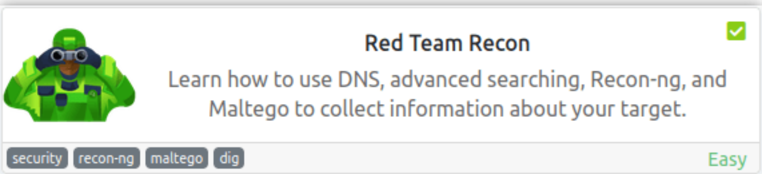
Tryhackme – Red Team Recon

Leave a Comment / CTF, Tryhackme / By admin

In this walk through, we will be going through the Red Team Recon room from Tryhackme. This room will teach us how to use DNS, advanced searching, Recon-ng, and Maltego to collect information about your target. On that note, let's get started.

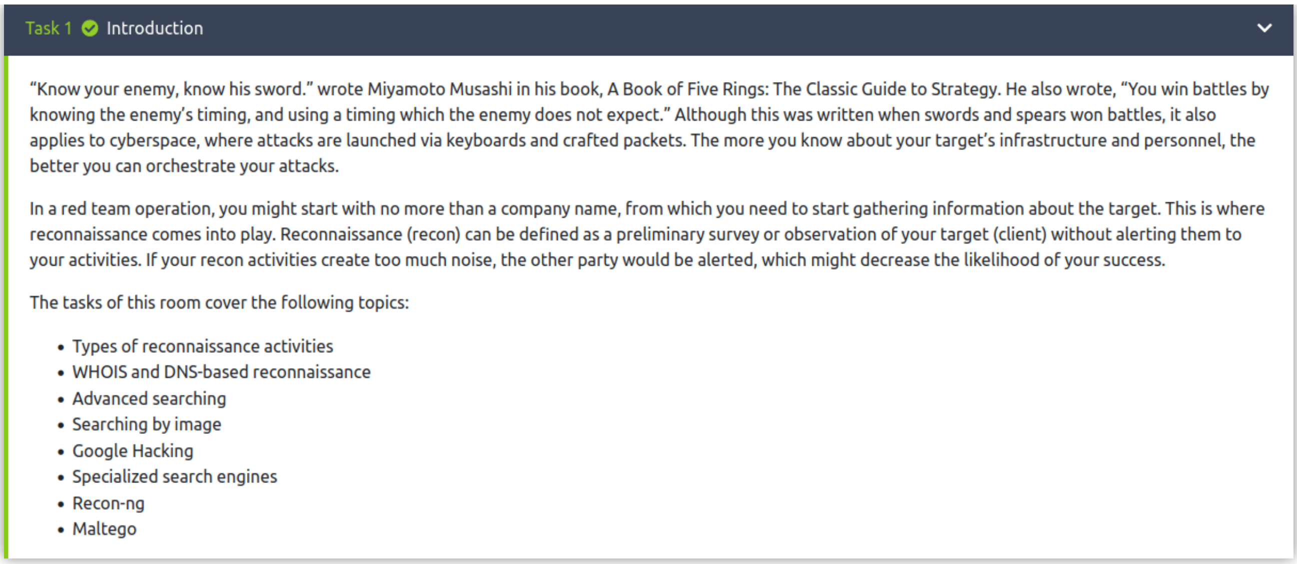


Red Team Recon ✓

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

Table of Contents

Task 1 – Introduction

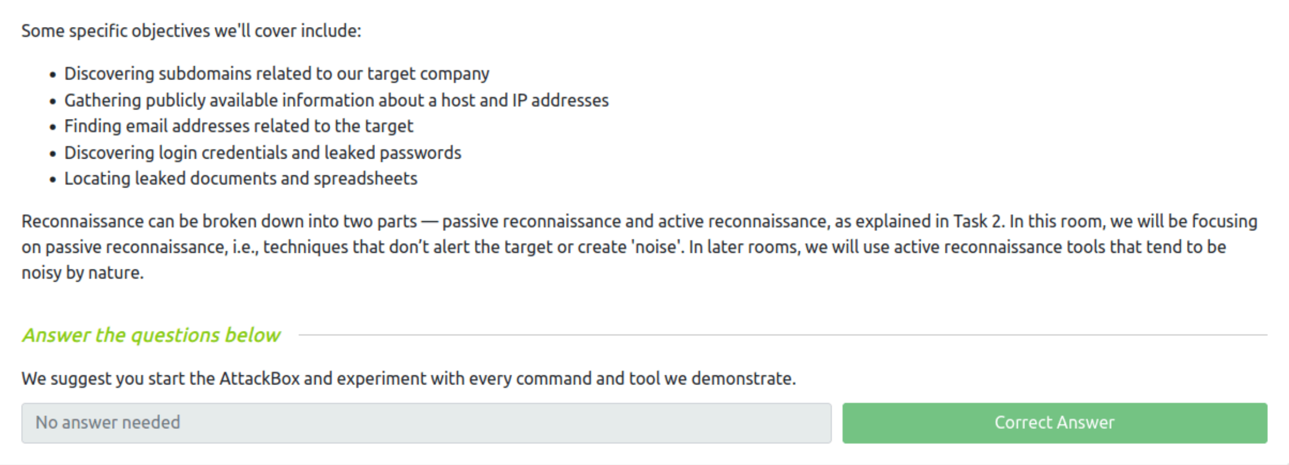


“Know your enemy, know his sword.” wrote Miyamoto Musashi in his book, A Book of Five Rings: The Classic Guide to Strategy. He also wrote, “You win battles by knowing the enemy’s timing, and using a timing which the enemy does not expect.” Although this was written when swords and spears won battles, it also applies to cyberspace, 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.

