host + Dispositivo/Señal/ubicación y…

1: https://github.com/RightToPrivacy/wipri

--------------------------------------

Herramienta todo en uno para la recopilación de información, el análisis de vulnerabilidades y el rastreo. Una herramienta imprescindible para todos los probadores de penetración.

1: https://github.com/Zaeem20/RED\_HAWK

--------------------------------------

La herramienta de redireccionamiento de páginas falsas más poderosa…

1: https://github.com/Zaeem20/VirusX5

--------------------------------------

Herramientas de suplantación de identidad por SMS

1: <https://github.com/XiphosResearch/smsisher>

--------------------------------------

Script OSINT simple para encontrar perfiles de Instagram por nombre y correo electrónico/teléfono

1: https://github.com/blackeko/yesitsme

--------------------------------------

Una secuencia de comandos python3 simple pero efectiva para realizar la suplantación de DNS a través del envenenamiento ARP

1: https://github.com/blackeko/mitm

--------------------------------------

Hyenae NG es un generador de paquetes de red multiplataforma avanzado y el sucesor de Hyenae. Cuenta con suplantación de identidad de capa de red completa, aleatorización de direcciones basada en patrones y mecanismos de ruptura de detección de inundaciones.

1: <https://github.com/r-richter/hyenae-ng>

--------------------------------------

Un buscador SSRF automatizado. ¡Solo da el nombre de dominio y tu servidor y relájate! ;) También tiene opciones para encontrar XSS y abrir redirecciones

1: https://github.com/ksharinarayanan/SSRFire

--------------------------------------

Recopile información simplemente enviando un enlace, incluidas las instantáneas de la cámara y la ubicación.

1: <https://github.com/Th30neAnd0nly/Psi>

--------------------------------------

OSRFramework, Open Sources Research Framework es un proyecto AGPLv3+ de i3visio centrado en proporcionar API y herramientas para realizar investigaciones en línea más precisas.

1: <https://github.com/i3visio/osrframework>

--------------------------------------

Punycode Alert es una extensión de Google Chrome, Chromium y Opera que advierte a los usuarios cuando la URL a la que acceden tiene algún contenido de punycode.

1: <https://github.com/i3visio/punycode-alert>

--------------------------------------

Marco de reconocimiento de red, publicado por @cg3\_ruben.\_.fuenla\_ . Cree sus propias alternativas autohospedadas y totalmente controladas a Shodan / ZoomEye / Censys y GreyNoise, ejecute su servicio de DNS pasivo, recopile y analice la inteligencia de red de sus sensores, ¡y mucho más!

1: <https://github.com/ivre/ivre>

--------------------------------------

Herramienta de búsqueda de violación de contraseña y OSINT de correo electrónico, localmente o usando servicios premium. Admite la búsqueda de correo electrónico relacionado

1: <https://github.com/khast3x/h8mail>

--------------------------------------

🕵️‍♂️Recopile un expediente sobre una persona por nombre de usuario de miles de sitios

1: <https://github.com/soxoj/maigret>

--------------------------------------

Herramienta que implementa ataques de canal lateral contra HTTPS

1: https://github.com/jselvi/fiesta

--------------------------------------

Herramienta NTP principal en el medio

1: https://github.com/PentesterES/Delorean

--------------------------------------

Script de ingeniería inversa para cargas útiles de Android Rat

1: <https://github.com/Max-IQ/Horus-Eye>

--------------------------------------

Esta herramienta brinda a desarrolladores, investigadores y empresas la capacidad de analizar paquetes de software de diferentes lenguajes de programación que están siendo o serán utilizados en sus códigos, brindándoles información que les permite saber con anticipación si esta librería cumple con los procesos. Desarrollo seguro, si actualmente es compatible, posibles puertas traseras (malicioso…

1: https://github.com/TelefonicaTC2Tech/packagedna

--------------------------------------

⛏️Extraiga información de cuentas de páginas personales en varios sitios para fines OSINT

1: https://github.com/soxoj/socid-extractor

--------------------------------------

La herramienta de código abierto más completa para el análisis de inteligencia de Twitter

1: <https://github.com/vaguileradiaz/tinfoleak>

--------------------------------------

ProtOSINT es un script de Python que lo ayuda a investigar las cuentas de Protonmail y las direcciones IP de ProtonVPN

1: <https://github.com/pixelbubble/ProtOSINT>

--------------------------------------

Herramienta de ataque y toma de huellas dactilares de Frontpage y Sharepoint.

1: https://github.com/sensepost/SPartan

--------------------------------------

Mi Recon Automatización

1: <https://github.com/mad-robot/SPartan>

--------------------------------------

🧬Extraiga y analice la información de los contribuyentes de los repositorios de git

1: <https://github.com/soxoj/gitcolombo>

--------------------------------------

💻 📱mip22 es una herramienta de phishing avanzada

1: https://github.com/makdosx/mip22

--------------------------------------

Encuentre direcciones de correo electrónico existentes por apodo usando métodos de verificación API/SMTP sin notificación al usuario. ¡Por favor, no dude en mejorar el trabajo del gato!🐱🔎 📬

1: <https://github.com/sharsil/mailcat>

--------------------------------------

ScanPro – Scripts de escaneo

1: https://github.com/Anlominus/ScanPro

--------------------------------------

La herramienta de código abierto más completa para el análisis de inteligencia de Twitter

1: <https://github.com/vaguileradiaz/tinfoleak>

--------------------------------------

Descargador de herramientas de hacking: descarga de herramientas de hacking y exportación por categorías al directorio $HOME

1: <https://github.com/Anlominus/HacKing>

--------------------------------------

KitsStart – Inicio y descarga de kits de instalación de Anlominus – Hacking, PenTest, AnyGen, AnySpam, AnyPhishing, Working.

1: <https://github.com/Anlominus/KitStart>

--------------------------------------

TeleHack: herramientas, paquetes, bots, información, administración, raspadores, sumadores, grupos y canales de Telegram, y más.

1: <https://github.com/Anlominus/TeleHack>

--------------------------------------

Diseñado para escanear y explotar vulnerabilidades dentro de los servicios ocultos de Tor. TORhunter permite que la mayoría de las herramientas funcionen con normalidad al resolver .onion

1: https://github.com/Err0r-ICA/TORhunter

--------------------------------------

Una herramienta de seguridad ofensiva de alto rendimiento para reconocimiento y exploración de vulnerabilidades

1: <https://github.com/evyatarmeged/Raccoon>

--------------------------------------

😱Una lista curada de OSINT increíblemente asombrosos

1: https://github.com/jivoi/awesome-osint

--------------------------------------

SpiderFoot automatiza OSINT para la inteligencia de amenazas y el mapeo de su superficie de ataque.

1: <https://github.com/smicallef/spiderfoot>

--------------------------------------

Una herramienta OSINT de geolocalización. Ofrece recopilación de información de geolocalización a través de plataformas de redes sociales.

1: https://github.com/ilektrojohn/creepy

--------------------------------------

Penetración automatizada y sistemas auxiliares, proporcionando XSS, XXE, registro de DNS, SSRF, RCE, web netcat y otros servidores, gin-vue-admin

1: <https://github.com/hktalent/go4hacker>

--------------------------------------

Nslookup

1: https://github.com/alsotang/nslookup

--------------------------------------

Un buscador SSRF automatizado. ¡Solo da el nombre de dominio y tu servidor y relájate! ;) También tiene opciones para encontrar XSS y abrir redirecciones

1: <https://github.com/ksharinarayanan/SSRFire>

--------------------------------------

La primera herramienta de pirateo de cámara compatible con Python

1: <https://github.com/sankethj/z-cam>

--------------------------------------

Análisis wifi usando airckrack-ng y elasticsearch

1: <https://github.com/mpruna/Wifi_analysis_using_Elk_Stack>

--------------------------------------

Hack de Bluetooth

1: https://github.com/kimbo/bluesnarfer

--------------------------------------

Herramienta de pirateo de wifi usando ESP8266 (método Evil-twin)

1: <https://github.com/sankethj/ZiFi>

--------------------------------------

Preparación para el examen Ec-council Certified Ethical Hacker 312-50

1: https://github.com/Brute-f0rce/CEH/blob/master/hacking-wireless-networks.md

--------------------------------------

Un rastreador de respuesta sorprendentemente rápido para encontrar cosas jugosas en el código fuente!😎🔥

1: <https://github.com/ksharinarayanan/SourceWolf>

--------------------------------------

Kit de herramientas de explotación posterior de Bash

1: https://github.com/redcode-labs/Bashark

--------------------------------------

Enumerar los recursos de la nube de AWS en función de las credenciales proporcionadas

1: https://github.com/bassammaged/awsEnum

--------------------------------------

Una RAT de Android multifuncional con panel web basado en GUI sin reenvío de puertos.

1: https://github.com/Th30neAnd0nly/AIRAVAT

--------------------------------------

Herramienta de enumeración de usuarios y distribución de contraseñas para probar Azure AD

1: https://github.com/optionalCTF/SSOh-No

--------------------------------------

Este script instalará todas las herramientas esenciales de recompensas por errores y encontrará algunas vulnerabilidades básicas. Hice este guión para mi caza diaria. La mejor característica de este script es simplemente ejecutarlo en segundo plano y luego analizar el objetivo manualmente.

1: https://github.com/machine1337/recon-automation

--------------------------------------

Un pequeño script para enviar mensajes de forma anónima. Script de envío de SMS muy rápido y seguro.

1: https://github.com/machine1337/fake-sms

--------------------------------------

Una herramienta de prueba de suplantación de correo electrónico que tiene como objetivo eludir SPF/DKIM/DMARC y falsificar firmas DKIM.🍻

1: https://github.com/chenjj/espoofer

--------------------------------------

Le permite conectar extraños entre sí e interceptar mensajes AKA Man in the Middle Attack

1: https://github.com/ash47/OmegleMiddleMan

--------------------------------------

OpenID Certified™ OpenID Connect y OAuth2 Server (OP, OpenID Provider): seguridad de API de código abierto, nativa de la nube y prioritaria para su infraestructura. Escrito en Go. SDK para cualquier idioma.

1: <https://github.com/error404-notfound/hydra>

--------------------------------------

Crear payloads para todo tipo de windows y tomar el control de ellos con una sesion meterpreter de Metasploit

1: <https://github.com/error404-notfound/TCREATOR-WIN>

--------------------------------------

FiercePhish es un marco de phishing completo para administrar todos los compromisos de phishing. Le permite rastrear campañas de phishing separadas, programar el envío de correos electrónicos y mucho más.

1: <https://github.com/error404-notfound/FiercePhish>

--------------------------------------

Termux (Host-Extractor): herramienta para el testeo, descubrimiento de host de paginas web.

1: <https://github.com/error404-notfound/hosterror404V2>

--------------------------------------

Cambiar iP del ordenador

1: <https://github.com/error404-notfound/MacSpoof>

--------------------------------------

Este escrito esta hecho con multas educativas y de información no nos responsabilizamos el mal uso que le pueden dar

1: <https://github.com/error404-notfound/Doxing-Error404>

--------------------------------------

Este script está diseñado con fines educativos es una extensión de carne para utilizarlo fuera de la red local

1: https://github.com/error404-notfound/Beef404

--------------------------------------

Realiza un ataque de suplantación de ARP utilizando los sockets sin procesar del kernel de Linux

1: <https://github.com/smikims/arpspoof>

--------------------------------------

Script simple para verificar en masa si las IP coinciden con las redes

1: https://github.com/UndeadSec/IP-NET

--------------------------------------

Una herramienta para hacer phishing a través de SMS. Esto utiliza la API gratuita de fast2sms para enviar SMS con un túnel ngrok que conduce a páginas de phishing a través de un matraz.

1: https://github.com/ishan-saha/SmishingTool

--------------------------------------

Kit de herramientas de phishing/smishing de código abierto

1: <https://github.com/b0n1t0/gosmish>

--------------------------------------

Verificar si existe el correo electrónico

1: <https://github.com/4w4k3/KnockMail>

--------------------------------------

Exploit Pack contiene un conjunto completo de más de 39.000 exploits, puede estar seguro de que su próximo pentest será imparable. Todos los sistemas operativos son compatibles como objetivos, incluidos: Windows, Linux, Unix, Minix, SCO, Solaris, OSX, etc. E incluso plataformas móviles y web.

1: <https://github.com/AngelSecurityTeam/Tool-ExploitPack>

--------------------------------------

Dork Search, Escáner de vulnerabilidades, Inyección SQL, XSS, LFI, RFI

1: https://github.com/AngelSecurityTeam/SQLiDumper-AngelSecurityTeam

--------------------------------------

Genere cargas útiles y controle máquinas remotas. [Interrumpido]

1: https://github.com/4w4k3/Insanity-Framework

--------------------------------------

Genere registradores de teclas de correo electrónico de Gmail para Windows.

1: https://github.com/franklintimoteo/BeeLogger

--------------------------------------

Genere correo electrónico, regístrese para cualquier cosa, obtenga la OTP/enlace

1: https://github.com/s0md3v/ote

--------------------------------------

Striker es un escáner de vulnerabilidades e información ofensiva.

1: https://github.com/s0md3v/Striker

--------------------------------------

Escaneo masivo de IPs para servicios vulnerables

1: https://github.com/s0md3v/Silver

--------------------------------------

Detecta direcciones URL malvadas que usan IDN Homograph Attack.

1: https://github.com/UndeadSec/checkURL

--------------------------------------

Blazy es un fuerza bruta de inicio de sesión moderno que también prueba CSRF, Clickjacking, Cloudflare y WAF.

1: https://github.com/UndeadSec/Blazy

--------------------------------------

Extensión del registrador de teclas de Chrome | Herramienta de explotación posterior

1: https://github.com/UndeadSec/HeraKeylogger

--------------------------------------

Inyectar código malicioso en \*.debs

1: https://github.com/UndeadSec/Debinject

--------------------------------------

Esto extraerá toda la información de una cuenta de instagram. La herramienta más poderosa de raspadores de Internet reacondicionada por xRO.

1: https://github.com/KiLL3R-xRO/Lucifer

--------------------------------------

Esta es una herramienta de creación de archivos basura que crea archivos basura en el almacenamiento interno

1: https://github.com/KiLL3R-xRO/fuzzy-boy

--------------------------------------

Capturador de IP web que usa el nombre de dominio incluido con varias funciones más fáciles de usar

1: https://github.com/KiLL3R-xRO/Spider

--------------------------------------

VIRUS STSTRONG QUE NO SON CAPTADOS POR LA SEGURIDAD DEL DISPOSITIVO DURANTE LA INSTALACIÓN🔥

1: https://github.com/KiLL3R-xRO/X-VIRUS

--------------------------------------

Codifica rápidamente el formato de texto en formatos hexadecimal, hash, binario y octal.

1: https://github.com/KiLL3R-xRO/N-Coder

--------------------------------------

Hackear cuenta de WhatsApp fácilmente (Android)

1: https://github.com/KiLL3R-xRO/X-Whatsapp

--------------------------------------

Aplicación para hackear cuentas de Whatsapp, realizar seguimientos y rastreos de los mensajes y conversaciones entre usuarios.

1: https://github.com/hackerwhatsapp/espiarmensajes

--------------------------------------

Smishing es un script de Python que envía SMS utilizando el marco Phishing Frenzy

1: https://github.com/stirtcanada/smishing

--------------------------------------

FBleaker extraerá el correo electrónico de su Facebook e intentará encontrar la contraseña si alguna vez se filtran

1: <https://github.com/ScRiPt1337/FBLeaker>

--------------------------------------

Javascript phishing professional; redirigir a la víctima si quiere iniciar sesión en PayPal u otro sitio web

1: <https://github.com/hakanonymos/javascript-phishing>

--------------------------------------

Keylogger envía los detalles de inicio de sesión por correo electrónico, número de tarjeta, cuenta de facebook, paypal… etc. Nuevo proyecto 2020

1: <https://github.com/hakanonymos/chrome-keylogger>

--------------------------------------

Javascript botnet browser V3 basado en Cloud 9 Botnet y mi botnet browser chrome. Capturar cualquier sitio web, clave virtual, paypal, facebook, comercio electrónico, obtener número de tarjeta, fecha de caducidad, CVV

1: https://github.com/hakanonymos/browser-javascript-botnet-cloud

--------------------------------------

Extensión keylogger chrome, obtener cookie, redirección a un sitio web falso o a otro sitio web

1: https://github.com/hakanonymos/chromeKeylogger

--------------------------------------

Ransomware cifra todos los archivos, descarga una imagen de un servidor remoto y luego cambia el fondo de pantalla después del cifrado de archivos

1: https://github.com/hakanonymos/ransomware

--------------------------------------

Botnet browser chrome, mozilla firefox, capturar número de tarjeta en cualquier sitio web, paypal, facebook, comercio electrónico, obtener número de tarjeta, fecha de caducidad, CVV, mejor keylogger javascript

1: https://github.com/hakanonymos/botnet-browser-chrome

--------------------------------------

Python roba la contraseña de Chrome todas las versiones del navegador son compatibles 100 % FUD

1: https://github.com/hakanonymos/steal-chrome-password-all-version

--------------------------------------

Esta es una aplicación espía de Android, que carga datos de usuario como contactos, mensajes, registro de llamadas, envía mensajes, fotos, videos, abre un enlace del navegador, etc. Android Rat

1: https://github.com/abhinavsuthar/Android\_Spy\_App

--------------------------------------

Esta herramienta se puede utilizar durante las pruebas de penetración internas para volcar las credenciales de Windows de un host ya comprometido. Permite volcar las colmenas SYSTEM, SECURITY y SAM y, una vez copiadas en las máquinas atacantes, ofrece la opción de eliminar estos archivos para borrar el rastro.

1: <https://github.com/Viralmaniar/HiveJack>

--------------------------------------

Passhunt es una herramienta simple para buscar credenciales predeterminadas para dispositivos de red, aplicaciones web y más. Busque a través de 523 proveedores y sus 2084 contraseñas predeterminadas.

1: <https://github.com/Viralmaniar/Passhunt>

--------------------------------------

La herramienta BigBountyRecon utiliza 58 técnicas diferentes utilizando varios tontos de Google y herramientas de código abierto para acelerar el proceso de reconocimiento inicial de la organización objetivo.

1: <https://github.com/Viralmaniar/BigBountyRecon>

--------------------------------------

Esta herramienta le permite realizar OSINT y reconocimiento en una organización o individuo. Permite buscar 1.400 millones de credenciales de texto sin cifrar que se descartaron como parte de la fuga de BreachCompilation. Esta base de datos hace que encontrar contraseñas sea más rápido y fácil que nunca.

1: <https://github.com/Viralmaniar/SMWYG-Show-Me-What-You-Got>

--------------------------------------

Puerta trasera basada en Python que usa Gmail para filtrar datos a través de archivos adjuntos. Esta RAT ayudará durante los compromisos del equipo rojo a la puerta trasera de cualquier máquina con Windows. Realiza un seguimiento de la actividad del usuario mediante una captura de pantalla y la envía a un atacante como un archivo adjunto de correo electrónico.

1: <https://github.com/Viralmaniar/Powershell-RAT>

--------------------------------------

Busque en la web profunda directamente desde su terminal

1: <https://github.com/josh0xA/darkdump>

--------------------------------------

Botnet browser chrome, mozilla firefox, capturar número de tarjeta en cualquier sitio web, paypal, facebook, comercio electrónico, obtener número de tarjeta, fecha de caducidad, CVV, mejor keylogger javascript

1: <https://github.com/hakanonymos/botnet-browser-chrome>

--------------------------------------

Agrega la capacidad de iniciar sesión con éxito en sitios web que tienen un retraso después del inicio de sesión y agrega el directorio de chromedriver, esta bifurcación se usó en el tutorial de Null Byte para Hatch.

1: <https://github.com/nsgodshall/Hatch>

--------------------------------------

Una pequeña secuencia de comandos para el patito de goma USB que navega hasta las credenciales de usuario almacenadas en Firefox y luego envía por correo electrónico una captura de pantalla de todos los correos electrónicos y contraseñas a una dirección de su elección.

1: <https://github.com/nsgodshall/Firefox-password-stealer>

--------------------------------------

Herramienta automatizada de rociado de contraseñas

1: <https://github.com/zshell/trident>

--------------------------------------

Algunas herramientas de Pentest. Instalar y mantener actualizadas algunas herramientas de pentesting.

1: <https://github.com/zshell/Some-Tools>

--------------------------------------

Una herramienta para generar certificados de firma de código falsos o firmar certificados reales

1: <https://github.com/Tylous/Limelighter>

--------------------------------------

Un buscador de dominios llamado GoogleSSLdomainFinder - Herramienta de consulta de subdominios basada en el certificado transparente SSL de Google

1: <https://github.com/We5ter/GSDF>

--------------------------------------

Un potente conjunto de herramientas de código abierto para piratas informáticos y automatización de la seguridad.

1: <https://github.com/We5ter/Scanners-Box>

--------------------------------------

Un marco para pentesting inalámbrico.

1: <https://github.com/Tylous/SniffAir>

--------------------------------------

Mercury es una herramienta de piratería que se utiliza para recopilar información y usarla para dañar aún más al objetivo.

1: <https://github.com/4n6strider/Mercury>

--------------------------------------

Ladrón de sesiones de la aplicación Telegram Desktop en windows 7, 8 y 10 🔑

1: <https://github.com/Nikait/TgStealer>

--------------------------------------

Herramienta de administración remota de Windows a través de Telegram. Escrito en Python

1: <https://github.com/Bainky/Telegram-RAT>

--------------------------------------

Robar cookies para Chrome y Mozilla Firefox, use otra extensión para iniciar sesión con la cookie robada

1: <https://github.com/hakanonymos/steal-cookie-chrome-firefox>

--------------------------------------

Un sitio web de confirmación de pago de paypal falso

1: <https://github.com/PixelSized/paypal-spoofer>

--------------------------------------

Programa capaz de detectar DNIs rotados en el plano XY mediante un algoritmo de visión artificial basado en la extracción de características a partir de los puntos de interés (keypoints) de una imagen. Detecta los DNIs en vigor desde el 2006 en adelante.

1: https://github.com/Suaro/DNIDetector

--------------------------------------

¡Es falso que acabas de enviar dinero a alguien con este sitio web!

1: <https://github.com/misspoken69/FakePayPalSender>

--------------------------------------

Automatice el registro de cuentas de usuario en Spotify.

1: <https://github.com/Azlxy/spotify-account-creator>

--------------------------------------

Creador de cuentas TikTok totalmente automatizado

1: https://github.com/hendrikbgr/TikTok-Account-Creator

--------------------------------------

Crear automáticamente cuentas de Twitter (antiguo)

1: https://github.com/d3rezz/twitter-account-creator

--------------------------------------

Un simple script de Python para ayudarlo a crear múltiples cuentas en cualquier sitio web usando proxies

1: https://github.com/1Blademaster/account-creator

--------------------------------------

Un script de bot de creación automática de cuentas para Instagram.

1: https://github.com/Alan4747/instagram-auto-create-account

--------------------------------------

Un lobbybot de Fortnite que puedes controlar a través de Discord.

1: https://github.com/Azlxy/Sirius

--------------------------------------

¡Haz un Lobbybot de Fortnite en 3 minutos!

1: https://github.com/noteason/GuffBot

--------------------------------------

Información sobre cómo registrarse para obtener una cuenta gratuita de Epic Games y obtener acceso al código fuente de UnrealEngine.

1: https://github.com/EpicGames/Signup

--------------------------------------

Secuestro de DNS a través de la herramienta de automatización de registros inactivos

1: <https://github.com/iinc0gnit0/DeadDNS>

--------------------------------------

[Juego de herramientas de piratería impulsado por solicitudes de extracción]

1: <https://github.com/iinc0gnit0/BlackKit>

--------------------------------------

Configuración de terminal para pentesters.

1: https://github.com/DreyAnd/PenTerm

--------------------------------------

WAFW00F permite identificar y tomar huellas dactilares de los productos de firewall de aplicaciones web (WAF) que protegen un sitio web.

1: <https://github.com/EnableSecurity/wafw00f>

--------------------------------------

Cifrar archivo usando php

1: <https://github.com/swagkarna/Php_Ransomware>

--------------------------------------

Este es un programa simple que le permite enviar mensajes a la fuerza a las personas que ha bloqueado y no pueden responder, útil para trolear y ha sido un problema con Discord durante casi 2 años. Encontrado por mí mismo en julio de 2018.

1: <https://github.com/swagkarna/Discord-Block-Bypass-Meme>

--------------------------------------

Herramienta de administración remota de Discord completamente escrita en Python

1: <https://github.com/Sp00p64/DiscordRAT>

--------------------------------------

Identifique direcciones de correo electrónico o nombres de dominio que pertenezcan a colegios o universidades. Ayude a automatizar el proceso de aprobación o rechazo de descuentos académicos.

1: https://github.com/anuragranj/swot

--------------------------------------

Red de Pirámide Espacial para Flujo Óptico

1: https://github.com/anuragranj/spynet

--------------------------------------

Cañón de iones de órbita baja: una herramienta de tensión de red de código abierto, escrita en C#. Basado en el proyecto LOIC de Praetox. USO BAJO SU PROPIO RIESGO. SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA.

1: https://github.com/NewEraCracker/LOIC

--------------------------------------

Herramienta OSINT para encontrar información de tarjetas de crédito violadas

1: <https://github.com/itsmehacker/CardPwn>

--------------------------------------

Una colección de increíbles recursos, herramientas y otras cosas brillantes para las pruebas de penetración. (No programa solo texto)

‘: <https://github.com/S3cur3Th1sSh1t/Pentest-Tools>

‘: <https://github.com/enaqx/awesome-pentest>

--------------------------------------

Marco patito de goma Arduino

1: <https://github.com/itsmehacker/Ducky-Exploit>

--------------------------------------

🔓😎Una lista seleccionada de increíbles guías, herramientas y otros recursos relacionados con la seguridad y el compromiso de cerraduras, cajas fuertes y llaves.

1: <https://github.com/enaqx/awesome-pentest#anonymity-tools>

--------------------------------------

Análisis de vulnerabilidad

1: <https://github.com/enaqx/sploitware>

--------------------------------------

PhEmail es una herramienta de correo electrónico de phishing de código abierto de Python que automatiza el proceso de envío de correos electrónicos de phishing como parte de una prueba de ingeniería social

1: <https://github.com/Dionach/PhEmail>

--------------------------------------

Recopilación de recursos relacionados con el phishing

1: https://github.com/PhishyAlice/awesome-phishing

--------------------------------------

SniperPhish: el kit de herramientas de suplantación de identidad (spear phishing) de correo electrónico web

1: <https://github.com/GemGeorge/SniperPhish>

--------------------------------------

Una colección de cosas asombrosas sobre el ecosistema React

1: https://github.com/enaqx/awesome-react

--------------------------------------

Cargas útiles sólidas con persistencia automatizada, cargas útiles de openport.io, conexiones encriptadas con fernet y su propio servidor de comandos (¡sin msf!)

1: <https://github.com/swagkarna/osprey-v2>

--------------------------------------

Una aplicación con ventanas emergentes que solo dice que se calle.

1: https://github.com/iiTiger25/Shutup.exe

--------------------------------------

MailSniper es una herramienta de prueba de penetración para buscar términos específicos (contraseñas, información privilegiada, información de arquitectura de red, etc.) en el correo electrónico en un entorno de Microsoft Exchange. Puede ser utilizado como usuario no administrativo para buscar su propio correo electrónico, o por un administrador para buscar en los buzones de correo de cada usuario en un dominio.

1: https://github.com/S3cur3Th1sSh1t/MailSniper

--------------------------------------

La herramienta consta de 1-ddos sección 2-ccgen sección 3-fb hack sección 4-insta hack sección 5-Gmail hack sección 6-spam sección

1: <https://github.com/mego323/mr-prime>

--------------------------------------

Ataques de listas de palabras en archivos Bitwarden data.json

1: <https://github.com/S3cur3Th1sSh1t/BitwardenDecryptBrute>

--------------------------------------

Un bombardero de SMS para Bangladesh

1: <https://github.com/Ign0r3dH4x0r/Xweapon>

--------------------------------------

Una herramienta fácil de pentesting.

1: https://github.com/kuburan/txtool

--------------------------------------

Una herramienta simple para bombardear correos electrónicos usando su Gmail.

1: https://github.com/ArnabXD/GmailBomber

--------------------------------------

HPomb es la herramienta CLI de Socail Engineering, utilizada para bombardeos, suplantación de identidad y anonimato disponible para Linux

1: https://github.com/secanonm/HPomb

--------------------------------------

Escanee el CORE del sitio web con 8 Vulnerablity Scanner para realizar pruebas de penetración.

1: https://github.com/Ign0r3dH4x0r/BloodyIP

--------------------------------------

Genere el paquete Android Virus Sploit .APK usando Linux y Termux.

1: https://github.com/Ign0r3dH4x0r/GenVirus#

--------------------------------------

DomainPasswordSpray es una herramienta escrita en PowerShell para realizar un ataque de rociado de contraseñas contra los usuarios de un dominio. De forma predeterminada, generará automáticamente la lista de usuarios del dominio. ¡TENGA MUCHO CUIDADO DE NO BLOQUEAR LAS CUENTAS!

1: <https://github.com/S3cur3Th1sSh1t/DomainPasswordSpray>

--------------------------------------

Pase el hash a una canalización con nombre para la suplantación de token

1: <https://github.com/S3cur3Th1sSh1t/SharpNamedPipePTH>

--------------------------------------

Kit de herramientas de explotación posterior de PowerShell Runspace

1: <https://github.com/S3cur3Th1sSh1t/p0wnedShell>

--------------------------------------

Kit de herramientas de explotación posterior de PowerShell Runspace

1: <https://github.com/S3cur3Th1sSh1t/p0wnedShell>

--------------------------------------

Herramienta OSINT de la Web Oscura

1: <https://github.com/S3cur3Th1sSh1t/TorBot>

--------------------------------------

Marco de generación de carga útil

1: https://github.com/S3cur3Th1sSh1t/SharpShooter

--------------------------------------

Automatización para pruebas internas de penetración de Windows / AD-Security

1: <https://github.com/S3cur3Th1sSh1t/WinPwn>

--------------------------------------

Automatizar la herramienta Pentest

1: <https://github.com/S3cur3Th1sSh1t/Yuki-Chan-The-Auto-Pentest>

--------------------------------------

Ubique con precisión teléfonos inteligentes usando ingeniería social

1: https://github.com/thewhiteh4t/seeker

--------------------------------------

📡Un programa de Python para crear un AP falso y rastrear datos.

1: <https://github.com/S3cur3Th1sSh1t/mitmAP>

--------------------------------------

♾️🌚✨Servicios ilegales✨🌚♾️

1: <https://github.com/Illegal-Services/Illegal_Services>

--------------------------------------

Tutorial de Python - || Buscar cuentas de redes sociales por nombres de usuario para inteligencia de fuente abierta ||

1: <https://github.com/ncorbuk/Python-Tutorial---Hunt-Down-Social-Media-Accounts-by-Usernames-for-Open-Source-Intelligence->

--------------------------------------

Plantillas Doxing | Buscar y publicar información privada o de identificación sobre (un individuo en particular) en Internet, generalmente con intenciones maliciosas.

1: https://github.com/akalankauk/DOX-Templates

--------------------------------------

Skeleton es un conmutador de ataques de herramientas de ingeniería social

1: <https://github.com/KURO-CODE/Skeleton>

--------------------------------------

Herramienta de doxing simple

1: https://github.com/KURO-CODE/DoxTracker

--------------------------------------

Script de Python para descifrar contraseñas almacenadas por mRemoteNG

1: <https://github.com/S3cur3Th1sSh1t/mRemoteNG-Decrypt>

--------------------------------------

Manipule dispositivos Chromecast en su red

1: <https://github.com/thewhiteh4t/killcast>

--------------------------------------

Log4j jndi herramienta de fuzz de inyección

1: https://github.com/zhzyker/logmap

--------------------------------------

Vulmap – Web

1: <https://github.com/zshell/vulmap>

--------------------------------------

Herramienta de fuerza bruta para romper el bloqueo de PIN en dispositivos Android

1: <https://github.com/papusingh2sms/WBRUTER-ANDROID>

--------------------------------------

Clona una voz en 5 segundos para generar un discurso arbitrario en tiempo real

1: <https://github.com/CorentinJ/Real-Time-Voice-Cloning>

--------------------------------------

Trax | Escáner de vulnerabilidad XSS automatizado actualmente en desarrollo🐍PROYECTO HACKTOBERFEST 2019

1: <https://github.com/M4cs/traxss>

--------------------------------------

Salsa Tools – ShellReverse TCP/UDP/ICMP/DNS/SSL/BINDTCP/Shellcode/SILENTTRINITY y AV bypass, parcheado AMSI

1: <https://github.com/Hackplayers/Salsa-tools>

--------------------------------------

Recsech es una herramienta para hacer Footprinting y Reconocimiento en la red de destino. Recsech recopila información como información de DNS, subdominios, HoneySpot detectado, adquisiciones de subdominios, reconocimiento en Github y mucho más que puede ver en Funciones en herramientas.

1: https://github.com/radenvodka/Recsech

--------------------------------------

El shell WinRM definitivo para hacking/pentesting

1: <https://github.com/Hackplayers/evil-winrm>

--------------------------------------

SVScanner: vulnerabilidad del escáner y explotación masiva.

1: <https://github.com/radenvodka/SVScanner>

--------------------------------------

PENTOL – Kit de herramientas Pentester para Fiddler2

1: <https://github.com/radenvodka/PENTOL>

--------------------------------------

Reconky es un excelente script bash de descubrimiento de contenido para cazadores de recompensas de errores que automatiza muchas tareas y se organiza de manera educada que los ayuda a mirar hacia adelante.

1: <https://github.com/ShivamRai2003/Reconky-Automated_Bash_Script>

--------------------------------------

Ashok es una herramienta OSINT Recon, también conocida como😍Cuchillo del ejército suizo .

1: <https://github.com/powerexploit/Ashok>

--------------------------------------

Correo masivo de Osint😎Herramienta de ataque.

1: <https://github.com/powerexploit/MailBomber>

--------------------------------------

Herramienta de reconocimiento todo en uno, rápida y sencilla

1: https://github.com/aufzayed/HydraRecon

--------------------------------------

Herramienta de búsqueda de violación de contraseña y OSINT de correo electrónico, localmente o usando servicios premium. Admite la búsqueda de correo electrónico relacionado

1: <https://github.com/khast3x/h8mail>

--------------------------------------

Escáner de vulnerabilidades de adquisición de subdominios

1: <https://github.com/m4ll0k/takeover>

--------------------------------------

SecretFinder: un script de Python para encontrar datos confidenciales (apikeys, accesstoken, jwt, …) y buscar cualquier cosa en archivos javascript

1: <https://github.com/m4ll0k/SecretFinder>

--------------------------------------

Una poderosa herramienta de rastreo y enumeración de DNS🔎

1: <https://github.com/jacopodl/DNSTorch>

--------------------------------------

Herramienta de ataque DHCP👿

1: https://github.com/jacopodl/dstar

--------------------------------------

Lookyloo es una interfaz web que permite a los usuarios raspar la página de un sitio web y luego mostrar un árbol de dominios que se llaman entre sí.

1: <https://github.com/ninoseki/lookyloo>

--------------------------------------

Herramienta de reconocimiento para pen-tester

1: https://github.com/kunshdeep2812/reco

--------------------------------------

Httpx es un kit de herramientas HTTP rápido y multipropósito que permite ejecutar múltiples sondeadores utilizando la biblioteca http reintentable, está diseñado para mantener la confiabilidad de los resultados con más subprocesos.

1: <https://github.com/ninoseki/httpx>

--------------------------------------

Sifter es un escáner de osint, reconocimiento y vulnerabilidad. Combina una plétora de herramientas dentro de diferentes conjuntos de módulos para realizar rápidamente tareas de reconocimiento, verificar el firewall de la red, enumerar hosts remotos y locales, y buscar las vulnerabilidades ‘azules’ dentro de microsft y, si no están parcheadas, explotarlas. Utiliza herramientas como blackwidow y konan para nosotros…

1: <https://github.com/kunshdeep2812/sifter>

--------------------------------------

Mapeo detallado de la superficie de ataque y descubrimiento de activos

1: https://github.com/OWASP/Amass

--------------------------------------

Código desarrollado para robar ciertos archivos de configuración del navegador (historial, preferencias, etc.)

1: <https://github.com/zshell/spybrowse>

--------------------------------------

Navaja suiza de reconocimiento

1: <https://github.com/s0md3v/ReconDog>

--------------------------------------

El escáner XSS más avanzado.

1: <https://github.com/s0md3v/XSStrike>

--------------------------------------

Genere correo electrónico, regístrese para cualquier cosa, obtenga la OTP/enlace

1: https://github.com/s0md3v/ote

--------------------------------------

Una herramienta para la ingeniería inversa de archivos apk de Android

1: <https://github.com/iBotPeaches/Apktool>

--------------------------------------

🤖SDK PHP de la API de bots de Telegram. ¡Te permite construir Telegram Bots fácilmente! Soporta Laravel fuera de la caja.

1: <https://github.com/iBotPeaches/telegram-bot-sdk>

--------------------------------------

Herramienta de recopilación de inteligencia de código abierto destinada a reducir el tiempo dedicado a recopilar información de fuentes abiertas.

1: <https://github.com/lanmaster53/recon-ng>

--------------------------------------

Herramienta para explotar vulnerabilidades de inyección SQL que sqlmap no puede encontrar.

1: https://github.com/lanmaster53/sqli-exploiter

--------------------------------------

Muchos errores de Apktool requieren que cree aplicaciones de prueba como pruebas unitarias. Comenzaré a almacenar la fuente de esas aplicaciones aquí.

1: <https://github.com/iBotPeaches/TestApks>

--------------------------------------

Script para generar una aplicación de Android para hackear archivos de imagen de WhatsApp.

1: https://github.com/sabriallani/whatshack

--------------------------------------

Herramientas SEO para Laravel

1: https://github.com/iBotPeaches/seotools

--------------------------------------

Un detector de DNS falso

1: https://github.com/ninoseki/rogue\_one

--------------------------------------

Una herramienta experimental de detección de kits de phishing

1: <https://github.com/ninoseki/miteru>

--------------------------------------

Atasco continuamente todos los clientes/enrutadores wifi

1: <https://github.com/DanMcInerney/wifijammer>

--------------------------------------

Araña XSS – 66/66 wavsep XSS detectado

1: https://github.com/DanMcInerney/xsscrapy

--------------------------------------

NodeRat es una herramienta de acceso remoto hecha con NodeJS y python

1: <https://github.com/sabriallani/NodeRAT>

--------------------------------------

Alimente a la herramienta con un archivo .nessus y obtendrá automáticamente su shell de MSF

1: <https://github.com/DanMcInerney/msf-autoshell>

--------------------------------------

Descargo de responsabilidad: esta herramienta solo tiene fines educativos. Cyber ​​Mission te ayuda a aprender a hackear.

1: https://github.com/cybersmission/WhatsHack

--------------------------------------

Un conjunto de datos de kits de phishing en la naturaleza

1: <https://github.com/ninoseki/phishing_kits_2021>

--------------------------------------

Descargo de responsabilidad: esta herramienta solo tiene fines educativos, nunca la use para actividades ilegales

1: https://github.com/cybersmission/SocialHacks

--------------------------------------

Calcule las huellas dactilares de un sitio web para la búsqueda OSINT

1: <https://github.com/ninoseki/mmhdan>

--------------------------------------

Hackear cuenta de WhatsApp fácilmente (Android)

1: <https://github.com/KiLL3R-xRO/X-Whatsapp>

--------------------------------------

Esto extraerá toda la información de una cuenta de instagram. La herramienta más poderosa de raspadores de Internet reacondicionada por xRO.

1: https://github.com/KiLL3R-xRO/Lucifer

--------------------------------------

Bot de creación automática de cuenta de Instagram

1: <https://github.com/FeezyHendrix/Insta-mass-account-creator>

--------------------------------------

Reenvío de puertos NetStat Grab wpa\_supplicant Activar/desactivar WiFi Mostrar Mac/Inet Eliminar contraseña Extraer apk de la aplicación Usar código clave Obtener estado de la batería Obtener actividad actual

1: <https://github.com/HackTeachz/Phonesploit>

--------------------------------------

Instagram: @g3\_ruben.\_.fnl\_ SUSCRÍBETE A NUESTRO CANAL de YouTube dekwik 58

1: https://github.com/HackTeachz/Brutal

--------------------------------------

Herramientas de Instagram de Node.JS

1: https://github.com/masokky/instagram-tools

--------------------------------------

Una extensión de navegador para la búsqueda OSINT

1: https://github.com/ninoseki/mitaka

--------------------------------------

Rastreador de sitios web con detección YARA

1: <https://github.com/ninoseki/uzen>

--------------------------------------

Manténgase en silencio😈y escucha el grito😭de tu victima

1: <https://github.com/hk4crprasad/Evil-sms>

--------------------------------------

Este programa captura los números SMS e IMSI de los teléfonos celulares que te rodean.

1: <https://github.com/ninjhacks/GSMEvil>

--------------------------------------

Rastreador de sms e imsi catcher

1: <https://github.com/0xbitx/dedsecimsi>

--------------------------------------

Rastreador de sms e imsi catcher

1: <https://github.com/0xbitx/dedsecimsi>

--------------------------------------

MVT es una herramienta forense para buscar signos de infección en dispositivos de teléfonos inteligentes

1: <https://github.com/papusingh2sms/mvt>

--------------------------------------

Androidqf (Android Quick Forensics) ayuda a recopilar rápidamente evidencia forense de dispositivos Android, para identificar posibles rastros de compromiso.

1: <https://github.com/botherder/androidqf>

--------------------------------------

Una biblioteca de sockets web, que incluye tanto el servidor como el cliente, para el procesamiento

1: https://github.com/botherder/processing\_websockets

--------------------------------------

(Abandonado) Extraer paquetes de un dispositivo Android

1: <https://github.com/botherder/snoopdroid>

--------------------------------------

Seguimiento de ubicación con dirección en vivo y ciudad en Termux

1: <https://github.com/mishakorzik/IpHack>

--------------------------------------

¡Hackeo forense de puerto de escaneo!

1: <https://github.com/mishakorzik/Port-Scanner>

--------------------------------------

Este repositorio lo mantiene principalmente Omar Santos e incluye miles de recursos relacionados con piratería ética/pruebas de penetración, análisis forense digital y respuesta a incidentes (DFIR), investigación de vulnerabilidades, desarrollo de exploits, ingeniería inversa y más.

1: https://github.com/The-Art-of-Hacking/h4cker

--------------------------------------

Captura de pantalla, audio, cursor, clics del mouse y pulsaciones de teclas

1: https://github.com/mishakorzik/Captura

--------------------------------------

Números virtuales gratis, ahora mismo! (No programa solo lectura)

1: https://github.com/mishakorzik/VirtualPhoneNumber

--------------------------------------

Herramienta OSINT para encontrar correo electrónico por nombre y apellido

1: https://github.com/mishakorzik/MailFinder

--------------------------------------

¡Ultra DDos en un script de python en línea ddos!

1: https://github.com/mishakorzik/Ultra-DDos

--------------------------------------

Servidor y cliente en TCP y UDP para el protocolo NNTP.

1: https://github.com/n0nuser/sockets

--------------------------------------

Servidor de sockets y resto para el curso de Angular

1: https://github.com/Klerith/socket-server

--------------------------------------

Hackingarticles.in sin conexión legible

1: <https://github.com/un4ckn0wl3z/hackingarticles-offline>

--------------------------------------

GsmEvil 2

1: https://github.com/ninjhacks/gsmevil2

--------------------------------------

Script que genera una App Android para hackear SMS a través de WAN

1: https://github.com/papusingh2sms/mysms

--------------------------------------

reNgine es un marco de reconocimiento automatizado destinado a recopilar información durante las pruebas de penetración de aplicaciones web. reNgine tiene motores de escaneo personalizables, que se pueden usar para escanear sitios web, puntos finales y recopilar información.

1: <https://github.com/ninjhacks/rengine>

--------------------------------------

Explotación del secuestro de DLL por DLL Proxying Súper fácilmente

1: <https://github.com/tothi/dll-hijack-by-proxying>

--------------------------------------

Herramienta enfocada a gastar bromas en nuestra Red Wifi o a otras Redes Wifi. [NO ME HAGO RESPONSABLE DEL MAL USO DE ESTA HERRAMIENTA]

1: https://github.com/XDeadHackerX/Wifi\_Troll

--------------------------------------

Ataque de delegación restringida basado en recursos de Kerberos desde el exterior mediante Impacket

1:https://github.com/tothi/rbcd-attack

--------------------------------------

Un ayudante para ejecutar consultas OSINT y administrar resultados continuamente

1: <https://github.com/zshell/mihari>

--------------------------------------

SMBMap es una práctica herramienta de enumeración SMB

1: https://github.com/ShawnDEvans/smbmap

--------------------------------------

Puerto telnet abierto en dispositivos HiSilicon modernos

1: <https://github.com/tothi/hs-dvr-telnet>

--------------------------------------

📱objeción: exploración móvil en tiempo de ejecución

1: https://github.com/sensepost/objection

--------------------------------------

Herramienta diseñada para ayudar a identificar aplicaciones Django configuradas incorrectamente que exponen información confidencial.

1: <https://github.com/jimywork/djangohunter>

--------------------------------------

El mejor script de ataque DDoS Python3, ataque cibernético con 36 metodos

1: <https://github.com/MHProDev/MHDDoS>

--------------------------------------

Bot potenciador de seguidores de Instagram

1: <https://github.com/muneebwanee/InstaBot>

--------------------------------------

GMailBomber es una forma de abuso de Internet que se perpetra mediante el envío de volúmenes masivos de correo electrónico a una dirección de correo electrónico específica con el objetivo de desbordar el buzón y saturar el servidor de correo que aloja la dirección, convirtiéndolo en una forma de ataque de denegación de servicio.

1: <https://github.com/muneebwanee/GMailBomber>

--------------------------------------

WpCrack es una herramienta de auditoría y fuerza bruta utilizada para probar de forma remota el software de blogs de WordPress

1: <https://github.com/22XploiterCrew-Team/WpCrack>

--------------------------------------

Una herramienta de recopilación forense escrita en Python.

1: <https://github.com/guelfoweb/CHIRP>

--------------------------------------

Mostrar información sobre el autor por url de foto de Facebook

1: <https://github.com/guelfoweb/fbid>

--------------------------------------

[BASH] Generador de contraseñas a través de una lista de palabras

1: <https://github.com/guelfoweb/passgen>

--------------------------------------

[BASH] Herramienta de conducción. Recopile todas las redes inalámbricas Wi-Fi en un archivo de registro (formato csv) omitiendo el duplicado.

1: <https://github.com/guelfoweb/iwmap>

--------------------------------------

Un objetivo en vivo (y legal) para simular una víctima de piratería de correo de voz

1: https://github.com/benjholla/VoicemailVictim

--------------------------------------

Escaneo de subdominio Knock

1: <https://github.com/guelfoweb/knock>

--------------------------------------

Una aplicación con ventanas emergentes que solo dice que se calle.

1: https://github.com/iiTiger25/Shutup.exe

--------------------------------------

Sistema automatizado para falsificación de llamadas y números de teléfono de marcación bruta para ingeniería social

1: https://github.com/CreativeMayhem/CallMeMaybe

--------------------------------------

[BASH] Fuerza bruta de Wordpress

1: https://github.com/guelfoweb/wpbrute

--------------------------------------

Una herramienta para recuperar direcciones de correo electrónico de dominio de los motores de búsqueda.

1: https://github.com/muneebwanee/RetrieveEmail

--------------------------------------

Virus para PC que hará que tu computadora muera.

1: https://github.com/muneebwanee/RAD

--------------------------------------

Esta herramienta se basa en expresiones regulares con estándares efectivos para detectar sitios de phishing en tiempo real usando certstream y también puede detectar ataques de punycode (IDNA).

1: <https://github.com/jimywork/certstreamcatcher>

--------------------------------------

Generador de códigos QR con JavaScript y Buefy

1: <https://github.com/parzibyte/generador-qr>

--------------------------------------

HERCULES es un generador de carga útil especial que puede pasar por alto los softwares antivirus.

1: <https://github.com/EgeBalci/HERCULES>

--------------------------------------

Archivo DDOS de RootSec (Escáneres, BotNets (Mirai y QBot Premium & Normal y más), Exploits, Métodos, Sniffers)

1: <https://github.com/EgeBalci/DDOS-RootSec>

--------------------------------------

Llamadas falsas gratis – Uso ilimitado

1: <https://github.com/0dayCTF/FireRTC-Call-Spoofer>

--------------------------------------

Bromea con tus amigos con llamadas y SMS

1: <https://github.com/hasanfirnas/Devil-s-Call>

--------------------------------------

🔨panel de administración de fuerza bruta del sitio en➡️Golang

1: <https://github.com/Nikait/brute_admin>

--------------------------------------

Facilite la configuración de una llamada automática a su propio teléfono (como si alguna vez necesita salir de algo)

1: <https://github.com/tscizzle/self-caller>

--------------------------------------

Thread Stack Spoofing: PoC para una técnica avanzada de evasión en memoria que permite ocultar mejor la asignación de memoria del shellcode inyectado de los escáneres y analistas.

1: <https://github.com/mgeeky/ThreadStackSpoofer>

--------------------------------------

Una colección de más de 160 herramientas, scripts, hojas de trucos y otros botines que he desarrollado a lo largo de los años para propósitos de auditorías de Red Teaming/Pentesting/IT Security. La mayoría de ellos fueron útiles en al menos uno de mis compromisos del mundo real. (Programas hacking)

‘: <https://github.com/mgeeky/Penetration-Testing-Tools>

--------------------------------------

Un script que te ayuda a entender por qué tu E-Mail terminó en Spam

1: <https://github.com/mgeeky/decode-spam-headers>

--------------------------------------

Un kit de herramientas de evaluación de Secure Email Gateway (SEG) de código abierto diseñado para equipos rojos.

