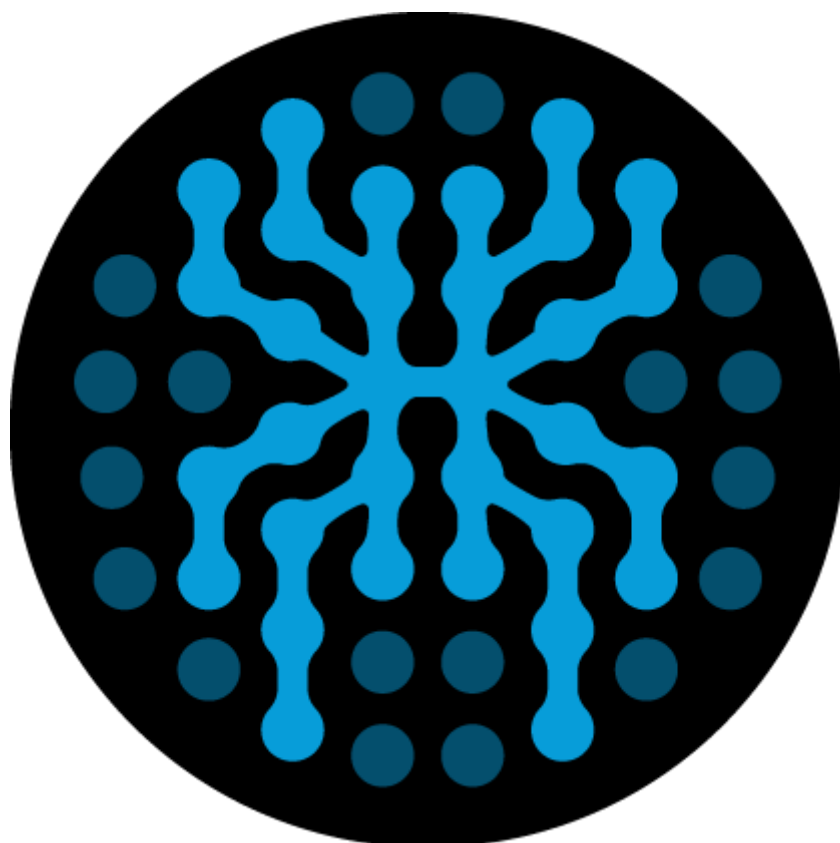


SPIDERFOOT



SPIDERFOOT

SpiderFoot is an open source intelligence (OSINT) tool which automates the process of gathering information about the target system. This tool uses for reconnaissance and gathering information about target system in the field of cybersecurity, threat intelligence and investigations. SpiderFoot can gather information from a wide range of sources, including WHOIS databases, DNS records, social media platforms, public databases, and more.

FEATURES OF SPIDERFOOT

1. **Active and Passive Scanning:** This tool allows both the Active and Passive scanning. In active scanning it interacts with target system directly, while passive scanning does not interact with target system and provide all the information available on the internet. This flexibility allows user to take correct decision during information gathering.
2. **Customizable Module:** This tool allows user to obtain data according to their requirement by customizing the 'by module' given in new scan area.
3. **Analysis and Visualization:** This tool provides feature to analysing and visualizing the collected data about the target. It helps user to identify the pattern and potential security risk of target.
4. **Report Generation:** This tool is capable to generate the report summarizing the collected information. This report can be share for findings purpose and to keep in record.
5. **Wide Range of Data Source:** This tool gathers information from wide range of source i.e., WHOIS database, DNS record, social media platform, public database and many more.
6. **Command Line – Graphical User Interface:** This tool provides both command line and graphical user interface which is easy to use and even individual with no advance technical skills can drive web interface tool very smoothly.
7. **API Support:** SpiderFoot may provide support for APIs, allowing users to integrate it with other security tools and systems.

GUIDE TO INSTALL SPIDERFOOT ON KALI LINUX

1. Open a Terminal:

- You can open the terminal in Kali Linux by clicking in terminal icon or open using the keyboard shortcut **Ctrl + Alt + T**.

