Red Team Recon

Reconnaissance (recon) can be defined as a preliminary survey or observation of your target (client) without alerting them to your activities.

topics:

- Types of reconnaissance activities
- WHOIS and DNS-based reconnaissance
- Advanced searching
- Searching by image
- Google Hacking
- Specialized search engines
- Recon-ng
- Maltego

Reconnaissance can be broken down into two parts — passive reconnaissance and active reconnaissance

Passive recon doesn't require interacting with the target. In other words, you aren't sending any packets or requests to the target or the systems your target owns. Instead, passive recon relies on publicly available information that is collected and maintained by a third party. Open Source Intelligence (OSINT) is used to collect information about the target and can be as simple as viewing a target's publicly available social media profile.

Active recon requires interacting with the target by sending requests and packets and observing if and how it responds. The responses collected - or lack of responses - would enable us to expand on the picture we started developing using passive recon. An example of active reconnaissance is using Nmap to scan target subnets and live hosts.

Active recon can be classified as:

1. **External Recon**: Conducted outside the target's network and focuses on the externally facing assets assessable from the Internet. One example is running Nikto from outside the company network.
2. **Internal Recon**: Conducted from within the target company's network. In other words, the pentester or red teamer might be physically located inside the company building. In this scenario, they might be using an exploited host on the target's network.

Task - 3

Built-in Tools

tools used in this:

- `whois`
- `dig`, `nslookup`, `host`
- `traceroute`/`tracert`

$ whois

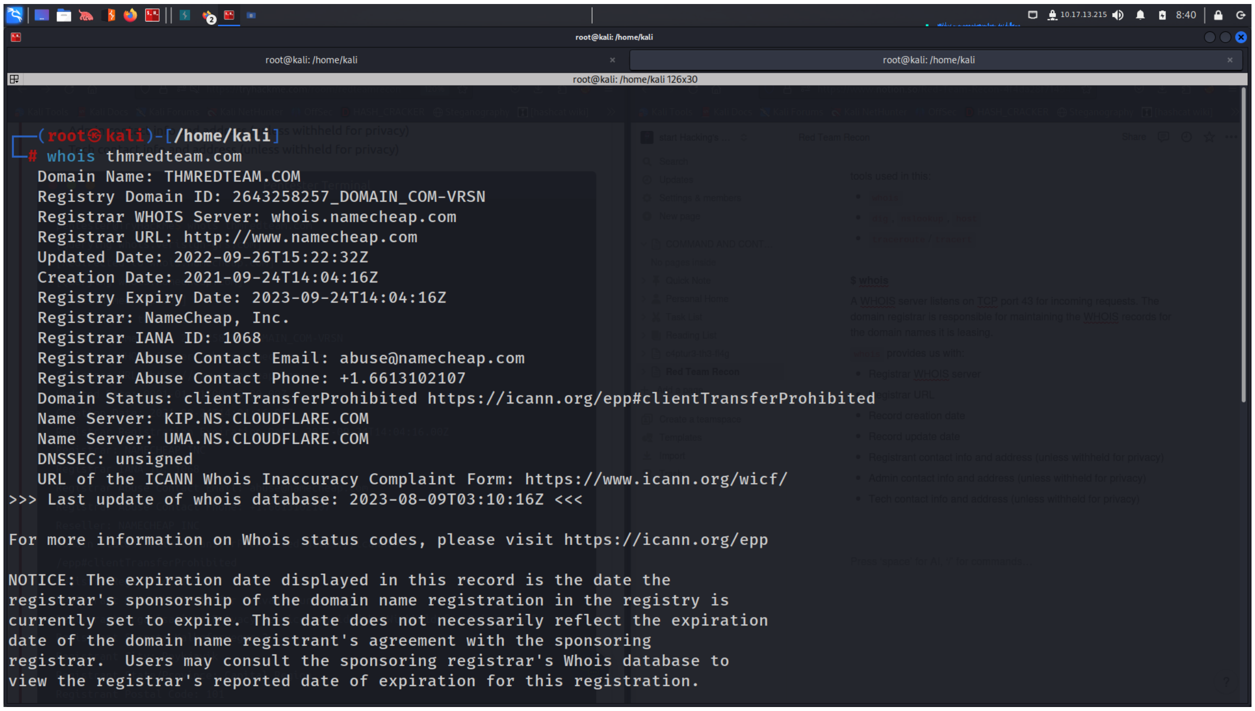
A WHOIS server listens on TCP port 43 for incoming requests. The domain registrar is responsible for maintaining the WHOIS records for the domain names it is leasing.

`whois` provides us with:

- Registrar WHOIS server
- Registrar URL
- Record creation date
- Record update date
- Registrant contact info and address (unless withheld for privacy)

