Red Team Recon: TryHackMe

Name: Daniel Mwendwa Mwithui

ADM NO. CS-SA04-23080

Program: Security Analyst

Date of submission: 8th June 2023

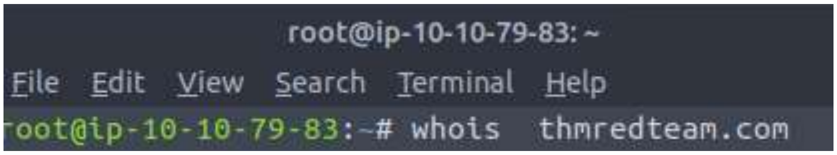
Introduction

Red team reconnaissance refers to the process of gathering information and conducting intelligence gathering activities from the perspective of an attacker or "red team." In this module, we will explore the fascinating world of red team reconnaissance, where we gather important information to identify potential weaknesses in security. We will learn about specialized search engines like ViewDNS.info and Shodan, as well as a cool tool called Recon-ng. These tools will help us gather information and understand how to find vulnerabilities.

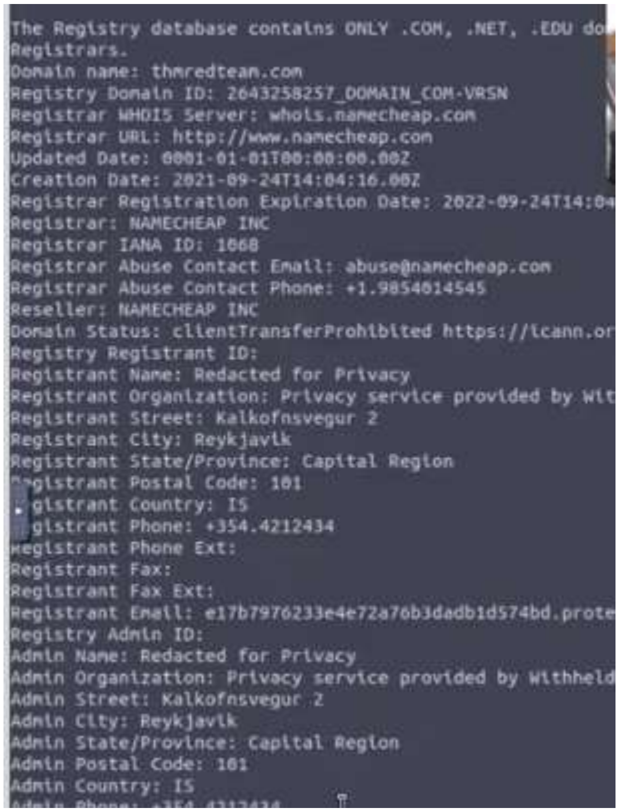
Task 1: built-in tools.

In this section, we will explore tools such as Whois, Nslookup, Dig, and Host. These tools help us gather information about domains, IP addresses, and DNS records, enabling us to understand target ownership, perform DNS lookups, and retrieve important details for effective reconnaissance. Here is how to solve specific tasks in this section.

Task 1a. To get When was *thmredteam.com* created do whois *thmredteam.com*.

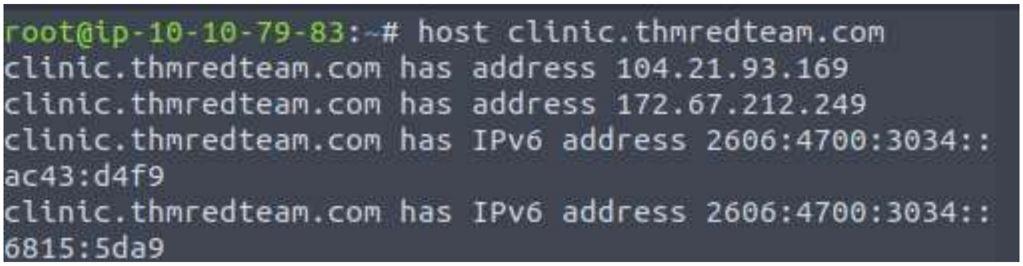


```
root@ip-10-10-79-83:~# whois  thmredteam.com
```



