

Product

Solutions

Resources

Open Source

Enterprise

Pricing

🔍

Sign in

Sign up

📄 1N3 / Sn1per Public

🔔 Notifications

🍴 Fork

1.8k

★ Star

8.1k

<> Code

🔗 Issues 3

🔗 Pull requests 4

💬 Discussions

🎬 Actions

📁 Projects

📖 Wiki

🛡 Security

📊 Insights

🔗 master ▾

🔗

📄

<> Code ▾

🕒 610 Commits

📁 .github/workflows

📁 bin

📁 conf

📁 loot

📁 modes

📁 pro

📁 templates

📁 wordlists

📄 CHANGELOG.md

📄 Dockerfile

📄 Dockerfile.blackarch

📄 LICENSE.md

📄 README.md

📄 docker-compose-blackarch.yml

📄 docker-compose.yml

📄 install.sh

📄 sn1per.desktop

📄 sn1per.png

📄 sniper

📄 sniper.conf

📄 uninstall.sh

📖 README

📄 License

About

Attack Surface Management Platform

🔗 sn1persecurity.com

security

hacking

cybersecurity

penetration-testing

pentesting

pentest-scripts

security-tools

pentest-tool

osint-framework

attack-surface

hacking-tools

pentest-tools

pentesting-tools

sn1per

sn1per-professional

osint-tool

bugbounty-platform

attacksurface

attack-surface-management

📖 Readme

📄 View license

📈 Activity

★ 8.1k stars

👁 332 watching

🍴 1.8k forks

Report repository

Releases 49

📦 Sn1per Community Edition v9.2 Latest

on Jul 29, 2023

+ 48 releases

Packages

No packages published

Contributors 32

+ 18 contributors

Languages

Shell 53.7%

Python 7.2%

JavaScript 0.5%

Dockerfile 0.1%

Lua 36.8%

XSLT 1.5%

HTML 0.2%

Page 1 of 8

SN1PER

The ultimate “all-in-one” offensive security framework

 Sn1perSecurity

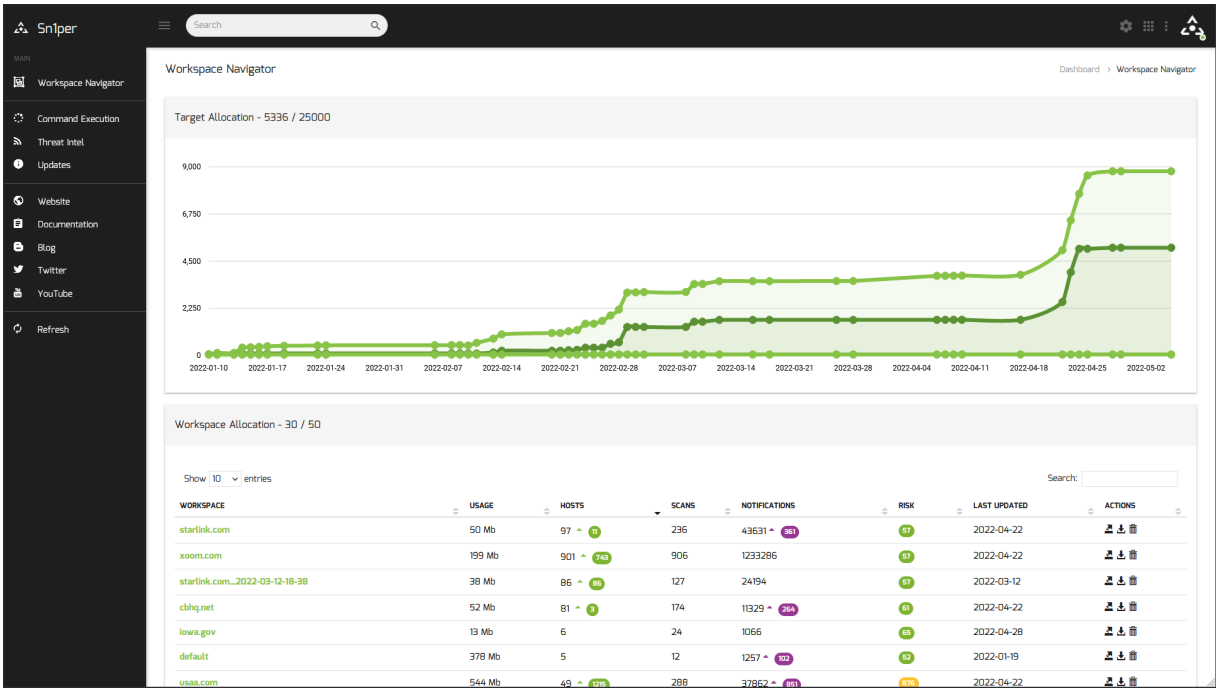
release v9.2 issues 3 open Stars 8.1k Follow 3.4k Tweet Follow