- Admin contact info and address (unless withheld for privacy)
- Tech contact info and address (unless withheld for privacy)

```
$ whois thmredteam.com
```



```
┌──(root㉿kali)-[/home/kali]
└─# whois thmredteam.com
   Domain Name: THMREDTEAM.COM
   Registry Domain ID: 2643258257_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.namecheap.com
   Registrar URL: http://www.namecheap.com
   Updated Date: 2022-09-26T15:22:32Z
   Creation Date: 2021-09-24T14:04:16Z
   Registry Expiry Date: 2023-09-24T14:04:16Z
   Registrar: NameCheap, Inc.
   Registrar IANA ID: 1068
   Registrar Abuse Contact Email: abuse@namecheap.com
   Registrar Abuse Contact Phone: +1.6613102107
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: KIP.NS.CLOUDFLARE.COM
   Name Server: UMA.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-08-09T03:10:16Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

After a `whois` lookup, we might get lucky and find names, email addresses, postal addresses, and phone numbers, in addition to other technical information. At the end of the `whois` query, we find the authoritative name servers for the domain in question.

nslookup:

DNS queries can be executed with many different tools found on our systems, especially Unix-like systems. One common tool found on Unix-like systems, Windows, and macOS is `nslookup`

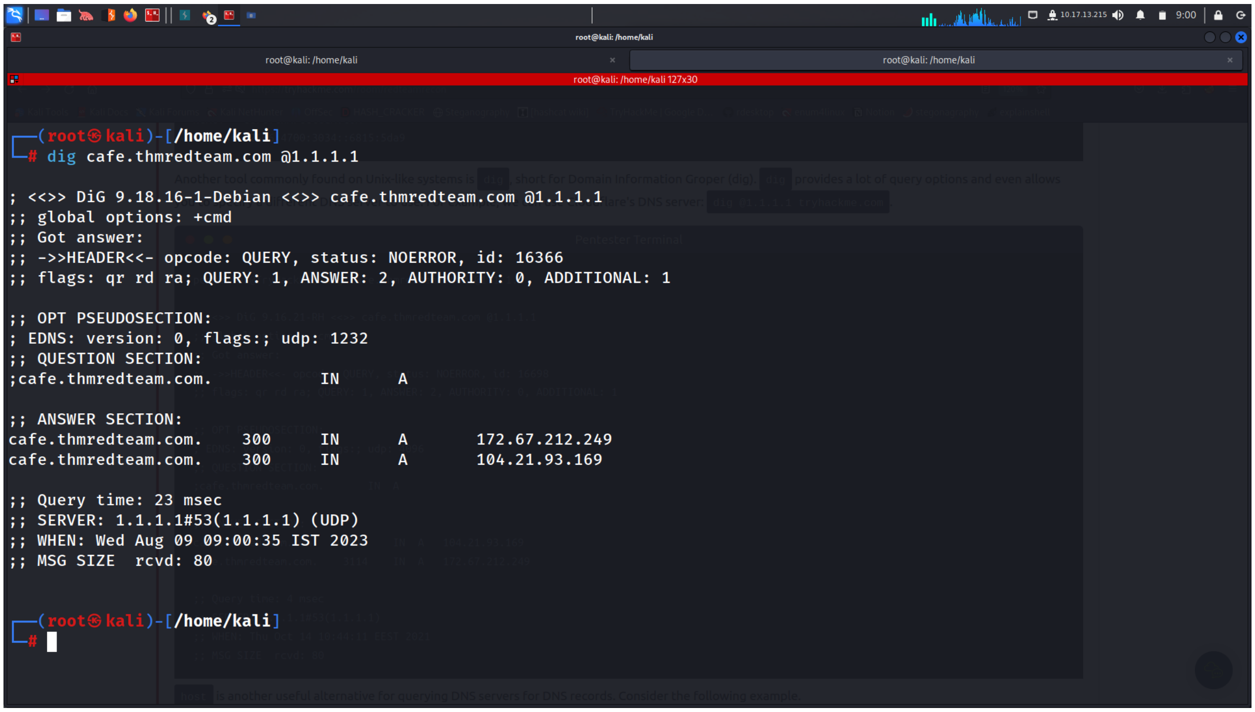
```
nslookup cafe.thmredteam.com
Server:         192.168.220.2
```

Address: 192.168.220.2#53

Non-authoritative answer:
Name: cafe.thmredteam.com
Address: 172.67.212.249
Name: cafe.thmredteam.com
Address: 104.21.93.169
Name: cafe.thmredteam.com
Address: 2606:4700:3034::6815:5da9
Name: cafe.thmredteam.com
Address: 2606:4700:3034::ac43:d4f9

dig

Another tool commonly found on Unix-like systems is `dig`, short for Domain Information Groper (dig). `dig`
 provides a lot of query options and even allows you to specify a
different DNS server to use. For example, we can use Cloudflare's DNS
server: `dig @1.1.1.1 tryhackme.com`



```
┌──(root㉿kali)-[/home/kali]
└─# dig cafe.thmredteam.com @1.1.1.1

; <<>> DiG 9.18.16-1-Debian <<>> cafe.thmredteam.com @1.1.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16366
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;cafe.thmredteam.com.           IN      A

;; ANSWER SECTION:
cafe.thmredteam.com.    300     IN      A       172.67.212.249
cafe.thmredteam.com.    300     IN      A       104.21.93.169

;; Query time: 23 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Wed Aug 09 09:00:35 IST 2023
;; MSG SIZE  rcvd: 80


┌──(root㉿kali)-[/home/kali]
└─# 
```

`host` is another useful alternative for querying DNS servers for DNS records. Consider the following example.

```
$ host cafe.thmredteam.comcafe.thmredteam.com has address 172.67.212.249
cafe.thmredteam.com has address 104.21.93.169
cafe.thmredteam.com has IPv6 address 2606:4700:3034::ac43:d4f9
cafe.thmredteam.com has IPv6 address 2606:4700:3034::6815:5da9
```

`traceroute`, it traces the route taken by the packets from out system to the target host. The console output below shows the traceroute provided us with the touter connecting us to the target system. its worth stressing that some routers dont respond to the packets sent bu tracetoute, and as as a result, we dont see their IP addresses; a * is used to indicate such a case.