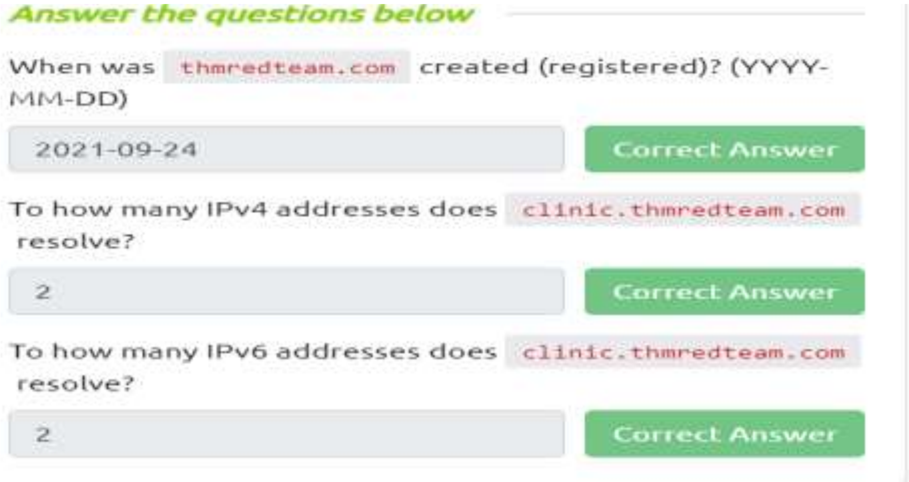
```
The Registry database contains ONLY .COM, .NET, .EDU do
Registrars.
Domain name: thmredteam.com
Registry Domain ID: 2643258257_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2021-09-24T14:04:16.00Z
Registrar Registration Expiration Date: 2022-09-24T14:04
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.9854014545
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.or
Registry Registrant ID:
Registrant Name: Redacted for Privacy
Registrant Organization: Privacy service provided by Wit
Registrant Street: Kalkofnsvegur 2
Registrant City: Reykjavik
Registrant State/Province: Capital Region
Registrant Postal Code: 101
Registrant Country: IS
Registrant Phone: +354.4212434
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: e17b7976233e4e72a76b3dadb1d574bd.prote
Registry Admin ID:
Admin Name: Redacted for Privacy
Admin Organization: Privacy service provided by Withheld
Admin Street: Kalkofnsvegur 2
Admin City: Reykjavik
Admin State/Province: Capital Region
Admin Postal Code: 101
Admin Country: IS
Admin Phone: +354.4212434
```

Task 2. To find how many IPv4 and IPV6 addresses does clinic.thmredteam.com resolve, do host *clinic.thmredteam.com*



```
root@ip-10-10-79-83:~# 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::
ac43:d4f9
clinic.thmredteam.com has IPv6 address 2606:4700:3034::
6815:5da9
```

Here is completion for this section.



Answer the questions below

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

2021-09-24

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

2

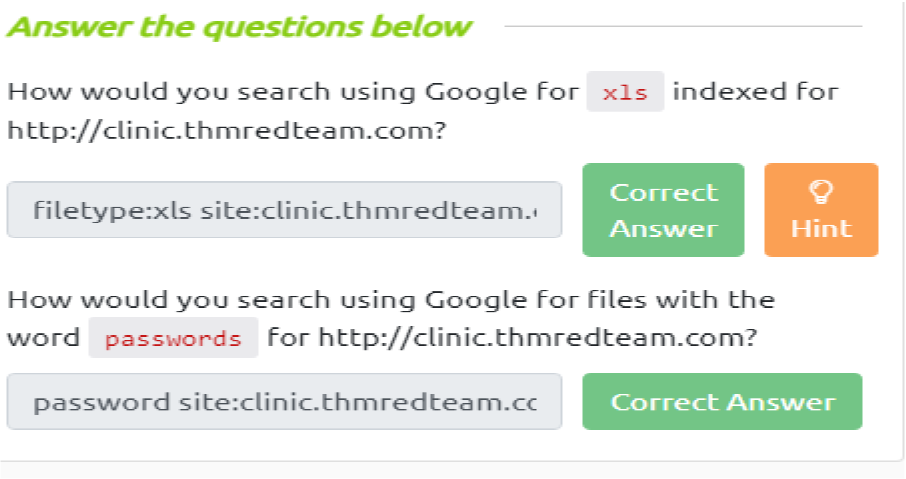
To how many IPv6 addresses does clinic.thmredteam.com resolve?