1: <https://github.com/mgeeky/Phishious>

--------------------------------------

Herramienta para encontrar la clave KPOT XOR utilizando un ataque de texto sin formato conocido.

1: https://github.com/EgeBalci/KPOT-Decryptor

--------------------------------------

CanIBeSpoofed es un proyecto de consola que utiliza la funcionalidad creada para el sitio web <https://canibespoofed.com/> . Este proyecto facilita el escaneo de dominios para obtener visibilidad sobre la cadena de suministro de correo electrónico y las vulnerabilidades SPF/DMARC.

1: <https://github.com/Rices/CanIBeSpoofed>

--------------------------------------

Rol autorizado de Ansible de PowerDNS

1: https://github.com/Ellestad1995/pdns-ansible

--------------------------------------

Copia de seguridad y recuperación automatizadas de entornos OpenStack de tamaño medio

1: https://github.com/Ellestad1995/Epic-Shelter

--------------------------------------

El código de Android para Monitor, una aplicación que evita la suplantación de identidad de llamadas. Presentado en el Simposio Junior de Texas A&M.

1: https://github.com/kaisubr/monitor\_android\_studio

--------------------------------------

Quescis es un potente troyano de acceso remoto para Windows💻en C++

1: https://github.com/Nikait/Quiescis

--------------------------------------

💥bombardero de sms avanzado en python para matar el teléfono

1: https://github.com/hasanfirnas/ni\_bomber

--------------------------------------

Bloque de ensamblaje para buscar y llamar a las funciones API de Windows dentro de la tabla de direcciones de importación (IAT) del archivo PE en ejecución.

1: https://github.com/EgeBalci/IAT\_API

--------------------------------------

Zippo es un generador de carga útil de archivo para probar vulnerabilidades de deslizamiento XSS (Zip/Tar/Gzip).

1: https://github.com/EgeBalci/zippo

--------------------------------------

Esta es una herramienta para explotar la vulnerabilidad Ticketbleed (CVE-2016-9244).

1: https://github.com/EgeBalci/Ticketbleed

--------------------------------------

Winsock accept() Implante de puerta trasera.

1: https://github.com/EgeBalci/WSAAcceptBackdoor

--------------------------------------

Este bot ayuda a los usuarios a denunciar masivamente las cuentas de Instagram

1: <https://github.com/anonymouslb/Instagram-mass-reporter>

--------------------------------------

Este repositorio contiene varios scripts de denegación de servicio o DDOS que se pueden usar para pruebas de penetración

1: https://github.com/Khanejo/DenialOfService-Scripts

--------------------------------------

Comuníquese con los programas de vigilancia del gobierno a través de sus metadatos.

1: https://github.com/tomwadley/sexting-xkeyscore

--------------------------------------

Mostrar ubicación de usuario en mapa, obteniendo coordenadas GPS en tiempo real

1: https://github.com/parzibyte/mostrar-ubicacion-mapa-gps

--------------------------------------

PoC de amplificación de DNS

1: https://github.com/danilovazb/damplify

--------------------------------------

Un bot de vigilancia masiva de Telegram en Python

1: https://github.com/jimywork/informer

--------------------------------------

Shodanwave es una herramienta para explorar y obtener información de la cámara IP Netwave.

1: https://github.com/jimywork/shodanwave

--------------------------------------

Dispositivos TP-Link Archer C50 V3 anteriores a Build 200318 Rel. 62209 permite a atacantes remotos provocar una denegación de servicio a través de un encabezado HTTP manipulado que contiene un campo de referencia inesperado.

1: https://github.com/thewhiteh4t/cve-2020-9375

--------------------------------------

Colección de cheatsheets de varias herramientas

1: <https://github.com/m4lal0/cheatsheets>

--------------------------------------

Herramienta OSINT para encontrar perfiles por nombre de usuario

1: https://github.com/bishalkharel/nexfil

--------------------------------------

Herramienta de ingeniería social (Creador de puerta trasera con Reverse Shell para Windows/Android) con Ngrok.

1: <https://github.com/m4lal0/backdoorPhish>

--------------------------------------

Un script para rastrear y decodificar mensajes de datos de entrada enviados hacia y desde una dirección de Ethereum en particular o desde cada transacción en un bloque.

1: <https://github.com/dafthack/Ethereham>

--------------------------------------

Comprobación de disponibilidad de dominio para Golang

1: https://github.com/haccer/available

--------------------------------------

Secuestrar servicios que se basan en la autenticación de código QR.

1: <https://github.com/cryptedwolf/ohmyqr>

--------------------------------------

Una pequeña herramienta para verificar servidores dns mal configurados

1: <https://github.com/internetwache/Python-AXFR-Test>

--------------------------------------

Un repositorio con 3 herramientas para crear sitios web con repositorios .git disponibles

1: https://github.com/cryptedwolf/GitTools

--------------------------------------

Una herramienta avanzada de raspado de Twitter y OSINT escrita en Python que no utiliza la API de Twitter, lo que le permite raspar a los seguidores, seguidores, tweets y más de un usuario mientras evade la mayoría de las limitaciones de la API.

1: <https://github.com/cryptedwolf/twint>

--------------------------------------

Un script simple que recupera medios de Instagram que están etiquetados con un término específico o publicados en una ubicación específica y produce una serie de resultados con fines de investigación.

1: <https://github.com/cryptedwolf/Visual-Tagnet-Explorer>

--------------------------------------

Descifrar contraseñas/cookies/historial/marcadores desde el navegador.

1: https://github.com/EgeBalci/HackBrowserData

--------------------------------------

HERCULES es un generador de carga útil especial que puede pasar por alto los softwares antivirus.

1: https://github.com/cryptedwolf/HERCULES

--------------------------------------

Una colección de herramientas para la recuperación de datos de Telegram

1: https://github.com/bernorieder/telegram\_tools

--------------------------------------

Nos permite hackear un android fuera de la red local

1: https://github.com/Cesar-Hack-Gray/shadow

--------------------------------------

Una herramienta para verificar si MFA está habilitado en múltiples servicios de Microsoft

1: https://github.com/dafthack/MFASweep

--------------------------------------

¿Quieres saber cuánto dinero en Bitcoin se mueve por el mundo? Script para inspeccionar las transacciones en el servicio de exploración de Blockchain.com

1: https://github.com/m4lal0/explorerBTC

--------------------------------------

Script para saber si una URL Web está en línea o caída.

1: <https://github.com/m4lal0/statusWeb>

--------------------------------------

EyeWitness está diseñado para tomar capturas de pantalla de sitios web, proporcionar información del encabezado del servidor e identificar las credenciales predeterminadas si es posible.

1: <https://github.com/dafthack/EyeWitness>

--------------------------------------

El repositorio de Social-Engineer Toolkit (SET) de TrustedSec: todas las versiones nuevas de SET se implementarán aquí.

1: <https://github.com/L1ghtn1ng/social-engineer-toolkit>

--------------------------------------

Pen Tester de aplicaciones web (interfaz web)

1: <https://github.com/DedSecInside/ViPER>

--------------------------------------

ReFleX – Bot de reconocimiento de imágenes profundas

1: <https://github.com/DedSecInside/ReFleX>

--------------------------------------

🍆 Un buen cli-wrapper alrededor de youtube-dl para descargar videos y seguir usuarios/canales en pornhub

1: <https://github.com/Nukesor/pornhub-dl>

--------------------------------------

SessionGopher es una herramienta de PowerShell que utiliza WMI para extraer información de sesión guardada para herramientas de acceso remoto como WinSCP, PuTTY, SuperPuTTY, FileZilla y Microsoft Remote Desktop. Se puede ejecutar de forma remota o local.

1: https://github.com/Arvanaghi/SessionGopher

--------------------------------------

Cosechador de correos electrónicos, subdominios y nombres – OSINT

1: <https://github.com/laramies/theHarvester>

--------------------------------------

Un kit de herramientas para atacar Office365

1: <https://github.com/mdsecactivebreach/o365-attack-toolkit>

--------------------------------------

👻Un chatbot de dropbox LAN controlable a través de Telegram

1: <https://github.com/xdavidhu/lanGhost>

--------------------------------------

Herramienta de monitoreo para sitios similares a PasteBin escritos en Python. Inspirado en pastemon

1: https://github.com/DanMcInerney/pystemon

--------------------------------------

Herramienta OSINT multinube. Enumere los recursos públicos en AWS, Azure y Google Cloud.

1: <https://github.com/dafthack/cloud_enum>

--------------------------------------

Una herramienta de PowerShell para tomar capturas de pantalla de múltiples servidores web rápidamente.

1: https://github.com/dafthack/PowerWebShot

--------------------------------------

Automatiza algunos trabajos de pentest a través del archivo nmap xml

1: https://github.com/dafthack/pentest-machine

--------------------------------------

Obtenga todas las direcciones IP públicas vinculadas a su cuenta de AWS. Funciona con redes IPv4/IPv6, clásicas/VPC y en todos los servicios de AWS

1: https://github.com/dafthack/aws\_public\_ips

--------------------------------------

Script hecho en Python para realizar webscraping.

1: <https://github.com/m4lal0/webScraping>

--------------------------------------

Script en Python para saber el Sistema Operativo de acuerdo al valor TTL de una IP

1: <https://github.com/m4lal0/SystemTTL>

--------------------------------------

Script en Bash para representar toda la información de los datos capturados sobre una red Wifi objetivo al correr Airodump

1: https://github.com/m4lal0/parseAirodump

--------------------------------------

Herramienta para comprobar nombre de usuario en más de 100 sitios web, foros y redes sociales.

1: https://github.com/m4lal0/userSearch

--------------------------------------

Keyloger android

1: <https://github.com/RahulPalve/Android-keylogger-with-email>

--------------------------------------

SecLists es el compañero del probador de seguridad. Es una colección de múltiples tipos de listas utilizadas durante las evaluaciones de seguridad. Los tipos de lista incluyen nombres de usuario, contraseñas, direcciones URL, cadenas grep de datos confidenciales, cargas útiles de fuzzing y muchos más.

1: https://github.com/S3cur3Th1sSh1t/SecLists

--------------------------------------

Checker de tarjetas

1: <https://github.com/kyo1337/CCEXTRAP>

--------------------------------------

Último generador de páginas web de phishing FUD Gmail

1: <https://github.com/kinghacker0/Love-Dose>

--------------------------------------

FrameDomain Framework: herramienta de enumeración de subdominios para probadores de penetración

1: <https://github.com/AngelSecurityTeam/FrameDomain>

--------------------------------------

¡Un bombardero superrápido de SMS y llamadas para Linux y Termux!

1: <https://github.com/anubhavanonymous/XLR8_BOMBER>

--------------------------------------

El proyecto central OWASP ZAP

1: <https://github.com/zaproxy/zaproxy>

--------------------------------------

Una lista de recursos para aquellos interesados ​​en comenzar con las recompensas por errores

1: <https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters>

--------------------------------------

Herramientas para trabajar con archivos android .dex y java .class

1: https://github.com/pxb1988/dex2jar

--------------------------------------

Una lista seleccionada de varias herramientas de recompensas por errores

1: https://github.com/vavkamil/awesome-bugbounty-tools

--------------------------------------

|| Active Burp Suite Pro con Loader y Key-Generator ||

1: https://github.com/SNGWN/Burp-Suite

--------------------------------------

Burp – programa de copia de seguridad y restauración

1: https://github.com/grke/burp

--------------------------------------

La navaja suiza para reconocimiento de redes 802.11, BLE, IPv4 e IPv6 y ataques MITM.

1: https://github.com/bettercap/bettercap

--------------------------------------

Inicio de sesión ultrarrápido, estructurado y nivelado en Go.

1: <https://github.com/uber-go/zap>

--------------------------------------

Aprenda piratería ética. Obtenga información sobre reconocimiento, piratería de Windows/Linux, tecnologías web de ataque y redes inalámbricas de pruebas de penetración. Recursos para aprender análisis de malware e ingeniería inversa.

1: https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

--------------------------------------

Certificado eLearnSecurity Junior Penetration Tester (eJPT) Notas PTS

1: https://github.com/osV22/ejpt\_notes

--------------------------------------

🔑comprueba de forma segura una contraseña para ver si se ha expuesto previamente en una violación de datos

1: https://github.com/djadmin/passw0rd

--------------------------------------

Hackear cualquier portal cautivo utilizando la técnica de suplantación de MAC

1: https://github.com/systematicat/hack-captive-portals

--------------------------------------

Recuperar la contraseña de LAPS desde LDAP

1: <https://github.com/swisskyrepo/SharpLAPS>

--------------------------------------

Herramienta de adivinación de nombres de usuario principalmente para usar contra el servicio SMTP predeterminado de Solaris. Puede usar EXPN, VRFY o RCPT TO.

1: <https://github.com/pentestmonkey/smtp-user-enum>

--------------------------------------

Herramienta para identificar enrutadores en la LAN local y rutas a Internet

1: <https://github.com/pentestmonkey/gateway-finder>

--------------------------------------

Básicamente prueba muchas combinaciones de nombres de usuario locales y remotos para ejecutar comandos a través de RSH

1: <https://github.com/pentestmonkey/rsh-grind>

--------------------------------------

Herramienta para ayudar a identificar ataques de sincronización

1: https://github.com/pentestmonkey/timing-attack-checker

--------------------------------------

Escaneo automático a vulnerabilidad SSL

1: <https://github.com/hahwul/a2sv>

--------------------------------------

Herramientas para la ingeniería inversa del firmware de Utimaco

1: <https://github.com/secretsquirrel/utimaco>

--------------------------------------

Un cliente rápido y sucio para la API diavgeia opendata que le permite buscar pagos por nombre o número de IVA

1: https://github.com/fotisl/diavgeia-client

--------------------------------------

Una botnet privada que utiliza múltiples entornos de nube para pentesters y red teamers. – Construido por la comunidad durante un hackathon en la conferencia de seguridad WWHF 2018

1: https://github.com/secretsquirrel/proxycannon-ng

--------------------------------------

Fuzzer SSRF automático y herramienta de explotación

1: <https://github.com/swisskyrepo/SSRFmap>

--------------------------------------

Nishang: PowerShell ofensivo para el equipo rojo, pruebas de penetración y seguridad ofensiva.

1: <https://github.com/samratashok/nishang>

--------------------------------------

Script escrito en python para realizar un ataque de delegación restringida basada en recursos (RBCD) aprovechando el kit de herramientas de Impacket.

1: <https://github.com/samratashok/RBCD>

--------------------------------------

365-Stealer es una herramienta de simulación de phishing escrita en python3. Se puede usar para ejecutar un ataque de concesión de consentimiento ilícito.

1: <https://github.com/samratashok/365-Stealer>

--------------------------------------

Kautilya: herramienta para facilitar el uso de dispositivos de interfaz humana para pruebas de seguridad y penetración ofensivas.

1: <https://github.com/samratashok/Kautilya>

--------------------------------------

PowerSploit: un marco de trabajo posterior a la explotación de PowerShell

1: <https://github.com/PowerShellMafia/PowerSploit>

--------------------------------------

Ps-Tools, un conjunto de herramientas de monitoreo de procesos avanzado para operaciones ofensivas

1: <https://github.com/HarmJ0y/Ps-Tools>

--------------------------------------

Explotar las credenciales presentes en archivos y memoria

1: <https://github.com/giMini/PowerMemory>

--------------------------------------

Una herramienta para ayudar a los pentesters a encontrar dulces deliciosos, por @l0ss y @Sh3r4 (Twitter: @/mikeloss y @/sh3r4\_hax)

1: <https://github.com/SnaffCon/Snaffler>

--------------------------------------

Herramienta para auditar y atacar entornos LAPS

1: https://github.com/leoloobeek/LAPSToolkit

--------------------------------------

Asesino del registro de eventos de Windows

1: https://github.com/hlldz/Phant0m

--------------------------------------

Escanear puertos abiertos de un rango de IP en Shodan

1: https://github.com/giMini/Posh-Recon

--------------------------------------

PowerUpSQL: un kit de herramientas de PowerShell para atacar SQL Server

1: https://github.com/HarmJ0y/PowerUpSQL

--------------------------------------

Comentarios spam con AnonSpam

1: <https://github.com/swagkarna/AnonSpam>

--------------------------------------

Extracción de contraseñas de texto sin cifrar de mstsc.exe utilizando API Hooking.

https://github.com/HarmJ0y/RdpThief

--------------------------------------

Herramienta de enumeración y phishing de Powershell MS Outlook

1: https://github.com/b4rtik/EmailRaider

--------------------------------------

Robar firmas y hacer una firma no válida a la vez

1: https://github.com/b4rtik/SigThief

--------------------------------------

Evadir el robo de credenciales ATP de WinDefender

1: <https://github.com/HarmJ0y/ATPMiniDump>

--------------------------------------

Esta herramienta de Termux Hacking Tools Programación de BM Hacker

1: <https://github.com/bmh1cker/MyTools>

--------------------------------------

Este proyecto es para TERMUX Call Flooder 100% Warking This Tool

1: https://github.com/bmh1cker/Termux-Call-Flooder

--------------------------------------

Cómo crear un sitio web de cebolla por android

1: https://github.com/bmh1cker/onion-website

--------------------------------------

Nota: Este virus es inofensivo y solo puede apagar la PC…

1: https://github.com/bmh1cker/I-Love-You-Virus

--------------------------------------

PASS – Perfilador de contraseñas de usuarios comunes

1: https://github.com/bmh1cker/pass

--------------------------------------

Keylogger Javascript moderno con panel web

1: https://github.com/bmh1cker/Flash-Keylogger

--------------------------------------

Apk de pirateo de sms entrantes creado y enviado a Victim Mobile

1: https://github.com/bmh1cker/IncomingSmS-Hacking

--------------------------------------

Script simple para cambiar esquemas de color y fuentes para Termux.

1: https://github.com/adi1090x/termux-style

--------------------------------------

Capture la captura de pantalla del usuario usando un archivo de acceso directo (Omitir UAC)

1: <https://github.com/swagkarna/screenspy>

--------------------------------------

Informe automático de cuentas de instagram (SPAM BOT)

1: <https://github.com/Awtxl/007spam-BOT>

--------------------------------------

Nmap: el mapeador de redes. Espejo de Github del repositorio oficial de SVN.

1: https://github.com/error404-notfound/nmap

--------------------------------------

Alojar troyanos en sitios Web

1: <https://github.com/error404-notfound/Delorian>

--------------------------------------

Guarde, administre y comparta sus comandos de scripts de shell.

1: <https://github.com/Sanix-Darker/b4sh-api>

--------------------------------------

Conectores disponibles para recuperar datos en aplicaciones pequeñas de Toucan Toco

1: https://github.com/Sanix-Darker/toucan-connectors

--------------------------------------

Un motor de búsqueda-cli-scraper para más de 15 motores de búsqueda, incluido Google. Duckduckgo, Bing, Ask, etc…

1: <https://github.com/Sanix-Darker/falla>

--------------------------------------

NAT Slipstreaming permite que un atacante acceda de forma remota a cualquier servicio TCP/UDP vinculado a una máquina de la víctima, sin pasar por el NAT/cortafuegos de la víctima, con solo que la víctima visite un sitio web.

1: <https://github.com/ncorbuk/slipstream>

--------------------------------------

SubZone - ¡Subdominios, registros Dns y más! || Tutorial de Python || Abuso de autoridad certificadora || Avanzado || Hacking/Info-Sec ||

1: <https://github.com/ncorbuk/SubZone>

--------------------------------------

Herramienta de fuerza bruta X 🔓 WordPress, Joomla, DruPal, OpenCart, Magento

1: <https://github.com/Moham3dRiahi/XBruteForcer>

--------------------------------------

Herramienta de ataque X ☣ Escáner de vulnerabilidades de sitios web y explotador automático

1: <https://github.com/ncorbuk/XAttacker>

--------------------------------------

Rastree la ubicación con dirección en vivo y precisión en Termux

1: <https://github.com/noob-hackers/ipdrone>

--------------------------------------

Instale Metasploit y repare Metasploit en Termux con sencillos pasos

1: <https://github.com/noob-hackers/m-wiz>

--------------------------------------

Este programa te muestra los números IMSI de los teléfonos celulares que te rodean.

1: https://github.com/ncorbuk/IMSI-catcher

--------------------------------------

Bombardero/bomba de correo electrónico de Python

1: https://github.com/ncorbuk/Python---Email-Bomber

--------------------------------------

¡Transforme su repositorio github/gitlab en una base de datos NoSQL que maneje archivos json/yaml/csv!

1: https://github.com/Sanix-Darker/gitrowspack-api

--------------------------------------

¡Un motor de búsqueda simple para proyectos de código abierto en Github, GitLab y Bitbucket en un solo lugar!

1: https://github.com/Sanix-Darker/zzollo

--------------------------------------

Impresionantes herramientas para explotar Windows!

1: https://github.com/IAmBlackHacker/Windows

--------------------------------------

Inicie Android Studio Simulator sin abrir Android Studio….

1: <https://github.com/IAmBlackHacker/AndroidStudio-Simulator>

--------------------------------------

Wireshark es un analizador de tráfico de red, o “sniffer”, para Linux, macOS, \*BSD y otros sistemas operativos Unix y similares a Unix y para Windows. Utiliza Qt, una biblioteca de interfaz gráfica de usuario, y libpcap y npcap como bibliotecas de filtrado y captura de paquetes.

1: <https://gitlab.com/wireshark/wireshark>

--------------------------------------

La utilidad de recuperación de contraseñas más rápida y avanzada del mundo

1: <https://github.com/hashcat/hashcat>

--------------------------------------

SpiderFoot automatiza OSINT para la inteligencia de amenazas y el mapeo de su superficie de ataque.

1: <https://github.com/smicallef/spiderfoot>

--------------------------------------

Patator es un juego de fuerza bruta polivalente, con un diseño modular y un uso flexible.

1: <https://github.com/lanjelot/patator>

--------------------------------------

Rastrear Google y Bing para encontrar correos electrónicos, subdominios y URL asociados a un dominio de destino

1: <https://github.com/lanjelot/web-hunter>

--------------------------------------

Recursos de prueba SSRF (falsificación de solicitud del lado del servidor)

1: https://github.com/cujanovic/SSRF-Testing

--------------------------------------

Herramienta de ingeniería social

1: <https://github.com/Gameye98/santet-online>

--------------------------------------

Restablezca su contraseña de Linux desde un pendrive externo

1: <https://github.com/IAmBlackHacker/Linux-Password-Reset>

--------------------------------------

Una plantilla de página web para ingeniería social, el despliegue de cargas útiles.

1: <https://github.com/graylagx2/Android-SE-web-template>

--------------------------------------

Fawkes es una herramienta para buscar objetivos vulnerables a la inyección SQL. Realiza la búsqueda utilizando el motor de búsqueda de Google.

1: <https://github.com/greenmind-sec/fawkes>

--------------------------------------

Entropy Exploit es un exploit de cámara web IP también llamado Netwave y GoAhead IP Camera exploit. Entropy es una poderosa herramienta de explotación para las pruebas de penetración de cámaras web.

1: <https://github.com/attackgithub/entropy>

--------------------------------------

Manera fácil de directorio web de fuerza bruta.

1: <https://github.com/abaykan/CrawlBox>

--------------------------------------

Una herramienta que crea un certificado falsificado de cualquier sitio web en línea y firma un Ejecutable para AV Evasion. Funciona tanto para Windows como para Linux.

1: <https://github.com/paranoidninja/CarbonCopy>

--------------------------------------

Webshell, servidor privado virtual (VPS) y base de datos cPanel

1: <https://github.com/c0delatte/carina>

--------------------------------------

Script basado en Python para la recopilación de información.

1: https://github.com/abaykan/53R3N17Y

--------------------------------------

E-mail osint

1: <https://github.com/likescam/h8mail_email_OSINT>

--------------------------------------

Remitente de Python SMS con SMS Gateway API. Enviar mensajes SMS desde línea de comandos/terminal

1: <https://github.com/aarnhub/python-sms-sender>

--------------------------------------

🤖El escáner de puertos moderno🤖

1: <https://github.com/RustScan/RustScan>

--------------------------------------

Dropper de carga útil multiplataforma

1: <https://github.com/UndeadSec/Enigma>

--------------------------------------

E-ntel es una herramienta que recopila información de cuentas de correo electrónico (ip, nombre de host, país,…) de diferentes fuentes públicas (motores de búsqueda, servidores de claves pgp y shodan) y verifica si los correos electrónicos se filtraron utilizando la API de correos electrónicos pirateados. Es una herramienta realmente simple, pero muy efectiva para las primeras etapas de una prueba de penetración o simplemente para conocer la visibilidad de su empresa en…

1: <https://github.com/CybernetiX-S3C/E-ntel>

--------------------------------------

Ultimate Forensics Framework se utiliza principalmente para reconocer sitios web y direcciones IP en busca de vulnerabilidades para una solución de pentesting más fácil. El script se basa en las herramientas de Kali Linux ya preinstaladas.

1: <https://github.com/CybernetiX-S3C/T.U.F.F>.

--------------------------------------

Jok3r v3 BETA 2 – Marco de automatización de red y Web Pentest

1: <https://github.com/koutto/jok3r>

--------------------------------------

Skeleton es un conmutador de ataques de herramientas de ingeniería social

1: https://github.com/KURO-CODE/Skeleton

--------------------------------------

Ataque de red Ataque wifi Ataque vlan Ataque arp Ataque Mac Ataque revelado etc../

1: <https://github.com/Matrix07ksa/EvilNet>

--------------------------------------

¡Instala las herramientas más populares de Hacking!

1: <https://github.com/R3LI4NT/kali-tools>

--------------------------------------

Ghost Eye – Herramienta de recopilación de información | Ghost Eye es una herramienta de recopilación de información escrita en bash. Para ejecutar Ghost Eye, solo necesita un dominio o ip. Ghost Eye puede funcionar con cualquier distribución de Linux

1: <https://github.com/celidon/ghost_eye>

--------------------------------------

Script que usa regex y ensamblado para recopilar IPA de cámara, para pruebas de penetración o simplemente para tomar un pico, compatible con 91 países

1: <https://github.com/ArkAngeL43/cam-stalker>

--------------------------------------

Cibermapa

1: <https://github.com/AnonymousAt3/cybermap>

--------------------------------------

Herramienta de generador de carga útil automatizada

1: https://github.com/AnonymousAt3/cyberdoor

--------------------------------------

NMscript

1: https://github.com/cabesonwiliams/NMscript

--------------------------------------

Sesiones fuerza bruta

1: https://github.com/Gameye98/black-hydra

--------------------------------------

E4GL30S1NT – Herramienta sencilla de recopilación de información

1: <https://github.com/C0MPL3XDEV/E4GL30S1NT>

--------------------------------------

Herramienta de recopilación de información

1: https://github.com/CybernetiX-S3C/InfoSploit

--------------------------------------

Una herramienta que crea un certificado falsificado de cualquier sitio web en línea y firma un Ejecutable para AV Evasion. Funciona tanto para Windows como para Linux.

1: https://github.com/sankethj/CarbonCopy

--------------------------------------

La primera herramienta de pirateo de cámara compatible con Python

1: https://github.com/sankethj/z-cam

--------------------------------------

Inyectar código malicioso en \*.debs

1: https://github.com/UndeadSec/Debinject

--------------------------------------

Recopilar o buscar sitios web que son vulnerables a la inyección de sql (herramientas GUI)

1: https://github.com/Ranginang67/WSS

--------------------------------------

🔥Herramientas de pentest de Firecrack: ataque aleatorio de piratería de Facebook, desfiguración, buscador de administradores, Bing dorking:

1: https://github.com/Ranginang67/Firecrack

--------------------------------------

🔍Crypton: herramientas linux Pentester, pruebas de penetración y piratería ética

1: https://github.com/Ranginang67/Crypton

--------------------------------------

Scripts de bash personalizados que se utilizan para automatizar diversas tareas de pruebas de penetración, incluidos el reconocimiento, el escaneo, el análisis y la creación de cargas maliciosas y oyentes con Metasploit.

1: https://github.com/leebaird/discover

--------------------------------------

⛤Generador Keylogger para Windows escrito en Python⛤

1: https://github.com/FZGbzuw412/SATANKLGR

--------------------------------------

Una herramienta de piratería para crear virus.

1: https://github.com/sina-yeganeh/pc-killer

--------------------------------------

Herramienta de ataque de red

1: <https://github.com/hatRiot/zarp>

--------------------------------------

Dorking google con python (fácil) (soporte Termux)

1: https://github.com/Yutixcode/Dolkings

--------------------------------------

Herramienta de ataque automático de IP o dominio (#1)

1: https://github.com/Bhai4You/Ip-Attack

--------------------------------------

Marco Evil-Droid.

1: https://github.com/M4sc3r4n0/Evil-Droid

--------------------------------------

Un programa SOCMINT/OSINT que le permite recopilar todos los datos de ubicación disponibles en las publicaciones de un perfil de Instagram para ubicarlos en un mapa.

1: <https://github.com/bernsteining/instaloctrack>

--------------------------------------

Use Ngrok en Termux con opciones avanzadas

1: <https://github.com/noob-hackers/tunnel>

--------------------------------------

Obtenga tokens de Discord, contraseñas y cookies de Chrome, y más

1: <https://github.com/NightfallGT/Mercurial-Grabber>

--------------------------------------

Una herramienta para la explotación remota de ADB en Python3 para todas las máquinas.

1: <https://github.com/aerosol-can/PhoneSploit>

--------------------------------------

¡Instala Kali Linux en Android usando Termux!

1: <https://github.com/MasterDevX/Termux-Kali>

--------------------------------------

¡Instala las herramientas ADB y FastBoot en Termux!

1: <https://github.com/MasterDevX/Termux-ADB>

--------------------------------------

Atajo de teclas Termux

1: https://github.com/karjok/terkey

--------------------------------------

Lockphish es una herramienta para ataques de phishing en la pantalla de bloqueo, diseñada para capturar las credenciales de Windows, el PIN de Android y el código de acceso de iPhone.

1: <https://github.com/JasonJerry/lockphish>

--------------------------------------

Verifique si un correo electrónico O número de teléfono O nombre de usuario está asociado con una cuenta de Facebook y obtenga información sobre la cuenta

1: <https://github.com/yasserjanah/FBchecker>

--------------------------------------

cSploit: el conjunto de herramientas profesional de seguridad de TI más completo y avanzado en Android.

1: https://github.com/cSploit/android

--------------------------------------

🖼️Una herramienta de información del sistema de línea de comandos escrita en bash 3.2+

1: https://github.com/dylanaraps/neofetch

--------------------------------------

Herramienta de red, reconocimiento y seguridad ofensiva para sistemas Linux.

1: <https://github.com/medpaf/hawk>

--------------------------------------

Reescritura del popular auditor de redes inalámbricas, “wifite”

1: <https://github.com/derv82/wifite2>

--------------------------------------

Herramienta de descifrado de todas las bibliotecas base

1: https://github.com/Err0r-ICA/Basekiller

--------------------------------------

Morpheus – Automatización de Ettercap TCP/IP (herramienta de secuestro MITM)

1: https://github.com/r00t-3xp10it/morpheus

--------------------------------------

Script para generar una aplicación de Android para rastrear la ubicación en tiempo real

1: https://github.com/indexnotfound404/DroidTracker

--------------------------------------

Ataques para la herramienta de enrutador

1: https://github.com/byteSalgado/router-kill

--------------------------------------

💣Kit de herramientas de denegación de servicio de Impulse

1: <https://github.com/LimerBoy/Impulse>

--------------------------------------

Eliminar cuenta de Facebook (informe masivo)

1: <https://github.com/bhikandeshmukh/fbreport>

--------------------------------------

DragonMS es herramientas para ddos, escáner, rastreador, generador de carga útil msfvenom y scraping

1: https://github.com/Malam-X/DragonMS

--------------------------------------

👽Programa para el control remoto de computadoras con Windows a través del bot de Telegram. Escrito en C#

1: <https://github.com/LimerBoy/ToxicEye>

--------------------------------------

Esta herramienta se usa para ataques de inundación.

1: <https://github.com/IncredibleHacker/Fl00d-Attacker>

--------------------------------------

Rastreador de ubicación GPS preciso (teléfonos Android, IOS, Windows).

1: https://github.com/bhikandeshmukh/MapEye

--------------------------------------

📡Herramienta de sobrecarga DDOS (capa 7)

1: https://github.com/7zx/overload

--------------------------------------

Crea hasta mil puntos de acceso WiFi con SSID personalizados.

1: https://github.com/spacehuhn/esp8266\_beaconSpam

--------------------------------------

🔑Descifrar contraseñas de navegadores basados ​​en cromo, cookies, tarjetas de crédito, historial, marcadores, autocompletar. Se admite la versión > 80.

1: https://github.com/LimerBoy/Adamantium-Thief

--------------------------------------

Python SYN Flood Attack Tool, puede iniciar el ataque SYN Flood con esta herramienta. Simple y eficiente.

1: https://github.com/EmreOvunc/Python-SYN-Flood-Attack-Tool

--------------------------------------

Script multiplataforma para encontrar rápidamente el proveedor asociado con una dirección MAC

1: <https://github.com/henriksb/MACVendorLookup>

--------------------------------------

Convierta rápidamente cualquier archivo en un troyano disfrazado de cualquier tipo de archivo

1: <https://github.com/henriksb/TrojanGenerator>

--------------------------------------

Script de python extremadamente simple para encontrar anagramas

1: <https://github.com/henriksb/Anagram-solver>

--------------------------------------

Herramientas Spoof IP IPv4 IPv6 ( hackingyseguridad.com )

1: <https://github.com/hackingyseguridad/spoof>

--------------------------------------

Fuerza bruta

1: <https://github.com/hackingyseguridad/bruteweb>

--------------------------------------

Busca hostname IP en los DNS por palabra o dominio (hackingyseguridad.com)

1: <https://github.com/hackingyseguridad/buscahost>

--------------------------------------

Análisis automático de vulnerabilidades WEB ( hackingyseguridad.com )

1: <https://github.com/hackingyseguridad/webaudit>

--------------------------------------

Utilidades de explotación SSH por fuerza bruta

1: <https://github.com/hackingyseguridad/ssha>

--------------------------------------

BlackStorm Ataque DDOS, envio paquetes UDP a activos IP con filtrado que reflexionan respondiendo con ICMP type 3 code 3 a IP origen victima

1: https://github.com/hackingyseguridad/blackstorm

--------------------------------------

Detectar vulnerabilidades de Path traversal con nmap1: https://github.com/hackingyseguridad/nmap

--------------------------------------

Suplantacion pagina web con captura de credenciales

1: <https://github.com/hackingyseguridad/post>

--------------------------------------

Espia trafico de la red NETSPY.sh ( hackingyseguridad.com )

1: <https://github.com/hackingyseguridad/netspy>

--------------------------------------

URL de prueba XSS ( hackingyseguridad.com )

1: <https://github.com/hackingyseguridad/xsstest>

--------------------------------------

Linux como router con reenvío de IP (hackingyseguridad.es)

1: https://github.com/hackingyseguridad/ipforward

--------------------------------------

Dnspoison inyecta respuestas dns con IP host falso

1: https://github.com/hackingyseguridad/dnspoison

--------------------------------------

Tortura de agua. Ataques a los DNS autoritativos de un dominio (hackingyseguridad.com)

1: https://github.com/hackingyseguridad/watertorture

--------------------------------------

¡Escanee aplicaciones sospechosas con más de 60 antivirus diferentes con solo dos clics y cinco segundos!

1: https://github.com/henriksb/VirusTotalScanner

--------------------------------------

Izanami Framework es un marco de ataques de phishing, que utiliza un ataque de suplantación de identidad ARP y un ataque de suplantación de DNS para redirigir todas las solicitudes HTTP de los dispositivos LAN a una dirección específica para realizar un ataque de phishing potente, IZanami inyecta el archivo beef-xss hook.js en cada página HTML solicitada , para apuntar y explotar los navegadores de los usuarios.

1: <https://github.com/yasserjanah/IZanamiFramework>

--------------------------------------

Rastrear usuarios de Omegle (no se para que sirve xd)

1: https://github.com/yasserjanah/OmegleTracker

--------------------------------------

El script de Python ataca todas las cuentas de redes sociales

1: https://github.com/yasserjanah/ZeS0MeBr

--------------------------------------

Compruebe si un {id, nombre de usuario, número de teléfono, correo electrónico} está asociado con una cuenta de Facebook

1: https://github.com/yasserjanah/FacebookChecker

--------------------------------------

CNA es un script de automatización de redes para acelerar la configuración de enrutadores y conmutadores de Cisco

1: https://github.com/yasserjanah/CiscoNetworkAutomation

--------------------------------------

Phish archivos de Excel protegidos con contraseña.

1: <https://github.com/S3cur3Th1sSh1t/Excel-Phish>

--------------------------------------

MR\_SPOOF es una herramienta de suplantación de paquetes arp

1: <https://github.com/swagkarna/MR_SPOOF>

--------------------------------------

Ladrón simple de Google Chrome, envía contraseñas a través de Telegram a un canal privado

1: <https://github.com/MLX15/Google-Stealer>

--------------------------------------

Cargador remoto automático rclone, con soporte para múltiples emparejamientos remotos/carpetas. Funcionalidad de UnionFS Cleaner: eliminación de archivos de eliminación de UnionFS y sus archivos correspondientes en controles remotos rclone. Sincronizador remoto automático: sincronización entre diferentes controles remotos a través de una instancia de servidor de Scaleway, que se crea y destruye en cada sincronización.

1: <https://github.com/l3uddz/cloudplow>

--------------------------------------

La herramienta de reconocimiento simple automatiza su proceso de reconocimiento

1: <https://github.com/0xarun/s1mr3c>

--------------------------------------

La locura de Katty [L7/L4 DDOS y HERRAMIENTAS]

1: <https://github.com/electr0lulz/kattymad>

--------------------------------------

Explotación masiva para CVE 2022-29464 en Carbon

1: <https://github.com/electr0lulz/Mass-exploit-CVE-2022-29464>

--------------------------------------

Vajra es una herramienta basada en la interfaz de usuario con múltiples técnicas para atacar y enumerar en el entorno de Azure y AWS del objetivo. Cuenta con una interfaz de usuario intuitiva basada en la web construida con el módulo Python Flask para una mejor experiencia de usuario. El enfoque principal de esta herramienta es tener diferentes técnicas de ataque en un solo lugar con interfaz de interfaz de usuario web …

1: <https://github.com/TROUBLE-1/Vajra>

--------------------------------------

Detector de intrusos WIFI/LAN. Verifica los dispositivos conectados y te alerta con dispositivos desconocidos. También avisa de la desconexión de dispositivos "siempre conectados"

1: <https://github.com/pucherot/Pi.Alert>

--------------------------------------

SMS, correo electrónico, WhatsApp, Telegram, bombardero Discord y atacante DoS. Plataformas compatibles: Windows, Linux, MacOS, Termux

1: <https://github.com/ebankoff/Beast_Bomber>

--------------------------------------

Esta herramienta escaneará todas las URL en el archivo y proporcionará la longitud del contenido, el código de estado, el servidor y más.

1: <https://github.com/TROUBLE-1/codeza>

--------------------------------------

sigs3scann3r es una herramienta para escanear los permisos de depósito de AWS S3 y volcar el contenido del depósito cuando corresponda.

1: <https://github.com/hueristiq/hqs3scann3r>

--------------------------------------

¡Con este programa puedes crear un virus “falso”!.

1: <https://github.com/swagkarna/Virus-Creator>

--------------------------------------

Web Scraper es una mezcla de herramientas web para la piratería web, el reconocimiento, la recompensa por errores, etc. Esta herramienta consta de las 20 herramientas web más utilizadas para la evaluación de la seguridad.

1: <https://github.com/Encryptor-Sec/Web-Scraper>

--------------------------------------

Un kit de herramientas de piratería web (imagen acoplable).

1: <https://github.com/hueristiq/web-hacking-toolkit>

--------------------------------------

ZipKiller es una herramienta basada en Python para descifrar contraseñas de archivos zip utilizando el método de fuerza bruta. La herramienta contiene una muestra de Wordlist de 1000 contraseñas. El usuario puede cambiar el diccionario de contraseñas en consecuencia.

1: <https://github.com/Encryptor-Sec/ZipKiller>

--------------------------------------

XSSearch es una herramienta completa de XSS reflejada construida en el marco de Selenium en lenguaje Python. Contiene más de 3000 payloads para automatizar ataques XSS y validar puntos finales XSS

1: <https://github.com/Encryptor-Sec/XSSearch>

--------------------------------------

Sentry es el monitoreo de aplicaciones multiplataforma, con un enfoque en el informe de errores.

1: <https://github.com/getsentry/sentry>

--------------------------------------

Urraca secreta - Herramienta de detección de secretos

1: <https://github.com/punk-security/secret-magpie-cli>

--------------------------------------

dnsReaper: ¡herramienta de adquisición de subdominios para atacantes, cazarrecompensas de errores y el equipo azul!

1: <https://github.com/punk-security/dnsReaper>

--------------------------------------

Escaneo vuls: 15000+PoC; 23 tipos de descifrado de contraseñas de aplicaciones; 7000+huellas dactilares web; 146 protocolos y más de 90000 reglas Escaneo de puertos; Fuzz, HW, increíble BugBounty ( ͡° ͜ʖ ͡°)…

1: <https://github.com/hktalent/scan4all>

--------------------------------------

Suplantar los datos de su ubicación y el agente de usuario

1: <https://github.com/z0ccc/Vytal>

--------------------------------------

ZipKiller es una herramienta basada en Python para descifrar contraseñas de archivos zip utilizando el método de fuerza bruta. La herramienta contiene una muestra de Wordlist de 1000 contraseñas. El usuario puede cambiar el diccionario de contraseñas en consecuencia.

1: <https://github.com/Encryptor-Sec/ZipKiller>

--------------------------------------

Esto incluye los métodos de reconocimiento y explotación de Bug Bounty.

1: <https://github.com/glyptho/myreconmethods>

--------------------------------------

Rastreador rápido de contratos inteligentes

1: <https://github.com/0xsha/ChainWalker>

--------------------------------------

ExifLooter encuentra la geolocalización en todas las direcciones URL y directorios de imágenes y también se integra con OpenStreetMap

1: <https://github.com/glyptho/myreconmethods>

--------------------------------------

DLLirant es una herramienta para automatizar las investigaciones de DLL Hijacking en un binario específico.

1: <https://github.com/Sh0ckFR/DLLirant>

--------------------------------------

DNS para sitios web de omisión de restricciones de país y rastreadores de anuncios de bloque

1: <https://github.com/Zusyaku/DNS-Setting-Android>

--------------------------------------

TheRouter es un enrutador de paquetes de software basado en bibliotecas DPDK y NPF.

1: <https://github.com/alexk99/the_router>

--------------------------------------

NPF: filtro de paquetes con inspección de estado, NAT, conjuntos de IP, etc.

1: <https://github.com/rmind/npf>

--------------------------------------

CrimeFlare es una herramienta útil para eludir sitios web protegidos por CloudFlare WAF, con esta herramienta puede ver fácilmente la IP real de los sitios web que han sido protegidos por CloudFlare. La información resultante es ciertamente muy útil para realizar más pruebas de penetración y analizar sitios web con el mismo servidor.

1: <https://github.com/zidansec/CloudPeler>

--------------------------------------

Root: acceda a los privilegios de root en termux sin rootear el dispositivo Android

1: <https://github.com/adarshaddee/root>

--------------------------------------

Avance más profundamente en las redes al descubrir hosts y puertos, utilizando una máquina comprometida a través de SSH

1: <https://github.com/Xeonrx/Puwr>

--------------------------------------

Una herramienta automatizada que puede rastrear, llenar formularios, activar páginas de error/depuración y "saquear" secretos del código de sitios orientado al cliente simultáneamente.

1: <https://github.com/redhuntlabs/HTTPLoot>

--------------------------------------

Sitio que recopila palabras y billeteras secretas, y luego lo agregaremos y enviaremos datos a los telegramas. Después de recibir las palabras y direcciones secretas de las billeteras criptográficas, puede restaurarlas y venderlas o venderlas.

1: <https://github.com/trewisscotch/DeFi-phishing->

--------------------------------------

Escalada de privilegios de Linux con secuencias de comandos para la vulnerabilidad CVE-2022-0847 "Dirty Pipe"

1: <https://github.com/rexpository/linux-privilege-escalation>

--------------------------------------

Omita el antivirus y obtenga un shell inverso en Windows con Powercat v2

1: <https://github.com/rexpository/reverseshell-powercat-v2>

--------------------------------------

Panel DDoS de capa 7 con Cloudflare Bypass (UAM, CAPTCHA, BFM, etc.)

1: <https://github.com/firstapostle/Blood>

--------------------------------------

Zero-attacker es una herramienta de piratería multipropósito con más de 24 herramientas como token-gen, ddos ​​y más (código público en algún momento)

1: <https://github.com/AsjadOooO/Zero-attacker>

--------------------------------------

Esta herramienta lo ayudará a extraer el número de teléfono de la URL masiva

1: <https://github.com/W3LLLL/WWP>

--------------------------------------

Un escáner de vulnerabilidades "Spring4Shell".

1: <https://github.com/redhuntlabs/Hunt4Spring>

--------------------------------------

Esta herramienta validará todos los números de teléfono de forma masiva y los ordenará por región.

1: <https://github.com/W3LLLL/WPV>

--------------------------------------

Un escáner de información de identificación personal (PII) impulsado por IA.

1: <https://github.com/redhuntlabs/Octopii>

--------------------------------------

Seema - Herramienta generadora de contraseñas aleatorias. Esto puede ayudarlo a aumentar la protección de su privacidad.

1: <https://github.com/adarshaddee/Seema>

--------------------------------------

Hackear la base de datos de Google Chrome: obtener nombre de usuario y contraseñas

1: <https://github.com/ncorbuk/Google-Chrome-Browser-Database-Hack>

--------------------------------------

Reconocimiento de rostros con android

1: <https://github.com/everblut/Face-detection>

--------------------------------------

Este script esta creado con finers educativos (creador de payloads)

1: https://github.com/error404-notfound/PayloadCreator-Termux

--------------------------------------

Generación y escucha de diferentes tipos de payloads de Metasploit-framework de forma rápida y fácil, dentro y fuera de la red local!

1: https://github.com/error404-notfound/PayloadCreator-Dialog

--------------------------------------

Este es un grupo dedicado a temas de hacking ético los guiones son hechos de manera educativa no nos responsabilizamos de su uso… Porque el conocimiento debe ser libre …..

1: https://github.com/error404-notfound/Error404-Social-Termux

--------------------------------------

Código de bot de Discord para detener a los usuarios que están estafando con mensajes falsos de discord nitro gratis en los servidores para robar las cuentas de los usuarios.

1: <https://github.com/H3cJP/AntiScam>

--------------------------------------

Funciones o scripts útiles para usar en Pentesting

1: https://github.com/H3cJP/usefulTools

--------------------------------------

Cookies Phishing Usando Wifi

1: <https://github.com/TRKBKR/DEPRESS-WIFI>

--------------------------------------

Obtén cierto tipo de información básica de un número de teléfono en específico

1: <https://github.com/LCA-HACK/DoxPhone>

--------------------------------------

Script en bash que te automatiza una máquina enfocada al pentesting basado en el entorno de s4vitar

1: <https://github.com/sikumy/bspwm4pentest>

--------------------------------------

🕵🏻‍♂️ bifurcación mínima de nanospy, con más funciones

1: <https://github.com/Aslemammad/tinyspy>

--------------------------------------

Un sencillo programa para mostrar la pantalla como estaba hace 5 segundos

1: <https://github.com/globalpolicy/Rewind5s>

--------------------------------------

Este repositorio contiene el código fuente de la aplicación de Android que se puede importar en Android Studio. Actualmente obtiene todas las notificaciones, chats de whatsapp, chats de instagram en tiempo real.

1: <https://github.com/patanjalikr13/Android-Undetectable-Spy-App>

--------------------------------------

Módulo creado para la gestión de Wi-Fi en Android con python

1: <https://github.com/yaxter/wifidroid>

--------------------------------------

DoS attack, Ataque DoS a redes Wifi, herramienta capaz de Expulsar a todos los usuarios de una red Wifi dejándolos sin acceso a internet.

1: https://github.com/yaxter/DoSWifi

--------------------------------------

Bloquear la conexión wifi y los micrófonos de todos los dispositivos Amazon Echo y Google Home que te rodean

1: https://github.com/T-vK/alexa-jammer

--------------------------------------

Crear espías automáticos desde clases.

1: https://github.com/hirezio/auto-spies

--------------------------------------

Una herramienta de administración remota para dispositivos Android

1: https://github.com/globalpolicy/PhoneMonitor

--------------------------------------

Bot de WhatsApp, es un bot automatizado para juegos e información que se ejecuta con nodejs

1: <https://github.com/FG98F/dylux-bot>

--------------------------------------

Modifique un mensaje para que tenga la firma CRC deseada.

1: <https://github.com/madler/spoof>

--------------------------------------

Sistema basico para la realizacion de Email Spoofing atravez de una cosola bash y un servidor con http

1: https://github.com/MatiasTillerias/email-spoof

--------------------------------------

Revisión y verificación de la especificación del formato de datos comprimidos de Brotli.

1: https://github.com/madler/brotli

--------------------------------------

Apkatshu es una herramienta para extraer URL, correos electrónicos, direcciones IP y datos interesantes de archivos APK

1: <https://github.com/0xPwny/Apkatshu>

--------------------------------------

HEAP (Notas/Técnicas/Explotación/Reseñas)

1: <https://github.com/0xPwny/heap_bible>

--------------------------------------

Este es un script fácil y rápido para ser usuario root en Termux

1: <https://github.com/JoseZpt/T-root>

--------------------------------------

Explotador masivo automatizado

1: <https://github.com/NullArray/AutoSploit>

--------------------------------------

Script de Python con tecnología de Selenium para automatizar la búsqueda de aplicaciones web vulnerables.