```
$ traceroute cafe.thmredteam.comtraceroute to cafe.thmredteam.com (172.67.212.249), 30 hops
 max, 60 byte packets
 1  _gateway (192.168.0.1)  3.535 ms  3.450 ms  3.398 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  172.16.79.229 (172.16.79.229)  4.663 ms  6.417 ms  6.347 ms
 8  * * *
 9  172.16.49.1 (172.16.49.1)  6.688 ms 172.16.48.1 (172.16.48.1)  6.671 ms 172.16.49.1 (17
2.16.49.1)  6.651 ms
10  213.242.116.233 (213.242.116.233)  96.769 ms 81.52.187.243 (81.52.187.243)  96.634 ms  9
6.614 ms
11  bundle-ether302.pastr4.paris.opentransit.net (193.251.131.116)  96.592 ms  96.689 ms  9
6.671 ms
12  193.251.133.251 (193.251.133.251)  96.679 ms  96.660 ms  72.465 ms
13  193.251.150.10 (193.251.150.10)  72.392 ms 172.67.212.249 (172.67.212.249)  91.378 ms  9
1.306 ms
```

1. **When was `thmredteam.com` created (registered)? (YYYY-MM-DD)**

   ans: **2021-09-24** we will get this answer with the command

$ **whois thmredteam.com**

2. **To how many IPv4 addresses does `clinic.thmredteam.com` resolve?**

ans: **2**

command used to get the answer was

$ **nslookup clinic.thmredteam.com**

3. **To how many IPv6 addresses does `clinic.thmredteam.com` resolve?**

ans: **2**

command used to get the answer was

$ **nslookup clinic.thmredteam.com**

Task - 4

Advanced Searching

Symbol / Syntax	Function
`"search phrase"`	Find results with exact search phrase
`OSINT filetype:pdf`	Find files of type `PDF` related to a certain term.
`salary site:blog.tryhackme.com`	Limit search results to a specific site.
`pentest -site:example.com`	Exclude a specific site from results
`walkthrough intitle:TryHackMe`	Find pages with a specific term in the page title.
`challenge inurl:tryhackme`	Find pages with a specific term in the page URL.

Combining advanced Google searches with specific terms, documents containing sensitive information or vulnerable web servers can be found. Websites such as Google Hacking Database (GHDB) collect such search terms and are publicly available.

Let's take a look at some of the GHDB queries:

- **Footholds**Consider GHDB-ID: 6364 as it uses the query `intitle:"index of" "nginx.log"` to discover Nginx logs and might reveal server misconfigurations that can be exploited.
- **Files Containing Usernames**For example, GHDB-ID: 7047 uses the search term `intitle:"index of" "contacts.txt"` to discover files that leak juicy information.