2

Task 2: Advanced Sharing.

The Advanced Searching section in this module explores techniques to enhance reconnaissance by using advanced search operators, search engine dorks, and open-source intelligence (OSINT). These methods help extract valuable information, refine search queries, and uncover potential vulnerabilities. To complete this section, see the description below.

Task 2 a, b: This task needs to read on introduction part of this section. Here is the screenshot showing completion of this section. The answers below mean that you are searching for xls and password but on a specific site which is clinic.thmredteam.com.



Answer the questions below

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

filetype:xls site:clinic.thmredteam.

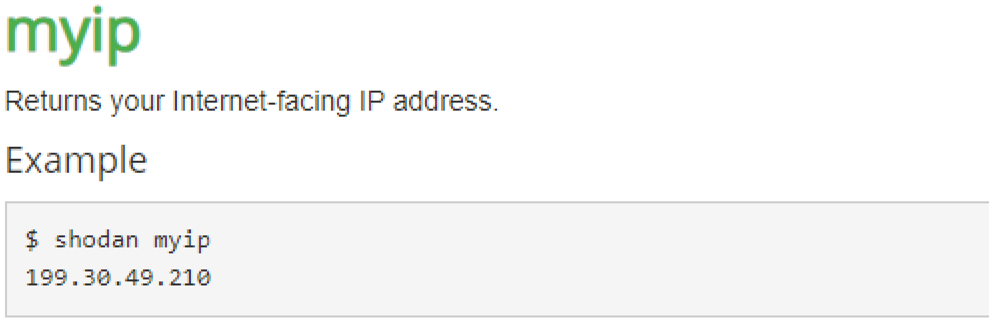
How would you search using Google for files with the word passwords for http://clinic.thmredteam.com?

password site:clinic.thmredteam.cc

Task 3: specialized search engine

In this section, we will learn about specialized search engines like ViewDNS.info and Threat Intelligence Platforms. These tools are designed specifically for cybersecurity professionals and provide valuable information related to domains, IP addresses, DNS records, and potential threats. By utilizing these specialized search engines, we can gather targeted intelligence and enhance our reconnaissance efforts. We will also learn about Shodan. By using Shodan, we can identify and analyze internet-connected devices, such as webcams, routers, and servers, to gain insights into their configurations and potential security risks.

To complete this task, search https://cli.shodan.io/ and scroll down to find the command shown below.

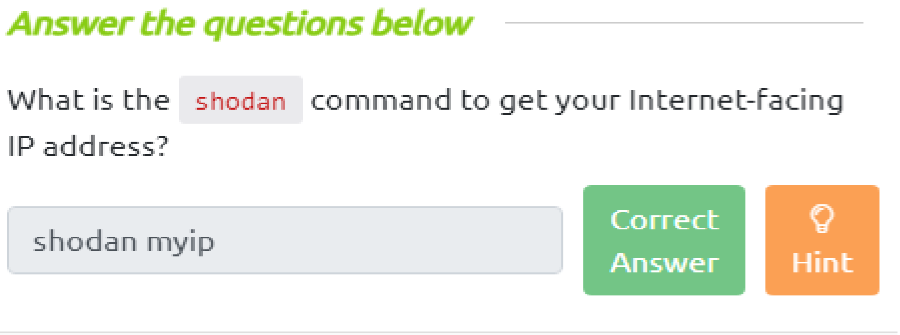


myip

Returns your Internet-facing IP address.

