

# Using OSINT Tools

## Introduction

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. 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.

## Part 1: Examine OSINT Resources

### Step 1: Access the OSINT Framework

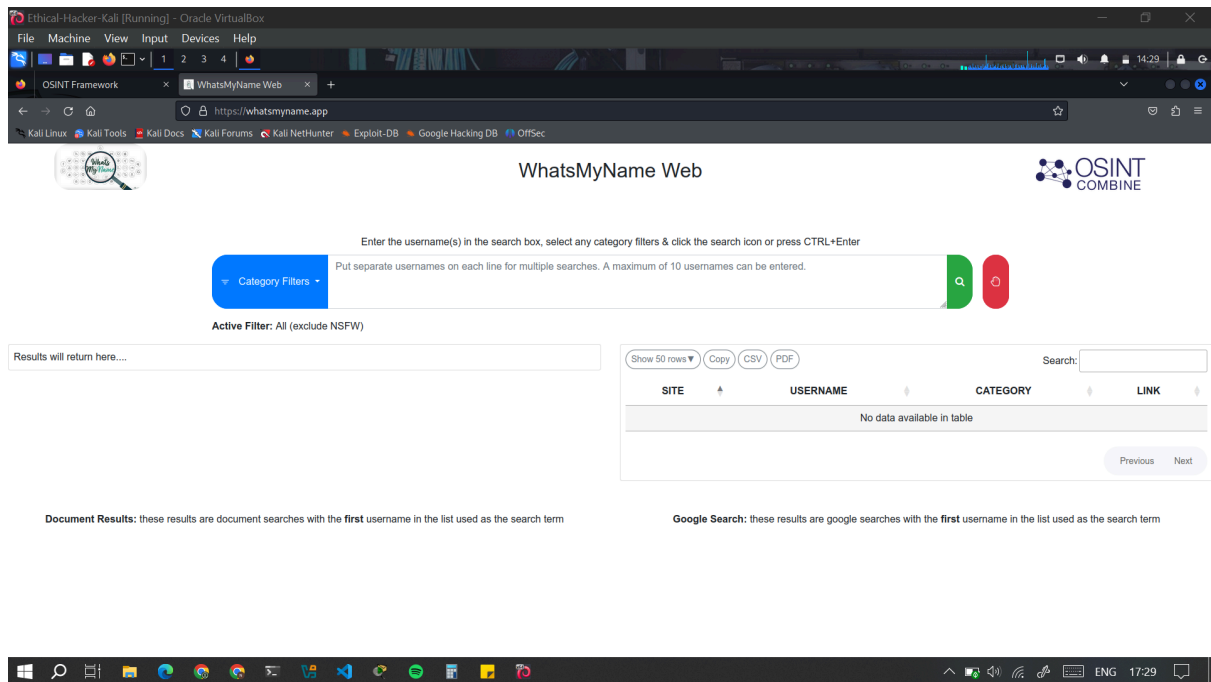
The OSINT Framework is a useful way to visualize the OSINT tools and resources that are available at <https://osintframework.com/>.

I clicked **Username** at the top of the tree and under **Username Search Engines**, clicked **WhatsMyName(T)** tool. The T Indicates a link to the tool that must be installed and run locally