In a red team operation, you might start with no more than a company name, from which you need to start gathering information about the target. This is where reconnaissance comes into play. Reconnaissance (recon) can be defined as a preliminary survey or observation of your target (client) without alerting them to your activities. If your recon activities create too much noise, the other party would be alerted, which might decrease the likelihood of your success.

The tasks of this room cover the following topics:

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



Some specific objectives we'll cover 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
- Locating leaked documents and spreadsheets

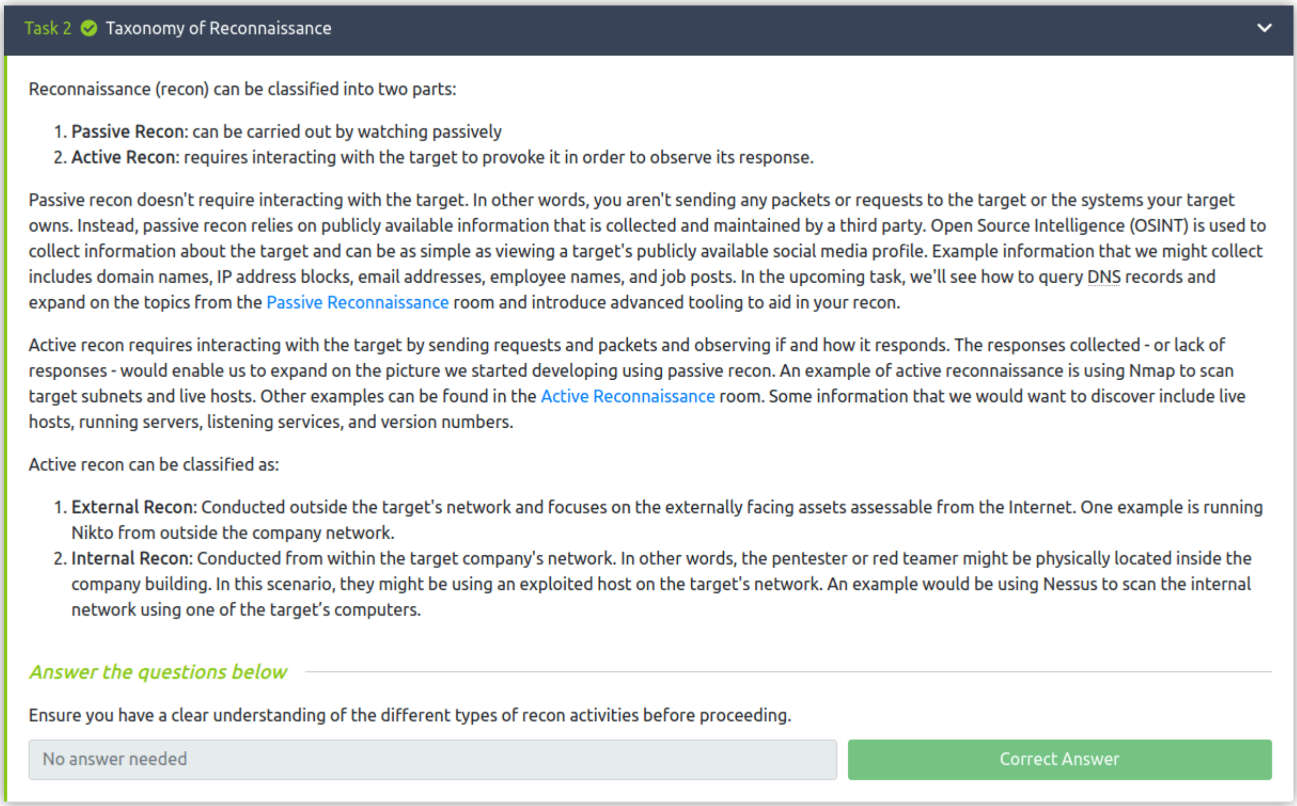
Reconnaissance can be broken down into two parts — passive reconnaissance and active reconnaissance, as explained in Task 2. In this room, we will be focusing on passive reconnaissance, i.e., techniques that don’t alert the target or create 'noise'. In later rooms, we will use active reconnaissance tools that tend to be noisy by nature.