- **Sensitive Directories**For example, consider GHDB-ID: 6768, which uses the search term `inurl:/certs/server.key` to find out if a private RSA key is exposed.
- **Web Server Detection**Consider GHDB-ID: 6876, which detects GlassFish Server information using the query `intitle:"GlassFish Server - Server Running"`.
- **Vulnerable Files**For example, we can try to locate PHP files using the query `intitle:"index of" "*.php"`, as provided by GHDB-ID: 7786.
- **Vulnerable Servers**For instance, to discover SolarWinds Orion web consoles, GHDB-ID: 6728 uses the query `intext:"user name" intext:"orion core" -solarwinds.com`.
- **Error Messages**Plenty of useful information can be extracted from error messages. One example is GHDB-ID: 5963, which uses the query `intitle:"index of" errors.log` to find log files related to errors.

1. **How would you search using Google for `xls` indexed for http://clinic.thmredteam.com?**

ans: **filetype:xls site:clinic.thmredteam.com**

2. **How would you search using Google for files with the word `passwords` for http://clinic.thmredteam.com?**

ans: **passwords site:clinic.thmredteam.com**

Task - 5

Advanced Searching

whois and DNS related

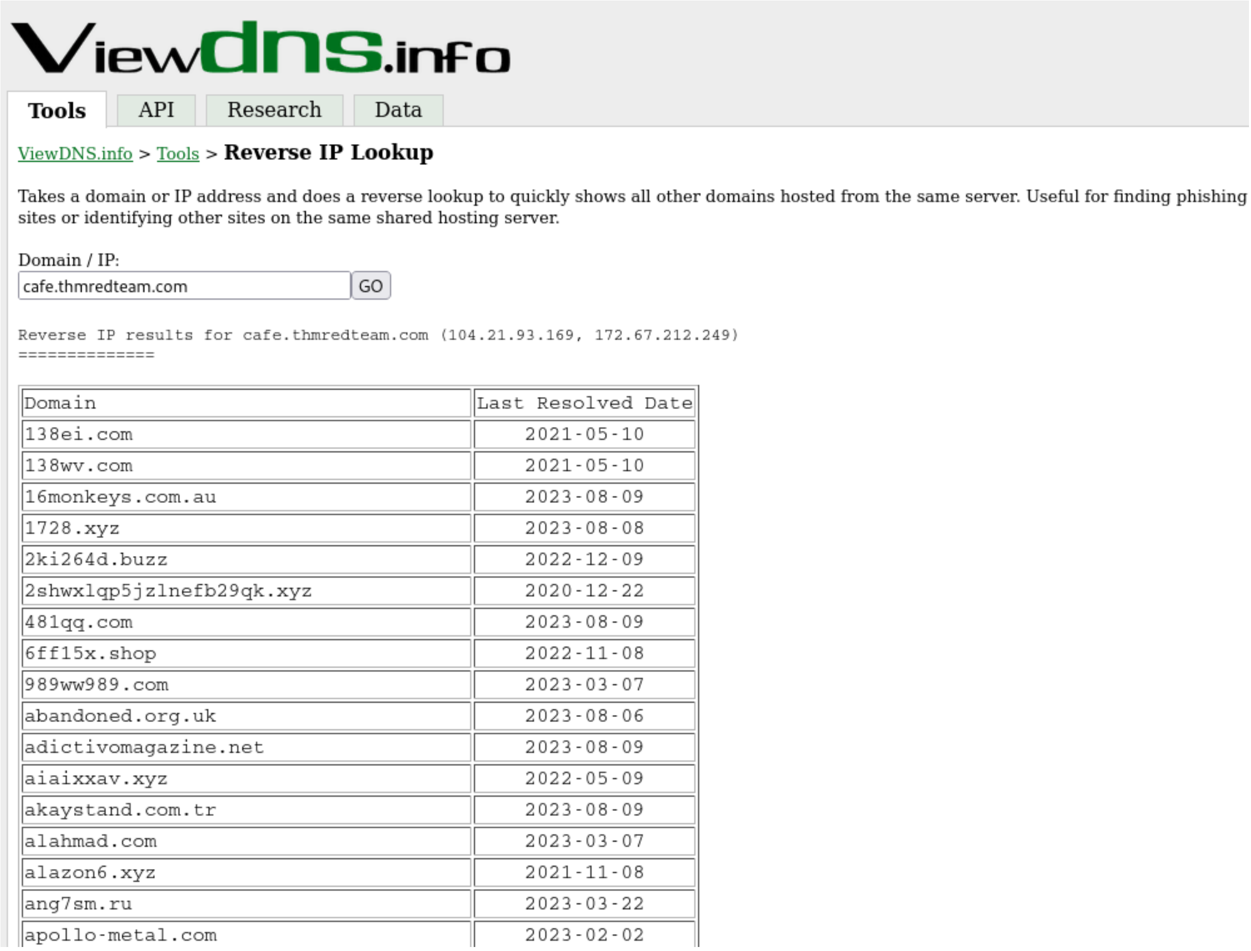
Beyond the standard WHOIS and DNS query tools that we covered in Task 3, there are third parties that offer paid services for historical WHOIS data. One example is WHOIS history, which provides a history of WHOIS data and can come in handy if the domain registrant didn't use WHOIS privacy when they registered the domain.

There are a handful of websites that offer advanced DNS services that are free to use. Some of these websites offer rich functionality and could have a complete room dedicated to exploring one domain.

- ViewDNS.info
- Threat Intelligence Platform

ViewDNS.info

ViewDNS.info offers *Reverse IP Lookup*. Initially, each web server would use one or more IP addresses; however, today, it is common to come across shared hosting servers. With shared hosting, one IP address is shared among many different web servers with different domain names.



ViewDNS.info > Tools > **Reverse IP Lookup**

Takes a domain or IP address and does a reverse lookup to quickly shows all other domains hosted from the same server. Useful for finding phishing sites or identifying other sites on the same shared hosting server.

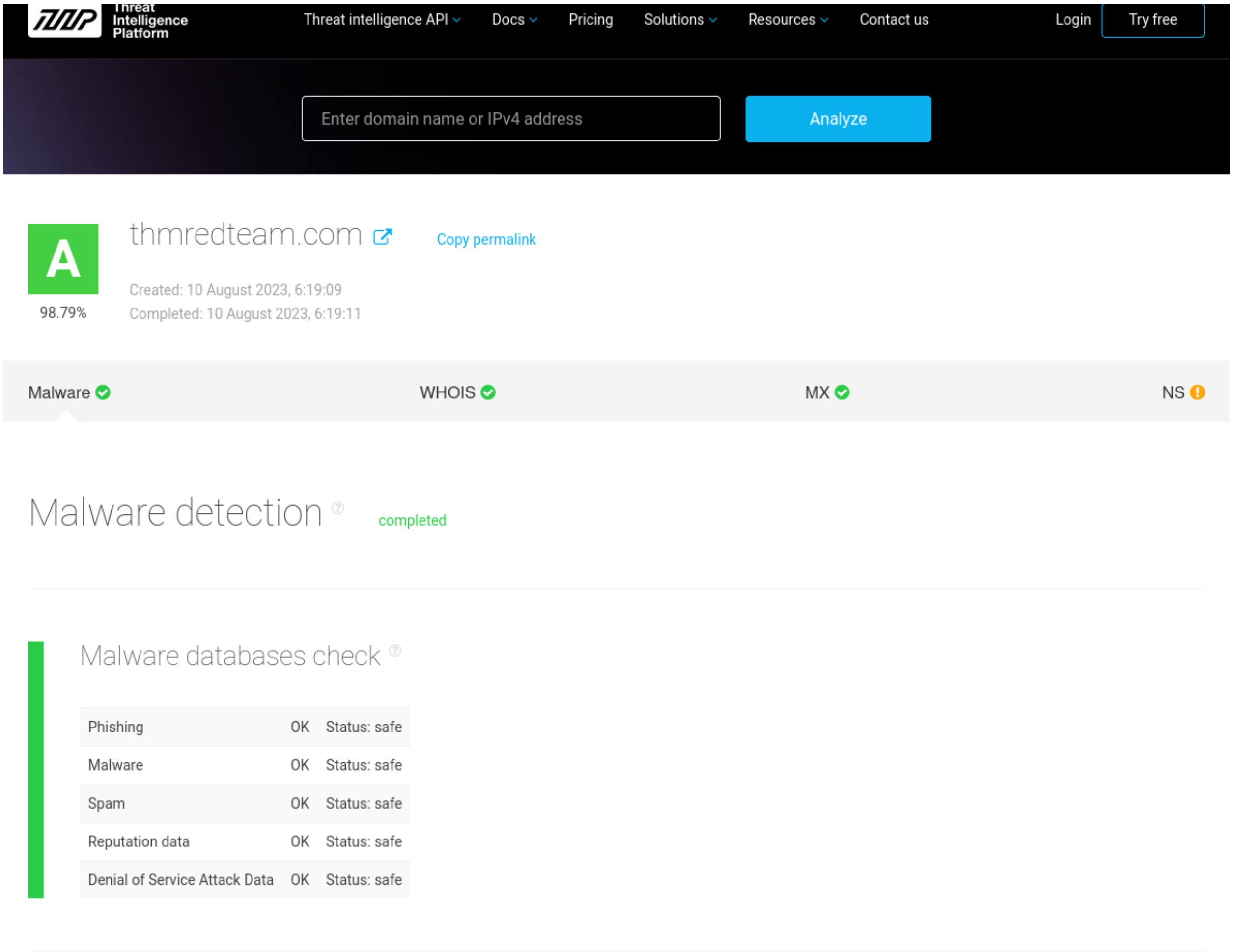
Domain / IP: cafe.thmredteam.com

