



SpiderFoot

Information Security Inc.

Contents

- About SpiderFoot
- What can I do with SpiderFoot?
- Install SpiderFoot
- Run SpiderFoot
- References

About SpiderFoot

- SpiderFoot is an open source intelligence automation tool. Its goal is to automate the process of gathering intelligence about a given target, which may be an IP address, domain name, hostname or network subnet



What can I do with SpiderFoot?

- The data returned from a SpiderFoot scan will reveal a lot of information about your target, providing insight into possible data leaks, vulnerabilities or other sensitive information that can be leveraged during a penetration test, red team exercise or for threat intelligence

Install SpiderFoot

- Install dependencies

```
# pip install lxml netaddr M2Crypto cherrypy mako requests bs4
Requirement already satisfied: lxml in /usr/local/lib/python2.7/dist-packages
Requirement already satisfied: netaddr in /usr/lib/python2.7/dist-packages
Requirement already satisfied: M2Crypto in /usr/lib/python2.7/dist-packages
Collecting cherrypy
  Downloading CherryPy-14.0.0-py2.py3-none-any.whl (430kB)
    100% |#####| 440kB 2.1MB/s
Requirement already satisfied: mako in /usr/lib/python2.7/dist-packages
Requirement already satisfied: requests in /usr/local/lib/python2.7/dist-packages
Requirement already satisfied: bs4 in /usr/local/lib/python2.7/dist-packages
Collecting portend>=2.1.1 (from cherrypy)
  Downloading portend-2.2-py2.py3-none-any.whl
Collecting cheroot>=5.9.1 (from cherrypy)
  Downloading cheroot-6.0.0-py2.py3-none-any.whl (61kB)
    100% |#####| 71kB 4.1MB/s
Requirement already satisfied: six>=1.11.0 in /usr/lib/python2.7/dist-packages (from cherrypy)
Requirement already satisfied: certifi>=2017.4.17 in /usr/lib/python2.7/dist-packages (from requests)
Requirement already satisfied: chardet<3.1.0,>=3.0.2 in /usr/lib/python2.7/dist-packages (from requests)
Requirement already satisfied: urllib3<1.22,>=1.21.1 in /usr/local/lib/python2.7/dist-packages (from requests)
Requirement already satisfied: idna<2.6,>=2.5 in /usr/local/lib/python2.7/dist-packages (from requests)
Requirement already satisfied: beautifulsoup4 in /usr/local/lib/python2.7/dist-packages (from bs4)
Collecting tempora>=1.8 (from portend>=2.1.1->cherrypy)
  Downloading tempora-1.10-py2.py3-none-any.whl
Collecting more-itertools>=2.6 (from cheroot>=5.9.1->cherrypy)
  Downloading more-itertools-4.1.0-py2-none-any.whl (47kB)
    100% |#####| 51kB 4.9MB/s
Requirement already satisfied: pytz in /usr/local/lib/python2.7/dist-packages (from tempora>=1.8->portend>=2.1.1->cherrypy)
Installing collected packages: tempora, portend, more-itertools, cheroot, cherrypy
Successfully installed cheroot-6.0.0 cherrypy-14.0.0 more-itertools-4.1.0 portend-2.2 tempora-1.10
```

Install SpiderFoot

- Clone the GitHub repository

```
# git clone https://github.com/smicallef/spiderfoot.git
Cloning into 'spiderfoot'...
remote: Counting objects: 5369, done.
remote: Total 5369 (delta 0), reused 0 (delta 0), pack-reused 5369
Receiving objects: 100% (5369/5369), 5.76 MiB | 1.41 MiB/s, done.
Resolving deltas: 100% (3818/3818), done.
```

Run SpiderFoot

- Run SpiderFoot

```
~/spiderfoot# python sf.py 0.0.0.0:5001
Starting web server at http://0.0.0.0:5001 ...

*****
Use SpiderFoot by starting your web browser of choice and
browse to http://<IP of this host>:5001
*****

[09/Feb/2018:17:09:20] ENGINE Listening for SIGHUP.
[09/Feb/2018:17:09:20] ENGINE Listening for SIGTERM.
[09/Feb/2018:17:09:20] ENGINE Listening for SIGUSR1.
[09/Feb/2018:17:09:20] ENGINE Bus STARTING
[09/Feb/2018:17:09:20] ENGINE Serving on http://0.0.0.0:5001
[09/Feb/2018:17:09:20] ENGINE Bus STARTED
```