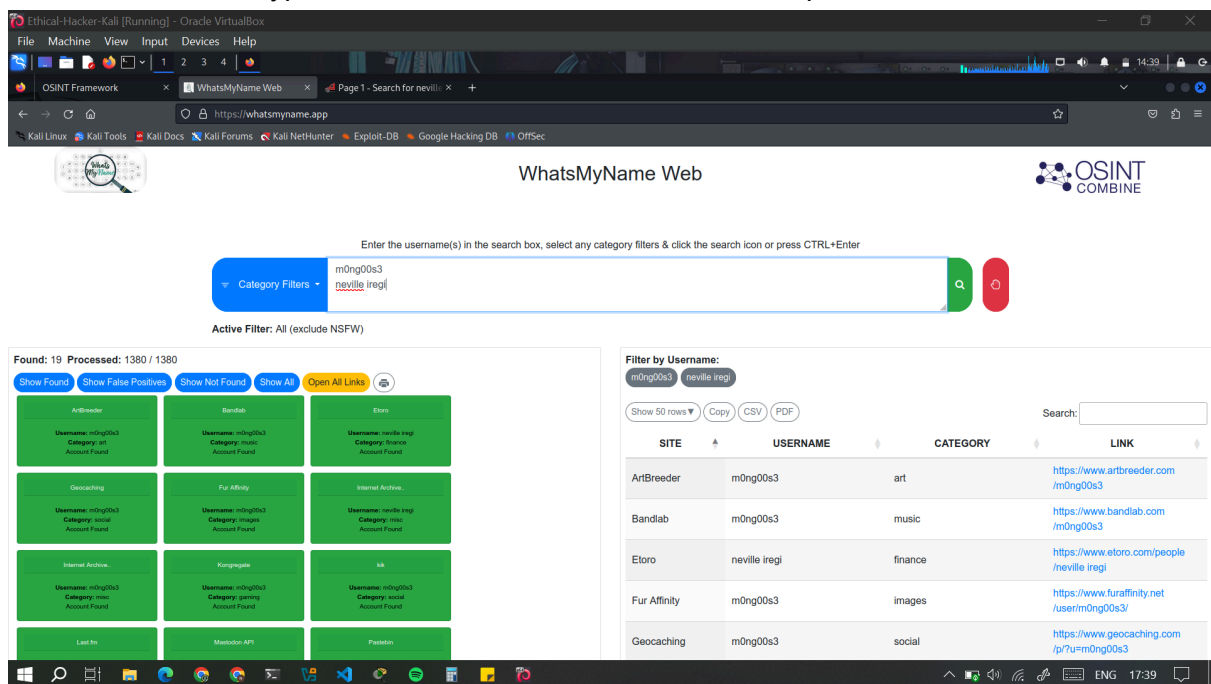
The screenshot shows a web browser window displaying the OSINT Framework website. The browser's address bar shows the URL <https://osintframework.com/>. The website's main content is a tree diagram of OSINT tools. The 'Username' category is expanded, showing 'Username Search Engines' and 'Specific Sites'. Under 'Username Search Engines', the 'WhatsMyName (T)' tool is highlighted. A legend on the right explains the symbols: (T) for tools to be installed and run locally, (D) for Google Dorks, (R) for registration, and (M) for manual URL editing. A 'Toggle dark mode' button is also visible.

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. The tool has a web interface at <https://whatsmyname.app/>



In the search box, I typed in a some usernames, each on a separate line.



- 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.

The value of doing username searches and account enumeration include:

1. Username searching can identify accounts that important enterprise personnel may have on various sites. Because other sites can be vulnerable, it is possible that

hackers could gain access to personnel information from those accounts, including passwords, addresses, and telephone numbers.

2. The types of sites that personnel have registered for can also provide details of their lives and interests. These details could be used in **social engineering attacks**.

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

The [start.me](https://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. You can enter OSINT-relevant search terms to find links to related resources.

At the time of writing, this project has been shut down.

## Part 2: Use SpiderFoot

SpiderFoot is an automated OSINT scanner. It is included with Kali. SpiderFoot queries over 1000 open-information sources and presents the results in an easy-to-use GUI. SpiderFoot can also be run from a console. SpiderFoot seeds its scan with one of the following:

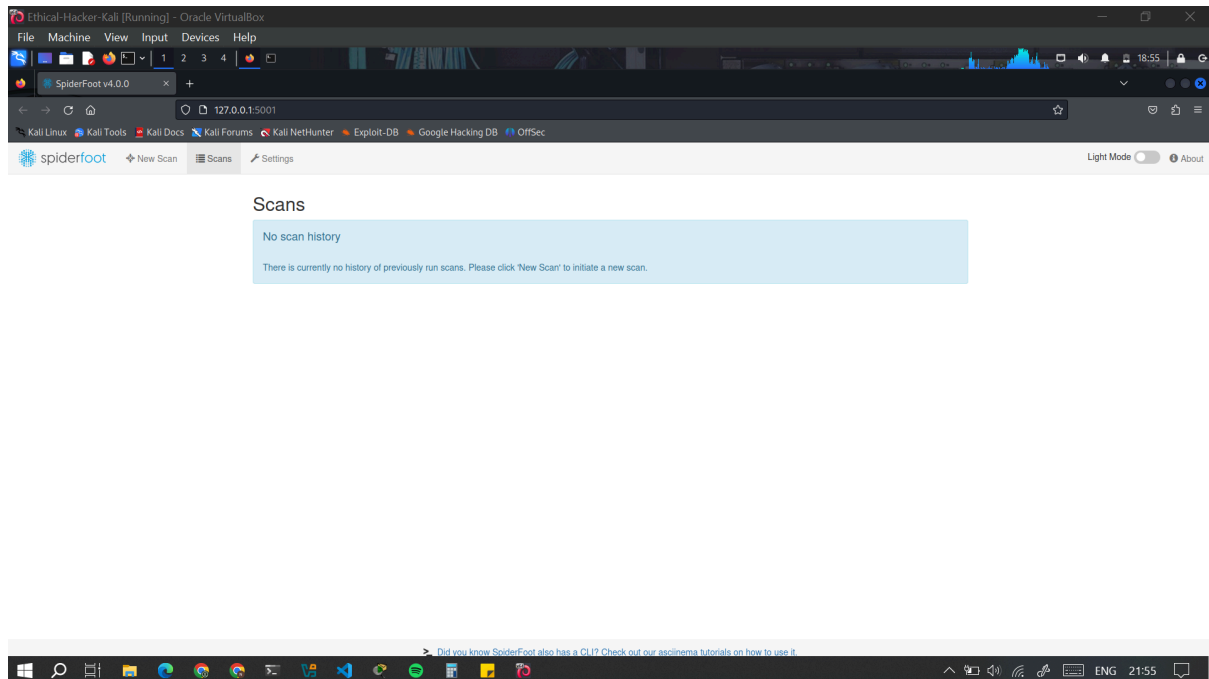
- Domain names
- IP addresses
- Subnet addresses
- Autonomous System Numbers (ASN) - a unique identifier (16-bit or 32-bit integer) assigned to a network, such as an ISP or large organization, to enable routing information exchange across the internet using the Border Gateway Protocol (BGP)
- Email addresses
- 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:

