

Lab - Using OSINT Tools

Objectives

In this lab, you will explore several OSINT tools that are commonly used by pentesters.

- Examine OSINT resources
- Use SpiderFoot
- Investigate Recon-ng
- Find interesting files with Recon-ng

Background / Scenario

When performing information gathering activities, passive reconnaissance uses open, publicly accessible data to guide active reconnaissance efforts and to gather information about the enterprise and employees. In OSINT, it is the data that is open source. OSINT tools may or may not be open source. Some tools are free and open, others require registration to use free versions, and others require a fee for use. OSINT commonly uses data sources that are available to any hacker, so part of the PenTesting effort is to report on sensitive information that is commonly available in order to evaluate vulnerabilities that it may cause.

The objectives of OSINT are:

- To determine the digital footprint of the organization.
- Determine what data about the organization is available to cyber criminals.

Required Resources

- Kali VM customized for Ethical Hacker course
- Internet access

Instructions

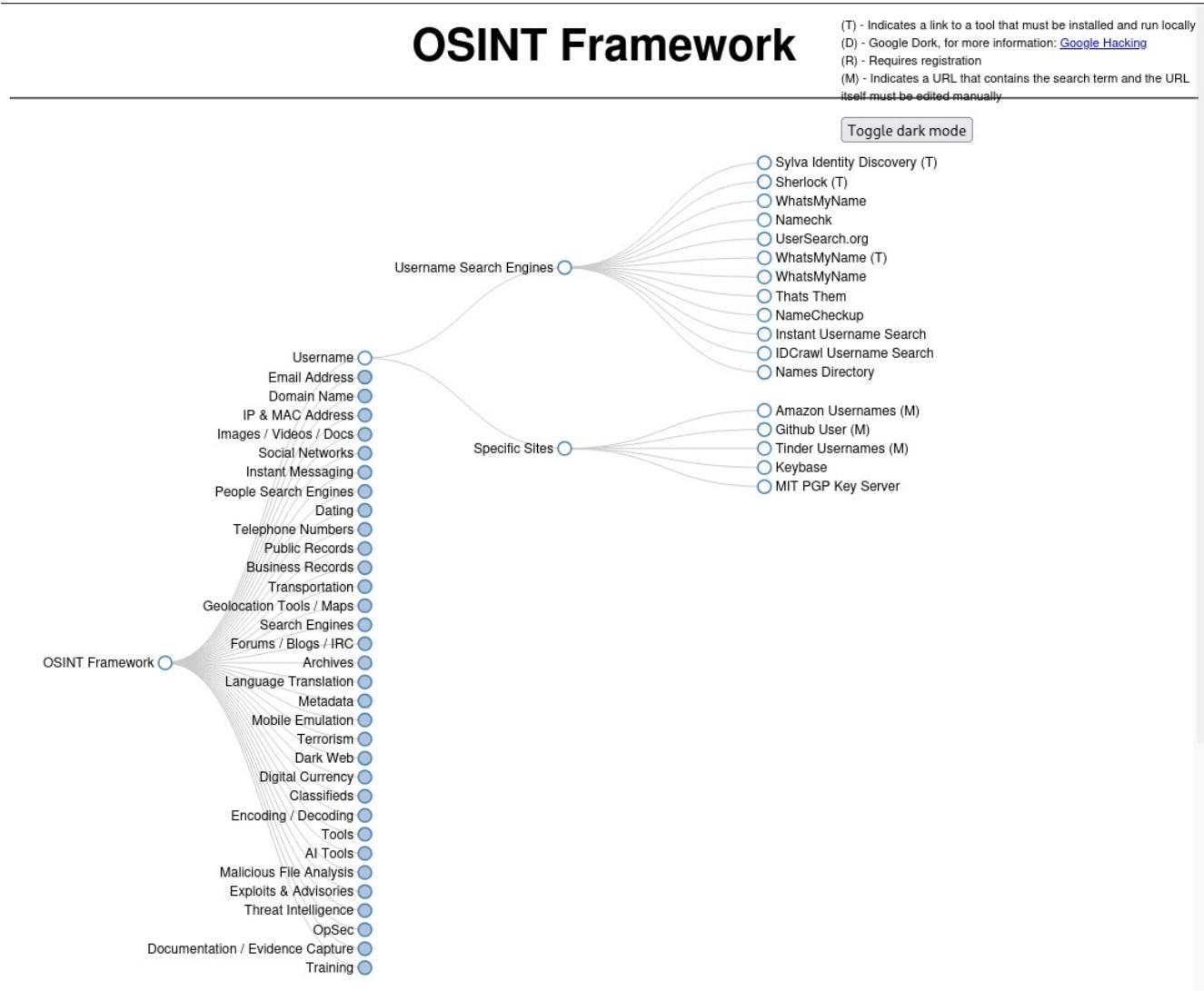
Part 1: Examine OSINT Resources

Step 1: Access the OSINT Framework

The OSINT Framework is a useful way to visualize the OSINT tools and resources that are available. Unfortunately, it has become a bit outdated, with some resources no longer available. It is still valuable to help you understand the types of tools available and their uses. In many cases, the links are still good.

- Go to the OSINT Framework site at <https://osintframework.com/>.

- You will see a vertical tree-like structure that consists of categories of OSINT tools and resources that can be reached from the framework. Click **Username** at the top of the tree. You will then see two subcategories appear. Click each to open the resource trees for each subcategory. Note in the upper-right corner of the page is a legend that identifies the type of resource.



- Under **Username Search Engines**, click "**WhatsMyName(T)**".
- The link takes you to a Git repository for the WhatsMyName project. In the **README.md** content for the tool, the various sites that implement WhatsMyName are listed. Feel free to explore these, but we will click the first link <https://whatsmyname.app/> to visit a free website that implements WhatsMyName. The parent organization for the site, <https://www.osintcombine.com/>, has several interesting free tools available.
- In the search box, type in a few usernames, each on a separate line. Use your own usernames or others that you find. Try searching the internet for **common username wordlist** for other potential search terms. You can filter the results based on the category filters, but for now, just click the green magnifying glass button to start the search.



Enter the username(s) in the search box, select any category filters & click the search icon or press CTRL+Enter

Category Filters

cygleh
cybergirl
anonymous
shawn

Active Filter: All (exclude NSFW)

Found: 226 Processed: 1534 / 2788

Show Found	Show False Positives	Show Not Found	Show All	Open All Links
about.me Username: shawn Category: social Account Found	7dach Username: anonymous Category: social Account Found	35photo Username: cybergirl Category: social Account Found		
skriga Username: shawn Category: hobby Account Found	Arduino (Forum) Username: anonymous Category: tech Account Found	Arch Linux GitLab Username: anonymous Category: social Account Found		
3dtoday Username: shawn Category: hobby Account Found	Arduino (Project..) Username: anonymous Category: tech Account Found	Aparat Username: shawn Category: social Account Found		
Aparat Username: anonymous Category: social Account Found	anonup Username: shawn Category: social Account Found	AllMyLinks Username: cybergirl Category: social Account Found		
7cap	AICoder	Audioglobe		

Filter by Username:

cygleh
cybergirl
anonymous
shawn[Show 50 rows](#) [Copy](#) [CSV](#) [PDF](#)

Search:

SITE	USERNAME	CATEGORY	LINK
35photo	cybergirl	social	https://35photo.pro/@cybergirl/
3dtoday	shawn	hobby	https://3dtoday.ru/blogs/shawn
7cup	shawn	social	https://www.7cups.com/@shawn
7dach	anonymous	social	https://7dach.u/profile/anonymous
about.me	shawn	social	https://about.me/@shawn
akniga	shawn	hobby	https://akniga.org/profile/@shawn
AllMyLinks	cybergirl	social	https://allmylinks.com/cybergirl
anonup	shawn	social	https://anonup.com/@shawn
Aparat	shawn	social	https://www.aparat.com/@shawn
Aparat	anonymous	social	https://www.aparat.com/@anonymous
Arch Linux GitLab	anonymous	social	https://gitlab.archlinux.ninja/anonymous

In a pentest, you would use another tool, such as **SpiderFoot** (below) to find usernames in email addresses that are associated with a company or domain.

- Investigate the results. You can open the links to the accounts either from the green rectangles or the table of results.