Run SpiderFoot

- Run a New Scan, scan using Tor “Onion City” search engine

The screenshot shows the SpiderFoot web interface in a browser. The address bar displays the URL `192.168.10.12:5001/newscan#`. The page title is "SpiderFoot" and the navigation bar includes "New Scan", "Scans", "Settings", and "About". The "New Scan" form is active, with the "Scan Name" field containing "Onion" and the "Seed Target" field containing "rtma.tk". A tooltip titled "Usage" is displayed over the form, providing instructions on target formats: "The *Seed Target* can be one of the following. SpiderFoot will automatically detect the target type based on the format of your input." The tooltip lists examples for Domain Name, IP Address, Hostname/Sub-domain, Subnet, and E-mail address. Below the form, there are two buttons: "Select All" and "De-Select All". A list of checkboxes is visible, including "abuse.ch", "Accounts", "AdBlock Check", "Ahmia", "AlienVault OTX", "AlienVault IP Reputation", and "Archive.org".

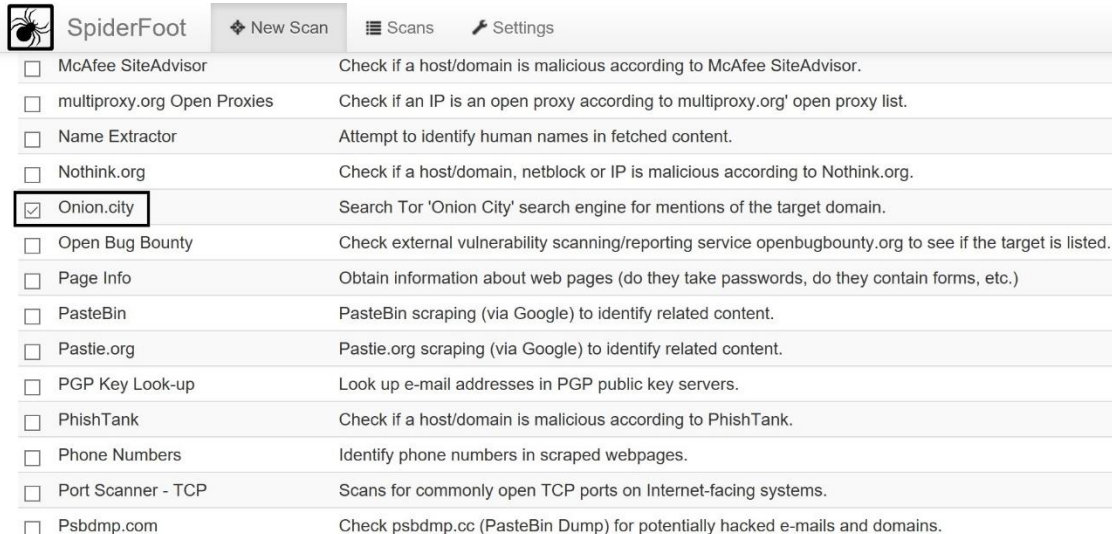
Usage

The *Seed Target* can be one of the following. SpiderFoot will automatically detect the target type based on the format of your input.

Domain Name: e.g. *example.com*
IP Address: e.g. *1.2.3.4*
Hostname/Sub-domain: e.g. *abc.example.com*
Subnet: e.g. *1.2.3.0/24*
E-mail address: e.g. *bob@example.com*

Run SpiderFoot

- Run a New Scan, scan using Tor “Onion City” search engine



The screenshot shows the SpiderFoot web interface. At the top, there is a navigation bar with the SpiderFoot logo, a 'New Scan' button, and links for 'Scans' and 'Settings'. Below the navigation bar is a list of scan options, each with a checkbox and a description. The 'Onion.city' option is selected, and its checkbox and label are highlighted with a red box.

