

Sn1per

URL:

<https://github.com/1N3/Sn1per>

<https://sn1persecurity.com/wordpress/>

Tipo de herramienta:

Suite de herramientas de seguridad ofensivas con diferentes funcionalidades: automatización de test de intrusión, descubrimiento de vulnerabilidades, etc

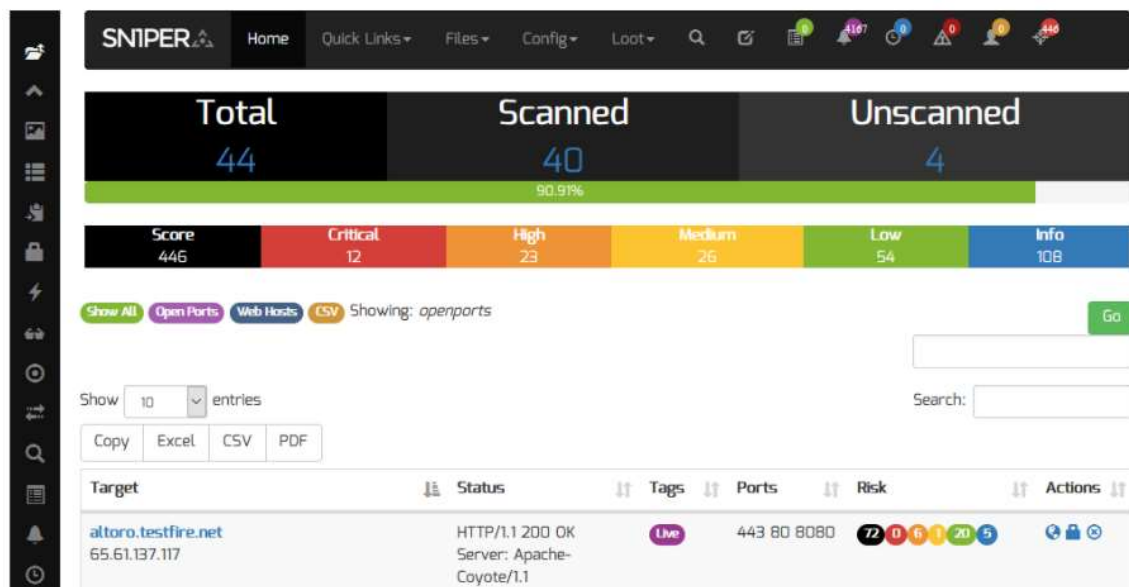
Descripción:

En lo referente a los test de intrusión Sn1per nos permite realizar un escaneo automatizado para enumerar y buscar vulnerabilidades.

Estas pueden ser explotadas con herramientas open source de hacking y seguridad.

El proceso se compone de tres fases:

Descubrimiento:

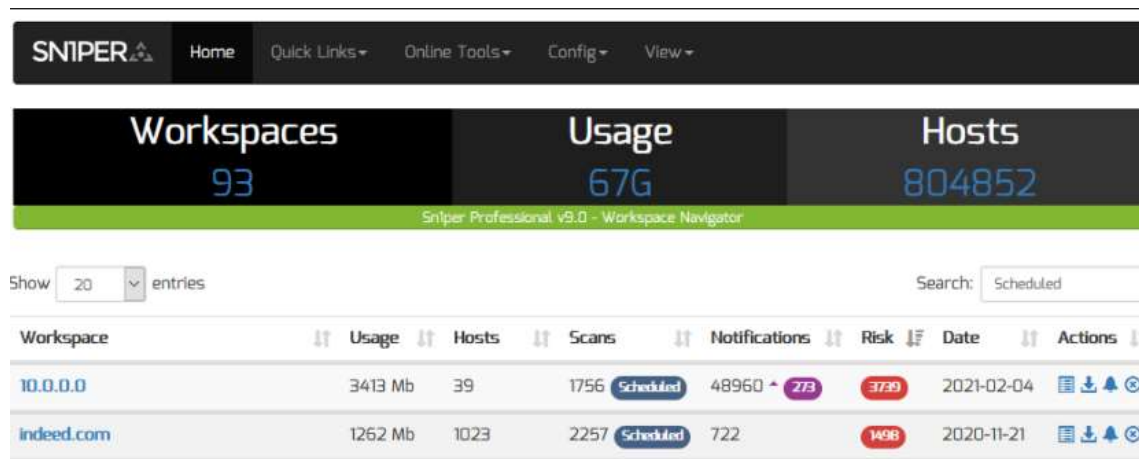


Análisis:

The screenshot shows the 'Vulnerabilities' report in SNIPER. It has a title bar 'SNIPER Vulnerabilities' and a subtitle 'Sniper Professional v9.0 - Workspace Vulnerability Report'. Below the title bar, there's a search bar and a 'Show 20 entries' dropdown. A table lists the vulnerabilities with columns for Criticality, Vulnerability, Target, and Evidence.

