Installing and Using Sn1per for Advanced Penetration Testing and Reconnaissance

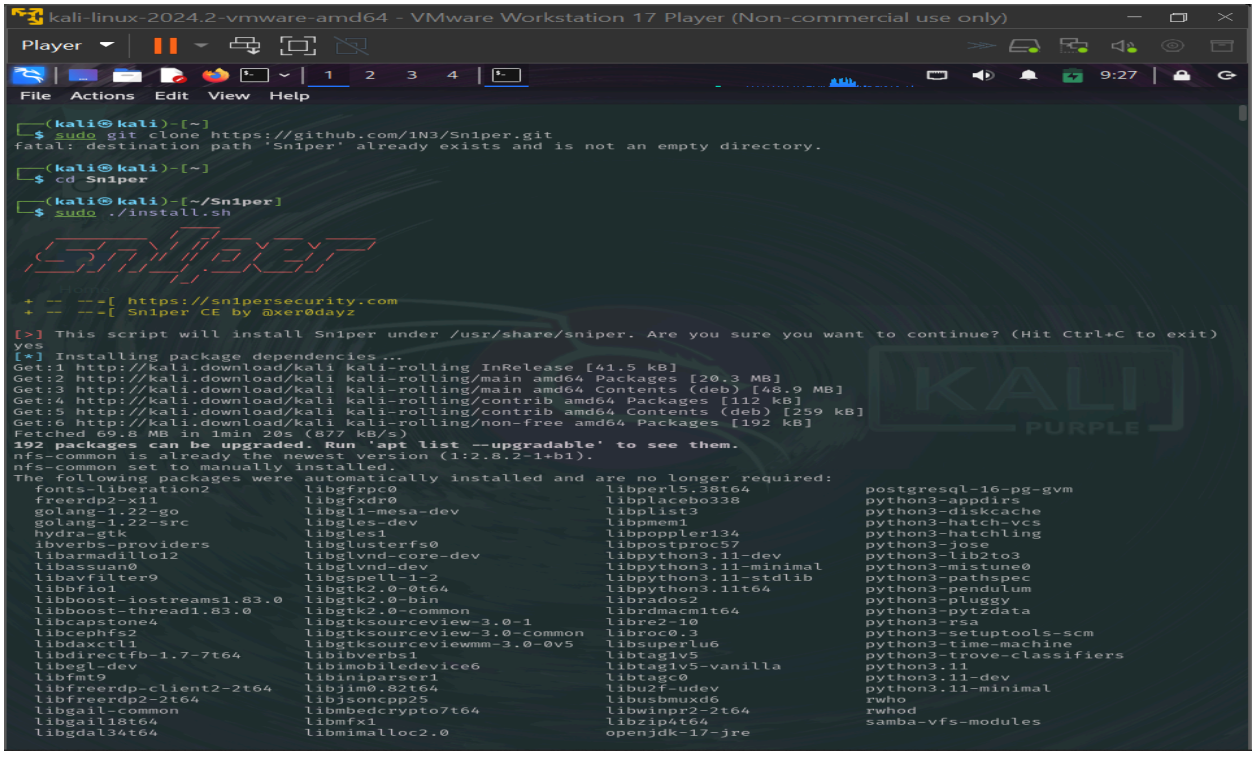
Tools : KALI LINUX, SN1PER
Site : 10.10.66.138

