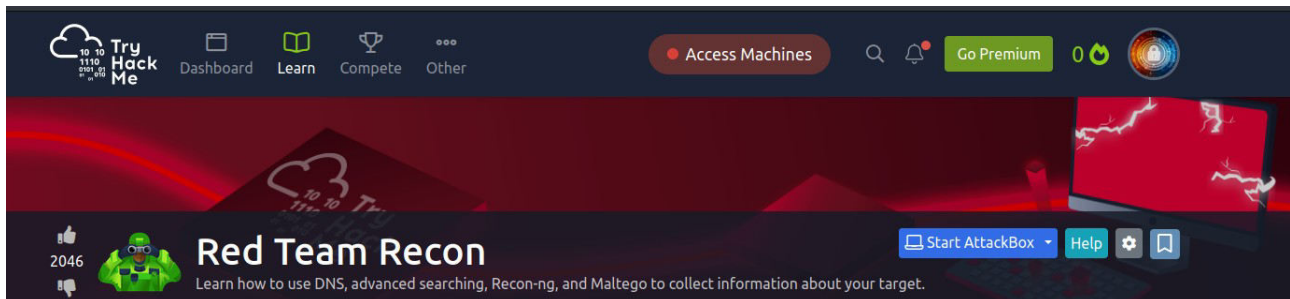




**Eric Mwenda**

**RED TEAM RECON**

<https://tryhackme.com/p/Ericm>



### **Introduction:**

In this room we start with a quote written by Miyamoto Musashi in his book, A Book of Five Rings, he states “Know your enemy, know his sword” he also continues to state: “You win battles by knowing the enemy’s timing, and using a timing which the enemy does not expect.”

This quote was written when battles were fought using swords and spears but it also applies to the cyber security space where attacks are launched via keyboards and crafted packets. The more you know about your target’s infrastructure and personnel, the better you can orchestrate your attacks.

I get also to understand what to expect from the red team operation. In my understanding red operations may begin from a very limited knowledge where you only know your targets company name and its upon you to gather all available information that can assist in your operations.

This information may include:- Discovering subdomains related to our target company, gathering publicly available information about a host and IP addresses, finding email addresses related to the target, discovering login credentials and leaked passwords and locating leaked documents and spreadsheets.

This is what we call in other words reconnaissance. This operation should also be as quiet as possible to avoid alerting the other party which may take precaution measures hindering thereby your operations.

This section also gives an explanation of Reconnaissance (Recon) as a preliminary survey or observation to a target, without alerting them of your activities.

## **Taxonomy of Reconnaissance.**

### **Reconnaissance can be classified into two:-**

1. Passive Reconnaissance.
2. Active Reconnaissance.

**Passive Reconnaissance** is carried out a survey without interacting with the target, you just observe the target operations or use third party information that is publicly available like Open Source Intelligence (OSINT).

OSINT can be used to gather information such as target's publicly available social media profile.

Example information that we might collect includes domain names, IP address blocks, email addresses, employee names, and job posts.

This is quite a lot of information in real sense, especially where you know your target's IP address information.

**Active Reconnaissance** require you to interact with the target, whereby for example the attacker can send requests and packets and observing if and how it responds. The responses collected or lack of responses will enable the attacker to expand on the picture developed on the first stage of Passive Recon.

This section gives a good example for Active Reconnaissance as use of the **Nmap** tool to scan targets subnets and live hosts. Nmap information that the attacker wishes to know may include defining live hosts, running servers, listening services, and version numbers.

Active Recon continues to be classified into 2 which is:-

1. External Reconnaissance – This is conducted on the external target's network, this are the externally facing assets assessable from the internet. A good tool to perform this is **Nikto**.
2. Internal Reconnaissance – This Recon is conducted within the target's company network. This means the pentester or attacker may be located physically inside the company building. A good example for this would be using **Nessus** to scan the internal network using one of the target's computers.