[\[Website\]](#) [\[Blog\]](#) [\[Shop\]](#) [\[Documentation\]](#) [\[Demo\]](#) [\[Find Out More\]](#)

Attack Surface Management Platform

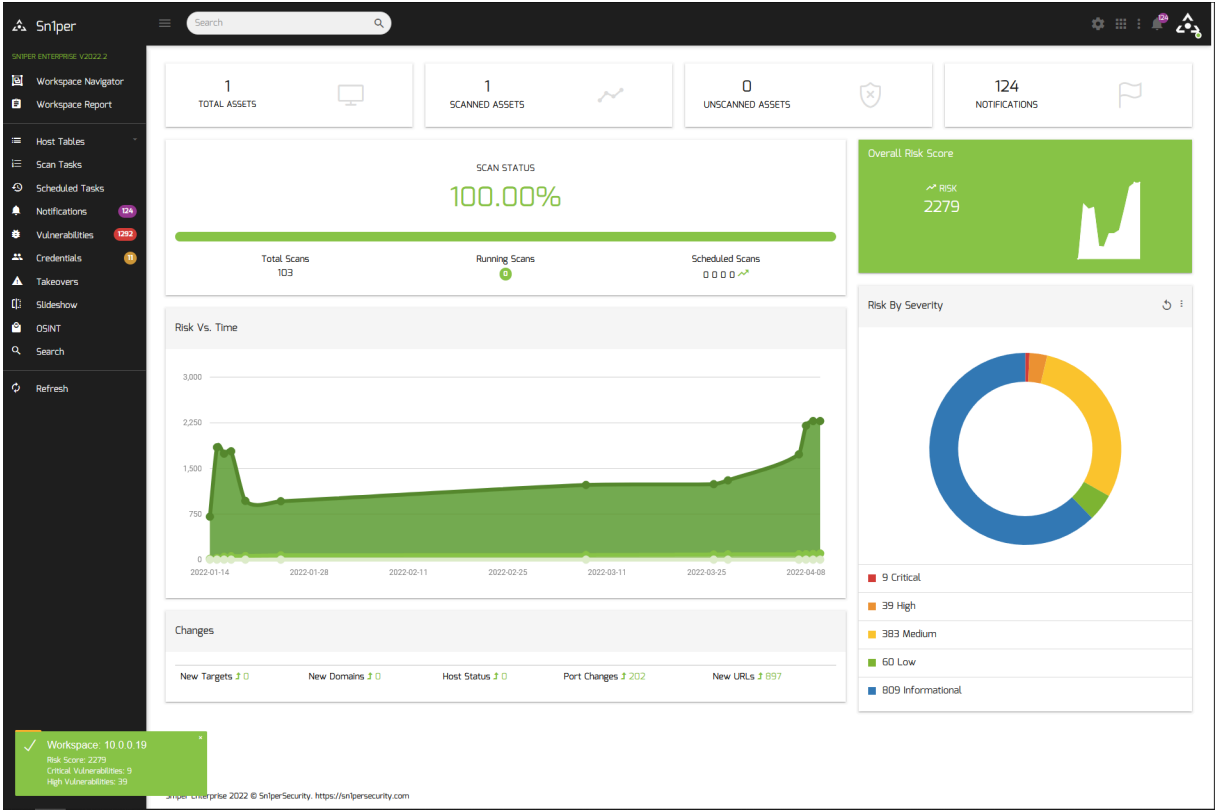
Discover hidden assets and vulnerabilities in your environment

[\[Find out more\]](#)



The ultimate pentesting toolkit

Integrate with the leading commercial and open source vulnerability scanners to scan for the latest CVEs and vulnerabilities.