Enter the username(s) in the search box, select any category filters & click the search icon or press CTRL+Enter

Category Filters

cygleh
cybergirl
anonymous
shawn

Active Filter: All (exclude NSFW)

Found: 226 Processed: 1534 / 2788

Show Found	Show False Positives	Show Not Found	Show All	Open All Links
about.me Username: shawn Category: social Account Found	7dach Username: anonymous Category: social Account Found	35photo Username: cybergirl Category: social Account Found		
skriga Username: shawn Category: hobby Account Found	Arduino (Forum) Username: anonymous Category: tech Account Found	Arch Linux GitLab Username: anonymous Category: social Account Found		
3dtoday Username: shawn Category: hobby Account Found	Arduino (Project..) Username: anonymous Category: tech Account Found	Aparat Username: shawn Category: social Account Found		
Aparat Username: anonymous Category: social Account Found	anonup Username: shawn Category: social Account Found	AllMyLinks Username: cybergirl Category: social Account Found		
7cap	AICoder	Audioglobe		

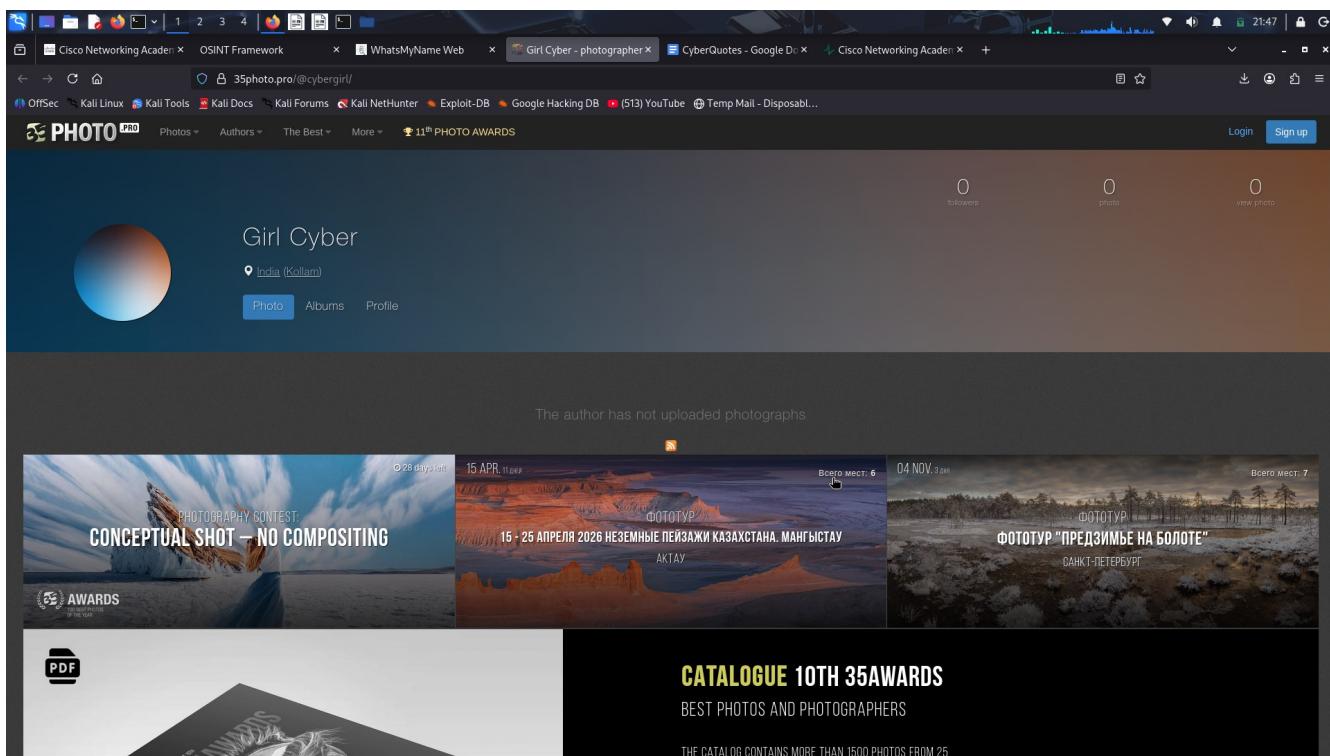
Filter by Username:

cygleh
cybergirl
anonymous
shawn[Show 50 rows](#) [Copy](#) [CSV](#) [PDF](#)

Search:

SITE	USERNAME	CATEGORY	LINK
35photo	cybergirl	social	https://35photo.pro/@cybergirl/
3dtoday	shawn	hobby	https://3dtoday.ru/blogs/shawn
7cup	shawn	social	https://www.7cups.com/@shawn
7dach	anonymous	social	https://7dach.u/profile/anonymous
about.me	shawn	social	https://about.me/@shawn
akniga	shawn	hobby	https://akniga.org/profile/@shawn
AllMyLinks	cybergirl	social	https://allmylinks.com/cybergirl
anonup	shawn	social	https://anonup.com/@shawn
Aparat	shawn	social	https://www.aparat.com/@shawn
Aparat	anonymous	social	https://www.aparat.com/@anonymous
Arch Linux GitLab	anonymous	social	https://gitlab.archlinux.ninja/anonymous

- WhatsMyName provides a very flexible report of the results. The results table can be sorted by column, and you can export the results as CSV or PDF for reporting purposes. In addition, you can easily filter by username and search within the results. Finally, you get links for the profile pages for the users at many different sites.



Step 2: Investigate SMART - Start Me Aggregated Resource Tool.

The start.me web service is a popular bookmark manager and productivity tool. The people at My OSINT Training (MOT) have set up a search system that finds all OSINT-related links that people have bookmarked and shared on start.me. There are many. You can enter OSINT-relevant search terms to find links to related resources.

- Go to <https://smart.myosint.training/>.

SMART - Start Me Aggregated Resource Tool

What was this?

SMART (Start Me Aggregated Resource Tool), was an OSINT Start.me page parser and aggregator.

There was an explosion of OSINT sites on the start.me bookmarking platform. There were too many OSINT start.me sites sharing too many resources. It was incredibly time consuming to click to all the sites and find resources to use. This project was an attempt to centralize OSINT start.me and other resource data in a single location. [Read more in this blog post.](#)

The bad news

Unfortunately, in 2023, the people at start.me changed how devices access the JSON files that drive their sites making our method of retrieving data ineffective.

Since the data in SMART was no longer accurate, we have decided to shut the project down for now.

[Visit My OSINT Training on Twitter](#) // [Check out our OSINT Courses](#).

© Copyright 2023 My OSINT Training - All Rights Reserved // [Visit My OSINT Training on Twitter](#) // [Check out our OSINT Courses](#)

Disclaimer!: Sadly we will not proceed with the next steps for SMART because the project is shutdown!

- b. In the search box, enter the term **usernames**. You will see a list of username-related OSINT tools that other people have found.
- c. Open some of the links to review the resources. Be careful however, these websites come from public sources. Some may be malicious.
- d. Choose some of the categories that you saw in the OSINT Framework and see what links appear.
- e. Use this site to search for OSINT tools and resources to help you in your pentesting work.

Part 2: Use SpiderFoot

SpiderFoot is an automated OSINT scanner. It is included with Kali

SpiderFoot seeds its scan with one of the following:

- Domain names
- IP addresses
- Subnet addresses
- Autonomous System Numbers (ASN)
- Email addresses
- Phone numbers
- Personal names