Example

```
$ shodan myip
199.30.49.210
```



Answer the questions below

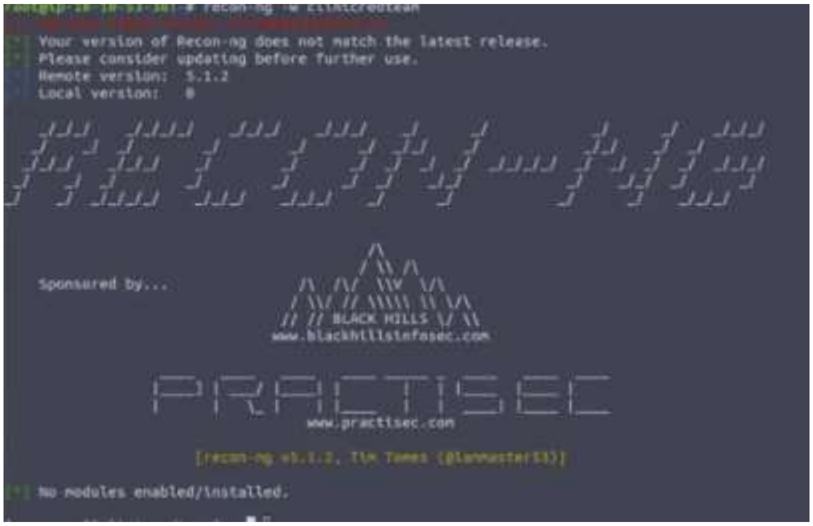
What is the `shodan` command to get your Internet-facing IP address?

shodan myip

Task 4. Recon-ng

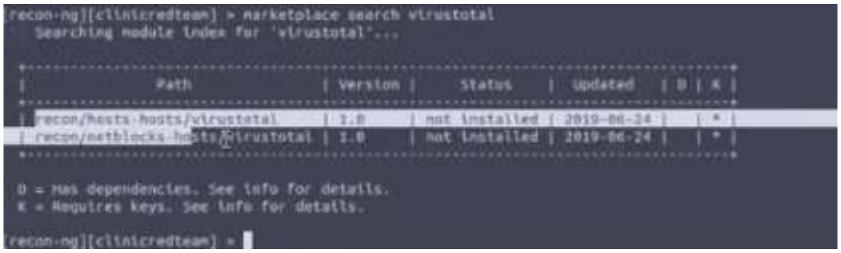
Recon-ng is a powerful reconnaissance framework used to gather information and conduct active reconnaissance on target systems, networks, and web applications. Recon-ng provides a wide range of modules and functionalities that aid in data collection from various sources, including public APIs, search engines, social media platforms, and more. By leveraging Recon-ng, red teamers can efficiently gather valuable intelligence, identify potential vulnerabilities, and analyze their targets, enhancing the overall effectiveness of the reconnaissance phase in a red team engagement. To complete this section, see the screenshot below.

To start *recon-ng* with the workspace *clinicredteam* do *recon-ng -w clinicredteam*



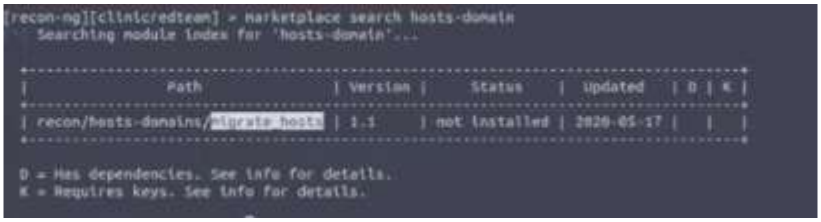
```
root@ip-10-10-53-38:~# recon-ng -w clinicredteam
[illegible]
[*] Your version of Recon-ng does not match the latest release.
[*] Please consider updating before further use.
[*] Remote version:  5.1.2
[*] Local version:   0

Sponsored by...

                    // // BLACK HILLS \/ \\
                  www.blackhillsinfosec.com

                       www.practisec.com

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

[*] No modules enabled/installed.
```

To find how many modules with the name virustotal exist, do *marketplace search virustotal* command.