Automate the most powerful tools

Security tools are expensive and time-consuming, but with Sn1per, you can save time by automating the execution of these open source and commercial tools to discover vulnerabilities across your entire attack surface.

The 'Host Table - Openports' view displays a detailed list of discovered open ports across various hosts. Each entry includes the target host, the open port, the associated service, and a risk score. The table is sortable by target, ports, services, tags, risk, and actions. A search bar is available for filtering the results.

| TARGET | PORTS | SERVICES | TAGS | RISK | ACTIONS |
|---|-----------|--|----------|------|---------|
| shopping.paypal.com 208.76.140.165 | 443 80 | http https http https Server: Apache Server: BigP | Live | 60 | 🔍 🛡️ 🗑️ |
| sandbox.paypal.com 64.4.250.36 64.4.250.37 | 443 80 | http https http https | Live | 45 | 🔍 🛡️ 🗑️ |
| creditapply.paypal.com c.paypal.com c.glb.paypal.com csl150.wpc.betacdn.net 192.229.210.155 | 443 80 | http https http https Server: ECACC (lsw/7BAB) server: ECACC (lsw/7BAB) | Live | 35 | 🔍 🛡️ 🗑️ |
| financing.paypal.com c.paypal.com c.glb.paypal.com csl150.wpc.betacdn.net 192.229.210.155 | 443 80 | http https http https Server: ECACC (lsw/7BAB) | Live | 27 | 🔍 🛡️ 🗑️ |
| pos.paypal.com www.glb.paypal.com www.fastly.glb.paypal.com 151.101.65.21 | 443 80 | http https http https Server: Varnish | Live | 24 | 🔍 🛡️ 🗑️ |
| safetymhub.paypal.com www.edge.glb.paypal.com 173.0.93.244 | 443 80 | http https http https | Live | 15 | 🔍 🛡️ 🗑️ |
| history.paypal.com www.paypal.com www.glb.paypal.com www.fastly.glb.paypal.com 151.101.1.21 | 443 80 | http https http https Server: Varnish server: Varnish | Live | 10 | 🔍 🛡️ 🗑️ |
| paypal.com 64.4.250.36 64.4.250.37 | 22 443 80 | http https http https | New Live | 8 | 🔍 🛡️ 🗑️ |
| advendor.paypal.com advendor.glb.paypal.com 173.0.93.100 | 443 80 | http https http https Server: nginx server: nginx | Live | 6 | 🔍 🛡️ 🗑️ |
| posprivate-api-31.paypal.com posapi31.posprivate-api31.akadns.net 163.172.131.108 | 22 80 | ssh http ssh http Server: Apache/2.4.41 (Ubuntu) | Live | 6 | 🔍 🛡️ 🗑️ |
| posprivate-svcs.paypal.com pos-svcs.posprivate-svcs.akadns.net 163.172.131.108 | 22 80 | Server: Apache/2.4.41 (Ubuntu) | Live | 6 | 🔍 🛡️ 🗑️ |
| iprpb.paypal.com iprpb.glb.paypal.com 64.4.248.8 | 443 80 | http https http https Server: nginx server: nginx | Live | 6 | 🔍 🛡️ 🗑️ |
| stage-www.edge.paypal.com 64.4.250.45 | 443 80 | | Live | 6 | 🔍 🛡️ 🗑️ |
| securepayments.sandbox.paypal.com www.sandbox.paypal.com www.sandbox.glb.paypal.com www.fastly.glb.paypal.com 151.101.193.21 | 443 80 | http https http https Server: Varnish server: Varnish | Live | 6 | 🔍 🛡️ 🗑️ |

Find what you can't see


Hacking is a problem that's only getting worse. But, with Sn1per, you can find what you can't see—hidden assets and vulnerabilities in your environment.