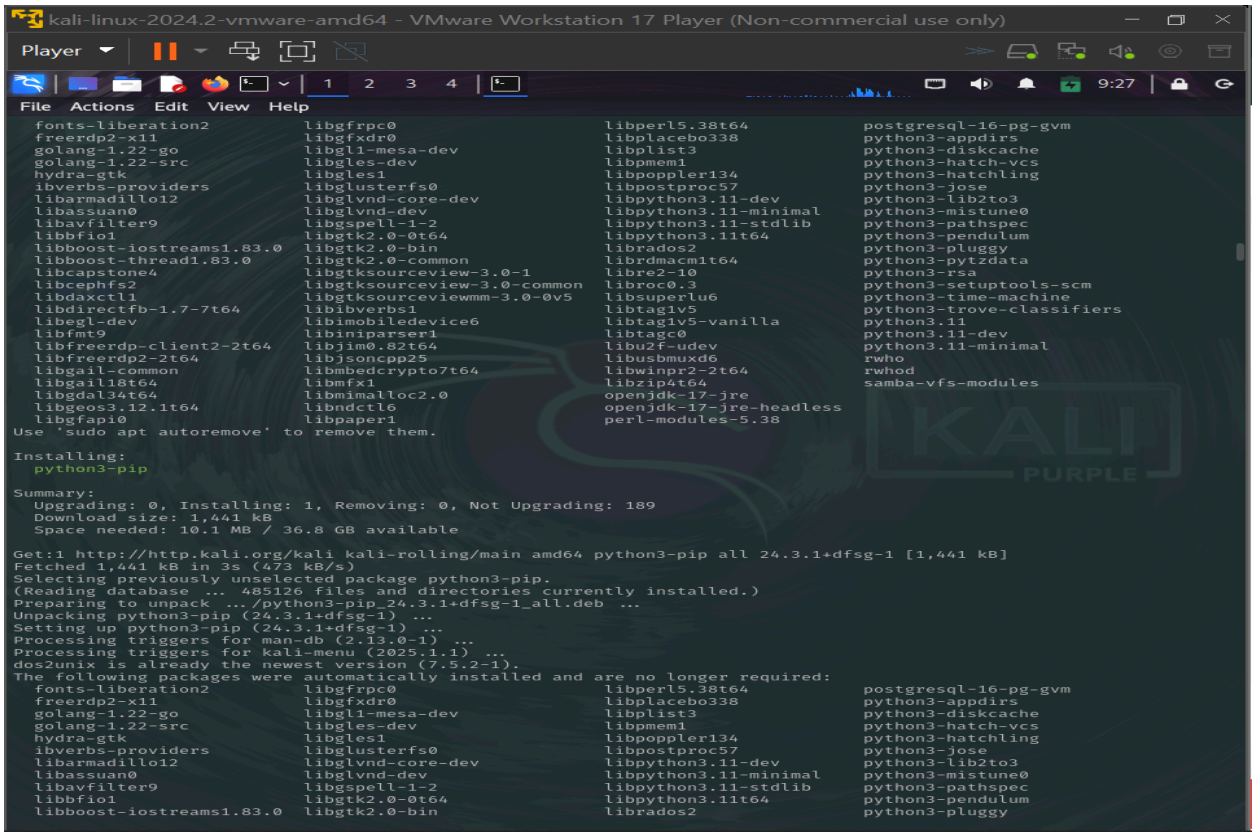
Sn1per: Offensive Security Reconnaissance Scanner

Introduction

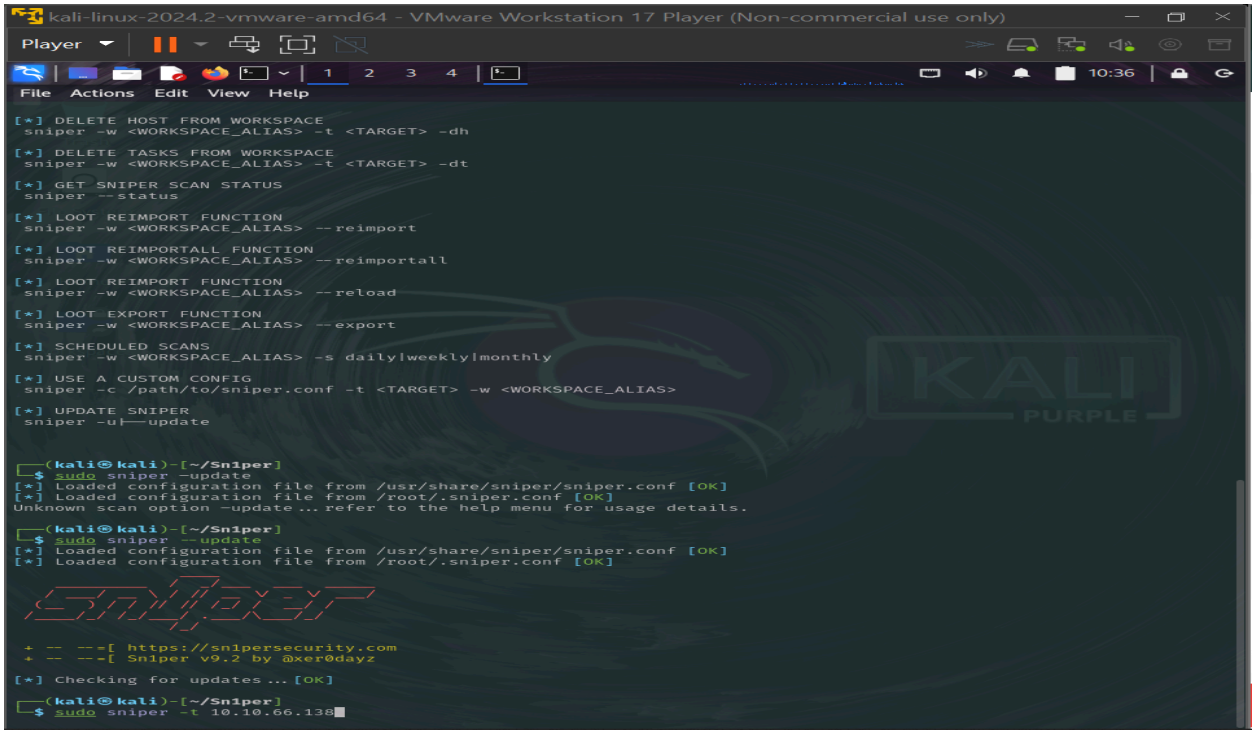
Sn1per is a **powerful open-source reconnaissance and penetration testing tool** designed to assist ethical hackers, security professionals, and red teamers in identifying vulnerabilities across networks, applications, and web services. It automates **information gathering, vulnerability assessment, and exploit enumeration**, making it an essential tool for cybersecurity experts.