### **Built in tools**

In this section we focus on the following tools

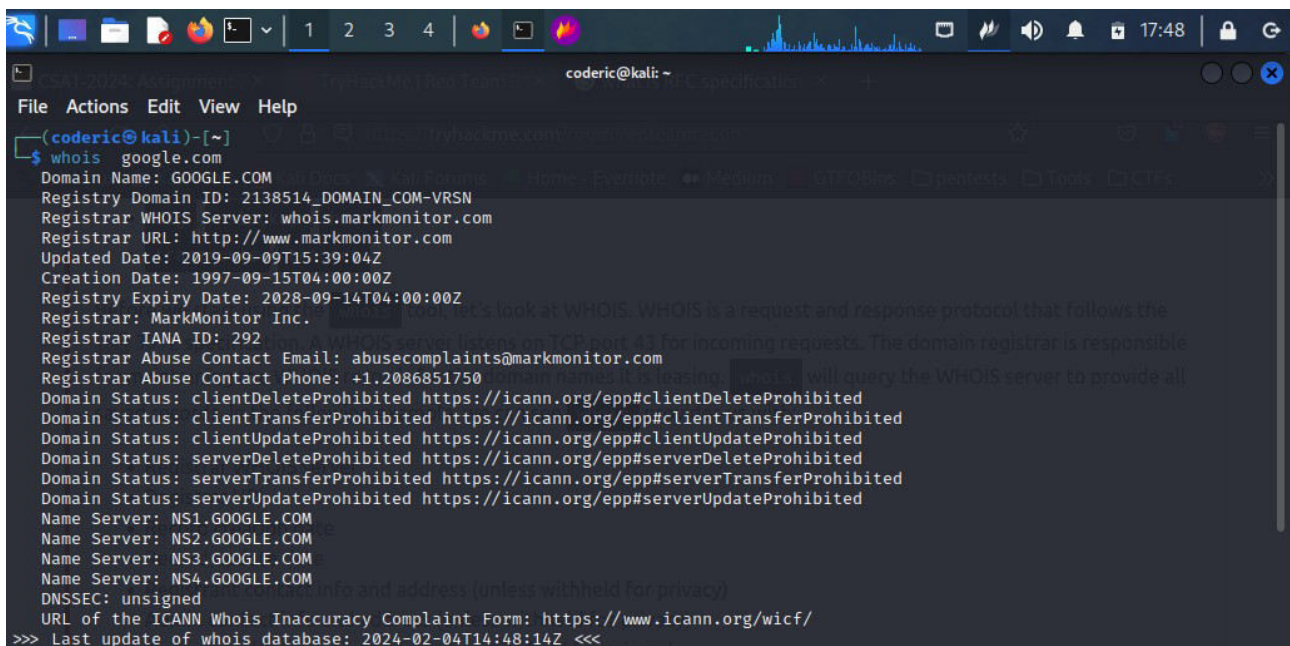
- **whois**
- **dig, nslookup, host**
- **traceroute/tracert**

First we begin by learning about WHOIS tool. TRYHACKME explains this tool as follows “WHOIS is a request and response protocol that follows the RFC 3912 specification. A WHOIS server listens on TCP port 43 for incoming requests.”

The domain registrar is the one responsible for maintaining updated records about the domain names it is leasing.

**A Request for Comments (RFC)** is a formal document from the Internet Engineering Task Force (IETF) that contains specifications and organizational notes about topics related to the internet and computer networking, such as routing, addressing and transport technologies.

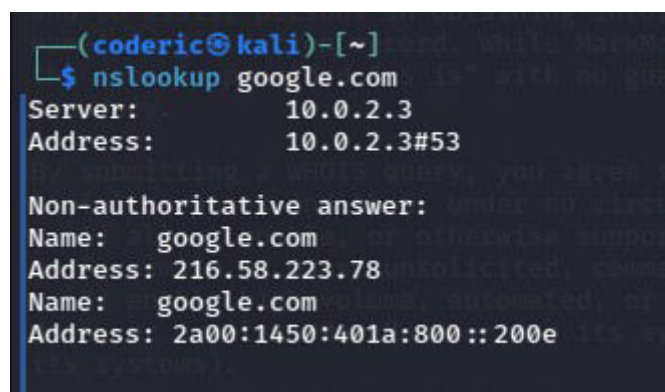
Next we look at how to find domain information using WHOIS tool, I try it out by checking up on **google.com** site. Command used:- **whois google.com**



```
(coderic@kali)-[~]
$ whois google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-02-04T14:48:14Z <<<
```

From this search result a lot of information is displayed, which evidently can be of good use to an attacker or a pentester.

We then proceeded to look at **nslookup** tool which is mostly common on Unix-like systems. This tool also is used to perform DNS queries.



```
(coderic@kali)-[~]
$ nslookup google.com
Server:      10.0.2.3
Address:     10.0.2.3#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.223.78
Name:   google.com
Address: 2a00:1450:401a:800::200e
```

The **nslookup** query uses the default DNS server to get the A and AAAA records related to our domain.

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

An example for this was **DNS server: dig @1.1.1.1 tryhackme.com.**

```
(coderic@kali)-[~]
$ dig @1.1.1.1 tryhackme.com

; <<>> DiG 9.18.12-1-Debian <<>> @1.1.1.1 tryhackme.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 16584
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
tryhackme.com.                300     IN      A      104.22.54.228
tryhackme.com.                300     IN      A      172.67.27.10
tryhackme.com.                300     IN      A      104.22.55.228

;; Query time: 84 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Sun Feb 04 18:01:40 EAT 2024
;; MSG SIZE rcvd: 90
```

We then proceeded to look at **host** which is another useful alternative for querying DNS servers for DNS records.

```
(coderic@kali)-[~]
$ host google.com
google.com has address 172.217.170.174
google.com has IPv6 address 2a00:1450:401a:804::200e
google.com mail is handled by 10 smtp.google.com.

(coderic@kali)-[~]
```

Our last tool to check was **traceroute** for Unix-like systems and **tracert** for Windows systems.