1: https://github.com/NullArray/DorkNet

--------------------------------------

Infectar movil con número de telefono

1: <https://github.com/novalattasya/6virus>

Pkg update && pkg upgrade

-pkg install bash

 -git clone <https://github.com/novalattasya/6virus>

-cd 6virus

-ls

-sh 6VIRUS.sh

--------------------------------------

Transforma tu payload.exe en un documento de palabra falsa (.ppt)

1: <https://github.com/r00t-3xp10it/backdoorppt>

--------------------------------------

Use una imagen falsa.jpg para explotar objetivos (ocultar extensiones de archivo conocidas)

1: <https://github.com/r00t-3xp10it/FakeImageExploiter>

--------------------------------------

Morpheus - Automatización de Ettercap TCP/IP (herramienta de secuestro MITM)

1: <https://github.com/r00t-3xp10it/morpheus>

--------------------------------------

Un script que crea un paylaod con msfvenom que admite: “Android/Linux/Windows” con las opciones para: “codificar” e “incrustar” e inicia un oyente

1: <https://github.com/yelhamer/Payload-Generator>

--------------------------------------

Las mejores aplicaciones de virus y la herramienta de creación de mensajes VIRUS

1: https://github.com/Devil-Tigers/TigerVirus

--------------------------------------

Crear troyano personalizado

1: <https://github.com/VWolf13/delator>

--------------------------------------

Rastreador de personas en Internet: herramienta de análisis e investigación OSINT de Jose Pino

1: <https://github.com/jofpin/trape>

--------------------------------------

Pruebe de forma remota la seguridad de la contraseña del software de blogs de WordPress

1: <https://github.com/atarantini/wpbf>

--------------------------------------

Clonador de Facebook Yahoo

1: https://gitlab.com/W1nz0N/fyc.git

--------------------------------------

Bot creado por spider también hecho con python

1: https://github.com/spider863644/Botel

--------------------------------------

Un raspador y verificador de enlaces de grupo de Whatsapp

1: <https://github.com/TheSpeedX/WhatScraper>

--------------------------------------

El AVCutter más peligroso para Android [PAYLOAD] Herramienta de ofuscación.

1: <https://github.com/CYBERSECARYAN/AVCutter>

--------------------------------------

Ladrón de contraseñas de ejecución automática USB / CD / DVD

1: <https://github.com/tresacton/PasswordStealer>

--------------------------------------

Remcos Professional crackeado por Alcatraz3222-Trojan-RAT de administración remota

1: <https://github.com/cybertoxin/Remcos-Professional-Cracked-By-Alcatraz3222>

--------------------------------------

Una red de bots HTTPS centralizada y de código abierto

1: https://github.com/Raffy27/OrionServer

--------------------------------------

(Una tontería xd.) Elimina la carpeta C:/Windows/System32 por ejecución.

1: <https://github.com/jimix-trz/System_Deleter>

--------------------------------------

Macro\_pack es una herramienta de @EmericNasi que se utiliza para automatizar la ofuscación y la generación de documentos de Office, scripts de VB, accesos directos y otros formatos para evaluaciones de pentest, demostración e ingeniería social. El objetivo de macro\_pack es simplificar la explotación, eludir el antimalware y automatizar el proceso desde la generación de scripts y macros maliciosos hasta fin…

1: <https://github.com/sevagas/macro_pack>

--------------------------------------

Shell inverso sobre TLS (en golang)

1: <https://github.com/loutrerusse/RevShellTLS>

--------------------------------------

🔐Método AES de cifrado de mensajes (256 bits, método CFB), muchos hashes, codificadores.

1: <https://github.com/loutrerusse/CryptoRusse>

--------------------------------------

📡 Convierta un nombre de host en una IP y una IP en un nombre de host, realice un WHOIS, obtenga toda la información de una IP o un nombre de host.

1: <https://github.com/loutrerusse/RusseIP>

--------------------------------------

Herramienta DDOS: para eliminar sitios web pequeños con HTTP FLOOD. Escáner de puertos: Para conocer los puertos abiertos de un sitio. FTP Password Cracker: para piratear el sistema de archivos de los sitios web. Banner Grabber: para ejecutar el servicio o el software en un puerto. (Después de conocer las vulnerabilidades del software que ejecuta Google). Web Spider: para recopilar aplicaciones web pirateadas en…

1: <https://github.com/ritvikb99/dark-fantasy-hack-tool>

--------------------------------------

Bot automatizado para entrar en grupos de whatsapp enviar mensajes y salir

1: <https://github.com/marcopandolfo/WhatsAppGroupsSpammer>

--------------------------------------

Un simple troyano de python para 3.8 que crea una puerta trasera a través de netcat. Utilice esto de manera legal. No soy responsable de los daños causados ​​por este software.

1: <https://github.com/swagkarna/Simple-Python-Trojan>

--------------------------------------

Javascript botnet browser chrome firefox V2 es un registrador de teclas para capturar el número de tarjeta, la fecha de vencimiento, CVV cualquier sitio web, paypal, facebook, comercio electrónico, etc. El mejor registrador de teclas javascript

1: <https://github.com/hakanonymos/JavascriptKeylogger>

--------------------------------------

Esta es una aplicación espía de Android, que carga datos de usuario como contactos, mensajes, registro de llamadas, envía mensajes, fotos, videos, abre un enlace del navegador, etc. Android Rat

1: <https://github.com/abhinavsuthar/Android_Spy_App>

--------------------------------------

Inicio de sesión súper rápido WordPress Brute Force

1: <https://github.com/swagkarna/WordPress-Brute-Force>

--------------------------------------

📷 Instagram Bot – Herramienta para interacciones automatizadas de Instagram

1: <https://github.com/InstaPy/InstaPy>

--------------------------------------

[ Buscador de panel de administración / Buscador de página de inicio de sesión de administrador ] ¢σ∂є∂ ву 👻 (❤-❤) 👻

1: <https://github.com/mIcHyAmRaNe/okadminfinder3>

--------------------------------------

Oculte su mensaje secreto en cualquier archivo de audio Wave.

1: <https://github.com/techchipnet/HiddenWave>

--------------------------------------

Cree fácilmente Raspberry Pi 3 o Raspberry Pi Zero w como un enrutador WiFi Cree fácilmente Raspberry Pi 3 o Raspberry Pi Zero w como un enrutador WiFi

1: <https://github.com/techchipnet/PiFi>

--------------------------------------

PiFiTorAP es un simple script bash para configurar su Raspberry Pi 3 B/B+ como un punto de acceso WiFi anónimo.

1: <https://github.com/techchipnet/RPI-Tor-Wireless-Hotspot>

--------------------------------------

Este script detectará Canary Token en documentos de Microsoft Word

1: https://github.com/techchipnet/CanaryTokensDetector

--------------------------------------

🛅Contraseñas usando información personal

1: <https://github.com/mIcHyAmRaNe/PUPI>

--------------------------------------

Envía mensajes de texto anónimos con TOR y la API de TextBelt

1: <https://github.com/Da2dalus/CerebroSMS>

--------------------------------------

Encuentre el número de teléfono de cualquier usuario de Telegram

1: <https://github.com/swagkarna/Telegram_User_Number_Finder>

--------------------------------------

Controle computadoras remotas usando discord bot y python 3.

1: <https://github.com/UndeadSec/Idisagree>

--------------------------------------

Iplogger que envía registros a través de discord.

1: <https://github.com/graysuit/iplogger>

--------------------------------------

Generar dominios Unicode para IDN Homograph Attack y detectarlos.

1: https://github.com/UndeadSec/EvilURL

--------------------------------------

El falsificador de direcciones MAC mi nuevo concepto impide el seguimiento de direcciones MAC mejor que otros; aleatoriza la dirección mac en momentos aleatorios, para evitar el seguimiento de la ubicación del punto de acceso WIFI (común)/análisis de patrones MAC, configuración mac permanente también

1: <https://github.com/RightToPrivacy/MACcleaner>

--------------------------------------

crear cebolla ssh - + otros scripts para ayudar a un amigo de forma remota

1: <https://github.com/RightToPrivacy/ssh-onion>

--------------------------------------

(Privacidad de metadatos de red) Falsificador de dirección MAC con combinación adicional (opciones): nombre de host + falsificador de señal - \*¡sin desconexiones!\* Cambio de privacidad con Brand Mimics: ejecutar como comando o una nueva identidad aleatoria opcional en cada arranque; incluye banderas para cambiar continuamente tiempos aleatorios/cambiar direcciones OUI válidas + Aleatorizador de nombre de host + Dispositivo/Señal/ubicación y...

1: <https://github.com/RightToPrivacy/wipri>

--------------------------------------

🐞 Una herramienta para cambiar su dirección MAC o falsificar su dirección MAC con direcciones mac aleatorias rápidamente.

1: <https://github.com/DAILYHIJACKS/RapidMAC>

--------------------------------------

Una herramienta de python que te consigue invitaciones a grupos de whatsapp explotando a los tontos de Google🧠

1: <https://github.com/DAILYHIJACKS/whatscrap>

--------------------------------------

Este proyecto puede ayudarlo a piratear cualquier navegador y acceder al MIC de cualquier teléfono y enviarle el archivo de audio directamente a su almacenamiento.

1: <https://github.com/DAILYHIJACKS/amiaudible>

--------------------------------------

⚡️ Heimdall es una herramienta destinada a obtener el panel de administración del sitio web utilizando la fuerza bruta con la lista de palabras. ⚡️

1: <https://github.com/ygorsimoes/Heimdall>

--------------------------------------

🍷Dionisio es una herramienta capaz de automatizar todo el proceso de una prueba de penetración en un sitio web.🍷

1: <https://github.com/AngraTeam/Dionisio>

--------------------------------------

Herramienta de ataque de portal cautivo

1: <https://github.com/RaphaelAccessGranted/BadPortal>

--------------------------------------

“Socialx” es una herramienta troyana de ingeniería social y acceso remoto. Puede generar fud backdoor e incrustar cualquier archivo que desee dentro del archivo exe.

1: <https://github.com/AzizKpln/Social_X>

--------------------------------------

ProtOSINT es un script de Python que lo ayuda a investigar las cuentas de Protonmail y las direcciones IP de ProtonVPN

1: <https://github.com/pixelbubble/ProtOSINT>

--------------------------------------

Ransomware .NET simple que requiere que el usuario haga clic en el botón patpat 1,000,000 de veces para descifrar archivos

1: <https://github.com/swagkarna/patpatware>

--------------------------------------

Script de Python para explotar la prueba de velocidad del chat en vivo.

1: <https://github.com/RealALeon/typing-speed-test>

--------------------------------------

compruebe si un {id, nombre de usuario, número de teléfono, correo electrónico} está asociado con una cuenta de Facebook

1: <https://github.com/yasserjanah/FacebookChecker>

--------------------------------------

Autenticación básica HTTP de fuerza bruta, escrita con Go

1: <https://github.com/yasserjanah/BasicAuthBruteForcer>

--------------------------------------

Izanami Framework es un marco de ataques de phishing, que utiliza un ataque de suplantación de identidad ARP y un ataque de suplantación de DNS para redirigir todas las solicitudes HTTP de dispositivos LAN a una dirección específica para realizar un ataque de phishing potente, IZanami inyecta el archivo beef-xss hook.js en cada página HTML solicitada , para apuntar y explotar los navegadores de los usuarios.

1: <https://github.com/yasserjanah/IZanamiFramework>

--------------------------------------

Carga automáticamente las cookies robadas de ChromePass

1: <https://github.com/darkarp/autocookie>

--------------------------------------

Inyecte su ejecutable x64 bit a cualquier proceso, enmascarándolo como un proceso legítimo para la evasión de Anti-Virus.

1: <https://github.com/0xyg3n/PEx64-Injector>

--------------------------------------

Hackea el patrón de Android de Termux con esta herramienta

1: https://github.com/noob-hackers/hacklock

--------------------------------------

Herramienta de fuerza bruta para spotify

1: <https://github.com/wuseman/wspotify>

--------------------------------------

Herramienta de piratería automatizada que encontrará bases de datos filtradas con una precisión del 97,1 % para obtener el correo y la contraseña juntos de cargas recientes de https://pastebin.com . Soporte de fuerza bruta para cuentas de spotify, cuentas de instagram, servidores ssh, clientes de microsoft rdp y cuentas de gmail

1: <https://github.com/wuseman/EMAGNET>

--------------------------------------

TechNowHorse es un generador RAT (troyano de administrador remoto) para sistemas Windows/Linux escrito en Python 3.

1: <https://github.com/PushpenderIndia/thorse>

--------------------------------------

Buscar de links de phishing

1: <https://github.com/Viralmaniar/MurMurHash>

--------------------------------------

Shell Script para atacar conexiones inalámbricas utilizando las herramientas integradas de Kali. Admite todos los valores (WEP, WPS, WPA, WPA2)

1: <https://github.com/TermuxHackz/wifi-hacker>

--------------------------------------

Backdoor cualquier archivo .py – Implantador de puerta trasera para OS X y Linux

1: <https://github.com/SaltyViper/PyInfect>

--------------------------------------

xDisguise le permite disfrazar una extensión de archivo como cualquier otra extensión de su elección.

1: https://github.com/SaltyViper/xDisguise

--------------------------------------

Archivo de Python simple que envía la IP de la víctima, el nombre del host, la ubicación, etc., a su dirección de correo

1: <https://github.com/gowtham758550/ip-finder>

--------------------------------------

Responder es un envenenador LLMNR, NBT-NS y MDNS, con un servidor de autenticación no autorizado HTTP/SMB/MSSQL/FTP/LDAP incorporado que admite NTLMv1/NTLMv2/LMv2, seguridad extendida NTLMSSP y autenticación HTTP básica.

1: <https://github.com/SpiderLabs/Responder>

--------------------------------------

Una poderosa herramienta de sensor para descubrir paneles de inicio de sesión y escaneo POST Form SQLi

1: <https://github.com/Mr-Robert0/Logsensor>

--------------------------------------

Cross Site "Scripter" es un marco automático para detectar, explotar y reportar vulnerabilidades XSS en aplicaciones basadas en web.

1: <https://github.com/Xcod3bughunt3r/xsser>

--------------------------------------

jsubfinder busca páginas web en busca de javascript y las analiza en busca de subdominios y secretos ocultos (wip).

1: <https://github.com/ThreatUnkown/jsubfinder>

--------------------------------------

Harvis está diseñado para automatizar su infraestructura C2.

1: <https://github.com/thiagomayllart/Harvis>

--------------------------------------

Un análisis de código estático para WordPress (y PHP)

1: <https://github.com/webarx-security/wpbullet>

--------------------------------------

Kit de herramientas de recolección posterior a la infección

1: <https://github.com/thomasareed/pict>

--------------------------------------

Marco de persistencia totalmente modular

1: <https://github.com/FortyNorthSecurity/PersistAssist>

--------------------------------------

EyeWitness está diseñado para tomar capturas de pantalla de sitios web, proporcionar información del encabezado del servidor e identificar las credenciales predeterminadas si es posible.

1: <https://github.com/FortyNorthSecurity/EyeWitness>

--------------------------------------

Herramienta de Windows para volcar archivos PE de malware de la memoria al disco para su análisis.

1: <https://github.com/glmcdona/Process-Dump>

--------------------------------------

Python Script para Telegram Bot está especialmente diseñado para pentest y bug bounty. Es como el caparazón de un telegrama.

1: <https://github.com/Drayko/Bot-Bounty>

--------------------------------------

Crybat (anteriormente conocido como Jlaive) es una herramienta de evasión de antivirus que puede convertir ejecutables en archivos por lotes indetectables. No se garantiza que los ensamblajes .NET funcionen.

1: <https://github.com/ch2sh/Crybat>

--------------------------------------

Una base de conocimientos de técnicas procesables de respuesta a incidentes

1: <https://github.com/atc-project/atc-react>

--------------------------------------

Reglas para validar recursos e infraestructura de Azure como código (IaC) mediante PSRule.

1: <https://github.com/Azure/PSRule.Rules.Azure>

--------------------------------------

ZMap es un rápido escáner de red de un solo paquete diseñado para encuestas de red en Internet.

1: <https://github.com/zmap/zmap>

--------------------------------------

🔮Visibility Across Space and Time: el motor de telemetría de red para investigaciones de seguridad basadas en datos.

1: <https://github.com/tenzir/vast>

--------------------------------------

Kit de investigación de ataques BloodHound

1: <https://github.com/BloodHoundAD/BARK>

--------------------------------------

🚌Threat Bus: una capa de difusión de inteligencia de amenazas para herramientas de seguridad de código abierto.

1: <https://github.com/tenzir/threatbus>

--------------------------------------

Urraca secreta - Herramienta de detección de secretos

1: <https://github.com/punk-security/secret-magpie-cli>

--------------------------------------

Durante mis compromisos de respuesta a incidentes, me di cuenta de que descargar datos volátiles siempre se hace mal (o al menos de una manera diferente a la mejor). Además, los datos nunca tienen el mismo formato, lo que hace que el análisis sea más difícil (si no imposible) de automatizar.

1: <https://github.com/gtworek/VolatileDataCollector>

--------------------------------------

Collect-MemoryDump: creación automatizada de instantáneas de memoria de Windows para DFIR

1: <https://github.com/evild3ad/Collect-MemoryDump>

--------------------------------------

Lockbit3.0 Microsoft Defender MpClient.dll DLL Secuestro PoC

1: <https://github.com/Sh0ckFR/Lockbit3.0-MpClient-Defender-PoC>

--------------------------------------

Script para ejecutar shodan-nrich en los subdominios de un dominio específico o una lista de dominios

1: <https://github.com/Sh0ckFR/easynrich>

--------------------------------------

Burp Requests Fusion es una extensión de Burp para agregar encabezados HTTP personalizados (también encabezados dinámicos) desde un servidor local a todas las solicitudes HTTP

1: <https://github.com/Sh0ckFR/Burp-Requests-Fusion>

--------------------------------------

Un patio de recreo eBPF

1: <https://github.com/quarkslab/peetch>

--------------------------------------

El uso de la herramienta de piratería WH-HackerExploit (WH-Boomber) para atacar objetivos sin previo consentimiento mutuo es ilegal. Es responsabilidad del usuario final obedecer todas las leyes locales, estatales y federales aplicables. Los desarrolladores no asumen ninguna responsabilidad y no son responsables de ningún mal uso o daño causado por este programa. Solo uso con fines educativos.

1: <https://github.com/swagkarna/WH-boomber>

--------------------------------------

💂 Un generador de carga útil de Android y monitor RAT para Android y PC.

1: https://github.com/swagkarna/Linux\_Droid

--------------------------------------

Proxphish es una herramienta de phishing avanzada

1: <https://github.com/swagkarna/proxphish>

--------------------------------------

Herramienta avanzada de phishing para Instagram

1: <https://github.com/swagkarna/GramPhish>

--------------------------------------

KratosKnife es una BOTNET avanzada escrita en Python 3 para el sistema operativo Windows. Viene con muchas funciones avanzadas, como métodos de detección de VM y persistencia, carpeta integrada, etc.

1: <https://github.com/swagkarna/KratosKnife>

--------------------------------------

Captura la pantalla de la víctima y envíala a Gmail

1: <https://github.com/swagkarna/SK-Shot>

--------------------------------------

Es un script simple para encontrar páginas de inicio de sesión de administrador.

1: <https://github.com/swagkarna/AdminDriller>

--------------------------------------

Este script es solo para distraer al usuario de la operación de su sistema operativo Windows.

1: https://github.com/swagkarna/Self-Replicating-Virus

--------------------------------------

Esta pequeña aplicación de ejemplo consulta el servicio web, ejem, de la DGT que permite obtener el tipo de distintivo ambiental asociado a una matrícula.

1: <https://github.com/mdelapenya/dgt>

--------------------------------------

Obtener información del sistema operativo usar golang

1: <https://github.com/mdelapenya/goInfo>

--------------------------------------

Herramienta para verificar si una aplicación está instalada en el dispositivo de destino a través de un enlace

1: https://github.com/swagkarna/underhanded

--------------------------------------

Generador de carga útil FUD win32 msfvenom

1: <https://github.com/swagkarna/catchyou>

--------------------------------------

Un script de aumento de vistas. Puede aumentar la visualización en cualquier sitio web que no esté protegido por cloudfare.

1: https://github.com/swagkarna/HBot

--------------------------------------

Mobile Security Framework (MobSF) es una aplicación móvil todo en uno automatizada (Android/iOS/Windows) para pruebas de penetración, análisis de malware y marco de evaluación de seguridad capaz de realizar análisis estáticos y dinámicos.

1: <https://github.com/swagkarna/Mobile-Security-Framework-MobSF>

--------------------------------------

Keylloger que envía registros en whatsapp

1: <https://github.com/swagkarna/keylogger_whatsapp>

--------------------------------------

Tutorial sobre la simulación de phishing a partir de una identificación de correo falsificada

1: <https://github.com/swagkarna/Phishing-with-spoofed-mail-id>

--------------------------------------

Herramienta Termux Hunter (Shikari): Hackea a tu víctima Termux con Shikari

1: https://github.com/swagkarna/Shikari

--------------------------------------

WRecon es un escáner web no invasivo de código abierto. Está diseñado para descubrir todas las URL en un sitio web de forma recursiva, sin usar fuerza bruta o acceso no autorizado. Viene con un motor de camuflaje y buenas características para pentesting.

1: https://github.com/swagkarna/wrecon

--------------------------------------

Solo una herramienta para explotar en Android.

1: <https://github.com/swagkarna/saydog-framework>

--------------------------------------

🤒 Un rastreador de tráfico de red alternativo y moderno.

1: <https://github.com/swagkarna/sniffer>

--------------------------------------

Azure Outlook Command & Control (C2): controle de forma remota un dispositivo Windows comprometido desde su buzón de correo de Outlook. Herramienta de emulación de amenazas para APT de Corea del Norte InkySquid / ScarCruft / APT37. TTP: use la API de Microsoft Graph para operaciones C2.

1: https://github.com/swagkarna/azureOutlookC2

--------------------------------------

Panel de administración del sitio.

1: <https://github.com/swagkarna/AdminHack>

--------------------------------------

Script simple de Python 3 para detectar la vulnerabilidad de la biblioteca Java “Log4j” (CVE-2021-44228) para una lista de URL con subprocesos múltiples

1: <https://github.com/swagkarna/log4j-detect>

--------------------------------------

Servidor C2 para conectarse a una máquina víctima a través de shell inverso

1: <https://github.com/swagkarna/C2_Server>

--------------------------------------

Sacar datos de cuenta discord

1: <https://github.com/swagkarna/Hande-Stealer>

--------------------------------------

Script para ataques DOS rápidos y sencillos en dispositivos bluetooth con fines de pentest

1: <https://github.com/swagkarna/BLUETOOTH-DOS-ATTACK-SCRIPT>

--------------------------------------

Software espía de Android de código abierto

1: <https://github.com/swagkarna/AdoBot>

--------------------------------------

Utilidad de fuerza bruta de esteganografía para descubrir datos ocultos dentro de archivos

1: <https://github.com/swagkarna/StegCracker>

--------------------------------------

Hacer que el virus sea indetectable para todos los antivirus

1: <https://github.com/swagkarna/VirusUndetectable>

--------------------------------------

Herramienta de raspado de grupo de telegramas. Obtener toda la información sobre los miembros del grupo

1: <https://github.com/swagkarna/TeleGram-Scraper>

--------------------------------------

𝐅𝐀𝐐𝐔𝐄; ES UNA IDENTIDAD FALSA: SPOOF-EMAIL, EL COMPAÑERO PERFECTO PARA EL PHISHING. (mejor fhishing e-mail que pude encontrar)

1: https://github.com/ByDog3r/FAQUE

--------------------------------------

HTML y CSS Página de phishing de Instagram que le envía las credenciales de la víctima a través de su webhook de Discord

1: <https://github.com/swagkarna/Instagram-Phishing>

--------------------------------------

Generador de puerta trasera | linux y windows

1: <https://github.com/swagkarna/BackHAck>

--------------------------------------

Una herramienta rápida para obtener URL de atributos HTML mediante el rastreo.

1: <https://github.com/swagkarna/galer>

--------------------------------------

Phishing paypal, francés, inglés

1: <https://github.com/swagkarna/phishing-paypal-2020>

--------------------------------------

Un keylogger escrito en python

1: <https://github.com/swagkarna/Keylogger-with-Email-send>

--------------------------------------

Programa ransomware completo y modificable

1: <https://github.com/swagkarna/Ransom-PY>

--------------------------------------

Esta herramienta es ideal para la recopilación de información y la post-explotación.

1: <https://github.com/Cybercrack-bot/Cybercrack>

--------------------------------------

Ransomware como servicio (RaaS)

1: <https://github.com/swagkarna/RAASNet>

--------------------------------------

Omita la restricción de edad de YouTube y vea cualquier video sin una cuenta de Google.

1: <https://github.com/connor-brooks/BypassTube>

--------------------------------------

Un genial asistente virtual para Windows que puede automatizar tus tareas diarias. Nota: no es un chatbot

1: <https://github.com/Cybercrack-bot/Olivia>

--------------------------------------

Este Script te ayudará a recopilar información sobre tu víctima o amigo

1: <https://github.com/swagkarna/007-TheBond>

--------------------------------------

Inyectar el código Shell de Metasploit en un proceso legítimo

1: <https://github.com/swagkarna/MetaInject>

--------------------------------------

Potente secuencia de comandos por lotes para desmantelar la protección completa de Windows Defender e incluso omitir la protección contra manipulaciones… Deshabilitar Windows-Defender de forma permanente… Hackear Windows. Punto de contacto

1: <https://github.com/swagkarna/Defeat-Defender-V1.2>

--------------------------------------

Android Rat escrito en Java con WebPanel para controlar a las víctimas… Hackear dispositivos Android

1: <https://github.com/ankit0183/Rafel-Rat>

--------------------------------------

Un cuentagotas de phishing diseñado para Pentest.

1: <https://github.com/swagkarna/Umbrella>

--------------------------------------

EVIL EMAIL/SMS BOMBER está hecho solo con fines de investigación y prueba. Bromea con tus amigos. EVIL EMAIL/SMS BOMBER puede enviar correo masivo o mensajes de texto SMS. DESCARGO DE RESPONSABILIDAD: ¡Úselo bajo su propio riesgo! No me hago responsable de tus acciones. Esto se hizo solo con fines de broma, prueba e investigación. Codificado por Jeff Childers

1: <https://github.com/swagkarna/EVIL-EMAIL-SMS-BOMBER>

--------------------------------------

Descifre contraseñas de navegadores basados ​​en cromo, cookies, tarjetas de crédito, historial, marcadores. Se admite la versión > 80.

1: <https://github.com/swagkarna/Adamantium-Thief>

--------------------------------------

Una RAT malvada (herramienta de administración remota) para macOS / OS X.

1: <https://github.com/swagkarna/EvilOSX>

--------------------------------------

Iconos y extensiones de archivos falsos en Windows

1: <https://github.com/swagkarna/ExtensionSpoofer>

--------------------------------------

Generador de carga útil de Shell inverso, Python 3.x

1: <https://github.com/swagkarna/sheller>

--------------------------------------

Descifre contraseñas de navegadores basados ​​en cromo, cookies, tarjetas de crédito, historial, marcadores. Se admite la versión > 80.

1: <https://github.com/swagkarna/Adamantium-Thief>

--------------------------------------

Una nueva solución USB de arranque.

1: <https://github.com/swagkarna/Ventoy>

--------------------------------------

Pequeña biblioteca personal para obtener historias de Instagram usando Golang

1: <https://github.com/wmw9/ig>

--------------------------------------

📼 Grabador automático de contracción

1: <https://github.com/ankit0183/rekoda>

--------------------------------------

Bomba de archivos

1: <https://github.com/swagkarna/2x0-File-Pumper>

--------------------------------------

Un script simple para generar una URL oculta para ingeniería social.

1: https://github.com/swagkarna/URLCADIZ

--------------------------------------

Esta biblioteca ayuda a mostrar el administrador de permisos de inicio automático de un teléfono al usuario para que pueda agregar una aplicación al inicio automático.

1: <https://github.com/swagkarna/AutoStarter>

--------------------------------------

🤖 deja de seguir a los usuarios de github que no te siguen, es compatible con la lista blanca.

1: <https://github.com/swagkarna/github-unfollow>

--------------------------------------

¡Un capturador de Chrome, Brave, Firefox Stealer y Discord Token creado exclusivamente con fines educativos!

1: <https://github.com/InstinctEx/INZStealer>

--------------------------------------

F4T3H-WinC2 es una herramienta C2 (comando y control) simple que ataca a las máquinas con Windows. Codificado en python3.

1: <https://github.com/swagkarna/F4T3H-WinC2>

--------------------------------------

Ladrón de cookies y contraseñas en tan solo 2 líneas, enviadas a Telegram.

1: <https://github.com/swagkarna/stink>

--------------------------------------

Los números en sus documentos pueden revelar su información personal. Esta herramienta es una herramienta OSINT para recopilar información de CC, código BIN, MICR, IFSC, número de teléfono

1: <https://github.com/swagkarna/arithmo-gather>

--------------------------------------

Esta es una plantilla de herramienta de phishing creada con conocimientos básicos de desarrollo web.

1: <https://github.com/swagkarna/phishing-Instagram>

--------------------------------------

MDPin es un servidor y un sitio web. Contiene una interfaz de usuario para falsificar una pantalla de inicio de sesión de Android para robar su código PIN. Funciona a través de un navegador web, yendo a pantalla completa.

1: <https://github.com/swagkarna/MDPin>

--------------------------------------

Convierte cualquier texto no deseado en una lista de palabras utilizable para fuerza bruta.

1: <https://github.com/swagkarna/haklistgen>

--------------------------------------

Una herramienta forense para ayudar en la investigación de correos electrónicos falsificados en función de los encabezados de correo electrónico.

1: <https://github.com/swagkarna/mailMeta>

--------------------------------------

Deshabilitar todas las versiones de Windows Defender

1: <https://github.com/swagkarna/Disable-Windows-Defender>

--------------------------------------

Este script obtendrá la ubicación exacta de las víctimas mediante algún método de phishing. Aquí está el sitio de demostración

1: <https://github.com/swagkarna/Covid19-Phishing-Steal-Location->

--------------------------------------

Script de Python simple que ataca la base de datos de los sitios de phishing con nombres de usuario y contraseñas falsos generados aleatoriamente para inundar sus bases de datos con datos falsos, a veces incluso elimina todo el sitio en el proceso.

1: <https://github.com/EwyBoy/Counter-Phishing-Tool>

--------------------------------------

Una herramienta para identificar y explotar las configuraciones incorrectas y las vulnerabilidades de las reglas de Sudo dentro de Sudo para la escalada de privilegios de Linux.

1: <https://github.com/swagkarna/SUDO_KILLER>

--------------------------------------

Use una imagen falsa.jpg para explotar objetivos (ocultar extensiones de archivo conocidas)

1: <https://github.com/swagkarna/FakeImageExploiter>

--------------------------------------

Una herramienta de acceso remoto que usa Google Apps Script como proxy para comando y control.

1: <https://github.com/swagkarna/google_RAT>

--------------------------------------

Este programa realiza análisis OSINT en sitios Tor. El programa tiene una CLI y una API REST.

1: <https://github.com/swagkarna/gotor>

--------------------------------------

CloudFlare-IP es una herramienta que tiene como objetivo recopilar la IP de origen del sitio web protegido por Cloudflare desde el icono de favicon del sitio web utilizando Shodan api

1: <https://github.com/karma9874/CloudFlare-IP>

--------------------------------------

CTF-CryptoTool es una herramienta escrita en python, para romper el texto criptográfico de los desafíos de CTF. Intenta decodificar el cifrado mediante fuerza bruta con todos los métodos conocidos de decodificación de cifrado fácilmente. También funciona para el cifrado que no tiene clave.

1: <https://github.com/karma9874/CTF-CryptoTool>

--------------------------------------

Una herramienta simple de administración remota de Android usando sockets. Utiliza java en el lado del cliente y python en el lado del servidor

1: <https://github.com/ankit0183/AndroRAT>

--------------------------------------

Herramienta de seguridad cibernética para piratear conexiones inalámbricas utilizando herramientas Kali integradas. Admite todos los valores (WEP, WPS, WPA, WPA2/TKIP/IES)

1: <https://github.com/ankit0183/Wifi-Hacking>

--------------------------------------

Pantalla de bloqueo de interfaz de crack, Metasploit y más piratería de Android / IOS

1: <https://github.com/tegal1337/CiLocks>

--------------------------------------

Herramienta de pentesting de intranet con webui

1: <https://github.com/FunnyWolf/Viper>

--------------------------------------

E-mail anonimo

?: <https://github.com/cyberkallan/anonymous-mail>

?: <https://github.com/AnonymousFromGeorgia/Anonymous-Mail>

--------------------------------------

Saber ip con e-mail

1: Whoreadme - Conseguir IP enviando un

email

--------------------------------------

Un script simple hecho para uso propio para omitir 403

1: <https://github.com/iamj0ker/bypass-403>

--------------------------------------

Saber correo con el nombre de GitHub

1: <https://emailaddress.github.io/>

--------------------------------------

Crear qr

1: <https://github.com/iinc0gnit0/coder>

--------------------------------------

Cambiar nombre de payload

1: <https://github.com/Darkmux/EvilIcon>

--------------------------------------

Smuggler: una herramienta de prueba de contrabando / desincronización de solicitudes HTTP escrita en Python 3

1: <https://github.com/defparam/smuggler>

--------------------------------------

Recon (nmap)

1: <https://github.com/TermuxHackz/recon>

--------------------------------------

Encriptar PDF

1: <https://github.com/TermuxHackz/Pdfencrypt>

--------------------------------------

Nginxpwner es una herramienta simple para buscar vulnerabilidades y configuraciones erróneas comunes de Nginx.

1: <https://github.com/stark0de/nginxpwner>

--------------------------------------

⛄ Obtenga el Usuario: Contraseña de Chrome (incluya la versión < 80 y la versión > 80)

1: <https://github.com/cckuailong/HackChrome>

--------------------------------------

Sitio web de actualización falsa (al hacer clic, descarga automática de Windows Payload)

1: <https://github.com/swagkarna/Fake-Update-Page>

--------------------------------------

| Escáner de vulnerabilidades web multiherramienta.

1: https://github.com/swagkarna/rapidscan

--------------------------------------

Token discord builder

1: <https://github.com/NightfallGT/Token-Grabber-Builder>

--------------------------------------

Discord nitro fake

1: <https://github.com/NightfallGT/Nitro-Ransomware>

--------------------------------------

SharpML es una herramienta de minería de datos de uso compartido de archivos de

prueba de concepto que utiliza Machine Learning en Python y C #.

1: <https://github.com/HunnicCyber/SharpML>

--------------------------------------

Netflix checker

1: <https://github.com/NightfallGT/Netflix-Checker>

--------------------------------------

Virus

1: <https://github.com/TermuxHackz/MyVirus>

--------------------------------------

Puede usar este .zip para crear un archivo .exe y usarlo para robar una sesión de Telegram.

1: <https://github.com/teleport21/Telegram_Stealer>

--------------------------------------

Scam

1: <https://github.com/Cesar-Hack-Gray/scam>

--------------------------------------

Saber ip de página web

1: <https://github.com/iinc0gnit0/ASN-Eagle>

--------------------------------------

Chromepass – Hackear contraseñas guardadas de Chrome

1: <https://github.com/darkarp/chromepass>

--------------------------------------

Una sesión de herramientas Secuestro y ladrón Código de acceso local Telegram Windows

1: <https://github.com/ultrasecurity/TeleKiller>

--------------------------------------

Datos

1: <https://github.com/mike90s15/Clownters.py>

--------------------------------------

Saber si una contraseña a sido filtrada

1: <https://github.com/nk4456542/Password-Checker>

--------------------------------------

PeTeReport es una herramienta de informes de vulnerabilidades de aplicaciones de código abierto.

1: <https://github.com/1modm/petereport>

--------------------------------------

Multi tool

1: <https://github.com/jank3/jk-multitool>

--------------------------------------

Una puerta trasera basada en Python que utiliza esteganografía y un servicio de imágenes en la nube como servidor de comando y control.

1: <https://github.com/1modm/stegator>

--------------------------------------

Herramientas de penetración/explotación/secuestro, decodificadores SIP y RTP para Dshell

1: <https://github.com/1modm/Dshell_decoders>

--------------------------------------

Whalescan es un escáner de vulnerabilidades para contenedores de Windows, que realiza varias comprobaciones comparativas, además de comprobar si hay CVE/paquetes vulnerables en el contenedor.

1: <https://github.com/nccgroup/whalescan>

--------------------------------------

el Network Protocol Fuzzer que querremos utilizar.

1: <https://github.com/nccgroup/fuzzowski>

--------------------------------------

Google virtual machine

1: <https://colab.research.google.com/github/PradyumnaKrishna/Colab-Hacks/blob/master/Colab%20RDP/Colab%20RDP.ipynb#scrollTo=Q6bl1b0EifVG>

--------------------------------------

Extensión de registro avanzada de Burp Suite

1: https://github.com/nccgroup/LoggerPlusPlus

--------------------------------------

Router sploit

1: <https://github.com/reverse-shell/routersploit.git>

--------------------------------------

Metasploitable3 es una máquina virtual construida desde cero con una gran cantidad de vulnerabilidades de seguridad.

1: <https://github.com/rapid7/metasploitable3>

--------------------------------------

Este repositorio contiene todas las máquinas virtuales vulnerables. Estas máquinas vulnerables están basadas en Windows y Linux.

1: <https://github.com/RedTeamOperations/Vulnerable_Machine>

--------------------------------------

Gestión de línea de comandos para Google Workspace

1: <https://github.com/RedTeamOperations/GAM>

--------------------------------------

Un escáner de aplicaciones web basado en Python para recopilar OSINT y fuzz para las vulnerabilidades de OWASP en un sitio web de destino.

1: <https://github.com/ToR-0/BlackWidow>

--------------------------------------

Macro\_pack es una herramienta de @EmericNasi que se utiliza para automatizar la ofuscación y la generación de documentos de Office, scripts de VB, accesos directos y otros formatos para evaluaciones de pentest, demostración e ingeniería social. El objetivo de macro\_pack es simplificar la explotación, eludir el antimalware y automatizar el proceso desde la generación de scripts y macros maliciosos hasta fin…

1: <https://github.com/RedTeamOperations/macro_pack>

--------------------------------------

Herramientas y cosas interesantes para RedTeam Ops

1: <https://github.com/RedTeamOperations/RedTeam>

--------------------------------------

Un marco posterior a la explotación diseñado para operar de forma encubierta en entornos fuertemente monitoreados

1: <https://github.com/RedTeamOperations/shad0w>

--------------------------------------

Implante de extensión de Chrome que convierte los navegadores Chrome de las víctimas en proxies HTTP totalmente funcionales, lo que le permite navegar por los sitios como sus víctimas.

1: <https://github.com/RedTeamOperations/CursedChrome>

--------------------------------------

El shell WinRM definitivo para hacking/pentesting

1: <https://github.com/RedTeamOperations/evil-winrm>

--------------------------------------

Mapeo detallado de la superficie de ataque y descubrimiento de activos

1: <https://github.com/RedTeamOperations/Amass>

--------------------------------------

Genera código shell independiente de la posición x86, x64 o AMD64+x86 que carga ensamblajes .NET, archivos PE y otras cargas útiles de Windows desde la memoria y las ejecuta con parámetros

1: <https://github.com/RedTeamOperations/donut>

--------------------------------------

Se omite el script Pyhton para las respuestas HTTP 40X. Funciones: manipulación de verbos, encabezados, trucos #bugbountytips y 2454 agentes de usuario.

1: <https://github.com/lobuhi/byp4xx>

--------------------------------------

Herramienta de análisis de malware todo en uno.

1: <https://github.com/CYB3RMX/Qu1cksc0pe>

--------------------------------------

Kit de herramientas de pivote de red

1: <https://github.com/RedTeamOperations/PivotSuite>

--------------------------------------

Entornos vulnerables prediseñados basados ​​en Docker-Compose

1: https://github.com/vulhub/vulhub

--------------------------------------

Máquina virtual para emulación de adversarios y búsqueda de amenazas

1: https://github.com/RedTeamOperations/RedHunt-OS

--------------------------------------

Kit de herramientas de abuso de delegación sin restricciones de Kerberos

1: <https://github.com/RedTeamOperations/krbrelayx>

--------------------------------------

Una sencilla herramienta para comprobar si se ha filtrado tu contraseña.

1: https://github.com/cristianzsh/passwordcheck

--------------------------------------

Sh-kitty es una herramienta de sombrero negro/sombrero gris. Tiene muchas opciones que son excelentes para muchas cosas que ha planeado. Esta herramienta es muy confiable para las cosas cotidianas, pero al mismo tiempo tiene un lado de piratería (de sombrero negro). Siguientes opciones como. [1] ingrese 1 para el generador de contraseñas Anti-Brutefoce [2] para el ataque de fuerza bruta numérica .rar. (ser …

1: x\_john\_doe

--------------------------------------

𝐇𝐀𝐂𝐊-𝐈𝐍-𝐎𝐍𝐄; EL MEJOR JUEGO DE HERRAMIENTAS. < CAJA DE HERRAMIENTAS DE HACKEO | KIT DE HERRAMIENTAS DE PENSAMIENTO >

1: <https://github.com/ByDog3r/H4ck-In-One>

--------------------------------------

𝐖𝐢𝐧𝐓𝐨𝐨𝐥𝐊𝐢𝐭; Es un kit de herramientas de Windows: ¡Recupera tus contraseñas de wifi en segundos!

1: <https://github.com/ByDog3r/WinToolKit>

--------------------------------------

𝐚𝐳𝐚𝐭𝐡𝐨𝐭: KIT DE HERRAMIENTAS DE CARDADO >> HERRAMIENTAS DE CARDADO [ < CCGEN | BIN-INFO | COMPROBADOR > ].

1: <https://github.com/ByDog3r/azathot>

--------------------------------------

𝐀𝐮𝐭𝐨𝐖𝐚𝐫𝐝; DEJA QUE SEA SPAM EN: FACEBOOK, TWITCH, INSTAGRAM, TWITTER Y MAS.

1: <https://github.com/ByDog3r/auto-spammer>

--------------------------------------

Un rastreador y verificador de enlaces

grupales de Whatsapp

1: <https://github.com/TheSpeedX/WhatScraper>

--------------------------------------

scrapper de Youtube para eliminar toda la información de un canal

1: <https://github.com/TheSpeedX/YTScrapper>

--------------------------------------

Una RAT multifuncional multiplataforma (Windows / Linux / Mac).

1: <https://github.com/hash3liZer/SillyRAT>

--------------------------------------

DragonMS son herramientas para ddos, escáner, rastreador, generador de carga útil msfvenom y raspado

1: <https://github.com/ToR-0/DragonMS>

--------------------------------------

PDF brute

1: <https://github.com/TermuxHackz/pdfbruter>

?: <https://github.com/machine1337/pdfcrack>

--------------------------------------

Arbitrium es un troyano de acceso remoto multiplataforma, totalmente indetectable, para controlar Android, Windows y Linux y no requiere excepciones de firewall o reglas de reenvío de puertos.

1: <https://github.com/ToR-0/Arbitrium-RAT>

--------------------------------------

Whatsap fhising

1: https://github.com/Ignitetch/whatsapp-phishing

--------------------------------------

Marco de prueba de autenticación web

1: https://github.com/ToR-0/raider

--------------------------------------

Herramienta de eliminación de directorios / archivos, DNS y VHost escrita en Go

1: https://github.com/ToR-0/gobuster

--------------------------------------

Uber phishing

1: <https://github.com/Ignitetch/UberEats-Phishing>

--------------------------------------

Cast All The Things te permite enviar videos de muchas, muchas fuentes en línea a tu Chromecast.

1: https://github.com/skorokithakis/catt

--------------------------------------

El controlador Rickmote: secuestra televisores con Google Chromecast

1: https://github.com/BishopFox/rickmote

--------------------------------------

Sacar información faccebok

1: https://github.com/CiKu370/OSIF

--------------------------------------

Matar

1: <https://github.com/bahaabdelwahed/killshot>

--------------------------------------

Gestión de la postura de seguridad en la nube (CSPM)

1: https://github.com/ToR-0/cloudsploit

--------------------------------------

Script Bash que automatiza la enumeración de dominios y servidores DNS en la recopilación de información activa.

1: https://github.com/ToR-0/DNSExplorer

--------------------------------------

Un conjunto de herramientas que reúne herramientas de prueba de penetración, como herramientas inalámbricas,

herramientas web, herramientas para descifrar contraseñas, etc.

1: https://github.com/ToR-0/OmegaDSToolkit

--------------------------------------

Una herramienta OSINT de correo electrónico automatizada

1: https://github.com/ToR-0/mosint

--------------------------------------

Xteam All in one Instagram, Android, phishing osint y herramienta de pirateo wifi disponible

1: https://github.com/ToR-0/Xteam

--------------------------------------

VAIM-RAMSOM ES UN SIMPLE RANSOMWARE DE ANDROID PARA BROMAR CON TUS AMIGOS. MUCHAS VECES SOLO QUIERES BROMAR O JUGAR CON TU AMIGO.

1: https://github.com/ToR-0/Vaim-RamSom

--------------------------------------

Motor de permutación de nombres de dominio

para detectar ataques de phishing homógrafos, okupación de errores tipográficos y suplantación de marca.

1: https://github.com/ToR-0/dnstwist

--------------------------------------

Una herramienta que encripta y oculta sus datos dentro de sus imágenes.

1: https://github.com/ToR-0/stegreg

--------------------------------------

Toolkit faccebok

1: https://github.com/warifp/FacebookToolkit

--------------------------------------

Una herramienta que le permite buscar dispositivos Android vulnerables en todo el mundo y explotarlos.

1: https://github.com/ToR-0/AdbNet

--------------------------------------

Saber número de teléfono (no ip)

1: <https://github.com/ToR-0/phisherprice>

--------------------------------------

Capturador de apretón de manos

1: <https://github.com//HSCAP>

--------------------------------------

Marco de pruebas de penetración automatizado - Escáner de vulnerabilidades de código abierto - Gestión de vulnerabilidades

1: https://github.com/ToR-0/Nettacker

--------------------------------------

Herramienta OSINT para obtener información de un perfil de Github y Gitlab y encontrar las direcciones de correo electrónico de los usuarios filtradas en las confirmaciones.

1: https://github.com/ToR-0/gitrecon

--------------------------------------

Una herramienta para hackear la cámara de termux

1: https://github.com/ToR-0/grabcam

--------------------------------------

WireBug es un conjunto de herramientas para pruebas de penetración de voz sobre IP

1: https://github.com/ToR-0/WireBug

--------------------------------------

DNSTake: una herramienta rápida para verificar las zonas DNS alojadas que faltan y que pueden llevar a la toma de control del subdominio

1: <https://github.com/ToR-0/dnstake>

--------------------------------------

Un encriptador de línea de comando AES simple

1: <https://github.com/Aekras1a/DarkCrypter>

--------------------------------------

Toolkit

?: https://github.com/krintoxi/NoobSec-Toolkit

?: https://github.com/unkn0wnh4ckr/hackers-tool-kit

?: https://github.com/termuxhackers-id/SIGIT

--------------------------------------

Faccebok cracking

1: https://github.com/INDOnimous/FB-Crack-

--------------------------------------

PassLock es un administrador de contraseñas de seguridad media que cifra las contraseñas mediante el estándar de cifrado

avanzado (AES)

1: https://github.com/ToR-0/PassLock

--------------------------------------

Paquete de herramientas de piratería y generador de puertas traseras.

1: https://github.com/ToR-0/KitHack

--------------------------------------

🌘🦊 DalFox (Finder Of XSS) / Herramienta de análisis de parámetros y escaneo XSS basada en golang

1: https://github.com/ToR-0/dalfox

--------------------------------------

Herramienta de ataque X ☣ Escáner de vulnerabilidad de sitios web y explorador automático

1: https://github.com/ToR-0/XAttacker

--------------------------------------

Paquete de herramientas de piratería DARKARMY: un marco de prueba de penetración.

1: https://github.com/ToR-0/DARKARMY

--------------------------------------

Cloudflare by-pass

1: https://github.com/adolabsnet/cloudflare-bypass

--------------------------------------

MagicRecon es un poderoso script shell para maximizar el proceso de reconocimiento y recolección de datos de un objetivo y encontrar vulnerabilidades comunes, todo esto guardando los resultados obtenidos de manera organizada en directorios y con varios formatos.

1: https://github.com/ToR-0/magicRecon

--------------------------------------

Herramienta OSINT que le permite encontrar las cuentas y los correos electrónicos de una persona + correos electrónicos violados 🕵️

1: https://github.com/ToR-0/Profil3r

--------------------------------------

Faccebok descargar

1: https://github.com/barba99/facebook-

spot...-descargar

--------------------------------------

(Toolkit) Herramienta de información y pirateo de redes sociales

1: https://github.com/ToR-0/TgaHacking

--------------------------------------

El marco de trabajo de inteligencia de código abierto más avanzado (OSINT) para escanear direcciones IP, correos electrónicos, sitios web y organizaciones.

1: https://github.com/ToR-0/reconspider

--------------------------------------

Canadian Furious Beaver es una herramienta para monitorear el controlador de IRP en los controladores de Windows y facilitar el proceso de análisis, reproducción y fuzzing de los controladores de Windows en busca de vulnerabilidades.

1: <https://github.com/ToR-0/CFB>

--------------------------------------

Kahoot bots

1: https://github.com/Raymo111/kahoot-answer-bot

--------------------------------------

(Toolkit) ¡Herramientas de piratería todo en

uno para piratas informáticos! ¡Y más herramientas de piratería! ¡En termux y linux!