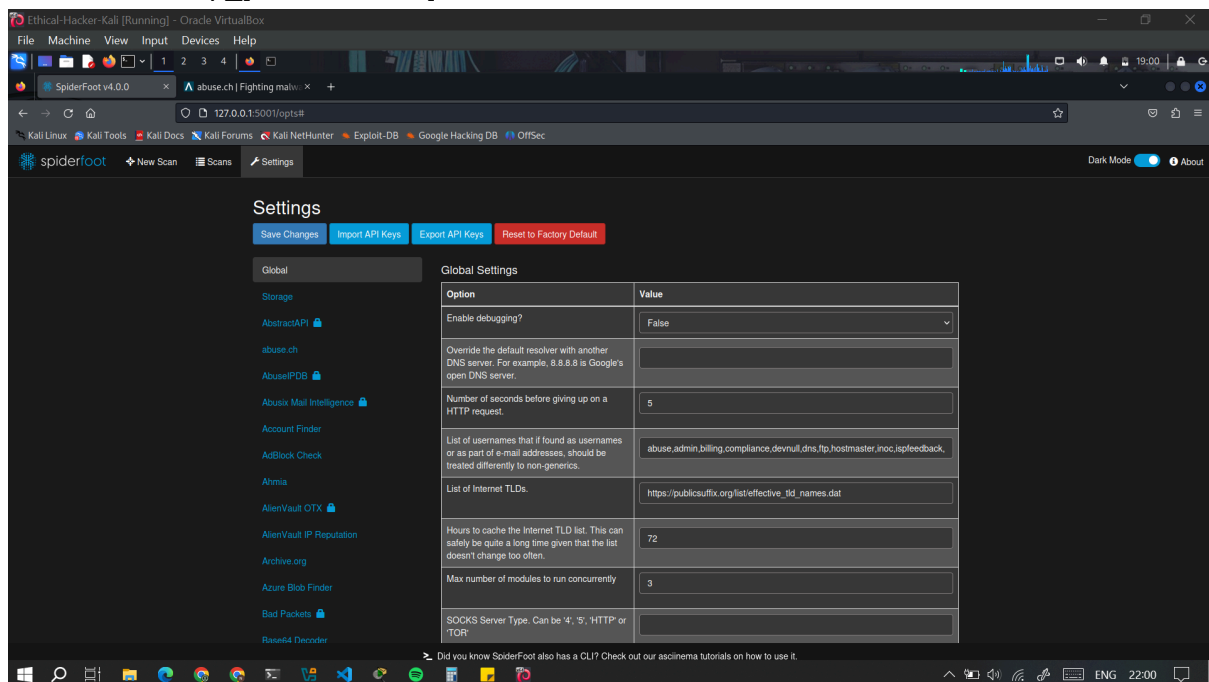
1. All – Get every possible piece of information about the target. This use case can take a very long time to complete.
2. Footprint – Understand the target's network perimeter, associated identities and other information that is yielded by extensive web crawling and search engine use.
3. Investigate – This is for targets that you suspect of malicious behavior. Footprinting, blacklist lookups, and other sources that report on malicious sites will be returned.
4. 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.

Using SpiderFoot in a terminal: `L$ spiderfoot -l 127.0.0.1:5001`

- -l indicates the ip and port to listen on
- Running the command opens a SpiderFoot web interface that displays a list of all the scans ran recently.