Traceroute traces the route taken by the packets from our system to the target host.

From this task I learnt that whenever I see the symbol “\*” in the traceroute results they represent those IP addresses for the routers that do not respond to the packets sent by **traceroute**

```
(coderic@kali)-[~]
$ traceroute google.com
traceroute to google.com (172.217.170.174), 30 hops max, 60 byte packets
 1 10.0.2.2 (10.0.2.2) 0.314 ms 0.227 ms 0.570 ms
 2 _gateway (192.168.100.1) 2.685 ms 2.627 ms 2.975 ms
 3 10.9.23.254 (10.9.23.254) 114.760 ms 114.664 ms 114.600 ms
 4 nt-09-v10.vggconnect.com (102.219.208.9) 12.052 ms 11.997 ms 11.941 ms
 5 10.219.213.101 (10.219.213.101) 19.585 ms 19.421 ms 19.373 ms
 6 10.219.213.177 (10.219.213.177) 114.108 ms 60.876 ms 57.674 ms
 7 10.219.213.133 (10.219.213.133) 10.582 ms 13.263 ms 13.137 ms
 8 10.219.213.122 (10.219.213.122) 19.493 ms 19.680 ms 19.218 ms
 9 196.60.66.13 (196.60.66.13) 34.092 ms 34.009 ms 33.927 ms
10 * * *
11 mba01s09-in-f14.1e100.net (172.217.170.174) 28.156 ms 18.096 ms 17.253.53.49 (172.253.53.49) 17.881 ms

(coderic@kali)-[~]
```

From this section I learnt that I can rely on:-

- **whois** to query the WHOIS database
- **nslookup, dig, or host** to query DNS servers

Querying either of this (WHOIS database and DNS servers) does not generate any suspicious traffic.

### Answer the questions below

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

**ANS: 2021-09-24**

```
(coderic@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: 2023-09-30T23:11:17Z
Creation Date: 2021-09-24T14:04:16Z
Registry Expiry Date: 2024-09-24T14:04:16Z
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
```

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

**ANS: 2**

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

**ANS: 2**

```
(coderic@kali)-[~]
$ host clinic.thmredteam.com
clinic.thmredteam.com has address 104.21.93.169
clinic.thmredteam.com has address 172.67.212.249
clinic.thmredteam.com has IPv6 address 2606:4700:3034::6815:5da9
clinic.thmredteam.com has IPv6 address 2606:4700:3034::ac43:d4f9
```

### Advance Searching.

In this section we covered on how the search engine can be an efficient tool to search for useful information/materials and how to use them to get the required information excluding other searches that may arise.

Some of the search engines discussed were **Google Refine Web Searches, DuckDuckGo Search Syntax, and Bing Advanced Search Options.**



By Combining advanced Google searches with specific terms, documents containing sensitive information or vulnerable web servers can be found.

I got to learn although most of this information is publicly available one should not pursue to access any files outside the scope of your legal agreement.

In this section, we explored two additional sources that can provide valuable information without interacting with our target:

- Social Media.

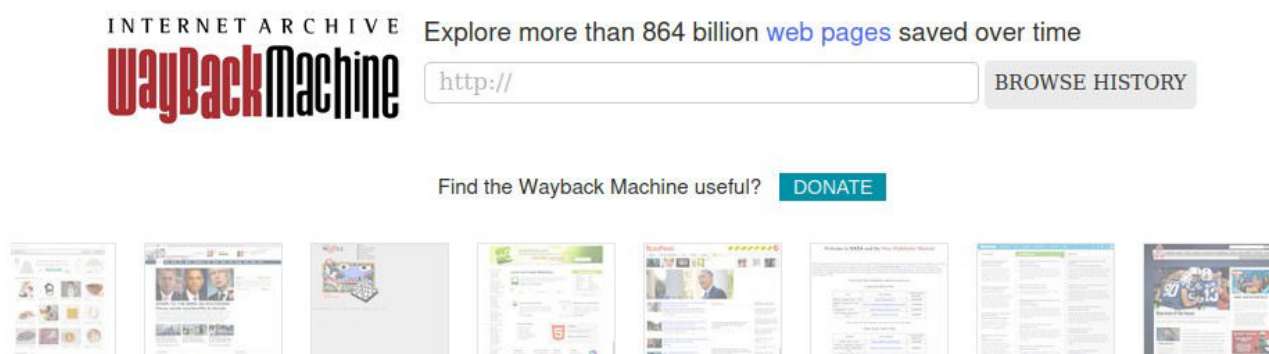
- Job ads.

**Social media** is one of the very popular website that is not only used on personal settings but also used by co-operations. This platforms can reveal tons of information about the target. This is especially true as many users tend to overshare details about themselves and their work.

Social media websites make it easy to collect the names of a given company's employees; moreover, in certain instances, you might learn specific pieces of information that can reveal answers to password recovery questions or gain ideas to include in a targeted wordlist. Posts from technical staff might reveal details about a company's systems and vendors.