1: https://github.com/ToR-0/AllHackingTools

--------------------------------------

Una navaja suiza para redes de pentesting

1: https://github.com/ToR-0/CrackMapExec

--------------------------------------

Un rastreador para Bluetooth 5 y 4.x LE

1: https://github.com/ToR-0/Sniffle

--------------------------------------

Herramienta CLI para inteligencia de amenazas y código abierto

1: https://github.com/ToR-0/harpoon

--------------------------------------

Discord gen bot

1: https://github.com/NightfallGT/Discord-Account-Generator

--------------------------------------

Tiktok check account

1: https://github.com/NightfallGT/TikTok-Username-Checker

--------------------------------------

Tiktok phishing

1: <https://github.com/swagkarna/Tiktok-Phishing->

--------------------------------------

Colección de scripts para evitar el control de acceso a la red (NAC, 802.1x)

1: https://github.com/ToR-0/nac\_bypass

--------------------------------------

Esta herramienta brinda información sobre el número de teléfono que ingresó. (También te da las redes sociales asociadas al número telefonico)

1: https://github.com/ToR-0/Moriarty-Project

--------------------------------------

CHAOS es una herramienta de administración remota gratuita y de código abierto que permite generar binarios para controlar sistemas operativos remotos.

1: https://github.com/ToR-0/CHAOS

--------------------------------------

HostHunter una herramienta de reconocimiento para descubrir nombres de

host utilizando técnicas OSINT.

1: https://github.com/ToR-0/HostHunter

--------------------------------------

WAFW00F permite identificar y tomar huellas dactilares de los productos de firewall de aplicaciones web (WAF) que protegen un sitio web.

1: https://github.com/ToR-0/wafw00f

--------------------------------------

Zero-Attacker es una herramienta de piratería multipropósito con más de 13 herramientas como token-gen, ddos ​​y más (código público en 75 estrellas)

1: https://github.com/ToR-0/Zero-attacker

--------------------------------------

este es un módulo de Python que contiene funciones y clases que se utilizan para probar la seguridad de aplicaciones web / de red. ¡Está codificado en Python puro y es una herramienta muy inteligente! Puede detectar fácilmente: XSS (relected /

almacenado), RCE (ejecución remota de código / comando), SSTI, SSRF, configuraciones incorrectas de CORS, carga de archivos, CSRF, recorrido de ruta, .... Además, ...

1: https://github.com/ToR-0/bane

--------------------------------------

Un motor de búsqueda de información proporcionada por fuentes OSINT para respaldar la evaluación de vulnerabilidades.

1: <https://github.com/ToR-0/VISE>

--------------------------------------

Pivoter es una herramienta proxy para que los pentesters tengan un movimiento lateral más fácil.

1: https://github.com/trustedsec/pivoter

--------------------------------------

🔎 Ayuda a encontrar la vulnerabilidad de la fuente troyana en el código 👀. Útil para la revisión de código en proyectos con múltiples colaboradores (CI / CD)

1: https://github.com/ToR-0/TrojanSourceFinder

--------------------------------------

Simplescan herramienta para realizar escaneo de puertos tcp. La herramienta

realiza escneos de tipo Stealth scan, Connect scan y Acknowledgement scan (ACK scan).

1: https://github.com/LW-Homeless/SimpleScan

--------------------------------------

A simple TCP/UDP port scanner

1: https://github.com/dnfetheus/port-scanner

--------------------------------------

La aplicación de una tienda electrónica se ha desarrollado en PHP y Laravel Framework

1: https://github.com/ToR-0/Ecommerce\_Laravel

--------------------------------------

escáner web - explotación - recopilación de información

1: https://github.com/ToR-0/Zeebsploit

--------------------------------------

Herramienta de reconocimiento que realiza una enumeración automática de los servicios descubiertos de una IP ó dominio.

1: https://github.com/m4lal0/autoRecon

--------------------------------------

Una Multiherramienta con cosas muy interesantes, solo para fines educativos

1: https://github.com/jank3/jk-multitool

--------------------------------------

APT-Hunter es una herramienta de búsqueda de amenazas para registros de eventos de Windows que se creó con la mentalidad de equipo púrpura para detectar movimientos de APT ocultos en el mar de registros de eventos de Windows para disminuir el tiempo para descubrir actividades sospechosas.

1: https://github.com/ToR-0/APT-Hunter

--------------------------------------

Herramienta de enumeración rápida de subdominios para probadores de penetración.

1: https://github.com/ToR-0/tugarecon

--------------------------------------

AndroBugs Framework es un eficiente escáner de vulnerabilidades de Android que

ayuda a los desarrolladores o investigadores de seguridad a encontrar posibles vulnerabilidades de seguridad en las aplicaciones de Android.

1: https://github.com/ToR-0/androbugs2

--------------------------------------

Una herramienta de Python para automatizar algunas cosas tontas para encontrar divulgaciones de información.

1: https://github.com/ToR-0/webdork

--------------------------------------

Scripts automatizados de Web Recon Shell

1: https://github.com/ToR-0/webrecon

--------------------------------------

Ig sniper

1: https://github.com/NightfallGT/IG-Sniper

--------------------------------------

Asu hacking

1: https://github.com/LOoLzeC/ASU

--------------------------------------

Faccebok report bot

1: https://github.com/IlayTamvan/Report

--------------------------------------

Discord scam qr

1: https://github.com/NightfallGT/Discord-QR-Scam

--------------------------------------

Web sploit

1: https://github.com/websploit/websploit

--------------------------------------

Buscador de vulnerabilidades web

1: https://github.com/iinc0gnit0/RVuln

--------------------------------------

Discord scam

1: https://github.com/BuildBot42/discord-scam-links

--------------------------------------

Fhising por e-mail

1: https://github.com/BiZken/PhishMailer

2: https://github.com/Darkmux/Falsify

--------------------------------------

Payloads

1: https://github.com/rapid7/metasploit-payloads

2: https://github.com/payloadbox/directory-payload-list

?: https://github.com/iinc0gnit0/pyload

!: https://github.com/jimywork/PayloadsAllTheThings

--------------------------------------

Payload virus created

1: https://github.com/TermuxHackz/payload-virus

--------------------------------------

Crear puntos de acceso y hackear

1: Https://github.com/s4vitar/evilTrust

2: <https://github.com/swagkarna/wifi-pumpkin-v3.0>

--------------------------------------

Airdroid (no funciona) (sploit)

1: https://github.com/s4vitar/AirDroidPwner

--------------------------------------

Programa hacker

1: https://github.com/Hack-with-Github/

Awesome-Hacking

--------------------------------------

Ataques DDoS

1: https://github.com/rapid7/metasploit-framework

2: https://github.com/grafov/hulk

3: https://github.com/cyweb/hammer

4: https://github.com/649/Memcrashed-DDoS-Exploit

?: https://github.com/edmark21/WebDos

--------------------------------------

Apk payload

1: https://github.com/Ignitetch/apk-payload-injector

--------------------------------------

Hackear contraseñas:

1: https://github.com/s0md3v/Hash-Buster

--------------------------------------

Botnets

1: https://github.com/malwaredllc/byob

2: https://github.com/epsylon/ufonet

?: https://github.com/frederikme/Botnet

?: <https://github.com/ToR-0/pybotnet>

--------------------------------------

Spam de números de teléfono

1: https://github.com/Darkmux/SETSMS

2: https://github.com/TheSpeedX/TBomb

3: <https://github.com/HACK3RY2J/Anon-SMS>

4: <https://github.com/MrHarshArora/CyberGhostWeapon>

5: <https://github.com/ebankoff/BoMbEr>

6: <https://github.com/IncredibleHacker/TBomb2.0>

7: https://github.com/Elliot290/BaapGAttack

--------------------------------------

SMS personalizados

1: https://github.com/Darkmux/DarkSMS

--------------------------------------

Spam de numeros de llamadas y de personalizados

no funcional: https://github.com/noob-hackers/spamx

1: https://github.com/FDX100/GOD-KILLER

--------------------------------------

Para insertar virus en apps:

1: https://github.com/Cesar-Hack-Gray/Destroyer-framework

2: https://github.com/noob-hackers/vanish

3: https://github.com/Hacking-pch/papaviruz

4: https://github.com/Ign0r3dH4x0r/GenVirus

--------------------------------------

Geolocalización

1: https://github.com/rajkumardusad/IP-Tracer

2: <https://github.com/maldevel/IPGeoLocation>

--------------------------------------

Para inyecciones SQL

1: https://github.com/sqlmapproject/sqlmap

--------------------------------------

Para rastrear información de un número

1: https://github.com/sundowndev/phoneinfoga

2: https://github.com/s41r4j/phomber

--------------------------------------

Exploit

1: https://github.com/offensive-security/

exploitdb

--------------------------------------

E-mail bomber

1: https://github.com/juzeon/fast-mail-bomber

2: https://github.com/ncorbuk/Python---Email-Bomber

3: https://github.com/sumanmanna6111/Emailboom

--------------------------------------

Whatsap bomber

1: https://github.com/iamajraj/spamWa-1

--------------------------------------

Instagram bomber

1: https://github.com/Gumbraise/instagram-bomber

2: https://github.com/cyberkallan/Instapostspamer

--------------------------------------

Otp scam

1: https://github.com/jainamoswal/otp-scam

--------------------------------------

Instagram report bot

1: https://github.com/2l21l1/IG-Report

2: https://github.com/Khanejo/Instagram-mass-reporter

?: https://github.com/tarik0/instaspamv4

--------------------------------------

Fortnite report bot

1: https://github.com/stl1988/fnReport-en

--------------------------------------

Hackear Cámara

0: https://github.com/kevop-s/Saycheese

1: https://github.com/techchipnet/CamPhish

2: https://github.com/hasanfirnas/symbiote

3: https://github.com/AngelSecurityTeam/Cam-Hackers

4: https://github.com/noob-hackers/seeu

5: https://github.com/KasRoudra/CamHacker

--------------------------------------

Hackear audio

1: <https://github.com/d093w1z/sayhello>

--------------------------------------

Echar intrusos de una red wifi

1: https://github.com/bitbrute/evillimiter

--------------------------------------

Localizar números de teléfono

1: https://github.com/howardchn/location-to-phone-number

2: <https://github.com/jimmy1212/GpsTracker---SIG>

--------------------------------------

Herramienta Yandex OSINT

1: <https://github.com/HowToFind-bot/YaSeeker>

--------------------------------------

Chimera es un script de ofuscación de PowerShell (brillante y muy pirateado) diseñado para eludir AMSI y las soluciones antivirus comerciales.

1: https://github.com/tokyoneon/Chimerah

--------------------------------------

Instagram hackear

1: https://github.com/umeshshinde19/instainsane

2: https://github.com/TermuxHackz/insta-crack

?: https://github.com/dhasirar/instax

?: https://github.com/BladeKnife/igbf

?: https://github.com/Pure-L0G1C/Instagram

?: https://github.com/noob-hackers/ighack

?: <https://github.com/swagkarna/Bypass-Insta-2FA->

?: https://github.com/xHak9x/instabrute

?: https://github.com/0xfff0800/Brute-force-Instagram-2021

--------------------------------------

Saber número de telefono con ip

1: https://github.com/AbirHasan2005/OPRecon

?: https://github.com/AbdeljalilSalhi-official/infoGather

?: https://github.com/l0qi/OSINTER

--------------------------------------

Twitter hackear

1: https://github.com/0xfff0800/Brute-Forc-Twitter-

--------------------------------------

Crear apk para hackear móvil

1: https://github.com/termuxhackers-id/SARA

--------------------------------------

Acortador de links

1: https://github.com/Darkmux/URLSpoof

2: https://github.com/Darkmux/ShortUrl

--------------------------------------

Payload sql

1: https://github.com/payloadbox/sql-injection-payload-list

--------------------------------------

Discord hackear

1: https://github.com/adolabsnet/Discord-Token-Brute-Force

--------------------------------------

Descargar contenido only fans

1: https://github.com/adolabsnet/onlyfans-dl

--------------------------------------

Faccebok hackear

1: https://github.com/m-primo/Facebook-Brute-Force

!: https://github.com/IAmBlackHacker/Facebook-BruteForce

?: https://github.com/TermuxHackz/FHF

--------------------------------------

Twitch hackear

1: <https://github.com/u0pattern/TwitchKIT>

--------------------------------------

Hackea el patrón de Android de Termux con esta herramienta

1: https://github.com/noob-hackers/infect

--------------------------------------

camara hackear & whatsapp virus & SMS bomber

1: https://github.com/TermuxHackz/Hacks

--------------------------------------

Gmail hackear

1: https://github.com/0xfff0800/Brute-force-gmail

2: https://github.com/Anontemitayo/Gmail-brute

--------------------------------------

Sacar información de instagram

1: https://github.com/SpookySec/OSINTed

2: https://github.com/megadose/toutatis

--------------------------------------

Carding

1: https://github.com/Anonymous3-SIT/Card-Number

2: https://github.com/itsmehacker/CardPwn

?: https://github.com/ToR-0/azathot

--------------------------------------

3: https://github.com/erwincatt/hackingtool

4: https://github.com/cyberkallan/cardershub

5: https://github.com/ByDog3r/azathot

--------------------------------------

Whatsap chat bot

1: https://github.com/lucioerlan/Whatsapp-Chatbot

--------------------------------------

Telegram bot

1: https://github.com/lucioerlan/Telegram-Bot

--------------------------------------

Email marketing

1: https://github.com/lucioerlan/Email-Marketing

--------------------------------------

Keylogger

1: <https://github.com/lucioerlan/Keylogger>

2: <https://github.com/BarrySad/Python-Keylogger>

--------------------------------------

Doxeos

1: https://github.com/ByDog3r/GvngSearch

2: https://github.com/khast3x/h8mail

--------------------------------------

Token discord grabber

1: https://github.com/baum1810/fixed-token-grabber

?: https://github.com/AstraaDev/Discord-Token-Grabber

--------------------------------------

Pentesting

?: https://github.com/gwen001/pentest-tools

!: https://github.com/thehackingsage/burpsuite

!: https://github.com/wireshark/wireshark

!: https://github.com/nmap/nmap

--------------------------------------

Doxeos web

1: https://github.com/Darkmux/DoxWeb

--------------------------------------

Otp ffa2

?: https://github.com/swarajsaaj/otpReader

?: https://github.com/Ross1337/SMSBotBypass

?: https://github.com/Ignitetch/ola-otpbypass

--------------------------------------

Para saber la contraseña de un wifi

1: https://github.com/s4vitar/wifiCrack

2: https://github.com/R3LI4NT/Wifi-Hack

--------------------------------------

Brute login

1: https://github.com/R3LI4NT/brute-force

!: https://github.com/Sanix-Darker/Brute-Force-Login

?: https://github.com/ToR-0/t14m4t

--------------------------------------

Brute login windows

1: https://github.com/DarkCoderSc/win-

brute-logon

--------------------------------------

Datos de tu propio movil

1: https://github.com/Cabbagec/termux-ohmyzsh

--------------------------------------

Saber que teclas se tocan

1: https://github.com/ggerganov/kbd-audio

--------------------------------------

Generador de contraseñas

1: https://github.com/noob-hackers/p-gen

--------------------------------------

?

?:https://github.com/Cesar-Hack-Gray/EMBED-PLUS

--------------------------------------

Metadatos

1: https://github.com/Darkmux/ExifTool

--------------------------------------

Para dejar de seguir a gente en instagram y etc

1: https://github.com/cyberkallan/inshackle-bot

--------------------------------------

E-mail spoof

1: https://github.com/Darkmux/EmailSpoofing

--------------------------------------

Suplantación e-mail

1: https://github.com/Darkmux/Email-Supplant

--------------------------------------

Buscador de camaras

1: https://github.com/Darkmux/CamSearch

--------------------------------------

Hackear Cámara ip

1: https://github.com/kancotdiq/ipcs

--------------------------------------

?

?:https://github.com/Darkmux/TORVPN

--------------------------------------

Virus indetectable

1: https://github.com/Darkmux/EvilIcon

--------------------------------------

?

1: https://github.com/Darkmux/ltserv

--------------------------------------

phishing foto

1: https://github.com/Cesar-Hack-Gray/FotoSploit

--------------------------------------

Creador de DNS falsa

1: https://github.com/Trackbool/DerpNSpoof

2: https://github.com/mustafadalga/dns-spoof

--------------------------------------

Spoffing etc

1: https://github.com/AdrMXR/KitHack

--------------------------------------

Web spoffing

1: https://github.com/kevop-s/Web-spoofing

--------------------------------------

Generador de dnis falsos

1: https://github.com/JuanMaRuiz/personal-document-generator

--------------------------------------

Hacker contraseña movil

1: https://github.com/urbanadventurer/Android-PIN-Bruteforce

--------------------------------------

SMS

1: https://github.com/s4vitar/spoofMe

--------------------------------------

Brute force camera IP

1: https://github.com/jimywork/shodanwave

--------------------------------------

Espiar movil

1: https://github.com/hamzaharoon1314/SpyNote

--------------------------------------

Peligro absoluto no usar programa por razones de peligro para la víctima:infectar PDF phising etc

1: https://github.com/Cesar-Hack-Gray/Spayer

--------------------------------------

Otro

?: https://github.com/KasRoudra/KasRoudra#My-Best-Works

?: https://github.com/zamarrowski/recursos-hacking-etico

--------------------------------------

Osint (buscador de cuentas)

1: https://github.com/Moham3dRiahi/Th3inspector

--------------------------------------

Herramientas para tirar o recolectar

información de wifi etc

1: <https://github.com/0x90/wifi-arsenal>

--------------------------------------

Kahoot bots

1: <https://replit.com/@dekwi1829/khoot-bot-by-sean-1#index.js>

--------------------------------------

Bot fortnite skin

1: <https://github.com/Amrsatrio/ak47-java>

--------------------------------------

osint

1: <https://github.com/sherlock-project/sherlock>

2: <https://github.com/jivoi/awesome-osint>

?: <https://github.com/Ignitetch/sifter>

--------------------------------------

Otp

1: <https://github.com/Ross1337/SMSBotBypass>

--------------------------------------

Herramientas para hackear

Scanner de webs

--------------------------------------

﻿Yawast

Dmitry

--------------------------------------

Phishing

--------------------------------------

Socialbox

Socialsploit

Nexphiser

Zphiser

Socialphish

--------------------------------------

DDoS

--------------------------------------

Hulk

Metasploit

Hammer

Memcrashed

--------------------------------------

Doxeos

Maltego

--------------------------------------

Sacar IP y datos de un servidor al entrar

https://www.netlimiter.com/

--------------------------------------

metadatos

https://www.metadata2go.com/

<https://www.pic2map.com/>

https://jimpl.com/

--------------------------------------

Datos que no importan mucho

Metadatos - sacar datos de una foto

Intranet - Una intranet es una red informática que utiliza la tecnología del protocolo de Internet

Log poisong - ¿Qué es el envenenamiento de troncos? El envenenamiento de registros es una técnica común utilizada para obtener un shell inverso de una vulnerabilidad LFI.

Lpt – licencia pentester tester

Ctf - wargame

RDP – Remote desktop protocol

Vishing - estafa al costo de la luz y estafa de llamadas

Análisis de frecuencias - En el criptoanálisis, la técnica de análisis de frecuencias consiste en el aprovechamiento de estudios sobre la frecuencia de las letras o grupos de letras en los idiomas para poder establecer hipótesis para aprovecharlas para poder descifrar un texto cifrado sin tener la clave de descifrado (romper).

Extrapolar cc - Básicamente extrapolar un BIN nos sirve para vulnerar una pagina con mayor facilidad, supongamos que queremos burlar http://www.lightinthebox.com/ usando el 414720. Generamos las tarjetas necesarias, en este caso generaré 10.

CLS - En informática, CLS es un comando utilizado por los intérpretes de línea de comandos COMMAND.COM y cmd.exe en los sistemas operativos DOS, Digital Research FlexOS, IBM OS / 2, Microsoft Windows y ReactOS para borrar la pantalla o la ventana de la consola de comandos y cualquier salida generada por ellos.

--------------------------------------

Espiar movil (app)

Spyzie

--------------------------------------

App para modificar apks y modificar Código etc

Apkeditor

--------------------------------------

Nmap online

<https://nmap.online/>

--------------------------------------

Jugar juegos de PSP en movil

Igames

--------------------------------------

Episodio completo de Bob Esponja en discord

<https://cdn.discordapp.com/attachments/971746118390149151/972991682477965372/SpongeBob_SquarePants_S01E01A_Help_Wanted.mp4>

--------------------------------------

Pelicula completa de Shrek en discord

<https://media.discordapp.net/attachments/870065131147657236/990364685301841930/SHREK2COMPLETALATINO.mp4>

--------------------------------------

como sacar ip de alguien en un grupo de pley

instalamos wireshark en nnuestro ordenador lo ejecutamos nos conectamos a una red cualquier que nos activa wireshark como red wifi y entramos a la red que tiene actividad y despues el programa nos dirá todo lo que hacemo en la nuestra ip y solo tenemos que buscar arriba en el buscador UDP entramos a un grupo de pley y nos saldrán muchas iPS y serán las iPS de las victimas o de nuestros amigos xd.

tutorial para por si no lo habéis entendido

[HOW YOU CAN PULL IPS ON PS4 & XBOX ONE (Educational Only, do not do this)](https://youtu.be/WUQvb1QtPd4)

[](https://youtu.be/WUQvb1QtPd4)

--------------------------------------

Bins

Generador: <https://www.freebinchecker.com/bin-generator/>

Checker: <https://checker.visatk.com/ccn1/>

--------------------------------------

Buscar datos de un correo/ip/domicilio/página web

<https://intelx.io/>

--------------------------------------

Call spoof (caller id spoof)

Any call

--------------------------------------

SMS spoof (enviar SMS con el número de otra persona)

<https://github.com/trustedsec/social-engineer-toolkit>

--------------------------------------

SMS spoof y call spoof

<https://github.com/IncredibleHacker/Fl00d-Attacker>

--------------------------------------

Crear iploggers

Iplogger.com

--------------------------------------

Bots en t

Zefoy.com

--------------------------------------

Como buzonear número de whatsap

Primero pide una verificación de número por llamada luego esperas 40 segundos y llamas y te saldrá el contestador del número abres el teclado están en la llamada y pones el Código de cada número +34 es un número distinto y el de otro país será otro tenéis que buscar el Código de cada país y para que el número sea vuestro para siempre tenéis que verificarlo en una aplicación que están y por si quieres hacer lo de buzonear sin que sepan tu número puedes ponertelo oculto poniendo esto donde para llamar #31# y ponemos el número de teléfono con el prefijo del país incluido o puedes usar la app any call que estan en Google play y para escuchar el buzón de voz del numero de teléfono buscamos como buzonear número whatsap +34

--------------------------------------

Sacar ip en Telegram

Hay un programa en el word que analiza el tráfico que se está enviando cuando llamamos a esa persona y mediante eso podemos descubrir la ip y mediante la ip podemos adivinar el número de teléfono con un programa que esta en este word aunque no se si es el Real el único que he visto que sabe hacerlo es s4vitar y con todo lo que he dicho aquí podemos saber muchos datos de alguien solo por su Telegram

--------------------------------------

Repetidor wifi

Módulo esp8266 de Arduino

--------------------------------------

Borrar objetos de fotos

<https://cleanup.pictures/>

--------------------------------------

Subir fotos a una página para que otros vean esa foto

<https://es.imgbb.com/>

--------------------------------------

Crear url acortada

https://www.shorturl.at/

--------------------------------------

Crear chat web

<https://hack.chat/>

--------------------------------------

nota privada

<https://privnote.com/>

--------------------------------------

Ip logger en una foto

[How to make an image ip logger on discord](https://youtu.be/4PadOjkW26Y)

[](https://youtu.be/4PadOjkW26Y)

--------------------------------------

Ganar dinero por ser amigo de alguien

<https://www.friendpc.com/>

--------------------------------------

Muchas cosas para hacer hacking

<https://start.me/p/L1rEYQ/osint4all>

<https://start.me/p/DPYPMz/the-ultimate-osint-collection>

--------------------------------------

Tips de pc

Restablecer graficos: Windows + Control + shift + B

Varios escritorios: Windows + CTRL + D

Captura de pantalla: Win + Shift + S

--------------------------------------

Pasar fotos a texto

https://www.text-image.com/convert/

--------------------------------------

Ver películas

Películasflix

Hdtoday

<https://www.watchfree.website/>

<https://ver.cuevana3.cc>

--------------------------------------

Ver como quedaría tu cuarto con otra distribucion

http://www.planyourroom.com/

--------------------------------------

Eliminar voces de una musica

Vocalremover

--------------------------------------

Crear video personalizo con inteligencia artifical

Synteshia.io

--------------------------------------

SMS de alta

<https://join.fun4all.cc/lpx/tsgxoO09El?aff=fm-a5d1c7bb-bbcb-42ac-9044-cad3c562a05b&reqid=wrj9ci1t8t79kg0e24j1gjf8&oid=0bf0ff0e-fe74-457c-bd47-ed373f936be2&affid=a5d1c7bb-bbcb-42ac-9044-cad3c562a05b&s1=9066>

<https://secure.fun4mobb.com/lpx/H5FUOmcM2C?aff=fm-2ae7a222-dbb5-428a-9ee7-102985d886b7&reqid=w71gegmghu2030sg2l3ql1es&oid=39aaa9a3-a049-4f78-8f1e-2dbead26d4f0&affid=2ae7a222-dbb5-428a-9ee7-102985d886b7&s1=1211_305088>

--------------------------------------

⃟

--------------------------------------

Libro hacking

<https://mega.nz/folder/ZJd3QCJB#B7cgAft705tk5FBsYoV9Fg>

--------------------------------------

🟡🔵🐔😳🥵😳😂🥶🥶

--------------------------------------

Máster en ciberseguridad

<https://ns2.elhacker.net/descargas/Cursos/Máster%20en%20Seguridad%20Informática.%20De%200%20a%20Experto%20.%20Año%202020>

--------------------------------------

😡👍👍😡👍😡😡👍

--------------------------------------

👨‍💻 Curso Completo Online de Hacking Ético (Udemy 8.26GB) 🔐

<https://www.mediafire.com/file/fn9f2xxswrtc4et/Curso+Completo+de+Hacking+%C3%89tico.zip/file>

--------------------------------------

👍😡😡👍😡👍😡👍🥵😔

--------------------------------------

[GRATIS] MEGA LISTA APK HACKEADOS (no tienen mucha utilidad pero todo lo que tenga que ver con seguridad informática hacking etc estará en este word)

1. WhatsApp+: <https://www.mediafire.com/file/shkqzszlndzteon/FMWhatsApp_14.11.4_Release.apk/file> ajustes de privacidad modificados, todo personalizable.

2. Instagram+: <https://www.mediafire.com/file/2n67i6x74i1d6i3/instander-v5.2_by_Thekruher.apk/file> + ajustes de privacidad, poder descargar fotos y videos.

3. Spotify Premium: <https://www.mediafire.com/file/sw8t1rrrh1wxudk/Spotify_Premium_v8.6.0.830_MOD_apkmody.io.apk/file> free premium.

4. Subway Surfers: <https://www.mediafire.com/file/k9qwxtj18wez9tf/subway-surfers-mod_2m.apk/file> moneda s infinitas.

5. Lucky Patcher: <https://www.mediafire.com/file/gnhwi6s6k3uecwa/lucky-patcher-9-4-0.apk/file> es una herramienta simple para ‘’hackear’’ apps. Funciona para móviles con o sin root.

6. NETFLIX+: <https://www.mediafire.com/file/qcoavtfwhrjcuv6/Netflix_v7.93.1_MOD_apkmody.io.apk/file> Peliculas y series gratis ;)

7. ASSASINS REBELION:

[https://www.mediafire.com/file/s6wras5c5usa5x8/assassins-rebellion-mod\_2.8.1.apk/file monedas infinitas](https://www.mediafire.com/file/s6wras5c5usa5x8/assassins-rebellion-mod_2.8.1.apk/file monedas infinitas8)

[8](https://www.mediafire.com/file/s6wras5c5usa5x8/assassins-rebellion-mod_2.8.1.apk/file monedas infinitas8). Transit king tycoon:

[https://www.mediafire.com/file/97f3zjn255uw891/Transit\_King\_Tycoon\_v3.6.apk/file mod menu](https://www.mediafire.com/file/97f3zjn255uw891/Transit_King_Tycoon_v3.6.apk/file mod menu9)

[9](https://www.mediafire.com/file/97f3zjn255uw891/Transit_King_Tycoon_v3.6.apk/file mod menu9). Counter Sniper:

[https://www.mediafire.com/file/qo8ww0kavagr3de/Countersnipe\_1.2.apk/file monedas infinitas](https://www.mediafire.com/file/qo8ww0kavagr3de/Countersnipe_1.2.apk/file monedas infinitas10)

[10](https://www.mediafire.com/file/qo8ww0kavagr3de/Countersnipe_1.2.apk/file monedas infinitas10). Into the death 2:

[https://www.mediafire.com/file/cznrosb7m41fcjf/Into\_the\_Dead\_2\_v1.32.0.apk/file monedas infinitas](https://www.mediafire.com/file/cznrosb7m41fcjf/Into_the_Dead_2_v1.32.0.apk/file monedas infinitas11)

[11](https://www.mediafire.com/file/cznrosb7m41fcjf/Into_the_Dead_2_v1.32.0.apk/file monedas infinitas11). Real Driving:

[https://www.mediafire.com/file/ovry576mr2q8002/Real\_Driving\_Sim\_v3.8.apk/file monedas infinitas](https://www.mediafire.com/file/ovry576mr2q8002/Real_Driving_Sim_v3.8.apk/file monedas infinitas12)

[12](https://www.mediafire.com/file/ovry576mr2q8002/Real_Driving_Sim_v3.8.apk/file monedas infinitas12). HIDE:

[https://www.mediafire.com/file/sv62xuxx4n7b0fx/HIDE-MOD-0.28.26.apk/file mod menú extenso](https://www.mediafire.com/file/sv62xuxx4n7b0fx/HIDE-MOD-0.28.26.apk/file mod menú extenso13)

[13](https://www.mediafire.com/file/sv62xuxx4n7b0fx/HIDE-MOD-0.28.26.apk/file mod menú extenso13). Legend of Solgard:

[https://www.mediafire.com/file/msvf98dkpcarmrz/Legend-of-Solgard-MOD-2.6.2.apk/file monedas infinitas](https://www.mediafire.com/file/msvf98dkpcarmrz/Legend-of-Solgard-MOD-2.6.2.apk/file monedas infinitas14)

[14](https://www.mediafire.com/file/msvf98dkpcarmrz/Legend-of-Solgard-MOD-2.6.2.apk/file monedas infinitas14). Metal Squad:

[https://www.mediafire.com/file/a2ff54njo2ekq0h/Metal-Squad-Shooting-Game-MOD-2.1.5.apk/file monedas infinitas](https://www.mediafire.com/file/a2ff54njo2ekq0h/Metal-Squad-Shooting-Game-MOD-2.1.5.apk/file monedas infinitas15)

[15](https://www.mediafire.com/file/a2ff54njo2ekq0h/Metal-Squad-Shooting-Game-MOD-2.1.5.apk/file monedas infinitas15). Prime peaks:

[https://www.mediafire.com/file/zqvke89e7c7ct55/prime-peaks-mod\_24.8.apk/file monedas infinitas](https://www.mediafire.com/file/zqvke89e7c7ct55/prime-peaks-mod_24.8.apk/file monedas infinitas16)

[16](https://www.mediafire.com/file/zqvke89e7c7ct55/prime-peaks-mod_24.8.apk/file monedas infinitas16). Among Us: https://apkadmin.com/whrbwv86y849/Among\_Us\_SUPER\_MOD\_MENU.apk.html

--------------------------------------

🥵🥵😱😱🥵🥵😱🥵😱🥵😱🥵

--------------------------------------

CURSO COMPLETO DE HACKING ETICO Y CIBERSEGURIDAD - SANTIAGO HERNANDEZ

https://drive.google.com/drive/folders/1DstNA5jbzYnSeqPkevndlZmwg9IG4D4H

--------------------------------------

😱🥵😱🥵😱🥵🥳🥵🥳🥵🤣🥵

--------------------------------------

👨‍💻CURSO BÁSICO DE CIBERSEGURIDAD (SOLO 2 HORAS)👨‍💻

<https://learndigital.withgoogle.com/activate/courses>

--------------------------------------

🥵🥳🥵🥵🥳🥵🥳🥵🥳

--------------------------------------

Borrar datos de la dns

abres CMD y pones este comando t borras todos los datos de la dns

ipconfig /flushdns

(Método para borrar datos de la dns si no eres de PC o no tienes un PC

chorme://net-internals/#dns

--------------------------------------

🥵😇😇😇☣︎☄︎🜲

--------------------------------------

Tools OSINT

¿Qué es el OSINT? En realidad el nombre es Inteligencia de fuentes abiertas El OSINT es la busqueda de informacion por ejemplo de un email en fuentes abiertas con fuentes abiertas me refiero a informacion que por ejemplo esta en google,facebook, redes sociales, etc.

Paginas de OSINT:

Osintframework: <https://osintframework.com/>

Osint techniques <https://www.osinttechniques.com/osint-tools.html>

Herramientas para OSINT para kali linux,parrot, etc.

Maltego: <https://www.maltego.com/>

Awesome-Osint: <https://github.com/jivoi/awesome-osint> (Lista de muchas tools de OSINT)

Passwordcheck (Herramienta para ver cuantas veces se ha filtrado una contraseña:: <https://github.com/cristianzsh/passwordcheck>

PhoneInfoga (Sacar informacion de un numero): <https://github.com/sundowndev/phoneinfoga>

Osintgram (Sacar informacion de una cuenta de un perfil de instagram): <https://github.com/Datalux/Osintgram>

Sherlock (Buscar un usuario en diferentes redes sociales): <https://github.com/sherlock-project/sherlock>

Instalaciones:

Passwordcheck:

Apt install git -y

Apt install python -y && apt install python3 -y

Pip install getpass

Pip install requests

Git clone <https://github.com/cristianzsh/passwordcheck>

Cd passwordcheck

Cd src

Python3 passwordcheck.py

Osintgram: <https://www.youtube.com/watch?v=nZovrZQdW7k>

--------------------------------------

😳🤣😇😐🥵🤨

--------------------------------------

Mail2Tor correo electrónico anónimo recibir correos anónimos y enviar correos de manera anónima

<http://mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion/>

--------------------------------------

🥶😂😂დ .•\*””\*• text •\*””\*•.დ

--------------------------------------

[CURSO] Hacking y Penetration Testing de Dispositivos Android

<https://mega.nz/folder/xllhgSpZ#vwb25HYrofXXfDh0Tpc1jA>

--------------------------------------

🥵🥵🐔🐔🐔💙

--------------------------------------

Curso hacking python

<https://mega.nz/folder/m5NQQbAI#YUPl8W2o3Ja_tZKhhP5PZA/folder/asNCWBbI>

--------------------------------------

🥵🤣🥵🤣🥵🤣🥵🤣👍🤣

--------------------------------------

Página para hacer justificantes médicos falsos

<http://jacasu.es/>

--------------------------------------

😐🤡😐🤡😐🙂😐🙂😐🙂🙂😐

--------------------------------------

Crear chat de whatsap falso

https://www.fakewhats.com/generator#

--------------------------------------

❣❣❢

--------------------------------------

Descifrar/cifrar -criptografia

https://www.google.com/amp/s/amp.base64decode.org/

<https://www.cryptool.org/en/cto/caesar>

--------------------------------------

`́́́`́́́

--------------------------------------

Leeme (pdf): <https://mega.nz/#!x85w2LCY!ZmBgQpjg5SARFPrw1ha5r60mFbUFawN-t6FHOYF99us>

Peso: 269 KB

Sesion 1 Introduccion

Link: <https://mega.nz/#!8kwllZBR!EO9ycAUXd7ETpk0k6xZftxKFIlaJuzJENog8d7bLkuk>

Peso: 71 MB

Sesion 2 Footprinting

Link: <https://mega.nz/#!UwgGRCpR!57uh1rwJtWo5mIA9Afx7QOTzv3WyaHIdWz2OGxT8I64>

Peso: 109 MB

Sesion 3. Scanning

Link: <https://mega.nz/#!QsJAQTZR!vIf-rpA-f7DXD9PdEold8VuTvN08GGHOSj114LbJrcw>

Peso: 126 MB

Sesion 4 Anonimato y privacidad

Link: <https://mega.nz/#!c0ID0JJY!5-UnPpcabCfF0OZtjyitQGKY5JdnbeAcORPXRwZZ4TM>

Peso: 101 MB

Sesion 5 Enumeracion

Link: <https://mega.nz/#!lphRlJIL!oMB00QReteTUbBxpiLnsx4xHrnIYoacEpA-3yWXxCBk>

Peso: 61 MB

Sesion 6 Ganando acceso

Link: <https://mega.nz/#!0kJ0FL6L!dPrXilAns6rWfGoL8TQtbnLvNZf2yvWTZEVPxMsUPCY>

Peso: 71 MB

Sesion 7 Escalando privilegios

Link: <https://mega.nz/#!Mxx0mCzI!kmInoAzl-C_HyQVXAECIaqI3XC8EhSVOeFc7ePLgvO0>

Peso: 79 MB

Sesion 8 Hardering

Link: <https://mega.nz/#!hsIACZYB!SiP263P-K9puV5Y_6MWKMsxHbyJF1mjZY5pKcV0EZTM>

Peso: 48 MB

Sesion 9 Introduccion al hacking avanzado

Link: <https://mega.nz/#!lxIUlL6J!C1kJ10iGf4JgPP09qI5K_QvSzpxKzw6X5mAJEosgaSg>

Peso: 6.6 MB

Sesion 10. Protocolos y servicios

Link: <https://mega.nz/#!Io4CDaZQ!n0mkrV5ujCy4fYCt7_e9Cte4mllWLJ1Lg2aSBKacMug>

Peso: 88 MB

Sesion 11. Reconocimiento y scanning

Link: <https://mega.nz/#!h9ZDASDC!e8gCXbOk9b-4LpfnsoqBozCrvwUitMaMcAJhvgiWrPQ>

Peso: 174 MB

Sesion 12. Enumeracion y vulnerabilidades

Link: <https://mega.nz/#!UshijQDI!-vqolIqGhEEmXsng_xMEyXoM8jakRwRAzI4liRwFH8w>

Peso: 67 MB

Sesion 13. System hacking

Link: <https://mega.nz/#!N15ChSTY!Zj79-HP1_hfdPskicZ_4mkEwf9WXMnEoWfwEnQwzu0s>

Peso: 59 MB

Sesion 14. Troyanos y backdoors

Link: <https://mega.nz/#!o1JRULhD!T670FjvW2Gj87u70AQ66Qb1odX8-sk6XpCBsOXaH01k>

Peso: 87 MB

Sesion 15. Virus y gusanos

Link: <https://mega.nz/#!ZtIyTCIL!HYVt3h8C-_yDvmkQeIFSpKcoRGr3nDJDvF0wqpSFDFY>

Peso: 91 MB

Sesion 16. Denegacion de servicio

Link: <https://mega.nz/#!c5onzSST!kSyuoiYuysD0s7weLV0sCs5Ae-JWWjfUQ_bWzOiUAMg>

Peso: 51 MB

Sesion 17. Hacking wireless

Link: <https://mega.nz/#!hhZQxZTZ!qsWBCw0-wo6nL4S-HBvvD_jLGlMman4Af7mkMfwyI04>

Peso: 248 MB

Sesion 18. Sql injection

Link: <https://mega.nz/#!otZEyTzR!QYUDg4R6hykDybnczaBzOubb9G3HJeSZySdSAqaRusI>

Peso: 46 MB

Sesion 19. Honeypots y honeynets

Link: <https://mega.nz/#!dlxhGIYZ!e7KosOOrOlFRuMqdN25F3O4pG9YKsWmsbhCTG_KqFuk>

Peso: 124 MB

Sesion 20. Seguridad en vpn

Link: <https://mega.nz/#!clYWRZCT!Q_Mb2iPj61Y-15gObqDarPkYxRCZWX8EIFBHlhsY5xs>

Peso: 22 MB

Sesion 21. Linux hacking

Link: <https://mega.nz/#!ctIimAgC!VaPb8pFq3Oev4gmFPT07pLeX_ORiMQwGSGt6fLtXens>

Peso: 72 MB

Sesion 22. Buffer overflow

Link: <https://mega.nz/#!V4o3WD4Z!kCIptkUty7hF0_a3V_POb1yo-RdWZCtIESdGQcVbbD0>

Peso: 24 MB

Sesion 23. Vulnerabilidades web

Link: <https://mega.nz/#!w8IFxAgD!gsvL8EYE1QwI-8sYmbrzp2p0y3sMIWmc2DA24JgaUzI>

Peso: 36 MB

Sesion 24. Criptografia – cifrado de datos

Link: <https://mega.nz/#!k8JTRQYL!Flc2_X8VifpivGfu1fyAybgHZVuWByIHSGAYRTCZMlc>

Peso: 607 MB

Sesion 25. Codigo virico

Link: <https://mega.nz/#!RhQzCSLK!LFEPTWLR7veDcbd6MwyOJg_ms0es7FYVxBeQx_7_ZKA>

Peso: 256 KB

Sesion 26. Escritura de exploits

Link: <https://mega.nz/#!J4o2yZia!zP0d2EQLDL-rVIzn6RQ6y3NNgZXJmmPRcyVMa52M_68>

Peso: 30 MB

Sesion 27. IDS y HIDS

Link: <https://mega.nz/#!IgYCiQwC!Ua_vZcS9Qhv4Crciio8AYX7JlHq203CnVofvkXKrxrY>

Peso: 70 MB

Extra:

Sesion Extra Analisis de trafico Metodo Sniffing

Link: <https://mega.nz/#!9gJkgCwR!H6ZUW6BFhfMBlncMzti46pXF_WHA9fBrWp1uhZqdkpY>

Peso: 60 MB

--------------------------------------

😡🥵🤓😡🥵🤓

--------------------------------------

-Matlab desde Cero—

<https://mega.nz/folder/5WphSSDQ#Is9RR9Ny4oy7HIIawnW1xQ>

--Libros de Reparacion en PC—

<https://mega.nz/folder/JK4lkKyB#4E3YEgVX34hPH-eX66HV6w>

--Seguridad en Redes IP—

<https://mega.nz/folder/ZepjiAoI#lyN4TRNv7SDL6_r5hcL1_g>

--Libros de Seguridad Informatica—

<https://mega.nz/folder/kKBEzTwI#K-Tgfon5ij9i9zmuBG40jA>

--Libros de VisualBasic—

<https://mega.nz/folder/1XgzTI4K#Ynt2sOcT8JA74UN9_D0yyw>

--Libros de Python—

<https://mega.nz/folder/ZHACwLDD#Kj45Sqj32PU5vV88DGkJUg>

--Libros de Java—

<https://mega.nz/folder/UH4D2IIA#BFMsD2OJqNbrfErcy77Ywg>

--Libros de JavaScript—

<https://mega.nz/folder/QSQEHBCB#sWrwm4iZZVvdztmoblM31w>

--Libros de Introduccion al Software Libre—

<https://mega.nz/folder/dKYWHBAS#TiNjknohDfeh3_mUkLqXSg>

--Diseno\_paginas\_web\_accesibles--

<https://mega.nz/file/kGJgwTjT#NuxPyfZFS6G003caaL1MXftal_tkY4Ox4BzqN9fTQng>

--36-Pasos-basicos-para-desarrollar-un-Sitio-Web--

<https://mega.nz/file/wSQ23LoC#aFCAcGFxVyZA3dC8b_Rw2oFr66bFZBQyuHNWbEHNoIU>

--TyScript desde cero—

<https://mega.nz/folder/NToFFSYB#Eq6qsJTSDI9ZG2FZ3kVz0Q>

--Git desde cero 2020—

<https://mega.nz/folder/lGJmjLrS#5YMIrsLmR1hIeFclaD9kHQ>

--Tablas Dinamicas en Excel—

<https://mega.nz/folder/oCYkiDQB#FRvPnSYCjaIzgUBasUmfUA>

--Master en C# en tiempo record—

<https://mega.nz/folder/EbYyURLD#pibx812O7WYAQKvPqRj8aw>

--Curso de Mecanica General—

<https://mega.nz/folder/ISYQBRaA#Yx2t9meoMx3a16eIP3ZPXg>

--Tu Guía Completa de Fotografía—

<https://mega.nz/folder/FKIS3JoB#5RIn_EP-5Gk18HQLPf6jMw>

--Dirección de Arte con Cinema 4D—

<https://mega.nz/folder/5aZ0yZBK#Hxhx-wHSx1Ds9PzmeUxURA>

--Udemy-Electron JS y React JS Creando un Spotify--

<https://mega.nz/folder/tKQmHTya#sioEwlxqjBA1zCeM6CXGWQ>

--Udemy-Excel para negocios Básico hasta avanzado—

<https://mega.nz/folder/Qah12AjC#uFHdQFN_uezHC4G9VKU4Ng>

--Curso de Pentestig—

<https://mega.nz/folder/gXRmCbLK#TXNZNUBtqQ-QyZa9kYdjRQ>

--------------------------------------

😎🤓😎🥵😎🥵😎🥵

--------------------------------------

\*Libros\*

\_Anonymus tools\_ <https://mega.nz/#F!wRBXFKRA!NHp2nHtmyga9p2pjn0y2BQ>

\_BUSCANDO VULNERABILIDAD\_ <https://mega.nz/#F!5VRQRIZa!S9UqtB2YNYz2tHuVGbivYg>

\_CREACION DE EXPLOITS\_ <https://mega.nz/#F!ZcgmGYLZ!rX3q_b7hrzNyG2kX7wjXuA>

\_CURSO DE BATCHS\_ <https://mega.nz/#F!cc50VYbR!OXE_P6qYhY7EPKaHygRpbA>

\_CURSO DE PERL+MANUALES\_ <https://mega.nz/#F!gJgzkbqR!f55hOXM8sR2aZIfPPMMswg>

\_CURSO DE BOOTSTRAP 3\_ <https://mega.nz/#F!gEZEyK4b!xhqeDdOvBk1o5feEvtipqg>

\_CURSO DE HT\_ <https://mega.nz/#F!FZ4WHYIK!aut73QZhXlAlQxZUMht85g>

\_CURSO DE HTML Y CSS\_ <https://mega.nz/#F!4MRyxCgI!sD1SYCXRyA-YIqeK_5a8Xg>

\_CURSO DE LINUX\_ <https://mega.nz/#F!JAYFUCaa!bYf4uexnwAIC3StJie3ZBQ>

\_CURSO DE NODE\_ <https://mega.nz/#F!xUxkBZZZ!QOh4vOMuzXaE_CF0zE9Ukw>

\_CURSO DE PYTHON\_ <https://mega.nz/#F!sEInnRCK!m0UplIKhQ4gAmKw83Nps8Q>

\_CURSO DE RESPONSIVE WEB DESING\_ <https://mega.nz/#F!NZBlFYDZ!YUt4RlpTsSircIJ6vAmIFQ>

\_CARPETA CURSO EH Y CEHv8\_ <https://mega.nz/#F!pNZnTT5K!kUrdcyqQALR2B_zKAkI8IQ>

\_CURSO LENGUAJE JAVA SCRIP\_ <https://mega.nz/#F!ZI5STRzD!HPtywhi29J_DjrJwBrNV7g>

\_CV9 TOOLS\_ <https://mega.nz/#F!IU4lgYRY!YEBY6aI-Lt6ktMfTpakzJQ>

\_HACKING\_ <https://mega.nz/#F!5YQVXZKZ!ClGnFFA2Cpd8Ni-pwXBNzA>

\_EL ARTE DE LA INTRUICION\_ <https://mega.nz/#F!sRJhlLAT!keORu4lBbHTYG-PSav5wAg>

\_GUIA PROGRAMADOR\_ <https://mega.nz/#F!wdJxzSbL!aHkbLJHCrza7HW3c4BwLSg>

\_HACKING SPOSED\_ <https://mega.nz/#F!YMhBkbQa!MkeyyuSr4FlvesPDP3Hf_w>

\_HACKING WIFI MIKROTIK\_ <https://mega.nz/#F!9Rg0TILY!RQs71eLNeC9RjoFGk6qDHQ>

\_INTRODUCCIÓN DE ALGORITMOS\_ <https://mega.nz/#F!dYgXRb7R!ipNSsW1b0SgOKUKdNy_CIA>

\_LIBRO DE AMENAZAS INFORMÁTICAS\_ <https://mega.nz/#F!xBR1BI5Q!BUSiiYzCze879nobibxb5g>

\_LIBRO KALI\_ <https://mega.nz/#F!VUAxHQiJ!WLze8B6g9vuOwUOPbpHTvg>

\_LIBRO EN BLOQUE\_ <https://mega.nz/#F!UZYyATrI!2HlUsbIiVQsoH8dlNhuvcg>

\_MAHYAN\_ <https://mega.nz/#F!YcJnFRwL!2SWlh2q0T83Aa5ebGpUKUQ>

\_MEGA PACK DE LIBROS , REDES E INFORMATICA (REPETIDOS)\_ <https://mega.nz/#F!YEYGELLA!hLBF_iN8VAMbwJHO3cRRhw>

\_PROYECTOS DE ELECTRONICA\_ <https://mega.nz/#F!RUISkCDK!zkUZh0tfrsIKAUvVoOyJUg>

\_LIBROS DE HACKER\_ <https://mega.nz/#F!RRRHmBiC!MXUgejPHX_cLOZqMp3gg4A>

\_LIBROS DE INFORMATICA\_ <https://mega.nz/#F!JE4xAART!SKWfdYeYPdBySXEzSMmHdg>

\_VULNERABILIDADES WEB\_ <https://mega.nz/#F!gABUDCRC!OLnaq7mSXYLwjLq-u9jzvg>

\_MICROSOFT WINDOWS SERVER 2\_ <https://mega.nz/#F!sdJHTRQK!gFJ0ToNj251Rk01vdKhryg>

\_ALGEBRA BALDOR\_ <https://mega.nz/#F!VcB0CDpB!B36aEAlmOXpypnLJ1H-ZOg>

\_ANGULAR\_ https://mega.nz/#F!pd4AybyT!ZZTClzhN1GJfV49semwNuQ

--------------------------------------

◤◢◣◥◤◢◣◥◤◢◣◥◤◢◣◥

--------------------------------------

Página de un grupo de hackers llamados Arvin Club autores de un ataque de ransomware publican información de varias cosas

<http://3kp6j22pz3zkv76yutctosa6djpj4yib2icvdqxucdaxxedumhqicpad.onion/>

--------------------------------------

Saber si eh sido pwneado

Correo/numero – <https://haveibeenpwned.com/>

Contraseñas - https://haveibeenpwned.com/Passwords

--------------------------------------

💙🐔🐔🐔🐔🐔

--------------------------------------

Espiar/archivar chats de WhatsApp

<http://ul.to/wwbnlql0>

<http://freakshare.com/files/30evclpj/extract_recovery.rar.html>

--------------------------------------

⟬Wiki⟭﹏〰︎

--------------------------------------

The Hidden wiki: <http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/>

* Página donde se pueden encontrar más links de la deep web armas, drogas, más wikis, etc

--------------------------------------

🥶😱😔😡😡😡😡😔😱😱

--------------------------------------

Receta de metanfetamina(C10H15N)

Igredientes:

• Fósforo rojo(50 g)

• Cristales de yodo(50g)

• Éter(50ml)

• Alcohol etílico de 96º(500 ml)

• Pastillas para la sinusitis/ibuprofeno de pseudofedrina(aprox. Unas 5 cajas)

• Ácido sulfúrico

• Cloruro de sodio

• sosa 1 L

Dónde conseguir los ingredientes:

El fósforo rojo se puede conseguir en cualquier ferreteria, los cristales de yodo se

Consiguen en una tienda de química o en Amazon xD, el éter es un conocido compuesto

Que se consigue en tiendas de bricolaje o en ferreterias industriales. El alcohol etílico de

96º es el alcohol sanitario de toda la vida, y las pastillas se compran en farmacias

Incluso en algunos supermercados. El cloruro de sodio es sal de mesa y el ácido

Sulfúrico se compra en cualquier droguería.

