Red Team Recon

Introduction

In this activity the learner is going to get to know how to use DNS, advanced searching, Recon-ng, and Maltego to collect information about the target.

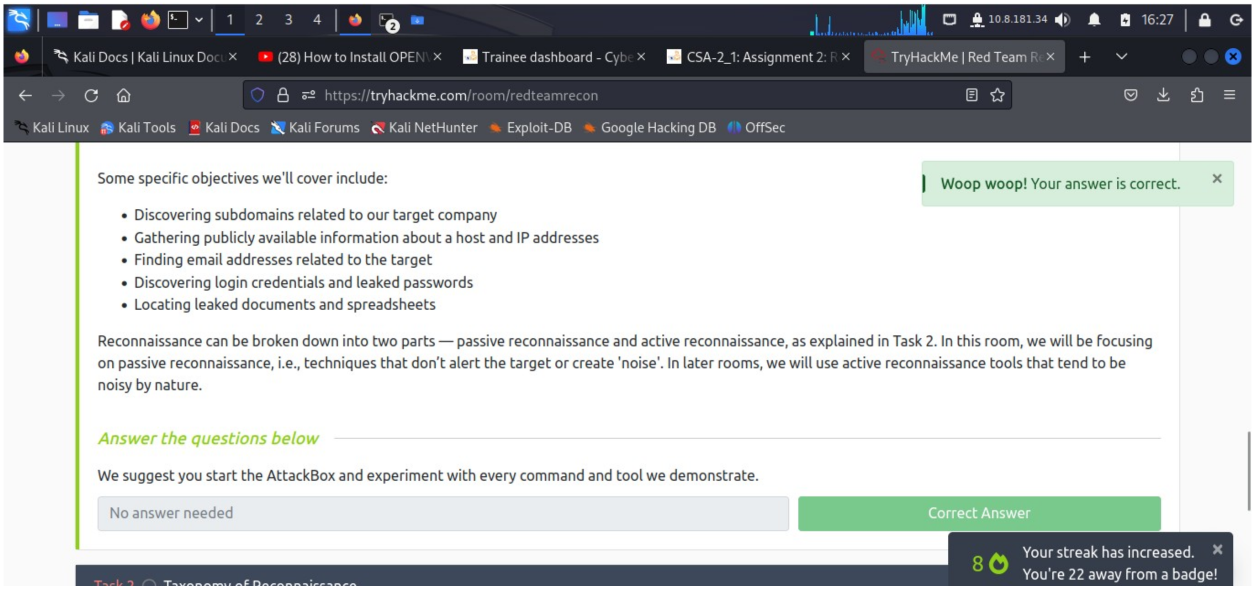
Before proceeding, what is Recon? Reconnaissance (recon) can be defined as a preliminary survey or observation of your target (client) without alerting them to your activities.

The activities to be learnt are as outlined in the following:

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

Activities

Task 1: Introduction



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

Correct Answer

Woop woop! Your answer is correct.

8 Your streak has increased. You're 22 away from a badge!

Task 2 ○ Taxonomy of Reconnaissance

Task 2: Taxonomy of Reconnaissance

Reconnaissance can be put into the following classifications:

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.