Scan Option	Description
<input type="checkbox"/> McAfee SiteAdvisor	Check if a host/domain is malicious according to McAfee SiteAdvisor.
<input type="checkbox"/> multiproxy.org Open Proxies	Check if an IP is an open proxy according to multiproxy.org' open proxy list.
<input type="checkbox"/> Name Extractor	Attempt to identify human names in fetched content.
<input type="checkbox"/> Nothink.org	Check if a host/domain, netblock or IP is malicious according to Nothink.org.
<input checked="" type="checkbox"/> Onion.city	Search Tor 'Onion City' search engine for mentions of the target domain.
<input type="checkbox"/> Open Bug Bounty	Check external vulnerability scanning/reporting service openbugbounty.org to see if the target is listed.
<input type="checkbox"/> Page Info	Obtain information about web pages (do they take passwords, do they contain forms, etc.)
<input type="checkbox"/> PasteBin	PasteBin scraping (via Google) to identify related content.
<input type="checkbox"/> Pastie.org	Pastie.org scraping (via Google) to identify related content.
<input type="checkbox"/> PGP Key Look-up	Look up e-mail addresses in PGP public key servers.
<input type="checkbox"/> PhishTank	Check if a host/domain is malicious according to PhishTank.
<input type="checkbox"/> Phone Numbers	Identify phone numbers in scraped webpages.
<input type="checkbox"/> Port Scanner - TCP	Scans for commonly open TCP ports on Internet-facing systems.
<input type="checkbox"/> Psbdmp.com	Check psbdmp.cc (PasteBin Dump) for potentially hacked e-mails and domains.

Run SpiderFoot

- Run a New Scan, scan using Tor “Onion City” search engine

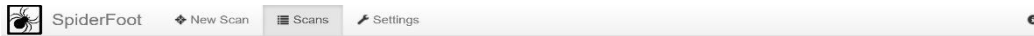
<input type="checkbox"/>	Wikipedia Edits	Identify edits to Wikipedia articles made from a given IP address or username.
<input type="checkbox"/>	XForce Exchange 	Obtain information from IBM X-Force Exchange
<input type="checkbox"/>	Yahoo	Some light Yahoo scraping to identify sub-domains and links.
<input type="checkbox"/>	Zone-H Defacement Check	Check if a hostname/domain appears on the zone-h.org 'special defacements' RSS feed.

Run Scan

Note: Scan will be started immediately.