Equipo necesario:

• Matraz Erlenmeyer de 500

• Matraz aforado(mezclas básicas)

• Molde de magdalenas o repostería(puede sonar absurdo pero es necesario)

• Unas 10 jeringuillas de plástico de 5 ml, no tienen por qué ser de buena calidad

• Bombeador de gas

• Mascarilla protectora

• Botiquín de emergencia

• Mechero de laboratorio

• Limpiaojos de emergencia

• Guantes

• Habitacion con ventilacion

Preparación:

1. Echamos en un bote todo el alcohol junto con las pastillas que has ido

Machacadas anteriormente. Se disuelve solo, esperar unos minutos.

1. Se cuela con el envoltorio de papel de la magdalena y se vierte en otro

Recipiente.

1. Por otra parte, se juntan en un recipiente cualquiera los cristales de yodo y el

Fósforo rojo.

1. El líquido sobrante (el del paso 1 y 2)se hierve en la matraz Erlenmeyer con el

Mechero

1. Y al fósforo y al yodo se le añade éter, posteriormente se extrae con una

Jeringuilla el líquido que hay en la parte superior

6. Añadimos 5 jeringuillas llenas al matraz Erlenmeyer mientras hierbe

7. Borboteamos con cloruro de hidrogeno, que se consigue juntando el acido

Sulfurico y la sal

8. Se le añade sosa 500ml

No esta explicado bien del todo ya que otros metodos mejor explicados son mas chungos este es el casero

No me hago responsable del mal uso que se le pueda dar a esto,solo lo posteo para fines educativos.

Hacer clic para expandir…Me ha salido un poco sosa, no le falta una pizca mas de sal? O como dirias tu, una pizca de cloruro de sodio✨

--------------------------------------

😂😂😔😂😂😔😡

--------------------------------------

Reverse Engineering and Malware Analysis Fundamentals – udemy

https://ns2.elhacker.net/descargas/Cursos/Reverse%20Engineering%20and%20Malware%20Analysis%20Fundamentals/

--------------------------------------

𓁭𓁡𓅢♿︎☤

--------------------------------------

No es .onion pero es una pagina para subir Doxxeos de todo

Doxbin: <https://doxbin.com/>

--------------------------------------

🪃🪃🪃🪃🪃🪃🎱🏀🏀🪀🪀🏓

--------------------------------------

LIBROS de 0xWORD

https://mega.nz/folder/dGokFSwC#uJGryx3sO6Jgvb1OxptZ3A

--------------------------------------

🙃🙃😎🙃😎🙃

--------------------------------------

1. 15 CARDING NEW VIDEOS :

—Use For Learn—

<https://mega.nz/folder/8Jg3UaiC#iHAu3ljJnTzKRmboRG6njA>

1. BTC TUTORIALS:

<https://mega.nz/#F!CDoXwY4B!pDFii8GS5RQzWpBa-KWeew>

<https://mega.nz/#F!uWAm0Q7I!UEwHfGHrykMB4S23Ylg50A>

1. FULL ANDROID HACKING :

<https://mygavilan-my.sharepoint.com/:f:/g/personal/kali_masi_my_gavilan_edu/EqHWjlOZBipFqojj04ZabS4B7rfBYUEqDe495Q5Q6QbXHA?e=MWn23f>

1. Rating 4.6 Feature Engineering for Machine Learning

<https://mega.nz/folder/FAwFQbrb#CQPxWKT1iM-cboK-ORe4DA>

1. 2 TB COURSES :

https://mega.nz/folder/rrJyDQIa#-QJeJqVThi\_uC9DTLX4ElA

--------------------------------------

🇺🇦🇺🇦🤨

--------------------------------------

?

https://www.ocr2edit.com/es

--------------------------------------

⃟

--------------------------------------

Libro de crackeo

<https://mega.nz/folder/dIkw2aYa#VPSXahuDOfoDUZ1zOlfrtw>

--------------------------------------

🥵📸🖤

--------------------------------------

Programa para hacer placas bases y demas

<https://www.altium.com/asp/youtube?utm_source=youtube&utm_medium=social&utm_campaign=yt-sponsor&utm_content=nate-gentile>

--------------------------------------

🥵🤨🥵🤨🥵🥵🔑🥵🔑

--------------------------------------

Una guía práctica para Red Teams y Offensive Security Enlace de descarga: <https://www.mediafire.com/file/kbg6kxqgt...m.pdf/file> Virustotal: <https://www.virustotal.com/gui/file/ed90...84b8c806db>

--------------------------------------

⃟⃤

--------------------------------------

Cámaras de seguridad de centros comerciales etc

<https://ghostbin.co/paste/ru9kr>

--------------------------------------

🕹🐶🕹🐶🔑🤨🔑🤨

--------------------------------------

Práctica ofensiva

--------------------------------------

⃟⃤�

--------------------------------------

Para acceder a dispositivos moviles

https://www.shodan.io/

Utilizaremos el buscador shodan.io ,os registráis y en la barra de búsqueda pondremos "airdroid", ahí nos saldrán montón de direcciones IP de móviles con airdroid instalado.

2º Solo tendremos que entrar a la ip en la flecha roja y se nos abrirá una nueva pestaña con la conexión al Airdroid.

3º Si aparece algo como "Conexión rechazada por el dispositivo", significa que la otra persona no acepto nuestra conexión... Podemos o pasar a otra o actualizar la página para enviar la misma petición.

Si tenemos suerte, la otra persona aceptará la conexión y estaremos dentro.

Cosas que podremos hacer:

Ver las imágenes, sonidos y videos de su galería.

Ver sus contactos, hacer y ver llamadas y sms.

Si quisiéramos ver sus cámaras o instalar aplicaciones a la otra persona le saltaría un aviso al que debe dar su permiso para que se inicie la cámara o la aplicación, por tanto levantaría sospechas.

Una cosa interesante que podemos hacer es robar su sesión de whatsapp.

Desde el airdroid nos llamamos a nuestro numero, así sabremos el numero de teléfono de la otra persona.

Registramos el whatsapp y cuando le llegue el SMS a la otra persona lo vemos en sus SMS recibidos en el airdroid y listo.

Este proceso vale para cualquier validación que se necesite un código por SMS.

--------------------------------------

⃟⃤█

--------------------------------------

Hacking etico

<https://www.mediafire.com/file/fn9f2xxswrtc4et/Curso+Completo+de+HackingCracking/hacking>

--------------------------------------

⃟⃤⃟⃤

--------------------------------------

Cracking/hacking

<https://mega.nz/folder/gN0WWaCa#-h4SkyqfcE3pzJ8aokptIA/folder/AZljVaYS>

--------------------------------------

👍👍👍👍👍👍

--------------------------------------

V1ruz

<https://mega.nz/file/a08X2ALS#vjgrtfeZpYj2ENv0sAWwP__J1lFFZzGrE8Ay88XMPTU>

--------------------------------------

🥵🥲😡😭🙂😡

--------------------------------------

Cracker cuentas Netflix, Amazon Prime, Disney+Hotstar, etc. Streaming

<https://www.mediafire.com/file/o6h5p83hwj4oj5q/MOMIX_2.1.8.2apk@nextalerts(1).apk/file>

--------------------------------------

😭😗😗😂😭💓😭💓😭

--------------------------------------

🔰 Top Websites to Get Followers/Likes in Instagram For Free 🔰

<https://famoid.com/get-free-instagram-followers/>

<https://www.digismm.com/free-trial/instagram-followers>

<https://skweezer.net/trial>

<https://www.instafollowers.co/free-instagram-followers>

<https://www.socialnoor.com/free-trial/in...followers/>

<https://instagrowing.net/free-instagram-followers/>

<https://www.idigic.net/trial/>

<https://uberinsta.com/free-trial>

<https://www.instandid.com/free-trial/>

<http://instamoda.org/>

<http://begeni.vip>

<https://takipci.instager.net/tools/>

<https://vipinstagramtakipci.com/>

<http://begenipanelim.com/>

<https://takipcistar.com/>

<https://igturk.com/>

<https://instagramtakipcihilesi.ist/ñ>

--------------------------------------

⃟⃤⃟⃤ ⃟⃤

--------------------------------------

Introducción al hacking etico s4vitar (mastermind)

Antiguo

<https://drive.google.com/drive/mobile/folders/1NWxH1_dk0HuteNuJ94WjfvQseqOhkP2O>

Actual

<https://www.mediafire.com/file/xgkdpeu6daf1v6j/Introducci%C3%B3n+Hacking+%C3%89tico+-+S4vitar.zip/file>

--------------------------------------

?⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤

--------------------------------------

Aprender a programar python

<https://onedrive.live.com/?authkey=%21AD9fcTZMZK17PFY&cid=4F92A222690CCFAC&id=4F92A222690CCFAC%21234346&parId=4F92A222690CCFAC%21220745&action=locate>

--------------------------------------

😎🙃

--------------------------------------

Controlar pc

<https://www.teamviewer.com/es/index.asp>

--------------------------------------

😱😔😱😔🥵😱😔🥳🥳

--------------------------------------

Tu identidad nunca será anónima

<https://anonfiles.com/1cf2Y6n4yb/Doxing_Tu_identidad_jamas_sera_anonima_2_pdf>

--------------------------------------

���⃟⃤

--------------------------------------

Programa para ganar todos los sorteos

<http://www.mediafire.com/file/hgd2nuvsxyyy6ou/SorteoPremiadov1.rar/>

--------------------------------------

😨😡😨😡🤨😡🤨🤨😡🤨😡

--------------------------------------

Apps para seguidores (que recomiendo yo para seguidores de instagram)

Hiketop

Topfollow

-darle muchas veces al botón para canjear seguidores y si el wifi va muy lento puedes hacer para pedir muchas veces seguidores y si el wifi va lento las monedas no se te quitan y aprovechas para pedirlo muchas veces y se te canjean todos los seguidores que pediste aunque las monedas que tuviese no fueran suficientes para canjear 1k de seguidores osea que si tenias 80 monedas que son 10 seguidores y el wifi te va muy lento puedes pedir muchos 10 10 10 seguidos y cuando los seguidores que pediste los procese el wifi aunque sólo reciba 1 el wifi en verdad esta recibiendo todos los que pediste y lo digo así para que se entienda pero en verdad así lo llaman los profesionales que mientras el servidor no procese la solicitud pedida no la procesa y puedes aprovechar esa vulnerabilidad para canjear más seguidores de los devidos

-formas de hacer que te vaya lento el wifi -con una vpn yo recomiendo usar windscribe se encuentra en la app store y play store y ponemos la vpn en el país más lejano a España que sería Suiza o alguno de esos sitios aunque para poder conectarnos a Suiza o esos sitios se requiere Premium pero da igual el país donde nos pongamos que la velocidad no cambiará tan exageradamente así que podéis poneros en Estados Unidos mismo no importa mucho -la otra forma es que nos alejamos del wifi para que nos vaya aún más lento -y si desconectamos el wifi y lo conectamos de nuevo eso haría que el wifi vaya más lento durante unos segundos (y pues solo tendrías que conbinar todas las formas que eh dicho para poder canjear muchos seguidores) pd: con auto clicker sería más eficaz osea con el auto clicker le damos para que habrá el menú de canjear los seguidores y luego cambiamos para que en vez de abrirlo los canje y conbinado todo lo que dije antes recibiríamos canjeando solo 10 seguidores haciendo el truco podríamos conseguir como 300 seguidores o menos mi recomendacion es que guardeis para canjear 1k de seguidores y hagáis el truco y la app de auto clicker esta en play store y en app store

Followerpars

--------------------------------------

😡🥶😡🥶🥶😡😡🥶

--------------------------------------

Formas de hackear cuentas (vale para todas las redes sociales)

-primera forma (fuerza bruta la fuerza bruta es una herramienta que esta automatizada para buscar contraseñas más posibles que puede tener una cuenta y para hacer que eso funciona hace falta un diccionario existen los públicos que son las contraseñas como 1234 o 4321 o incluso password y luego el privado son como el nombre de su perro su dirección nombre etc y actualmente en instagram no funciona pero hay otras maneras que funcionan para instagram que ahora comentaré

-segundo forma phishing es un enlace que envías a la víctima para que ponga sus datos y hackear le la cuenta y existen cosas para que la gente no se de cuenta que es para sacarles los datos como por ejemplo maskphish que es un enmascarador para por ejemplo si el enlace de phishing es localhost o ngrok y algunos número y con maskphish puedes poner un enlace como Instagram.com/24533/hacking/

-tercera forma ingeniería social la ingeniería social entra todo lo que dije antes y otros métodos

-cuarta forma con hxwhatsap puedes hacer bypass al número aunque estaría mejor dicho que hace un otp al número para sacar el Código de verificación del número y con eso poder pedir cambio de contraseña en instagram mediante número y si no tenemos el número de la víctima usamos osintgram que saca el número correo y ubicación de una fotografía analizando los metadatos de una publicación de la persona o si no nos funciona osintgram podemos intentar averiguar el número con un programa que pruebe números aleatorios y con un programa que mira si un número de teléfono tiene instagram o algunas otras redes sociales o con anycall podemos llamar con su mismo número y así poder escuchar su buzón de voz aunque instagram no deja buzones de voz para evitar hackeos pero whatsap si los deja pero con whatsap no se puede hacer nada pero con signal app de mensajería privada podemos vincular el número y todos los SMS llegan a la app

-quinta forma haciendo ADB al móvil que es poner la dirección mac de la víctima y luego tenemos acceso total al movil

-sexta forma usando grabbers que actuaría como si fuera un spyware nos daría los datos que le ordenamos al virus espía que nos de y nos los enviaría y puede ser usando python osea que se descargue python y después nuestro archivo para hackear le y sacarle los datos

-séptima forma keylogger - registrador de teclas sirve para que cuando la víctima este escribiendo algún texto nos llegue a nosotros lo que esta escribiendo y podremos hackear le la cuenta si introduce su contraseña

-octava forma man in the middle En criptografía, un ataque de intermediario​ es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad.​ El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas y procurar que ninguna de las víctimas conozca que el enlace entre ellos ha sido violado

-novena Vulnerabilidades en las plataformas

-décima Filtraciones por almacenar las claves

-once Claves genéricas

-doce autentificacion de escucha

-trece Proxy inverso En redes de computadoras, un proxy inverso es un tipo de servidor proxy que recupera recursos en nombre de un cliente desde uno uno o más servidores. Estos recursos se devuelven al cliente

-catorce relleno de credenciales El relleno de credenciales o la reutilización de credenciales robadas es un tipo de ataque cibernético en el que las credenciales de cuentas robadas

-quince pulverización de contraseñas es una variante de lo que se conoce como ataque de fuerza bruta. En un ataque tradicional de fuerza bruta, el perpetrador intenta obtener acceso no autorizado.

-dieciséis extracción de jugo es un tipo de ciberataque que involucra un puerto de carga que se duplica como una conexión de datos, normalmente a través de USB. A menudo implica la instalación de malware o la copia subrepticia de datos sensibles de un teléfono inteligente.

--------------------------------------

🤨😡🤨😡🤨😔😡🤨🥶

--------------------------------------

Como eliminar a una cuenta que no tenemos acceso

Contacta con la plataforma y diles que quieres borrarla y enseñas que es tuya y que tu la quieres borrar o puedes usar un auto report Bot de Instagram que un es un bot que reporta automáticamente la cuenta que elegiste que reporte hasta que borren la cuenta o puedes meter muchos seguidores muy rápido a esa cuenta para que a lo mejor la consiga banear Instagram o haciendo by-pass a tu cuenta y sacas el codigo para entrar a la cuenta si tenías el número vinculado a la cuenta.

--------------------------------------

❤😐😐❤❤😐😐❤😐❤

--------------------------------------

Como recuperar una cuenta de cualquier plataforma

haciendo otp para entrar a la cuenta bien sea de Google o de cualquier otro sitio haciendo fuerza bruta para sacar la contraseña contactando con Google y dando pruebas de que es tu cuenta para que te puedan ayudar o si es de Facebook podéis entrar aquí <https://facebook.com/hacked>.

--------------------------------------

💖😂💖😂😂💖💖😐💖😐😐💖💖😐

--------------------------------------

hackear móviles

-Primero ADB

-segundo evil twin crear una red falsa para tener acceso al dispositivo móvil

-tercero infect es un programa para infectar una app y poder tener acceso

-cuarto página web falsa crear una página web falsa y que acepte las cookies y poder tener acceso a su navegador y desde su navegador buscar cual es mi ip y pwnear su ip para obtener el máximo de datos o hacer osint

--------------------------------------

🥵😐🥵💖🥵💖🥵💖🥵💖🥵💖

--------------------------------------

hackear la Cámara de un dispositivo inteligente

Con shodan puedes buscar la ip de cualquier Cámara de vigilancia vía ip o de un dispositivo inteligente para poder tener acceso al mismo

--------------------------------------

⃟⃤�⃟⃤�⃟⃤��⃟⃤⃟⃤�⃟⃤�⃟⃤�⃟⃤�⃟⃤�⃟⃤⃟⃤

--------------------------------------

Crear ransomwares phishing etc

<https://mega.nz/folder/Cn42ECIC#k0DXI-YGKa6mhStQocoI3g>

--------------------------------------

😡😡🥳🥳😱..,,234🥳🥳😡

--------------------------------------

Curso hacking

<https://mega.nz/folder/4WQWFQjI#x-acNEHXeCWXwORCrZXBzg/folder/sO40jSJb>

--------------------------------------

👍😡🥳😡🥳😡🥵😔😔👍

--------------------------------------

Curso crackeo (dividido en 7 partes)

<https://mega.nz/folder/dIkw2aYa#VPSXahuDOfoDUZ1zOlfrtw>

--------------------------------------

😈

--------------------------------------

Guía cracking

<https://anonfiles.com/u6K4S6leub/GuiaCracking_pdf>

--------------------------------------

😡😱😡😱😡😱🥳😱🥳

--------------------------------------

tener Spotify Premium para siempre

(PC): 1. Descargar Spotify de la página oficial, no de la Microsoft Store, si no puede no funcionaros.

<https://www.spotify.com/es/download/windows/>

2. Descargar el Script y ejecutarlo.

<https://raw.githack.com/Daksh777/SpotifyNoPremium/main/install.bat>

3. La primera vez que os lo instaléis cuando os va a preguntar si tenéis Spitecify CLI instalada, tenéis que darle a que no. (Había abajo pero fue borrada)

4. Ya está, ahora os podéis logear con vuestra cuenta y ya no saldrán anuncios de cabecera ni tampoco entre canciones.

5. Cada cierto tiempo (1-2 semanas) deja de tener efecto, tener a mano el archivo install para cuando os pase eso, solo tenéis que volver a ejecutarlo, pero cuando os pregunte esta vez si tenéis Spicetify CLI instalado le dais a si. Llevo tiempo usándolo, si tenéis algún fallo os puedo ayudar.

(Android): Para Android es más fácil, solo hay que instalar una apk, os logeáis, cerráis la app y volvéis a entrar, ya se os quitan los anuncios y podéis saltaros las canciones.

<https://www.mediafire.com/file/yi3pcno1tz7x8yv/Spotify-v8.6.80.1014-Mod.apk/file>

--------------------------------------

😔🥵😔🥵😔🥳😔🥳😔🥳

--------------------------------------

Pack Stream NerdOrDie

<https://drive.google.com/drive/folders/17bzr4NzhwZ5GMII8iGAibYsL8YS7aTkw>

<https://drive.google.com/drive/folders/1nq9xUHLcuG1PqPVR1_tK0JlsML-qaAgX>

--------------------------------------

😃😞😃😞😃🥥😃

--------------------------------------

Criptografía desde 0

- HASH.

- Intercambio de Claves a través de medios inseguros.

- Cifrado Simétrico y Cifrado Asimétrico.

- Cómo implementar en Python nuestro propio RSA.

- Cómo haríamos nuestro propio sistema Esteganográfico.

- Cómo funciona el Correo Seguro y la Firma Digital.

- Cómo choca la Computación Cuántica con la criptografía actual.

- Las soluciones para protegernos de los peligrosos qubits.

--------------------------------------

😐😈

--------------------------------------

Curso hacking radiofrecuencias

1: <https://onedrive.live.com/?authkey=%21AL8%2D92ZIoJ3pfjM&cid=4F92A222690CCFAC&id=4F92A222690CCFAC%21233802&parId=4F92A222690CCFAC%21220745&action=locate>

2: <https://www.mediafire.com/file/5x1izcb8lufb1fz/Hacking_de_Radiofrecuencia-s4vitar.zip/file>

--------------------------------------

?

--------------------------------------

Programas hackers con virus (entrar con máquina virtual y con vpn)

<https://mega.nz/folder/rY8EWQRa#MWV_HWGKi9v3ArXQEmeN2g>

--------------------------------------

🧐🧐🧐☻☺︎

--------------------------------------

Muchos cursos de hacking etc

<https://mega.nz/folder/cMl0RB7Y#2CrbHcor32lsSW6o1VevHA>

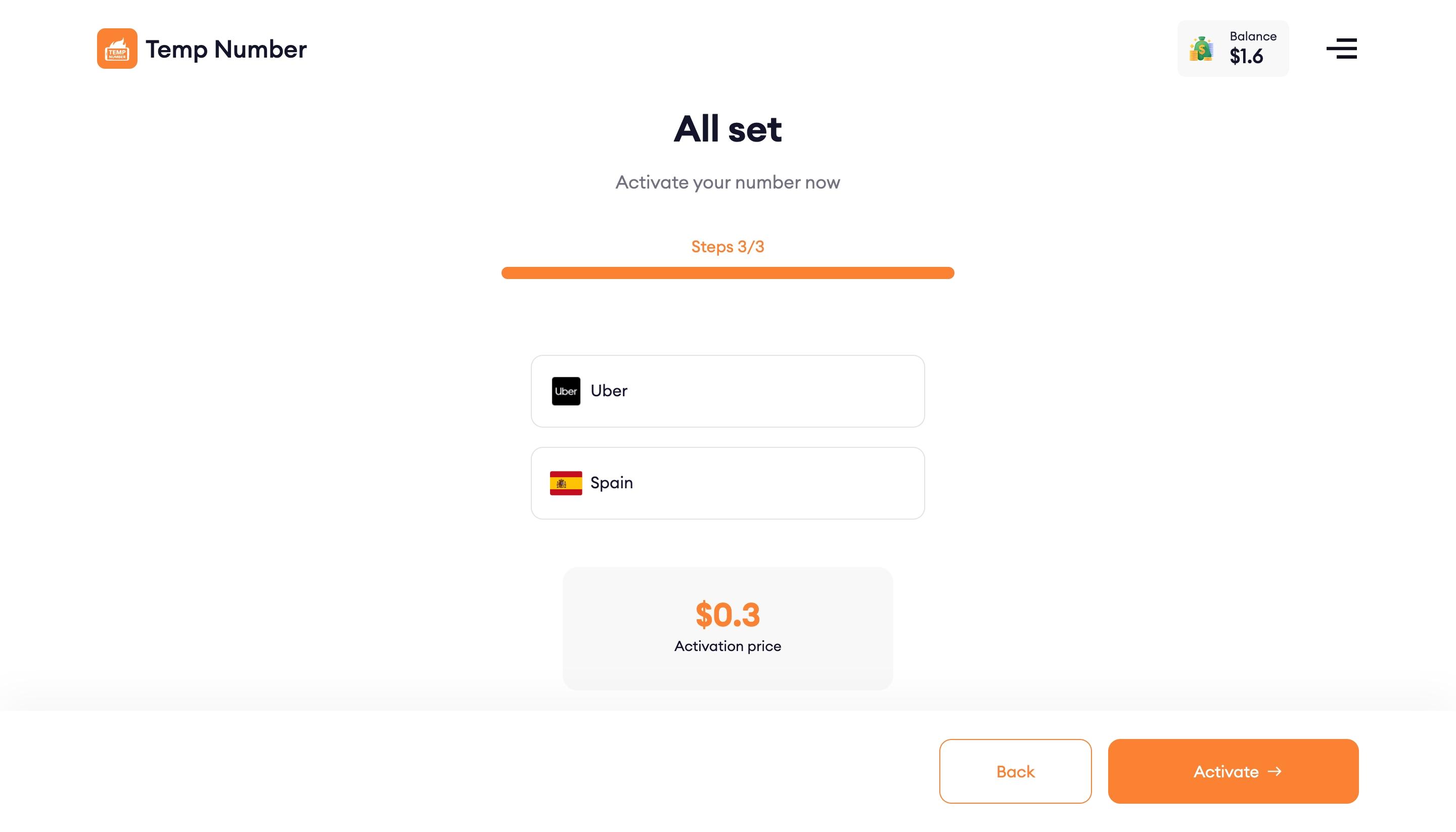
--------------------------------------

😈👑😡🤣👑👑👑

--------------------------------------

Uber eats ilimitado

1. Crear una cuenta en <https://temp-number.org/> y añadir 5€, es una web de fiar y que los números no estan saturados. (lo mínimo de ingreso son 5$)
2. Solicitar un numero temporal de españa y de uber como se ve en la foto (Cuesta 0,3$ cada mensaje)



3-Crear una cuenta de uber nueva con ese numero y esperar al sms de confirmación.

4-Se pueden poner datos ficticios en el email de uber.

5-Añadir nueva promocion en la cuenta de uber eats y poner el código “DISASTERCHEFSUBEREATS” (Si este no funcionase buscar en google otro codigo similar para nuevas cuentas)

6-A disfrutar la comida.

Para que no te baneen, usa VPN, máquinas virtuales y distintas direcciones (para cada cuenta)

BONUS:

Si no quieres pagar para recibir los mensajes puedes recibir 3 tarjetas sim gratis desde el siguiente link <https://www.lycamobile.es/es/>

Dando al botón verde, pedir sim gratis

--------------------------------------

█⃟⃤

--------------------------------------

Oscp examen completo para ser certificado

https://mega.nz/file/

E0lmCRzD#8S0uc28M1PUgE—s2GBJEWEUWncuFHBW8Ho5Hzo8kgc

Contraseña:https://learnhackingbynk.xyz/

--------------------------------------

⃟🤨📸⃟

--------------------------------------

Hacking Etico profesional

https://mega.nz/folder/gPhxBICB#kbkUHnBRQ\_eqG-q0BT03GA/folder/5fp3iS6C

--------------------------------------

😐😐

--------------------------------------

Libros sobre hacking juegos en phyton,malware y mas cosas

<https://mega.nz/fm/RsAAFaDL>

--------------------------------------

🤣😈🥵😈🥵😈🥵😈🥵

--------------------------------------

[EXCLUSIVO] Mailify (Mail-Access Checker) GRATIS! (VERSION ACTUALIZADA) []

DESCARGAR:

<https://mega.nz/file/WspyHKLa#RmYKWJ59YIjEGMBGOc1LmDQ3xc6xBKCDwPsfrLIqwfY>

--------------------------------------

🥵👍🥵👑🥵👑🥵👑🥵

--------------------------------------

Hola,

Encontré este método hace unos meses… Método de reembolso de la tarjeta de regalo.

Estoy ganando $ 500 a $ 1000 por día.

[IMPORTANTE]

# Este método aún funciona hoy 23/04/22. Pero no hay garantía de que funcionará por mucho tiempo.

# Cada vez que uses este método, borra tus cookies, historial de Chrome.

Link de descarga:

<https://mega.nz/folder/QItDgbCK#CP5zhnxNTCb-t46YuHumOA>

--------------------------------------

😡😡😈🤣🥶🥶😈😡

--------------------------------------

Gana +$150 al día | SIN ESFUERZO | Fácil [Noob-Friendly]

(No se que pasó con esto al parecer se borro solo eh probado a buscarlo otra vez pero parece que no lo encuentro)

--------------------------------------

🤣😞🤣😞🐦🤣🐦🐯🐦🐯🐯🐦

--------------------------------------

Sintetizar DrоGа (encriptado en base64

aHR0cHM6Ly9hbm9uZmlsZXMuY29tL0oxSThJM3ozdTQvb3BpdW1hbmRwb3BweWN1bHRpdnRpb24xX3BkZg==

AHR0cHM6Ly9hbm9uZmlsZXMuY29tL1AzSTRJYXo0dTQvaGVyb2lubWFudWZhY3R1cmVfcGRm

AHR0cHM6Ly9hbm9uZmlsZXMuY29tL044STZJYXphdTMvSGVyb2luX1N5bnRoZXNpc19VU0RfcGRm

aHR0cHM6Ly9hbm9uZmlsZXMuY29tL0xkSWFJYno2dWEvYnVsbGV0aW5fb25fbmFyY290aWNzXzIwMDdfWmVyZWxsX3BkZg==

aHR0cHM6Ly9hbm9uZmlsZXMuY29tL3BiTmFJYXpkdWEvc3ludGhlc2lzX29mX2NvbW1lcmNpYWxfZHJ1Z3NfMjAxMS0xMl8tX00yX0hhbm9pX3BkZg==

AHR0cHM6Ly9hbm9uZmlsZXMuY29tL25lTjJJOHo4dWMvZHJ1Z3Nlc3RpbWF0ZXNhbmRjaGFyYWN0ZXJpc3RpY3NfcGRm

aHR0cHM6Ly9hbm9uZmlsZXMuY29tL3YxTmRJZHo2dTAvYXJ0LW9mLWRydWdzLXN5bnRoZXNpc19wZGY=

--------------------------------------

👑🥵🤣🥵🤣🥵🤣🥵🤣

--------------------------------------

Hacking ético /////

<https://drive.google.com/drive/folders/1DstNA5jbzYnSeqPkevndlZmwg9IG4D4H>

--------------------------------------

🧐🧐😩😩🤑🤑

--------------------------------------

Biblia node.js

<https://mega.nz/folder/vahCmThZ#H1crIJoV1f_ZijREBEmmfA>

--------------------------------------

🕹🔑🐶🔑🐶❌🐶❌🐶

--------------------------------------

captura de paquete whatsap y otras plataformas

1. Ve a Google Play Store e instala una aplicación llamada Packet Capture.
2. Una vez instalada la aplicación ábrela y presiona el símbolo de play con un 1 y pon la aplicación Whatsapp.
3. Llame a la persona y cuando responda y luego cuelgue, y Packet Capture mostrará la IP de la persona

--------------------------------------

🥵🐶🥵🐶🥵❌🥵❌❌🥵

--------------------------------------

Proxy botnet

Instale PHProxy e instale un servidor web local con una herramienta como WAMP. Creo que entendiste esto, pero luego, por supuesto, necesitas reenviar un puerto, pero también puedes usar una herramienta como ngrok.io para hacer esto. Avíseme si asumo que está más lejos de lo que realmente está y lo explicaré con más profundidad.

--------------------------------------

Hackear snapchat (2022)

MÉTODO DE SNAPCHAT HACK UTILIZANDO LA PSICOLOGÍA HUMANA método de contraseña de snapchat el método funciona mejor en perras tontas usa este método sabiamente 1. Encuentre el objetivo y vaya a la página de inicio de sesión de Snapchat 2. Escriba su nombre de usuario en la sección superior 3. Empieza a adivinar la contraseña reuniendo información como... - cumpleaños – código postal – fecha de nacimiento – el segundo nombre funcionará su contraseña es más probable que sea corta y fácil de recordar, así que manténgala simple – prueba su nombre de usuario primero – pruebe su nombre con su año de nacimiento (por ejemplo, 2000/00) – pruebe su nombre con el día/mes de nacimiento (por ejemplo, 0101) – primer nombre con fecha de nacimiento completa (por ejemplo, 4406 = 02/06/2002) – pruebe el apellido con el año de nacimiento (por ejemplo, 2002) – prueba mayúsculas y @ - nombres de mascotas con cumpleaños / año Si tiene éxito, vaya solo a mis ojos e intente… - año de nacimiento o mes/día de nacimiento (por ejemplo, 2000 1/1/02) o prueba alguno de estos -2580 -1245 -1111 -1212 Los patrones generales también funcionan, pero la mayoría de las cuentas en las que he ingresado han sido muy básicas, ya que no esperan que nadie más esté en su cuenta. SI RECIBES MENSAJES DE ERROR O BLOQUEO DE IP PRUEBA ESTO – reiniciar snap – volver a la pantalla principal – apaga el wifi y prueba luego – cierre Snapchat, active el modo avión, luego vuelva a Snapchat y apáguelo – desinstalar y reinstalar Snapchat si no funciona \*\*\*\*\*\*\*\*\*SI ENTRA CON ÉXITO\*\*\*\*\*\*\*\*\*\*\*\* PRIMERO APAGAR SNAP MAPS ENTONCES VEA SI EL CORREO ELECTRÓNICO ESTÁ VERIFICADO SI NO CAMBIE LA CONTRASEÑA LO ANTES POSIBLE SI QUIERE NO ABRAS NINGUNA FOTOGRAFÍA NI TOMES FOTOS PARA QUE PUEDES MANTENERTE CLARO si no tengo éxito con mis ojos, solo busque sus chats guardados con su lista de mejores amigos y busque fotos / videos, información o secretos. \*\*\*\*\*\*\*\*\*\*\*\* AVISO \*\*\*\*\*\*\*\*\* INICIE SESIÓN TARDE EN LA NOCHE O CUANDO LA VÍCTIMA NO ESTÉ ACTIVA PARA QUE NO VUELVA A INICIAR SESIÓN O CAMBIE LA CONTRASEÑA

--------------------------------------

🥶😡😈😡👍🥶😡😡

--------------------------------------

GENERADOR DE TODO TIPO DE CUENTAS GRATIS [PYTHON]

https://mega.nz/file/OVVhwQRa#RcqGhQgJif4DRweAPvjFAw\_-1Vl4fnHDFTDWzMXQd0M

--------------------------------------

🤢⃢⃢⃢⃢☻

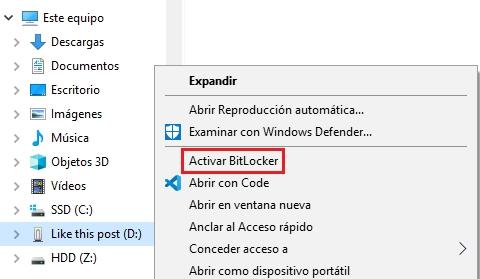
--------------------------------------

Poner contraseña usb

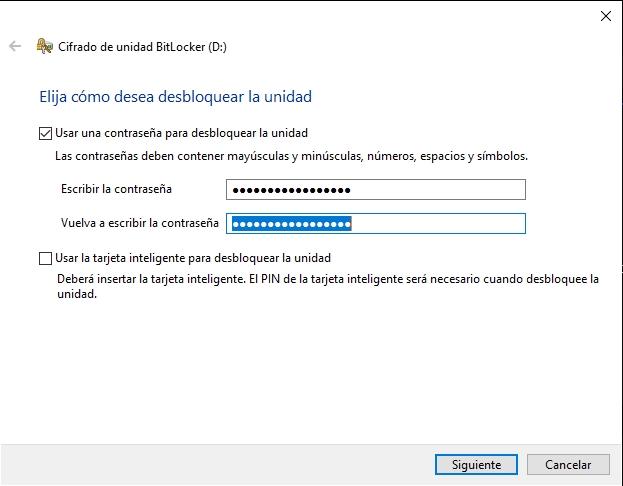
Como poner contraseña a un dispositivo USB de memoria:

Bien, deberemos tener BitLocker en el ordenador, todos los ordenadores con Windows ya tienen este programa por defecto, o eso tengo entendido, nunca he tenido problema en usarlo en cualquier versión de Windows.

Primero de todo, tenemos que conectar el dispositivo a nuestro ordenador.

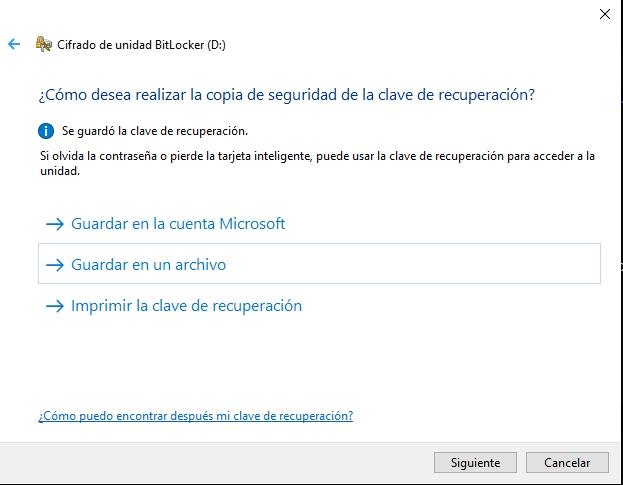
Después, tenemos que darle segundo click a ese dispositivo y elegimos la opción Activar BitLocker:

Una vez hecho esto, se abrirá una ventana donde pondremos la contraseña que queremos ponerle al dispositivo:

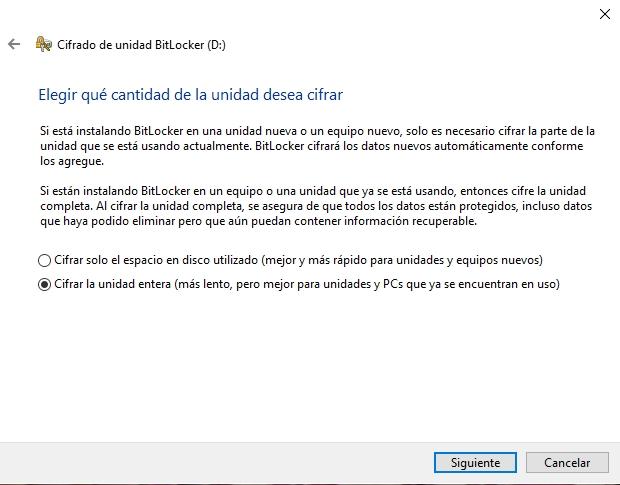


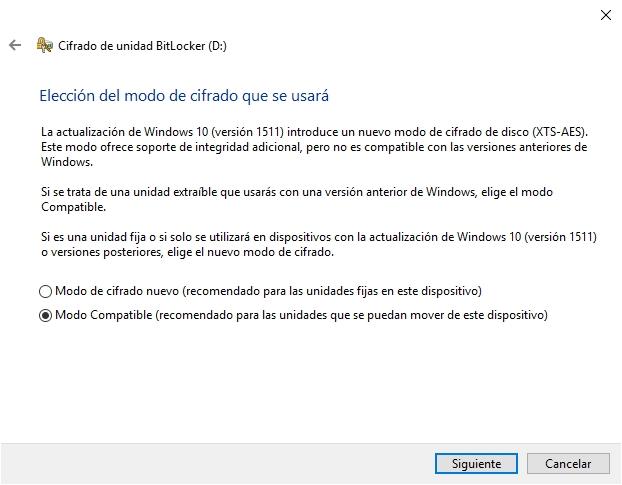
Una vez hecho esto, elegiremos donde guardar la copia de seguridad, yo prefiero en

Archivo, aunque nunca lo llego a usar:



Después, elegiremos que parte del dispositivo cifraremos, yo recomiendo cifrar el dispositivo entero:



Después elegiremos la forma de cifrado, yo suelo elegir la segunda:

Y ya estará todo listo, solo falta esperar a que se cifre el dispositivo:





--------------------------------------

🤨🤨🤨🤨

--------------------------------------

Cuentas Microsoft,minecraft etc

Página: https://web.h-gen.xyz/

Seleccionamos la que queramos, y le daremos a ''Generate'', en mi caso Origin .

Luego nos llevará a esta página donde tendremos que hacer dos cosas.

Daremos click en ''Discover interesting articles'' y nos esperaremos 13 segundos.

Luego daremos a la cruz y luego daremos a ''Watch a Video''. El vídeo suele ser de 1

minuto pero de mientras que el vídeo se reproduce podremos hacer otras cosas de mientras.

Una vez reproducido el minuto de video, le daremos a la cruz.

Una vez tengamos los ticks verdes le daremos a Continue.

Luego esperaremos 15 segundos.

Y le daremos a Go to Website .

Y ya nos daría una cuenta.

El formato es el siguiente : emailassword

Con esto lo que podremos hacer es vender las cuentas según los juegos que te toquen (en mi caso en Origin), o intercambiarlas.

En una cuenta me tocó Battlefield V, y más juegos...

--------------------------------------

₂₀ᷳ₂ᷫ₁ͨꦿ͜͡

--------------------------------------

Fraud bible 2019

<https://mega.nz/folder/hTBhnCqb#Qa9BuX9V0vZL71ljEu7RVg>

--------------------------------------

😡🤨❤

--------------------------------------

Generador de fichas de discordia

1: <https://www.mediafire.com/file/5elwt4jrs5pog5u/Discord-Token-Generator-v1.0.zip/file>

--------------------------------------

🤨

--------------------------------------

TikTok Shadow Bantool para Android

Mega.nz/file/TRUjFAya#G5NE021-vFKmouvmjQzHFDCts\_koEFtUmfNPjT2tWw8

--------------------------------------

🇩🇰🇩🇰🇩🇰🥵🥵😡😡

--------------------------------------

muchas recetas para hacer droga (lo encripto en base64 para que no me borren el word)

AHR0cHM6Ly9hbm9uZmlsZXMuY29tL1Jha2ZoYmEzeWMvRHJ1Z3NfcmFy

--------------------------------------

🤣🥵🤣🥵🥵🤣🤣🇩🇰

--------------------------------------

only fans gratis de muchas chicas (lo encripto por que no se si por esto me puedan borrar el word pd: encriptado en base64)

aHR0cHM6Ly9tYWdpY2ZhbnMubmV0bGlmeS5hcHAvd2hpdGVnaXJscy5odG1s

--------------------------------------

🟢😗🟢😗🟢😗🟢😗😗🟢

--------------------------------------

APK para Recargar Tarjeta del Bus con NFC

http://www.mediafire.com/file/8kpr3ku1k0yg80j/nfctuzsa.apk/file

--------------------------------------

🙃🤓🙃🤓🙃🤓🙃🤓

--------------------------------------

Apostilas

<https://mega.nz/folder/B0EmzKyB#68BJGAhiJ5-XrB2dm_6Kcg>

ciencia hacker

<https://mega.nz/folder/7wFiiLTJ#M62SaYcW2UbDPbEdGcpAJg>

Tutorial de denegación de servicio de video

<https://mega.nz/folder/6cZGDaIY#nJy545OxJkX3mix-nD2VEw>

Curso linux

<https://mega.nz/folder/SBEHVKJR#iVGhE5Ft8vcvzc94Wu5UrA/folder/TIlnTKjZ>

Curso Trampeando Celulares Android con Kali Linux

<https://mega.nz/folder/fmAnUYBI#IaJCj5U7_kwUV-U7X76FQw>

introducción

<https://mega.nz/folder/C34EDD5Q#xwcJ7BxIW_lIll83Ka-Sog/folder/O74EiL6b>

Hackeo de aplicaciones web – XPSecSecurity

<https://mega.nz/folder/W2Zh1KDT#cZDGwgnemVtAUowwXYpbcg>

Invasión de redes Wifi (Pentest) – EADCCNA

<https://mega.nz/folder/mqAGgLJA#neiV16YV5grXmili6OT-0A>

--------------------------------------

😡😡😡🤓😎😎

--------------------------------------

CARPETA 47 LIBROS DE HACKER <https://mega.nz/#F!RRRHmBiC!MXUgejPHX_cLOZqMp3gg4A>

LIBROS DE INFORMATICA <https://mega.nz/#F!JE4xAART!SKWfdYeYPdBySXEzSMmHdg>

CARPETA ACURRUCA, PARA DETECTAR VULNERABILIDADES WEB <https://mega.nz/#F!gABUDCRC!OLnaq7mSXYLwjLq-u9jzvg>

CARPETA ADM MICROSOFT WINDOWS SERVER 2 <https://mega.nz/#F!sdJHTRQK!gFJ0ToNj251Rk01vdKhryg>

CARPETA ALGEBRA BALDOR <https://mega.nz/#F!VcB0CDpB!B36aEAlmOXpypnLJ1H-ZOg>

CARPETA CURSO ANGULAR <https://mega.nz/#F!pd4AybyT!ZZTClzhN1GJfV49semwNuQ>

CARPETA ANONYMUS TOOLS <https://mega.nz/#F!wRBXFKRA!NHp2nHtmyga9p2pjn0y2BQ>

CARPETA BUSCANDO VULNERABILIDAD <https://mega.nz/#F!5VRQRIZa!S9UqtB2YNYz2tHuVGbivYg>

CARPETA CREACION DE EXPLOITS <https://mega.nz/#F!ZcgmGYLZ!rX3q_b7hrzNyG2kX7wjXuA>

CARPETA CURSO DE BATCHS <https://mega.nz/#F!cc50VYbR!OXE_P6qYhY7EPKaHygRpbA>

CARPETA CURSO DE PERL+MANUALES <https://mega.nz/#F!gJgzkbqR!f55hOXM8sR2aZIfPPMMswg>

CARPETA CURSO DE BOOTSTRAP 3 <https://mega.nz/#F!gEZEyK4b!xhqeDdOvBk1o5feEvtipqg>

CARPETA CURSO DE HT <https://mega.nz/#F!FZ4WHYIK!aut73QZhXlAlQxZUMht85g>

CARPETA CURSO DE HTML Y CSS <https://mega.nz/#F!4MRyxCgI!sD1SYCXRyA-YIqeK_5a8Xg>

CARPETA CURSO DE LINUX <https://mega.nz/#F!JAYFUCaa!bYf4uexnwAIC3StJie3ZBQ>

CARPETA CURSO DE NODE <https://mega.nz/#F!xUxkBZZZ!QOh4vOMuzXaE_CF0zE9Ukw>

CARPETA CURSO DE PYTHON <https://mega.nz/#F!sEInnRCK!m0UplIKhQ4gAmKw83Nps8Q>

CARPETA CURSO DE RESPONSIVE WEB DESING <https://mega.nz/#F!NZBlFYDZ!YUt4RlpTsSircIJ6vAmIFQ>

CARPETA CURSO DJANGO PROFESIONAL <https://mega.nz/#F!UdAm1boS!pU1FP0QPwY-LchGv5OJ5Qg>

CARPETA CURSO EH Y CEHv8 <https://mega.nz/#F!pNZnTT5K!kUrdcyqQALR2B_zKAkI8IQ>

CARPETA CURSO LENGUAJE JAVA SCRIP <https://mega.nz/#F!ZI5STRzD!HPtywhi29J_DjrJwBrNV7g>

CARPETA CV9 TOOLS <https://mega.nz/#F!IU4lgYRY!YEBY6aI-Lt6ktMfTpakzJQ>

CARPETA DVD HACKING MEXICO <https://mega.nz/#F!5YQVXZKZ!ClGnFFA2Cpd8Ni-pwXBNzA>

CARPETA EL ARTE DE LA INTRUICION <https://mega.nz/#F!sRJhlLAT!keORu4lBbHTYG-PSav5wAg>

7 libros de Python

<https://drive.google.com/drive/u/0/mobile/folders/1Uei0OSTgKg-7mv9uuP7ZmbD-aqKN2nve?usp=sharing>

CARPETA 47 LIBROS DE HACKER <https://mega.nz/#F!RRRHmBiC!MXUgejPHX_cLOZqMp3gg4A>

LIBROS DE INFORMATICA <https://mega.nz/#F!JE4xAART!SKWfdYeYPdBySXEzSMmHdg>

CARPETA ACURRUCA, PARA DETECTAR VULNERABILIDADES WEB <https://mega.nz/#F!gABUDCRC!OLnaq7mSXYLwjLq-u9jzvg>

CARPETA ADM MICROSOFT WINDOWS SERVER 2 <https://mega.nz/#F!sdJHTRQK!gFJ0ToNj251Rk01vdKhryg>

CARPETA ALGEBRA BALDOR <https://mega.nz/#F!VcB0CDpB!B36aEAlmOXpypnLJ1H-ZOg>

CARPETA CURSO ANGULAR <https://mega.nz/#F!pd4AybyT!ZZTClzhN1GJfV49semwNuQ>

CARPETA ANONYMUS TOOLS <https://mega.nz/#F!wRBXFKRA!NHp2nHtmyga9p2pjn0y2BQ>

CARPETA BUSCANDO VULNERABILIDAD <https://mega.nz/#F!5VRQRIZa!S9UqtB2YNYz2tHuVGbivYg>

CARPETA CREACION DE EXPLOITS <https://mega.nz/#F!ZcgmGYLZ!rX3q_b7hrzNyG2kX7wjXuA>

CARPETA CURSO DE BATCHS <https://mega.nz/#F!cc50VYbR!OXE_P6qYhY7EPKaHygRpbA>

CARPETA CURSO DE PERL+MANUALES <https://mega.nz/#F!gJgzkbqR!f55hOXM8sR2aZIfPPMMswg>

CARPETA CURSO DE BOOTSTRAP 3 <https://mega.nz/#F!gEZEyK4b!xhqeDdOvBk1o5feEvtipqg>

CARPETA CURSO DE HT <https://mega.nz/#F!FZ4WHYIK!aut73QZhXlAlQxZUMht85g>

CARPETA CURSO DE HTML Y CSS <https://mega.nz/#F!4MRyxCgI!sD1SYCXRyA-YIqeK_5a8Xg>

CARPETA CURSO DE LINUX <https://mega.nz/#F!JAYFUCaa!bYf4uexnwAIC3StJie3ZBQ>

CARPETA CURSO DE NODE <https://mega.nz/#F!xUxkBZZZ!QOh4vOMuzXaE_CF0zE9Ukw>

CARPETA CURSO DE PYTHON <https://mega.nz/#F!sEInnRCK!m0UplIKhQ4gAmKw83Nps8Q>

CARPETA CURSO DE RESPONSIVE WEB DESING <https://mega.nz/#F!NZBlFYDZ!YUt4RlpTsSircIJ6vAmIFQ>

CARPETA CURSO DJANGO PROFESIONAL <https://mega.nz/#F!UdAm1boS!pU1FP0QPwY-LchGv5OJ5Qg>

CARPETA CURSO EH Y CEHv8 <https://mega.nz/#F!pNZnTT5K!kUrdcyqQALR2B_zKAkI8IQ>

CARPETA CURSO LENGUAJE JAVA SCRIP <https://mega.nz/#F!ZI5STRzD!HPtywhi29J_DjrJwBrNV7g>

CARPETA CV9 TOOLS <https://mega.nz/#F!IU4lgYRY!YEBY6aI-Lt6ktMfTpakzJQ>

CARPETA DVD HACKING MEXICO <https://mega.nz/#F!5YQVXZKZ!ClGnFFA2Cpd8Ni-pwXBNzA>

--------------------------------------

⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟

--------------------------------------

Controlar movil mediante ordenador (TCP-IP)

Comandos para hacerla la ejecución del

programa

Instalar ADB

ADB conect (ip del movil de la víctima +puerto 9999 o puerto 8080 dependiendo si lo vamos a hacer por TCP O IP)

Y nos saldría una pantalla para controlar el movil

O con ADBtoolkit o con otro de ADB que haya en el word

--------------------------------------

🤨😔🤨😔😔🤨🤨😔

--------------------------------------

Página de +18 y -18 y hacking (no recomiendo entra hay contenido ilegal tanto en donde hacking como donde adultos pd:esta encriptado en base64 hay que descodificarlo para ver el enlace por que si pongo el enlace en si me borran el word)

IGh0dHA6Ly9vbmlvZHR1Nnh1ZGtpYmxjaWpyd3drZHV1MnRkbGUzcmF2N25sc3pyamhyeHBqdGtnNGJybWdxZC5vbmlvbg==

--------------------------------------

🤢😂🥵⃤⃤⃢⃢⃢⃢⃢⃢⃢☺︎⃠⃠⃠⃠⃠⃠⃠⃠⃠⃠⃠⃠⃠⃠⃠⃠⃠⃠⃟⃟⃢⃠⃠⃠⃢⃠⃢⃠☺︎⃠⃢⃠☺︎⃠⃢

--------------------------------------

Generador checker de tarjetas de regalo de muchas plataformas

<https://anonfiles.com/587ejb53xb/GF_CHECKER_1.4.0_rar>

--------------------------------------

🥵🥳🥳😔😔🥳😔🥳😔🥳

--------------------------------------

Mayor anonimato en Internet (si no está todo hay en el word tendré algo más para estar en máximo anonimato como DNS cifrada VPN otra Mac etc)

<https://anonfiles.com/f000Neley4/Guia_Anonimato_docx>

--------------------------------------

🥳🥵🤨🥵🤨😔🤨😔🤣

--------------------------------------

20 GB de DNI´s, PASAPORTES Y DOCUMENTACIÓN ROBADA

<https://mega.nz/folder/Qf4xgazb#XD2jfi79uqvHoRPAStWwng>

--------------------------------------

🥳🤨🥳🤨🥳🤨🥳

--------------------------------------

570GB DE CURSOS

<https://mega.nz/folder/cMl0RB7Y#2CrbHcor32lsSW6o1VevHA>

--------------------------------------

😎😡😡😎😎😎😎

--------------------------------------

\*\* 📘💎 SÚPER MEGA PACK DE LIBROS DE HACKING 💎📘\*\*

|| ■□■□■□■□■□■□■□■□■□

SUPER MEGA PACK LIBROS DE HACKING

Metasploid Unelashed en español.

