









 install.sh		
 sn1per.desktop		
 sn1per.png		
 sniper		
 sniper.conf		
 uninstall.sh		

 [README](#)  [License](#) 




SNIPER


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


 **SniperSecurity**


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

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

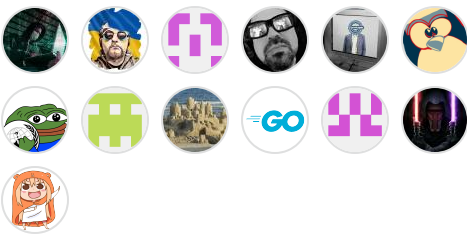
 **Sn1per Community Editi...** Latest
on Jul 29, 2023

[+ 48 releases](#)

Packages

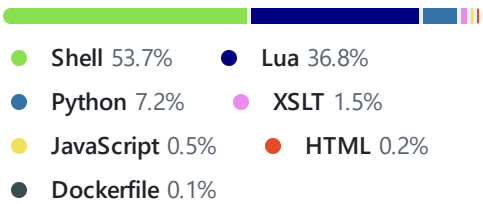
No packages published

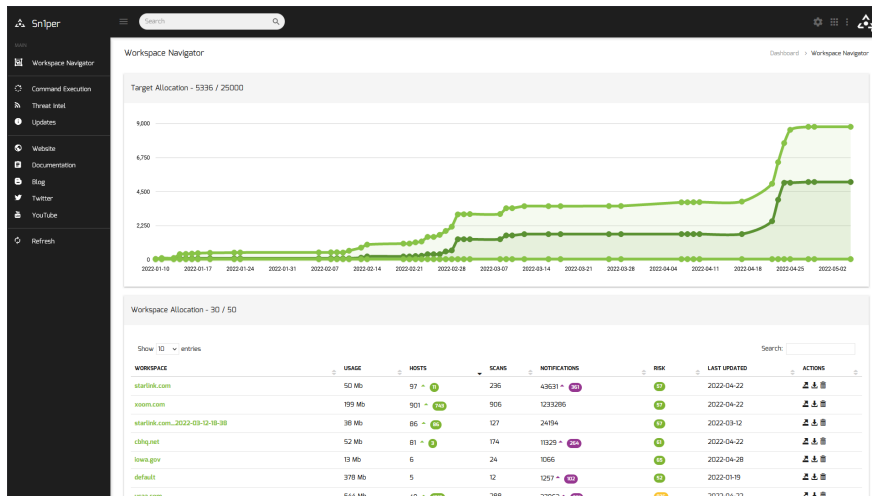
Contributors 32



[+ 18 contributors](#)