SpiderFoot uses over 200 scanners to build its reports. The Scanner name is in the settings menu. The module name appears in the details for the scanner. All SpiderFoot modules are referred to as `sfp_[module name]`.

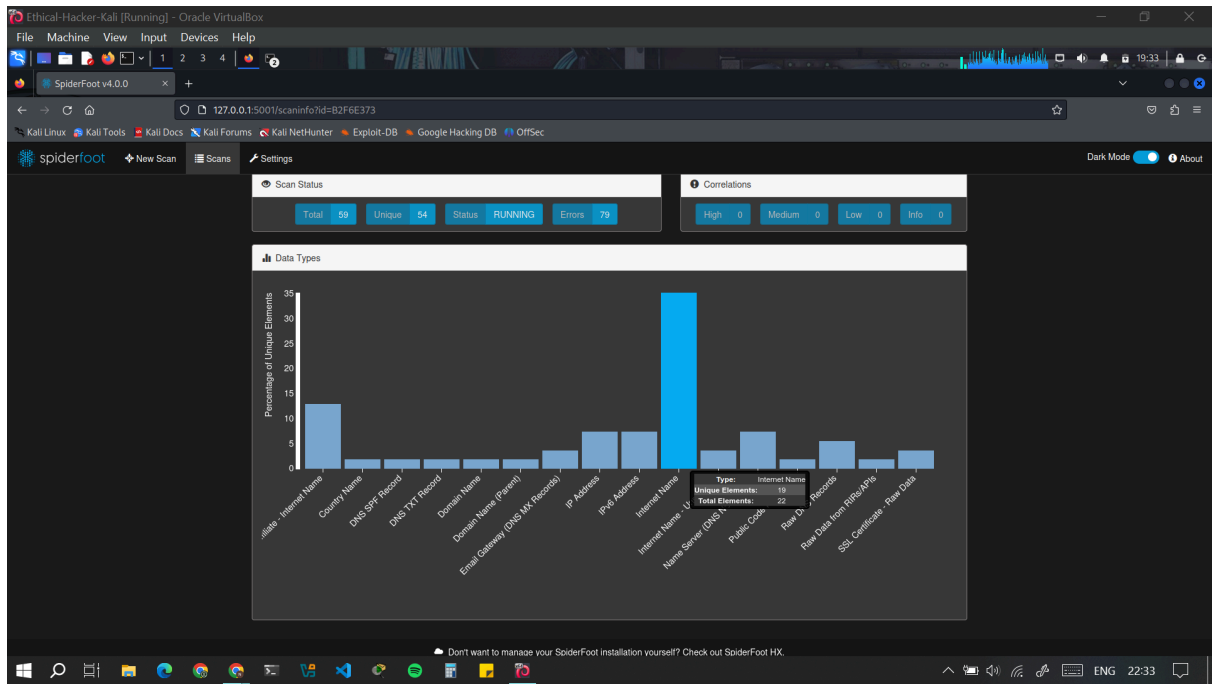


- scanners with a lock next to them indicate an API key is necessary. Further information regarding the key requirements is provided in the details for the scanner. Click the “?” icon next to the API Settings option.
- You can display all the modules that are available in SpiderFoot using `spiderfoot -M`

```
kali@kali:~$ spiderfoot -M
2020-02-23 19:04:23,394 [INFO] sf : Modules available:
sfp_abstractapi    Look up domain, phone and IP address information from AbstractAPI.
sfp_abusech        Check if a host/domain, IP address or netblock is malicious according to Abuse.ch.
sfp_abuseipdb      Check if an IP address is malicious according to AbuseIPDB.com blacklist.
sfp_abusix         Check if a netblock or IP address is in the Abusix Mail Intelligence blacklist.
sfp_accounts       Look for possible associated accounts on nearly 200 websites like Ebay, Slashdot, reddit, etc.
sfp_adblock        Check if linked pages would be blocked by Adblock-Plus.
sfp_adguard_dns    Check if a host would be blocked by AdGuard DNS.
sfp_ahmia           Search for 'Ahmia' search engine for mentions of the target.
sfp_alienvault     Obtain information from AlienVault Open Threat Exchange (OTX)
sfp_alienvaultiprep Check if an IP or netblock is malicious according to the AlienVault IP Reputation database.
sfp_apple_itunes   Search Apple iTunes for mobile apps.
sfp_archivorg      Identifies historic versions of interesting files/pages from the Wayback Machine.
sfp_arin           Queries ARIN registry for contact information.
sfp_azureblobstorage Search for potential Azure blobs associated with the target and attempt to list their contents.
sfp_badpackets     Obtain information about any malicious activities involving IP addresses found
sfp_basess         Identify Base64-encoded strings in URLs, often revealing interesting hidden information.
sfp_bogview        Obtain network information from Bogview API.
sfp_binaryedge     Obtain information from BinaryEdge.io Internet scanning systems, including breaches, vulnerabilities, torrents and passive DNS.
sfp_bingsearch     Obtain information from Bing to identify sub-domains and links.
sfp_bingshareip    Search Bing for hosts sharing the same IP.
sfp_binstring      Attempt to identify strings in binary content.
sfp_bitcoin        Identify bitcoin addresses in scraped webpages.
sfp_bitcoinabuse   Check Bitcoin addresses against the bitcoinabuse.com database of suspect/malicious addresses.
sfp_bitcoinwhoiswho Check for Bitcoin addresses against the bitcoin who's who database of suspect/malicious addresses.
sfp_blockchain     Queries blockchain.info to find the balance of identified bitcoin wallet addresses.
sfp_blocklistde    Check if a netblock or IP is malicious according to blocklist.de.
sfp_botscout       Searches BotScout.com's database of spam-bot IP addresses and e-mail addresses.
sfp_botvrij        Check if a domain is malicious according to botvrij.eu.
sfp_builtwith      Query BuiltWith.com's Domain API for information about your target's web technology stack, e-mail addresses and more.
sfp_csp            Queries the CSP API which offers various data (geo location, proxy detection, phone lookup, etc).
sfp_callername     Lookup US phone number location and reputation information.