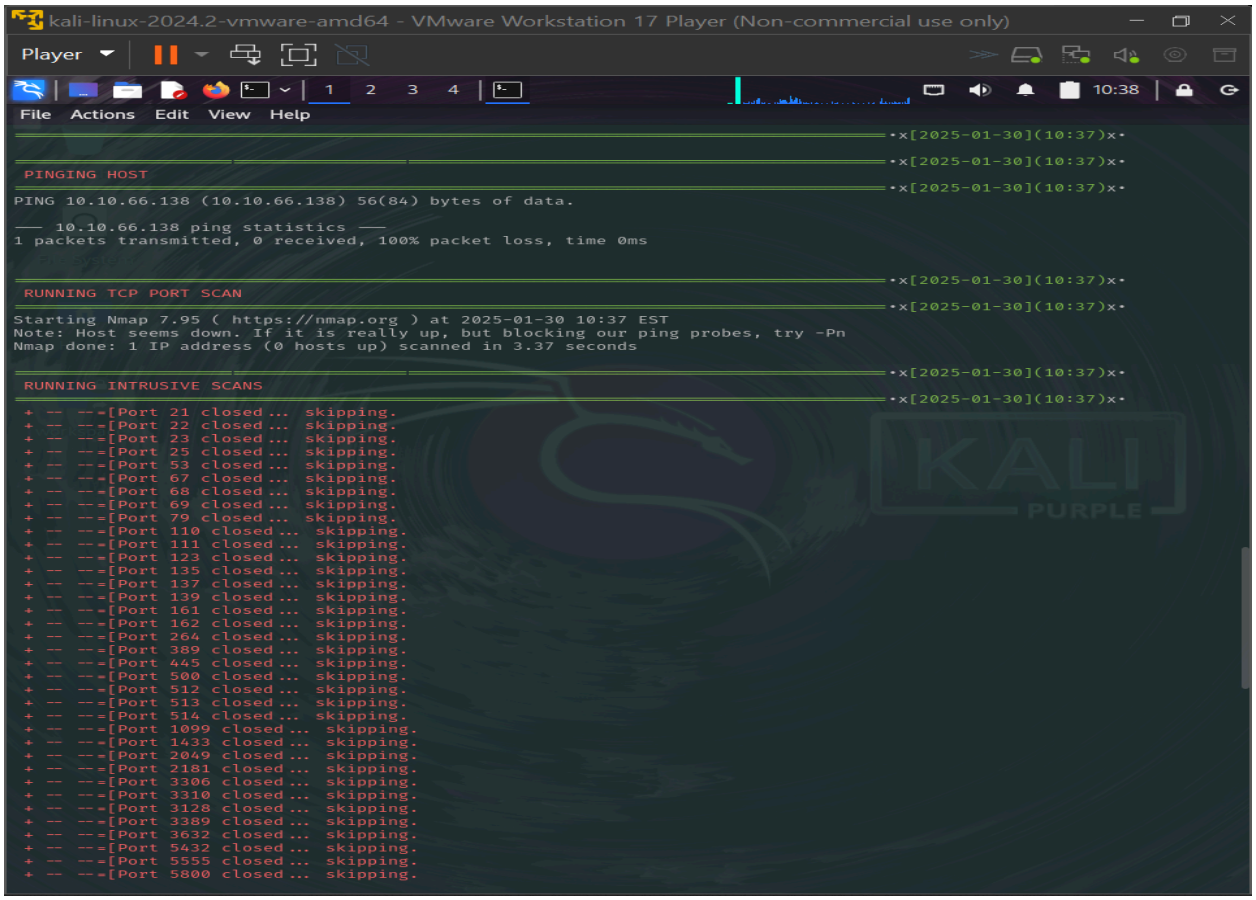
Input from kali :