Answer the questions below

We suggest you start the AttackBox and experiment with every command and tool we demonstrate.

No answer needed

Task 2 – Taxonomy of Reconnaissance



Reconnaissance (recon) can be classified into two parts:

1. **Passive Recon**: can be carried out by watching passively
2. **Active Recon**: requires interacting with the target to provoke it in order to observe its response.

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. Example information that we might collect includes domain names, IP address blocks, email addresses, employee names, and job posts. In the upcoming task, we'll see how to query DNS records and expand on the topics from the Passive Reconnaissance room and introduce advanced tooling to aid in your recon.

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. Other examples can be found in the Active Reconnaissance room. Some information that we would want to discover include live hosts, running servers, listening services, and version numbers.

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. An example would be using Nessus to scan the internal network using one of the target’s computers.

Answer the questions below

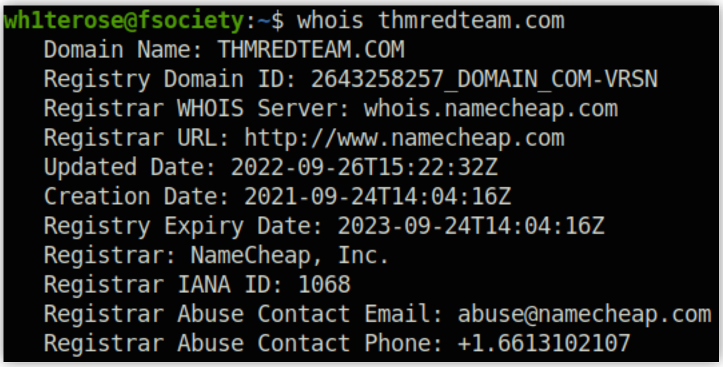
Ensure you have a clear understanding of the different types of recon activities before proceeding.

No answer needed

Task 3 – Built-in Tools

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

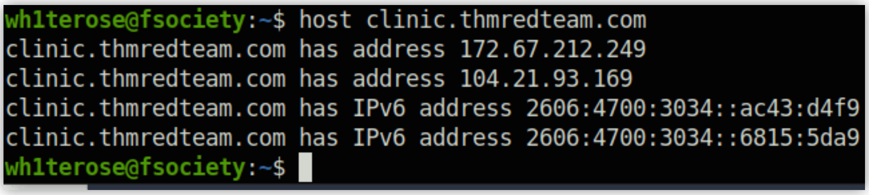
```
1.  whois thmredteam.com
```



```
wh1terose@fsociety:~$ 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
```

`2021-09-24`

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

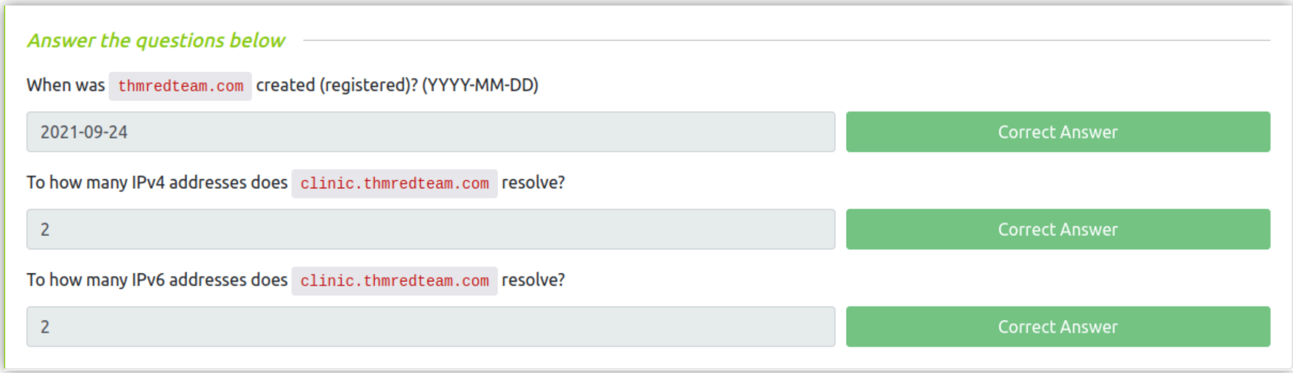


```
wh1terose@fsociety:~$ host clinic.thmredteam.com
clinic.thmredteam.com has address 172.67.212.249
clinic.thmredteam.com has address 104.21.93.169
clinic.thmredteam.com has IPv6 address 2606:4700:3034::ac43:d4f9
clinic.thmredteam.com has IPv6 address 2606:4700:3034::6815:5da9
wh1terose@fsociety:~$
```