2. Update Kali Linux:

- To make sure your Kali Linux is up-to-date run the following command:

Sudo apt update

3. Install SpiderFoot:

- Type the following command and hit enter:

sudo apt install spiderfoot

4. Change Directory to SpiderFoot:

- After installation you need to change the directory by following command:

cd spiderfoot

5. Run SpiderFoot:

- After installation completed you can run SpiderFoot using below command:

Sudo spiderfoot -l 127.0.0.1:5001

6. Access SpiderFoot Web-Interface:

- After executing the above command, you will get response with url then right click on that link and click to open link or open web browser and copy the url from terminal and paste in browser then hit enter.

```
(kali@kali)~$ sudo apt update
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1510 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali@kali)~$ sudo apt install spiderfoot
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  gdal-data gdal-plugins libarmadillo12 libarpack2 libcfitsio10 libfreexl1 libfyba0 libgdal34 libgeos-c1v5 libgeos3.12.1 libgeotiff5 libhdf4-0-alt libhdf5-hl-100 libkmlbase1 libkmlcore1 libkmlengine1 libnetcdf19
  libogdi4.1 libproj25 librttopo1 libspatialite8 libsuperlu6 liburiparser1 libxerces-c3.2 proj-bin proj-data python3-adblockparser python3-cherrypy-cors python3-dock python3-exifread python3-gdal python3-gexf p
  python3-ipwhois python3-networkx python3-phonenumbers python3-pptx python3-publicsuffixlist python3-pygraphviz python3-pydf2 python3-secure python3-whois unixodbc-common
Suggested packages:
  geotiff-bin gdal-bin libgeotiff-epsg libhdf4-doc libhdf4-alt-dev hdf4-tools odbc-postgresql tdsodbc ogdi-bin python-gexf-doc python-ipwhois-doc python-pptx-doc python-pygraphviz-doc
The following NEW packages will be installed:
  gdal-data gdal-plugins libarmadillo12 libarpack2 libcfitsio10 libfreexl1 libfyba0 libgdal34 libgeos-c1v5 libgeos3.12.1 libgeotiff5 libhdf4-0-alt libhdf5-hl-100 libkmlbase1 libkmlcore1 libkmlengine1 libnetcdf19
  libogdi4.1 libproj25 librttopo1 libspatialite8 libsuperlu6 liburiparser1 libxerces-c3.2 proj-bin proj-data python3-adblockparser python3-cherrypy-cors python3-dock python3-exifread python3-gdal python3-gexf p
  python3-ipwhois python3-networkx python3-phonenumbers python3-pptx python3-publicsuffixlist python3-pygraphviz python3-pydf2 python3-secure python3-whois spiderfoot unixodbc-common
0 upgraded, 46 newly installed, 0 to remove and 1510 not upgraded.
Need to get 31.3 MB of archives.
After this operation, 144 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 gdal-data all 3.8.2+dfsg-1 [343 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 gdal-plugins amd64 3.8.2+dfsg-1 [327 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libarpack2 amd64 3.9.1-1 [103 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 libsuperlu6 amd64 6.0.1+dfsg1-1 [170 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 libarmadillo12 amd64 1:12.6.7+dfsg-1 [102 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 libcfitsio10 amd64 4.3.0-2 [505 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libfreexl1 amd64 2.0.0-1 [39.6 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 libfyba0 amd64 4.1.1-8 [112 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 libgeos3.12.1 amd64 3.12.1-1 [877 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 libgeos-c1v5 amd64 3.12.1-1 [97.1 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 proj-data all 9.3.1-1 [6,268 kB]
Get:12 http://kali.download/kali kali-rolling/main amd64 libproj25 amd64 9.3.1-1 [1,343 kB]
Get:13 http://kali.download/kali kali-rolling/main amd64 libgeotiff5 amd64 1.7.1-5 [68.2 kB]
```