sfp_censys         Obtain host information from Censys.io.
sfp_certspotter    Gather information about SSL certificates from SSLMate CertSpotter API.
sfp_cinsscore      Check if a netblock or IP address is malicious according to Collective Intelligence Network Security (CINS) Army List.
sfp_cirille        Obtain information from CIRILLE's Passive DNS and Passive SSL databases.
sfp_citadel        Searches Leak-lookup.com's database of breaches.
sfp_cleanbrowsing  Check if a host would be blocked by CleanBrowsing.org DNS content filters.
sfp_clearbit       Check if a netblock or IP address is on clearbit.org's spam IP list.
sfp_cloudflaredns  Check for names, addresses, domains and more based on lookups of e-mail addresses on clearbit.com.
sfp_cloudlocke     Check if a host would be blocked by CloudFlare DNS.
sfp_cloudlocke     Check if a domain appears on CloudLocke lists.
sfp_commoncrawl    Searches for URLs found through CommonCrawl.org.
sfp_comodo         Check if a host would be blocked by Comodo Secure DNS.
sfp_company        Identify company names in any obtained data.
sfp_cookie         Extract Cookies from HTTP headers.
sfp_countryname    Identify country names in any obtained data.
sfp_creditcard     Identify Credit Card Numbers in any data.
sfp_crobot_api     Search Crobot API for subdomains.
sfp_crossref       Identify whether other domains are associated ('Affiliates') of the target by looking for links back to the target site(s).
sfp_crt            Gather hostnames from historical certificates in crt.sh.
sfp_crxcavator     Search CRXCavator for Chrome extensions.
```

A typical SpiderFoot scan for a domain in the GUI e.g [h4cker.org](https://hacker.org) requires one to select 'new scan' and enter the scan name and scan target as well choosing which method to scan by (use case/required data/individual module)

- Using the use case method, I selected '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.
- On running the scan, a bar graph appears. 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.



## 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). It consists of a series of modules that can be run in their own workspaces. The modules can be configured to run with option settings that are specific to the module. This simplifies running Recon-ng at the command line because options for the modules are independently set within the workspace. When you run the module, it uses these settings to perform its searches.

As the name suggests, Recon-ng is used to perform a wide range of reconnaissance activities on different settings that you provide.

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.



```

Ethical-Hacker-Kali (Running) - Oracle VirtualBox
File Machine View Input Devices Help
kai@Kali -
File Actions Edit View Help

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

[*] No modules enabled/installed.
[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] > modules
Interfaces with installed modules

Usage: modules <load|reload|search> [...]

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

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

[recon-ng][default] > workspaces list

Workspaces | Modified
-----|-----
default   | 2020-02-23 19:49:02

[recon-ng][default] > workspaces remove
Removes an existing workspace

Usage: workspace remove <name>

[recon-ng][default] > workspace create test
[recon-ng][default] > workspaces create test
[recon-ng][test] >

```

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.