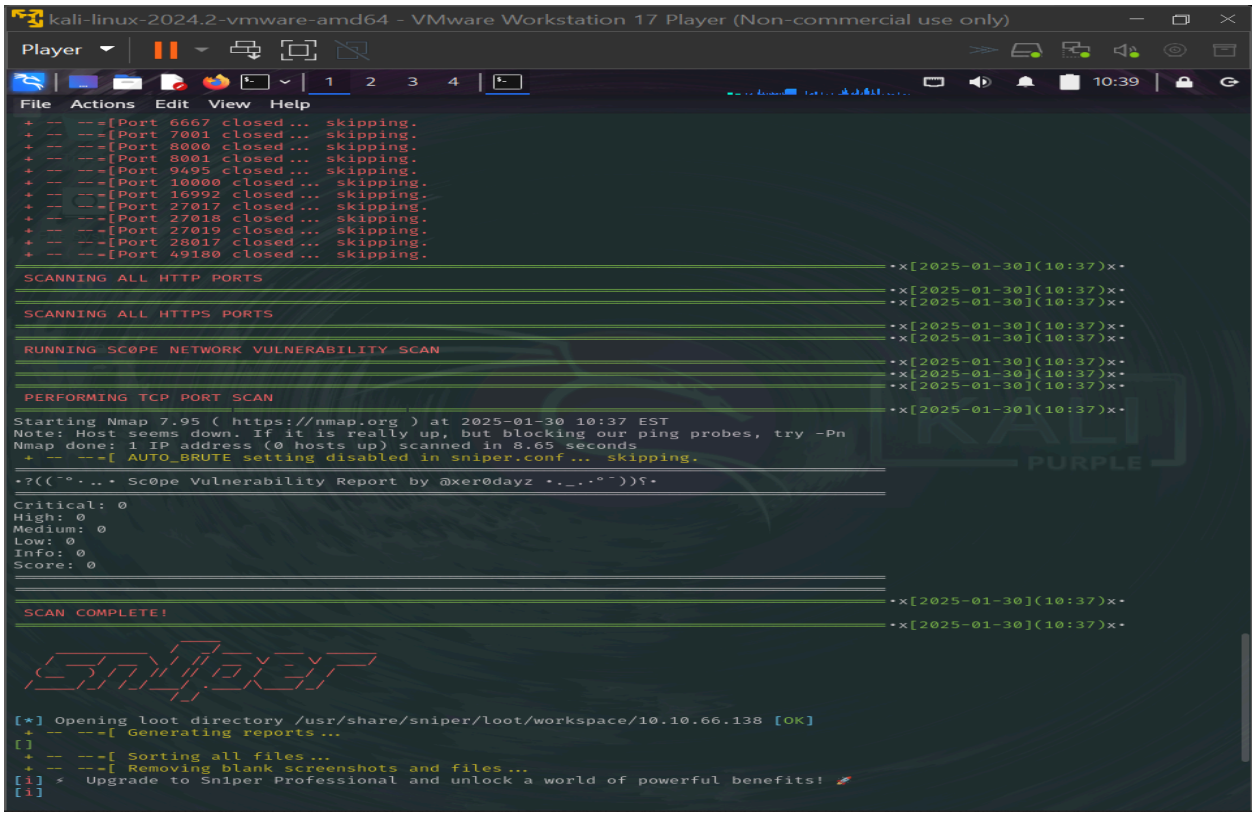


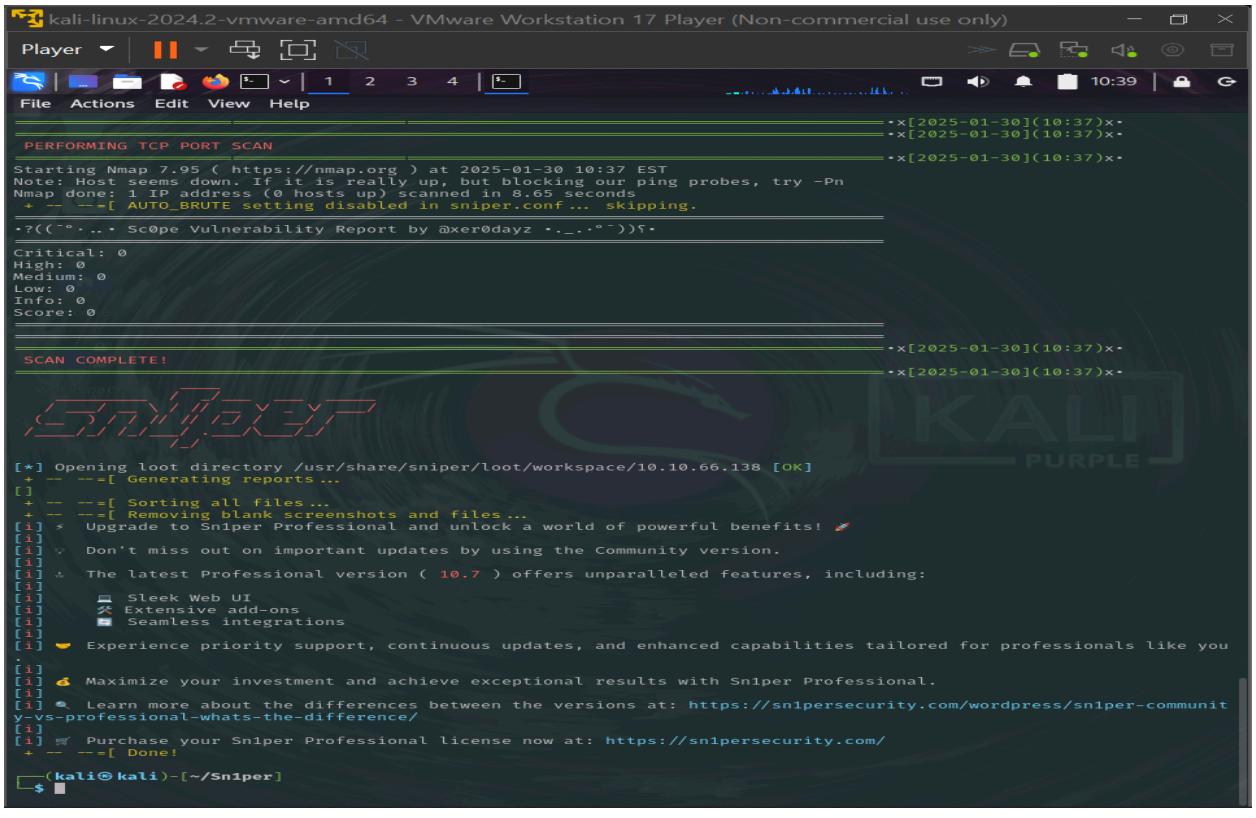

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
fonts-liberation2 libgfrpc0 libperl5.38t64 postgresql-16-pg-gvm
freerdp2-x11 libgfxdr0 libplacebo338 python3-appdirs
golang-1.22-go libgl1-mesa-dev libplist3 python3-diskcache
golang-1.22-src libgles-dev libpmem1 python3-hatch-vcs
hydra-gtk libgles1 libpoppler134 python3-hatchling
ibverbs-providers libglusterfs0 libpostproc57 python3-jose
libarmadillo12 libglvnd-core-dev libpython3.11-dev python3-lib2to3
libassuan0 libglvnd-dev libpython3.11-minimal python3-mistune0
libavfilter9 libgspell-1-2 libpython3.11-stdlib python3-pathspec
libbfio1 libgtk2.0-0t64 libpython3.11t64 python3-pendulum
libboost-iostreams1.83.0 libgtk2.0-bin librados2 python3-pluggy
libboost-thread1.83.0 libgtk2.0-common librdmacm1t64 python3-pytzdata
libcapstone4 libgtksourceview-3.0-1 libre2-10 python3-rsa
libcephfs2 libgtksourceview-3.0-common libroc0.3 python3-setuptools-scm
libdaxctl1 libgtksourceviewmm-3.0-0v5 libsuperlu6 python3-time-machine
libdirectfb-1.7-7t64 libibverbs1 libtag1v5 python3-trove-classifiers
libegl-dev libimobiledevice6 libtag1v5-vanilla python3.11
libfmt9 libiniparser1 libtagc0 python3.11-dev
libfreerdp-client2-2t64 libjim0.82t64 libu2f-udev python3.11-minimal
libfreerdp2-2t64 libjsoncpp25 libusbmuxd6 rwho
libgail-common libmbedcrypto7t64 libwinpr2-2t64 rwhod
libgail18t64 libmfx1 libzip4t64 samba-vfs-modules
libgdal34t64 libmimalloc2.0 openjdk-17-jre