```
Reverse IP results for cafe.thmredteam.com (104.21.93.169, 172.67.212.249)
==============
```

Domain	Last Resolved Date
138ei.com	2021-05-10
138wv.com	2021-05-10
16monkeys.com.au	2023-08-09
1728.xyz	2023-08-08
2ki264d.buzz	2022-12-09
2shwxlqp5jzlnefb29qk.xyz	2020-12-22
481qq.com	2023-08-09
6ff15x.shop	2022-11-08
989ww989.com	2023-03-07
abandoned.org.uk	2023-08-06
adictivomagazine.net	2023-08-09
aiaixxav.xyz	2022-05-09
akaystand.com.tr	2023-08-09
alahmad.com	2023-03-07
alazon6.xyz	2021-11-08
ang7sm.ru	2023-03-22
apollo-metal.com	2023-02-02

Threat Intelligence Platform

Threat Intelligence Platform requires you to provide a domain name or an IP address, and it will launch a series of tests from malware checks to WHOIS and DNS queries. The WHOIS and DNS results are similar to the results we would get using `whois` and `dig`, but Threat Intelligence Platform presents them in a more readable and visually appealing way. There is extra information that we get with our report. For instance, after we look up `thmredteam.com`



thmredteam.com

98.79%

Created: 10 August 2023, 6:19:09
Completed: 10 August 2023, 6:19:11

Malware detection completed

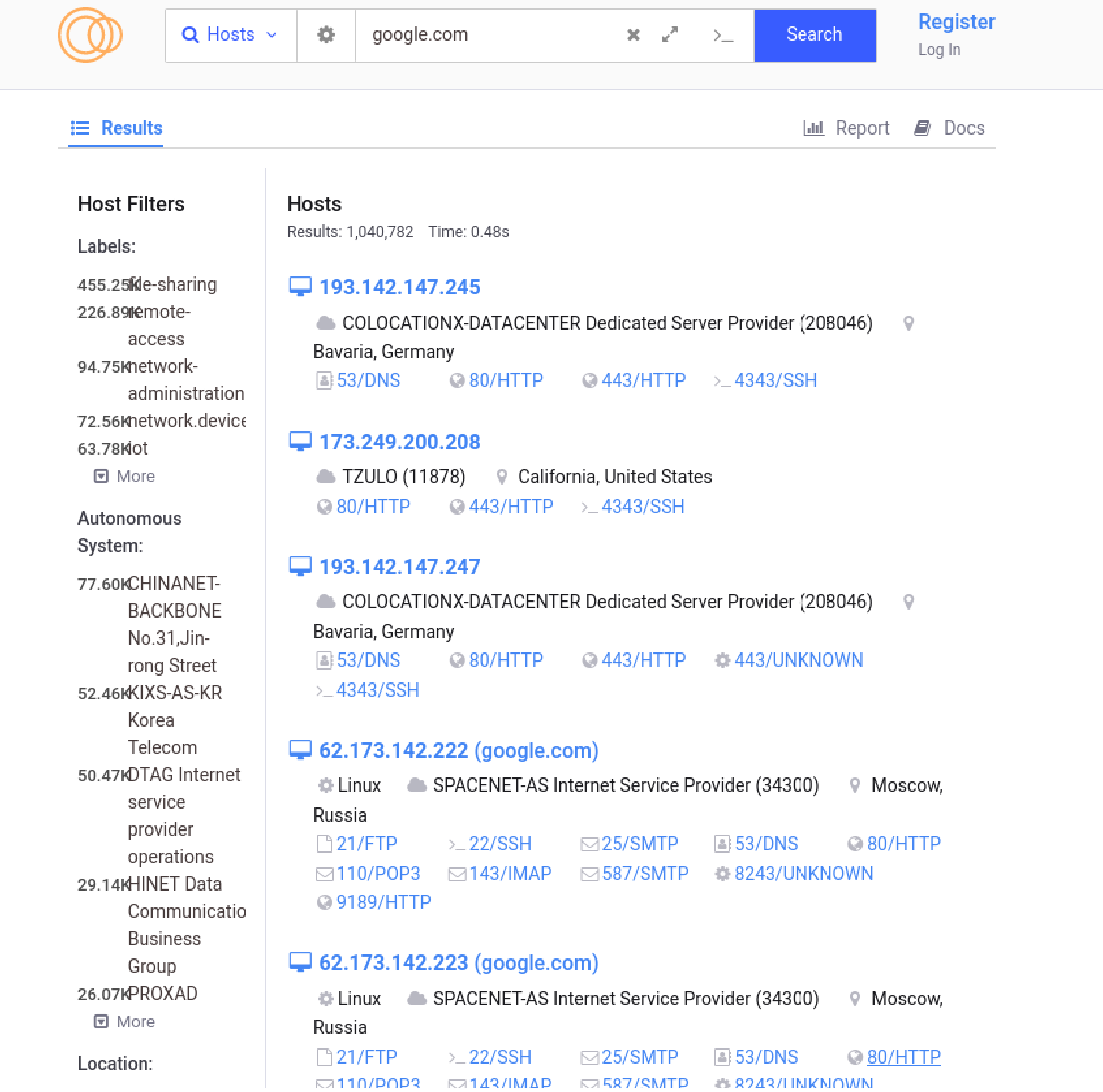
Malware databases check

Phishing	OK	Status: safe
Malware	OK	Status: safe
Spam	OK	Status: safe
Reputation data	OK	Status: safe
Denial of Service Attack Data	OK	Status: safe

Specialized Search Engines

Censys

Censys Search can provide a lot of information about IP addresses and domains.



Host Filters

Labels:

455.25K file-sharing
226.89K remote-access
94.75K network-administration
72.56K network.device
63.78K iot
More

Autonomous System:

77.60K CHINANET-BACKBONE No.31,Jin-rong Street
52.46K KIXS-AS-KR Korea Telecom
50.47K DTAG Internet service provider operations
29.14K HINET Data Communicatio Business Group
26.07K PROXAD
More

Location:

Hosts

Results: 1,040,782   Time: 0.48s

193.142.147.245
COLOCATIONX-DATACENTER Dedicated Server Provider (208046)   Bavaria, Germany
53/DNS   80/HTTP   443/HTTP   4343/SSH

173.249.200.208
TZULO (11878)   California, United States
80/HTTP   443/HTTP   4343/SSH

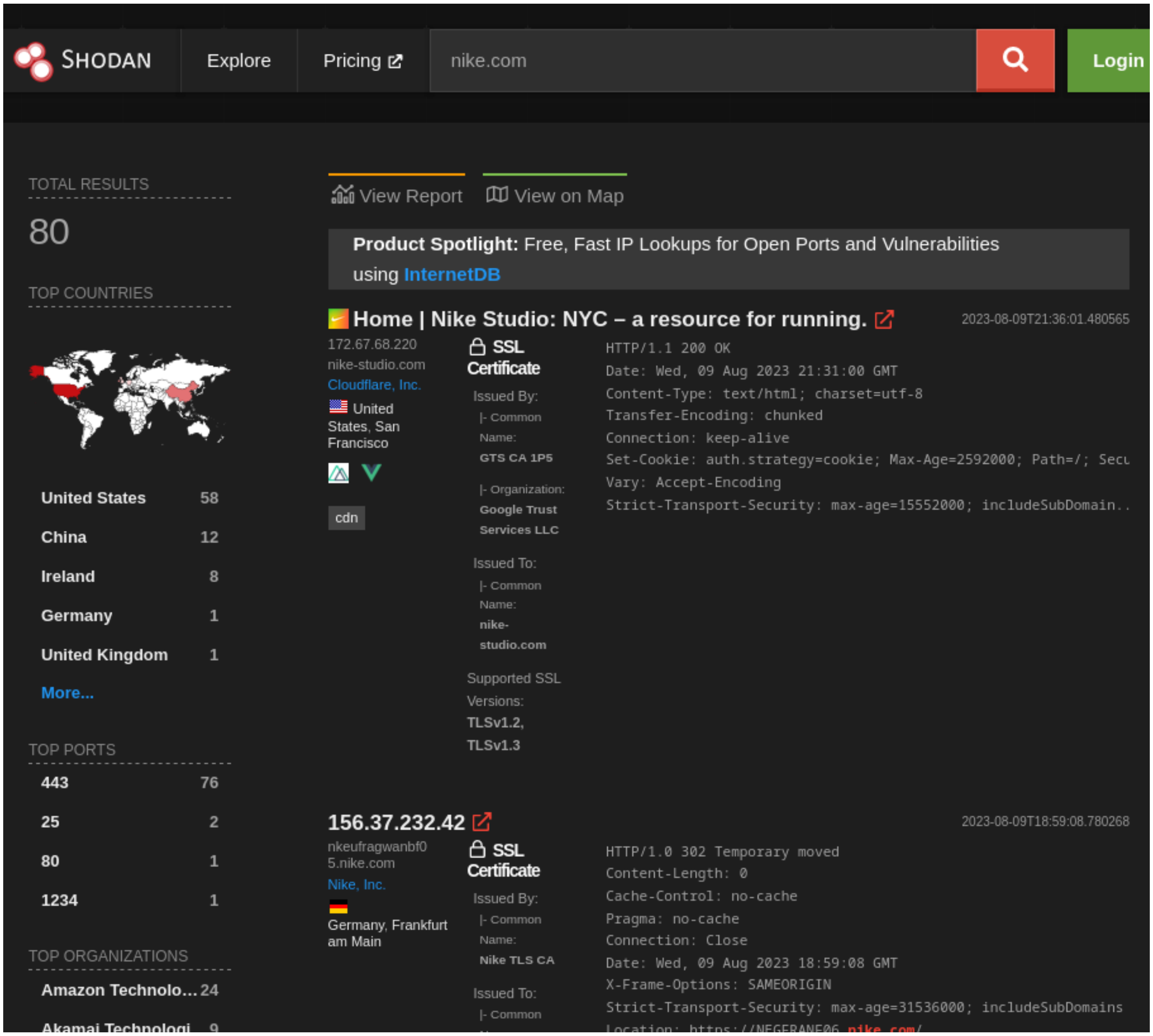
193.142.147.247
COLOCATIONX-DATACENTER Dedicated Server Provider (208046)   Bavaria, Germany
53/DNS   80/HTTP   443/HTTP   443/UNKNOWN   4343/SSH

62.173.142.222 (google.com)
Linux   SPACENET-AS Internet Service Provider (34300)   Moscow, Russia
21/FTP   22/SSH   25/SMTP   53/DNS   80/HTTP   110/POP3   143/IMAP   587/SMTP   8243/UNKNOWN   9189/HTTP

62.173.142.223 (google.com)
Linux   SPACENET-AS Internet Service Provider (34300)   Moscow, Russia
21/FTP   22/SSH   25/SMTP   53/DNS   80/HTTP   110/POP3   143/IMAP   587/SMTP   8243/UNKNOWN

Shodan

To use Shodan from the command-line properly, you need to create an account with Shodan, then configure `shodan` to use your API key using the command, `shodan init API_KEY`.



TOTAL RESULTS

80

TOP COUNTRIES

United States	58
China	12
Ireland	8
Germany	1
United Kingdom	1
More...	

TOP PORTS

443	76
25	2
80	1
1234	1

TOP ORGANIZATIONS

Amazon Technolo...	24
Akamai Technologi...	9

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

Home | Nike Studio: NYC – a resource for running. 2023-08-09T21:36:01.480565

172.67.68.220
nike-studio.com
Cloudflare, Inc.
United States, San Francisco
cdn

SSL Certificate
Issued By:
|- Common Name: GTS CA 1P5
|- Organization: Google Trust Services LLC
Issued To:
|- Common Name: nike-studio.com
Supported SSL Versions: TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Wed, 09 Aug 2023 21:31:00 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: auth.strategy=cookie; Max-Age=2592000; Path=/; Secu
Vary: Accept-Encoding
Strict-Transport-Security: max-age=15552000; includeSubDomain..
```