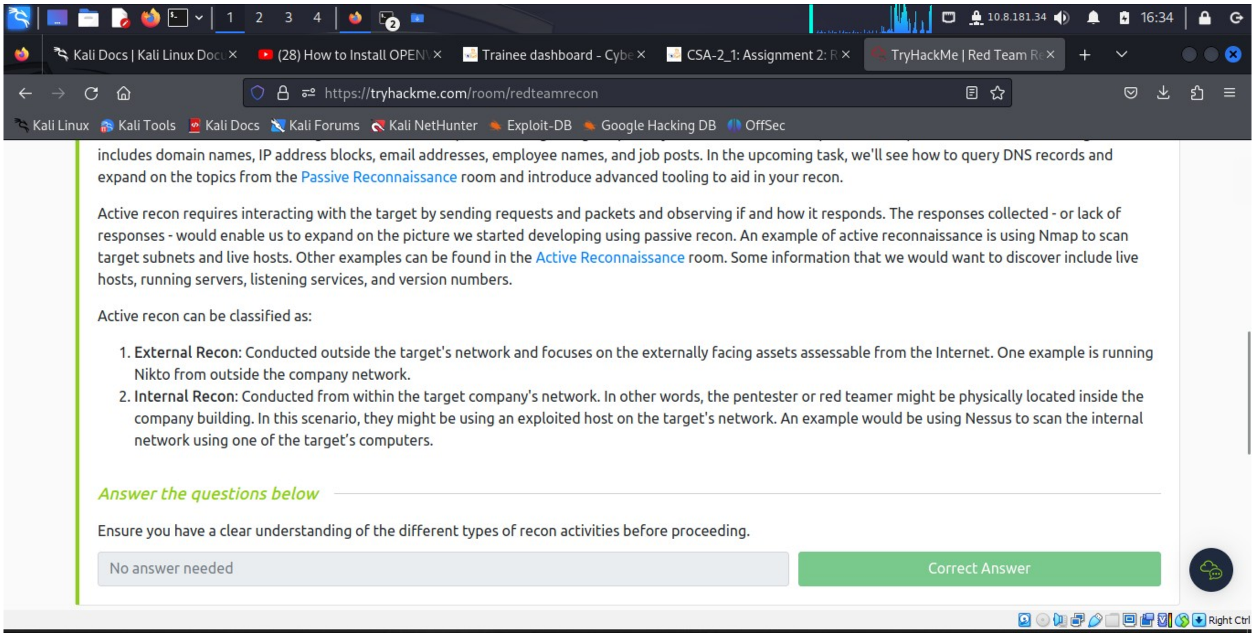
Passive recon doesn't require interacting with the target and relies on publicly available information that is collected and maintained by a third party.

Active recon requires interacting with the target by sending requests and packets and observing if and how it responds. An example of active reconnaissance is using Nmap to scan target subnets and live hosts.

Active recon can be classified as:

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.

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.



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

Correct Answer

Task 3: Built-in Tools

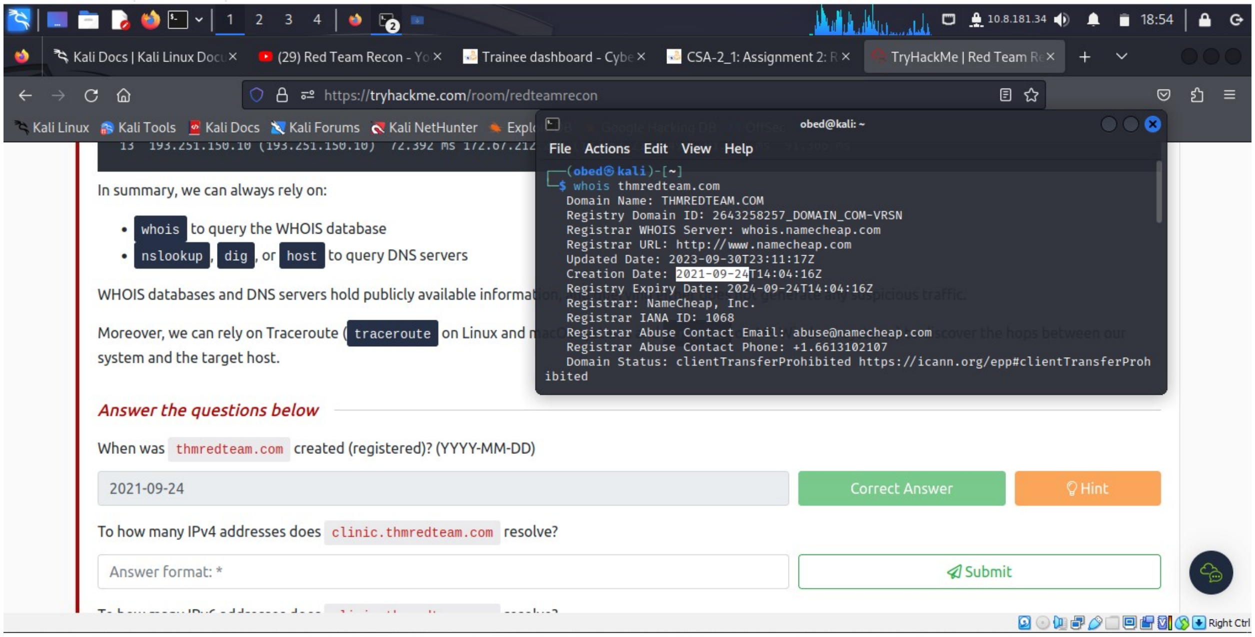
The learner, through this sub-task grasps the knowledge around whois; dig, nslookup, host; and traceroute/tracert.