- Command 'modules search' displays the currently installed modules

Recon-ng cannot function without modules which can be installed from the recon-ng marketplace (a github public repo). Using 'marketplace search' once can list all the modules currently available.

```

Ethical-Hacker-Kali (Running) - Oracle VirtualBox
File Machine View Input Devices Help
kai@Kali -
File Actions Edit View Help

[recon-ng][default] > modules search
!!! No modules found
Searches installed modules

Usage: modules search <regex>

[recon-ng][default] > marketplace search

Path | Version | Status | Updated | D | K |
-----|-----|-----|-----|---|---|
| discovery/info_disclosure/cache_snoop | 1.1 | not installed | 2020-10-13 | | |
| discovery/info_disclosure/interesting_files | 1.2 | not installed | 2021-10-04 | | |
| exploitation/injection/command_injector | 1.0 | not installed | 2019-06-24 | | |
| exploitation/injection/xpath_bruter | 1.2 | not installed | 2019-10-08 | | |
| import/csv_file | 1.1 | not installed | 2019-08-09 | | |
| import/list | 1.1 | not installed | 2019-06-24 | | |
| import/masscan | 1.0 | not installed | 2020-04-07 | | |
| import/rmap | 1.1 | not installed | 2020-10-06 | | |
| recon/companies-contacts/bing_linkedin_cache | 1.0 | not installed | 2019-06-24 | | *
| recon/companies-contacts/censys_email_address | 2.1 | not installed | 2022-01-31 | * *
| recon/companies-contacts/censys | 1.1 | not installed | 2019-10-15 | | |
| recon/companies-domains/censys_subdomains | 2.1 | not installed | 2022-01-31 | * *
| recon/companies-domains/censys | 1.1 | not installed | 2019-10-15 | | |
| recon/companies-domains/ptrdns_reverse_whois | 1.1 | not installed | 2020-06-17 | | *
| recon/companies-multi/censys_org | 2.1 | not installed | 2022-01-31 | * *
| recon/companies-multi/censys_tls_subjects | 2.1 | not installed | 2022-01-31 | * *
| recon/companies-multi/github_miner | 1.1 | not installed | 2020-05-15 | | *
| recon/companies-multi/shodan_org | 1.1 | not installed | 2020-07-01 | | *
| recon/companies-multi/whois_miner | 1.1 | not installed | 2019-10-15 | | |
| recon/contacts-contacts/abc | 1.0 | not installed | 2019-10-11 | | *
| recon/contacts-contacts/allrester | 1.0 | not installed | 2019-06-24 | | |
| recon/contacts-contacts/mangle | 1.0 | not installed | 2019-06-24 | | |
| recon/contacts-contacts/umangle | 1.1 | not installed | 2019-10-27 | | |
| recon/contacts-credentials/hbpb_breach | 1.2 | not installed | 2019-09-10 | | *
| recon/contacts-credentials/hbpb_paaste | 1.1 | not installed | 2019-09-10 | | *
| 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/contacts-profiles/fullcontact | 1.1 | not installed | 2019-07-24 | | *
| recon/credentials-credentials/afrobe | 1.0 | not installed | 2019-06-24 | | |
| recon/credentials-credentials/bozocrack | 1.0 | not installed | 2019-06-24 | | |
| recon/credentials-credentials/hashes_org | 1.0 | not installed | 2019-06-24 | | *
| recon/domains-companies/censys_companies | 2.1 | not installed | 2022-01-31 | * *
| recon/domains-companies/ppn | 1.1 | not installed | 2019-10-15 | | |
| recon/domains-contacts/whois_whois | 1.1 | not installed | 2020-06-24 | | *
| recon/domains-contacts/hunter_10 | 1.3 | not installed | 2020-04-14 | | *
| recon/domains-contacts/metacrawler | 1.1 | not installed | 2019-06-24 | | *
| recon/domains-contacts/ppn | 1.1 | not installed | 2019-10-15 | | |
| recon/domains-contacts/ppp_search | 1.4 | not installed | 2019-10-16 | | |
| recon/domains-contacts/whis_poc | 1.0 | not installed | 2019-06-24 | | |
| recon/domains-contacts/willmaker | 1.0 | not installed | 2020-04-08 | | |
| recon/domains-domains/brute_suffix | 1.1 | not installed | 2020-05-17 | | |
| recon/domains-hosts/binaryedge | 1.2 | not installed | 2020-06-18 | | *