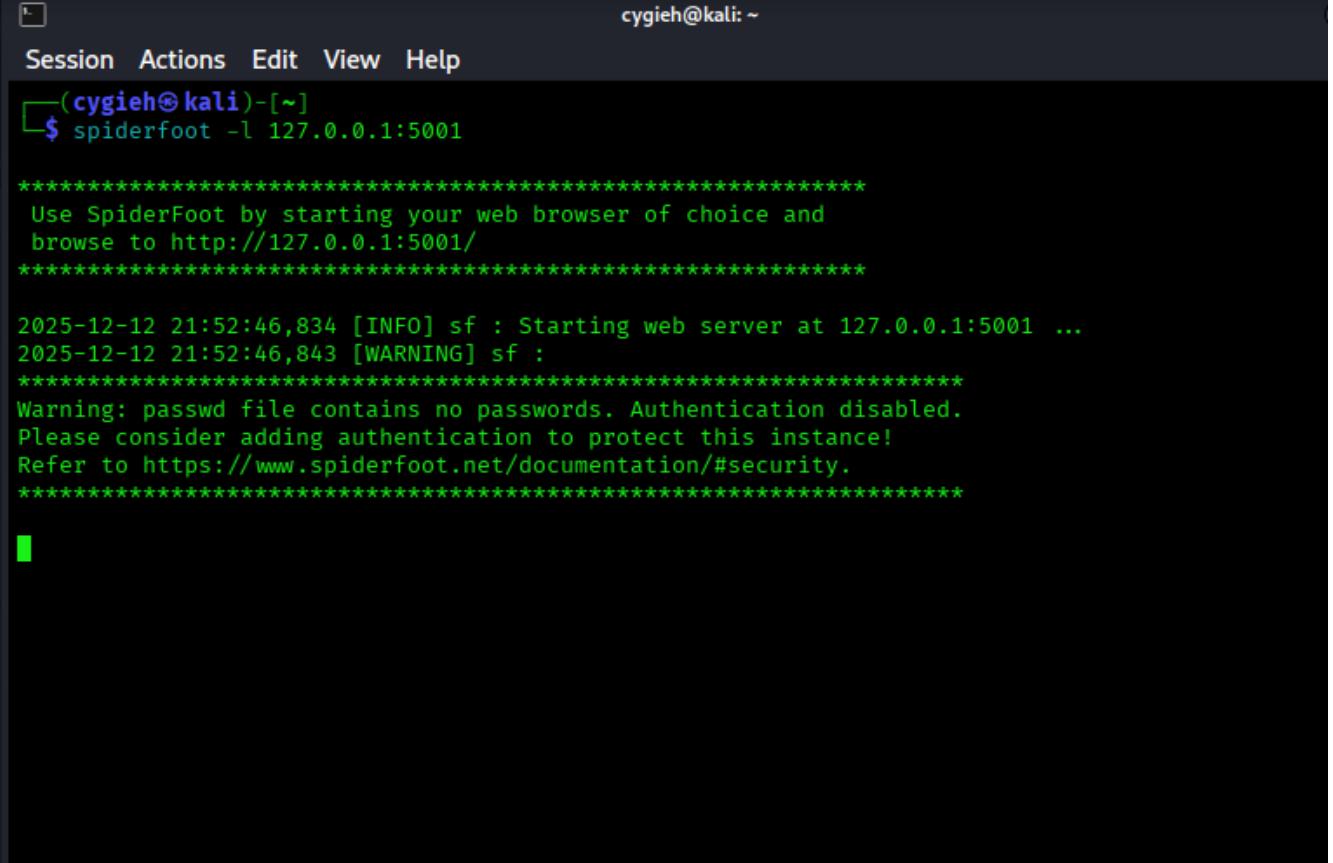
SpiderFoot offers the option of choosing scans based on use case, required data, and by SpiderFoot module.

The use cases are:

- **All** – Get every possible piece of information about the target. This use case can take a very long time to complete.
- **Footprint** – Understand the target's network perimeter, associated identities and other information that is yielded by extensive web crawling and search engine use.
- **Investigate** – This is or targets that you suspect of malicious behavior. Footprinting, blacklist lookups, and other sources that report on malicious sites will be returned.
- **Passive** – This type of scan is used if it is undesirable for the target to suspect that it is being scanned. This is a form of passive OSINT.

Step 1: Start and run SpiderFoot.

In a terminal, enter the following command: **spiderfoot -l 127.0.0.1:5001**



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says "Session Actions Edit View Help" and "cygieh@kali: ~". Below that, it shows a command line with a cursor: "(cygieh@kali)-[~]\$ spiderfoot -l 127.0.0.1:5001". The output starts with a series of asterisks, followed by instructions to use a web browser at "http://127.0.0.1:5001/". It then logs two messages: "[INFO] sf : Starting web server at 127.0.0.1:5001 ..." and "[WARNING] sf :". Another series of asterisks follows. After that, it displays a warning message: "Warning: passwd file contains no passwords. Authentication disabled. Please consider adding authentication to protect this instance! Refer to https://www.spiderfoot.net/documentation/#security." Another series of asterisks follows.

The command should run without errors. Open a browser and enter the IP address and port for the SpiderFoot GUI. You will see the SpiderFoot interface appear. If this is the first time that SpiderFoot has been opened in this VM, you will see the Scans screen. This screen displays a list of all the scans recently run.

The screenshot shows the SpiderFoot web application interface. At the top, there is a navigation bar with links for 'New Scan', 'Scans' (which is the active tab), and 'Settings'. On the far right of the top bar are 'Dark Mode' and 'About' buttons. Below the navigation bar is a section titled 'Scans' with a 'Filter: None' dropdown and several action buttons: 'C' (Create), 'S' (Scan), 'R' (Report), 'D' (Download), and 'Delete'. A table lists three completed scans: 'scan3' (target h4cker.org, started 2025-12-11 17:57:16, finished 2025-12-11 17:57:22, status FINISHED, 2 elements, 0 correlations), 'Scan2' (target h4cker.org, started 2025-12-11 17:52:59, finished 2025-12-11 17:53:03, status FINISHED, 2 elements, 0 correlations), and 'DomainScan' (target h4cker.org, started 2025-12-11 16:16:23, finished 2025-12-11 16:36:14, status ABORTED, 1259 elements, 0 correlations). Below the table are navigation controls (back, forward, search, etc.) and a message 'Scans 1 - 3 / 3 (3)'.

	Name	Target	Started	Finished	Status	Elements	Correlations	Action
1	scan3	h4cker.org	2025-12-11 17:57:16	2025-12-11 17:57:22	FINISHED	2	0 0 0 0	
2	Scan2	h4cker.org	2025-12-11 17:52:59	2025-12-11 17:53:03	FINISHED	2	0 0 0 0	
3	DomainScan	h4cker.org	2025-12-11 16:16:23	2025-12-11 16:36:14	ABORTED	1259	0 0 0 0	

Step 2: Explore SpiderFoot.

- Before we get started, look at the scanners that SpiderFoot uses to build its reports. Go to the **Settings** tab.
- The first two entries in the menu at the left are concerned with the operation of SpiderFoot. The entries below this are for the scanners that SpiderFoot uses. There are over 200 of them.

Click the scanners to see their SpiderFoot module name, details about the scanner, and settings that can be made, if any. Complete the table below with some examples. The Scanner name is in the settings menu. The module name appears in the details for the scanner.

Settings

[Save Changes](#)[Import API Keys](#)[Export API Keys](#)[Reset to Factory Default](#)

Global

Global Settings

Storage

Option

Value

AbstractAPI

Enable debugging?

False

abuse.ch

Override the default resolver with another DNS server. For example, 8.8.8.8 is Google's open DNS server.

8.8.8.8

AbuselPDB

Abusix Mail Intelligence

Account Finder

Number of seconds before giving up on a HTTP request.

5

AdBlock Check

Ahmia

AlienVault OTX

AlienVault IP Reputation

Archive.org

Azure Blob Finder

Bad Packets

Base64 Decoder

BinaryEdge

Bing

List of usernames that if found as usernames or as part of e-mail addresses, should be treated differently to non-generics.

abuse,admin,billing,compliance,devnull,dns,ftp,hostmaster,inoc,ispfeedback,

List of Internet TLDs.

https://publicsuffix.org/list/effective_tld_names.dat

Hours to cache the Internet TLD list. This can safely be quite a long time given that the list doesn't change too often.

72

Max number of

Follow SpiderFoot on Twitter for the latest updates.

All SpiderFoot modules are referred to as sfp_[module name].

Hint: scanners with a lock next to them indicate an API key is necessary. Further information regarding the key requirements is provided in the details for the scanner. Click the "?" icon next to the API Settings option.

Hint: You can interact with SpiderFoot from the terminal too. You can display all the modules that are available in SpiderFoot and pipe the output to a text file. Enter **spiderfoot -h** to view the command line options.

The **grep** command can then be used to search the file for keywords. This will not provide information

Information Type	Scanner/Module Name	API key required? Free?
Possible accounts associated with a domain	Account Finder sfp_accounts	No, N/A
Links that are associated with the target	Cross-Referencer, sfp_crossref	no
Email addresses associated with the target	EmailCrawlr, sfp_emailcrawlr	Yes, free plan
Domains and URLs that are associated with the target	grep.app, sfp_grep_app	Yes, free plan
Geolocation information	ipapi.com, sfp_ipapicom	Yes, free plan
Data breach information	Leak-Lookup, sfp_keybase	Yes, free

Step 3: Run a SpiderFoot Scan for a Domain.