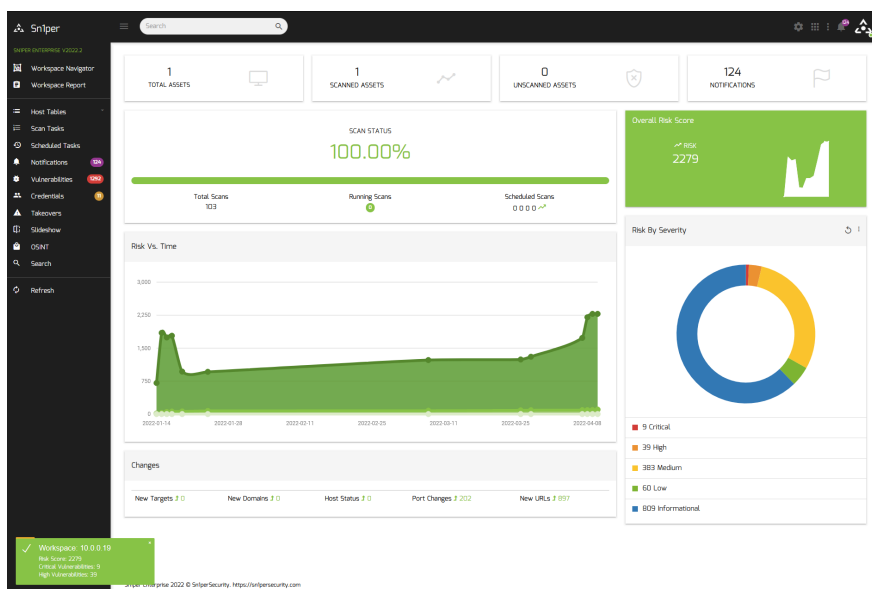
Languages





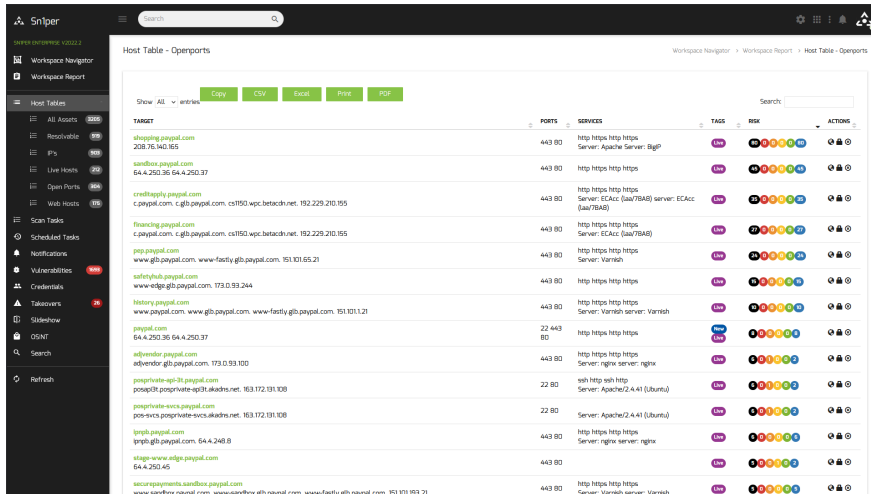
The ultimate pentesting toolkit

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.

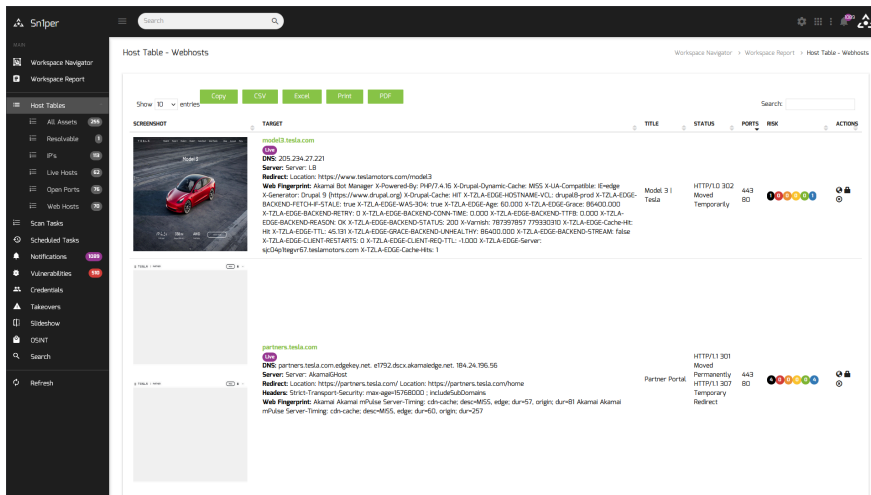


Host Table - Openports



TARGET	PORTS	SERVICES	TAGS	RISK	ACTIONS
shopping.paypal.com 208.76.140.165	443 80	http https http https Server: Apache Server: BgPr	Live	Low	🔍 🛡️ 🔄
sandbox.paypal.com 64.4.250.36 64.4.250.37	443 80	http https http https	Live	Low	🔍 🛡️ 🔄
creditapply.paypal.com c.paypal.com, c.glb.paypal.com, ca750.wpc.betacdn.net, 192.229.210.155	443 80	http https http https Server: EC2Acc (jss/7BA8) server: EC2Acc (jss/7BA8)	Live	Low	🔍 🛡️ 🔄
financing.paypal.com c.paypal.com, c.glb.paypal.com, ca750.wpc.betacdn.net, 192.229.210.155	443 80	http https http https Server: EC2Acc (jss/7BA8)	Live	Low	🔍 🛡️ 🔄
ppp.paypal.com www.glb.paypal.com, www.fastly.glb.paypal.com, 151.101.65.21	443 80	http https http https Server: Varnish	Live	Low	🔍 🛡️ 🔄
safetyhub.paypal.com www.edge.glb.paypal.com, 173.0.93.244	443 80	http https http https	Live	Low	🔍 🛡️ 🔄
history.paypal.com www.paypal.com, www.glb.paypal.com, www.fastly.glb.paypal.com, 151.101.121	443 80	http https http https Server: Varnish server: Varnish	Live	Low	🔍 🛡️ 🔄
paypal.com 64.4.250.36 64.4.250.37	22 443 80	http https http https	New Live	Low	🔍 🛡️ 🔄
edjendor.paypal.com edjendor.glb.paypal.com, 173.0.93.100	443 80	http https http https Server: nginx server: nginx	Live	Low	🔍 🛡️ 🔄
proprinate-egp3l.paypal.com proprinate-egp3l.akadns.net, 163.172.131.108	22 80	ssh http web http Server: Apache/2.4.41 (Ubuntu)	Live	Low	🔍 🛡️ 🔄
proprinate-evcs.paypal.com pro-evcs.proprinate-evcs.akadns.net, 163.172.131.108	22 80	Server: Apache/2.4.41 (Ubuntu)	Live	Low	🔍 🛡️ 🔄
trnglb.paypal.com trnglb.glb.paypal.com, 64.4.248.8	443 80	http https http https Server: nginx server: nginx	Live	Low	🔍 🛡️ 🔄
stage-www.edge.paypal.com 64.4.250.45	443 80		Live	Low	🔍 🛡️ 🔄
securepayments.sandbox.paypal.com www.sandbox.paypal.com, www.sandbox.glb.paypal.com, www.fastly.glb.paypal.com, 151.101.93.21	443 80	http https http https Server: Varnish server: Varnish	Live	Low	🔍 🛡️ 🔄

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.