<https://drive.google.com/open?id=0B6f2iRL-wf3Mbmc2ckl6X2ZVbTA>

■□■□■□■□■□■□■□■□■□

Kali Linux español.

<https://drive.google.com/open?id=0B6f2iRL-wf3MZVdwbDNoUm9BSTA>

■□■□■□■□■□■□■□■□■□

Introduccion al Hacking Español.

<https://drive.google.com/open?id=0B6f2iRL-wf3MTEYzRC16dWhFZEE>

■□■□■□■□■□■□■□■□■□

Haking Etico Español,

<https://drive.google.com/open?id=0B6f2iRL-wf3MMzVBa0dlX3ZPUVU>

■□■□■□■□■□■□■□■□■□

Generando Scrips Maliciosos con Metasploid.

<https://drive.google.com/open?id=0B6f2iRL-wf3MMHRWZmZLYnBPLXc>

■□■□■□■□■□■□■□■□■□

Explotacion con Metasploid.

<https://drive.google.com/open?id=0B6f2iRL-wf3MZEdXSl8zVE5HVEU>

■□■□■□■□■□■□■□■□■□

El Arte del Engaño Español.

<https://drive.google.com/open?id=0B6f2iRL-wf3Mblo1djBNT1lqUjQ>

■□■□■□■□■□■□■□■□■□

<https://drive.google.com/open?id=0B6f2iRL-wf3MR25CLUdOYWdtb1E>

■□■□■□■□■□■□■□■□■□

Curso Metasploid.

<https://drive.google.com/open?id=0B6f2iRL-wf3MaXdHRk1HUXFYWW8>

■□■□■□■□■□■□■□■□■□

Backtrack 5 Wireless Pentesting (kali linux)

<https://drive.google.com/open?id=0B6f2iRL-wf3MQkg1MGlJcmNteXM>

■□■□■□■□■□■□■□■□■□

XSS.

<https://drive.google.com/open?id=0B6f2iRL-wf3MYk83d2hjN19iV3c>

■□■□■□■□■□■□■□■□■□

XSS Tunneling.

<https://drive.google.com/open?id=0B6f2iRL-wf3MQzFVRUFsUmRON3M>

■□■□■□■□■□■□■□■□■□

XSS Javascript.

<https://drive.google.com/open?id=0B6f2iRL-wf3MMzZEemxtdDVaSUE>

■□■□■□■□■□■□■□■□■□

XSS a fondo.

<https://drive.google.com/open?id=0B6f2iRL-wf3MU0tiYkpaaS1HczA>

■□■□■□■□■□■□■□■□■□

RRA Facebook.

<https://drive.google.com/open?id=0B6f2iRL-wf3MSGxOZDQxMmxiY2s>

■□■□■□■□■□■□■□■□■□

Nessus.

<https://drive.google.com/open?id=0B6f2iRL-wf3MTUNOVmZnR0s0QXM>

■□■□■□■□■□■□■□■□■□

Manual Basico Metasploid.

<https://drive.google.com/open?id=0B6f2iRL-wf3MNy1GS0VmZi1qN2s>

■□■□■□■□■□■□■□■□■□

Hackers Los piratas del Chip y del Internet.

<https://drive.google.com/open?id=0B6f2iRL-wf3MaHp5ZXVORUNTOVU>

■□■□■□■□■□■□■□■□■□

Backtrack 5 Manual español (kali linux).

<https://drive.google.com/open?id=0B6f2iRL-wf3MR21aWkhtVVF3b1k>

■□■□■□■□■□■□■□■□■□

Internet, Hackers y Software Libre.

<https://drive.google.com/open?id=0B6f2iRL-wf3McTc0cUJ3WmN3bk0>

■□■□■□■□■□■□■□■□■□

Hackers Secrets Revealed Ingles.

<https://drive.google.com/open?id=0B6f2iRL-wf3MdlVPYVIzejZNUG8>

■□■□■□■□■□■□■□■□■□

Los clanes de la Red 2000.

<https://drive.google.com/open?id=0B6f2iRL-wf3MZFo0WmNGZGdjclE>

■□■□■□■□■□■□■□■□■□

Guia de Iniciacion al Hacking.

<https://drive.google.com/open?id=0B6f2iRL-wf3MNVowNGV0UzV0cEk>

■□■□■□■□■□■□■□■□■□

Escaneo a Sistemas con Backtrack 5 (kali linux)

<https://drive.google.com/open?id=0B6f2iRL-wf3MckhmcFB3TjRkU3M>

■□■□■□■□■□■□■□■□■□

Deface a PHP.

<https://drive.google.com/open?id=0B6f2iRL-wf3MZVpfMUZ5NW9pMEE>

■□■□■□■□■□■□■□■□■□

Como conocer a las personas por su lenguaje corporal.

<https://drive.google.com/open?id=0B6f2iRL-wf3MaXVtNFp4NVFKVzQ>

■□■□■□■□■□■□■□■□■□

Ataques a aplicaciones Web.

<https://drive.google.com/open?id=0B6f2iRL-wf3MMmJQQmRrZU80MFE>

■□■□■□■□■□■□■□■□■□

(Tutorial) Hacking Etico Avanzado:

<https://mega.nz/#F!pmQjSQTJ!_98x8K3Q4w9rqf1LGMlKYQ>

■□■□■□■□■□■□■□■□■□

Libros de pragramacion:

<https://mega.nz/#F!k3xlEQCT!nYaypRwx1wCL0nQE49FFEw>

■□■□■□■□■□■□■□■□■□

Matemáticas(pdf):

<https://mega.nz/#F!Yy5ESQZD!np-Rb3MEbN5lFhj5duSsUg>

■□■□■□■□■□■□■□■□■□

Ud3my :

<https://mega.nz/#F!lOwVjKxC!TC2syGqAoLnpSBbfPWkv_A>

■□■□■□■□■□■□■□■□■□

Curso de Angular 2 en Español – Crea webapps desde cero

<https://mega.nz/#F!9DozlJAa!T4RMsvQu8Oy0NCZe20uQLA>

||

--------------------------------------

ඩා𖨆꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰

--------------------------------------

Inyección SQL

<https://mega.nz/folder/oM1wjS4R#mn0Es8Qin63lk7ij_sa9ig>

--------------------------------------

🥳😂🥳👍🥳👍🥳👍😡

--------------------------------------

Gana dinero por chatear

<https://www.todatefree.com/fission-share-hurrah/index.html?code=634BAZ>

--------------------------------------

🤨😂🤨😂😂🤨😐😐🥵😐🥵😐

--------------------------------------

Cursos unity

Crear videojuegos

<https://ns2.elhacker.net/descargas/Videos/Tutorial%20completo%20de%20Unity%202020%20%20-%20Aprende%20a%20crear%20videojuegos%20desde%20cero.mp4>

Dominar el mundo de los videojuegos

<https://ns2.elhacker.net/descargas/Cursos/Curso.completo.de.Unity.2020.domina.el.mundo.de.videojuegos/>

Desarrollo de videojuegos

<https://ns2.elhacker.net/descargas/Cursos/Udemy%20-%20La%20gu%c3%ada%20definitiva%20del%20desarrollo%20de%20videojuegos%20con%20Unity/>

43gb de cursos unity

<https://ns2.elhacker.net/descargas/Cursos/Curso%20de%20Unity/>

--------------------------------------

█

--------------------------------------

Otros cursos

"Más Cursos en Español - Cupones

Autodesk Revit Arquitectura 2019: Curso Definitivo

Más Cursos en Inglés - Cupones

(2021) Economic Analysis of “Sales”

Adobe Illustrator CC 2020 MasterClass

CPU Mining Tutorial | Mine Crypto on Free VPS | XMR SUGAR

Certification in Renko Chart Trading & Taj Mahal Strategy

Complete Course in Adobe Photoshop CC

Computer Network Fundamentals- IT Helpdesk & Desktop Support

Crisis Management

Data Augmentation in NLP

Diversity At Workplace

Emotional Intelligence 2 - Confidence and Career Mastery

Lifting yourself out of negativity...

Master Trigonometry and Calculus in MATLAB

RoboAuthor: Content Writing Automation 2021 - Part 1

Scriptwriting for short films: 16 hours; 16 screenplays!

Unleash Your Motivation & Boost Your

Energy - 30' Guide

Más Cursos en Español - Sin Cupones

Análisis de Ciclo de VidaI

Curso Gratuito Procreate: Como Pintar el Rostro Humano

Curso Python Las Bases para Aprender

Curso de Python - Introducción desde cero y primeros pasos

Edición de video con Adobe Premiere Pro

Fundamentos de Excel

Inteligencia Emocional. "El secreto del bienestar"

Introducción al Servicio al Cliente

Introducción Gratuita a Python Data Science

Lo básico de Python

Los 7 Hábitos Gerenciales de Creativos Exitosos.

Master en Machine Learning - Aprende R y Python desde cero

Master en Python 3.x. Aprende de 0 a

EXPERTO con Práctica.

Metodología de la Investigación y Proyectos

UX Design: Conceptos básicos para principiantes"

https://www.nodo313.net/post/cursos-gratis-de-python-procreate-adobe-autodesk-y-otros-udemy-espanol-ingles.49316/#:~:text=M%C3%A1s%20Cursos%20en,b%C3%A1sicos%20para%20principiantes

--------------------------------------

🤨📸⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤⃟⃤��⃟⃤�?⃟⃤��?��

--------------------------------------

Herramientas para usar en la dark web

The Hidden Wiki

Navegador TOR

Tor3web - Buscador red TOR

Torchtorsearch.com - Buscador red TOR

Ahmia.fi - Buscador red TOR

IACA - Buscador red tor

--------------------------------------

🤣🤣🤣🤣🤣🤣😡

---------------------------------------

proteccion

Protomail - Email seguro

Simitator - Generador de perfiles y mensajes Fake

Yopmail - Cuentas de Email temporales

Email Temporal gratis

Whonix - Sistema operativo navegación anónima

Emkei - Suplantar el email de otra persona

Gigatribe - Comparte archivos grandes encriptados

Generador de conversaciones de WhatsApp

Emails y SMS anónimos

Eff.org - Guías de privacidad y seguridad

Navegador TOR

Mailinator - Cuentas de Email temporales

Tutanota - Email anónimo

Tutoriales configurar privacidad RRSS

Cifrar emails

Mohmal - Email temporal gratis

Generador de Tarjetas de crédito

10minutemail - Cuentas de email temporales

Tails - Sistema operativo navegación anónima

Tunnelbear - VPN gratuito?

--------------------------------------

🤨📸🤨📸🤨📸🤨📸🤨📸🤨📸🤨📸🤨📸

--------------------------------------

Dnis/CIF

Boletines oficiales municipales

BORME - Anuncios de registro mercantil

Boletines oficiales autonómicos

Boletines oficiales provinciales

TESTRA - buscador de sanciones de tráfico

BOE - Tablón de anuncios (multas, embargos)

BOE - Buscar en todo el boletín

--------------------------------------

⃟⃤⃟⃤�����������������.

--------------------------------------

"Emails 1.0

Comprobar si existe en gmail

Metricsparrow.com - Generador de supuestos emails

Comprobar si existe en Twitter

Ashley.cynic.al - Buscador datos comprometidos

Domainbigdata - Búsqueda inversa

Comprobar si existe en Yahoo

Comprobar si existe en Facebook

Toolbox Google - Analizador de cabeceras

Verifyemailaddress.org - Verificar email

Comprobar si existe en Myspace

Comprobar si existe en Ebay

Whoreadme - Conseguir IP y mas datos

Dehashed - Buscador datos comprometidos

EO-Ripper - OSINT a cuentas de email

Infobyip.com - Verificar email

Haveibeenpwned.com - Buscador datos comprometidos

Inteltechniques - Generador de supuestos Emails y los busca

Muestra la cuenta de LinkedIn de un eMail

Ghostproject - Buscador datos comprometidos

SpyCloud - Buscador datos comprometidos"

https://www.nodo313.net/post/mega-hilo-herramientas-open-source-intelligence-osint.13922/#:~:text=Emails%201.0,SpyCloud%20%2D%20Buscador%20datos%20comprometidos

--------------------------------------

....................................................................................

--------------------------------------

Curso CEH y programas

<https://mega.nz/folder/9gEiERhD#YRWn21BpekOVN4ir3T-vTQ>

--------------------------------------

,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

--------------------------------------

Extensiones

OsintBrowser - Repositorio de tools OSINT

FireShot - Capturador de pantalla completa

Herramientas para Facebook

Búsqueda inversa de imágenes

Verificador de vídeos e imágenes

AFS - Búsquedas avanzadas de Facebook

Traductor de Google

360social - Información adicional de contactos en RRSS

Descargar contenido de Instragram

Cual es el hosting de una web

Información de Dominios e IPs

Tunnelbear - VPN para el navegador

Borrar historial navegador

Save a Pocket - Guarda urls en la nube

Lastpass - Gestor de contraseñas

TinEye - Búsqueda inversa de imágenes

Descargar vídeos y fotos de Instagram

Información sobre plugins de página Web

Resalta los resultados de Google

--------------------------------------

Lol OMG

--------------------------------------

Privacidad 1.0

Protomail - Email seguro

Simitator - Generador de perfiles y mensajes Fake

Yopmail - Cuentas de Email temporales

Email Temporal gratis

Whonix - Sistema operativo navegación anónima

Emkei - Suplantar el email de otra persona

Gigatribe - Comparte archivos grandes encriptados

Generador de conversaciones de WhatsApp

Emails y SMS anónimos

Eff.org - Guías de privacidad y seguridad

Navegador TOR

Mailinator - Cuentas de Email temporales

Tutanota - Email anónimo

Tutoriales configurar privacidad RRSS

Cifrar emails

Mohmal - Email temporal gratis

Generador de Tarjetas de crédito

10minutemail - Cuentas de email temporales

Tails - Sistema operativo navegación anónima

Tunnelbear - VPN gratuito

--------------------------------------

😅😄

--------------------------------------

Privacidad 1.1

Generador de identidades

Onionshare - Comparte archivos de forma anónima

https://github.com/Sanix-Darker/onionshare

Anonymousemail - Email sin registro

Servicios de Email Temporales y/o desechables

Sadd - Escritorio virtual temporal

Boomeranggmail - Programar envio de email

Receive-sms-online - Recibir SMS online

--------------------------------------

😨😨

--------------------------------------

Borrar Identidad

Eliminar Facebook

Eliminar Instagram

Desactivar Twitter

Deseat.me - Borrar cuentas de Internet

Eliminar cuenta de Pinterest

Eliminar actividad en Google

Eliminar cuenta de Google

Justdeleteme - Eliminar todas las cuentas de Internet

Eliminar cuenta de Linkedin

Accountkiller.com - Eliminar todas las cuentas de RRSS

OSI.es - Guía para borrar tu identidad digital

Mydatarequest - Descargar información personal de servicios online

Eliminar cuenta Microsoft

--------------------------------------

👍

--------------------------------------

Buscadores 1.0

Duckduckgo

Google

Searchenginecolossus.com - Buscadores por paises

Shodan

Buscador personalizado de Google para OSINT

Baidu

Pdffetch (Buscador de archivos PDF)

Buscador Forocoches

Yandex (RU)

Qwant

Google Correlate

Lycos

CSE - Buscar en varias RRSS a la vez

Instya.com - Busca en muchos buscadores

Zapmeta - Buscar en varios buscadores

Yippy - Resultados por categorías

Globograma - Listado de Buscadores

Etools - Metabuscador

Searx - Metabuscador

Millionshort - Filtra por resultados

profundos

--------------------------------------

**DataLeaks**

image1641918916974.png

 Ashley.cynic.al - Buscador de datos comprometidos

image1641918917045.png

 Haveibeenpwned.com - Buscador de datos comprometidos

image1641918917047.png

 Dehashed - Buscador de datos comprometidos

image1641918917048.png

 Ghostproject - Buscador de datos comprometidos

image1641918917062.png

 Weleakinfo - Buscador datos comprometidos

image1641918917064.png

 Avast - Buscador de datos comprometidos

image1641918917065.png

 SpyCloud - Buscador de datos comprometidos

image1641918917066.png

 Iintelx.io - Buscador datos comprometidos

image1641918917068.png

 Psbdmp - Buscador datos comprometidos

image1641918917076.png

 Leakedsource - Buscador datos comprometidos

--------------------------------------

🤣🤣

--------------------------------------

Emails 1.0

Comprobar si existe en gmail

Metricsparrow.com - Generador de supuestos emails

Comprobar si existe en Twitter

Ashley.cynic.al - Buscador datos comprometidos

Domainbigdata - Búsqueda inversa

Comprobar si existe en Yahoo

Comprobar si existe en Facebook

Toolbox Google - Analizador de cabeceras

Verifyemailaddress.org - Verificar email

Comprobar si existe en Myspace

Comprobar si existe en Ebay

Whoreadme - Conseguir IP y mas datos

Dehashed - Buscador datos comprometidos

EO-Ripper - OSINT a cuentas de email

Infobyip.com - Verificar email

Haveibeenpwned.com - Buscador datos comprometidos

Inteltechniques - Generador de supuestos Emails y los busca

Muestra la cuenta de LinkedIn de un eMail

Ghostproject - Buscador datos comprometidos

SpyCloud - Buscador datos comprometidos

--------------------------------------

🥵😄

--------------------------------------

Emails 1.1

Avast - Buscador datos comprometidos

Buscar en Google Groups

Buscar emails en varios servicios

Comprobar si existe en Apple

Iintelx.io - Buscador datos comprometidos

Comprobar si existe en Amazon

Psbdmp - Buscador datos comprometidos

Colección Inteltechniques.com

Comprueba si existe en Gravatar

Comprobar si existe en Linkedin

Whoismind - Búsqueda inversa

Inteltechniques.com - Búsqueda de emails en currículums

Iplogger - Conseguir IP por email

Hunter.io - Verificar email

Como ver las cabeceras de un email

--------------------------------------

😛😛

--------------------------------------

Geolocalizar

Averigua desde donde Twittea

GeoCreepy - App ubicar a través de las RRSS

Google Maps

Localizar mediante el envio de un email

Conseguir IP y ubicarla

Bing Mapas

Ubicar IP

Tinfoleak - Ubicación de Tweets

Wikimapia

Geolocalizar en base a perfil Twitter

Buscar fotos geolocalizadas

Seguimiento de pedidos

Señales de tráfico de todo el mundo

Ogimet - Qué tiempo hizo en una fecha

--------------------------------------

🥲🥲

--------------------------------------

Google Hacking

Herramienta para hacking con Google y Bing

Usuarios y contraseñas de una Web

Búsqueda de frase exacta

Omitir palabra o frase

Base de datos de Google Hacking

Subdominios y/o intranets de una web

Base de datos con usuario y contraseña

Directorios y subdirec. con archivos visibles

Logins en documentos .txt de una Web

Tlfs, emails, curriculums, calle, en una web

Formularios de acceso a paneles web

Acceso a carpeta con fotos subidas

Base de datos con usuario y contraseña II

Base de datos pública de una web

Archivo TXT con contraseñas

--------------------------------------

😔😔

--------------------------------------

Imágenes

Localiza fotos

Averiguar ID Flickr

Google Imágenes

Pictriev - Reconocimiento facial

Firstdraftnews - Verificación rápida de imágenes

Google - Buscar en Flickr por cámara de fotos

Plaghunter - Monitoriza imágenes en internet

Lector de código de barras

Exif.regex - Metadatos de una imagen

Impulseadventure - Analiza si la imagen es original (App)

Busca fotos por ubicación - Flickr

Twitter Imágenes

Diffchecker - Diferencia entre dos imágenes

Detectar logo en vídeo

--------------------------------------

☺☺

--------------------------------------

Imágenes 1.1

OCR - Reconocimiento OCR de texto

Letsenhance - Mejora la nitidez de una imagen

Photobucket

Flickr - Buscar fotos geolocalizadas

Google Fotos

FOCA - Análisis de metadatos de imagen (App)

Imgops - Tools en línea para investigar imágenes

Azure - Reconocimiento Facial. Compara 2 imágenes

Stolencamerafinder - Busca imágenes por nº serie cámara

Logos.iti - Colección de logos

Karmadecay - Imagen inversa en Reddit

Flickr - Plataforma de imágenes

Rootabout - Buscador de imágenes

Pic2map - Muestra en un mapa la ubicación

Picsearch - Buscador de imágenes

Imageidentify - Identifica contenido en imagen

Imageedited - Analiza si la imagen es original (Online)

29a - Análisis forense de una imagen

--------------------------------------

🤬

--------------------------------------

IPS

Ipdata.co - Información avanzada de IP

Ipinfo.io - Información sobre una IP

Tracemyip - Localizar IP

Grabify - Conseguir IP mediante enlaces

Iplogger - Conseguir IP mediante enlaces

Mapper.info - Conseguir IP mediante enlaces

Whoreadme - Conseguir IP enviando un email

Comprueba IP desde varias plataformas

Saber que Torrents se descarga una IP

Ip-tracker - Localizar IP

https://www.geolocation.com/ localizar ip

Colección Inteltechniques.com

Maxmind - Localiza ciudad e ISP

--------------------------------------

🥱🥱🤡

--------------------------------------

Productividad

Yoga - Flujo de trabajo OSINT

Crear checklist online

Office Online

Draw - Diagramas online

Mindomo - Mapas mentales

Casefile - Mapas mentales

Xmind - Mapas mentales y esquemas

WenBreacher - Flujo de trabajo OSINT

Trello - Gestor de tareas

--------------------------------------

🤡

--------------------------------------

Software

Reaper.social - Herramienta de raspado de Redes Sociales

Maltego - Obtención de información de personas y empresas

FOCA - Análisis de metadatos de archivos

Browser Fingerprinting - Genera huella digital del navegador

Osirtbrowser - Navegador OSINT

Fawproject.com - Navegador OSINT

Navegador Mantra - OSINT, Footprint, Fingerprint

Hunch.ly - Recolector de evidencias (De Pago)

Tinfoleak - Análisis de Twitter

Casefile - Mapas mentales

--------------------------------------

🥱🤡

--------------------------------------

Repositorios 1.2

Osint.link - Herramientas OSINT

Uk-osint.net - Herramientas OSINT

Osintframework.com - Herramientas OSINT

Researchclinic.net - Herramientas OSINT

Onstrat.com - Herramientas OSINT

Reuser.biz - Herramientas OSINT

--------------------------------------

☺🤡

--------------------------------------

Repositorios 1.1

Awesome - Herramienta OSINT

Periodismo.com - Herramientas para periodistas de investigación

Toddington.com - Herramientas OSINT

Start.me - Herramientas OSINT

Digitalmethods.net - Herramientas OSINT

Neuskool - Sencillo todo en uno

Osinttechniques.com - Herramientas OSINT

Andyblackassociates.co.uk - Herramientas OSINT

Inteltechniques.com - Herramientas OSINT

Start.me - Herramientas OSINT para verificación

Awesome OSINT - Herramientas OSINT

Atlas.mindmup - Herramientas OSINT

Tomokodiscovery - Herramientas OSINT

Herramientas y Apps sobre contactos y citas

Herramientas OSINT: Una recopilación de tools para obtener datos y convertirlos en ciberinteligencia"

Fuente:

https://derechodelared.com/herramientas-osint-recopilatorio/

🛠 Google Dorks https://www.exploit-

db.com/google-hacking-database https://www.sans.org/security-resources/GoogleCheatSheet.pdf

🛠 Bing Dorks

🛠 Shodan https://www.shodan.io/

🛠 Maltego https://www.maltego.com/

🛠 TheHarvester https://github.com/laramies/theHarvester

🛠 Recon-ng https://github.com/lanmaster53/recon-ng

🛠 Censys https://censys.io/

🛠 Crt.sh https://crt.sh/

🛠 Creepy https://www.geocreepy.com/

🛠 DnsDumpster https://dnsdumpster.com/

🛠 Spyse https://spyse.com/

🛠 Metagoofil https://github.com/laramies/metagoofil

🛠 FOCA https://github.com/ElevenPaths/FOCA

🛠 Ipinfo.io https://ipinfo.io/

🛠 WaybackMachine (archive.org) https://

archive.org/

🛠 Osintgram https://github.com/Datalux/Osintgram

🛠 Spiderfoot https://www.spiderfoot.net/

🛠 Google Imagenes (Búsqueda inversa)

🛠 Tinfoleak https://www.isecauditors.com/herramientas-tinfoleak

🛠 Wappalyzer https://www.wappalyzer.com/

🛠 OSINT Framework https://osintframework.com/

--------------------------------------

😝😍

--------------------------------------

Teléfonos

Opencnam - Idenficador de llamadas

Saber de que operadora es un teléfono

Sync - Buscador de números de teléfono

Colección Intelchniques.com

Truecaller - Buscador de teléfonos

Abcteléfonos - Buscador de teléfonos

Twilio - Validador de números de teléfono

Búsqueda personalizada en Google I

Búsqueda personalizada en Google II

Milanuncios

Whocalld - Idenficador de llamadas

Everyoneapi - Identificador de llamadas

--------------------------------------

😍🤡

--------------------------------------

Webs

Whois con información complementaria

Securitytrails - Subdominios y dominios misma DNS

Conversor de IP a Host y viceversa

Donde está alojada una web

Riskiq.com - Información muy completa de webs

Whois (icann.org)

Whoxy - Historial Whois y búsqueda inversa

Buscar subdominios

Similarsites.com - Webs similares

Plataforma, subdominios, links, IP

Texto plagiado

Mapa visual de una web

Domaineye - Whois inverso y relaciones con otros dominios

Site24x7 - Herramientas varias de análisis web

Whois, plugins e historial de DNS

Robtex - Información de un dominio o IP

Whoisology - Búsqueda inversa de Whois

Información SEO

Completo reporte de estadísticas e info de la web

--------------------------------------

😍😝🤡

--------------------------------------

Webcams

Webcams de tráfico en directo

Eltiempodeunvistazo - Tiempo y tráfico en directo

DGT - Cámaras de tráfico

--------------------------------------

😵😳

--------------------------------------

Vehículos

BOE - Tablón de anuncios

TESTRA - Buscador de sanciones de tráfico

DGT - Informes de vehículos

Vin-info - Información de un nº VIN

Aire - Registro de aeronaves civiles

Airfleets - Buscador de aeronaves y compañías

Seguridadaerea - Registro de matrícula de aeronaves

Seguridadaerea - PDF con listado de matrículas aeronaves

Aena - Información sobre vuelos

Flightaware - seguimiento de vuelos en vivo

Fomento - Capitanías y Distritos Marítimos

Exponav - Interpretación de matrículas barcos

Marinetraffic - Tráfico marítimo en vivo

Flightaware - Información sobre vuelos y aeronaves

--------------------------------------

📸

--------------------------------------

UAE pasaporte

https://mega.nz/file/sloDgSxA#YhaNpMQsfZ8baP\_RX1B6L\_94YbYfFFOEqog0eAOlh30

--------------------------------------

🥵

--------------------------------------

Crear troyano personalizado

https://mega.nz/file/

hB03VQzD#V1ioEdfS82hx91lrp5d4jXMoLZUhVT402cLMv\_rTSKQ

--------------------------------------

Recuperar cuentas de Facebook

<https://facebook.com/hacked>

--------------------------------------

🔵🐔💚🟡

--------------------------------------

Hacking tools

<https://m.apkpure.com/es/phone-hacker-tools-simulator/com.ergames.hackingsim>

--------------------------------------

🔵🟡🟣😳🥰🥰𖤐

--------------------------------------

Sniffing

<https://web.archive.org/web/20140725195333/http://bluesniff.shmoo.com/>

--------------------------------------

😳📸😳🖤😳🖤

--------------------------------------

TUTORIAL DE CÓMO EVITAR LA VERIFICACIÓN MÓVIL DE GMAIL 🔰

PASO 1

◾️Ir a K7.net Regístrese allí.

PASO 2

◾️Cree una cuenta en gmail, pero en la ubicación llene Estados Unidos.

PASO 3

◾️Después de crear su cuenta de correo electrónico, ahora lo llevará a la página de verificación móvil.

ETAPA 4

◾️Aquí seleccione la opción de Llamada de voz y complete el no: que obtuvo del sitio web (k7.net)

PASO-5

◾️Ahora recibirá un correo con un código de verificación como correo de voz en esa cuenta desde la que se registró.

PASO-6

◾️Ve a abrirlo,

--------------------------------------

☙☙☙☙🤩🤩

--------------------------------------

Correo electrónico rastrear etc

<https://www.getnotify.com/>

--------------------------------------

📸🐔🐔

--------------------------------------

SO: Windows

Lenguaje de programación: Python

Simplemente siga las instrucciones en el archivo setup.ps1.

Descripción: Esta red de bots se creó para funcionar con varios C2.

Puede ejecutar 1 comando al mismo tiempo para todos los bots.

Puede ejecutar 1 comando en 1 bot.

Solo puede usar una contraseña o clave SSH para conectarse a los bots.

La mayor ventaja de esta botnet es que cuando agrega un bot al C2, puede cargar el mismo programa en el bot y luego controlar todos los bots desde allí de forma segura a través de SSH.

Entonces, si su servidor de comando y control no funciona, siempre puede usar otro bot para este propósito.

<https://hackforums.net/attachment.php?aid=424>

--------------------------------------

🔑🐶🥵❌🐶❌🥵❌🥵❌

--------------------------------------

Página hackers deep web

<https://wwhclublci77vnbi.onion/>

<http://verified2ebdpvms.onion/>

<https://forum.exploit.in/>

<http://crdclub4wraumez4.onion/>

<https://probiv7jg46vmbox.onion/>

<http://damagelabo2jiykj.onion/>

--------------------------------------

🥰😳🐔🔵🟣💚🟡

--------------------------------------

Deep web

El http Hidden Wiki: //zqktlwi4fecvo6ri.onion/wiki/index.php/Main\_Page

El Uncensored Ocultos http wiki: //uhwikih256ynt57t.onion/wiki/index.php/Main\_Page

Bóveda 43 (útil) http: //vault43z5vxy3vn3.onion/

Biblioteca Imperial de TOR http: //xfmro77i3lixucja.onion/

Sin embargo, otro directorio tor http: //bdpuqvsqmphctrcs.onion/

Gramos (búsqueda) http: //grams7enufi7jmdl.onion/

The Hub (foro) http: //thehub7dnl5nmcz5.onion/

Agora Foro http: //lacbzxobeprssrfx.onion/

Sopa de cebolla http (enlaces N Stuff): //soupksx6vqh3ydda.onion/

Torum (foro) http: //torum4kqr55yqui6.onion/

Overchan (un poco de todo lo que parece) http: // oniichanylo2tsi4. Cebolla /

TORCH (búsqueda) http: //xmh57jrzrnw6insl.onion/

Francés Tor IRC http: //fitwebwmjekqsyrw.onion/

TORsearch http: //kbhpodhnfxl3clb4.onion/

Yacy (búsqueda) http: //yacy2tp5a2dhywmx.onion/

OnionDir (enlaces) http: //dirnxxdraygbifgc.onion/

Burnout (enlaces) http: //burnoutxf6o2yvsw.onion/

TOR Servicio Ocultos (búsqueda) http: //msydqstlz2kzerdg.onion/search/

Q & A (como yahoo respuestas) http: //pequ3i77q5l4w4sw.onion/

De Benji Blog http: //Sonntag6ej43fv2d.onion/en

Secret Stash (blog) http: //dn4hcr3qhlpaiygr.onion/

Foro Cebolla Cruel (foro para “malas cosas \*) http: //cruel2ijkqggizy5.onion/forum/

The Plague (enlaces y cosas) http: //zseijor556d5t4yf.onion/

Noticias Oscuro (foro) http: //xhb4vpn4a67sug7t.onion/

Spreadit (se ve un poco como reddit) http: //jdl3nf2hr3ehzyoc.onion/

Hechicería y Steamwork (búsqueda) http: // kaarvixjxfdy2wv2. Cebolla /

Myles Braithwaite http: //gvvsa367g2zkzjj3.onion/

TOR vincula http: //torlinkbgs6aabns.onion/

Nudista Paraíso (sitio para nudistas) http: //qvchmzewlf4efhcw.onion/

DeepWeb Ministerios (religios web) http: //hxnibog5m2ocjeef.onion /

SIN Red de Inteligencia Estratégica (estar preparado para cualquier situación) http: //4iahqcjrtmxwofr6.onion/

Añadir estos vínculos (links) http: //vizpz65utiopch7t.onion/

Vida Shadow (noticias) http: //shadow7jnzxjkvpz.onion/

Búsqueda de archivos de Usenet http: //wbyi72yt6gitdcqd.onion/

Blog de ¿?la Libertad (blogs gratuitos) http: //crylibertytwta4s.onion/

Intel Exchange (foro) http: //rrcc5uuudhh4oz3c.onion/

GUROChan (tablón de anuncios) http: //gurochanocizhuhg.onion/

Maxima Culpa (confesiones virtuales) http: //nsmgu2mglfj7za6s.onion/

Cebolla DIR (enlaces) http: //chl7b5p6rr64po3s.onion/

Leonhard Weese (blog personal) http: //liongrasr5uy5roo.onion/

YHIMA (enlaces) http: //ogbinmlotgjwgkeo.onion /

Suicidio Sancionado (foro) http: //suicideocymrgxq7.onion/

Anon confesiones http: //confessx3gx46lwg.onion/

OnionNet (Links Noticias etc) http: //ubbchzof2pxs4swi.onion/

Ley Surveilance http: //7vrl523532rjjznj.onion/

Blue Onion (libros) http: //blue3237xytrz5rk.onion/blueonion/

El http Ocultos Foro: //ewd5a7hnvc4necnf.onion/index.php

Simple http tienda: //dharyyzdhok5eudi.onion/store/

Malas ideas Foro http: //7x5rg44gkhtovwjt.onion/ foro / index.php

FUD (discusión bordo) http: //bssjumzkbj3vlhiy.onion/

Enlaces ocultos http: //hidhost5gk6w7ahf.onion/hidlinks/links.php

Facebook en tor? https: //facebookcorewwwi.onion/

FBI Chan http: //fbichanc6yfagl4l.onion/

Lectores club http: //c3jemx2ube5v5zpg.onion/

Weblog http: //6e3i6bqjgnmtn3fu.onion/

Mercados y Tiendas Negros.

EasyCoin – Bitcoin Wallet con conexión Bitcoin Mixer. http: //easycoinsayj7p5l.onion/

WeBuyBitcoins – Vender tus Bitcoins para el efectivo, PP y más. http: //jzn5w5pac26sqef4.onion/

OnionWallet – Anónimo Bitcoin Wallet y Bitcoin lavandería. http: //ow24et3tetp6tvmk.onion/

EuCanna – ‘First Class Cannabis Healthcare’ http: //rso4hutlefirefqp.onion/

Pueblos Drug Store – del Darkweb Mejor Proveedor de Drogas! http: //newpdsuslmzqazvr.onion/

Hierbas favoritas – Finest Orgánica Cannabis sale de EE.UU.. http: //smoker32pk4qt3mx.onion/

CannabisUK – Reino Unido al por mayor de Cannabis Proveedor. http: //fzqnrlcvhkgbdwx5.onion/

DeDope – Weed alemán y tienda de Hash. (Bitcoin) http: //kbvbh4kdddiha2ht.onion/

BitPharma – proveedor de la UE para la cocaína, la velocidad, mdma, psicodélicos. http: //s5q54hfww56ov2xc.onion/

Brainmagic – Mejores psicodélicos en la red oscura. http: //ll6lardicrvrljvq.onion/

NLGrowers – Cafetería grado de cannabis de los Países Bajos. http: //25ffhnaechrbzwf3.onion/

Kamagra para Bitcoin – Igual que el Viagra, pero más barato! http: //k4btcoezc5tlxyaf.onion/

Tienda móvil – iPhones desbloqueados y otros teléfonos inteligentes. http: //mobil7rab6nuf7vx.onion/

Reino Unido Guns and Ammo – Armas y Munición de venta del Reino Unido. http: //tuu66yxvrnn3of7l.onion/

Rent-A-Hacker – Hacking, DDOS, Sociales Ingeniería etc. http: //2ogmrlfzdthnwkez.onion/

Cebolla Servicios de Identidad – Pasaportes Vendiendo e ID-Tarjetas. http: //abbujjh5vqtq77wg.onion/

HQER – cuentas euro de alta calidad réplicas / falsificaciones. http: //y3fpieiezy2sin4a.onion/

Falsificaciones USD – USD falsificaciones de alta calidad. http: //qkj4drtgvpm7eecl.onion/

Ciudadanía EE.UU. – Obtener un verdadero pasaporte EE.UU.. http: //xfnwyig7olypdq5r.onion/

Apples4Bitcoin – productos baratos Apple para Bitcoin. http: //tfwdi3izigxllure.onion/

ccPal – CC, CVV2s, Ebay, Paypals y más. http: //3dbr5t4pygahedms.onion/

EuroGuns – Su # 1 traficante de armas europeo. http: //2kka4f23pcxgqkpv.onion/

Británicos Pasaportes – Original Pasaportes del Reino Unido. http: //vfqnd6mieccqyiit.onion/

USfakeIDs – alta calidad EEUU licencias de conducir falsas. http: //en35tuzqmn4lofbk.onion/

Tecnología, las computadoras, los hackers de alquiler, materiales / anarquía relacionados de hacking.

Cualquier cosa me encuentro con que se ve técnica de ninguna manera serán agrupados en esta categoría. Podría ser sólo una pequeña snipet de código. Podría ser hackear cepas / phreak desde hace 20 años. Podría ser una empresa que ofrece algún tipo de servicio relacionado con la informática que yo sólo no entiendo

MacLemon (seguridad, noticias, enlaces) http: //fzybdgczph7xfdnr.onion/

Estado TOR – Tor estado de la red http: //jlve2y45zacpbz6s.onion/

Clave pública TorPGP http servidor: //torpgp3ujaysucll.onion/

Altera Praxis (no estoy seguro de qué se trata TBH) http: //ncivdawfxihoh7sj.onion/about.html

Keybase (una especie de pirata / herramienta acosador idk) http: //fncuwbiisyh6ak3i.onion/

Tor Web devolper (de alquiler) http: //qizriixqwmeq4p5b.onion/

Programador Web (en alquiler) http: //kobrabd77ppgjd2r.onion/

Servicio de Hacking de Ozy (pirata informático de alquiler) http: //ozy7mnciacbc5idc.onion/

Servicios de Pioopioo (pirata informático para el alquiler ) http: //rowtogxp2akwem6n.onion/

Lugar Hacker http: //hackerw6dcplg3ej.onion/

Parazite (info anarquía principalmente) http: //kpynyvym6xqi7wz2.onion/

Foro de soporte DNS http: //mj6vjwhtyahcj6fx.onion/

BitMessage correo de puerta de enlace http: / /bitmailendavkbec.onion/

Keys Open Doors http: //wdnqg3ehh3hvalpe.onion/

Servicio Ocultos howto http: //nfokjgfj3hxs4nwu.onion/

JRat (herramienta de administración remota de Java) http: //jratoc334zo7zgis.onion/

FILTH (carajo te quiero hackear) http: //om2ak3coziov3dbc.onion/forum/index.php

Cebolla Dominios y MD5 http: //xlmvhk3rpdux26dz.onion/

Soylent Noticias http: //skgmctqnhyvfava3.onion/

Azulado Coder http: //mh7mkfvezts5j6yu.onion/

Visor Cable (idk lo esto no es más que su irritable) http: //leakager742hufco.onion/

Xerbot http: //xfthw4bq7lx2y726.onion/

Hack Canadá http: //hackcanl2o4lvmnv.onion/

Imperial http despotismo anarquista: //rgeo5wj7gneidzh3.onion/

Directory listing denied (web anon ftp) http: //wtutoxfznz45gf6c.onion/

Anarplex (una especie de anarquía ordenador) http: //y5fmhyqdr6r7ddws.onion/

GhostDeveloper (programador freelance) http: //develggxuazrcokn.onion/

SKS Cebolla http servidor de claves: //lbnugoq5na3mzkgv.onion /index.html

GNUPG http: //ic6au7wa3f6naxjq.onion/

Hechos Cat http: //2v7ibl5u4pbemwiz.onion/

Ajedrez (juego) http: //theches3nacocgsc.onion/

Ciudad Necro (enlaces n cosas) http: //nekrooxwwskakacj.onion/

Cifrado Password Generator http: //pwgenmwi7eqsys76.onion/

Rows.io jabber http: //yz6yiv2hxyagvwy6.onion/

M5S fugas http: //33pvcdba2nm3afnj.onion/

Un proxy HTTP cgi: //x5yd2gfthlfgdqjg.onion/

FIT francesa http IRC TOR: //fit2v7z4plpfyh2h.onion/

El Proyecto de Documentación de Linux http: //3c2rvufmbcggnqi6.onion/

http Crypto Partido: //cpartywvpihlabsy.onion/

Hive Archivos http: //thehivemwon6a5mp.onion/

Txtorcon (python biblioteca contril para tor) http: // timaq4ygg2iegci7.onion /

Rodio (cosas ciencia) http: //rhodiumio4b7b4rm.onion/

http Hackerspace Praga: //pmwdzvbyvnmwobk5.onion/

Porno,Erotica.

Pron tormenta http: //prnstmrpfkgkaw5v.onion/

http Fetichismo: //fetishuonjww3xvt.onion/

\*\*\*\*\* y Scat http: //shitscats6qomwxm.onion/

Nórdica http porno escandinavos: //xnordic6virmmls3.onion/

Historias Extreme Boy http: //dembtxtlnu2cospb.onion/

Secret Story Archive (relatos eróticos, arte, etc) http: //pja3dhxxpn4cba63.onion/TSSA/index.html

Xcomics (cómics para adultos) http: //xcomics5vvoiary2.onion/

Girls Liberadas (fotos) http: //k4jmdeccpnsfe43c.onion/

(fotos y vids) http: //mjt54q6pagohhimn.onion/

Escándalos Oscuras (mujeres chantaje en las cosas) http: //hhokbk2kujwujm3w.onion/

El romance oculto de Soreking (historia de amor) http: //sorekingemb36w65.onion/

Pee fotos (chicas meando) http: //peepicsjswxrkhuc.onion/

http levas JailBait: //byu4ifhwhzyo44bf.onion/index.php

La pesadilla de los Animales (foro de maltrato animal) http: //7adopgjsyman2el2.onion/

Boy vids http: // boyvidsthnubdaub. Cebolla / index.php

Mosca en la pared http: //7ulefmuz3jowwjb4.onion/

Galería Fappening http: //fappen53mnvayq4o.onion/

http porno: //bernd33lcq7im5nw.onion/regeln/

Enlaces http: //jjvxrbpckwpz3kwu.onion/LINKS/

Central Park (enlaces) http: //boysopidonajtogl.onion/

Clase Galaxy (chatear + archivo de host / acción) http: //startrekoqeow6e3.onion/galaxy.cgi

http levas JailBait: //spe7fcy6kmupwvr3.onion/

conocer a mis hermanas http: // 4e6avcmbxn5y253g.onion /

http porno: //pussybadk7h65tcn.onion/

Crossdress y esas cosas http: //dressupbmylprqbf.onion/

Políticos, activistas, grupos, el periodismo, la denuncia de irregularidades etc.

Juventud foro Rage http: //neyigf7eragkp5nq.onion/forum/

Asociados denunciantes http: //w6csjytbrl273che.onion/#/

Comunidad X contratación http: //gp5tycij54ri7xcz.onion/

Código Verde ( ética hacktivismo) http: //pyl7a4ccwgpxm6rd.onion/

Infodio Fugas http: //ymi7h25hgp3bj63v.onion/#/

Wiki Leaks http: //zbnnr7qzaxlk5tms.onion/

http dominio de Zwitterion: //3il6wiev2pnk7dat.onion/

Asegure silbato vida silvestre soplando http: / /ppdz5djzpo3w5k2z.onion/#/

Libertad de prensa http fundación: //freepress3xxs3hk.onion/

La loli http servidor de promoción: //lolikaastbgo5dtk.onion/

Global Fugas http: //h73hx2munq7q465s.onion/#/

http Tactical Technology: // hrkdpwrkh3lbow2l.onion /

Fondo de las http lucha islámico: //teir4baj5mpvkg5n.onion/

http Transparencia Gobernanza de Internet: //k52lcjc5fws3jbqf.onion/

Luchamos http censura: //3kyl4i7bfdgwelmf.onion/

Insiders Anon http: //imtrjn3qe2tzh5ae.onion/

Mapa Mos maiorum (ayuda de los refugiados) http: //iuektur6bicvfwcq.onion/ushahidi/

Fugas wiki http: //jwgkxry7xjeaeg5d.onion/

El anonimato, Seguridad.