156.37.232.42 2023-08-09T18:59:08.780268

nkeufragwanbf05.nike.com
Nike, Inc.
Germany, Frankfurt am Main

SSL Certificate
Issued By:
|- Common Name: Nike TLS CA
Issued To:
|- Common

```
HTTP/1.0 302 Temporary moved
Content-Length: 0
Cache-Control: no-cache
Pragma: no-cache
Connection: Close
Date: Wed, 09 Aug 2023 18:59:08 GMT
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
Location: https://NEGEFRANE06.nike.com/
```

1. **What is the `shodan` command to get your Internet-facing IP address?**

ans: **shodan myip**

Task - 6

Recon-ng

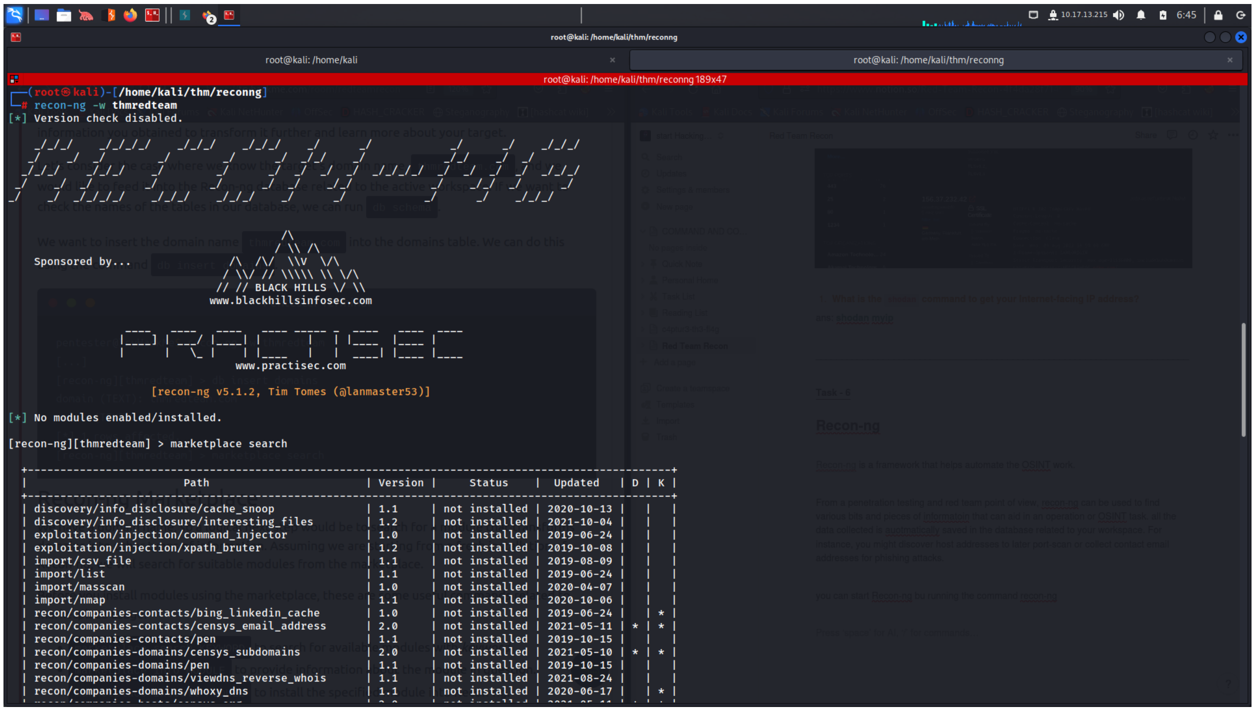
Recon-ng is a framework that helps automate the OSINT work.