```

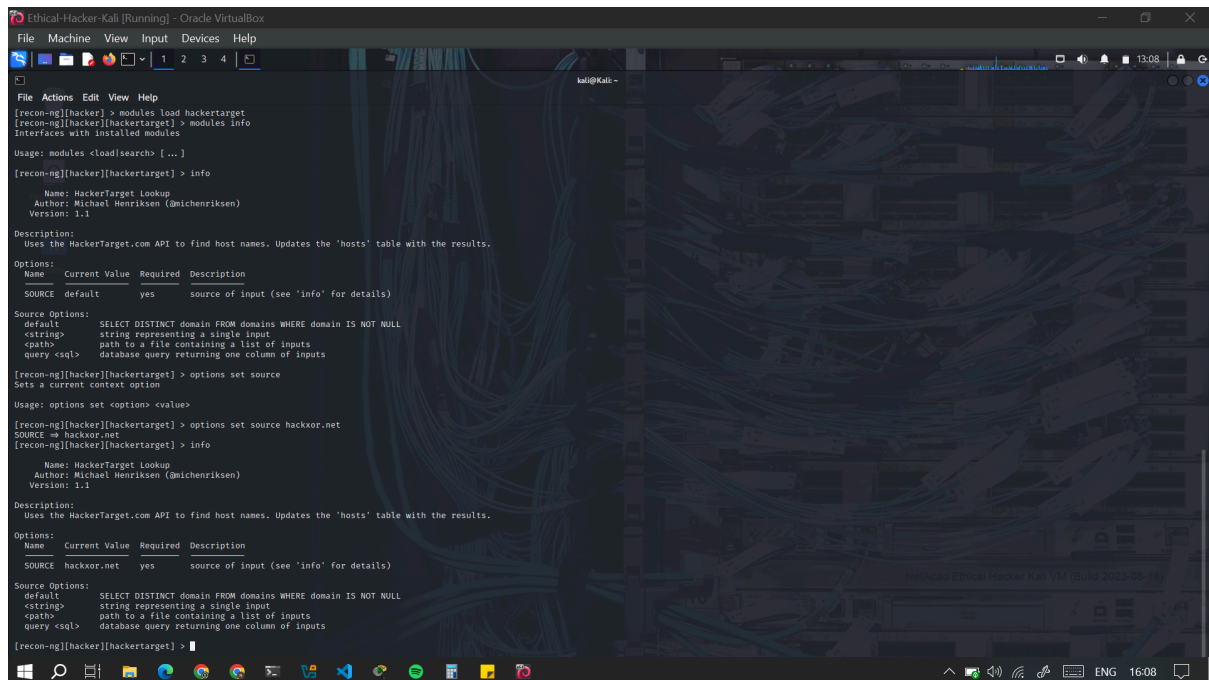
The module tables have columns for D and K.

- D = Has dependencies.





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. I used the *'options set source'* command to set the only option for this module. I then completed the command by specifying the target as [hackxor.net](https://hackxor.net) and verified the option setting with the info command.

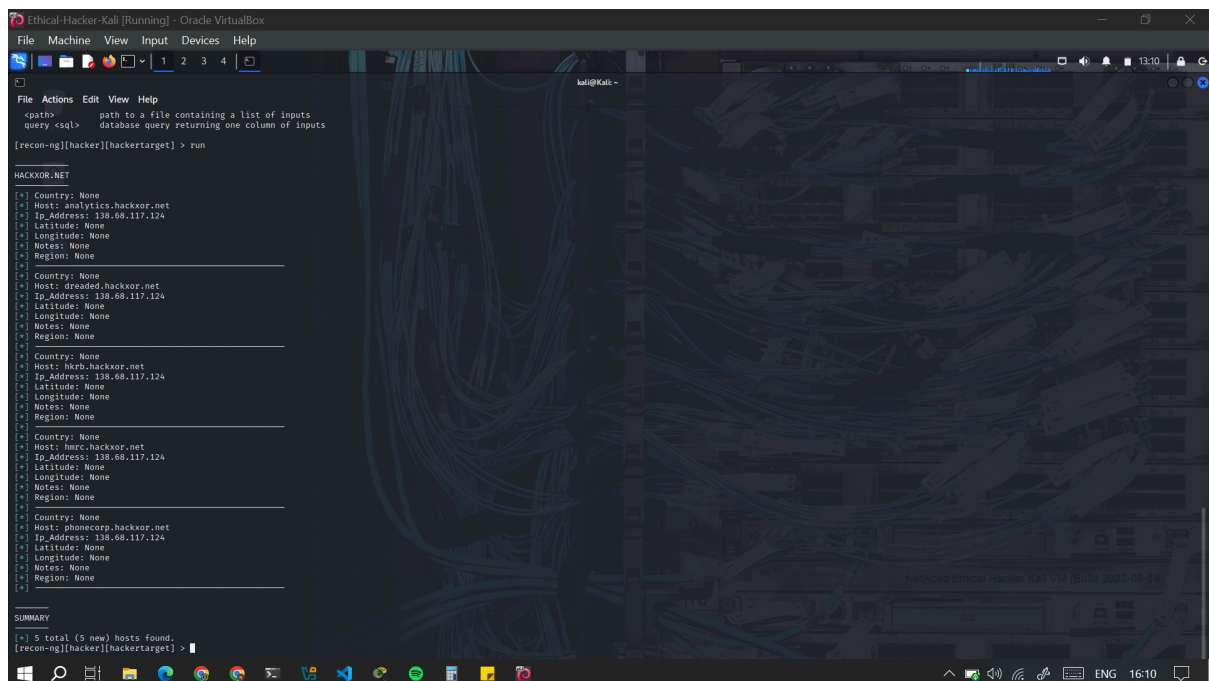


```

Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[recon-ng][hacker] > modules load hackertarget
[recon-ng][hacker][hackertarget] > modules info
Interfaces with installed modules
Usage: modules <load|search> [...]
[recon-ng][hacker][hackertarget] > info
Name: HackerTarget Lookup
Author: Michael Henriksen (Amichenriksen)
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][hacker][hackertarget] > options set source
Sets a current context option
Usage: options set <option> <value>
[recon-ng][hacker][hackertarget] > options set source hackxor.net
SOURCE => hackxor.net
[recon-ng][hacker][hackertarget] > info
Name: HackerTarget Lookup
Author: Michael Henriksen (Amichenriksen)
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][hacker][hackertarget] >