Domain Information Groper (dig). **dig** provides a lot of query options and even allows you to specify a different DNS server to use.

Another concept is traceroute, or on MS Windows systems, tracert. As the name indicates, it traces the route taken by the packets from our system to the target host.

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 responsible for maintaining the WHOIS records for the domain names it is leasing. whois will query the WHOIS server to provide all saved records. In the following example, we can see 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)



```
13  193.251.150.10 (193.251.150.10)  72.392 ms 172.67.212
```

In summary, we can always rely on:

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

WHOIS databases and DNS servers hold publicly available informat

Moreover, we can rely on Traceroute (`traceroute` on Linux and mac
system and the target host.

Answer the questions below

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

2021-09-24

Correct Answer

Hint

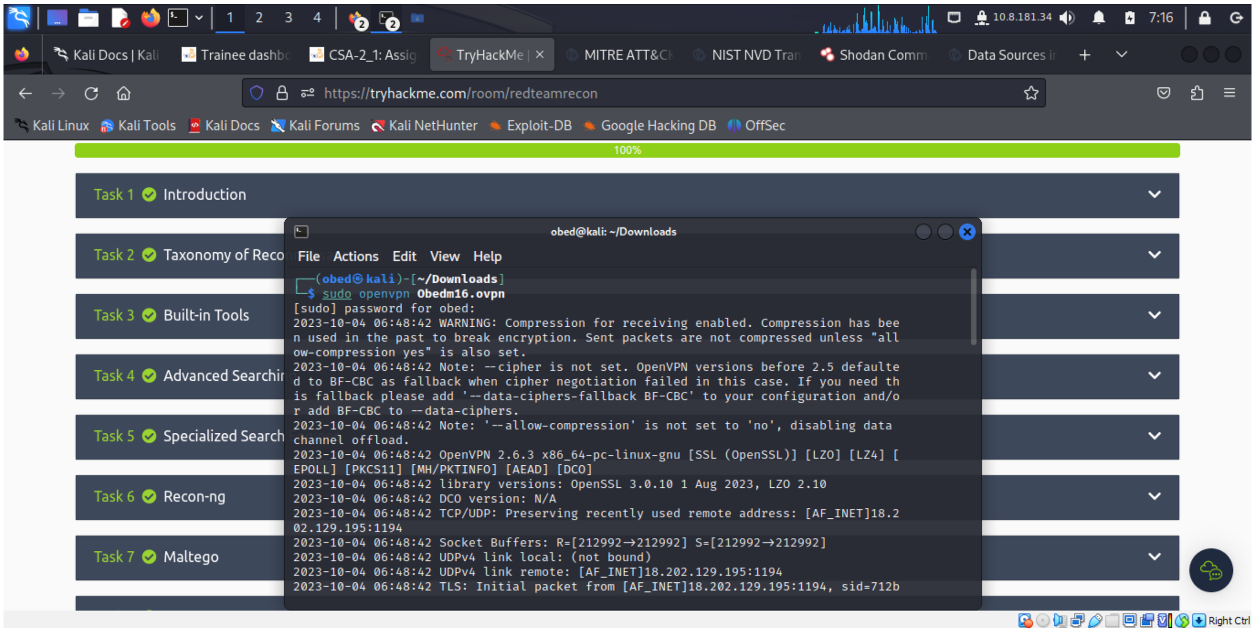
To how many IPv4 addresses does `clinic.thmredteam.com` resolve?

Answer format: *

Submit

```
┌──(obed㉿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#clientTransferProh
ibited
```

To be able to execute the practicalities the learner used a virtual device to initiate remote connection instead of using the other option of ‘Attackbox’.