Host Table - Webhosts


SCHEMATIC	TARGET	TITLE	STATUS	PORTS	RISK	ACTIONS
	model3.tesla.com DNS: 205.234.27.221 Server: Server: LB Redirect: Location: https://www.teslamotors.com/model3 Web Fingerprint: Akamai Bot Manager X-Powered-By: PHP/7.4.16 X-Output-Dynamic-Cache: M05 X-UA-Compatible: IE=edge X-Generator: Drupal 9 https://www.drupal.org X-Drupal-Cache: HIT X-TZL-A-EDGE-A05-NAME-V01: drupalprod X-TZL-A-EDGE-BACKEND-FETCH-STATUS: true X-TZL-A-EDGE-WAS-304: true X-TZL-A-EDGE-Age: 60.000 X-TZL-A-EDGE-Grace: 36000.000 X-TZL-A-EDGE-BACKEND-RETRY: 0 X-TZL-A-EDGE-BACKEND-COIN-TIME: 0.000 X-TZL-A-EDGE-BACKEND-TIME: 0.000 X-TZL-A-EDGE-BACKEND-REASON: OK X-TZL-A-EDGE-BACKEND-STATUS: 200 X-TZL-A-EDGE-Reason: 78739757 77932310 X-TZL-A-EDGE-CacheHit: Hit X-TZL-A-EDGE-TTL: 45.181 X-TZL-A-EDGE-GRACE-BACKEND-UNHEALTHY: 36000.000 X-TZL-A-EDGE-BACKEND-STREAM: false X-TZL-A-EDGE-CLIENT-REST-WATS: 0 X-TZL-A-EDGE-CLIENT-REST-TTL: 1.000 X-TZL-A-EDGE-Server: iQDapftrgr67.teslamotors.com X-TZL-A-EDGE-Cache-Hits: 1	Model 3 Tesla	HTTP/1.0 302 Moved Temporarily	443 80	Low	🔍 🛡️ 🔄
	partners.tesla.com DNS: partners.tesla.com.edgekey.net, e1752.dscx.akamaiedge.net, 184.24.196.56 Server: Server: AkamaiGHost Redirect: Location: https://partners.tesla.com/ Location: https://partners.tesla.com/home Headers: Strict-Transport-Security: max-age=67583000 ; includeSubDomains Web Fingerprint: Akamai Akamai mPulse Server-Timing: cdn-cache: desc=M05, edge: dur=57, origin: dur=81 Akamai Akamai mPulse Server-Timing: cdn-cache: desc=M05, edge: dur=60, origin: dur=257	Partner Portal	HTTP/1.1 301 Moved Permanently HTTP/1.1 307 Temporary Redirect	443 80	Low	🔍 🛡️ 🔄

Discover and prioritize risks in your organization

Sn1per is a next-generation information gathering tool that provides automated, deep, and continuous security for organizations of all sizes.