libgeos3.12.1t64 libndctl6 openjdk-17-jre-headless
libgfapi0 libpaper1 perl-modules-5.38
Use 'sudo apt autoremove' to remove them.
Installing:
python3-pip
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 189
Download size: 1,441 kB
Space needed: 10.1 MB / 36.8 GB available
Get:1 http://http.kali.org/kali kali-rolling/main amd64 python3-pip all 24.3.1+dfsg-1 [1,441 kB]
Fetched 1,441 kB in 3s (473 kB/s)
Selecting previously unselected package python3-pip.
(Reading database ... 485126 files and directories currently installed.)
Preparing to unpack .../python3-pip_24.3.1+dfsg-1_all.deb ...
Unpacking python3-pip (24.3.1+dfsg-1) ...
Setting up python3-pip (24.3.1+dfsg-1) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...
dos2unix is already the newest version (7.5.2-1).
The following packages were automatically installed and are no longer required:
fonts-liberation2 libgfrpc0 libperl5.38t64 postgresql-16-pg-gvm
freerdp2-x11 libgfxdr0 libplacebo338 python3-appdirs
golang-1.22-go libgl1-mesa-dev libplist3 python3-diskcache
golang-1.22-src libgles-dev libpmem1 python3-hatch-vcs
hydra-gtk libgles1 libpoppler134 python3-hatchling
ibverbs-providers libglusterfs0 libpostproc57 python3-jose
libarmadillo12 libglvnd-core-dev libpython3.11-dev python3-lib2to3
libassuan0 libglvnd-dev libpython3.11-minimal python3-mistune0
libavfilter9 libgspell-1-2 libpython3.11-stdlib python3-pathspec
libbfio1 libgtk2.0-0t64 libpython3.11t64 python3-pendulum
libboost-iostreams1.83.0 libgtk2.0-bin librados2 python3-pluggy