The 'Host Table - Webhosts' view displays a list of discovered web assets, including their titles, status, ports, risk scores, and actions. A search bar is available for filtering the results. The table includes a 'SCREENSHOT' column for visual verification of the assets.

| SCREENSHOT | TARGET | TITLE | STATUS | PORTS | RISK | ACTIONS |
|------------|---|-----------------|--|--------|------|---------|
| | model3.tesla.com DNS: 205.234.27.221 Server: LB Redirect: Location: https://www.teslamotors.com/model3 Web Fingerprint: Akamai Bot Manager X-Powered-By: PHP/7.4.16 X-Dupli-Dynamic-Cache: MISS X-UA-Compatible: IE=edge X-Generator: Drupal 9 (https://www.drupal.org) X-Cdnal-Cache: HIT X-TZLA-EDGE-CDNNAME: VCL: drupal9prod X-TZLA-EDGE-BACKEND-FETCH-IF-STALE: true X-TZLA-EDGE-WAS-304: true X-TZLA-EDGE-Age: 60.000 X-TZLA-EDGE-Grace: 86400.000 X-TZLA-EDGE-BACKEND-RETRY: 0 X-TZLA-EDGE-BACKEND-CONN-TIME: 0.000 X-TZLA-EDGE-BACKEND-TTFB: 0.000 X-TZLA-EDGE-BACKEND-REASON: OK X-TZLA-EDGE-BACKEND-STATUS: 200 X-Varnish: 787397857 779380310 X-TZLA-EDGE-Cache-Hit: Hit X-TZLA-EDGE-TTL: 45 131 X-TZLA-EDGE-GRACE-BACKEND-UNHEALTHY: 86400.000 X-TZLA-EDGE-BACKEND-STREAM: false X-TZLA-EDGE-CLIENT-RESTARTS: 0 X-TZLA-EDGE-CLIENT-REQ-TTL: 1.000 X-TZLA-EDGE-Server: ejc04ptegvr67.teslamotors.com X-TZLA-EDGE-Cache-Hits: 1 | Model 3 Tesla | HTTP/1.0 302 Moved Temporarily | 443 80 | 6 | 🔍 🛡️ 🗑️ |
| | partners.tesla.com DNS: partners.tesla.com.edgekey.net e1792.dscx.akamaiedge.net 184.24.186.56 Server: Server: AkamaiGHost Redirect: Location: https://partners.tesla.com/ Location: https://partners.tesla.com/home Headers: Strict-Transport-Security: max-age=15768000 ; includeSubDomains Web Fingerprint: Akamai Akamai mPulse Server-Timing: cdn-cache, desc=M55, edge: dur=57, origin: dur=81 Akamai mPulse Server-Timing: cdn-cache, desc=M55, edge: dur=60, origin: dur=257 | Partner Portal | HTTP/1.1 301 Moved Permanently HTTP/1.1 307 Temporary Redirect | 443 80 | 6 | 🔍 🛡️ 🗑️ |