- Click the **New Scan** tab in the GUI.
- Enter a **name** for the scan and select a **target**. In this case, we will use **h4cker.org**.
- You will scan **by use case**. Note that you can also scan by the type of information required or by selecting the individual scanner modules that you would like to use. By executing narrower scans, you can learn more about the modules and information that can be gathered.
- Select the scan use case as **Footprint**.

Note: The **All** use case scan may use active scanning. Unless you have permission to scan the target, you should avoid this setting. To be completely safe, the Passive use case should avoid any problems with unauthorized scanning.

- Click the **Run Scan Now** button.

New Scan

Scan Name

FirstScan

Scan Target

h4cker.org

💡 Your scan target may 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
IPv4 Address: e.g. 1.2.3.4
IPv6 Address: e.g. 2606:4700:4700::1111
Hostname/Sub-domain: e.g. abc.example.com
Subnet: e.g. 1.2.3.0/24
Bitcoin Address: e.g.
1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R

E-mail address: e.g. bob@example.com
Phone Number: e.g. +12345678901 (E.164 format)
Human Name: e.g. "John Smith" (must be in quotes)
Username: e.g. "jsmith2000" (must be in quotes)
Network ASN: e.g. 1234

 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.**

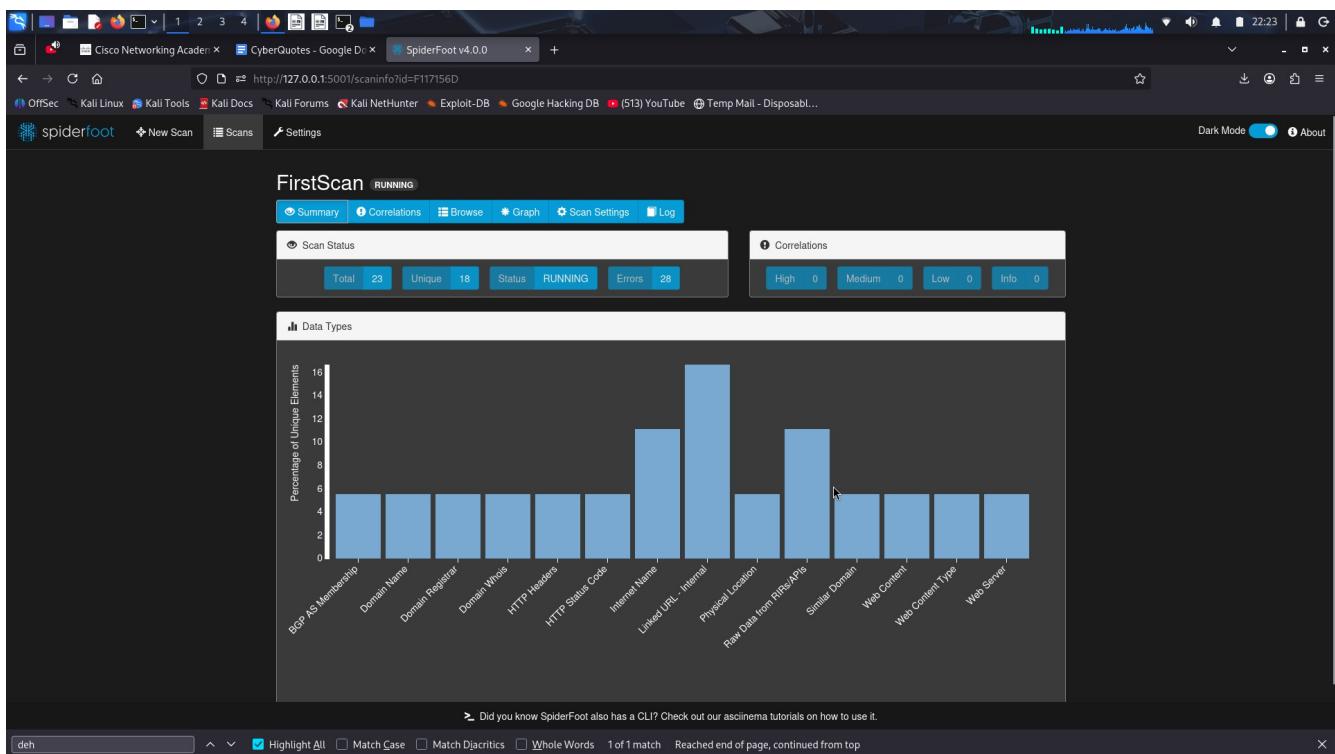
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

 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 Now

- You should see a bar graph appear. The scan statistics will start to increment, and new bars will appear in the graph as new results are obtained. Mouse over the bars for a summary of the findings for that data type.



- SpiderFoot scans are very detailed and can take a very long time. Give this scan at least 30 minutes so that there is a nice collection of information. To get the most details, a scan could take hours. While the scan is running, you can browse the results.

The screenshot shows the SpiderFoot web interface with the title "FirstScan" and status "RUNNING". The "Browse" tab is active, showing a table of identified data elements. The table has columns: Data Element, Source Data Element, Source Module, and Identified. The data shows six entries, all originating from "h4cker.org" and identified by "sfp_spider" or "sfp_urlscan".

Data Element	Source Data Element	Source Module	Identified
http://h4cker.org	h4cker.org	sfp_spider	2025-12-12 22:22:58
http://h4cker.org	h4cker.org	sfp_urlscan	2025-12-12 22:23:04
http://h4cker.org/	h4cker.org	sfp_urlscan	2025-12-12 22:23:04
https://h4cker.org/	h4cker.org	sfp_spider	2025-12-12 22:23:00
https://h4cker.org/	h4cker.org	sfp_urlscan	2025-12-12 22:23:04

Step 4: Investigate Scan Results.

- Go back to the scan results, by clicking the **Scans** tab. You will see a table with the currently running scan and any previous scans displayed.

The screenshot shows the SpiderFoot web interface with the "Scans" tab selected. A single scan named "FirstScan" is listed. The table has columns: Name, Target, Started, Finished, Status, Elements, Correlations, and Action. The "FirstScan" row shows the target "h4cker.org", started at "2025-12-12 22:22:50", and is currently "RUNNING" with 23 elements identified and 0 correlations.

Name	Target	Started	Finished	Status	Elements	Correlations	Action
FirstScan	h4cker.org	2025-12-12 22:22:50	Not yet	RUNNING	23	0 0 0 0	[Action]

- b. Click the black square in the right-most column of the scans table to stop the scan. Some information is not available until the scan is aborted or completed.

The screenshot shows the SpiderFoot web application. At the top, there are navigation links: 'spiderfoot', 'New Scan', 'Scans', and 'Settings'. Below this is a table titled 'Scans' with columns: 'Name', 'Target', and 'Started'. A single row is visible: 'FirstScan' with target 'h4cker.org' and start date '2025-12-12 22:23:00'. To the right of the table is a modal dialog box with the title 'Stop scan?'. Inside the dialog, the message 'Are you sure you wish to stop this scan?' is displayed. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'. The background of the main interface shows a dark-themed dashboard with various metrics and a timeline at the bottom.

- c. Click the name of the scan in the table to return to the scan view. You will be taken to the **Browse** tab. Each row in the table represents data found by the various modules. Some modules contribute to multiple types of data.

The screenshot shows the 'FirstScan' view in the SpiderFoot interface. The browser address bar indicates the URL is 'http://127.0.0.1:5001/scaninfo?id=F117156D'. The page title is 'FirstScan' with a status badge 'ABORT-REQUESTED'. Below the title is a navigation bar with tabs: 'Summary', 'Correlations', 'Browse' (which is active), 'Graph', 'Scan Settings', and 'Log'. There is also a search bar and a 'Dark Mode' toggle. The main content area is a table titled 'Type' with columns: 'Type', 'Unique Data Elements', 'Total Data Elements', and 'Last Data Element'. The table lists various data types and their counts, such as 'BGP AS Membership' (1 unique, 2 total, last seen 2025-12-12 22:23:30). At the bottom of the table, it says 'Raw Data from RIIRsAPIs'. The footer of the page includes a link to follow SpiderFoot on Twitter and a search bar with filters like 'Highlight All', 'Match Case', etc.

- d. Investigate the results.