Run SpiderFoot

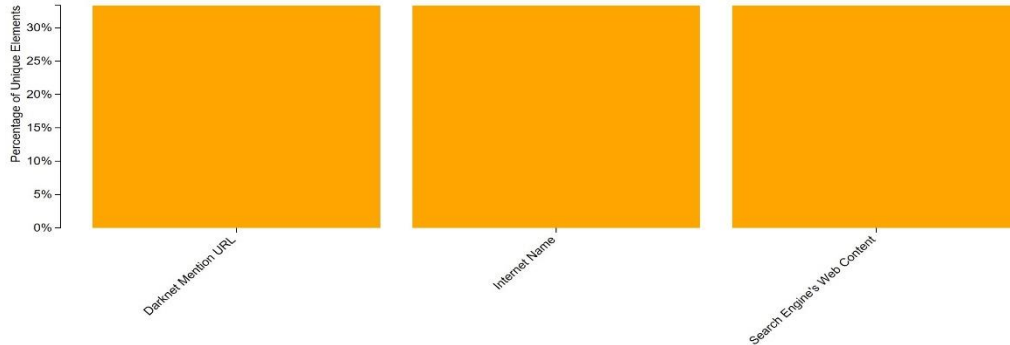
- Scan Results



Onion

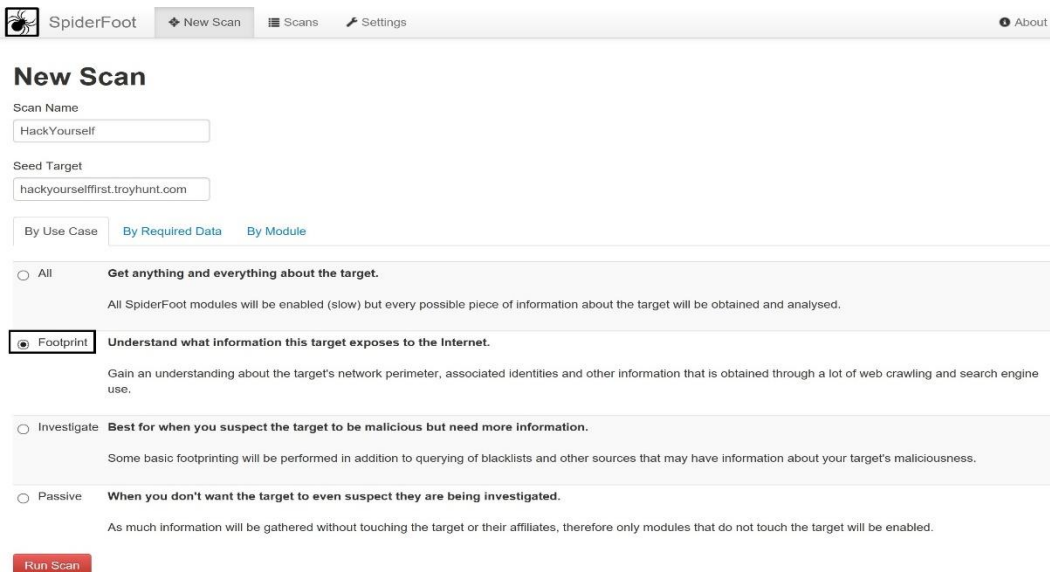


Total **3** Unique **3** Status **FINISHED** Errors **0**



Run SpiderFoot

- Footprint Scan



The screenshot shows the SpiderFoot web interface. At the top, there is a navigation bar with the SpiderFoot logo, a 'New Scan' button, 'Scans' and 'Settings' menus, and an 'About' link. Below the navigation bar is the 'New Scan' section. It contains a 'Scan Name' input field with the value 'HackYourself', a 'Seed Target' input field with the value 'hackyourselffirst.troyhunt.com', and three tabs: 'By Use Case', 'By Required Data', and 'By Module'. Under the 'By Use Case' tab, there are four radio button options: 'All', 'Footprint', 'Investigate', and 'Passive'. The 'Footprint' option is selected. Each option has a brief description of what it does. At the bottom of the form is a red 'Run Scan' button.

SpiderFoot [New Scan](#) [Scans](#) [Settings](#) [About](#)

New Scan

Scan Name

Seed Target

[By Use Case](#) [By Required Data](#) [By Module](#)

All **Get anything and everything about the target.**
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

Footprint **Understand what information this target exposes to the Internet.**
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

Investigate **Best for when you suspect the target to be malicious but need more information.**
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

Passive **When you don't want the target to even suspect they are being investigated.**
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

[Run Scan](#)