Vulnerabilities			
Show: All	▼ entries	Copy	Csv
		Excel	Print
		PDF	
		Search: <input type="text"/>	
CRITICALITY	FINDING	TARGET	EVIDENCE
C1 - CRITICAL	Anonymous SMB Login	10.0.0.19	[*] Server 10.0.0.19 allows sessions using username "
C1 - CRITICAL	Apache Tomcat Springshell Compromised Host (CVE-2022-22965)	http://10.0.0.19:8080/tomcatwar.jsp?pwd=5cme4e4h302u4w0password	
C1 - CRITICAL	Default Credentials - Nmap	10.0.0.19	root:5h4mp3y - Valid credentials
C1 - CRITICAL	Joomla! Unsupported Version Detection	10.0.0.19:8012	The remote host contains an unsupported version of Joomla!
C1 - CRITICAL	Nuclei Vulnerability Scan	[knew-default:login]	http://10.0.0.19:8080/login.php
C1 - CRITICAL	SQLMap SQL Injection	10.0.0.19	Payload: username=U7u/ AND (SELECT(SLEEP(5)))7u/ AND 'SnQ'='SnQ&password= 10.0.0.19
C1 - CRITICAL	SQLMap SQL Injection	10.0.0.19	back-end DBMS: MySQL -- 5.0.10 10.0.0.19
C1 - CRITICAL	nginx 0.8.x + 1.20.1 14byte Memory Overwrite RCE	10.0.0.19:8080	The remote web server is affected by a remote code execution vulnerability.
C1 - CRITICAL	nginx 0.8.x + 1.20.1 14byte Memory Overwrite RCE	10.0.0.19:8089	The remote web server is affected by a remote code execution vulnerability.
C2 - HIGH	Apache Tomcat Springshell Remote Code Execution (CVE-2022-22965)	http://10.0.0.19:8089 [k4c1-D05E_1NOT_ENVST]	Apache Tomcat/9.0.0
C2 - HIGH	Burpsuite Vulnerability Scan	10.0.0.19	Client sent submission of password - http://10.0.0.19:8080/leavamp3e/ap/Security/protected/index.jsp
C2 - HIGH	Burpsuite Vulnerability Scan	10.0.0.19	00E5Scan - 01 - [Expression Language] Injection - http://10.0.0.19:8080/docs/structure/startup/ServerStartup.pdf
C2 - HIGH	Burpsuite Vulnerability Scan	10.0.0.19	00E5Scan - Local File Include - web.xml retrieved - http://10.0.0.19:8080/docs/appdev/web.xml.txt
C2 - HIGH	Burpsuite Vulnerability Scan	10.0.0.19	Possible 403 Bypass - http://10.0.0.19:8080/host-manager.html
C2 - HIGH	Burpsuite Vulnerability Scan	10.0.0.19	Possible 403 Bypass - http://10.0.0.19:8080/manager/status
C2 - HIGH	Burpsuite Vulnerability Scan	10.0.0.19	Websocket URL poisoning (DOM based) - http://10.0.0.19:8080/leavamp3e/websocket/testu.xhtml
C2 - HIGH	CGI Generic SQL Injection (blind time based)	10.0.0.19:8087	
C2 - HIGH	CGI Generic SQL Injection (blind)	10.0.0.19:8080	A CGI application hosted on the remote web server is potentially
C2 - HIGH	CGI Generic SQL Injection (blind)	10.0.0.19:8087	A CGI application hosted on the remote web server is potentially
C2 - HIGH	Clear-Text Protocol - HTTP	http://10.0.0.19:8088/	HTTP/1.1 200 OK

See Sn1per in action



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

SORT




SNIPER
Getting Started

2:13

Getting Started With Sn1per Enterprise

Sn1perSecurity




SNIPER
Running Scans

3:54

Running Scans With Sn1per Enterprise

Sn1perSecurity

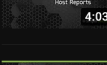


SNIPER
Workspace Reports

2:33

Sn1per Enterprise Workspace Reports

Sn1perSecurity




SNIPER
Host Reports

4:03

Sn1per Enterprise Host Reports

Sn1perSecurity




SNIPER
Nessus Integration

1:50

Sn1per Enterprise Nessus Integration

Sn1perSecurity




SNIPER
OpenVAS GVM Integration

1:50

Sn1per Enterprise OpenVAS GVM Integration

Sn1perSecurity



SNIPER
Burpsuite Professional Integration

1:32

Sn1per Enterprise Burpsuite Professional Integration

Sn1perSecurity

News

- [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:

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

Docker Install



Kali Linux-based Sn1per

1. Run the Docker Compose file

```
sudo docker compose up
```



2. Run the container

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



BlackArch-based Sn1per

1. Run the Docker Compose file

```
sudo docker compose -f docker-compose-blacki
```



2. Run the container

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



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 WEBSKAN 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

```
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 WEBSKAN 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|mon

[*] 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 license and legal information, refer to the [LICENSE.md](#) file in this repository.

Purchase Sn1per Professional

To obtain a Sn1per Professional license, go to <https://sn1persecurity.com>.

External attack surface management, Attack surface monitoring, Attack Surface Management Platform, Attack Surface Management Solutions, Vulnerability management, Threat intelligence, Cybersecurity risk assessment, Security posture assessment, Digital footprint analysis, Attack surface mapping, Web application security, Network security, Infrastructure security, Cloud security, Third-party risk management, Incident response, Penetration testing, Asset discovery, Patch management, Security scanning, Firewall configuration, Intrusion detection system, Security awareness training, Data breach prevention, Web server security, Endpoint security, Phishing protection, Vulnerability assessment, Network security, Web application testing, Ethical hacking, Security assessment, Information security, Red teaming, Cybersecurity testing, Pen testing tools, Exploitation techniques, Wireless network testing, Social engineering, Security auditing, Incident response, Intrusion detection, Firewall testing, Security assessment methodology, Risk assessment, Security controls, Web vulnerability scanning, Password cracking, Security testing services, Security architecture, System hardening, Network reconnaissance, Red teaming, Penetration testing, Cybersecurity, Vulnerability assessment, Attack simulation, Threat intelligence, Risk assessment, Security testing,

