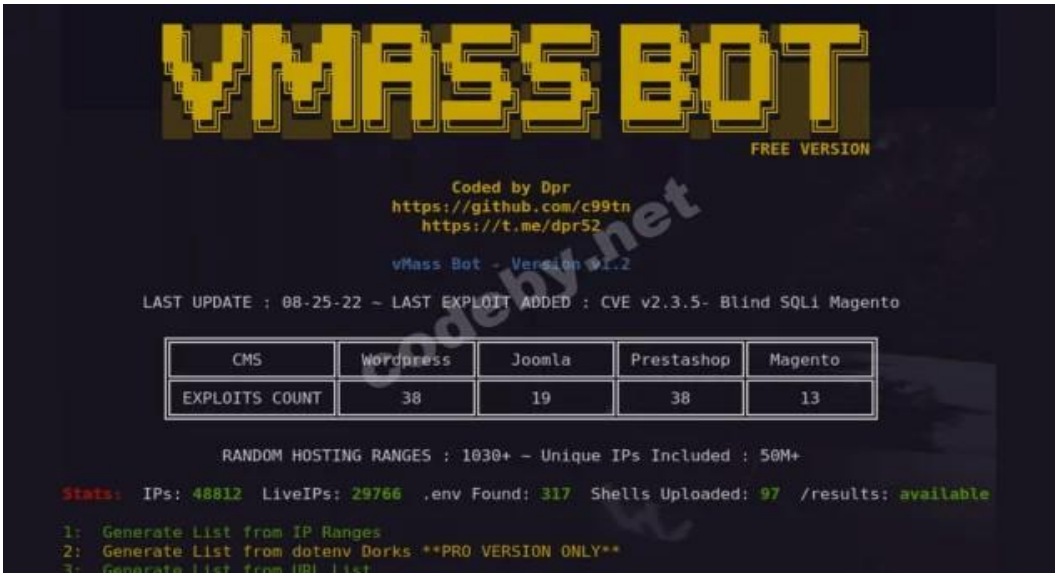
Código abierto. Escáneres de vulnerabilidades

Seguridad primero: Escáneres de código abierto y de vulnerabilidades para proteger tu sistema de forma fiable

Los escáneres de código abierto y de vulnerabilidades pueden convertirse en tu asistente fiable. Código abierto significa que el código fuente de la aplicación está disponible para su visualización y modificación. Esto permite a los usuarios probar exactamente cómo funciona el programa, hacer cambios y mejorarlo según sus necesidades. Esto es especialmente útil en el caso de los escáneres de vulnerabilidades, ya que permiten identificar posibles debilidades en el sistema y sugerir medidas para solucionarlas. Los escáneres de vulnerabilidades son herramientas que permiten detectar y analizar automáticamente posibles vulnerabilidades en sistemas informáticos, redes o programas. Realizan comprobaciones sistemáticas de seguridad para identificar posibles problemas, como medidas de seguridad insuficientes, aplicaciones desactualizadas o configuraciones débiles. Con la ayuda de escáneres de vulnerabilidades, puedes garantizar un alto nivel de seguridad para tu sistema y evitar posibles amenazas.

El uso de escáneres de código abierto y de vulnerabilidades te permite tener control total sobre la seguridad de tu sistema, así como garantizar que esté protegido eficazmente frente a posibles amenazas. Puedes utilizar estas herramientas para comprobar la seguridad de tu red, sitio web o aplicación, identificar debilidades y tomar las medidas necesarias para asegurarte de que se solucionen. Los escáneres de vulnerabilidades y de código abierto te ofrecen potentes herramientas de análisis

vMass Bot



vMass Bot – automatiza la explotación de los hosts remotos intentando encontrar archivos de entorno (.env) en los hosts objetivo y extraer herramientas e información de ellos. El bot detectará entonces el CMS del servidor objetivo y explotará automáticamente las vulnerabilidades para descargar cargas útiles del shell usando la suite de vulnerabilidades vMass. vMass Bot puede crear listas de servidores a partir de rangos de IP, listas de URL, pistas individuales de dotenv y fragmentos de motores de búsqueda (por ejemplo, Bing, DuckDuckGo). También puedes usar rangos de IP de diferentes proveedores de hosting para obtener el mejor porcentaje de resultados de rastreo. Las listas generadas pueden ser comprobadas por un bot para eliminar hosts inválidos. Las herramientas eliminadas pueden filtrarse y comprobarse para dejar solo las que funcionen.