https://tryhackme.com/room/redteamrecon

Task 1 Introduction

Task 2 Taxonomy of Reco

Task 3 Built-in Tools

Task 4 Advanced Searchi

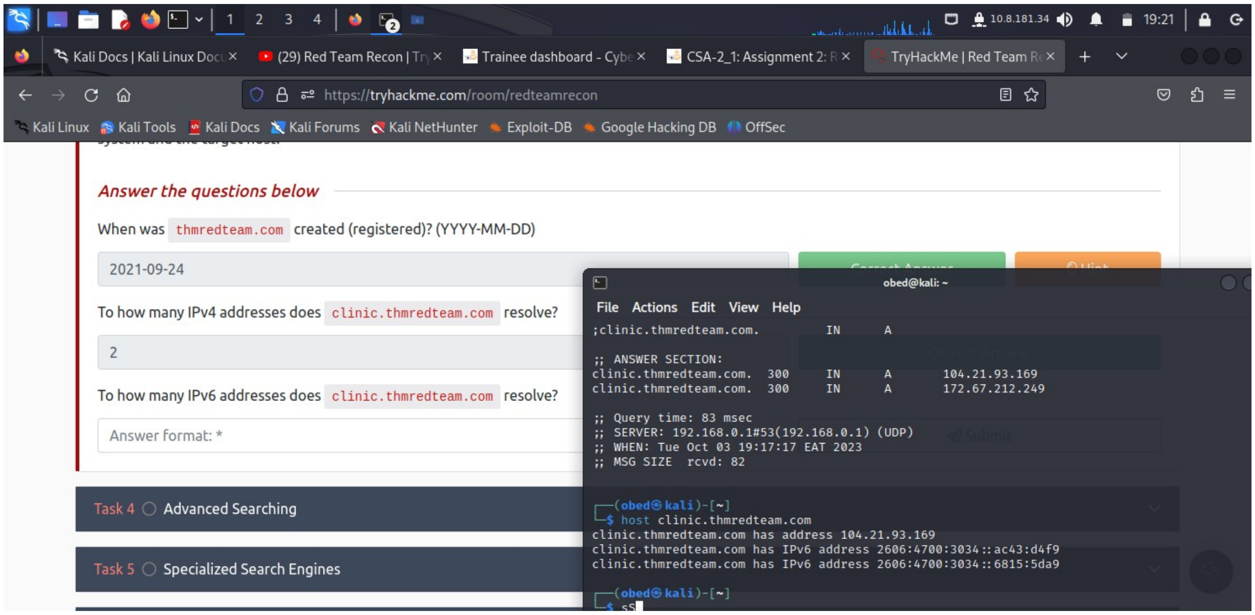
Task 5 Specialized Search

Task 6 Recon-ng

Task 7 Maltego

obed@kali: ~/Downloads

```
┌──(obed㉿kali)-[~/Downloads]
└─$ sudo openvpn Obedm16.ovpn
[sudo] password for obed:
2023-10-04 06:48:42 WARNING: Compression for receiving enabled. Compression has bee
n used in the past to break encryption. Sent packets are not compressed unless "all
ow-compression yes" is also set.
2023-10-04 06:48:42 Note: --cipher is not set. OpenVPN versions before 2.5 defaulte
d to BF-CBC as fallback when cipher negotiation failed in this case. If you need th
is fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/o
r add BF-CBC to --data-ciphers.
2023-10-04 06:48:42 Note: '--allow-compression' is not set to 'no', disabling data
channel offload.
2023-10-04 06:48:42 OpenVPN 2.6.3 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [
EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2023-10-04 06:48:42 library versions: OpenSSL 3.0.10 1 Aug 2023, LZO 2.10
2023-10-04 06:48:42 DCO version: N/A
2023-10-04 06:48:42 TCP/UDP: Preserving recently used remote address: [AF_INET]18.2
02.129.195:1194
2023-10-04 06:48:42 Socket Buffers: R=[212992->212992] S=[212992->212992]
2023-10-04 06:48:42 UDPv4 link local: (not bound)
2023-10-04 06:48:42 UDPv4 link remote: [AF_INET]18.202.129.195:1194
2023-10-04 06:48:42 TLS: Initial packet from [AF_INET]18.202.129.195:1194, sid=712b
```



https://tryhackme.com/room/redteamrecon

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?