**Job Ads (Job Advertisements)** can also tell a lot of information, Some of this information may reveal names and email addresses, job posts for technical positions could give insight into the target company's systems and infrastructure.

Another tool was introduced that is use of **Wayback Machine** to retrieve previous versions of a job opening page on your client's site.



**Answer the questions below**

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

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

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

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

### Answer the questions below

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

Correct Answer

Hint

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

Correct Answer

## Specialized Search Engines.

In this section we look at third parties that offer paid services for historical WHOIS data.

For WHOIS data we have a tool called **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.

We also looked at some tools that can give advanced DNS services that are free to use.

Some of these websites are:-

- **ViewDNS.info**

- **Threat Intelligence Platform**

**ViewDNS.info** offers Reverse IP Lookup. With the ability that has evolved in the recent days, 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. With reverse IP lookup, starting from a domain name or an IP address, you can find the other domain names using a specific IP address(es).

Domain	Last Resolved Date
138ei.com	2021-05-10
138wv.com	2021-05-10
16monkeys.com.au	2024-02-03
2ki264d.buzz	2022-12-09
2shwx1qp5jz1nefb29qk.xyz	2020-12-22
481qq.com	2024-02-03
69tz.cn	2024-02-02
6ff15x.shop	2022-11-08
829490.com	2024-02-03

## Threat Intelligence Platform

This was the most amazing tool that I came across, it offers a wide range of information, all in one search.

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.

The screenshot displays the Threat Intelligence Platform interface. At the top, there's a navigation bar with the platform's logo and various menu items like 'Threat intelligence API', 'Docs', 'Pricing', 'Solutions', 'Resources', and 'Contact us'. Below this, a search bar prompts the user to 'Enter domain name or IPv4 address' with an 'Analyze' button. The main content area shows a report for 'thmredteam.com'. It includes a green 'A' grade badge, a '99.09%' score, and a 'completed' status. A progress bar at the bottom indicates the status of various checks: 'Malware' (green), 'WHOIS' (green), 'MX' (green), and 'NS' (yellow). The 'Malware detection' section is highlighted, showing a 'completed' status. Below this, a 'Malware databases check' is shown with a green progress bar.

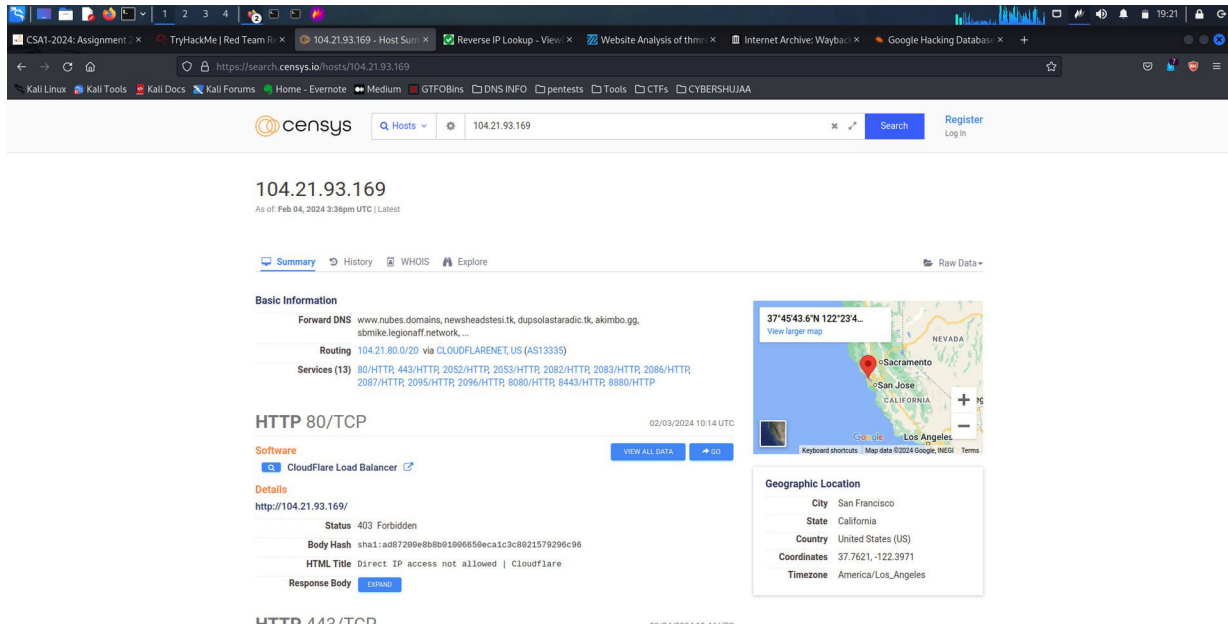


## Specialized Search Engines

The first tool we look at **Censys**.

This tool provides a lot of information about an IP address and domains. Here is an example result of one of the IP address that I came across on the task on the [nslookup.cafe.thmredteam.com](https://nslookup.cafe.thmredteam.com).