Discover and prioritize risks in your organization

| Vulnerabilities | | | |
|----------------------------|---|--|---|
| Show All ▾ entries | | Copy CSV Excel Print PDF | Search: <input type="text"/> |
| CRITICALITY | FINDING | TARGET | EVIDENCE |
| P1 - CRITICAL | Anonymous SMB Login | 10.0.0.19 | [*] Server 10.0.0.19 allows sessions using username " |
| P1 - CRITICAL | Apache Tomcat Spring4Shell Compromised Host (CVE-2022-22965) | http://10.0.0.19:8888/tomcatwar.jsp?pwd=j5cmdcrah%20etc/passwd | |
| P1 - CRITICAL | Default Credentials - NMap | 10.0.0.19 | I root:&iltempty - Valid credentials |
| P1 - CRITICAL | Joomla! Unsupported Version Detection | 10.0.0.19:9002 | The remote host contains an unsupported version of Joomla!. |
| P1 - CRITICAL | Nuclei Vulnerability Scan | [dvw4-defaults-login] | http://10.0.0.19:8888/login.php |
| P1 - CRITICAL | SQLMap SQL Injection | 10.0.0.19 | Payload: username=UTLr' AND (SELECT 6305 FROM (SELECT(SLEEP(5)))yTtJ) AND 'SeQl='SeQl&password= 10.0.0.19 |
| P1 - CRITICAL | SQLMap SQL Injection | 10.0.0.19 | back-end DBMS: MySQL => 5.0.12 10.0.0.19 |
| P1 - CRITICAL | nginx 0.6.x + 1.20.1-1-Byte Memory Overwrite RCE | 10.0.0.19:8888 | The remote web server is affected by a remote code execution vulnerability. |
| P1 - CRITICAL | nginx 0.6.x + 1.20.1-1-Byte Memory Overwrite RCE | 10.0.0.19:8888 | The remote web server is affected by a remote code execution vulnerability. |
| P2 - HIGH | Apache Tomcat Spring4Shell Remote Code Execution (CVE-2022-22965) | http://10.0.0.19:8888 /u04_DOES_NOT_EXIST | Apache Tomcat/9.0.60 |
| P2 - HIGH | Burpsuite Vulnerability Scan | 10.0.0.19 | Cleartext submission of password - http://10.0.0.19:8080/examples/jsp/security/protected/index.jsp |
| P2 - HIGH | Burpsuite Vulnerability Scan | 10.0.0.19 | J2EEScan - EL (Expression Language) injection - http://10.0.0.19:8080/docs/architecture/startup/serverStartup.pdf |
| P2 - HIGH | Burpsuite Vulnerability Scan | 10.0.0.19 | J2EEScan - Local File Include - web.xml retrieved - http://10.0.0.19:8080/docs/appdev/web.xml.txt |
| P2 - HIGH | Burpsuite Vulnerability Scan | 10.0.0.19 | Possible 403 Bypass - http://10.0.0.19:8080/host-manager/html |
| P2 - HIGH | Burpsuite Vulnerability Scan | 10.0.0.19 | Possible 403 Bypass - http://10.0.0.19:8080/manager/status |
| P2 - HIGH | Burpsuite Vulnerability Scan | 10.0.0.19 | WebSocket URL poisoning (DOM-based) - http://10.0.0.19:8080/examples/websocket/echo.html |
| P2 - HIGH | CGI Generic SQL Injection (blind time based) | 10.0.0.19:8887 | |
| P2 - HIGH | CGI Generic SQL Injection (blind) | 10.0.0.19:8080 | A CGI application hosted on the remote web server is potentially |
| P2 - HIGH | CGI Generic SQL Injection (blind) | 10.0.0.19:8887 | A CGI application hosted on the remote web server is potentially |
| P2 - HIGH | Clear-Text Protocol - HTTP | http://10.0.0.19:8888/ | HTTP/1.1 200 OK |



SNIPER

Getting Started

PLAY ALL

@Sn1perSecurity


Sn1per Enterprise Bootcamp

7 videos • 251 views • Updated 2 days ago


Public

Get the training you need to leverage the full potential of Sn1per Enterprise with our #sn1perbootcamp series.