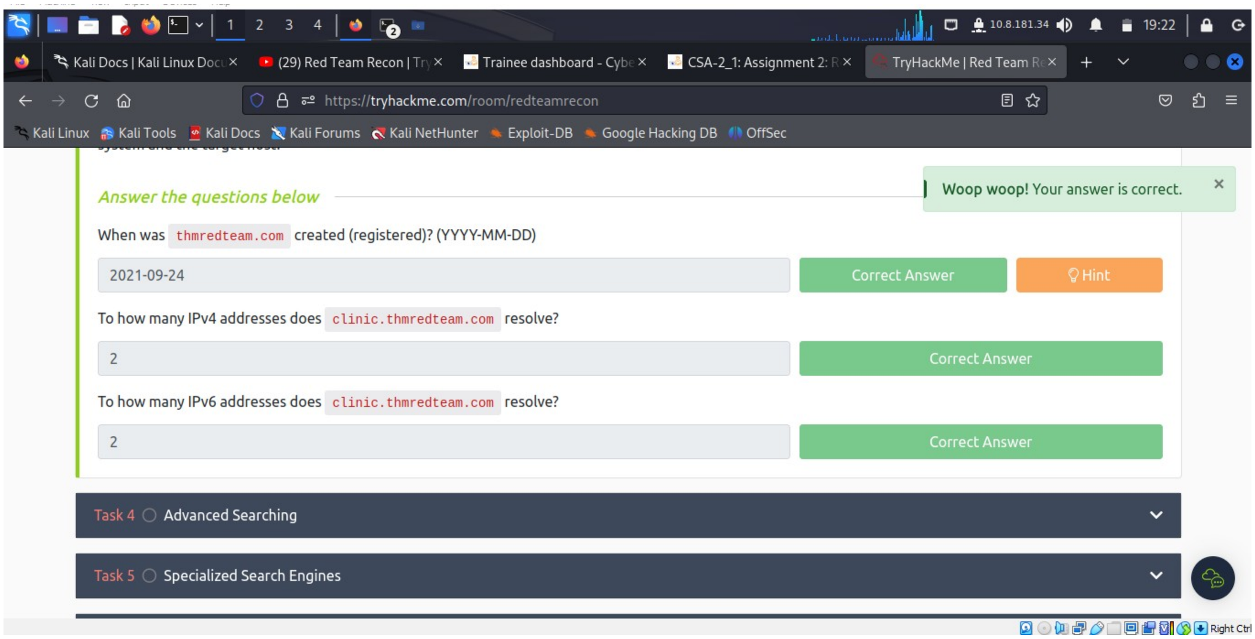
Answer format: *

Task 4 Advanced Searching

Task 5 Specialized Search Engines

obed@kali: ~

```
;clinic.thmredteam.com.         IN      A

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

;; Query time: 83 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Tue Oct 03 19:17:17 EAT 2023
;; MSG SIZE  rcvd: 82

┌──(obed㉿kali)-[~]
└─$ host clinic.thmredteam.com
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

┌──(obed㉿kali)-[~]
└─$ ss
```



Answer the questions below

Woop woop! Your answer is correct.