**IP: 104.21.93.169**



The screenshot shows the Censys search results for the IP address 104.21.93.169. The page displays various details including Basic Information, HTTP 80/TCP, and Geographic Location. The Basic Information section shows Forward DNS, Routing, and Services. The HTTP 80/TCP section shows Software (CloudFlare Load Balancer) and Details (Status 403 Forbidden, Body Hash, HTML Title, and Response Body). The Geographic Location section shows City (San Francisco), State (California), Country (United States (US)), Coordinates (37.7621, -122.3971), and Timezone (America/Los\_Angeles).

## Shodan

Next task was to use **shodan** on the command line.

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**.

Using shodan host IP\_ADDRESS, we can get the geographical location of the IP address and the open ports, below is an example;

```
pentester@TryHackMe$ shodan host 172.67.212.249

172.67.212.249
City: San Francisco
Country: United States
Organisation: Cloudflare, Inc.
Updated: 2021-11-22T05:55:54.787113
Number of open ports: 5

Ports:
  80/tcp
  443/tcp
  |-- SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2, TLSv1.3
  2086/tcp
  2087/tcp
  8080/tcp
```

## Answer the questions below

What is the shodan command to get your Internet-facing IP address?

ANS: shodan myip

## Recon-ng

**Recon-ng** is a framework that helps to automate OSINT (Open Source Intelligence).

It uses modules from various authors and provides a multitude of functionality. Some modules require keys to work; the key allows the module to query the related online API.

In this section we went a step by step process of creating a new workspace for a project, Inserting the starting information into the database, Searching the marketplace for a module and learn about it before installing, Listing the installed modules and load one and finally Running the loaded module.

## Creating a Workspace

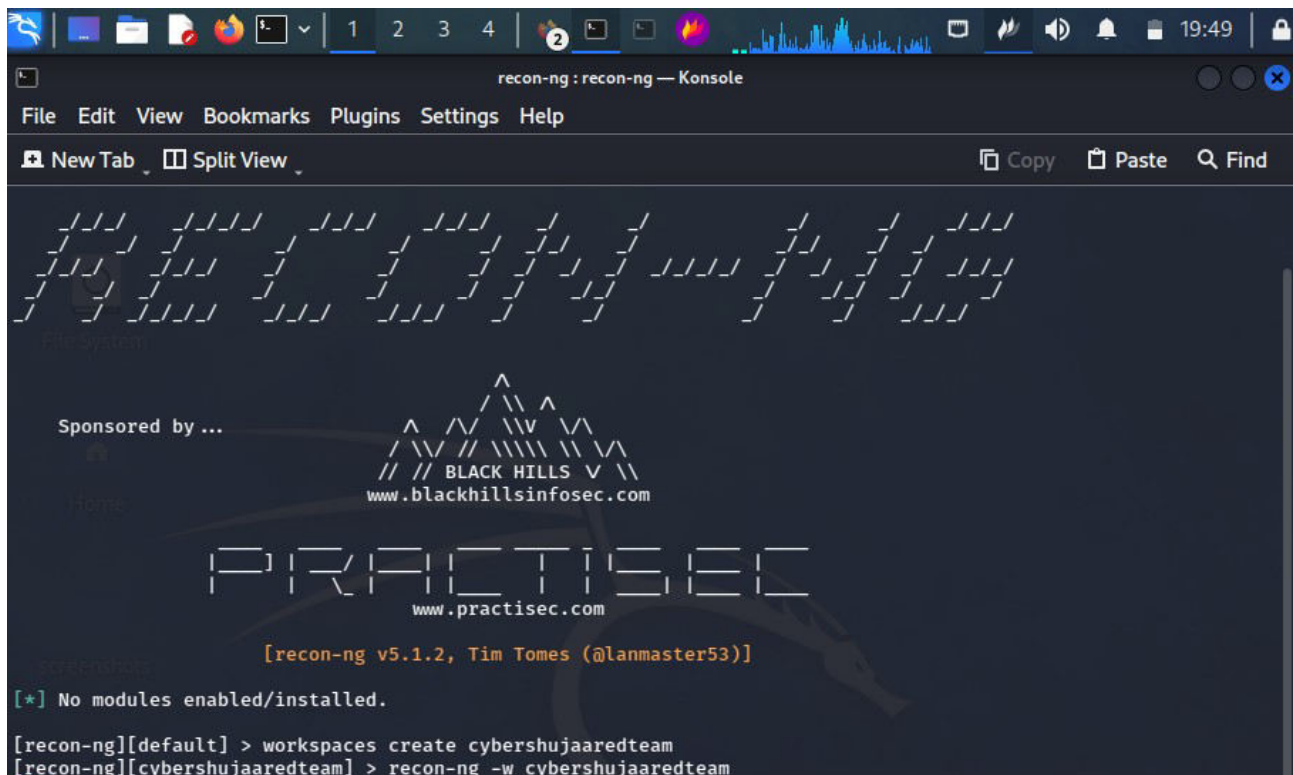
Run workspaces create WORKSPACE\_NAME to create a new workspace for your investigation.