External Attack Surface Management | Offensive Security | Web Application Security | Penetration Testing | OSINT | Reconnaissance | Bug Bounty




Sn1perSecurity



Getting Started With Sn1per Enterprise

Sn1perSecurity


2:13



Running Scans With Sn1per Enterprise

Sn1perSecurity


3:54



Sn1per Enterprise Workspace Reports

Sn1perSecurity


2:33



Sn1per Enterprise Host Reports

Sn1perSecurity


4:03



Sn1per Enterprise Nessus Integration

Sn1perSecurity


1:50



Sn1per Enterprise OpenVAS GVM Integration

Sn1perSecurity

1:50



Sn1per Enterprise Burpsuite Professional Integration

Sn1perSecurity

1:32

- [Sn1per Enterprise v20240608 Released!](#)
- [Sn1per Scan Engine v10.6 Released!](#)
- [Sn1per Enterprise v20231025 Released!](#)
- [Automated Penetration Testing Guide - Your Ultimate Resource](#)
- [Dark Web Monitoring: Securing Your External Attack Surface](#)
- [Sn1per: The Next Generation of Tools for Security Professionals](#)
- [5 Ways Sn1per Can Automate Your Security Workflow](#)
- [External Attack Surface Management with Sn1per](#)
- [Sn1per Enterprise Released!](#)
- [Sn1per Professional v10.0 Released!](#)

Kali/Ubuntu/Debian/Parrot Linux Install

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



AWS AMI (Free Tier) VPS Install



To install Sn1per using an AWS EC2 instance:

- Go to <https://aws.amazon.com/marketplace/pp/prodview-rmloab6wnymno> and click the "Continue to Subscribe" button
- Click the "Continue to Configuration" button
- Click the "Continue to Launch" button
- Login via SSH using the public IP of the new EC2 instance

Docker Install



Kali Linux-based Sn1per

- Run the Docker Compose file

```
sudo docker compose up
```



- Run the container

```
sudo docker run -it sn1per-kali-linux /bin/bash
```



BlackArch-based Sn1per

- Run the Docker Compose file

```
sudo docker compose -f docker-compose-blackarch.yml up
```



- Run the container

```
sudo docker run -it sn1per-blackarch /bin/bash
```



Usage

```
[*] NORMAL MODE
sniper -t <TARGET>

[*] NORMAL MODE + OSINT + RECON
sniper -t <TARGET> -o -re

[*] STEALTH MODE + OSINT + RECON
sniper -t <TARGET> -m stealth -o -re
```



```
[*] DISCOVER MODE
sniper -t <CIDR> -m discover -w <WORKSPACE_ALIAS>

[*] SCAN ONLY SPECIFIC PORT
sniper -t <TARGET> -m port -p <portnum>

[*] FULLPORTONLY SCAN MODE
sniper -t <TARGET> -fp

[*] WEB MODE - PORT 80 + 443 ONLY!
sniper -t <TARGET> -m web

[*] HTTP WEB PORT MODE
sniper -t <TARGET> -m webporthttp -p <port>

[*] HTTPS WEB PORT MODE
sniper -t <TARGET> -m webporthttps -p <port>

[*] HTTP WEBSCAN MODE
sniper -t <TARGET> -m webscan

[*] ENABLE BRUTEFORCE
sniper -t <TARGET> -b

[*] AIRSTRIKE MODE
sniper -f targets.txt -m airstrike

[*] NUKE MODE WITH TARGET LIST, BRUTEFORCE ENABLED, FULLPORTSCAN ENAI
sniper -f targets.txt -m nuke -w <WORKSPACE_ALIAS>

[*] MASS PORT SCAN MODE
sniper -f targets.txt -m massportscan

[*] MASS WEB SCAN MODE
sniper -f targets.txt -m massweb

[*] MASS WEBSCAN SCAN MODE
sniper -f targets.txt -m masswebscan

[*] MASS VULN SCAN MODE
sniper -f targets.txt -m massvulnscan

[*] PORT SCAN MODE
sniper -t <TARGET> -m port -p <PORT_NUM>

[*] LIST WORKSPACES
sniper --list

[*] DELETE WORKSPACE
sniper -w <WORKSPACE_ALIAS> -d

[*] DELETE HOST FROM WORKSPACE
sniper -w <WORKSPACE_ALIAS> -t <TARGET> -dh

[*] GET SNIPER SCAN STATUS
sniper --status

[*] LOOT REIMPORT FUNCTION
sniper -w <WORKSPACE_ALIAS> --reimport

[*] LOOT REIMPORTALL FUNCTION
sniper -w <WORKSPACE_ALIAS> --reimportall

[*] LOOT REIMPORT FUNCTION
sniper -w <WORKSPACE_ALIAS> --reload

[*] LOOT EXPORT FUNCTION
sniper -w <WORKSPACE_ALIAS> --export

[*] SCHEDULED SCANS
sniper -w <WORKSPACE_ALIAS> -s daily|weekly|monthly

[*] USE A CUSTOM CONFIG
sniper -c /path/to/sniper.conf -t <TARGET> -w <WORKSPACE_ALIAS>
```



```
[*] UPDATE SNIPER
sniper -u|--update
```