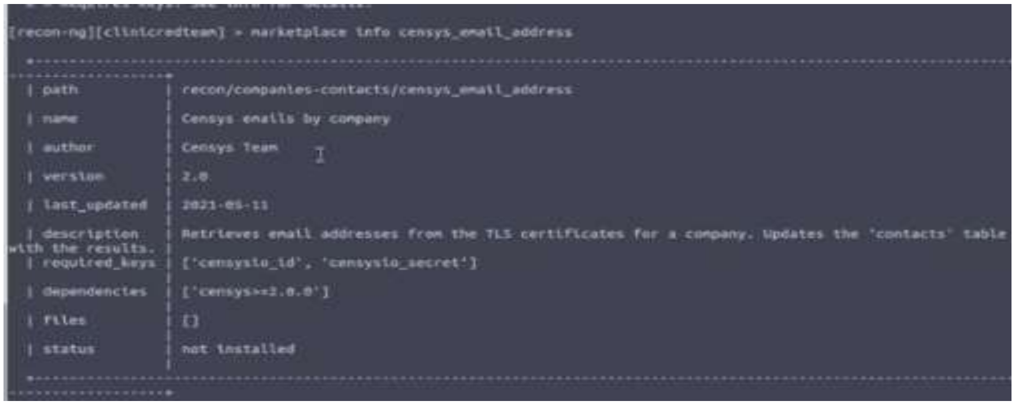
```
[recon-ng][clinicredteam] > marketplace search virustotal
[*] Searching module index for 'virustotal'...

  +-------------------------------------------------------------------------+
  |                 Path                 | Version |     Status    |  Updated   | D | K |
  +-------------------------------------------------------------------------+
  | 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.

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

To find the name of the module under hosts-domains, do *marketplace search host-domain*



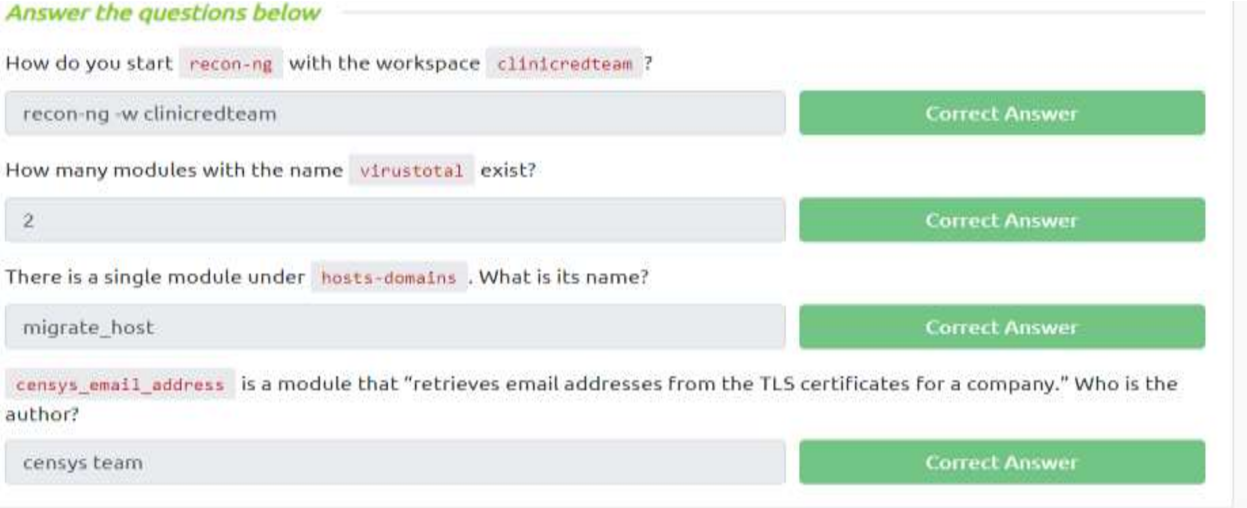
```
[recon-ng][clinicredteam] > marketplace search hosts-domain
[*] Searching module index for 'hosts-domain'...

  +-------------------------------------------------------------------------+
  |                 Path                  | Version |     Status    |  Updated   | D | K |
  +-------------------------------------------------------------------------+
  | recon/hosts-domains/migrate_hosts      | 1.1     | not installed | 2020-05-17 |   |   |
  +-------------------------------------------------------------------------+

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

To find the author of *censys_email_address* do *marketplace info censys_email_address*



```
[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
  |                |
  +------------------------------------------------------------------------------------------
------------------+
```

Here is the completion screenshot of this section.



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

recon-ng -w clinicredteam

How many modules with the name `virustotal` exist?