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
(kali㉿kali)-[~/Sn1per]
$ sudo sniper -help | more
[sudo] password for kali:
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
Unknown scan option -help ... refer to the help menu for usage details.
(kali㉿kali)-[~/Sn1per]
$ sudo sniper --help | more
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
+ -- --=[https://sn1persecurity.com
+ -- --=[Sn1per v9.2 by @xer0dayz
[*] NORMAL MODE
sniper -t <TARGET>
[*] SPECIFY CUSTOM CONFIG FILE
sniper -c /full/path/to/sniper.conf -t <TARGET> -m <MODE> -w <WORKSPACE>
[*] 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 <WORSPACE_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


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
10:36
[*] DELETE HOST FROM WORKSPACE
sniper -w <WORKSPACE_ALIAS> -t <TARGET> -dh
[*] DELETE TASKS FROM WORKSPACE
sniper -w <WORKSPACE_ALIAS> -t <TARGET> -dt
[*] 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
(kali㉿kali)-[~/Sn1per]
$ sudo sniper -update
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
Unknown scan option -update ... refer to the help menu for usage details.
(kali㉿kali)-[~/Sn1per]
$ sudo sniper --update
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
+ -- --=[https://sn1persecurity.com
+ -- --=[Sn1per v9.2 by @xer0dayz
[*] Checking for updates ... [OK]
(kali㉿kali)-[~/Sn1per]
$ sudo sniper -t 10.10.66.138


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
10:38
x[2025-01-30](10:37)x
PINGING HOST
PING 10.10.66.138 (10.10.66.138) 56(84) bytes of data.
10.10.66.138 ping statistics
1 packets transmitted, 0 received, 100% packet loss, time 0ms
RUNNING TCP PORT SCAN
Starting Nmap 7.95 (https://nmap.org) at 2025-01-30 10:37 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.37 seconds
RUNNING INTRUSIVE SCANS
+ -- --=[Port 21 closed ... skipping.
+ -- --=[Port 22 closed ... skipping.
+ -- --=[Port 23 closed ... skipping.
+ -- --=[Port 25 closed ... skipping.
+ -- --=[Port 53 closed ... skipping.
+ -- --=[Port 67 closed ... skipping.
+ -- --=[Port 68 closed ... skipping.
+ -- --=[Port 69 closed ... skipping.
+ -- --=[Port 79 closed ... skipping.
+ -- --=[Port 110 closed ... skipping.
+ -- --=[Port 111 closed ... skipping.
+ -- --=[Port 123 closed ... skipping.
+ -- --=[Port 135 closed ... skipping.
+ -- --=[Port 137 closed ... skipping.
+ -- --=[Port 139 closed ... skipping.
+ -- --=[Port 161 closed ... skipping.
+ -- --=[Port 162 closed ... skipping.
+ -- --=[Port 264 closed ... skipping.
+ -- --=[Port 389 closed ... skipping.
+ -- --=[Port 445 closed ... skipping.
+ -- --=[Port 500 closed ... skipping.
+ -- --=[Port 512 closed ... skipping.
+ -- --=[Port 513 closed ... skipping.
+ -- --=[Port 514 closed ... skipping.
+ -- --=[Port 1099 closed ... skipping.
+ -- --=[Port 1433 closed ... skipping.
+ -- --=[Port 2049 closed ... skipping.
+ -- --=[Port 2181 closed ... skipping.
+ -- --=[Port 3306 closed ... skipping.
+ -- --=[Port 3310 closed ... skipping.
+ -- --=[Port 3128 closed ... skipping.
+ -- --=[Port 3389 closed ... skipping.
+ -- --=[Port 3632 closed ... skipping.
+ -- --=[Port 5432 closed ... skipping.
+ -- --=[Port 5555 closed ... skipping.
+ -- --=[Port 5800 closed ... skipping.