In my case I will create a workspace named:- **cybershujaaredteam**

Command:- **workspaces create cybershujaaredteam**

In the case the workspace is already there we start **recon-ng** on this specific workspace.

Command:- **recon-ng -w cybershujaaredteam**



```
recon-ng : recon-ng — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find
PRAXIS
Sponsored by ...
BLACK HILLS
www.blackhillsinfosec.com
PRACTISE
www.practisec.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installed.
[recon-ng][default] > workspaces create cybershujaaredteam
[recon-ng][cybershujaaredteam] > recon-ng -w cybershujaaredteam
```

## Seeding the Database

Whenever we are carrying out a reconnaissance, we start with one piece of information and transforming it into new pieces of information. For instance, starting the research with a company name and use that to discover the domain name(s), contacts and profiles. After this you use the new information obtained to transform it further and learn more about your target.

In this stage I assume the target's domain name for **cybershujaaredteam** is **thmredteam.com**.

We want to insert the domain name thmredteam.com into the domains table.

To insert a database we run **db insert domains**. Incase we want to check the names of the tables in our database, we can run **db schema**.

Adding the record example.



```
PRATISEC
www.practisec.com

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

[*] No modules enabled/installed.

[recon-ng][cybershujaaredteam] > db insert domains
domain (TEXT): thmredteam.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][cybershujaaredteam] > 
```

## Recon-ng Marketplace

Having already a domain name the next logical step would be to search for a module that transforms domains into other types of information. Assuming we are starting from a fresh installation of Recon-ng, we will search for suitable modules from the marketplace.

Before you install modules using the marketplace, these are some 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.

The modules are grouped under multiple categories, such as discovery, import, recon and reporting. Moreover, recon is also divided into many subcategories depending on the transform type.

We run **marketplace search** to get a list of all available modules.

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

Path	Version	Status	Updated	D	K
discovery/info_disclosure/cache_snoop	1.1	not installed	2020-10-13		
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/companies-hosts/censys_tls_subjects	2.0	not installed	2021-05-11	*	*
recon/contacts-domains/migrate_contacts	1.1	not installed	2020-05-17		
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	*	*

There are a number of results displayed such as domains-contacts, and domains-hosts. This naming tells us what kind of new information we will get from that transformation. For instance, domains-hosts means that the module will find hosts related to the provided domain.

Some modules, like whoxy\_whois, require a key, as we can tell from the \* under the K column. This requirement indicates that this module is not usable unless we have a key to use the related service.

Other modules have dependencies, indicated by a \* under the D column. Dependencies show that third-party Python libraries might be necessary to use the related module.

In our example **recon/domains-hosts/google\_site\_web** module was installed, which I also choose to install. Command:- **marketplace install google\_site\_web**

```
[recon-ng][cybershujaaredteam] > marketplace install google_site_web
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules ...
[recon-ng][cybershujaaredteam] > 
```

## Working with Installed Modules

We can work with modules using:

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

Since we have already installed the module **google\_site\_web**, we then proceed to load it using command: **load google\_site\_web** and **run it with run.**

```
recon-ng: recon-ng — Console
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
[recon-ng][cybershujaaaredteam] > modules search
Recon
recon/domains-hosts/google_site_web
[recon-ng][cybershujaaaredteam] > modules load google_site_web
[recon-ng][cybershujaaaredteam][google_site_web] > run

THMREDTEAM.COM

[*] Searching Google for: site:thmredteam.com
[*] Country: None
[*] Host: ww12.thmredteam.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: clinic.thmredteam.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: cafe.thmredteam.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Searching Google for: site:thmredteam.com -site:ww12.thmredteam.com -site:clinic.thmredteam.com -site:cafe.thmredteam.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 201.
[*] Searching Google for: site:thmredteam.com -site:ww12.thmredteam.com -site:clinic.thmredteam.com -site:cafe.thmredteam.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 301.
[*] Searching Google for: site:thmredteam.com -site:ww12.thmredteam.com -site:clinic.thmredteam.com -site:cafe.thmredteam.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 401.
[*] Searching Google for: site:thmredteam.com -site:ww12.thmredteam.com -site:clinic.thmredteam.com -site:cafe.thmredteam.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 501.
[*] Searching Google for: site:thmredteam.com -site:ww12.thmredteam.com -site:clinic.thmredteam.com -site:cafe.thmredteam.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 601.
[*] Searching Google for: site:thmredteam.com -site:ww12.thmredteam.com -site:clinic.thmredteam.com -site:cafe.thmredteam.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 701.
[*] Searching Google for: site:thmredteam.com -site:ww12.thmredteam.com -site:clinic.thmredteam.com -site:cafe.thmredteam.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 801.
[*] Searching Google for: site:thmredteam.com -site:ww12.thmredteam.com -site:clinic.thmredteam.com -site:cafe.thmredteam.com
```