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

2021-09-24

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

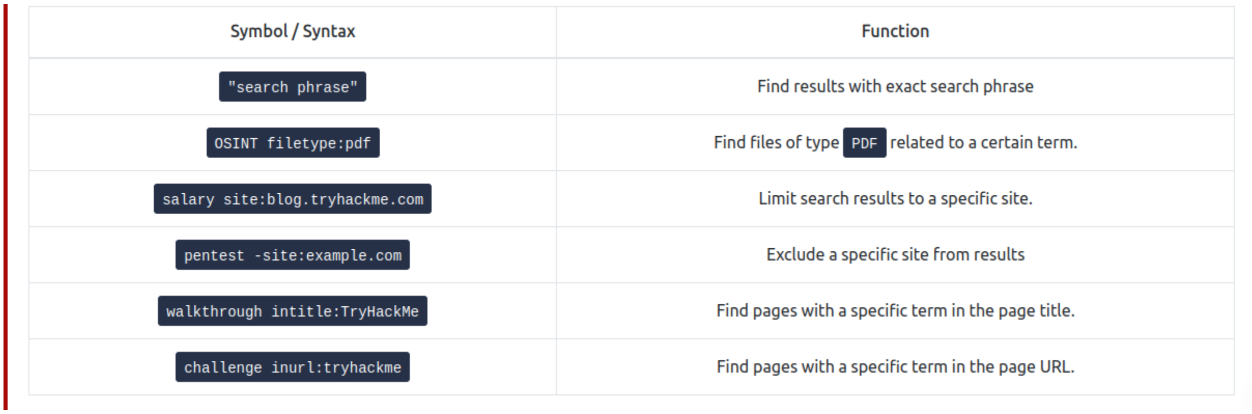
2

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

2

Task 4: Advanced Searching

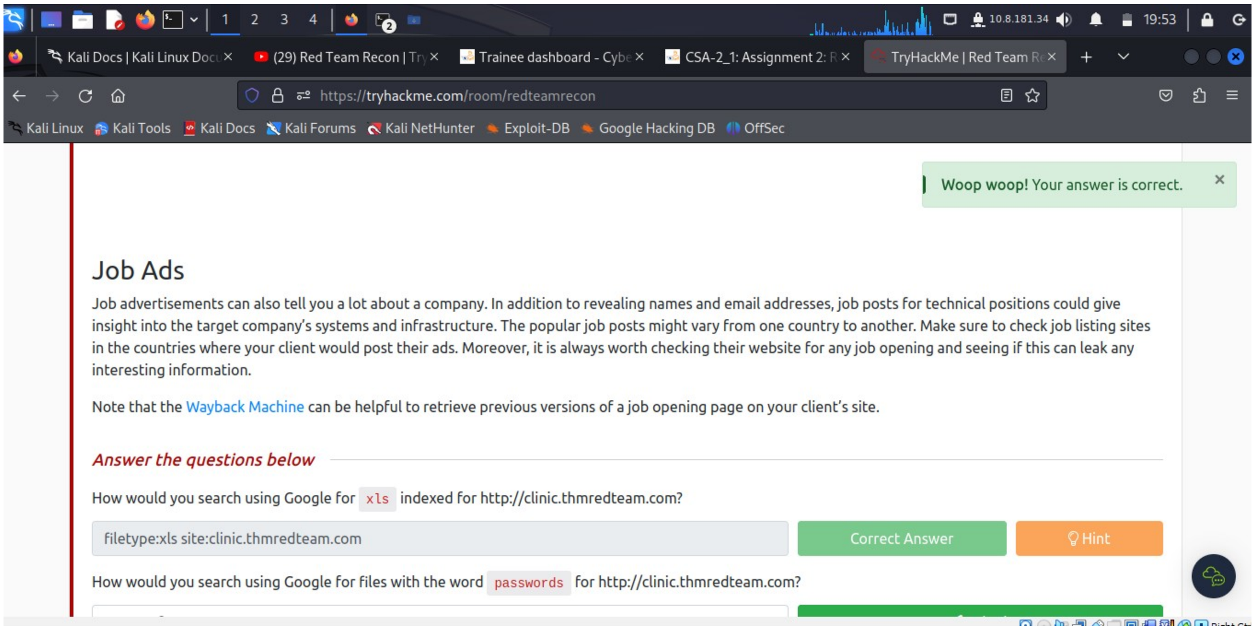
Being able to use a search engine efficiently is a crucial skill. In this module the learner goes through popular search modifiers:



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.

Search engines crawl the world wide web day and night to index new web pages and files.

Besides that, the learner undertakes the task of understanding sources that can provide valuable information without interacting with the target. These are Social Media and job Ads.



Woop woop! Your answer is correct.

Job Ads

Job advertisements can also tell you a lot about a company. In addition to revealing names and email addresses, job posts for technical positions could give insight into the target company's systems and infrastructure. The popular job posts might vary from one country to another. Make sure to check job listing sites in the countries where your client would post their ads. Moreover, it is always worth checking their website for any job opening and seeing if this can leak any interesting information.

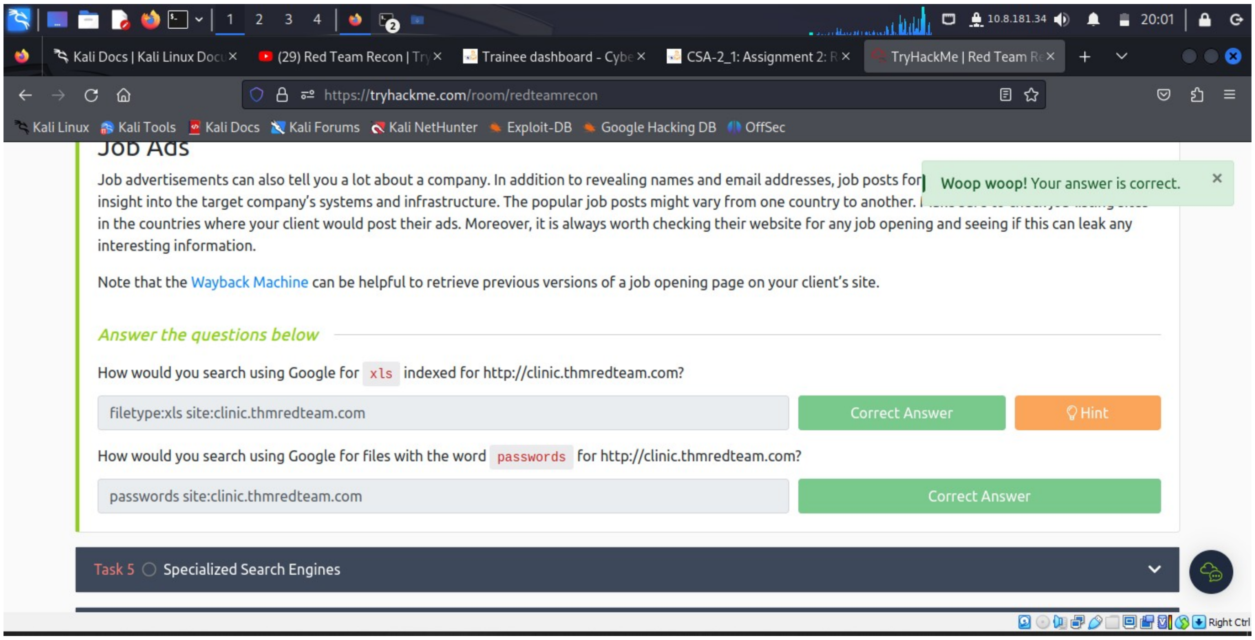
Note that the Wayback Machine can be helpful to retrieve previous versions of a job opening page on your client's site.