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
10:39
+ -- --=[Port 6667 closed ... skipping.
+ -- --=[Port 7001 closed ... skipping.
+ -- --=[Port 8000 closed ... skipping.
+ -- --=[Port 8001 closed ... skipping.
+ -- --=[Port 9495 closed ... skipping.
+ -- --=[Port 10000 closed ... skipping.
+ -- --=[Port 16992 closed ... skipping.
+ -- --=[Port 27017 closed ... skipping.
+ -- --=[Port 27018 closed ... skipping.
+ -- --=[Port 27019 closed ... skipping.
+ -- --=[Port 28017 closed ... skipping.
+ -- --=[Port 49180 closed ... skipping.
SCANNING ALL HTTP PORTS
SCANNING ALL HTTPS PORTS
RUNNING SC0PE NETWORK VULNERABILITY SCAN
PERFORMING TCP PORT SCAN
Starting Nmap 7.95 (https://nmap.org) at 2025-01-30 10:37 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 8.65 seconds
+ -- --=[AUTO_BRUTE setting disabled in sniper.conf ... skipping.
Sc0pe Vulnerability Report by @xer0dayz
Critical: 0
High: 0
Medium: 0
Low: 0
Info: 0
Score: 0
SCAN COMPLETE!
[*] Opening loot directory /usr/share/sniper/loot/workspace/10.10.66.138 [OK]
+ -- --=[Generating reports ...
+ -- --=[Sorting all files ...
+ -- --=[Removing blank screenshots and files ...
[i] Upgrade to Sn1per Professional and unlock a world of powerful benefits!


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
10:39
PERFORMING TCP PORT SCAN
Starting Nmap 7.95 (https://nmap.org) at 2025-01-30 10:37 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 8.65 seconds
+ -- --=[AUTO_BRUTE setting disabled in sniper.conf ... skipping.
Sc0pe Vulnerability Report by @xer0dayz
Critical: 0
High: 0
Medium: 0
Low: 0
Info: 0
Score: 0
SCAN COMPLETE!
[*] Opening loot directory /usr/share/sniper/loot/workspace/10.10.66.138 [OK]
+ -- --=[Generating reports ...
+ -- --=[Sorting all files ...
+ -- --=[Removing blank screenshots and files ...
[i] Upgrade to Sn1per Professional and unlock a world of powerful benefits!
[i] Don't miss out on important updates by using the Community version.
[i] The latest Professional version (10.7) offers unparalleled features, including:
Sleek Web UI
Extensive add-ons
Seamless integrations
[i] Experience priority support, continuous updates, and enhanced capabilities tailored for professionals like you.
[i] Maximize your investment and achieve exceptional results with Sn1per Professional.
[i] Learn more about the differences between the versions at: https://sn1persecurity.com/wordpress/sn1per-community-vs-professional-whats-the-difference/
[i] Purchase your Sn1per Professional license now at: https://sn1persecurity.com/
+ -- --=[Done!
(kali㉿kali)-[~/Sn1per]
$

Unlike many pre-installed penetration testing tools in **Kali Linux**, Sn1per is **not included by default**. Therefore, we must download and install it manually. This guide provides a step-by-step approach to setting up, configuring, and using Sn1per effectively.

Step 1: Downloading Sn1per

Since Sn1per is not bundled with Kali Linux, we need to **clone the official GitHub repository** to obtain the latest version. Open a **terminal** and run the following command:

```
sudo git clone https://github.com/1N3/Sn1per.git
```

This command fetches the **Sn1per source code** and its associated files from the repository.