2

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

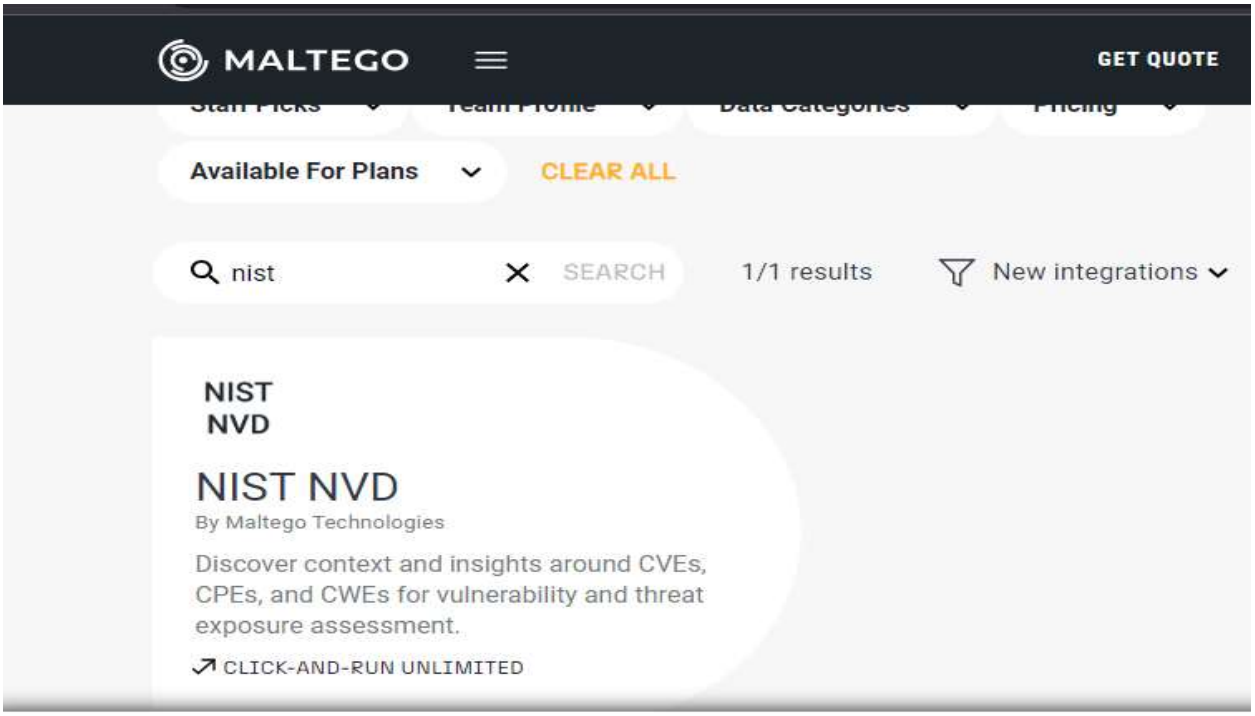
migrate_host

`censys_email_address` is a module that "retrieves email addresses from the TLS certificates for a company." Who is the author?

censys team

Task 5: Maltego

Maltego is a reconnaissance tool that gathers and visualizes information about individuals, organizations, and networks. It connects and analyzes diverse data sources to identify connections and patterns, providing valuable insights for cybersecurity engagements. To complete this section, you can find answers in this link https://www.maltego.com/transform-hub/