The screenshot shows the SpiderFoot FirstScan interface. At the top, there are tabs for Summary, Correlations, Browse, Graph, Scan Settings, and Log. Below the tabs is a toolbar with icons for search, refresh, and file operations. A search bar is also present. The main area displays a table titled "Identified" with the following data:

	Data Element	Source Data Element	Source Module	Identified
1	http://h4cker.org	h4cker.org	sfp_spider	2025-12-12 22:22:58
2	http://h4cker.org	h4cker.org	sfp_urlscan	2025-12-12 22:23:04
3	http://h4cker.org/	h4cker.org	sfp_urlscan	2025-12-12 22:23:04
4	https://h4cker.org/	h4cker.org	sfp_spider	2025-12-12 22:23:00
5	https://h4cker.org/	h4cker.org	sfp_urlscan	2025-12-12 22:23:04

Step 5: Register API Keys (optional).

API keys will enhance the functionality of SpiderFoot. Some of these API keys require free registration. The pentesting tools that are available are constantly evolving. Some tools or services that were once free and open can become fee-based over time.

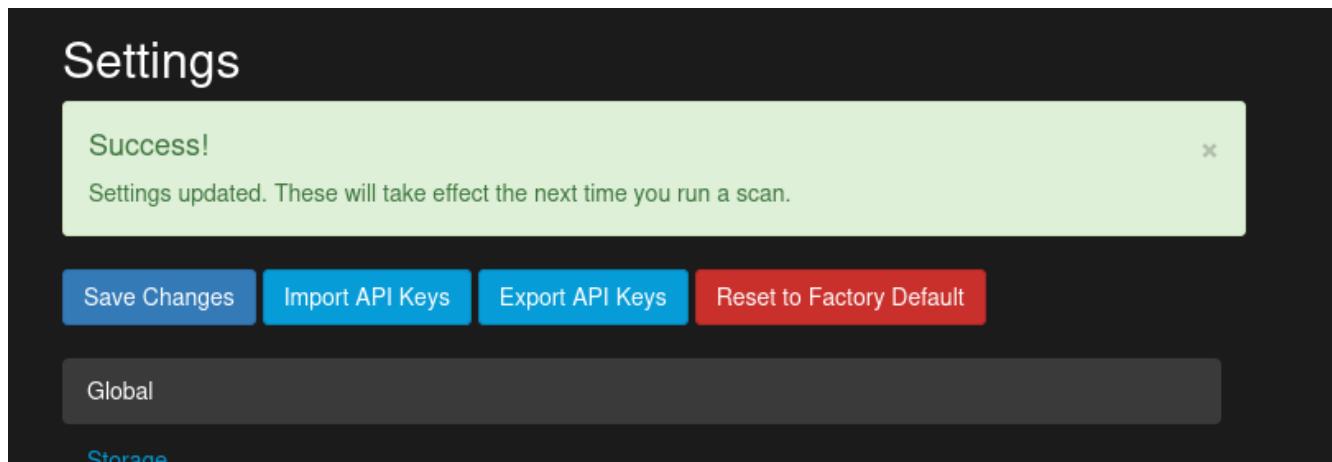
Note: Some APIs may limit your results after you have reached a prescribed number of uses.

- a. Go to the **Settings** tab.
- b. Find the four modules in the table below. Open the page for the module and complete the table including the type of information that module searches for. For each module in the table, click the ? next to the API option. Follow the instructions to get API keys for the four modules.

Module	Type of Information	Your API Key, etc
Builtwith	Answer Area and country based analytics for all web technologies.	Answer Area 1a03b92a-d53d-45c5-8e45-c5748fe97713
Hunter.io	Answer Area Check for e-mail addresses and names	Answer Area Enter your answer here
Onion.link	Answer Area Enabling search and global access to Tor's onion sites.	Answer Area AlzaSyDk22nlZk8Pjy6-dlF2byq1Fdj5BgYweds
IntelligenceX	Answer Area Obtain information about identified IP addresses, domains, e-mail addresses	Answer Area f816f212-c462-40d8-a829-3a028b2dd1e5

Module	Type of Information	Your API Key, etc
Builtwith	web software in use	Answers will vary.
Hunter.io	email address search	Answers will vary.
Onion.link	Tor onion site search	Answers will vary.
IntelligenceX	everything	Answers will vary.

Enter the API keys in the settings for each module. Be sure to save your changes.



The screenshot shows the 'Settings' page with a dark background. At the top, there is a green success message box containing the text 'Success!' and 'Settings updated. These will take effect the next time you run a scan.' Below the message box are four buttons: 'Save Changes' (blue), 'Import API Keys' (blue), 'Export API Keys' (blue), and 'Reset to Factory Default' (red). Below these buttons is a grey bar with the word 'Global' in white. At the bottom of the page, there is another grey bar with the word 'Storage' in white.

- Click **New Scan**. Go to the By Module tab. Select only the modules for which you have added API keys. All other modules should be unchecked.
- Enter the target as **h4cker.org** and click **Start Scan**. Feel free to scan other domains but be sure to observe the terms and conditions of this course.

New Scan

Scan Name
SecondScan

Scan Target
h4cker.org

Your scan target may 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
IPv4 Address: e.g. 1.2.3.4
IPv6 Address: e.g. 2606:4700:4700::1111
Hostname/Sub-domain: e.g. abc.example.com
Subnet: e.g. 1.2.3.0/24
Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R
E-mail address: e.g. bob@example.com
Phone Number: e.g. +12345678901 (E.164 format)
Human Name: e.g. "John Smith" (must be in quotes)
Username: e.g. "jsmith2000" (must be in quotes)
Network ASN: e.g. 1234

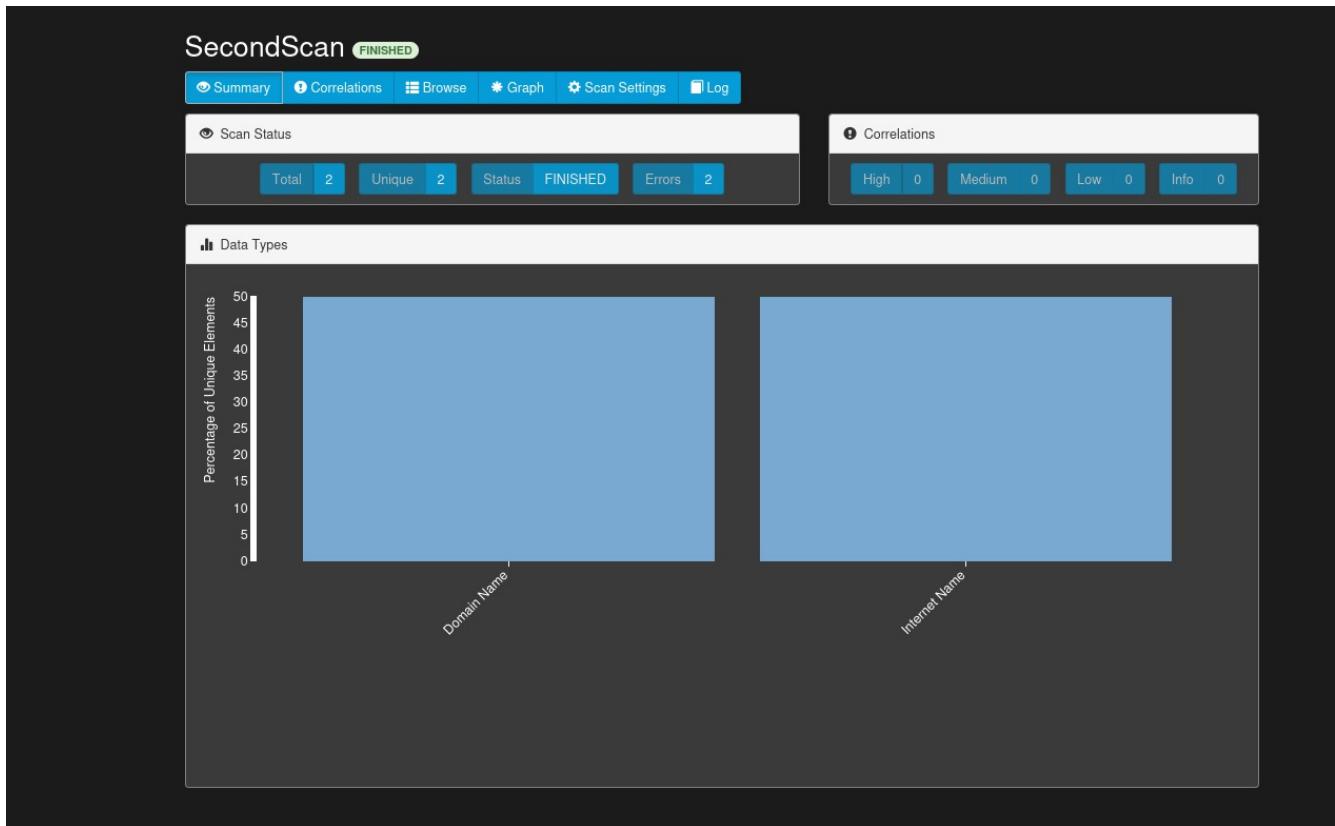
By Use Case By Required Data By Module Select All De-Select All