Step 2: Installing Sn1per

Once the repository is downloaded, navigate into the **Sn1per** directory and initiate the installation process:

```
cd Sn1per
```

```
sudo ./install.sh
```

This installation script will:
✅ **Install dependencies** such as `nmap`, `metasploit`, `whatweb`, and other reconnaissance tools.
✅ **Configure necessary settings** to optimize Sn1per's performance.
✅ **Integrate Sn1per into your Kali Linux environment** for seamless execution.

🔹 **Note:** The installation process may take some time, as it downloads and sets up all required packages.

Once the installation is complete, **close your terminal** and open a new one to start using Sn1per.

Step 3: Viewing the Help Menu

To explore Sn1per's capabilities and available commands, use:

```
sudo sn1per --help | more
```

The `| more` commands allows you to **scroll through the output** one screen at a time, making it easier to read.

Step 4: Updating Sn1per

Before launching any scans, ensure that Sn1per is **up to date** with the latest security checks and features by running:

```
sudo sn1per --update
```

This ensures that Sn1per has the most recent **vulnerability signatures, exploit methods, and reconnaissance techniques** available.

Step 5: Running a Comprehensive Scan

To perform a **default scan** on a target machine, use:

```
sudo sn1per -t 10.10.66.138
```

Sn1per will automatically:

- Conduct **port scanning** to detect open ports.
- Perform **service enumeration** to identify running applications.
- Detects **potential vulnerabilities** using various security tools.
- Attempt **web application analysis** to find exploitable flaws.

Sn1per integrates with **popular penetration testing frameworks** like:

- **Nmap** – For network scanning and service detection.

- **Metasploit** – To identify known exploits and attack vectors.
- **WhatWeb** – To fingerprint web technologies.
- **Gobuster** – For brute-force directory enumeration.
- **SQLmap** – For SQL injection detection.
- **Smuggler** – To test for HTTP request smuggling.

This makes Sn1per **a highly versatile and powerful security auditing tool**.

Step 6: Understanding Sn1per's Scanning Modes

Sn1per offers various **scanning modes** to suit different penetration testing needs. Below is a detailed breakdown of each mode:

1. NORMAL Mode

```
sudo sn1per -t target.com
```

🔹 **Purpose:** Performs a **basic** scan of the target, detecting open ports and gathering **active** and **passive** reconnaissance data.

2. STEALTH Mode

```
sudo sn1per -t target.com stealth
```

🔹 **Purpose:** Conducts a **non-intrusive scan** to bypass **firewalls (WAF)** and **intrusion prevention systems (IPS)**, minimizing detection.

3. FLYOVER Mode

```
sudo sn1per -t target.com flyover
```

🔹 **Purpose:** Performs a **fast multi-threaded** scan to collect high-level data on multiple hosts simultaneously.

4. AIRSTRIKE Mode

```
sudo sn1per /full/path/to/targets.txt airstrike
```

🔹 **Purpose:** Scans multiple targets from a file and performs **basic fingerprinting** on each one.

5. NUKE Mode

```
sudo sn1per /pentest/loot/targets.txt nuke
```

🔹 **Purpose:** Conducts **full-scale penetration testing** on multiple targets. Ideal for **large-scale security assessments**.

6. DISCOVER Mode

```
sudo sn1per 192.168.0.0/16 discover
```

🔹 **Purpose:** Automatically scans **all hosts within a subnet or CIDR range** and launches reconnaissance on each detected system.

7. WEB Application Modes

Sn1per offers specialized scanning for **web applications**:

WEB Mode:

```
sudo sn1per -t target.com web
```

- ✅ Focuses on **port 80 (HTTP) & 443 (HTTPS)**.
  ✅ Ideal for testing **website security** but may take longer.

MASSWEB Mode:

```
sudo sn1per -f targets.txt massweb
```

- ✅ Runs **web scans** on multiple targets listed in a file.

WEBSCAN Mode:

```
sudo sn1per -t target.com webscan
```

- ✅ Uses **BurpSuite** and **Arachni** for deep web security auditing.

8. VULNERABILITY Scanning Modes

Sn1per integrates with **OpenVAS**, a powerful vulnerability scanner:

VULNSCAN Mode:

```
sudo sn1per -t target.com vulnscan
```

- ✅ Runs **OpenVAS** to detect security flaws.

MASSVULNSCAN Mode:

```
sudo sn1per -f targets.txt massvulnscan
```

- ✅ Scans multiple hosts for vulnerabilities in bulk.

Conclusion

Sn1per is an **exceptionally powerful** penetration testing framework, combining multiple **reconnaissance, vulnerability scanning, and exploitation tools** into a single interface. Whether you're performing **network security assessments, web application testing, or large-scale reconnaissance**, Sn1per offers an **efficient and automated** solution.