Final results are:-

```
thmredteam.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 4201.
[*] Searching Google for: site:thmredteam.com -site:ww12.thmredteam.com -site:clinic.thmredteam.com -site:cafe.thmredteam.com
[*] Google CAPTCHA triggered. No bypass available.

SUMMARY

[*] 3 total (3 new) hosts found.
[recon-ng][cybershujaaaredteam][google_site_web] > █
```

This module has queried Google and discovered three hosts:-

```
[recon-ng][cybershujaaaredteam] > modules load google_site_web
[recon-ng][cybershujaaaredteam][google_site_web] > run

THMREDTEAM.COM

[*] Searching Google for: site:thmredteam.com
[*] Country: None
[*] Host: ww12.thmredteam.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: clinic.thmredteam.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: cafe.thmredteam.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
```

1. ww12.thmredteam.com
2. clinic.thmredteam.com
3. cafe.thmredteam.com



## How do you start recon-ng with the workspace clinicredteam?

**ANS: recon-ng -w clinicredteam**

```
(coderic@kali)-[~/Downloads/tryhackme/recon_ng_workspaces]
$ recon-ng -w clinicredteam
[*] Version check disabled.
```

```
Sponsored by ...
```

```
// // BLACK HILLS \ \ \\ 
www.blackhillinfosec.com
```

```
PRACTISEC
www.practisec.com
```

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

```
[1] Recon modules
[recon-ng][clinicredteam] > |
```

How many modules with the name `virustotal` exist?

**ANS: 2**

```
| 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 | | | |
| recon/hosts-domains/migrate_hosts | 1.1 | not installed | 2020-05-17 | | | |
| recon/hosts-hosts/censys_query | 2.0 | not installed | 2021-05-10 | * | * |
| 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.
```

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

ANS:migrate\_hosts

```
recon/domains-hosts/crtsh | 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/censys_query | 2.0 | not installed | 2021-05-10 | * | *
recon/hosts-hosts/virustotal | 1.0 | not installed | 2019-06-24 | | *
recon/netblocks-hosts/virustotal | 1.0 | not installed | 2019-06-24 | | *
```

censys\_email\_address is a module that “retrieves email addresses from the TLS certificates for a company.” Who is the author?

**ANS: Censys Team**

```
[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] > 
```

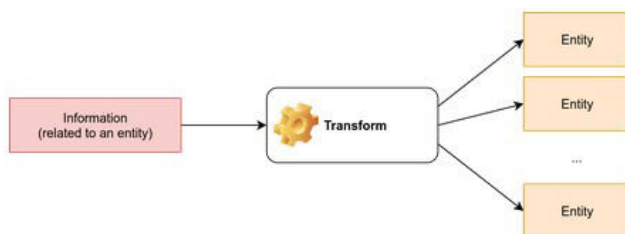
## **Maltego.**

**Maltego** is an application that blends mind-mapping with OSINT.

In general, you would start with a domain name, company name, person’s name, email address, etc. Then you can let this piece of information go through various transforms.

For the information collected in Maltego it can be used for later stages. For instance, company information, contact names, and email addresses collected can be used to create very legitimate-looking phishing emails.

In maltego an entity is passed through a stage called transform, **transform** is a piece of code that would query an API to retrieve information related to a specific entity.



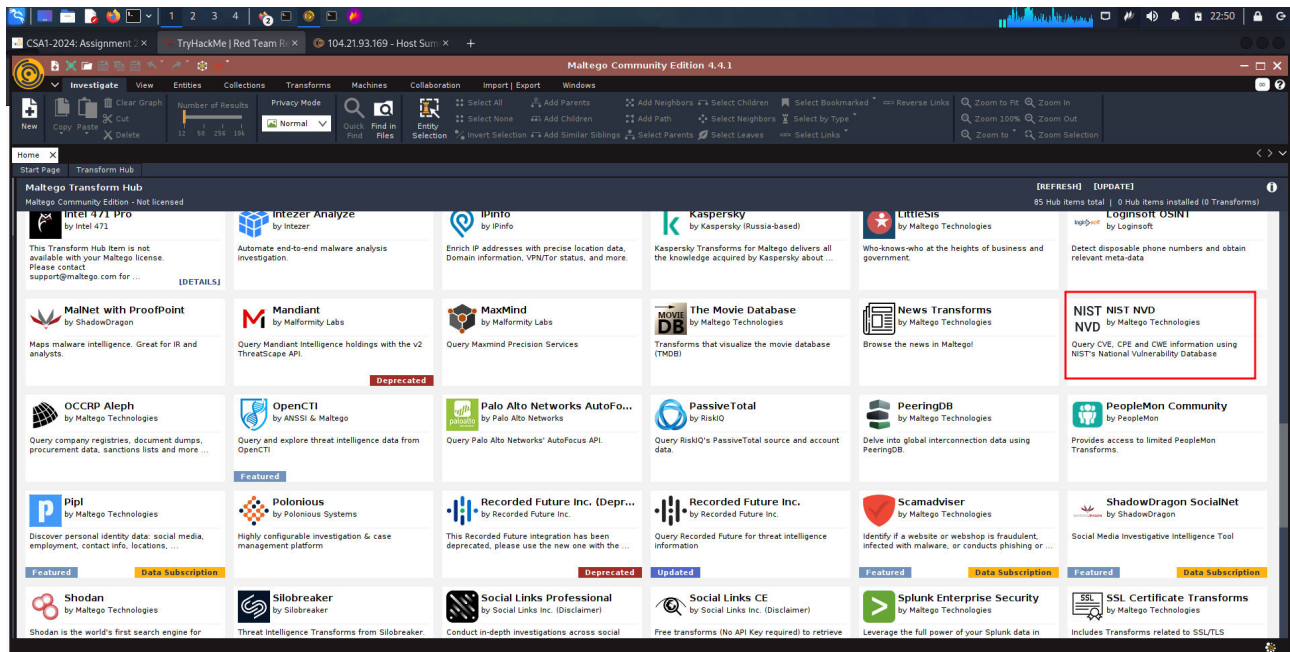
While using maltego you have to be careful on how you use some of the transforms available. Some of them might actively connect to the target system. Therefore, it is better to know how the transform works before using it if you want to limit yourself to passive reconnaissance.