`2`

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

`2`



Answer the questions below

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

2021-09-24

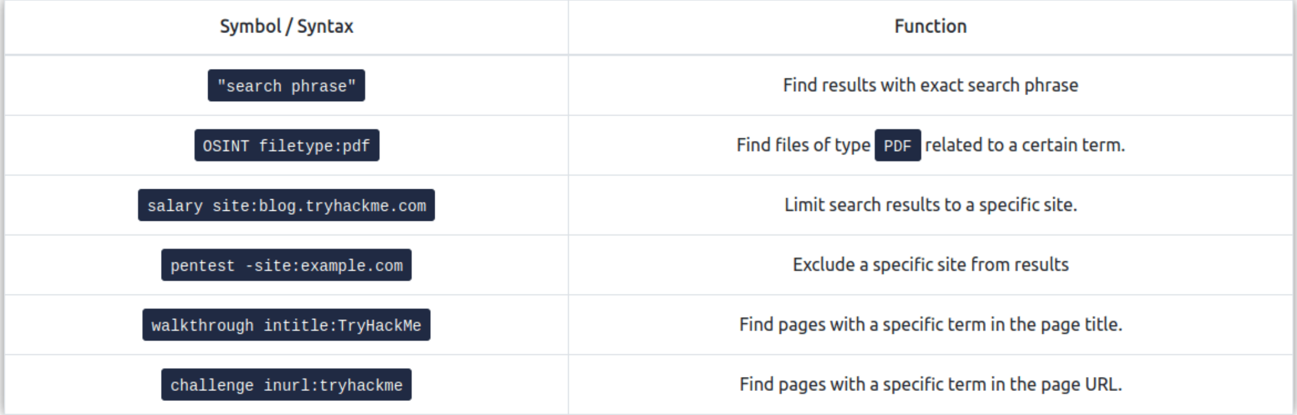
To how many IPv4 addresses does `clinic.thmredteam.com` resolve?

2

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

2

Task 4 – Advanced Searching



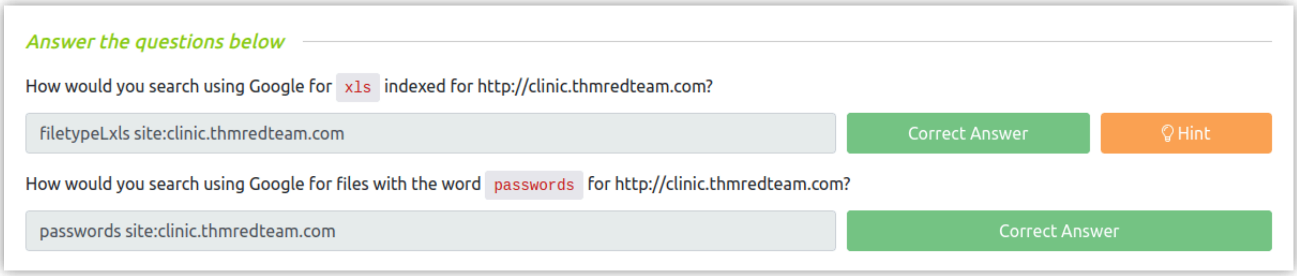
Symbol / Syntax	Function
`"search phrase"`	Find results with exact search phrase
`OSINT filetype:pdf`	Find files of type `PDF` related to a certain term.
`salary site:blog.tryhackme.com`	Limit search results to a specific site.
`pentest -site:example.com`	Exclude a specific site from results
`walkthrough 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.

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

```
filetypeLxls site:clinic.thmredteam.com
```

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

```
passwords site:clinic.thmredteam.com
```



Answer the questions below

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

filetypeLxls site:clinic.thmredteam.com

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

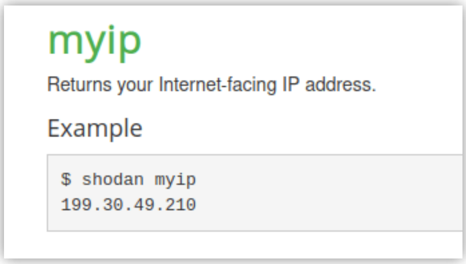
passwords site:clinic.thmredteam.com

Trending

Hacking Android pin password using Lockphish

Task 5 – Specialized Search Engines

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



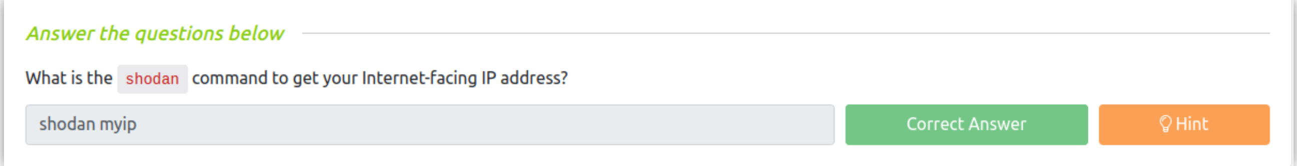
myip

Returns your Internet-facing IP address.