nist

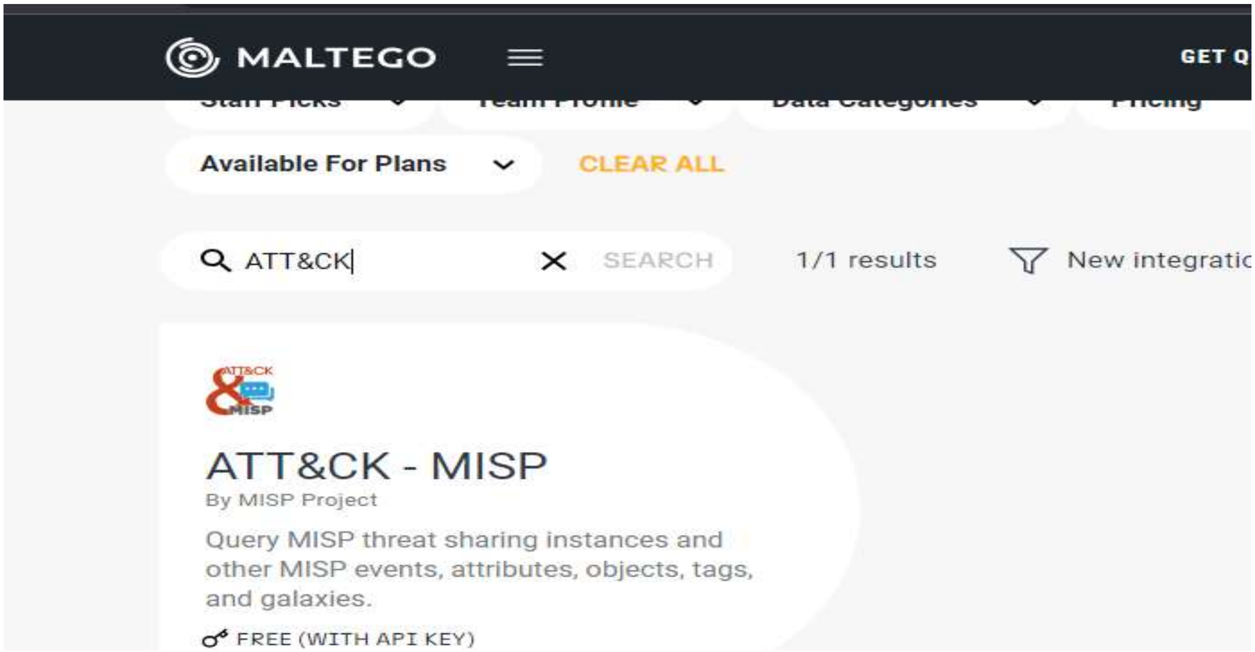
1/1 results

NIST NVD

By Maltego Technologies

Discover context and insights around CVEs, CPEs, and CWEs for vulnerability and threat exposure assessment.

CLICK-AND-RUN UNLIMITED



ATT&CK

1/1 results

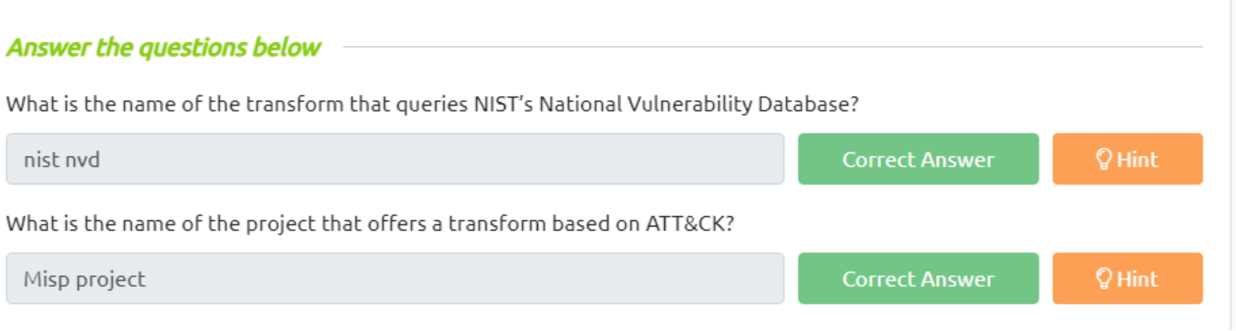
ATT&CK - MISP

By MISP Project

Query MISP threat sharing instances and other MISP events, attributes, objects, tags, and galaxies.

FREE (WITH API KEY)