From a penetration testing and red team point of view, recon-ng can be used to find various bits and pieces of informatoin that can aid in an operation or OSINT task. all the data collected is auotmatically saved in the database related to your workspace. For instance, you might discover host addresses to later port-scan or collect contact email addresses for phishing attacks.

you can start Recon-ng bu running the command recon-ng

`$ recon-ng -w thmredteam`

`[recon-ng][thmredteam] > marketplace search`



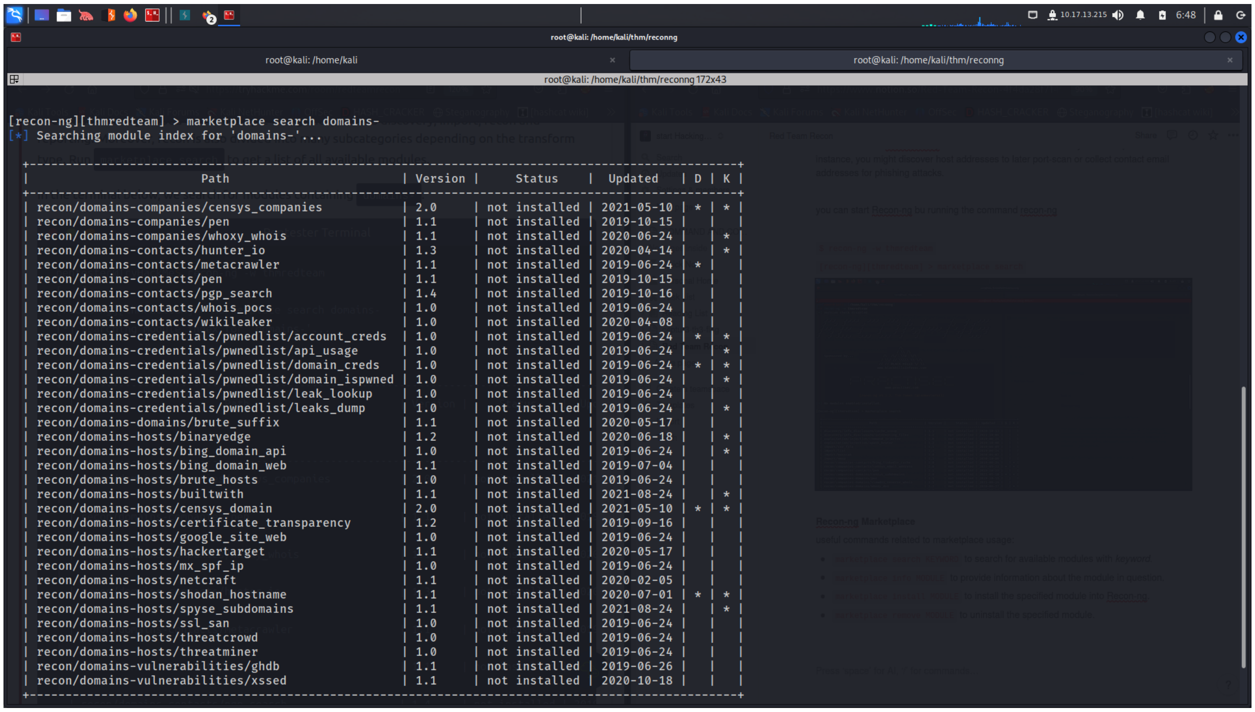
```
┌──(root㉿kali)-[/home/kali/thm/reconng]
└─# recon-ng -w thmredteam
[*] Version check disabled.

                                     /\
                                    / \\ /\
    Sponsored by...          /\  /\/  \\V  \/\
                            / \\/ // \\\\\ \\ \/\
                           // // BLACK HILLS \/ \\
                          www.blackhillsinfosec.com

                              www.practisec.com

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

[*] No modules enabled/installed.

[recon-ng][thmredteam] > 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/nmap                                         | 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       | 2.0     | not installed | 2021-05-11 | * | * |
  | recon/companies-contacts/pen                        | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/companies-domains/censys_subdomains           | 2.0     | not installed | 2021-05-10 | * | * |
  | 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-domains/whoxy_dns                   | 1.1     | not installed | 2020-06-17 |   | * |
```

Recon-ng Marketplace

useful commands related to marketplace usage:

- `marketplace search KEYWORD` to search for available modules with *keyword*.
- `marketplace info MODULE` to provide information about the module in question.
- `marketplace install MODULE` to install the specified module into Recon-ng.
- `marketplace remove MODULE` to uninstall the specified module.

```
$ recon-ng -w thmredteam
[recon-ng][thmredteam] > marketplace search domains-
```



```
[recon-ng][thmredteam] > marketplace search domains-
[*] Searching module index for 'domains-'...

  +---------------------------------------------------------------------------------------------------+
  |                        Path                        | Version |     Status    |  Updated   | D | K |
  +---------------------------------------------------------------------------------------------------+
  | recon/domains-companies/censys_companies           | 2.0     | not installed | 2021-05-10 | * | * |
  | 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-credentials/pwnedlist/account_creds  | 1.0     | not installed | 2019-06-24 | * | * |
  | recon/domains-credentials/pwnedlist/api_usage      | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/domains-credentials/pwnedlist/domain_creds   | 1.0     | not installed | 2019-06-24 | * | * |
  | recon/domains-credentials/pwnedlist/domain_ispwned | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/domains-credentials/pwnedlist/leak_lookup    | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-credentials/pwnedlist/leaks_dump     | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/domains-domains/brute_suffix                 | 1.1     | not installed | 2020-05-17 |   |   |
  | recon/domains-hosts/binaryedge                     | 1.2     | not installed | 2020-06-18 |   | * |
  | recon/domains-hosts/bing_domain_api                | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/domains-hosts/bing_domain_web                | 1.1     | not installed | 2019-07-04 |   |   |
  | recon/domains-hosts/brute_hosts                    | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/builtwith                      | 1.1     | not installed | 2021-08-24 |   | * |
  | recon/domains-hosts/censys_domain                  | 2.0     | not installed | 2021-05-10 | * | * |
  | recon/domains-hosts/certificate_transparency       | 1.2     | not installed | 2019-09-16 |   |   |
  | recon/domains-hosts/google_site_web                | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/hackertarget                   | 1.1     | not installed | 2020-05-17 |   |   |
  | recon/domains-hosts/mx_spf_ip                      | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/netcraft                       | 1.1     | not installed | 2020-02-05 |   |   |
  | recon/domains-hosts/shodan_hostname                | 1.1     | not installed | 2020-07-01 | * | * |
  | recon/domains-hosts/spyse_subdomains               | 1.1     | not installed | 2021-08-24 |   | * |
  | recon/domains-hosts/ssl_san                        | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/threatcrowd                    | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/threatminer                    | 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 |   |   |
  +---------------------------------------------------------------------------------------------------+
```