Example

```
$ shodan myip
199.30.49.210
```

```
shodan myip
```



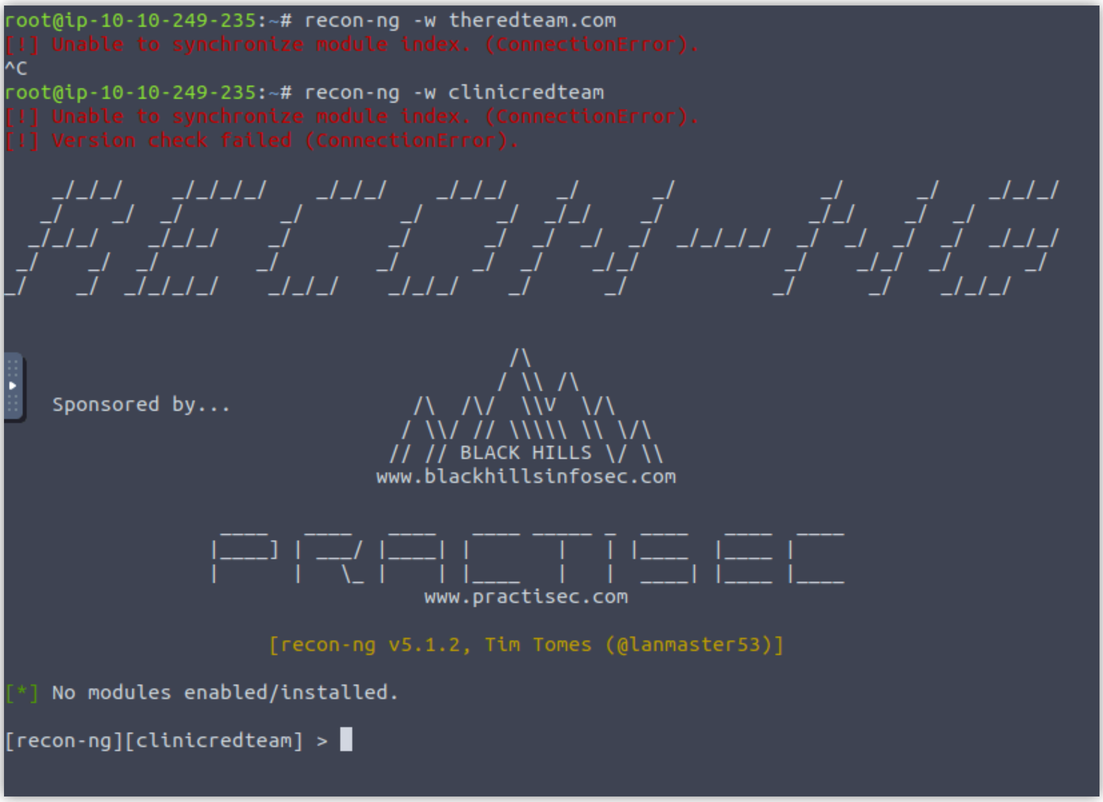
Answer the questions below

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

shodan myip

Task 6 – Recon-ng

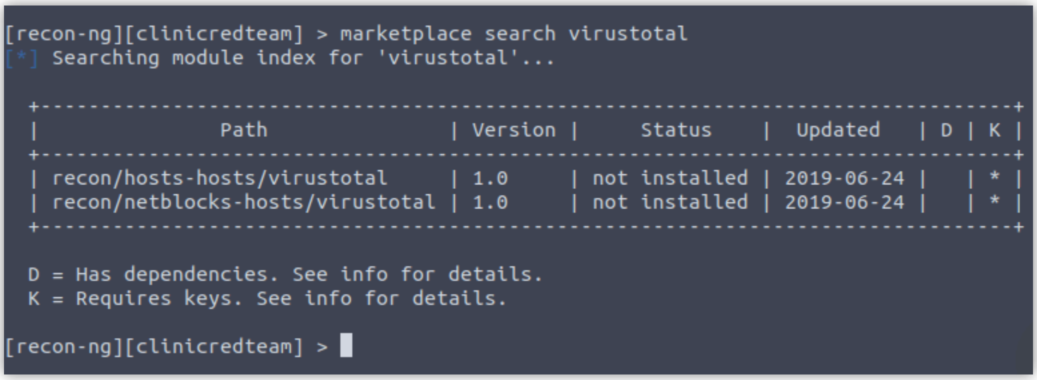
Question 1 – How do you start `recon-ng` with the workspace `clinicredteam`?



```
root@ip-10-10-249-235:~# recon-ng -w theredteam.com
[!] Unable to synchronize module index. (ConnectionError).
^C
root@ip-10-10-249-235:~# recon-ng -w clinicredteam
[!] Unable to synchronize module index. (ConnectionError).
[!] Version check failed (ConnectionError).

    _/_/_/    _/_/_/_/    _/_/_/    _/_/_/    _/      _/            _/      _/    _/_/_/
   _/    _/  _/        _/        _/      _/  _/_/    _/            _/_/    _/  _/
  _/_/_/    _/_/_/    _/        _/      _/  _/  _/  _/  _/_/_/_/  _/  _/  _/  _/  _/_/_/
 _/    _/  _/        _/        _/      _/  _/    _/_/            _/    _/_/  _/      _/
_/    _/  _/_/_/_/    _/_/_/    _/_/_/    _/      _/            _/      _/    _/_/_/


                                          /\
                                         / \\ /\
    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][clinicredteam] >
```