Instalación

Toda la instalación se llevará a cabo en Kali Linux.

Clonación del repositorio

Code:

```
git clone https://github.com/c99tn/vMass.git cd vMass
```

Instalación de módulos Perl necesarios usando solo un script bash.

Código:

```
chmod +x install.sh bash install.sh
```

Ejecutando vMass Bot.

Código:

```
perl vMass.pl
```

Funciones

Solo las características que no están resaltadas en amarillo están disponibles en la versión gratuita.

1. (Seguridad) Crea hosts objetivo a partir de un rango de IP dado, puedes usar tantos rangos como quieras
2. Crea hosts objetivo a partir de dorks concretos o usando dorks del entorno bot, puedes especificar la región de los hosts objetivo, TLD y motores de búsqueda.
3. (Libre) Crea hosts objetivo a partir de una lista determinada de sitios web, PD: Las listas de URL deben ser domain.com solo sin www ni https.
4. (Libre) Crea hosts objetivo desde el rango de IP proporcionado, el rango se selecciona aleatoriamente, puedes cambiar el rango antes de empezar.
5. (Libre) Comprueba los hosts objetivo para filtrar IPS en ejecución en vivo de los inactivos.
6. (Libre) El bot de escanear los hosts objetivo para posibles archivos .env revisará todos los directorios de host y guardará el host si no se encuentra ningún env.

7. Escanear los hosts objetivo para .env y realizar exploits automáticos basados en el CMS del host para descargar la carga útil (108 exploits)

8. En desarrollo.

9. (Libre) Extrae herramientas de los hosts donde reside el archivo env dependiendo del tipo de herramienta.

10. Revisa el SMTP eliminado, ¿necesitas introducir un correo electrónico? Si SMTP se entrega, la información de SMTP estará en el cuerpo del correo.

11. Comprueba la corrección y el equilibrio de las APIs TWILIO eliminadas

12. Intenta navegar hasta la página de inicio de sesión de phpmyadmin y sigue el método de captura de administrador para cargar el shell en los hosts CMS de WordPress.

13. Mueve todas las herramientas a un canal privado de Telegram.

14. Sigue todos los pasos anteriores uno a uno, solo tienes que configurar el bot, ejecutarlo y los resultados se entregarán a tu Telegram, que es mejor usarlo para RDP/VPS y con una lista amplia de hosts objetivo.

SARENKA

La herramienta de inteligencia de código abierto OSINT extrae datos de servicios como Shodan, Censys y más. en un solo programa. Recupera Vulnerabilidades y Consecuencias Comunes (CVEs), Listas de Vulnerabilidades Comunes (CWEs) y cuenta con una base de datos que mapea los CVE con los CWEs. La app ahora también tiene herramientas sencillas como una calculadora de hash y un escáner de puertos muy sencillo.

Funciones

Get data from Censys by ip

Get data from Shodan by ip

Get data from Criminalip by ip

Get DNS data

Get WHOIS data
Encuentra CVE por
CWE

Crea un informe en
formato pdf

También puedes:

Compute hashes on a per-user basis

Comprueba si el puerto está abierto o cerrado

Instalación

Clonar el repositorio

Código:

```
git clone https://github.com/pawlaczyk/sarenka.git
```

Ve al directorio de aplicaciones

Código:

```
cd sarenka
```

Crea venv

Código:

```
python3 -m venv env
```

Activar venv

Código:

```
source venv/bin/activate
```

Dependencias de instalación

Código:

```
pip3 install -r requirements.txt
```

Compilación del programa usando el script sarenka.py

Código:

```
python3 sarenka/sarenka.py
```

Empezando

Antes de empezar, deberías crear cuentas en los servicios Shodan y Censy s. Por defecto, el programa se lanzará desde el enlace http://localhost:8000/

Código:

```
python3 backend/manage.py runserver
```

Añadir credenciales de usuario a **Configuración**

XSStrike

El detector de scripts multi-sitio está equipado con cuatro analizadores de escritura a mano, un generador inteligente de carga útil, un potente motor discord y un escáner extremadamente rápido.