Incluye correo electrónico seguro, chat, etc

Anonet wiki http: //xz2rtmpjjwvdw44p.onion/

Secure Messaging http: //sms4tor3vcr2geip.onion/

MailTor http: //mailtoralnhyol5v.onion/src/login.php

Lelantos correo electrónico http: // lelantoss7bcnwbv.onion /

Cebolla correo http: //p6x47b547s2fkmj3.onion/

JitJat (mensajería) http: //jitjatxmemcaaadp.onion/login.php

TOR PasteBin http: //postits4tga4cqts.onion/

RetroShare chatear servidor http: //chat7zlxojqcf3nv.onion/

ProtectTOR55 http: //protector55z5s7j.onion/

Zerobin http: //zerobinqmdqd236y.onion/

TOR el chat ruleta http: //tetatl6umgbmtv27.onion/

SIGAINT (email) http: //sigaintevyh2rzvw.onion/

Marino http servidor de correo: // inocncymyac2mufx. Cebolla /

Web / irc charla cosa http: //6ejbuiwnp77gu67h.onion/

FreeFor (chatear) http: //tns7i5gucaaussz4.onion/

Volátiles (chatear n cosas) http: //vola7ileiax4ueow.onion/

Hosting, Web, Archivos, Imágenes.

Onionweb File Hosting (límite de 100mb) http: //3fnhfsfc2bpzdste.onion/

Ocultos http Hosting: //7zzohostingx4mes.onion/

Gratuito vínculos Hosting http: //a5ok374pjcq7bsyp.onion/

Servicios Darknet http: // darknet4x3hcv5zp .onion /

Infernet oscuro http Hosting: //a5ok374pjcq7bsyp.onion/

IMG.BI (alojamiento de imágenes) http: //imgbifwwqoixh7te.onion/

Secure gota http: //v6gdwmm7ed4oifvd.onion/

CYRUSERV http: //cyruservvvklto2l.onion/

Gratuito TOR http Hosting: //zuxtem3jcv2fvmgk.onion/

Hosting Inicio (cómo) http: //dmru36nvfgtywx47.onion/

http Hosting real: //hosting6iar5zo7c.onion/

TorSafe (alojamiento de archivos) http: //torsafeiwttlkul6.onion/accounts/login/

Bienes Hosting http: //ezuwnhj5j6mtk4xr.onion/

http TOR VPS: //torvps7kzis5ujfz.onion/index.php/TorVPS

Kowloon (hosting) http: //kowloon5aibdbege.onion/

Cebolla Pastebin http: //pastetorziarobi7.onion/

Popfiles (archivo hosting) http: //popfilesxuru7lsr.onion/

Ocultos http Hosting: //offshore6gq7ykr7.onion/

Darknet Soluciones (hosting y diseño) http: //darknet47je5xwm6.onion/

Cargador Cebolla (alojamiento de archivos de hasta 100 MB) http: // nk3k2rsitogzvk2a. cebolla /

Media, música, películas, arte, dibujos animados, cómics, etc \*

Skeletor.bit http: //okzatvfk2jzgvmf4.onion/

Yay Ponis http: //ponieslzi3ivbynd.onion/

HFS (música) http: //wuvdsbmbwyjzsgei.onion/

Gatito Mar Palacio (torrentes) http: //wtwfzc6ty2s6x4po.onion/

Manga http: //negimarxzov6ca4c.onion/

Comics http: //7etxnv26hro7mmuu.onion/

Profundo Tune (música) http: //tune4xs6mj2evcr6.onion/

TorFlix (películas) http: / /jl4m7ubpotnu2yos.onion/

Sin nombre, no estoy seguro si su música o hablar pero http de su mp3: //xf3fjq4b7j6pswuq.onion/

Cosas Gone (imágenes imprimibles) http: //32ixi6myw3things.onion/

ORVoice (música) http: // orvoicemur72h7rx. Cebolla / TOR /

Índice de (música) http: //uuxrei5or65anucg.onion/

Mi pequeño pony http: //mlpfimf74svi6y4q.onion/s01/

El http bóveda audiolibro: //xmctuxj7dsymumwf.onion/

Otros…

http Riseup: //zsolxunfmbfuq7wf.onion/rc/

Place (alargamiento del pene) Thunder http: //thundersplv36ecb.onion/

Smart5 (foro, por lo que idk aunque) http: //smart5ywvuwbmzfd.onion/

TOR Biblioteca Alemana (documentos, archivos, sobre qué tema idk) http: //pqfja3rzroprkfq6.onion

Dying Breed (foro, idk qué) http: //g6o7aurv4c3ixalq.onion/index.php

Hers algunos cordones aleatorios. Latitud / longitud http: //4k2oq3fswx35a72s.onion/

Zyprexa mata http: //tdkhrvozivoez5ad.onion/

Gato fuera de la bolsa de http: //vkpriz2cjzymgpsp.onion/

XL33tVill3 (enlaces y idk qué) http: //tt75atziadj4duff.onion/sindex .html

Realmente no sé qué decir http: //rjzdqt4z3z3xo73h.onion/

Pantalla solar http: //zgypn3izock2oqny.onion/

Archivos GIF (archivos de inteligencia mundial) http: //gkqmy7ioqptiru5o.onion/gifiles/

http Hacked: // 7º46qra2jkz3k3kx .onion /

GreatDumps http: //www.greatobxvv7etokq.onion/ login.do/?

Revista internacional de la prueba de concepto o GTFO http: //pocgtfo7tu77thrp.onion/

Evolución http: //k5zq47j6wd3wdvjq.onion/login request\_path =% 2F

Elize chatbot http: //opnju4nyz7wbypme.onion/

Cryptome (im no sabe dónde poner esto por lo que su aquí) http: //y6q2mnorhmsfdm3r.onion/

Pastebin http: //5aklnwbibkhrtbs6.onion/

http: //boysopidonajtogl.onion/

http: //xplayyyyyirxui4n.onion/

http: //boysopidonajtogl.onion/

--------------------------------------

😡🥰😳🐔😄

--------------------------------------

Hacking redes inalambricas

<https://www.mediafire.com/folder/jkie9hp26pn80/Hacking+Redes+Inalambricas+S4VITAR>

--------------------------------------

🖤🖤📸🖤📸🖤📸ஐ

--------------------------------------

Descargar videos yt

<https://Yt1s.com>

--------------------------------------

🥳🥳🤣🤣🤣🤣🤣🤣

--------------------------------------

Only fans full pack

6TB -https://mega.nz/folder/fYE0zDAQ#pShUFkBaxB1LmYa1Sl2Nzg

5TB(Updated) - <https://mega.nz/folder/cfB3HQpJ#h8tiFweThyp84JFoBwugLQ>

3TB - <https://mega.nz/folder/VIgn2aqZ#eGkqIctcTOBoW0uysjrVWQ>

685GB - https://mega.nz/folder/8JMBwaIB#HUAKRTOsebjUSgmM1gowTA

517GB - <https://mega.nz/folder/nlV0WDpK#Zms-p2Cu1tcVbCgnqsj93Q/folder/W19mXTZb> | KEY - Zms-p2Cu1tcVbCgnqsj93Q

360GB - <https://mega.nz/folder/D4RzECSD> | KEY – 66AlLLFKF\_lfbVTS3WxNAg

335GB - https://mega.nz/folder/RRoGVY7T#jVl1Pm9i2TRCAQgqpg0M1g

50GB - <https://mega.nz/folder/zFtW3Q7Y#U_Fnvz4Ck2NajECx-k8DvQ>

45GB - <https://mega.nz/folder/B3wR1RZa#cnGf61l4SJ7nmZzHsUTU8A>

41GB - <https://mega.nz/folder/yA1glCSY#2DQoNyVzsE8JtfllBHbLZw>

22GB Tik Tok - <https://mega.nz/folder/GFR3DQyA#e5-GGXdKicP39Mfy6a5Ajw>

10GB - <https://mega.nz/folder/Z01RlKzC#nmynQ7Q_vCo_Z3bjJ71YLA>

Brenda V -

<https://drive.google.com/drive/u/0/folders/1v4g5Ocd3ckJQU4W0jrpc4C8r5IdECtTt>

Zara Jordan - <https://www.erome.com/a/OVzu8dMD>

Alva Jay - <https://mega.nz/folder/0ghSnZIT#II7nyb7uQUDasm_3WFIp-w>

Heidi Grey - <https://mega.nz/folder/t2ISHJwK#DBKostyHSGF8oOyFHaPQVg>

Matimarroni - <https://drive.google.com/drive/u/0/folders/19mbJ5K-fzTXFXNN1HGiwF0DkOExKYGxT>

Taylor White - <https://mega.nz/folder/Qxpk2RaY#zaeXmjDAjI0utRtcwFlp3Q>

RealMissLizzy - <https://drive.google.com/drive/u/0/folders/1L58mJXsPRS31NnOmS885y3MSzDSUF309>

MackzJones - <https://drive.google.com/drive/u/0/folders/1IORjssJz0w7M6JP06XjHQ_SSXzV-siBO>

Kayle Keeps - <https://mega.nz/folder/F0JnRQLK#oN2xFZf0MRiniptsoY745g>

C p - <https://mega.nz/folder/73plEaSY#ntM_YJSp9U_rmmMIouRMvA>

Lauren Jasmine - <https://mega.nz/folder/JoAAnBrI#BEnbRrL6BXwgVEZp1ScA8g>

Skylar Vox - <https://mega.nz/folder/hxQDgKrB#LvXUK-tTKkpO7dfrzXLt3Q>

Ashley Tervort - <https://mega.nz/folder/J0p20L6D#wNAtBu7BULPW8m4oyH8dUA>

Juanita Belle - <https://mega.nz/folder/oMhURapB#a_ICDQLVWACi7p9m4t30ag>

Kaaki - <https://drive.google.com/drive/u/0/folders/1-3Aya6PxCHCLdnlBBvfz1MwxGRtafFjG>

Mia Malkova -

<https://mega.nz/folder/7tw0URTZ#rV6ffl6st08Bmfk5doOwNQ>

Jasmin OF - <https://drive.google.com/drive/u/0/folders/1V1huoAIDsYwyBOPz4J3YHK-PnriVdJwV>

Burch Sisters - <https://mega.nz/folder/kexUmbAT#KmM--xfSLU6vNMjRP4p9Ng> | KEY - KmM—xfSLU6vNMjRP4p9Ng

JadeTeen - <https://mega.nz/folder/1epSDRjQ#VwwOpZIm2zsSqGtEAe70LA> | KEY – VwwOpZIm2zsSqGtEAe70LA

Violet Summers - <https://mega.nz/folder/Z9ZRkIgI#qBo4FgYQsfwQjkfQddQKdw>

Leah Wilde - <https://mega.nz/folder/clAnVKJR#vl4vDNKGmEUTzuuAZRt1Ew>

Carrot Cake - <https://mega.nz/folder/59oE3J6A#JqwXz7KDrRBMfIV6HRmKWA>

Aria Taylor - <https://mega.nz/folder/ltYB2AAZ#-Og3yFP7SaR2RA3pdGVNdw>

Emily Cheree -

<https://mega.nz/folder/Nx50kYaQ#poMPeF5PcSn368Hqh4krHg>

Brittanya Razavi - <https://mega.nz/folder/k9NnXCiL#VgtIJbmAoBFPG-QgGrbp5w>

Morganlanexo - <https://mega.nz/folder/1upTTZ7C#ldBg_3XqzFsI4tB6Kv2j9Q>

Desi9 -

<https://mega.nz/folder/Nlo0jCSL#jaIQ2y0y5HveDw9dbP9CIw>

Alexa Fanbus - <https://mega.nz/folder/4ip12KrC#QSyU9RqGtgZwjpUj7K-gdQ>

Pia Bunny - <https://mega.nz/folder/KJc3BYhY#UkObGa_StdK0etpYtq_lTg>

Hentai/E-Whore - <https://mega.nz/folder/oN5xxTzL#we3Um_6XoJuz-1Er6k8mWQ>

Lasirena69 - <https://mega.nz/folder/ZLYkXRgY#yAlo3n_DAj6mVrhr3Dz0ug>

Purple Bitch - <https://mega.nz/folder/AGRQ3TpY#3yeLZKJgBlQbNdZ9EvFxDg>

Asian Girls 22GB - <https://mega.nz/folder/sPQgmJqL#ixiso_aYifiMe7FTenaXdQ>

Monique - <https://mega.nz/folder/8Ho23ILT#_7D_FpgqXSQF4YJEjIoq5g>

Nataliaxstarr - <https://mega.nz/folder/AF5TRT6J#39hfNWSwJKFHt6ppPjSt0Q>

Fai -

<https://mega.nz/folder/158VxK5Y#vO-GdC5uwnx9LNWhDR1LrA>

Nursh - <https://mega.nz/folder/xHYFhCQL#1kvoFqANBvSjS8qyjnlpVg>

Savannah Bond - <https://mega.nz/folder/MTgwxZaC#YFWnKwF7VIebzw8zDvFzVQ>

Chloe K - <https://drive.google.com/drive/u/0/folders/1CtFW2SJNqKA_Fg6dwcFg0vJldMiaqSMf>

JcTapes - <https://mega.nz/folder/Qxs2HJib#eUKXuBjw1fd03hAmWcwxeQ>

Lanar Hoades -

<https://mega.nz/folder/Z5tnHIAT#zXpgug7--eil9waurysN9g>

Riley reid - <https://mega.nz/folder/hp4FjCaJ#K_JG9JjZsc9ajkIBnKlyPA>

Rinaudo - <https://mega.nz/folder/tkpACD7T#UWTUM2tJnp-tEyvPg83UBw>

Megan - <https://mega.nz/folder/tpkCDLKL#PFaV4p-5CCm7D4EC6g7R-A>

Sara Mascara - <https://mega.nz/folder/1ssU1Lpb#dJaGK0bAy6Ce_XptnG5hJQ>

Carmela Clutch -

<https://mega.nz/folder/IZUwDJST#5OfCM6WckpWEptbw3ZYPTg>

Ana Hendryx - <https://mega.nz/folder/UhBSiBIL#QR7mAQmRsdzIayHdZQRWhw>

Kkvsh -

<https://mega.nz/folder/M8B2lJKC#vsGFkEL9_PmfTRuL9DCIJQ>

Belle Delphine - <https://mega.nz/folder/HsgVxYJZ#xqKIRXnULjEhTgnqsGIoPQ>

Alexas Morgan - <https://mega.nz/folder/HoFk1Zpa#fO7w42Buzh0gtVj0R8jjWg>

Jem Wolfie -

<https://mega.nz/folder/8WRFFQLT#_7KAQvEiiZSgi4NZ43CbAg>

csblondebombshell - <https://drive.google.com/drive/u/0/folders/1US48cCbVBnSIDV6yBEx2zCNGwPAfXH8B>

Sherlyn Chopra -

<https://gofile.io/d/LIBrB4>

Isabella Ramirez -

<https://mega.nz/folder/XQ1V2CBD#NqfRwNtdmL_I9iIzVqGELQ>

Serena Becker -

<https://mega.nz/folder/AKA3CAbD#Yti6X551cO4kJgoT9hWvrg>

Wet Kitty - <https://mega.nz/folder/wG4DySZZ#Zu6XJVuoYL7yMs2nzRqx1A>

Jade Teen -

<https://mega.nz/folder/ISgEHAaL#QjUISuTF8X9sPm87cVtavA>

Neiva Mara -

<https://mega.nz/folder/uYFh1SiY#EaYykX4DOgQ8v7LBN1OrXw>

Stormimaya - <https://mega.nz/folder/WREgiZ6D#S8L5r3Kt4bdIth6mncPbkw>

MyCherryCrush - <https://mega.nz/folder/i0cVBSrS#ydqYLLFnrmfDVTOi7Tf9uQ>

Blake Blossom - <https://mega.nz/folder/VzQhSKrY#0fJ2FB903yLAZHDJg78a0Q>

Bethany Lily - <https://mega.nz/folder/SD4wDIiL#MH9zFJEgL_tE168jFpY0mA>

Ashe Maree - <https://mega.nz/folder/nVFSnJgI#On8CZ5yPm6XE4A5KXXvtrg>

Julia Tica - <https://mega.nz/folder/3JU00LYT#0edwJTAMfr2dqDdj2tLzqQ>

Mia -

<https://mega.nz/folder/6jQEjYJR#DIl9TmhOp7rEvD0pMF4h5Q>

Ana Cheri - <https://mega.nz/folder/QnxEhJIB#3IxPe5tkJni6-7cOGBeiiQ>

Miss Lola - <https://mega.nz/folder/YzhGFBJQ#1TWHUkrSN0nCq71kTTggNw>

Bridale New -

<https://drive.google.com/drive/u/0/folders/1hsFBpakN-9LWQNErjq5ESnERbvkH1oH8>

Ashley Danielle - <https://mega.nz/folder/6MNSxTRY#3CVMB7UiDxwSrIXcCcAB1A>

Tessa fowler - <https://mega.nz/folder/mFMXkKwR#HigxIKoSl8_5wzB5VpvLmQ>

Lauren Lovin - <https://mega.nz/folder/wvwmEBTK#ByWdIqfSfLWoLLxQXQXQ6g>

Lauren Lovin - <https://mega.nz/folder/wvwmEBTK#ByWdIqfSfLWoLLxQXQXQ6g>

Emira Foods - <https://mega.nz/folder/75sDGBob#5VfGyVcF_ejiPhym0WoJ9A>

Malu Trejevo - <https://mega.nz/folder/cmZWVBDZ#vNwGsgTiGg4sP98NdnW4YQ>

Becky Crocker - <https://mega.nz/folder/JSwmUZaT#-C059kN34tfK3tpRdYiGGw>

laynaboosxtapes -

<https://mega.nz/folder/lvgh3ChJ#4lUTlATeKxDnzt21i4OPVA>

Dani Daniels - <https://mega.nz/folder/ZChUhJZQ#M1rnsr-t9n2WWKrnl3rw1w>

EtherGher - <https://mega.nz/folder/GIQUBIRC#xT_AkDIHeXq1-hdxC32glQ>

Alison Rainer -

<https://mega.nz/folder/Bu4WFC7Z#euzAuvVbEFwxLu4UmHNJDQ>

Anri Okita -

<https://sendvid.com/1q6ts2xy>

<https://sendvid.com/a6atx70g>

<https://sendvid.com/de363nrl>

HOT4LEXI -

<https://mega.nz/folder/JmhGhb7I#uarcopPQf3m8SvXgVA4L2w>

Yuu Sakura - <https://mega.nz/folder/Z3xkxJjA#SwtRAK0b8O_tewY-MIlDLw>

Yinyleon -

<https://mega.nz/folder/trowRTRC#wUsqTtWdjpEa3DyLa0s8wA>

Carrot Cake - <https://mega.nz/folder/jJ1SRKrL#V_BcFriD2_DaPyc05Z4YfQ> | KEY - #V\_BcFriD2\_DaPyc05Z4YfQ

Brandy Wolf - <https://mega.nz/folder/ajwmyAZA#I46pRc-RthO4EziuJeCXug>

blondetittypiercings - <https://mega.nz/folder/UZ5FWJLT#ujmuivqbTrlZxFHW5J7Gjw> | KEY - #ujmuivqbTrlZxFHW5J7Gjw

AliceRedLips - <https://mega.nz/folder/tck0ybZb#fn2ydkV5hl59tJ1OSOdRnA>

Bbygirl29 - <https://mega.nz/folder/8lNRRShR#0sMYupsfcBaKVnYgzpRekA>

Sophie Mudd - <https://mega.nz/folder/SEFGgDpZ#2ohjlpkE-_spgsiS4eQWmQ>

Amanda Trivizas - <https://mega.nz/folder/QLxQDIKA#Qqn7uvXI4E9w7zNAO6G9lg> | KEY - !Qqn7uvXI4E9w7zNAO6G9lg

Awesome Kate - <https://mega.nz/folder/zpZDXKrJ#Aj8RP085xnffzNmVITEgJQ>

melwood - <https://mega.nz/folder/aYs1yKhK#vXgq4pJuqtaJVXZX38toFg> | KEY – vXgq4pJuqtaJVXZX38toFg

Awesome Kate - <https://mega.nz/folder/zpZDXKrJ#Aj8RP085xnffzNmVITEgJQ>

melwood - <https://mega.nz/folder/aYs1yKhK#vXgq4pJuqtaJVXZX38toFg> | KEY – vXgq4pJuqtaJVXZX38toFg

Violet Summers - <https://mega.nz/folder/gTY0nbjT#Sl09lf8br70ZYKDeihA_oQ> | KEY – Sl09lf8br70ZYKDeihA\_oQ

lyssamaxiscute - <https://mega.nz/folder/Z1MQRRbL#vszKURlMmn3fvOlA1Q_2eg>

Mikaela Testa - <https://mega.nz/folder/aM1jEKYB#MVjTE95cD-EUPvHdM00wkw>

Moriah Mills - <https://mega.nz/folder/TYkjmSbK#75-R7_dKCEF2v09X3nEazw>

Noey Yanisa - <https://mega.nz/folder/fYsUTCib#snLh6_JZl8WRDhiNnBbRkw>

Desi - <https://mega.nz/folder/OVl2zSwR#wXEpYCcuDlTSAdxYPxgcLA>

Jenna Shea - <https://mega.nz/folder/vUsgwCCB#vPmX7oTR4dd9xQUHQWs5RA>

Ariella Ferrera - <https://mega.nz/folder/SAkQVSCb#eo_ueDrqi_txUhVw9ugJaQ>

Briana Monique -

<https://mega.nz/folder/RD5GAazR#3L1n8-dDpibO_DQnAo0low>

Bela Torne - <https://mega.nz/folder/ADgChIBD#3Y5t3yRqEY_kZGi0wbg5ew>

Mini Tiktok collection - <https://mega.nz/folder/5CwCmCAZ#PeTi7EvAuXmg0wtKl2p3nA>

Kaylen Ward -

<https://mega.nz/folder/UepWHCQL#mbDQde7bzzrRN0SQ6LpglA>

Celina Powell - <https://mega.nz/folder/xCxW0CrY#KKC0LEB3zPoQnagVDO3oBg>

Sara Gold - <https://mega.nz/folder/cewyHAgA#BDvvpJ9YZJFykHcrOCI2JA>

Ts Jane - <https://mega.nz/folder/zds02CLD#QcEpRpoAck02JrkxcSqxrA>

AsianBarbieTina - <https://mega.nz/folder/7Y9UVACT#G2vEaO-16NsYXochzMVZQg>

Mia Khalifa - <https://mega.nz/folder/teIUhbxK#slWHMN9yP-JzHcSaI5RB8Q>

Lovegina - <https://mega.nz/folder/tbo2iQiR#whxNjRWItK9T16Zo7-yevg>

Sophie Dee - <https://mega.nz/folder/ZepFhK7L#6fsqUXbltTbcXV9cX2oJZQ>

Amanda Nicole - <https://mega.nz/folder/Dc820CpA#oHzRh7LcwL35prW7I6x6Qw>

Autumns Bum - <https://mega.nz/folder/t8o2CAiI#ONJrkhjwKXP5KhNR7suSmw>

Jasmine Tea - <https://mega.nz/folder/E9wAUAJB#xeRyN1Cd1zOCREWH50fYRA>

Ashwitha - <https://mega.nz/folder/s542gCQC#9qEnqZuwmOHC50eO03Jt3A>

LaciKaySomers - <https://mega.nz/folder/edkCAQRI#uOa0B_kW5Uj6EVWrymr5OA>

Angela White - <https://mega.nz/folder/bJ8UXAha#z80ot_gM4e19tIWcDIfqXQ>

Lindsey Pelas - <https://mega.nz/folder/SF00gSSR#exC3c_a-GpA1H3yGaId5Lw>

Olivia Chei - <https://mega.nz/folder/7FkyiISI#sECohFHiZIZjEOBvijgbNw>

Pandora Kaaki - <https://mega.nz/folder/DYlgUSBT#Nq_wX7sa0S9LkXulbgH0Tg>

Dracuina - <https://mega.nz/folder/mItGHQYa#b6mKfhjhnM_060yl9CvYHA>

Call me Sherni - <https://mega.nz/folder/rF1ylaLK#L8IYHQz-IcZNFyx-gXToow>

Valerien Bele - <https://mega.nz/folder/yE12WQhD#GG4o7rV_WEhd_8u2FSD5pQ>

Alexa Morgan - <https://mega.nz/folder/jE0AVQaB#lHE3gilxekZYhggww4BvRA>

Lilmissanna - <https://mega.nz/folder/WB0gjYQD#NJt5jkcsMQ-gbALFxKw_wQ>

Dreafcknlicious - <https://mega.nz/folder/zElSlKjK#HbmunBlJyYCBNPb900O47g>

FullTimeCryBaby - <https://mega.nz/folder/vF0SkIwa#PNqfzN8E-ektDYjzRzxV4A>

Naomi Woods - <https://mega.nz/folder/GZcSGDTJ#-36laQiy6ccr_btA5fwWoQ>

Artdikaya - <https://mega.nz/folder/CNVWUDSb#fb79fPGYLlFXucxqnk1znA>

Megnutt02 - <https://mega.nz/folder/HdUyQJra#ptJf90yLL8fqqqTysPOjFg>

Ana Lorde - <https://mega.nz/folder/jF00gA6D#Wr51VgNxWegTeQdmuOm4iQ/folder/bYlWlIqL>

Hailey Queen - <https://mega.nz/folder/uU8kGKib#ntFuY9ZjyO-vXXmBwt3ykw>

Jenna Chew - <https://mega.nz/folder/6A0gAKRa#BoVX7J8RU_np5JJToNkpMg>

Dawn Marie - <https://mega.nz/folder/nt5hGAoR#cLlELBlWUV61B6LhMI9Nig>

Natalya Krasavina - <https://mega.nz/folder/7hYDwCiZ#eOIOdAXQBIC-JtGt6_yu6g>

Reya Sunshine - <https://mega.nz/folder/Slo0CLqa#Bxn4G1kimt3ucRmIRzTiNQ>

MattiNew - <https://famousgirls.win/drive/s/liXTBGQnSRRETaw2nKauzuL5C8gaKk>

Shaiden - <https://mega.nz/folder/ZYkGxajB#XtKq7HK6skz6dzBYoa98dA>

NagaiMaria - <https://mega.nz/folder/FlV12ITC#KqerG47GMhOTfFItPso2MA> | KEY – KqerG47GMhOTfFItPso2MA

bbypocahontas - <https://mega.nz/folder/NcNQAR6T#vycqqjSdUaKJUv0OR4Pimw> | KEY – vycqqjSdUaKJUv0OR4Pimw

Rae Lil Black - <https://mega.nz/folder/GE1zEQIb#VtLuvnHc3MaVBkwL6oK-1w> | KEY - VtLuvnHc3MaVBkwL6oK-1w

TheTayJean - <https://mega.nz/folder/IJUxxYzR#fCTTUMM6eUMwUXzM_QbCVw> | KEY – fCTTUMM6eUMwUXzM\_QbCVw

Undrgrndqueeen - <https://mega.nz/folder/6Z9gCIyS#eiMc7fSyeF-BRmuOgwtxqg>

Ash Kash - <https://mega.nz/folder/GVFkXDaS#jbj5EIOB4O1Q13-ibXQAcQ>

Amora Luv - <https://mega.nz/folder/zYE2nboC#LnAD40b1GLHL25k0tsvbnA>

Theconneltwins - <https://mega.nz/folder/CJ1kxYqT#5uETD-ZY3ltOyNGtUKPoPg>

blacchyna - <https://mega.nz/folder/05EjnALA#mWfglGG_XyG2upRhLew18A>

Almond Milkhunni - <https://mega.nz/folder/yM9zGKoB#MBeiEuRKwijuYHNy6YSrug>

Mackz Jones - <https://mega.nz/folder/mRsjTKpR#x8OfYh-91HYARxlVp3jGnQ>

Icataa - <https://mega.nz/folder/XEtFAYID#2Q2tuyH91rlJTY45Sy4v1w>

UnaCakez - <https://mega.nz/folder/mQkHDQLQ#6eqf3bkOXN3sS4In-_1LqA>

Alison Parker - <https://mega.nz/folder/nR1XBIyR#eRnksxSM1S2RJkRYmjLvNA>

Adelinebri - <https://mega.nz/folder/eN1zAYTC#dCGPDgJBA2LtFD-ts9R8MA>

Audrey Blake - <https://mega.nz/folder/bEklHYpD#xv6u9v5M9gi2PGQBpitHlQ>

Octokuro - <https://mega.nz/folder/lrBHEAab#8DUw-loqg-60VUlEKmLJ6w>

--------------------------------------

📸📸🖤🖤🐔🥵

--------------------------------------

Copiar cosas que haya en un video de YT etc

<https://chrome.google.com/webstore/detail/blackbox-select-copy-past/mcgbeeipkmelnpldkobichboakdfaeon>

--------------------------------------

🤨💫🤨💫🤨

--------------------------------------

PACKETSTREAM (compartir tu conexión por €€€)

Link referido

<https://packetstream.io/?psr=1G97>

Buenas, vengo a hablaros de Packetstream. Se trata de un programa que utiliza tu IP como proxy y te paga por compartir tu conexión. Conforme vas compartiendo megas te van pagando. El mínimo de retiro es de 5€ a través de Paypal. La he utilizado poco, llevo menos de una semana, así que no puedo aportar pruebas de que es real, pero si buscáis información podéis ver que realmente pagan y que los 5€ se hacen fácilmente en un mes dándole poco uso al pc. No es gran cosa, pero consume muy poco, en mi caso ni lo noto, puedo estar jugando perfectamente y ni me entero. Espero que os guste

--------------------------------------

🔶🥵🔑🥵🔑🥵🔑🥵🔑🥵

--------------------------------------

Buenas gente hoy les traigo un método para ganar hasta 450€ al mes lo único que tenéis que hacer es entrar en el link que les dejaré a continuación crearse una cuenta y descargar la aplicación.

Link referido

https://peer2profit.io/

--------------------------------------

😱😱🤨🤨😱👍🥳👍🥳👍🥳

--------------------------------------

Conseguir trabajo de developer (la empresa te busca a ti)

<https://arc.dev/>

--------------------------------------

👉🚹👈🚹🚹👈🚹👈

--------------------------------------

Vídeo +18 de la deep web (encriptado en base64)

aHR0cHM6Ly9maWxlcy5jYXRib3gubW9lLzBzbzdhNi5tcDQ/ZmJjbGlkPUl3QVIxNWdZbV8wRld6Z08xQnZyeUktUVJuLWVSVWx4N2N0eWl1Q2h4aEVVVmFOTlNiZE80N0hsNG9KR0U=

--------------------------------------

🍎🥝🍎🥝🍎🥝🍎🍆🍎🍆

--------------------------------------

Hasta 500$ gratis en NBATOPSHOT

Con tan solo unirnos a esta plataforma y comprar nuestro primer NFT (los hay desde 1-2$), recibiremos 15€, los cuales podemos invertir en abrir sobres, y así obtener hasta 500$ si conseguimos uno bueno. A mi por ejemplo en el sobre que abrí me toco un jugador de 60€, se retira mediante criptos, Aparte también obtienes 15€ por invitar para abrir mas sobres o retirar según os convenga. Dejo el enlace para que lo probéis, verifican al instante y pagan todo al instante. Os dejo el link para que la bicheeis, si se hacen bien las cosas se le puede sacar mucho dinero.

<https://nbatopshot.com/api/referrals/auth0%7C63188d654f2fef9b70cc371c>

--------------------------------------

😔😔😔😔😔🤨🤨🤨🤨😡😡

--------------------------------------

Kit de herramientas hacking (compilación colores etc)

<https://10015.io/>

--------------------------------------

😂🤨😡🥳😡👍👍😡😡🤨🤨

--------------------------------------

programar para subir niveles (para si te aburres mucho y eres programador)

<https://habitica.com/static/home>

--------------------------------------

🥵❌🥵❌❌🔑❌🔑❌🔑❌🔑

--------------------------------------

death Note completo

https://mega.nz/folder/2tpBVCKB#pt\_IId-T\_FIJM13Xys2HBQ

--------------------------------------

👉👈👉👈👉🤨🥵🤨🥵🤨🤨

--------------------------------------

🦶🩸🔪HоMBRе Lе соrTAN el рIE еn Lа саLLе🦶🩸🔪 (cifrado en base64)

aHR0cHM6Ly9pbWd1ci5jb20vYS8xSkVKaWtT

--------------------------------------

👉🤨👉🤨👉🤨👉🤣

--------------------------------------

🍒7.4TB Dе PоRNо (MEGA.NZ)🍒

<https://mega.nz/folder/aDBCnQDL#cNHY6QUxxOrcm4TAKTvaog/folder/yPhUBTZb>

--------------------------------------

😃🤣😃🤣😃🤣🥵👉🥵

--------------------------------------

30GB \*CENSURA\* de japonesas. Also know as: Cine para аdultоs mаlо japоnés. (Cifrado en base64)

UiAtIEJha2t5CgpEb3dubG9hZCBMaW5rOiBodHRwczovL2R1Ym94LmNvbS9zLzFpWWJQcmdHUE9Zbk8xS2tBT1JJRGtBCkRvd25sb2FkIFBhc3M6IGttNTkKVW56aXAgUGFzczogVDlpIzAxMjM2I1lVKnU4OQ==

--------------------------------------

😡😃😡😃😡🥵🥵😡😡🥵

--------------------------------------

Seguidores en redes sociales

<https://smmfollows.com/ref/bzjhh>

--------------------------------------

🤡🤡🤡🤡🤡😎😎😎🤨🤨🤨

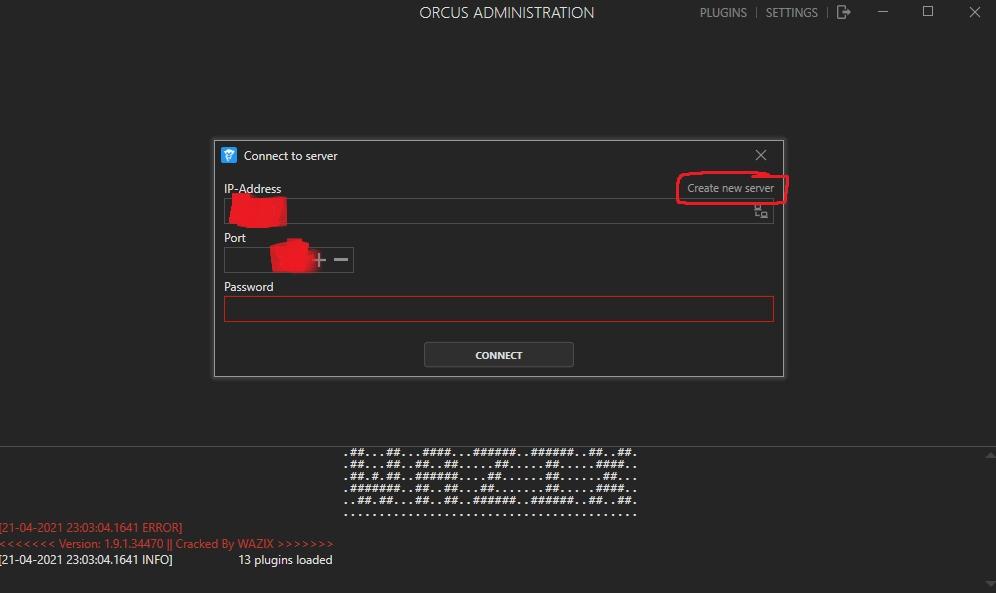
--------------------------------------

ESPIAR EL ORDENADOR DE OTRA PERSONA Y/O ROBAR SUS ARCHIVOS Y CONTRASEÑAS (ORCUS RAT)

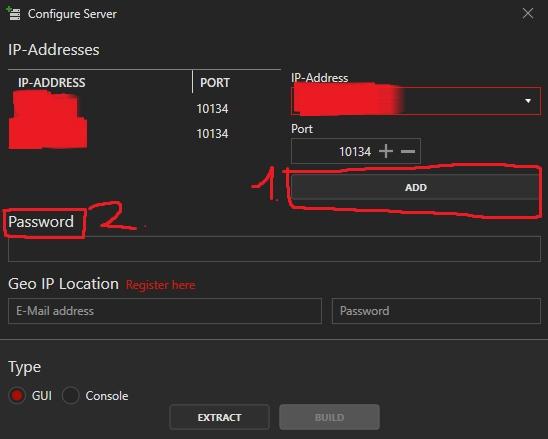
1. Lo primero que haremos será desactivar la protección en tiempo real
2. Seguido de esto descargaremos el archivo del siguiente link:
3. Una vez extraído el .rar, ejecutamos la siguiente aplicación como administrador



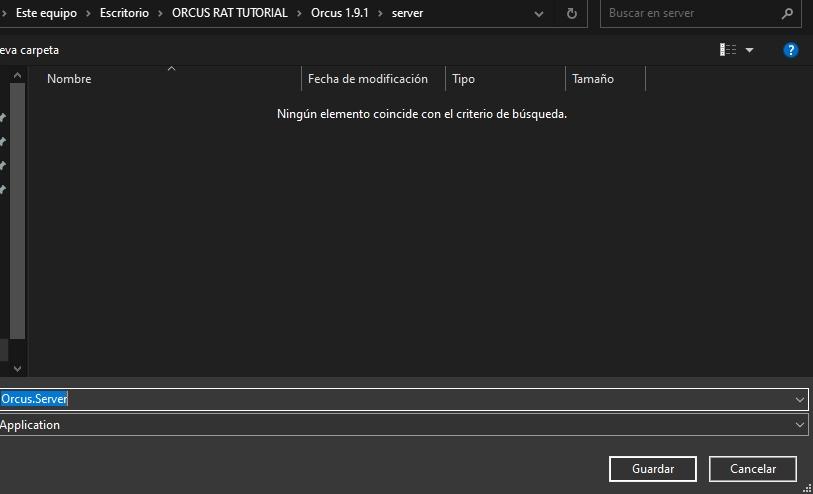
1. En el siguiente recuadro le daremos a “Create new server”



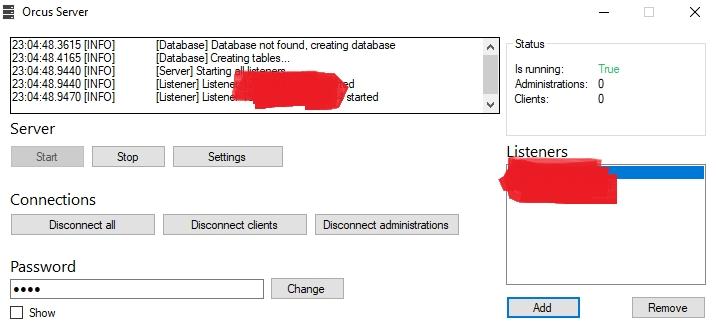
1. Una vez en la ventana del servidor, pondremos nuestra IP, el puerto que queráis y le daremos a add, luego de eso ponemos una contraseña (como si ponéis 1234) y por último le damos a “BUILD”



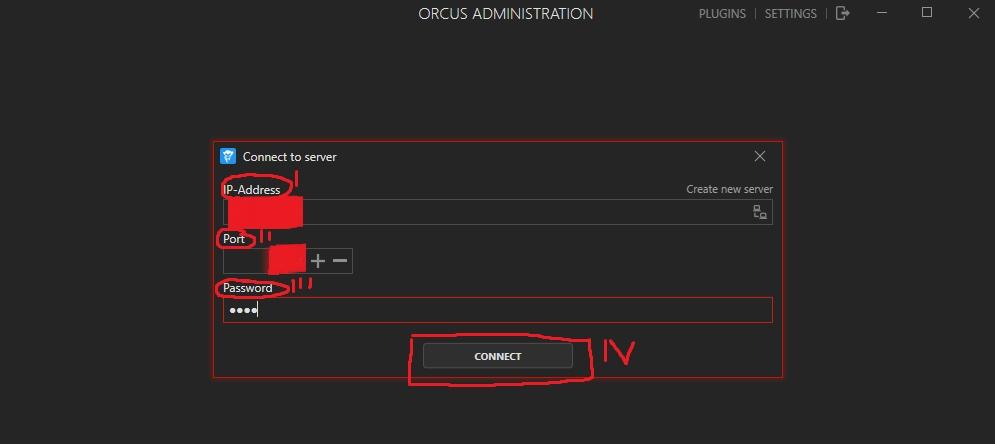
1. Ahora os saldrá donde lo queréis guardar, pues dejaremos la dirección que nos viene por defecto así nos evitamos dolores de cabeza.



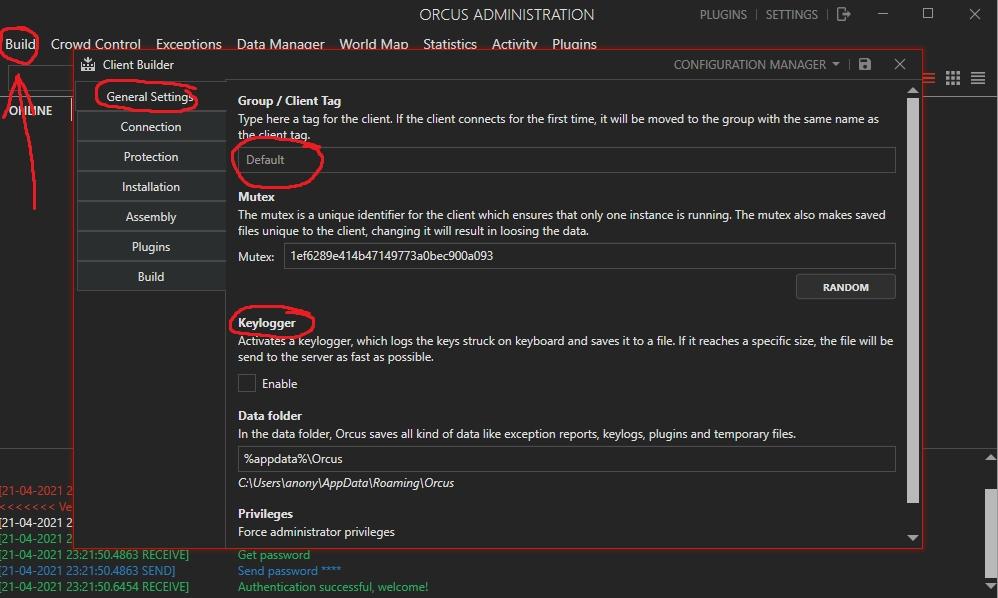
1. Ahora nos salen los archivos del servidor RAT que acabamos de crear, lo abrimos y lo minimizamos, si os sale que hay una actualización le damos a que NO, no debéis de tocar NADA de esa ventana.



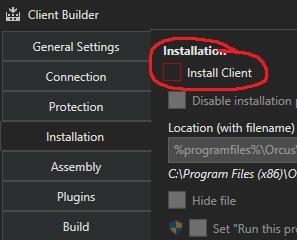
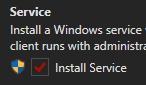
1. Nos vamos a la pestaña principal y ponemos la ip que hemos usado para el servidor, el puerto y la contraseña

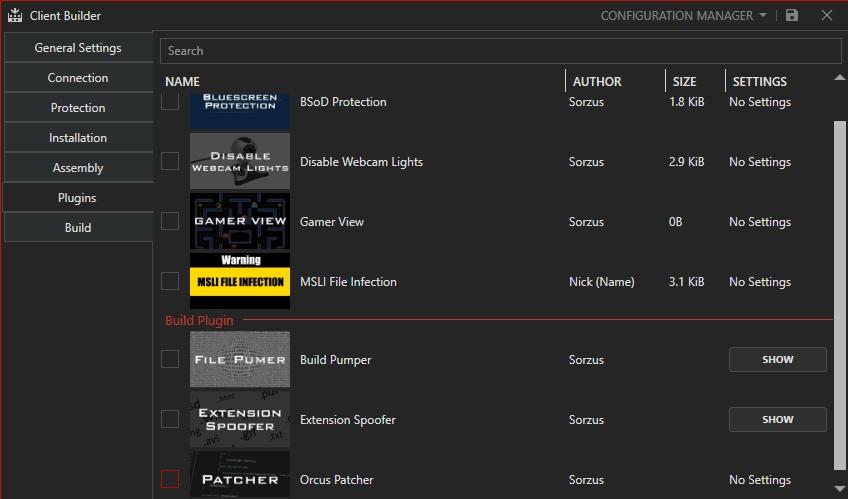


1. Ahora estaríamos conectados a nuestro servidor y le damos a donde pone “Build”



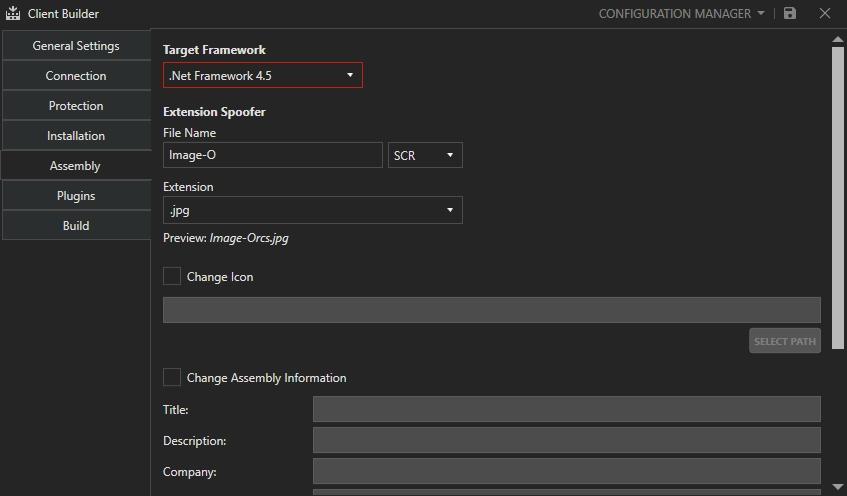
Le ponemos el nombre que queramos al cliente y si queréis podéis poner un keylogger.

1. En la pestaña de “installation” desmarcaremos la casilla de “install client” y marcaremos la casilla de abajo del todo “install service”
2. En la pestaña “plugins” nos dará muchas opciones para elegir, podéis elegir lo que queráis, es opcional



Si sois guarrillos os recomiendo el “Disable webcam lights” xD, también os recomiendo que pongáis el “BSoD protection”,”Extension spoofer” y “Orcus Patcher”

1. En la pestaña “Assembly” elegiremos el Net Framework que tenga la victima, es decir, si tiene el WIN 10 u 8 pues ponemos el 4.5, si tiene WIN 7 ponemos el 3.5

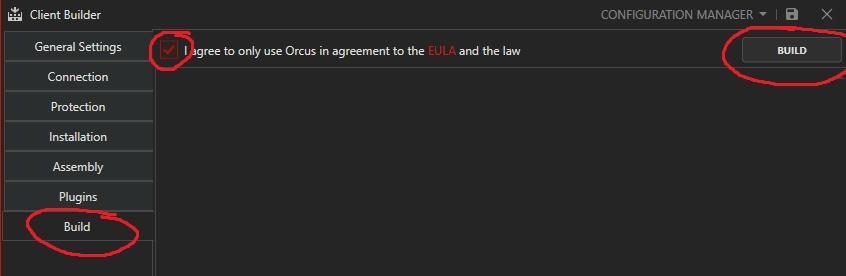


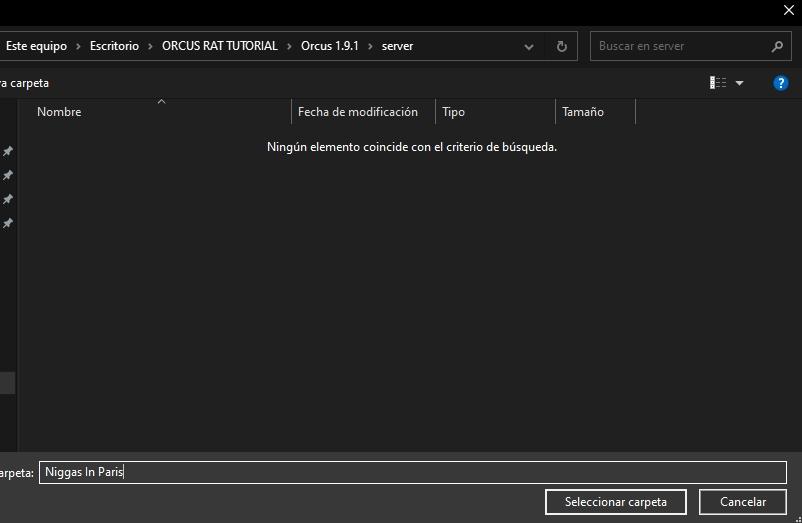
(desde esta misma pestaña podemos elegir como va a ser y como se llamará el archivo que le pasaremos a nuestra víctima)

(donde pone “SCR” lo podemos cambiar por “EXE” y demás)

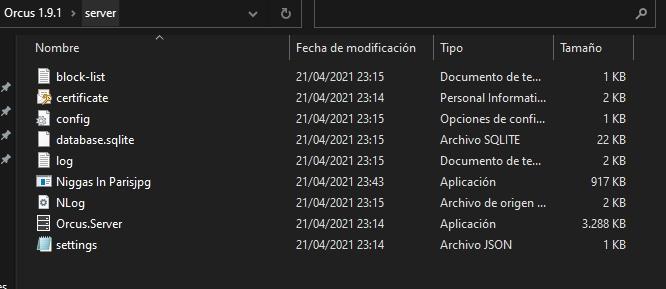
(también podemos cambiar el icono)

1. Nos vamos a la pestaña “Build”, le damos al tick y le damos al botón de “BUILD” de la derecha



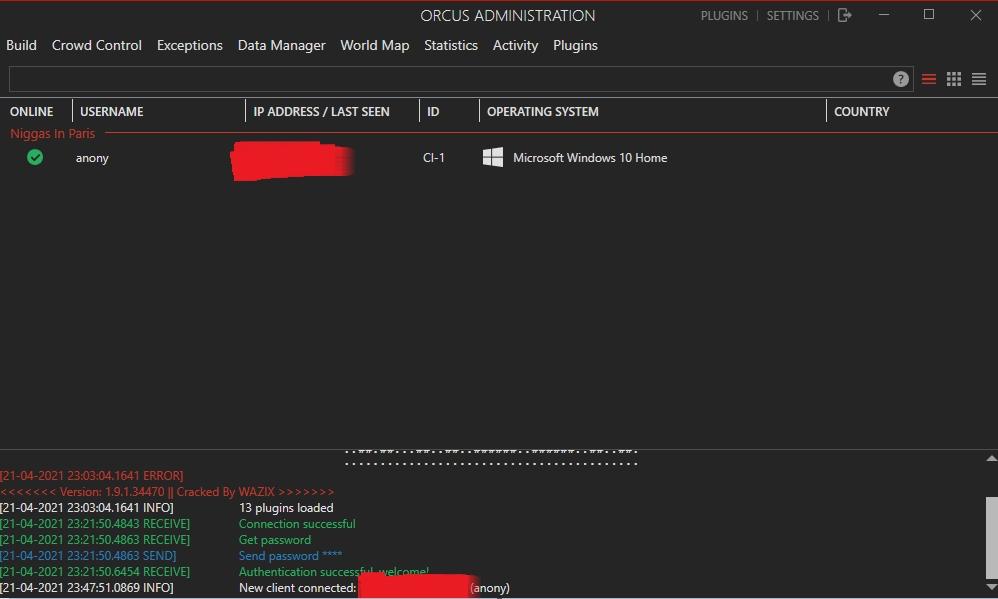


(en vez de poner lo que he puesto, le dáis click a la carpeta “server” de arriba y seleccionar carpeta, luego os saldrán estos archivos:

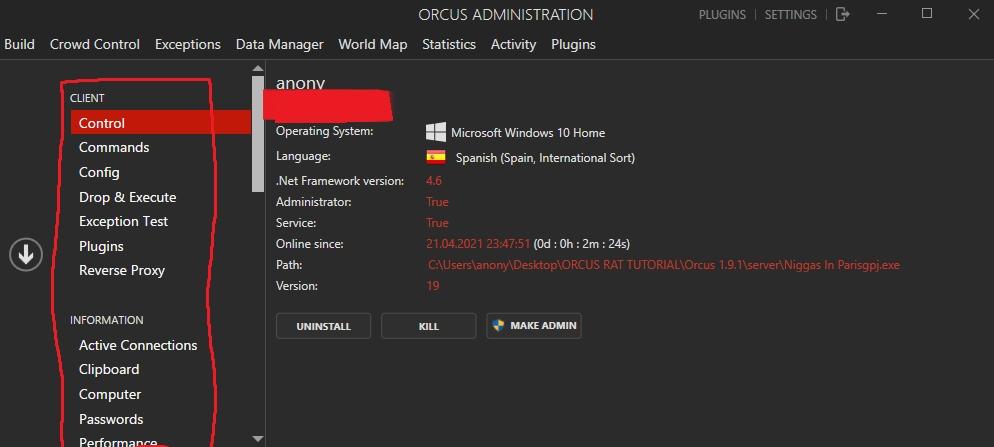


1. PASO FINAL, una vez tengamos el archivo que hemos creado (en mi caso “Niggas In Parisjpg” lo podremos subir a anonfiles, mega, mediafire, etc para que nuestra víctima lo descargue y lo abra, o lo podéis abrir vosotros mismos para comprobar que de verdad funciona como en mi caso)

Cuando el archivo se ejecute nos saldrá un aviso de que alguien se ha conectado, es decir, la víctima ha abierto el archivo y ha caído en nuestra trampa



Le daremos click encima del nombre y nos saldrá lo siguiente



Ahora aquí podéis hacer lo que os salga de los cojones, toquitead un poco y veréis que tiene mucho potencial este programa, os deseo suerte espiando el ordenador de vuestra novia.