recon-ng -w clinicredteam

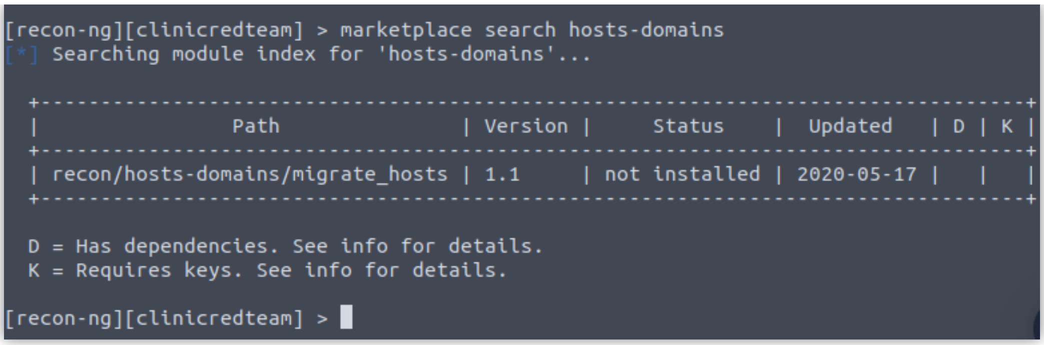
Question 2 – How many modules with the name `virustotal` exist?



```
[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] >
```

2

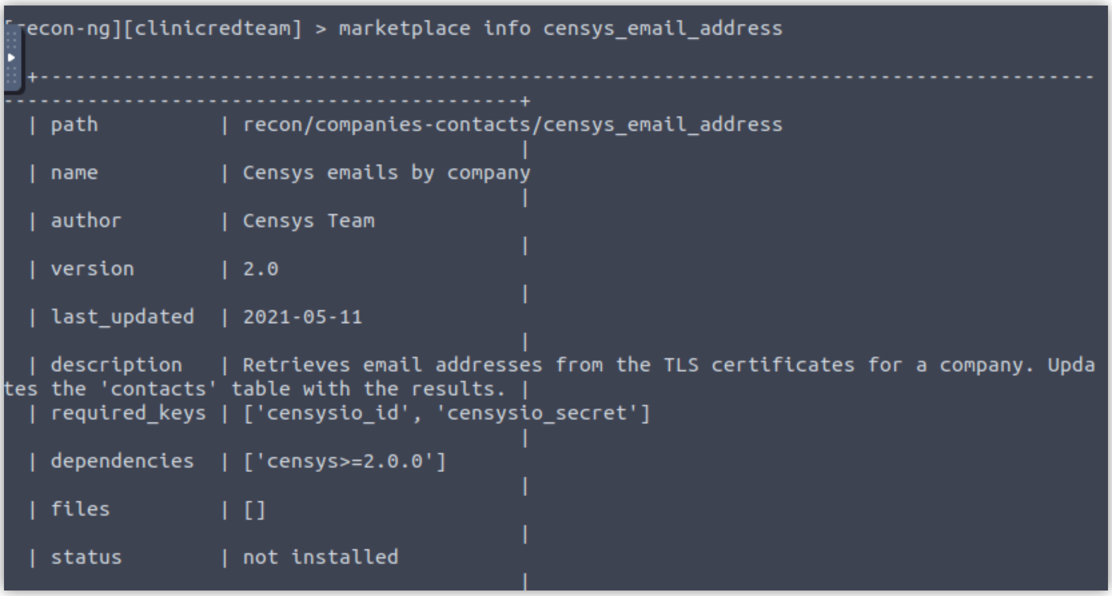
Question 3 – There is a single module under `hosts-domains`. What is its name?



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

  +---------------------------------------------------------------------------------------+
  |                 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.