En lugar de añadir una carga útil y probar su rendimiento como hacen todos los demás mecanismos, XSStrike analiza la respuesta usando múltiples analizadores y luego genera cargas útiles que garantizan que funcionarán usando el análisis contextual incorporado de la herramienta.

Características principales

Reflected and DOM XSS scanning

Multithreaded scanning

Contextual analysis

Configurable kernel

WAF detection and evasion

Scan for deprecated JS library

Intelligent payload generator

Homemade HTML and JavaScript parser

Powerful phasing engine

Blind XSS support

Thoroughly studied work process

Full HTTP support

Retrieval of useful data from a file

Works on Photon, Zetanize and Arjun

Payload encoding

Instalación

Clonando el repositorio.

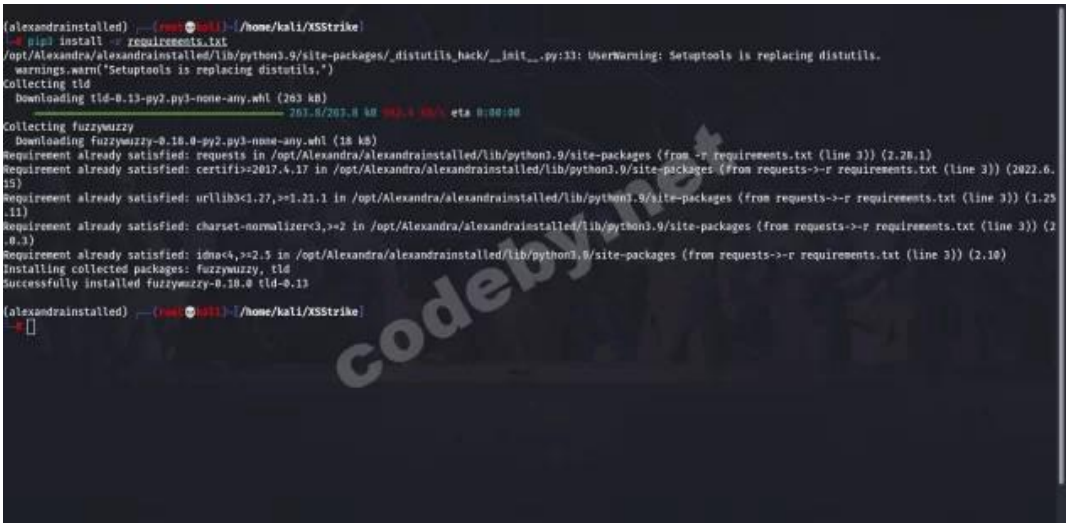
Código:

```
git clone https://github.com/s0md3v/XSStrike
```

Establecer dependencias.

Código:

```
pip3 install -r requirements.txt
```



Lanzando.

Código:

```
python3 xsstrike.py
```

RustScan

Un escáner de puertos moderno. Una búsqueda rápida de puertos a la velocidad del idioma Rust convierte un escaneo Nmap de 17 minutos en 19 segundos. Encuentra rápidamente todos los puertos abiertos reenviándolos automáticamente a Nmap.

Funciones

Scans all 65K ports in 8 seconds

Saves an hour by automatically sending ports to Nmap. No manual copying and pasting.

Good at his job. The only goal is to improve the Nmap scanner

Lets you choose which Nmap commands to run or use by default

Instalación

Para la instalación más rápida y eficiente en Kali Linux, basta con visitar la página de lanzamiento, descargar el archivo .deb e instalarlo a través de dpkg-i, el archivo .deb. Para iniciar el escaneo, solo tienes que introducir el código:

```
rustscan -a IP
```