<input type="checkbox"/> AbstractAPI	Look up domain, phone and IP address information from AbstractAPI.
<input type="checkbox"/> abuse.ch	Check if a host/domain, IP address or netblock is malicious according to Abuse.ch.
<input type="checkbox"/> AbuseIPDB	Check if an IP address is malicious according to AbuseIPDB.com blacklist.
<input type="checkbox"/> Abusix Mail Intelligence	Check if a netblock or IP address is in the Abusix Mail Intelligence blacklist.
<input type="checkbox"/> Account Finder	Look for possible associated accounts on nearly 200 websites like Ebay, Slashdot, reddit, etc.
<input type="checkbox"/> AdBlock Check	Check if linked pages would be blocked by AdBlock Plus.
<input type="checkbox"/> AdGuard DNS	Check if a host would be blocked by AdGuard DNS.
<input type="checkbox"/> Ahmia	Search Tor 'Ahmia' search engine for mentions of the target.
<input type="checkbox"/> AlienVault IP Reputation	Check if an IP or netblock is malicious according to the AlienVault IP Reputation database.
<input type="checkbox"/> AlienVault OTX	Obtain information from AlienVault Open Threat Exchange (OTX)
<input type="checkbox"/> Amazon S3 Bucket Finder	Search for potential Amazon S3 buckets associated with the target and attempt to list their contents.
<input type="checkbox"/> Apple iTunes	Search Apple iTunes for mobile apps.
<input type="checkbox"/> Archive.org	Identifies historic versions of interesting files/pages from the Wayback Machine.
<input type="checkbox"/> ARIN	Queries ARIN registry for contact information.
<input type="checkbox"/> Azure Blob Finder	Search for potential Azure blobs associated with the target and attempt to list their contents.
<input type="checkbox"/> Bad Packets	Obtain information about any malicious activities involving IP addresses found
<input type="checkbox"/> Base64 Decoder	Identify Base64-encoded strings in URLs, often revealing interesting hidden information.
<input type="checkbox"/> BGPView	Obtain network information from BGPView API.

> Did you know SpiderFoot also has a CLI? Check out our asciinema tutorials on how to use it.

Step 6: Analyze Results of API Modules Scans.

- a. This scan should not take very long.



SecondScan FINISHED

	Data Element	Source Data Element	Source Module	Identified
	h4cker.org	h4cker.org	SpiderFoot UI	2025-12-12 22:36:15

- b. Browse the scan to look at the results. Pay attention to the **Source Module** column. You should see some of the scanners that you configured with API keys.

SecondScan FINISHED

	Data Element	Source Data Element	Source Module	Identified
	h4cker.org	h4cker.org	SpiderFoot UI	2025-12-12 22:36:15

- c. Go to the Leak Site URL type in the table of results.

Part 3: Investigate Recon-ng

Recon-ng is an OSINT framework that is similar to the Metasploit exploitation framework or the Social-Engineering Toolkit (SET).

Recon-**ng** is used to perform a wide range of reconnaissance activities on different settings that you provide. Some modules are available with the Kali installation and others are available for download and installation in the Recon-**ng** modules marketplace.

Step 1: Create a workspace.

Recon-**ng** has auto complete. Press the tab button to complete commands and command options. Use the tab key twice to list the available commands and options at different places in the command line. This is very handy.

- a. To run Recon-ng, open a new terminal window and enter **recon-ng**. You can also start the program by going to the Kali tools menu, searching for the app, and clicking the icon.

```
(c) (cygieh㉿kali)-[~]
$ recon-ng
[*] Version check disabled.

Sponsored by ...
          ^__^
         /  \_\
        o   o\  \
        ||----w |
        ||     || \\
        \  \  \  \
        www.blackhillsinfosec.com

          [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
          www.practisec.com

[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] > █
```

- b. Note that the terminal prompt changes to indicate that you are working within the Recon-*ng* framework. Enter **help** to get a sense of the commands that are available.

```
[recon-ng][default] > help

Commands (type [help|?] <topic>):

back           Exits the current context
dashboard      Displays a summary of activity
db             Interfaces with the workspace's database
exit           Exits the framework
help           Displays this menu
index          Creates a module index (dev only)
keys           Manages third party resource credentials
marketplace    Interfaces with the module marketplace
modules        Interfaces with installed modules
options        Manages the current context options
pdb            Starts a Python Debugger session (dev only)
script         Records and executes command scripts
shell          Executes shell commands
show           Shows various framework items
snapshots      Manages workspace snapshots
spool          Spools output to a file
workspaces     Manages workspaces

[recon-ng][default] > █
```

- c. Recon-*ng* uses workspaces to isolate investigations from one another. Workspaces can be created for different parts of a test or different customers for example. Type **workspaces help** to view options for the workspaces command.

```
[recon-ng][default] > workspaces help
Manages workspaces

Usage: workspaces <create|list|load|remove> [ ... ]

[recon-ng][default] > █
```

How can you display the available workspaces?

```
[recon-ng][default] > workspaces list

+-----+
| Workspaces |      Modified      |
+-----+
| default    | 2025-12-12 22:46:12 |
+-----+
```

How can you create a workspace?

```
[recon-ng][default] > workspaces create jana  
[recon-ng][jana] > back
```

How can you remove a workspace?

```
[recon-ng][default] > workspaces remove jana  
[recon-ng][default] > █
```

Create a workspace named **test** by entering **workspaces create** followed by the workspace name. Note that the prompt has changed to indicate that you are in this workspace.

Type **help** to see the commands that are available within workspaces.

```
[recon-ng][default] > workspaces create test  
[recon-ng][test] > help  
  
Commands (type [help|?] <topic>):  


---



|             |                                             |
|-------------|---------------------------------------------|
| back        | Exits the current context                   |
| dashboard   | Displays a summary of activity              |
| db          | Interfaces with the workspace's database    |
| exit        | Exits the framework                         |
| help        | Displays this menu                          |
| index       | Creates a module index (dev only)           |
| keys        | Manages third party resource credentials    |
| marketplace | Interfaces with the module marketplace      |
| modules     | Interfaces with installed modules           |
| options     | Manages the current context options         |
| pdb         | Starts a Python Debugger session (dev only) |
| script      | Records and executes command scripts        |
| shell       | Executes shell commands                     |
| show        | Shows various framework items               |
| snapshots   | Manages workspace snapshots                 |
| spool       | Spools output to a file                     |
| workspaces  | Manages workspaces                          |


```

Step 2: Investigate modules.

Recon-ng is a modular framework. Modules are Python programs with different functions. They are stored in an external marketplace that permits developers to create their own modules and contribute them for use by others.

Return to the Recon-ng prompt. Enter the **modules search** command. This will display the currently installed modules.

Step 3: Investigate the module marketplace.

Recon-**ng** will not function without modules. In this step, we will install modules from the Recon-**ng** marketplace. The module marketplace is a GitHub public repository. Search the web for **recon-**ng**-marketplace** to view the repository. Explore the folders to learn more about the modules.

- a. In the terminal, view help for the **marketplace** command. Use the **search** option to list all the modules that are currently available.