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

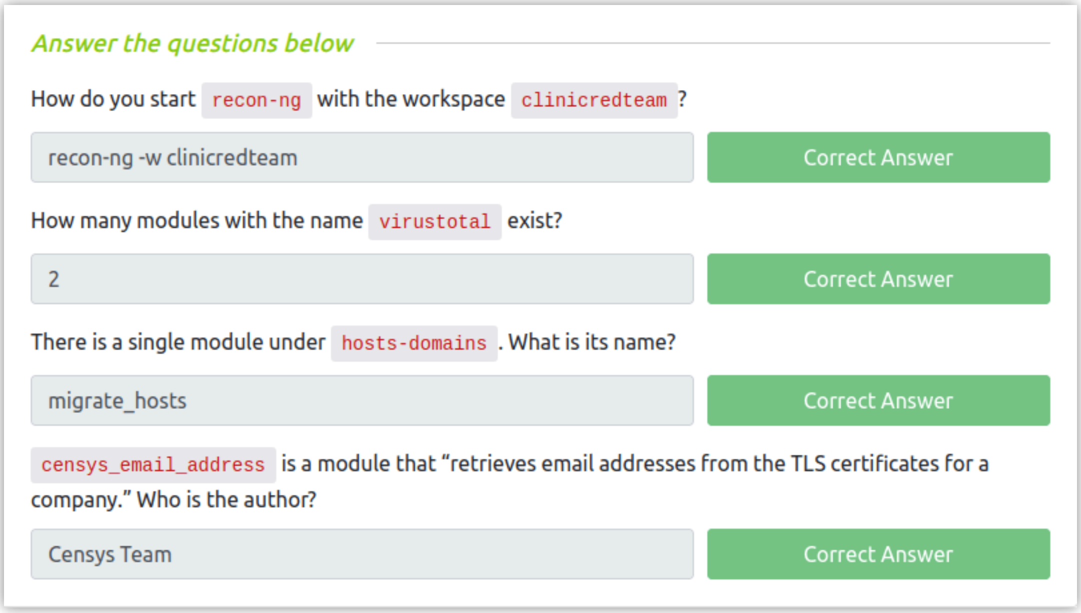
`migrate_hosts`

Question 4 – `censys_email_address` is a module that "retrieves email addresses from the TLS certificates for a company." Who is the author?



```
[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. Upda
tes the 'contacts' table with the results. |
  | required_keys | ['censysio_id', 'censysio_secret']
                                         |
  | dependencies  | ['censys>=2.0.0']
                                         |
  | files         | []
                                         |
  | status        | not installed
                                         |
```

`Censys Team`



Answer the questions below

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

recon-ng -w clinicredteam

Correct Answer

How many modules with the name `virustotal` exist?

2

Correct Answer

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

migrate_hosts

Correct Answer

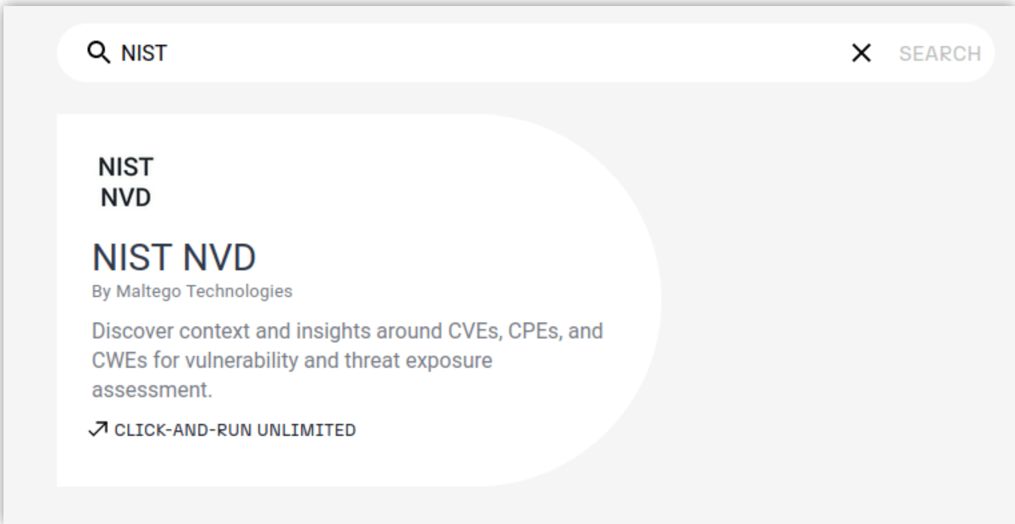
`censys_email_address` is a module that "retrieves email addresses from the TLS certificates for a company." Who is the author?

Censys Team

Correct Answer

Task 7 – Maltego

Question 1 – What is the name of the transform that queries NIST's National Vulnerability Database?