Here is completion for this section



Answer the questions below

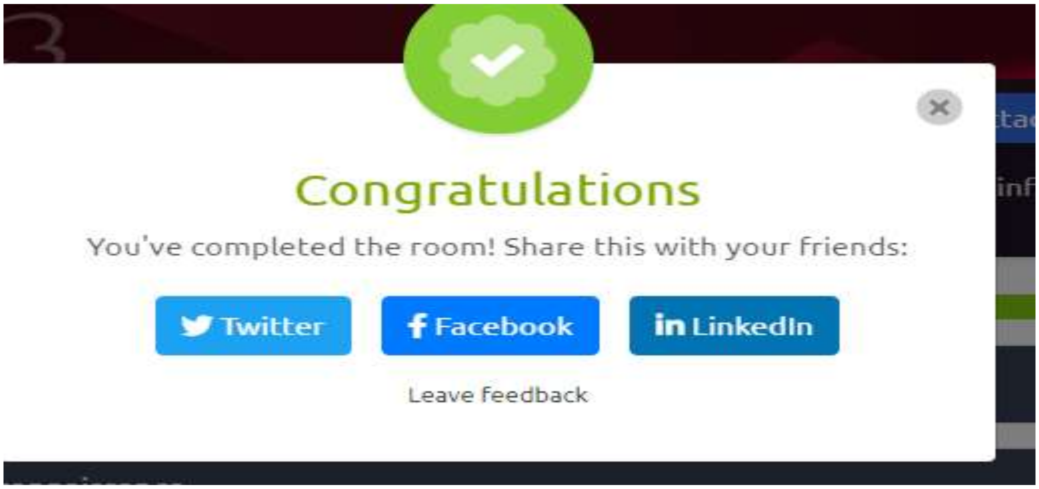
What is the name of the transform that queries NIST's National Vulnerability Database?

nist nvd

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

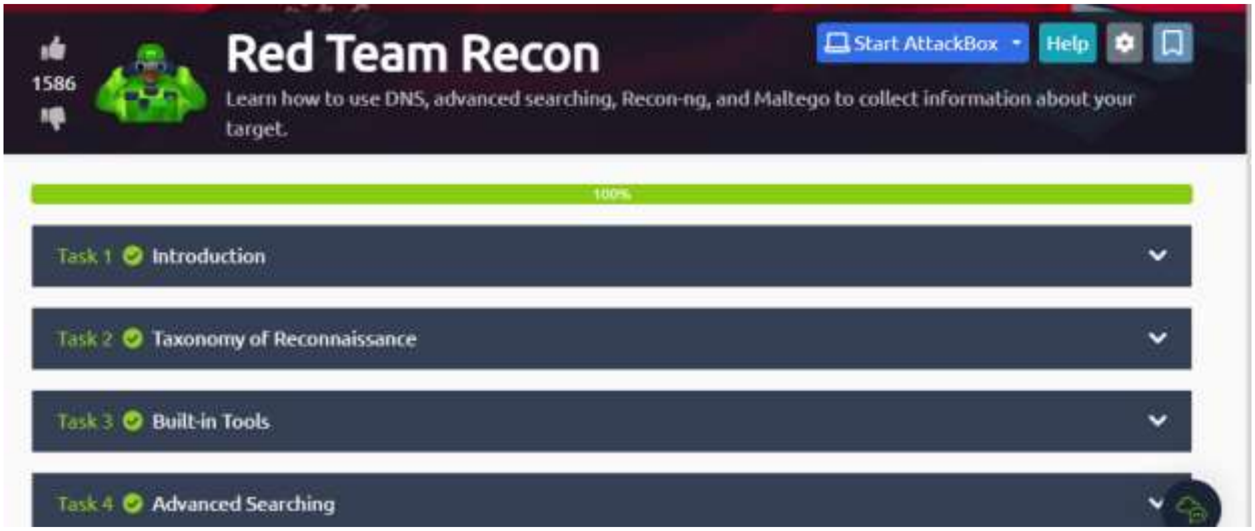
Misp project

Here is completion level for the module and sharable link



Congratulations

You've completed the room! Share this with your friends:



Red Team Recon

Learn how to use DNS, advanced searching, Recon-ng, and Maltego to collect information about your target.

1586

100%

Task 1 Introduction

Task 2 Taxonomy of Reconnaissance

Task 3 Built-in Tools

Task 4 Advanced Searching

Link: https://tryhackme.com/room/redteamrecon

Conclusion

Completing the Red Team Recon assignment on TryHackMe has been an amazing learning experience. We have discovered how to use specialized search engines like ViewDNS.info and

Shodan, and we’ve also learned about a handy tool called Recon-ng. These tools have taught us how to gather important information and identify security weaknesses. We now feel more confident in our ability to contribute to cybersecurity efforts. This assignment has provided us with practical knowledge and hands-on experience that we can apply in real-world situations.