sublist3r

Sublist3r es una herramienta de código abierto utilizada para enumerar subdominios de un dominio en particular. Es popular entre los profesionales de la seguridad y los investigadores, ya que ayuda a descubrir subdominios de manera rápida y eficiente. Sublist3r utiliza varios motores de búsqueda y servicios como Google, Yahoo, Bing, Baidu, Ask, Netcraft, DNSdumpster, Virustotal, ThreatCrowd, SSL Certificates, y más, para recolectar información sobre los subdominios.

## Características principales:

- \*\*Enumeración de subdominios\*\*: Busca y lista todos los subdominios asociados con un dominio principal.

- \*\*Integración con múltiples motores de búsqueda\*\*: Utiliza diversos servicios y motores de búsqueda para obtener resultados más completos.

- \*\*Simplicidad y rapidez\*\*: Es fácil de usar y puede ejecutar búsquedas rápidamente.

## Uso:

La herramienta se puede ejecutar desde la línea de comandos con un comando simple, por ejemplo:

```bash

python sublist3r.py -d ejemplo.com

```

Esto buscará todos los subdominios relacionados con "ejemplo.com".

Sublist3r es una herramienta útil en el ámbito de la seguridad informática y pruebas de penetración, ya que permite identificar puntos potenciales de ataque en una infraestructura de red.

Nmap (Network Mapper) es una herramienta de código abierto utilizada para el descubrimiento de redes y auditorías de seguridad. Fue diseñada para escanear grandes redes, pero también funciona bien contra hosts individuales. Nmap utiliza paquetes IP en bruto de diversas maneras para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y versión) esos hosts están ofreciendo, qué sistemas operativos (y versiones de SO) están ejecutando, qué tipo de filtros/ firewalls están en uso, y otras características.

## Características principales:

- \*\*Escaneo de puertos\*\*: Identifica los puertos abiertos en un host o red.

- \*\*Detección de sistemas operativos\*\*: Identifica el sistema operativo de los hosts.

- \*\*Detección de servicios\*\*: Identifica los servicios que se ejecutan en los puertos abiertos.

- \*\*Escaneo de scripts\*\*: Utiliza el Nmap Scripting Engine (NSE) para detectar vulnerabilidades y realizar otras tareas de red avanzadas.

- \*\*Creación de mapas de red\*\*: Mapea la red para identificar dispositivos y conexiones.

## Uso:

Nmap se ejecuta desde la línea de comandos y tiene una variedad de opciones y comandos. Aquí hay algunos ejemplos básicos:

### Escaneo de puertos

```bash

nmap ejemplo.com

```

### Escaneo de un rango de IPs

```bash

nmap 192.168.1.1-254

```

### Detección de sistema operativo

```bash

nmap -O ejemplo.com

```

### Uso del Nmap Scripting Engine (NSE)

```bash

nmap --script vuln ejemplo.com

```

### Escaneo rápido de puertos comunes

```bash

nmap -F ejemplo.com

```

### Escaneo detallado

```bash

nmap -A ejemplo.com

```

Nmap es una herramienta poderosa y flexible, ampliamente utilizada por administradores de sistemas y profesionales de seguridad para evaluar la seguridad de sus redes y sistemas.