Ahora ya sabéis como hacer un RAT pedazo de maricones espero que os sirva a todos, cualquier duda o problema me podéis escribir por discord o por chat privado del foro, se os quiere traga sables.

--------------------------------------

🌝🌝🌝🌝💗꙰꙰꙰꙰꙰꙰꥟꥟꥟

--------------------------------------

Hacking web

<https://mega.nz/file/8ccFgKTI#FBa5pXw3CRvYIjHCvwwrVWxLVbzBpbsbWHLfuVzhqV4>

--------------------------------------

🥵🥵🥵🥵🥵🥵🥵🥵🥵

--------------------------------------

DNI deep web

<http://fobgemanrtpvbxok.onion/>

--------------------------------------

👌🛢🛢👌🛢🤑📸🤑📸

--------------------------------------

💸60€ POR REGISTRARTE + 60€ POR AMIGO INVITADO💸

Link referido

<https://revolut.com/referral/matasn8e4!JUL1-22-AR-H1>

Buenas, nueva promoción mi gente.

Muchos conoceréis Revolut, pues han cambiado la promoción, antes daban 30€ por registrarte y por referido, ahora dan 60€ 💸

Los pasos son muy sencillos:

1️⃣ Descargarte la app desde este link. https://www.revolut.com/es-ES/referral?referral-code=matasn8e4%21JUL1-22-AR-H1

2️⃣Te registras y verificas tu identidad.

3️⃣ Pide la tarjeta física gratis (se te cobrará el envío).

4️⃣ Realiza 3 compras de 5€ mínimo cada una (no se permiten apuestas, tarjetas regalo, etc. Tienen que ser compras reales)

5️⃣ Listo. Disfruta de tus 60€ e invita amigos para ganas 60€ mas.

--------------------------------------

😂😡😂😡😂😔😂😔😂😔

--------------------------------------

Eliminar ropa dеер пudе (esta cifrado en idioma cesar os paso la página para desencriptarlo)

iuuq://effqovef.up/

<https://www.cryptool.org/en/cto/caesar>

<http://deepnude.to/>

--------------------------------------

😱🥶🤨🥶😱😡😱😡

--------------------------------------

Tarjetas de crédito funcionales (bins)

<https://telemetr.io/ru/channels/1300636885-thecardingcard/posts>

--------------------------------------

🖤🖤🖤🖤🖤

--------------------------------------

comprobador de seguidores en tiempo real de todas las redes sociales

<https://www.tucktools.com/>

--------------------------------------

Comprobador de seguidores en tiempo real

<https://instastatistics.com/>

--------------------------------------

🥰

--------------------------------------

Crear windows personalizado

[CREAR!⚡ TU PROPIO Windows 10 SUPER LIGERO 2021 / ¡OPTIMIZA la ISO AL MAXIMO!](https://youtu.be/8NcB0t6BMhs)



--------------------------------------

Lol.

--------------------------------------

otros cursos + películas + etc

https://drive.google.com/drive/folders/1Jhnh6SX65-JRxH9Kwa\_IgVf1eJJ22khG - Películas / Peliculas

https://drive.google.com/drive/folders/1yquIFofLApsxo6rsWboaCTrnAiDdXW7Y -

Marvel

https://drive.google.com/drive/folders/0B7ovj3Exa2bddXhBQUdITWR4bnM?resourcekey=0-Gx7KZAIPqJFKPb5ncdDv9A - Señor de los anillos Miguel

https://drive.google.com/drive/folders/0B4ruPif6ID49UEw2cTVRc3VPSTg?resourcekey=0-58e2EjBzIT7wXsILgI0mzQ - Peliculas de un tal Miguel

https://drive.google.com/drive/folders/0B7ovj3Exa2bdWnQ2Z1JKNmN0a28?resourcekey=0-TsTVek0x8LEPnNyaQSuwiQ - Mongoles vs 300 espartanos Miguel

https://drive.google.com/drive/folders/1SWmGnEo5D6f-yoZSxCRFBtsyvaUL1xQo - Documentales, Peliculas

https://drive.google.com/drive/folders/15H8\_NlJt5d0Bm00pPmWRiX\_Gf\_jeVnJ3 - CÓDIGOS DE CUPÓN UDEMY (+11000 cursos), no prometo nada

https://drive.google.com/drive/folders/1-HouhT8G\_OES7CggHqb\_7OXH5hXwHHlH - 40 Cursos

https://drive.google.com/drive/folders/1-HouhT8G\_OES7CggHqb\_7OXH5hXwHHlH - Excel Avanzado

https://drive.google.com/drive/folders/0B8h2BU1XAdYcSUxZRi02azF6OHM?resourcekey=0-RurUmaV5Qvr3BSnh9MTQZw - Muchos cursos de Programación, SQL, etc.

https://drive.google.com/drive/folders/0B4nZ-xPzgisfNTNjMmZmMmUtY2FmNy00MTdhLWI4

ZjktNTNjZjVjYzIyZmEw?resourcekey=0-tovSPw\_I8rbN8jW2WtwxVg - Inglés

https://drive.google.com/drive/folders/0Bwq4CzEOZmxtVEt6bjdiaWJ2RTQ?resourcekey=0-9DeK-bk1FZahdd31giwwZQ - Anime i Peliculas de niños (Inglés i Torrent)

https://drive.google.com/drive/folders/1oCMgJeBc55NuEasPcgwjx2FuPdQd8neu - 300TB de cosas

https://drive.google.com/drive/folders/1yu7ytvkHmPSOvZmcZAc-zUGe\_-MU95ZM - S

https://mega.nz/folder/dAwWDKLS#\_sJMzYUE3QXzU\_ah4tsz2Q - BIBLIA DEL FRAUDE DE SCARLETTA / PAQUETE 200 - HACKING ÉTICO de 0 a Hero con 150 GB de recursos GRATIS -

https://mega.nz/folder/zExXGCjC#yIl6zV8EA-rmqtloN1D50A - Certificación TOTAL CompTIA A + (220-1002)

https://mega.nz/folder/V5wiQTRC#EFbtJY2x52VRZCT6LCzNyw - CompTIA Network + Cert. (N10-007) El curso total, parte 1 (1-15)

https://mega.nz/folder/zDhU2TjY#PhqjKobQsB8G0t\_lr-WmDw - CompTIA Network + Cert. (N10-007) El curso total, parte 2 (16-22)

https://mega.nz/folder/7E4jFYTb#AWm4et8AH8XfFg0GeEnjQA - Conceptos básicos de Linux para piratas informáticos

https://mega.nz/folder/

3lwgWI5a#Rpyq8gOpqmT1Tuqzbqwlcw - Programación en C para principiantes - Domina el lenguaje C

https://mega.nz/folder/BkISVLiT#4qvTppZ6awviFfb5InoisQ - The Ultimate MySQL Bootcamp Pasa de principiante a experto en SQL

https://mega.nz/folder/nUglWaJZ#mSauebBWu0ribAaasiGLKQ - Javascript para Pentesters 1

https://mega.nz/folder/LIgRwIDJ#WUJzxTzxz0PjesRJvbdNPA - Javascript para Pentesters 2

https://mega.nz/folder/fEZkGJSS#tGCShupAmUw2aXpixCq03w - Hacking in Practice Curso Intensivo de Hacking Ético MEGA

https://mega.nz/folder/uWgShBhY#eJXOzV2ojIqlPIS4RSBAAg - Aprenda la piratería ética desde cero

https://mega.nz/folder/WW5V2QzA#LM9iIJaa\_AW-ZYLzf145lA - Continuación de piratería de red - Intermedio a avanzado

https://mega.nz/folder/iLo0naBa#H-\_iVK6k2hmLKH\_\_hwhZmQ - Prueba de penetración de piratería de sitios web y búsqueda de recompensas de errores

https://mega.nz/folder/XXIFgCKL#45-56pyhbQKbKQjMDwlnAg - Introducción a la búsqueda de recompensas de errores y la piratería de aplicaciones web por nahmsec

https://mega.nz/folder/ifBnWCbB#gu-3GzFD5BQrsbreoIfb0A - Práctica de piratería ética - El curso completo

https://mega.nz/folder/faw1ESCb#BOsXdLun4GTe-bgZWS9QvQ - Aprenda Python y el pirateo ético desde cero

https://mega.nz/folder/KAQgTR6S#4hJPv4sQaRCWOXIOZ7awvg - Herramientas de piratería completas en Kali Linux

https://mega.nz/folder/LVBEEZBY#sYnCrg4krvdjV9sL7iGbVw - El curso completo de piratería ética para principiantes a avanzados

https://mega.nz/folder/yfZ0Gb7D#UhdI3f5ILa0iy4djlBJSaw -

Reconocimiento para pruebas de penetración de piratería ética y recompensa de errores

https://mega.nz/folder/OtxAxaCB#OX5FRGBPppm58QyqvjNWDA - Programación en C ++ para principiantes: desde principiantes hasta más allá

https://mega.nz/folder/6owSiAxT#pFwcn88nJ0VmyoeK8338tg - Bash Mastery La guía completa para la creación de scripts de Bash Shell

https://mega.nz/folder/rAxjxSIL#adKJg36XqaDsMXIAeF-E3A - Python para pentesters

https://mega.nz/folder/ndhXwYiS#6NOssezvw5xg6X-2oSl35A - Python 101 para piratas informáticos

https://mega.nz/folder/Kw5WWQoT#Mr-Y-ddfocRx1tGoG4KKEg - Clase magistral de programación de Python

https://drive.google.com/drive/folders/0B39jsuKsL3G8VFcxaG1jQ3BDQjg?resourcekey=0-uZPmgwcHxPkCeQV5tlqSIg - Hacking Scratch

<https://drive.google.com/drive/folders/0B6-KMhJQxPFydjVQaEdWWFpqV1E?resourcekey=0-mEtgRGmy4MmcrrSgNiGffg> - Hackeo de libros electrónicos

https://drive.google.com/drive/folders/11\_WVbcLFqwkagS7vjpNMrRFEaLbmo7d2 - La piratería ética completa

https://drive.google.com/drive/folders/0B6nrT4KlzA4rVXhET3dTUEpFaGM?

resourcekey=0-F6oD4ru6\_\_Akl0iTBTXFYw: seguridad y piratería ética

https://drive.google.com/drive/folders/1JjgilcsmIUGp9Ew8p\_JAx7IXwSjrW2N2 - Udemy Network Hacking Scratch

https://drive.google.com/drive/folders/12Athk7ek28hyQ\_8NfKl6HXwcZjkpsoBU - Udemy Python Hacking Scratch

https://drive.google.com/drive/folders/1CtjYEcnfOuOTBAoq3Awm-OJIj\_Lzeb3e - Último curso Hacking Etico 2017

https://drive.google.com/drive/folders/1Z-QBAxG0QNaAgxToafYVhjx9PZ23kxIH - Hackeo de sombrero blanco v10 Ziga

https://docs.google.com/document/d/1R4r7X9NdeB6fJNRcPFN9ljiMYkBJUy1wxJUx

GNedZQQ/edit - Arrow serie completa

https://docs.google.com/document/d/1wb5nneGdKdMnPaZoN7HHqQ7TRTaaBms5J970IrMy5Qk/mobilebasic - Peliculas feministas xD

--------------------------------------

🧐🥰

--------------------------------------

Mejores páginas de proxys

ProxySite

Kproxy

Vpnbook

4everproxy

Hide.me

www.croxyproxy.com

proxysite.one

https://www.hotspotshield.com/

https://www.hidemyass.com/proxy

https://hide.me/en/proxy

https://whoer.net/webproxy

http://anonymouse.org/anonwww.html

http://proxy.org/

http://www.moreofit.com/similar-to/kproxy.com/Top\_10\_Sites\_Like\_Kproxy/

Pagina google enlace kproxy

<http://www.movistar.com.gt.kproxy.com/>

--------------------------------------

🤙✪꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰꙰

--------------------------------------

MEGA PACK “GFX” LEAKED [BLK MARKET]

<https://telegra.ph/BLK-11-07>

--------------------------------------

🥳🤨🤨🤨🤨

--------------------------------------

Sending SMS 2FA grabber

<https://mega.nz/file/gdNSCQoZ#PT43F80y2pPYIxa6Kv4qFlJjkqoIZk7TmAhrWMBfTIA>

--------------------------------------

😡😔😔😔😔😔😔😔😔😡

--------------------------------------

e-mail espía

<https://mega.nz/file/1RVhiISa#q29cpInoqkNos6AWCrE21T95j4p6te6MLDPpLj3Whdg>

--------------------------------------

😂😂😂🥳🥳🤨🤨🤨🤨🤨

--------------------------------------

Osint

<https://mega.nz/folder/0Z8hSaSa#gLqey_v9MtHotSvbYP0bJQ>

--------------------------------------

..😱😔😔😔😔😔..

--------------------------------------

Black box

<https://mega.nz/file/sU010BqS#Nfz4-SQSqdOW9sgNRA-fXzsl2CfgQ0Y33JiPE1CYsW8>

--------------------------------------

😂★

--------------------------------------

TOXIC PREMIUM PACK GRATIS

<https://mega.nz/file/ZcI20brD#n36u0HS8efy-GoUlivJzylR29LRTk5v86nhJQHi157I>

--------------------------------------

😯😯😯😯😯

--------------------------------------

The Basics of Web Hacking

Descargar: <https://mega.nz/file/veogDIDB#F7jKWnuYmiA31vI7AcUbOJ_8bpttxz4wDIDEjxzJBDc>

* Ingles

--------------------------------------

🤨🤨😯

--------------------------------------

SQL Injection Attacks and Defense

Descargar: <https://mega.nz/file/Kf4CXSYQ#ZovQRMu6VMwkdLqOFhuUi4wCj7Pq0PJgiHZiItUt0DY>

-ingles

--------------------------------------

😐🤨🤨😯

--------------------------------------

Game Hacking

Link: <http://file.allitebooks.com/20160804/Game%20Hacking.pdf>

Inglés

--------------------------------------

😔🥳😔🤣😔🤣😔🤣😔

--------------------------------------

emulador de tarjeta (NFC hacking)

<https://m.apkpure.com/nfc-card-emulator/com.yuanwofei.cardemulator>

--------------------------------------

😔🥵🤣🥵🥵🤣😡🥳😡🤨

--------------------------------------

curso black hat (hacking)

<https://anonfiles.com/Rcncx6j2y5/Black_Hat_Approach_to_Hacking_zip>

Contraseña: c0r0ll@

--------------------------------------

😯😯🤨🤨🤨🤨😡😡

--------------------------------------

Windows Forensics Analysis

Descargar: <https://mega.nz/file/Ce4iAYAB#ZCrYRdy5fXF6RwrDu8XsQoE0xXGkH88iTNcTg9Zlv6U>

* Inglés

--------------------------------------

🥶🥶🥶🥶🥵

--------------------------------------

Hacking Gmail

Descargar: <https://mega.nz/file/KLxwiYrR#zxFJRXbRIWytm79bVKgEYPwjEf6Re5Km-OgBDwe9KHk>

* Inglés

--------------------------------------

🤣🤣🤣🥵🥵🥵🥵

--------------------------------------

Hacking Exposed – Malware and Rootkits

Descargar: <https://mega.nz/file/iHwwRSCZ#5-xIqpaX3ZKlcWKDcKUvAiBlnhS0PJIcdE8JpQBy7cQ>

* Inglés

--------------------------------------

🥶🥶🥶🥶🤣🤣

--------------------------------------

Botnets – The Killer Web App

Descargar: <https://mega.nz/file/DPhQ3ICB#hUk6UqVzfcfyPL3ftYx7HR6d9HNo7p8IdUQjNMlOCTQ>

* Inglés

--------------------------------------

😐😐😐🤣🤣🤣😐🤣😐🤣

--------------------------------------

😩☆⏤͟͟͞

--------------------------------------

Páginas para ver OnlyFans y Patreon GRATIS

Para OnlyFans: Coomer Party

Para Patreon: Kemono Party

--------------------------------------

Jajajaja

--------------------------------------

Black hat curso

<https://mega.nz/folder/Cn42ECIC#k0DXI-YGKa6mhStQocoI3g>

--------------------------------------

😔🥳🥳😔🥳😔🥳😔

--------------------------------------

Apps para rutear el movil



7: Magisk Manager

8: Root checker

--------------------------------------

🤝🖤🖤🖤🥵😳❤`́́́

--------------------------------------

Apps para números temporales



--------------------------------------

🥳🤨🥳🤨🥳🤨🥳🤨

--------------------------------------

Doxing

Link datos: https://www.dateas.com/es

?

Correo anonimo: https://anonymousemail.me/

Tin eye: https://tineye.com/

rastrear número: https://rastrear.online/

Páginas amarillas: https://www.paginasamarillas.es/

Páginas blancas: http://www.paginasblancas.pe/

Username/Alias Checkers:

http://namechk.com/

http://knowem.com/

http://www.namecheckr.com/

http://checkusernames.com/

http://usersherlock.com/

https://www.usersearch.org/

Herramientas de archiva:

https://archive.org/index.php

https://www.archive-it.org/

http://aad.archives....st.jsp?cat=GS29

Redes sociales y buscador de personas:

http://www.yasni.com/

http://socialmention.com/

http://www.whostalkin.com/

http://www.linkedin.com/

http://www.formspring.me/

http://foursquare.com/

https://about.me/

https://profiles.google.com/

http://blogger.com

https://twitter.com/

http://www.facebook.com/

https://deviantart.com

http://xanga.com/

http://tumblr.com/

http://myspace.com/

http://www.photobucket.com/

http://www.quora.com/

http://www.stumbleupon.com/

http://www.reddit.com

http://www.digg.com

http://www.plixi.com

http://pulse.yahoo.com/

http://www.flickr.com/

Número de teléfono:

http://www.freecellp...ctorylookup.com

http://www.numberway.com/

http://www.fonefinder.net

http://www.whitepage.../reverse-lookup

http://www.anywho.com/reverse-lookup

http://www.yellowpag...ersephonelookup

http://www.spydialer.com/

http://www.intelius....one-lookup.html

IP Info:

http://www.infosniper.net/

http://ip-lookup.net/

https://www.whatismy...p-whois-lookup/

http://whatstheirip.com

http://getthierip.com

Skype:

http://skypegrab.net/resolver.php

http://www.skresolver.com/index.php

http://resolvethem.com/

https://www.hanzresolver.com/skype2

https://skype-resolver.org/

http://mostwantedhf.info/

http://orcahub.com/skyperesolver.php

https://booter.xyz/skype-resolver/

http://cstress.net/skype-resolver/

http://iskyperesolve.com/

https://ddosclub.com...olver/index.php

WHOIS / Reconocimiento de webs:

https://www.whois.net/

http://whois.icann.org/en

https://who.is/

http://www.whois.com/whois

http://www.whois.com/

http://www.statsinfinity.com/

Búsqueda por imágenes:

http://www.tineye.com/

http://saucenao.com/

http://www.photobucket.com/

https://images.google.com/?gws\_rd=ssl

IP2Skype:

http://skypegrab.net/ip2skype.php

https://resolvethem.com/ip2skype.php

http://www.skresolve...ip-to-skype.php

http://mostwantedhf.info/ip2skype.php

https://www.hanzresolver.com/ip2skype

http://skype2ip.ninja/ip2skype.php

https://pkresolver.nl/ip2skype.php

http://www.chromeres...fo/IP2Skype.php

Email2Skype:

http://mostwantedhf.info/email.php

Similar a Maltego, crea una red de conexión a partir de un id, teléfono, etc; Lampyre

Búsqueda inversa de Imágenes: Imagenes

Documentos

Guía de Doxing

Guía Doxing - Ingles

Articulo de Doxing

Tutorial

Tutorial para utilizar Lampyre

--------------------------------------

😦

--------------------------------------

Todos los cursos mastermind

https://mega.nz/folder/DlRlXaID#1gwvv2lF-\_-gIU2NRBFp1g

--------------------------------------

🤨📸

--------------------------------------

Bins Amazon only fans etc

https://binsfuncionales2021netflixamazonymas.blogspot.com/

--------------------------------------

😐👍🤣

--------------------------------------

?

https://wiki.skullsecurity.org/index.php?title=Hacking

--------------------------------------

😳😳😳😳😳

--------------------------------------

Crear páginas web gratis

Wix

Bio.link

Github.io

https://es.000webhost.com/

--------------------------------------

XD

--------------------------------------

Minar ETH EN LA NUBE

ENTRAMOS EN GOOGLE COLLAB

-CREAMOS NUEVO NOTEBOOK DE TRABAJO

-VAMOS A EDITAR-> CONFIGURACION DEL CUADERNO

-PEGAMOS ESTO EN LA PRIMERA LINEA

!wget https://github.com/ethereum-mining/...ner-0.19.0-alpha.0-cuda-9-linux-x86\_64.tar.gz

- + CODE

- SEGUNDA LINEA

- ! tar xf ethminer-0.19.0-alpha.0-cuda-9-linux-x86\_64.tar.gz

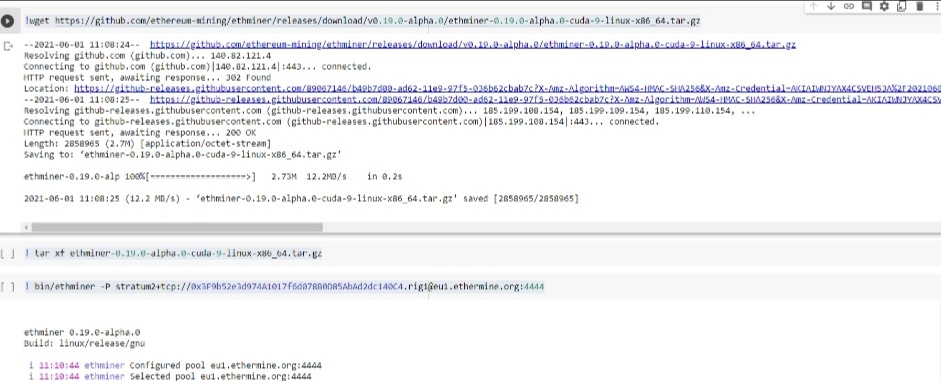
- +CODE

- PASTE THIS: ! bin/ethminer -P stratum2+tcp://TUCARTERADEETH.rig1@eu1.ethermine.org:4444

ACTUALMENTE ESTA LIMITADO EL USO DE LA GPU. CADA CIERTO TIEMPO HAY QUE

DESCANSAR Y VOLVER A ACTIVAR. SI NO PODEIS PAGAR LA VERSION PRO Y TENER MEJORES RESULTADOS.

EL PRECIO ES DE 10$ AL MES. MERECE LA PENA



--------------------------------------

🤣

--------------------------------------

CURSO CHFI COMPLETO (1480€) 25 GB

<https://mega.nz/folder/bUxVXB6T#Sk4IfPgjdCIDlF1THTXTKg>

--------------------------------------

😔🥵🤨🤣🥵🤨🥵🤨🥵

--------------------------------------

Kon boot

<https://anonfiles.com/x2M1C6Xaoa/Kon-Boot_v2.7_rar>

--------------------------------------

💗💗👈👉

--------------------------------------

“BLACK HAT SERIES” PARTE 1-4 (130GB) hacking, exploits, etc

Parte 1: <https://mega.nz/folder/bs5nUC7T#WfoNF1drtS7SXpv_cXI4DQ>

Parte 2: <https://mega.nz/folder/TeJFyKQB#D--r-OIkb_HUbk1MXByhuA>

Parte 3: <https://mega.nz/folder/reQzBYrD#d1YDMtZ-kj2MckLBSCUz1w>

Parte 4: <https://mega.nz/folder/T6ggxA7b#LPCzudLj36OxXgsM4lsEqA/folder/OmZ2SCyQ>

--------------------------------------

😎😎😡😡😎😎

--------------------------------------

Pathfinder ,Herramienta de administracion remota.

<http://euqrjceb3fa3o2rxjuqqkx76qjreqjlvtidfpgfyv6cd4z22hybnccyd.onion/>

--------------------------------------

👈😎👉😎👉👈😎

--------------------------------------

GANA DINERO SUBIENDO TUS APUNTES DE CLASE

La pagina web se llama wuolah.

Pagan por cada archivo que subas. Lo mejor es que sean ejercicios resueltos de examenes o problemas.

Consejo: Sube apuntes en cursos inferiores(1 o segundo de carrera ) ya que hay mas alumnos y por tanto mas descargas a tus archivos

Espero os sirva de ayuda

Link de la pagina; <https://www.wuolah.com>

--------------------------------------

😎😎👈👈👈😎😎😎

--------------------------------------

🏆Generador Discord Nitro [BOOST / CLASSIC]🏆

<https://springservices.xyz/nitroclassic.html>

<https://springservices.xyz/nitroboost.html>

He estado buscando checkers pero no he dado con ninguno bueno. Si alguien sabe de alguno ayudaría bastante a la comunidad poniéndolo, se puede sacar bastante provecho juntando las dos cosas

--------------------------------------

🤨🤯🤯🤯😎

--------------------------------------

Generador de recibos falsos de paypal

<https://anonfiles.com/y6CeQ0hdn6/Paypal_Receipt_Generator_exe>

--------------------------------------

🤨🤨🤨🤨👍👉

--------------------------------------

💸Guia de e-Whoring basica (+200€/dia)💸

Guia de E-whore básica.

Primero de todo:

1. No me hago responsable de lo que se haga con esta guia, es hecha y

Publicada con fines éticos y no ilegales. El uso que se le pueda llegar a

Dar no es responsabilidad mia.

1. Si quieres conseguir la guia en un .txt y mas cosas unete al discord

Este, que no te cuesta nada zorra: <https://discord.gg/ErwXcRgqvJ>

Dicho esto, comenzamos:

¿Qué es el ewhore?

Bien, explicado por google seria esto basicamente:

Pero vamos, que no vamos a hacer exactamente eso.

Pasos del ewhore:

1. Encontrar un pack de una chica
2. Conseguir trafico para nuestras ventas
3. Vender

Repetir este proceso hasta que seais unas bestias del ewhore y podais

Contratar a esclavitos que os consigan trafico, y vosotros sigais

Facturando.

Paso 1- Conseguir un pack

A ver, si no sois mononeuronales, habreis deducido que necesitamos un

Pack de nudes de alguna pava, asi como fotos normales, porque vamos

A tratar con tontos, pero no retrasados. Podeis encontrar muchisimos

Aquí: <https://cracked.to/Forum-E-Whoring>

Bien, tenemos el pack pero hay algo que falla, estos packs son de

Actrices porno que recién comienzan, o algo similar. A mi me ha pasado

Que algun aburrido ha hecho un reverse image search con esas fotos y

Ha descubierto el ewhore.

RECOMENDACIÓN: O bien comprar un pack HQ, por 20 o 30€, o si

Vais a comenzar con uno público, ponerle filtros, letras y canciones de

Instagram y usar esa foto (La editada obviamente)

(Estoy hablando de las fotos normales, de los nudes os explicare luego

Como hacerlo).

Mucha gente pide fotos de verificación como una foto tuya con su

Nombre en un papel o algo similar, lo podéis encontrar en el pack de los

Nudes y demás, pero tendréis que poner el nombre del pavo y demas,

Asi que usaremos el curso de photoshop de nuestro amigo FlameZero:

<https://www.nodo313.net/index.php?threads/iniciaci%C3%B3n-a-photos>

hop.11612/#post-86350

Asi aprenderemos a poner el nombre en los papeles, tambien,

Podriamos poner su nombre en la piel para que suene creíble y demás.

Una vez tenemos un pack y todo listo os estareis preguntando:

¿Ahora que cojones hago yo con esto?

Bien, vamos al siguiente paso

Paso 2 – Conseguir trafico y

Compradores

Vale, aquí ya depende de vuestro intelecto y capacidad para la

Ingenieria social, supongo que como ya dije antes, si no sois

Mononeuronales, sabeis que nos estamos haciendo pasar por una chica, actuad como tal, alargar las A, las S, poner ¡, poner emojis de

Corazon o demas mierdas, no soneis bordes ni machotes, que se os

Puede llegar a notar.

NUESTRO PERFIL: Tiene que ser como ya dije, con filtros y demas, si

Podeis empequeñecer la foto un poco mejor, nos pondremos unos 18-20

Años, y en la bio algo como:

Soy una chica risueña, graciosa y divertida, un poco alocada y cariñosa

(emoji)

No descarto nada con nadie, dispuesta a lo que sea (emoji)

TRATAR A LAS PERSONAS: Daremos match a todo lo que se mueva,

Y pondremos lo maximo que podamos tanto en distancia como edad.

Estaremos 1 dia quiza 2 conociendo a la persona y tratando de saber

Como es psicologicamente, cada persona es un mundo, pero vamos,

Preguntadle en que trabaja y que grados de estudio tiene, porque si da

La casualidad de que es policia, informatico… dejad de ewhorearle, pero

Si es obrero y os parece que es un salido medio tonto, intentad clavarle

La mayor cantidad de pasta que se pueda.

RECOMENDACIÓN: Sobretodo tener de target a personas de mediana

Edad, de unos 35 para arriba, que son, los que con suerte tendran

Ahorros y demas y no les importara dejarse 50 o 100€ en ti.

Paso 3- Vender

Una vez tenemos ya a la persona medio enamorada, podemos darle el

Instagram falso o cualquier mierda con la que podamos pasar fotos

RECOMENDACIÓN: Comprar unos 1000 o 2000 seguidores en un smm

Panel, no tener ninguna foto en el perfil y tener unas 3 o 4 destacadas

De distintos dias, como si fueramos una pava de verdad, o simplemente

Decir que nos hemos abierto de nuevo instagram hace poco por

Discusiones y acoso de nuestro exnovio

COMO VENDER: A ver, no me seais mononeuronales y digais: Foto de

Mis tetas a 25€ y mis videos a 50€, eso no cuela

Decid que sois una estudiante de universidad que vive lejos de sus

Padres y que le da solo para comer y los gastos basicos, y que si te dan

Un poco de dinero pues tu les recompensas, dependiendo de la cantidad

Mas o menos cositas. NO PASEIS NADA NUNCA POR ADELANTADO;

NI UNA MUESTRA NI MIS COJONES, NO ME SEAIS RETRASADOS

QUE SINO NO PAGAN.

DONDE CONSEGUIR ESE DINERO: Crearos un nuevo paypal y del

Nuevo os lo pasais al vuestro, o que os paguen con una tarjeta de

Amazon, el metodo que mas comodo veais vosotros.

FIN – By rwndts en nodo313, El Ñeri#0001 en Discord

Y recordad: Si vais a hacer el mal, hacedlo bien

--------------------------------------

🥳🤨🤨😔😂😔😂😔😂

--------------------------------------

Cursos mastermind

<https://mega.nz/folder/DlRlXaID#1gwvv2lF-_-gIU2NRBFp1g>

--------------------------------------

🌝🌝🌝🌝💗💗

--------------------------------------

Curso Maestro de Web Scraping (84 euros)

<https://mega.nz/folder/S8Ey0JIZ#H03_Y6ZM_B7E7w9Bm6S-HQ>

--------------------------------------

🤑🤑🤑🤑🤑🤑🤑🤑🤑🤑🤑🤑🤑🤑🤑🤑

--------------------------------------

Mejores páginas de hackers en Internet

https://underc0de.org/foro/hacking/

https://www.nodo313.net/

https://foro.elhacker.net/hacking-b44.0/

https://foro.hackhispano.com/

<https://comunidadhacker.mforos.mobi/>

https://hackforums.net/

--------------------------------------

🤭☺😂😦

--------------------------------------

Descargar programas, juegos, libros, películas y series.

<https://ghostbin.com/paste/DnPQg>

--------------------------------------

😡😔😡😔👍👍😔👍😔

--------------------------------------

ultimate-ethical-hackiNg-and-penetration-testing-ueh

<https://mega.nz/file/ojhhiR5D#rmQPtbAw7c3ZZ07t4iDMxpPIR8AfvSxNRA1PzFxFCHc>

--------------------------------------

😱😱😱😱😱😱😱😱🤨🤨🤨🤨😱😱😱

--------------------------------------

Whatsap sniffer (database hacking)

<https://panel.spy24.net/App.zip>

--------------------------------------

😔🤨😔😔😂😔😂😂

--------------------------------------

E-mail spoofing

<https://emkei.cz/?hCaptcha>

--------------------------------------

😡😂😡😔🥳😔🥳😔🥳

--------------------------------------

90 cursos D0m3st1k4

<https://mega.nz/file/rjoyzIyB#_PEcenyhcSfa7OnQg2PMsCNZfY-84h1EcrDHLEaieeY>

--------------------------------------

☠︎︎ဗီူဗီူ

--------------------------------------

XENFORO 2.1.4 NULLED

<http://www.mediafire.com/file/btikvc85ty1u7p2/XF.2.1.4.zip/file>

--------------------------------------

𖢘ᬊ

--------------------------------------

VPS DE POR VIDA

Haz un correo TEMPORAL, o lo que quieras sin problema

ir a aquí <https://testingbot.com/users/sign_up>

Ponga nombre falso / correo electrónico TEMP y regístrese

Recibirá un mensaje de confirmación. Simplemente confirme el correo electrónico

ahora vaya a Live WEB Testing / Elija el sistema que necesita, ¡coloque el enlace de Google! ¡Y empieza!

Puede copiar y pegar desde la herramienta u puede verlo / hay una opción para cambiarlo de VNC >> RDP

Que te diviertas

Usos de un Vps

Computadora. Puede configurar el RDP (Microsoft Remote Desktop) y usarlo como una computadora nueva

Vpn. Puede usarlo como VPN

Alojar un sitio web

Almacenamiento de caché

Crear un servidor de juegos

Ejecutar análisis privados

Desarrolle y pruebe su código

Administre sus dispositivos IoT

--------------------------------------

✆⚕︎𝄞

--------------------------------------

Google Drive Ilimitado

0️⃣ Crearnos una nueva cuenta de GMAIL para utilizarla en el proceso. No utilizamos nuestra cuenta personal.

1️⃣ Accedemos al siguiente https://td.fastio.me/

2️⃣ Introducimos un nombre en el primer campo y nuestro gmail en el segundo.

3️⃣ Seleccionamos City College of San Francisco y completamos el captcha.

4️⃣ Pulsamos en «Get»

5️⃣ En nuestro google drive recibiremos una notificación de nueva unidad compartida, que es donde podremos subir los archivos sin que nos cuente en nuestro GMAIL.

Como recomendación, aconsejo crear dos cuentas diferentes y la sincronicéis en la misma carpeta donde la subáis. De esta manera, si os tiran una cuenta, podéis utilizar la otra y así no perdéis los datos subidos. (Cuidado con los archivos con copyright)

También, que no subáis archivos personales, tipo fotos y eso. Utilizadlo para subir pelis encriptadas y cosas que os ocupan espacio y queréis hacer otra copia de seguridad.

Todo lo que introduzcamos en dicha unidad compartida de Drive no ocupará espacio en nuestra cuenta de Google. Además podremos invitar a nuevos miembros, ya que seremos los únicos administradores de dicha unidad.

A modo de aprendizaje, esto podemos hacerlo porque formaremos parte de una cuenta universitaria, las cuales son gratuitas e ilimitadas. Tenemos que tener en cuenta que este método puede ser revocado en cualquier momento, ya que cuando Google se de cuenta que no somos parte de esa universidad, nos mandará a paseo.

--------------------------------------

🤑🤑🤑

--------------------------------------

Google drive ilimitado 2

Google drive ilimitado

Aquí os dejo unos enlaces para convertir vuestra cuenta de google drive a ilimitada sin necesidad de pagar nada aunque es baneable por lo que no useis el email persona podeis crear uno que no cuesta nada.

Comporbado en diciembre y funcionaba

<https://gd.zxd.workers.dev/>

<https://teamdrive.mfoxx.workers.dev/>

<https://gd.404edu.workers.dev/>

<https://teamdrive.xcpx.workers.dev/>

<https://gdrive.zppcw.cn/>

<https://teamdrive.xcpx.workers.dev>

<https://td.fastio.me>

<https://team.gdrive.vip/>

<https://driveteam.nguyenvanlong.blog/>

<https://gdx10der.ml/>

<https://tv.ssr.workers.dev/>

--------------------------------------

👉💗👈🤯

--------------------------------------

TWITCH LEAK TORRENT DESCARGA (la mayor filtración en Twitch)

<https://pastebin.com/LjmaPNam> <https://pastebin.com/S1SGxd0B>

<https://nodo313.net/twitch.leak.fixed_nodo313.txt>

--------------------------------------

🤝🤝😡😡

--------------------------------------

Ip tracer etc

<https://www.ipalyzer.com/>

--------------------------------------

🤝❤🖤❤

--------------------------------------

Crear word corrupto

<https://corrupt-a-file.net/>

--------------------------------------

🤑🤑😂

--------------------------------------

Bot discord

<https://github.com/PolarLofy/Discord-Mass-Dm>

--------------------------------------

𖧮𖧶

--------------------------------------

Comprobar pagina web(etc)

<https://webrate.org/index.php/site/google.com/>

--------------------------------------

𓉳᭕𓆩ᥫ᭡⃠⃢⃠⃢⃢⃢⃢

--------------------------------------

Comprobar ping de una pagina

<https://check-host.net/>

--------------------------------------

🥵👍🥵👍👍🥵👍🥵👍🥵

--------------------------------------

para encontrar un PDF de cualquier tipo gratis en internet

Typefile:pdf (y el nombre de loque queremos buscar)

--------------------------------------

🥳🥳🥳🥳🥳👍👍👍👍👍

--------------------------------------

emulador de juegos online

<https://emulatorgames.online/>

--------------------------------------

☺↻𓊉

--------------------------------------

Juegos online

<https://getgamez.net/>

--------------------------------------

😳😳

--------------------------------------

2.25k UPLAY+ 1.1k Origin+ 600 STEAM +2.3k Disney+ + 36 GEOGESSER

https://anonfiles.com/Z3l03aV8uc/990\_UPLAY\_txt

https://anonfiles.com/b4md34Vbu6/800\_UPLAY\_txt

https://anonfiles.com/N4xbw8Vau1/Geogesser\_txt

https://anonfiles.com/12x6O7Vdu8/712\_DISNEY\_txt

https://anonfiles.com/lfj534V7u9/1.6k\_DISNEY\_txt

https://anonfiles.com/5cf33dVbud/600\_STEAM\_txt

https://anonfiles.com/F8wcO9V1u7/1138x\_Origin\_txt

https://anonfiles.com/Tdv4O5V2u1/535\_UPLAY\_txt

--------------------------------------

🧐😕

--------------------------------------

Contraseñas predeterminadas de BIOS etc

BIOS

http://www.cirt.net/cgi-bin/passwd.pl

http://www.phenoelit.de/dpl/dpl.html

http://www.xs4all.nl/~matrix/mpwlist.html

http://www.elfqrin.com/docs/biospw.html <-

ROUTERS

http://www.adslayuda.com/password\_router.html

http://www.routerpasswords.com/

http://phenoelit.darklab.org/cgi-bin/display.pl

http://www.phenoelit.de/dpl/dpl.html

http://www.anameless.com/blog/default-passwords.html

http://www.governmentsecurity.org/articles/DefaultLoginsandPasswordsforNetworkedDevices.php

http://www.glug-howrah.org/modules.php?name=Forums&file=printview&t=386&start=0

http://ap0c.freeflux.net/files/router-default-list.txt

http://www.cirt.net/cgi-bin/passwd.pl

http://artofhacking.com/etc/passwd.htm

http://www.adslayuda.com/

SSID "THOMSON" con WEP, password "0123456789"

WPA de FON

Desde

8651022000

8651022001

8651022002

...

hasta

8704019999

WPA de routers Thompson con ESSID SpeedTouch\*\*\*\*\*\*

http://foro.elhacker.net/index.php/topic,208312.0.html

Revisado, modificado y compilado para los

modelos salidos desde el año 2004 y los que saldran durante el 2008:

DESCARGA: http://download.wifislax.com:8080/SpeedTouchKeys-v0.1.zip

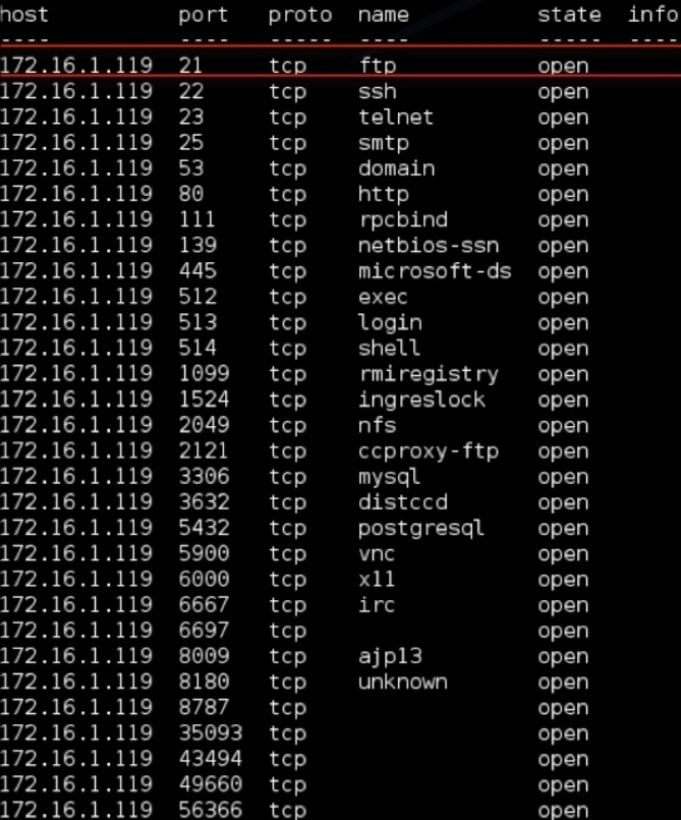
MD5: 2b5ea7d4539ea5b02fc8ea569e5566f6

--------------------------------------

😃😃😃🤮

--------------------------------------

Puertos de iPS



--------------------------------------

Protocolos network

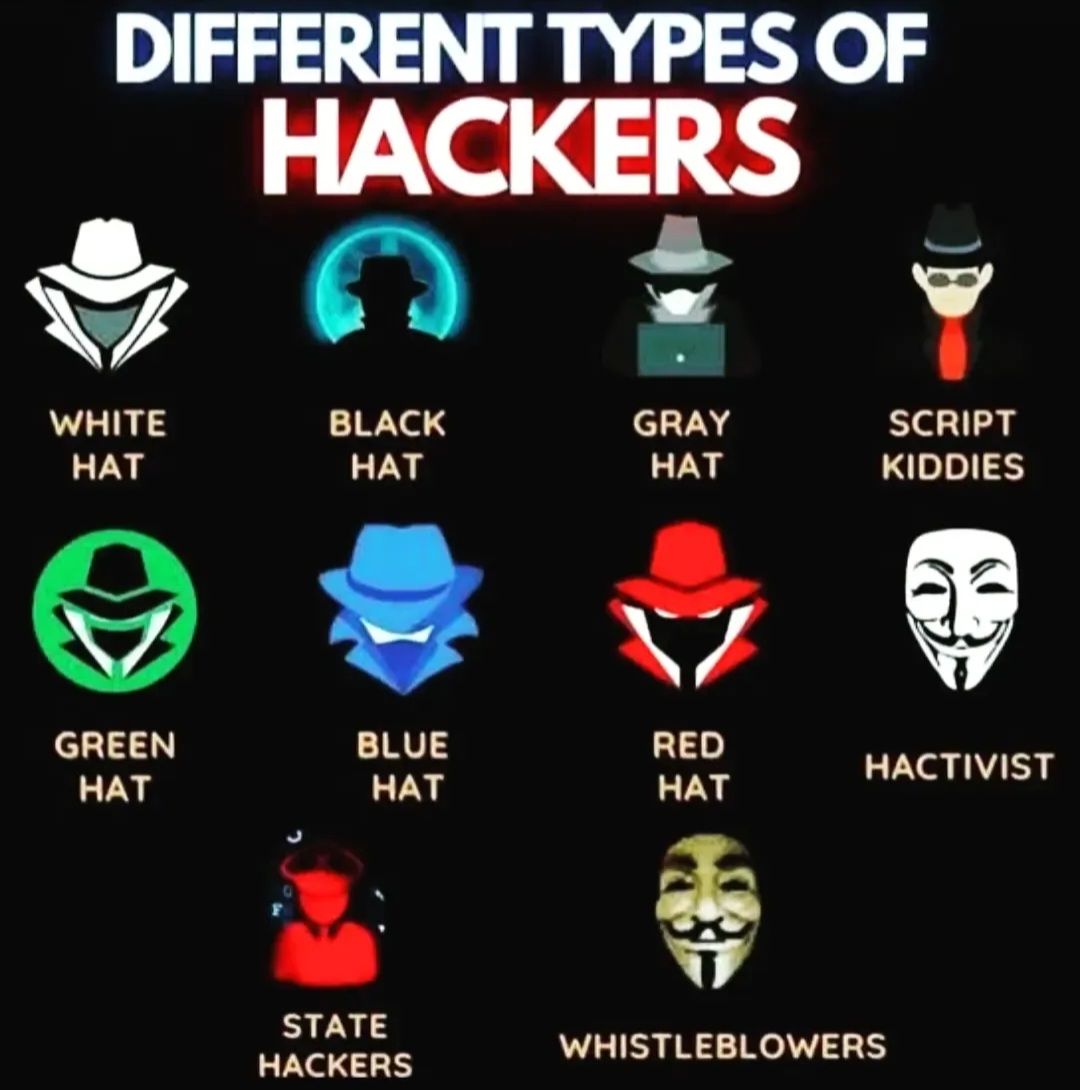


--------------------------------------

😂😂😂😂😂😂😂😂😂😂

--------------------------------------

tipos de de hackers



--------------------------------------

😃😐

--------------------------------------

Hacking ético tutorial YT

https://youtu.be/lUr9C05NfPM

--------------------------------------

⃟⃤..

--------------------------------------

Steam cuenta funcional hasta 2038

Nombre: sv3nyo Contraseña: heero3004

--------------------------------------

Letra rara

<https://replit.com/@g3piton/Letrarara#main.py>

--------------------------------------

`́́́

--------------------------------------

ࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩࣩ

--------------------------------------

Código pico Catwoman (no canjeable solo broma para amigos)

LLKP8ZTVBATEL462UEA9

--------------------------------------

🟡💲🟡💲🟡🟡👍🟡

--------------------------------------

Word glitching (word con todo sobre glitch es en fortnite y islas que tengo publicadas)

<https://1drv.ms/w/s!Ajq5e3lYwCw8ewq9Yh7aG9LQemA>

--------------------------------------