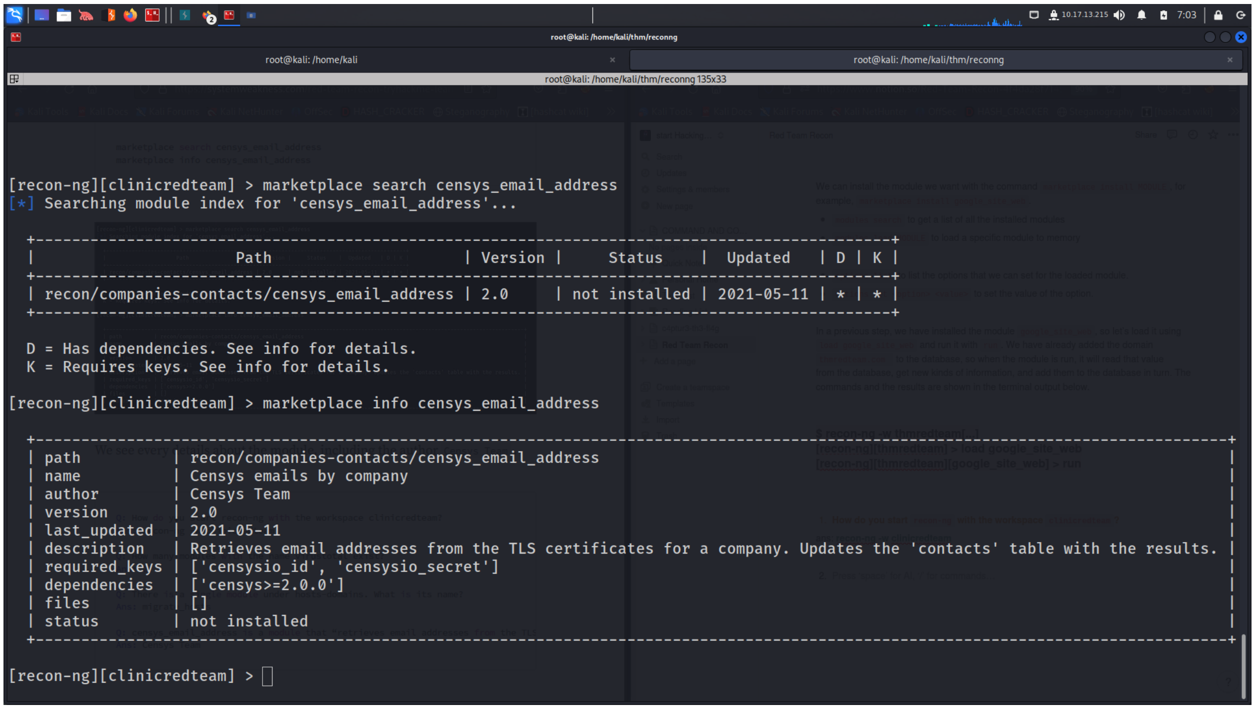
We can install the module we want with the command `marketplace install MODULE`, for example, `marketplace install google_site_web`.

- `modules search` to get a list of all the installed modules
- `modules load MODULE` to load a specific module to memory

- `options list` to list the options that we can set for the loaded module.
- `options set <option> <value>` to set the value of the option.

In a previous step, we have installed the module `google_site_web`, so let's load it using `load google_site_web` and run it with `run`. We have already added the domain `thmredteam.com` to the database, so when the module is run, it will read that value
from the database, get new kinds of information, and add them to the database in turn.
The commands and the results are shown in the terminal output below.

$ recon-ng -w thmredteam[...]
[recon-ng][thmredteam] > load google_site_web
[recon-ng][thmredteam][google_site_web] > run



```
[recon-ng][clinicredteam] > marketplace search censys_email_address
[*] Searching module index for 'censys_email_address'...

  +----------------------------------------------------------------------------------------------+
  |                     Path                      | Version |    Status     |  Updated   | D | K |
  +----------------------------------------------------------------------------------------------+
  | recon/companies-contacts/censys_email_address | 2.0     | not installed | 2021-05-11 | * | * |
  +----------------------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][clinicredteam] > marketplace info censys_email_address

  +-----------------------------------------------------------------------------------------------------------------------------------+
  | path          | recon/companies-contacts/censys_email_address                                                                     |
  | name          | Censys emails by company                                                                                          |
  | author        | Censys Team                                                                                                       |
  | version       | 2.0                                                                                                               |
  | last_updated  | 2021-05-11                                                                                                        |
  | description   | Retrieves email addresses from the TLS certificates for a company. Updates the 'contacts' table with the results. |
  | required_keys | ['censysio_id', 'censysio_secret']                                                                                |
  | dependencies  | ['censys>=2.0.0']                                                                                                 |
  | files         | []                                                                                                                |
  | status        | not installed                                                                                                     |
  +-----------------------------------------------------------------------------------------------------------------------------------+

[recon-ng][clinicredteam] > 
```

1. **How do you start `recon-ng` with the workspace `clinicredteam`?**

ans: **recon-ng -w clinicredteam**

2. **There is a single module under `hosts-domains`. What is its name?**

ans: **2**

3. **There is a single module under `hosts-domains`. What is its name?**

ans: **migrate_hosts**

4. **`censys_email_address` is a module that “retrieves email addresses from the TLS certificates for a company.” Who is the author?**

ans: **censys team**

Task - 7

Maltego

Maltego is is an application that blends ming-mapping with OSINT. in general, you would start with a domain name, company name, persons name, email address, etc. then you can let this piece of information go through various transforms.

1. **What is the name of the transform that queries NIST’s National Vulnerability Database?**

ans: **nist nvd**

2. **What is the name of the project that offers a transform based on ATT&CK?**

ans: **misp project**