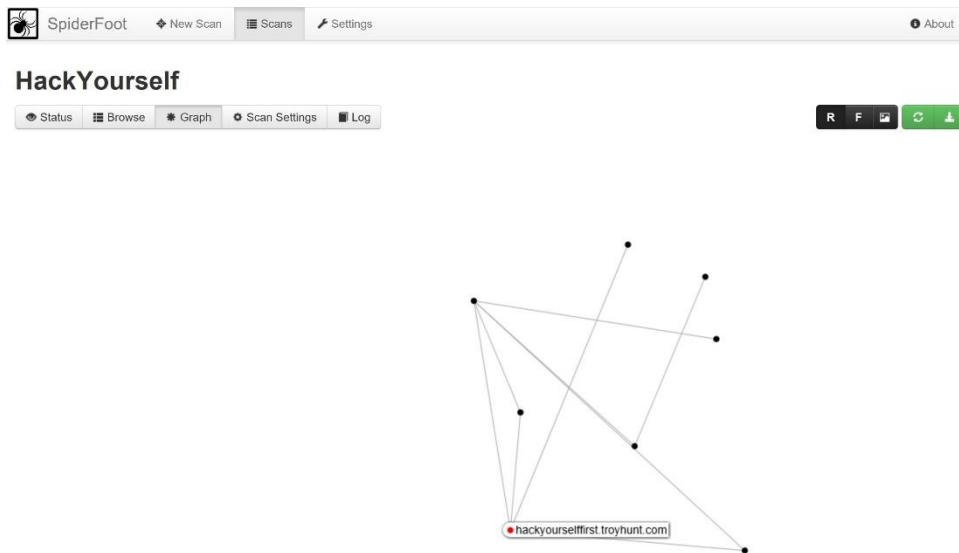
Run SpiderFoot

- Footprint Scan



Run SpiderFoot

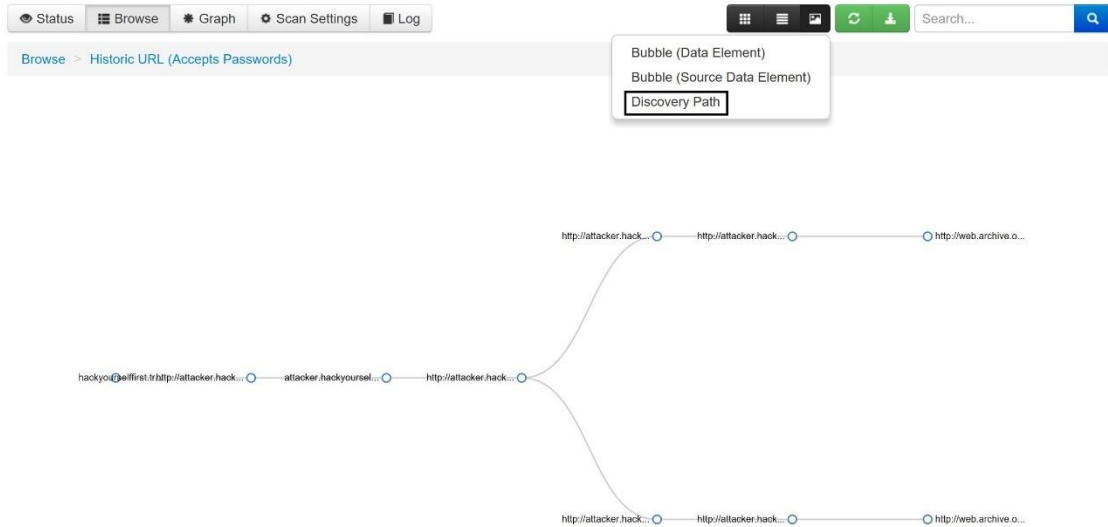
- Footprint Scan => Domains, subdomains Graph



Run SpiderFoot

- Visualize Discovery Path

HackYourself



Run SpiderFoot

- Visualize Bubble (Source Data Element)



Run SpiderFoot

- Browse > URL (Accepts Passwords)

HackYourself

● Status 🗉 Browse 📊 Graph ⚙️ Scan Settings 📄 Log 🔄 🗉 📄 📄 🔄 📄 🔍 Search...

Browse > URL (Accepts Passwords)

<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	http://attacker.hackyourselffirst.troyhunt.com/Account/Login	http://attacker.hackyourselffirst.troyhunt.com/Account/Login	sfp_page_info	2018-02-09 18:05:46
<input type="checkbox"/>	http://attacker.hackyourselffirst.troyhunt.com/Account/Register	http://attacker.hackyourselffirst.troyhunt.com/Account/Register	sfp_page_info	2018-02-09 18:04:18
<input type="checkbox"/>	http://attacker.hackyourselffirst.troyhunt.com/bundles/jque-ryva1?v=k095ZjRLUEVNzBf1waT1hs30t0ngQhk32HeNdumCbrM1	http://attacker.hackyourselffirst.troyhunt.com/bundles/jque-ryva1?v=k095ZjRLUEVNzBf1waT1hs30t0ngQhk32HeNdumCbrM1	sfp_page_info	2018-02-09 18:06:04
<input type="checkbox"/>	http://hackyourselffirst.troyhunt.com/Account/Login	http://hackyourselffirst.troyhunt.com/Account/Login	sfp_page_info	2018-02-09 18:11:13
<input type="checkbox"/>	http://hackyourselffirst.troyhunt.com/Account/Register	http://hackyourselffirst.troyhunt.com/Account/Register	sfp_page_info	2018-02-09 18:10:47

References

- SpiderFoot

<http://www.spiderfoot.net/index.html>

- Github

<https://github.com/smicallef/spiderfoot>

- SpiderFoot documentation

<http://www.spiderfoot.net/documentation/>