Modes

- **NORMAL:** Performs basic scan of targets and open ports using both active and passive checks for optimal performance.
- **STEALTH:** Quickly enumerate single targets using mostly non-intrusive scans to avoid WAF/IPS blocking.
- **FLYOVER:** Fast multi-threaded high level scans of multiple targets (useful for collecting high level data on many hosts quickly).
- **AIRSTRIKE:** Quickly enumerates open ports/services on multiple hosts and performs basic fingerprinting. To use, specify the full location of the file which contains all hosts, IPs that need to be scanned and run ./sn1per /full/path/to/targets.txt airstrike to begin scanning.
- **NUKE:** Launch full audit of multiple hosts specified in text file of choice. Usage example: ./sniper /pentest/loot/targets.txt nuke.
- **DISCOVER:** Parses all hosts on a subnet/CIDR (ie. 192.168.0.0/16) and initiates a sniper scan against each host. Useful for internal network scans.
- **PORT:** Scans a specific port for vulnerabilities. Reporting is not currently available in this mode.
- **FULLPORTONLY:** Performs a full detailed port scan and saves results to XML.
- **MASSPORTSCAN:** Runs a "fullportonly" scan on multiple targets specified via the "-f" switch.
- **WEB:** Adds full automatic web application scans to the results (port 80/tcp & 443/tcp only). Ideal for web applications but may increase scan time significantly.
- **MASSWEB:** Runs "web" mode scans on multiple targets specified via the "-f" switch.
- **WEBPORTHTTP:** Launches a full HTTP web application scan against a specific host and port.
- **WEBPORTHTTPS:** Launches a full HTTPS web application scan against a specific host and port.
- **WEBSCAN:** Launches a full HTTP & HTTPS web application scan against via Burpsuite and Arachni.
- **MASSWEBSCAN:** Runs "webscan" mode scans of multiple targets specified via the "-f" switch.
- **VULNSCAN:** Launches a OpenVAS vulnerability scan.
- **MASSVULNSCAN:** Launches a "vulnscan" mode scans on multiple targets specified via the "-f" switch.

Help Topics

- ☒ [Plugins & Tools](#)
- ☒ [Scheduled Scans](#)
- ☒ [Sn1per Configuration Options](#)
- ☒ [Sn1per Configuration Templates](#)
- ☒ [Sc0pe Templates](#)

Integration Guides

- ☒

[Github API integration](#)
- ☒

[Burpsuite Professional 2.x integration](#)
- ☒

[OWASP ZAP integration](#)
- ☒

[Shodan API integration](#)
- ☒

[Censys API integration](#)
- ☒

[Hunter.io API integration](#)
- ☒

[Metasploit integration](#)
- ☒

[Nessus integration](#)
- ☒

[OpenVAS API integration](#)
- ☒

[GVM 21.x integration](#)
- ☒

[Slack API integration](#)
- ☒

[WPScan API integration](#)

License & Legal Agreement

For more information, please see the [LICENSE](#) and [LEGAL](#) files in this repository.



© 2024 GitHub, Inc.

[Terms](#)

[Privacy](#)

[Security](#)

[Status](#)

[Docs](#)

[Contact](#)

[Manage cookies](#)

[Do not share my personal information](#)