```

I used the *'run'* command to execute the module



```

Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
<path>    path to a file containing a list of inputs
query <sql> database query returning one column of inputs
[recon-ng][hacker][hackertarget] > run
HACKXOR.NET
[*] Country: None
[*] Host: analytics.hackxor.net
[*] Ip Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: drcaded.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: phonecorp.hackxor.net
[*] Ip Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
SUMMARY
[*] 5 total (5 new) hosts found.
[recon-ng][hacker][hackertarget] >

```

- 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.
- One can also 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.

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

```

[recon-ng][hacker][hackertarget] >
[recon-ng][hacker] > modules load hackertarget
[recon-ng][hacker][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 | 5 |
| Contacts | 0 |
| Credentials | 0 |
| Leaks | 0 |
| Pushpins | 0 |
| Profiles | 0 |
| Repositories | 0 |

[recon-ng][hacker][hackertarget] > show hosts

+----+-----+-----+-----+-----+-----+-----+-----+
| rowid | host | ip_address | region | country | latitude | longitude | notes | module |
+----+-----+-----+-----+-----+-----+-----+-----+
| 1 | analytics.hackxor.net | 138.68.117.124 | | | | | | hackertarget |
| 2 | dreaded.hackxor.net | 138.68.117.124 | | | | | | hackertarget |
| 3 | hcrb.hackxor.net | 138.68.117.124 | | | | | | hackertarget |
| 4 | hmc.hackxor.net | 138.68.117.124 | | | | | | hackertarget |
| 5 | phonecorp.hackxor.net | 138.68.117.124 | | | | | | hackertarget |
+----+-----+-----+-----+-----+-----+-----+-----+

[*] 5 rows returned
[recon-ng][hacker][hackertarget] >

```

Recon-ng also 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. To use it:

1. I opened a new terminal and entered the recon-web command to start the Recon-ng server process.
2. I was then able to access the webpage using the URL information provided in the output.

```

kali@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.
[*] Version check disabled.
[*] Workspace initialized: default
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on http://127.0.0.1:5000
Press CTRL-C to quit
127.0.0.1 - [24/Feb/2026 13:21:39] "GET / HTTP/1.1" 200 -
127.0.0.1 - [24/Feb/2026 13:21:40] "GET /recon.css HTTP/1.1" 200 -
127.0.0.1 - [24/Feb/2026 13:21:40] "GET /normalize.css HTTP/1.1" 200 -
127.0.0.1 - [24/Feb/2026 13:21:40] "GET /skeleton.css HTTP/1.1" 200 -
127.0.0.1 - [24/Feb/2026 13:21:40] "GET /jquery.min.js HTTP/1.1" 200 -
127.0.0.1 - [24/Feb/2026 13:21:40] "GET /sortable.js HTTP/1.1" 200 -
127.0.0.1 - [24/Feb/2026 13:21:40] "GET /recon.js HTTP/1.1" 200 -
127.0.0.1 - [24/Feb/2026 13:21:40] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - [24/Feb/2026 13:21:40] "PATCH /api/workspaces/default HTTP/1.1" 200 -
127.0.0.1 - [24/Feb/2026 13:21:40] "GET /api/tables/ HTTP/2.1" 200 -
127.0.0.1 - [24/Feb/2026 13:21:40] "GET /api/reports/ HTTP/1.1" 200 -
127.0.0.1 - [24/Feb/2026 13:21:40] "GET /api/dashboard HTTP/1.1" 200 -

```