[recon-ng][default] > **marketplace search**

cygieh@kali: ~

	Session	Actions	Edit	View	Help
	recon/netblocks-hosts/censys_netblock	2.1	not installed	2022-01-31 *	
	recon/netblocks-hosts/reverse_resolve	1.0	not installed	2019-06-24	
	recon/netblocks-hosts/shodan_net	1.2	not installed	2020-07-21 *	
	recon/netblocks-hosts/virustotal	1.0	not installed	2019-06-24	
	recon/netblocks-ports/census_2012	1.0	not installed	2019-06-24	
	recon/netblocks-ports/censysio	1.0	not installed	2019-06-24	
	recon/ports-hosts/migrate_ports	1.0	not installed	2019-06-24	
	recon/ports-hosts/ssl_scan	1.1	not installed	2021-08-24	
	recon/profiles-contacts/bing_linkedin_contacts	1.2	not installed	2021-08-24	
	recon/profiles-contacts/dev_diver	1.1	not installed	2020-05-15	
	recon/profiles-contacts/github_users	1.0	not installed	2019-06-24	
	recon/profiles-profiles/namechk	1.0	not installed	2019-06-24	
	recon/profiles-profiles/profiler	1.2	not installed	2023-12-30	
	recon/profiles-profiles/twitter_mentioned	1.0	not installed	2019-06-24	
	recon/profiles-profiles/twitter_mentions	1.0	not installed	2019-06-24	
	recon/profiles-repositories/github_repos	1.1	not installed	2020-05-15	
	recon/repositories-profiles/github_commits	1.0	not installed	2019-06-24	
	recon/repositories-vulnerabilities/gists_search	1.0	not installed	2019-06-24	
	recon/repositories-vulnerabilities/github_dorks	1.0	not installed	2019-06-24	
	reporting/csv	1.0	not installed	2019-06-24	
	reporting/html	1.0	not installed	2019-06-24	
	reporting/json	1.0	not installed	2019-06-24	
	reporting/list	1.0	not installed	2019-06-24	
	reporting/proxifier	1.0	not installed	2019-06-24	
	reporting/pushpin	1.0	not installed	2019-06-24	
	reporting/xlsx	1.0	not installed	2019-06-24	
	reporting/xml	1.1	not installed	2019-06-24	
-+					
	D = Has dependencies. See info for details.				
	K = Requires keys. See info for details.				
[recon-ng][default] > █					

- b. Note that the modules are organized by their category and type. This appears as a path prepended to the name of the module. You can filter the output by adding a search term to the marketplace search command. Try a few different search terms that are related to OSINT information to get a sense of the modules that are available.

```
[recon-ng][default] > marketplace search grep | reporting
[*] Searching module index for 'grep | reporting' ...
[!] No modules found.
Searches marketplace modules

Usage: marketplace search [<regex>]

[recon-ng][default] > marketplace info
Shows detailed information about available modules

Usage: marketplace info <<path>|<prefix>|all>
```

To learn more about individual modules, use the **marketplace info** command followed by the full name of the module, including its category and type. It is easier to select the name of the module and copy and paste it into the command line.

```
[recon-ng][default] > marketplace info reporting/xml
+---+
| path      | reporting/xml
| name      | XML Report Generator
| author    | Eric Humphries (@e2fsck) and Tim Tomes (@lanmaster53)
| version   | 1.1
| last_updated | 2019-06-24
| description | Creates an XML report.
| required_keys | []
| dependencies | []
| files     | []
| status     | not installed
+---+
[recon-ng][default] > █
```

Step 4: Install a new module.

Recon-ng accesses modules from the Github repository and downloads them to Kali when they are installed.

- a. Search the marketplace modules using **bing** as a search term. Locate a module that requires no dependencies or API keys.

```
[recon-ng][default] > marketplace info bing

+-
+--+
| path      | recon/companies-contacts/bing_linkedin_cache
|
| name      | Bing Cache Linkedin Profile and Contact Harvester
|
| author    | Joe Black (@MyChickenNinja), @fullmetalcache, and Brian King
|
| version   | 1.0
|
| last_updated | 2019-06-24
|
| description | Harvests profiles from LinkedIn by querying the Bing API cache for LinkedIn pages related to the given companies, and adds them to the 'profiles' table. The module will then parse the resulting information to extract the user's full name and job title (title parsing recently improved). The user's full name and title are then added to the 'contacts' table. This module does not access LinkedIn at any time.
| required_keys | ['bing_api']
|
| dependencies | []
```

```

+-----+
| path      | recon/domains-hosts/bing_domain_web
|           |
| name      | Bing Hostname Enumerator
|           |
| author    | Tim Tomes (@lanmaster53)
|           |
| version   | 1.1
|           |
| last_updated | 2019-07-04
|           |
| description | Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table with the results.
| required_keys | []
|           |
| dependencies | []
|           |
| files     | []
|           |
| status     | not installed
+-----+
+-----+

```

- View information for this module.
- To install the module, copy the full name, including the path, to the clipboard.
- Enter the **marketplace install** command followed by the full name of the module.
- [recon-ng][default] > **marketplace install recon/domains-hosts/bing_domain_web**
- After installation, enter the **modules search** command to verify that the new module is now available.

```

[recon-ng][default] > marketplace install recon/domains-hosts/bing_domain_web
[*] Module installed: recon/domains-hosts/bing_domain_web
[*] Reloading modules ...
[recon-ng][default] > modules search
Recon
-----
recon/domains-hosts/bing_domain_web
[recon-ng][default] > █

```

- Repeat the process to install the **hackertarget** module.

```
[recon-ng][default] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][default] > module search
[!] Invalid command: module search.
[recon-ng][default] > modules search

Recon
_____
recon/domains-hosts/bing_domain_web
recon/domains-hosts/hackertarget

[recon-ng][default] > █
```

Step 5: Run the new modules

- Create a new workspace. Name it as you wish.

```
[recon-ng][default] > workspaces create Test1
[recon-ng][Test1] > █
```

- To start working with a module, it must be initialized. Enter **modules load hackertarget** to begin working with the module. Note that the prompt changes to reflect the loaded module.

```
[recon-ng][Test1] > modules load hackertarget
[recon-ng][Test1][hackertarget] > █
```

- Each module is its own environment. The developers of recon-ng have taken care to keep the framework consistent, so the same commands are available for each module. However, the options can vary. Type **info** at the module prompt to view important details about the module.

```
[recon-ng][Test1][hackertarget] > info

  Name: HackerTarget Lookup
  Author: Michael Henriksen (@michenriksen)
  Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name   Current Value  Required  Description
  _____
  SOURCE  default       yes       source of input (see 'info' for details)

Source Options:
  default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>     string representing a single input
  <path>       path to a file containing a list of inputs
  query <sql>   database query returning one column of inputs

[recon-ng][Test1][hackertarget] > █
```

- Instead of passing options at the command line, in Recon-*ng* you set the options and then enter a simple command to execute the module. Use the **options set source** command to set the only option for this module. Complete the command by specifying the target as **hackxor.net**.
- Verify the option setting with the **info** command.

```
[recon-ng][Test1][hackertarget] > options set source hackxor.net
SOURCE => hackxor.net
[recon-ng][Test1][hackertarget] > info

    Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
    Version: 1.1

Description:
    Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name  Current Value  Required  Description
  _____
  SOURCE  hackxor.net    yes      source of input (see 'info' for details)

Source Options:
  default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>     string representing a single input
  <path>       path to a file containing a list of inputs
  query <sql>   database query returning one column of inputs

[recon-ng][Test1][hackertarget] > █
```

- Type **run** to execute the module.

```
[recon-ng][Test1][hackertarget] > run
```

HACKXOR.NET

```
[*] Country: None
[*] Host: Host: research1.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: dreaded.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: hkrb.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: hmrc.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: intranet.hackxor.net
[*] Ip_Address: 10.60.10.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: research1.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: transparency.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
```

- Inspect the output of the command. The output is stored in a database so you can refer to it later. The data that is stored is specific to the workplace in which it was gathered.
- Enter the **dashboard** command. This queries the Recon-ng database and provides a summary of the information that has been gathered. It is specific to this workspace.

```
[recon-ng][Test1][hackertarget] > dashboard

+-----+
|          Activity Summary          |
+-----+
|          Module           | Runs |
+-----+
| recon/domains-hosts/hackertarget | 1   |
+-----+


+-----+
|          Results Summary          |
+-----+
|      Category     | Quantity |
+-----+
| Domains       | 0
| Companies     | 0
| Netblocks     | 0
| Locations     | 0
| Vulnerabilities | 0
| Ports         | 0
| Hosts         | 7
| Contacts       | 0
| Credentials    | 0
| Leaks          | 0
| Pushpins       | 0
| Profiles        | 0
| Repositories   | 0
+-----+


[recon-ng][Test1][hackertarget] > █
```