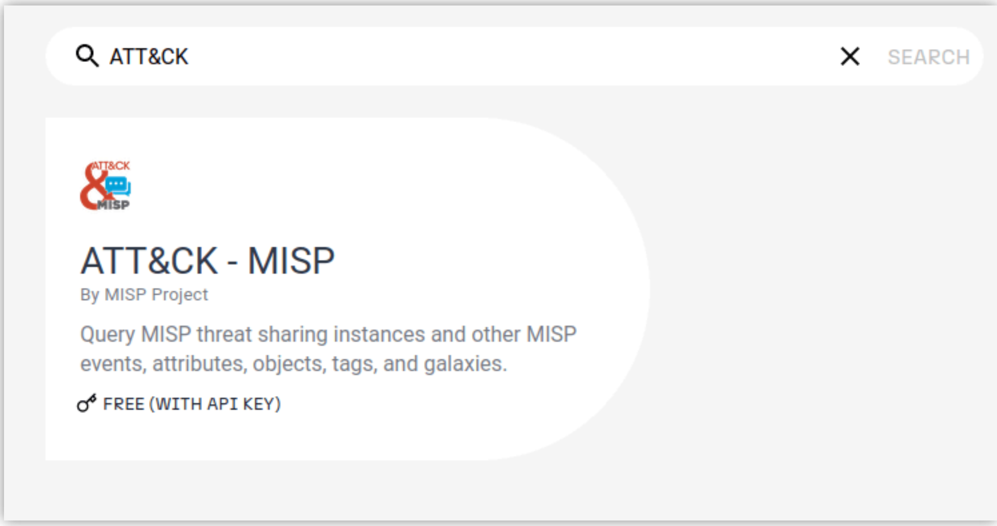
NIST NVD

By Maltego Technologies

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

```
NIST NVD
```

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



ATT&CK - MISP

By MISP Project

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

```
MISP Project
```

Task 7 - Maltego

Task 8 – Summary

Task 8 - Summary

Also Read: Tryhackme – Red Team Engagements

So that was **"Red Team Recon"** for you. In this room, we have learned how to use DNS, advanced searching, Recon-ng, and Maltego to collect information about your target. We have covered the taxonomy of reconnaissance, some built in tools like whois, nslookup and traceroute. Further, we got into some Google Dorking and Shodan Searching. At last, we peeked into some of the famous Red Team Recon framework like Recon-ng and Maltego. On that note, i will take your leave and meet you in next one. So stay tuned and till then, **“Hack the planet”.**

← Previous Post

Next Post →

Related Posts

The Ultimate Guide on How to get started in CTFs?

The Ultimate Guide on How to get started in CTFs?

CTF, Cybersecurity / By admin

Tryhackme – Tutorial

Tryhackme – Tutorial

CTF, Tryhackme / By admin

Tryhackme - Nmap Walkthrough

Tryhackme – Nmap

CTF, Tryhackme / By admin

Leave a Comment

Your email address will not be published. Required fields are marked *

Type here..

□ I'm not a robot

reCAPTCHA
Privacy - Terms

Name*

Email*

Website

□ Save my name, email, and website in this browser for the next time I comment.

Post Comment »

Search...

Recent Posts

How to hack Android Phone using Kali Linux

Steganography: Hiding secrets like Mr. Robot

How Hackers Become Anonymous While Hacking

Hacking Windows via WhatsApp Messenger RCE

Hacking Windows with Fake Captchas

Recent Comments

Varun on How to hack Android Phone using Kali Linux

Rahul on How to hack Android Phone using Kali Linux

Vulnab - Media on Vulnlab – Feedback

How to hack Android Phone using Kali Linux on How Hackers Become Anonymous While Hacking

ali on How to hack Android Phone using Kali Linux

Archives

November 2024

October 2024

August 2024

July 2024

June 2024

May 2024

April 2024

March 2024

February 2024

January 2024

December 2023

November 2023

October 2023

September 2023

August 2023

July 2023

June 2023

May 2023

March 2023

February 2023

December 2022

November 2022

September 2022

August 2022

July 2022

November 2021

May 2021

April 2021

November 2020

October 2020

September 2020

August 2020

July 2020

June 2020

May 2020

April 2020

June 2019

Categories

A1 – Injection

A1 – Injection

A2 – Broken Auth & Session Management

A2 – Broken Auth & Session Mgmt.

A3 – Cross Site Scripting (XSS)

A3 – Sensitive Data Exposure

A4 – Insecure Direct Object References

A4 – XML External Entities

A5 – Broken Access Control

A5 – Security Misconfiguration

A6 – Security Misconfiguration

A6 – Sensitive Data Exposure

A7 – Cross Site Scripting (XSS)

Android hacking

bWAPP

Computer Science

CTF

Cybersecurity

DVWA

Electronics 101

Hack The Box

Labs

Mutillidae

Opsec

OSCP Prep

Pentesting

Programming

Projects

Proving Grounds

Python

Python Projects

Research

Social Engineering

tech news

Tryhackme

Uncategorised

Vulnlab

Web Server Hacking

WebApp Hacking

Webgoat

Meta

Log in

Entries feed

Comments feed

WordPress.org

Who are we ?

Invent Your Shit is an online portal designed for hackers which helps them to learn ethical hacking and cybersecurity online for free. Join now and head-start your hacking journey with us.

Quick Navigation

- Home
- Privacy
- Whoami
- Contact

Contact Us

Contact here

Join community