SPIDERFOOT INSTALLATION STEP: 1, 2 & 3 SCREENSHOT

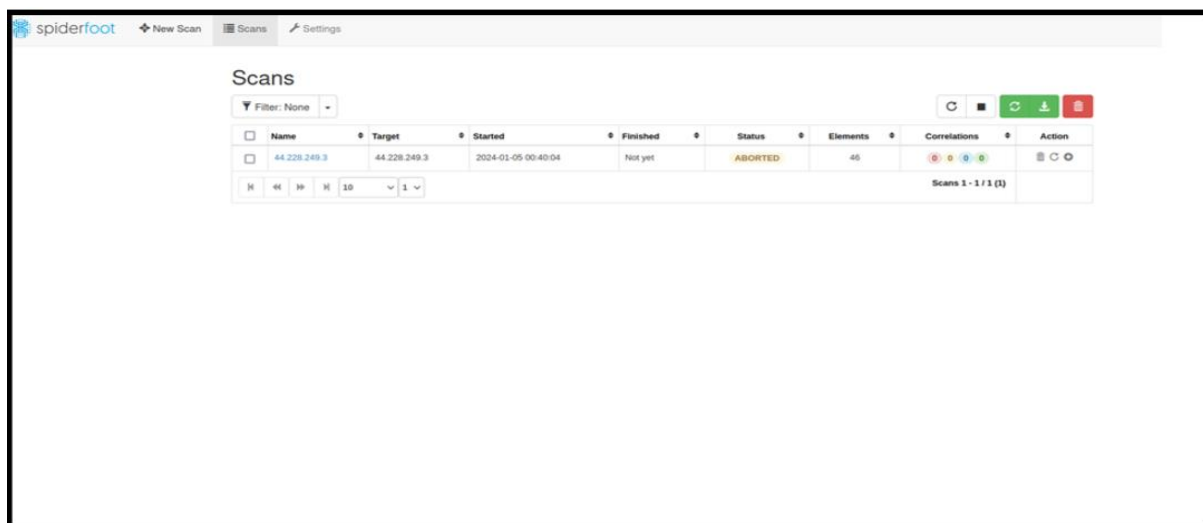
```
(kali@kali)~$ cd spiderfoot

(kali@kali)~/spiderfoot$ spiderfoot -l 127.0.0.1:5001
2024-01-07 03:12:40,626 [INFO] sf : Starting web server at 127.0.0.1:5001 ...

Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5001/

2024-01-07 03:12:40,645 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****
```

SPIDERFOOT INSTALLATION STEP: 4 & 5 SCREENSHOT



SPIDERFOOT WEB-INTERFACE STEP: 6

ADVANTAGES OF SPIDERFOOT TOOL

1. **Regular Updates:** This tool is actively maintained and updated by the community. Which helps other users to get updated information about risk and other parameters during information gathering process.
2. **Cross-Platform Compatibility:** SpiderFoot is designed to be cross platform tool so that users can run this tool on various operating system such as Linux, Windows OS & Mac OS.

HOW TO SCAN USING INTERFACE

Once the user access to the web-interface of SpiderFoot, then simply user needs to enter the **scan name** and **scan target** details. After entering the details, you'll see there are four different scan categories to gather information about target. Choose according to your requirement and then click on **RUN SCAN NOW**.

The screenshot displays the SpiderFoot web interface. At the top, there's a navigation bar with 'spiderfoot' logo, 'New Scan', 'Scans', and 'Settings' tabs. Below this, the 'Scan Name' field contains 'Test' and the 'Scan Target' field contains 'tryhackme.com'. To the right of these fields, a box lists supported input formats: Domain Name, IPv4 Address, IPv6 Address, Hostname-Sub-domain, Subnet, Bitcoin Address, E-mail address, Phone Number, Human Name, Username, and Network ASN. Below the input fields, there are three tabs: 'By Use Case', 'By Required Data', and 'By Module'. Under 'By Use Case', four options are listed: 'All' (selected), 'Footprint', 'Investigate', and 'Passive'. Each option has a brief description of what it will gather. At the bottom of the form is a red 'Run Scan Now' button. A footer message says 'Want more OSINT automation capabilities? Check out SpiderFoot HX.'

NEW SCAN ON SPIDERFOOT WEB-INTERFACE

REFERENCES

<https://linux-packages.com/kali-linux/package/spiderfoot>

<https://www.youtube.com/>

<https://chat.openai.com/>