- The **show** command displays the data for specific categories. Enter the **show hosts** command to display the list of hosts that were discovered.

```
[recon-ng][Test1][hackertarget] > show hosts

+-----+
| rowid | host | ip_address | region | country | latitude | longitude |
+-----+
| 1     | Host: research1.hackxor.net | 138.68.117.124 | | | | |
| 2     | hackertarget | | | | | |
| 2     | dreaded.hackxor.net | 138.68.117.124 | | | | |
| 3     | hackertarget | | | | | |
| 3     | hkrb.hackxor.net | 138.68.117.124 | | | | |
| 4     | hackertarget | | | | | |
| 4     | hmrc.hackxor.net | 138.68.117.124 | | | | |
| 5     | hackertarget | | | | | |
| 5     | intranet.hackxor.net | 10.60.10.18 | | | | |
| 6     | hackertarget | | | | | |
| 6     | research1.hackxor.net | 138.68.117.124 | | | | |
| 7     | hackertarget | | | | | |
| 7     | transparency.hackxor.net | 138.68.117.124 | | | | |
+-----+
[★] 7 rows returned
[recon-ng][Test1][hackertarget] >
```

- Now repeat the process with the **bing** module. Compare the results with the **hackertarget** module.

```
[recon-ng][default] > workspaces create Test2
[recon-ng][Test2] > modules load bing
[recon-ng][Test2][bing_domain_web] > info
  Name: Bing Hostname Enumerator
  Author: Tim Tomes (@lanmaster53)
  Version: 1.1

  Description:
    Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table with the results.

  Options:
    Name      Current Value  Required  Description
    SOURCE    default      yes       source of input (see 'info' for details)

  Source Options:
    default   SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
    <string>  string representing a single input
    <path>   path to a file containing a list of inputs
    <query>  database query returning one column of inputs

[recon-ng][Test2][bing_domain_web] > options set source bing.net
SOURCE => bing.net
[recon-ng][Test2][bing_domain_web] > info
  Name: Bing Hostname Enumerator
  Author: Tim Tomes (@lanmaster53)
  Version: 1.1

  Description:
    Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table with the results.

  Options:
    Name      Current Value  Required  Description
    SOURCE    bing.net      yes       source of input (see 'info' for details)

  Source Options:
    default   SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
    <string>  string representing a single input
    <path>   path to a file containing a list of inputs
    <query>  database query returning one column of inputs

[recon-ng][Test2][bing_domain_web] > run

BING.NET
[*] URL: https://www.bing.com/search?first=0&q=domain%$Abing.net
[recon-ng][Test2][bing_domain_web] > dashboard
```

Step 6: Investigate the web interface.

Recon-NG has a web interface that simplifies and improves viewing results that are stored in Recon-NG databases. It also allows easy export of the results tables for reporting purposes.

- a. Open a new terminal.
 - b. Enter the **recon-web** command to start the Recon-*ng* server process. Note the command output.
 - c. In a new browser tab, access the webpage using the URL information provided in the output.

The screenshot shows a Kali Linux desktop environment with several open windows. In the top left, a browser window titled 'Recon-web' displays the interface for the 'recon-ng' tool, showing sections for domains, companies, netblocks, locations, vulnerabilities, ports, and hosts, all currently reporting 0 findings. The URL is `http://127.0.0.1:5000`. In the top right, a terminal window titled 'Session Actions Edit View Help' is running as user 'cylciah@kali'. It shows the initial configuration of 'recon-ng', including welcome messages, API endpoints, and workspace initialization. A warning at the bottom states: 'WARNING: This is a development server. Do not use it in a production deployment. Use a production WS GI SERVER instead.' The terminal also shows log entries for various HTTP requests to the local server. The system tray in the top right corner shows the date and time as 23:22.

- d. The web interface shows data from the default workspace when first opened. Click the orange workspace name at the top of the page to display data from different workspaces.

```

Session Actions Edit View Help
cygied@kali:~$ recon-web
=====
* Welcome to Recon-Web, the analytics and reporting engine for Recon-ng!
* This is a web-based user interface. Open the URL below in your browser to begin.
* Recon-web includes the Recon-API, which can be accessed via the '/api/' URL.
=====
[*] Marketplace disabled
[*] No modules installed.
* Workspace initialized: default
WARNING: This is a development server. Do not use it in a production deployment. Use a production WS
GI server instead.
* Running on http://127.0.0.1:5000
[recon-web] - [recon-web]
=====
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET / HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /recon.css HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /normalize.css HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /recon.js HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /datatable.js HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /jquery.min.js HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /skeleton.css HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /favicon.ico HTTP/1.1" 404 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /api/recon HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "PATCH /api/workspaces/default HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /api/tables/ HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /api/dashboard HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /api/reports/ HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /api/tables/Test1 HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:21:26] "GET /api/dashboard HTTP/1.1" 200 -
* Workspace initialized: Test1
27.0.0.1 - - [12/Dec/2025:23:22:24] "PATCH /api/workspaces/Test1 HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:22:44] "GET /api/tables/ HTTP/1.1" 200 -
27.0.0.1 - - [12/Dec/2025:23:22:44] "GET /api/dashboard HTTP/1.1" 200 -
* Workspace initialized: Test2
27.0.0.1 - - [12/Dec/2025:23:22:44] "PATCH /api/workspaces/Test2 HTTP/1.1" 200 -

```

Part 4: Find Interesting Files with Recon-ng

In this part of the lab, we will install and use another plugin.

Step 1: Install another module.

- Search the marketplace for a module that will discover interesting files in a domain. The plugin that you use should have no dependencies or key requirements.

```
[recon-ng][default] > marketplace search grep | domain
[*] Searching module index for 'grep | domain' ...
```

Path	Version	Status	Updated	D	K
discovery/info_disclosure/cache_snoop	1.1	not installed	2020-10-13		
recon/companies-domains/pen	1.1	not installed	2019-10-15		
recon/companies-domains/viewdns_reverse_whois	1.1	not installed	2021-08-24		
recon/companies-multi/censys_tls_subjects	2.1	not installed	2022-01-31	*	*
recon/contacts-domains/censys_email_to_domains	2.1	not installed	2022-01-31	*	*
recon/contacts-domains/migrate_contacts	1.1	not installed	2020-05-17		
recon/domains-companies/censys_companies	2.1	not installed	2022-01-31	*	*
recon/domains-companies/pen	1.1	not installed	2019-10-15		
recon/domains-companies/whoxy_whois	1.1	not installed	2020-06-24		*
recon/domains-contacts/hunter_io	1.3	not installed	2020-04-14		*
recon/domains-contacts/metacrawler	1.1	not installed	2019-06-24	*	
recon/domains-contacts/pen	1.1	not installed	2019-10-15		
recon/domains-contacts/pgp_search	1.4	not installed	2019-10-16		
recon/domains-contacts/whois_pocs	1.0	not installed	2019-06-24		
recon/domains-contacts/wikileaker	1.0	not installed	2020-04-08		
recon/domains-hosts/builtwith	1.1	not installed	2021-08-24		*
recon/domains-hosts/censys_domain	2.1	not installed	2022-01-31	*	*
recon/domains-hosts/mx_spf_ip	1.0	not installed	2019-06-24		
recon/domains-hosts/ssl_san	1.0	not installed	2019-06-24		
recon/domains-vulnerabilities/ghdb	1.1	not installed	2019-06-26		
recon/domains-vulnerabilities/xssed	1.1	not installed	2020-10-18		
recon/hosts-domains/migrate_hosts	1.1	not installed	2020-05-17		
recon/hosts-hosts/virustotal	1.0	not installed	2019-06-24		*
recon/netblocks-hosts/virustotal	1.0	not installed	2019-06-24		*

D = Has dependencies. See info for details.

K = Requires keys. See info for details.

Install and load the plugin.

```
[recon-ng][default] > marketplace install discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Reloading modules ...
[recon-ng][default] > modules load discovery/info_disclosure/cache_snoop
[recon-ng][cache_snoop] >
```

Step 2: Run the new module.

- Set the source option to **hackxor.net** or another location of your choice. (Please comply with the terms of the course when choosing a domain.) The h4cker.org website is interesting also.
- Run the command. This module creates a .csv file in the recon-ng/data folder.
- Locate the file and view the contents. Some of these files can be downloaded or viewed using the URLs in the command output.