Every transform might lead to several new values.

## Answer the questions below

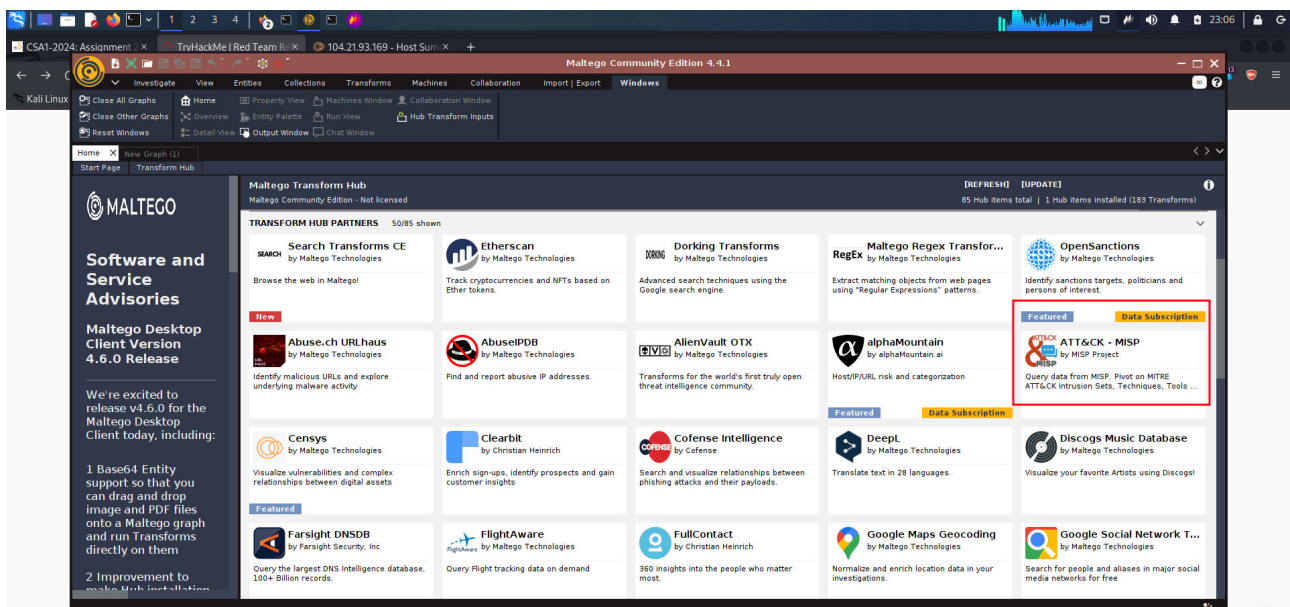
What is the name of the transform that queries NIST's National Vulnerability Database?

**ANS: NIST NVD**



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

**ANS: MISP Project**



## **Summary.**

This section summaries with a quote from Sun Tzu that says, “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

In connection to cyber security it gives an explanation of why you also need to understand the tactics and skills used by the red teams to be more effective as an ethical hacker to give the best protection to your networks.

## **Conclusion.**

In conclusion to this room, I have gained solid introduction in both essential built-in tools such as **whois**, **dig**, and **tracert** and explored the power of search engines most appropriate in passive reconnaissance activities. I have also been able to learn about **Recon-ng** and **Maltego**, that allow us to collect information from various sources and present them in one place.

This room has taught me on how to perform activities such as open-source intelligence gathering, network scanning and enumeration to identify potential vulnerabilities. By giving examples to real-world scenarios, this room has imparted me with knowledge on how I can help individuals or organizations enhance their Cybersecurity defenses by addressing weaknesses.

**Thank you.**