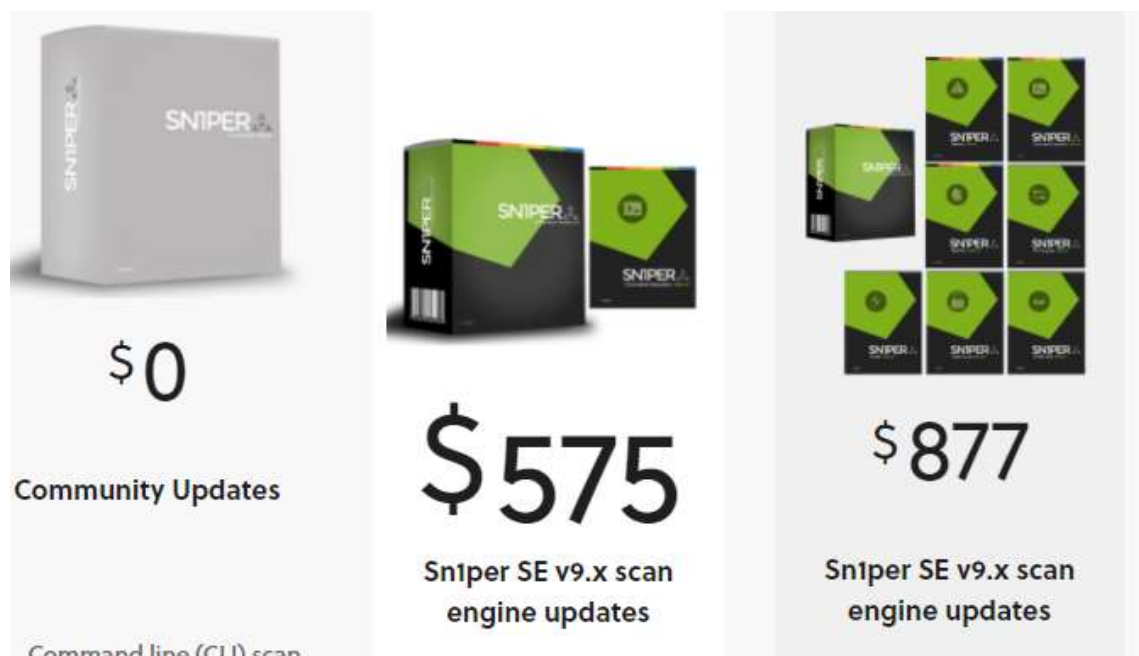
Criticality	Vulnerability	Target	Evidence
P1 - CRITICAL	Default Credentials - BruteX	10.0.0.64	[80][http-get] host: 10.0.0.64 login: admin password: 111111
P1 - CRITICAL	Default Credentials - NMap	10.0.0.1	administrator:administrator - Valid credentials


Y repetición:



Workspace	Usage	Hosts	Scans	Notifications	Risk	Date	Actions
10.0.0.0	3413 Mb	39	1756 Scheduled	48960 273	3739	2021-02-04	[Icons]
indeed.com	1262 Mb	1023	2257 Scheduled	722	1498	2020-11-21	[Icons]

Tiene una versión gratuita para la comunidad, pero si queremos tener toda la suite es una herramienta de pago:






\$0


Community Updates

Command line (CLI) scan



\$575

Sn1per SE v9.x scan engine updates



\$877

Sn1per SE v9.x scan engine updates

Ejemplo:

Instalación:

Podemos realiza la instalación de dos maneras:

1. En sistemas Linux clonando el repositorio de github:

```
git clone https://github.com/1N3/Sn1per
cd Sn1per
bash install.sh
```

2. Mediante Docker:

```
Download https://raw.githubusercontent.com/1N3/Sn1per/master/Dockerfile
docker build -t sn1per .
docker run -it sn1per /bin/bash
```

or

```
docker pull xer0dayz/sn1per  
docker run -it xer0dayz/sn1per /bin/bash
```

Uso:

Una vez instalado basta con lanzar el comando sniper con los parámetros deseados:

```
sniper -t <target> -m <mode> -p <port> ...
```

El uso y los modos se pueden consultar en la página de github indicada al inicio.

Aquí se puede ver un video de ejemplo de la herramienta:

<https://www.youtube.com/watch?v=Fy4XEpFsk70&list=PL40Vp978dDP9KX2V3VLnNzgJuf4nJrRo9&index=2>