Answer the questions below

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

filetype:xls site:clinic.thmredteam.com

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



Job Ads

Woop woop! Your answer is correct.

Job advertisements can also tell you a lot about a company. In addition to revealing names and email addresses, job posts for technical positions could give insight into the target company's systems and infrastructure. The popular job posts might vary from one country to another. I
in the countries where your client would post their ads. Moreover, it is always worth checking their website for any job opening and seeing if this can leak any interesting information.

Note that the Wayback Machine can be helpful 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?

filetype:xls site:clinic.thmredteam.com

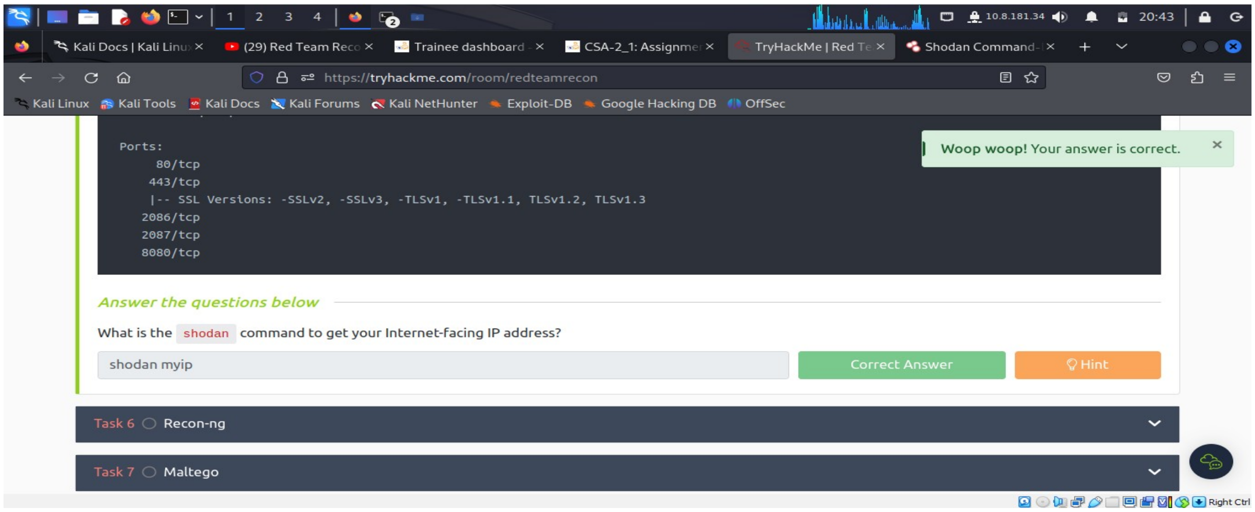
How would you search using Google for files with the word `passwords` for http://clinic.thmredteam.com?

passwords site:clinic.thmredteam.com

Task 5: Specialized Search Engines

As a learner meets more 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.

A handful of websites offer advanced DNS services that are free to use, these include ViewDNS.info (offers *Reverse IP Lookup*) and 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).



```
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?

shodan myip

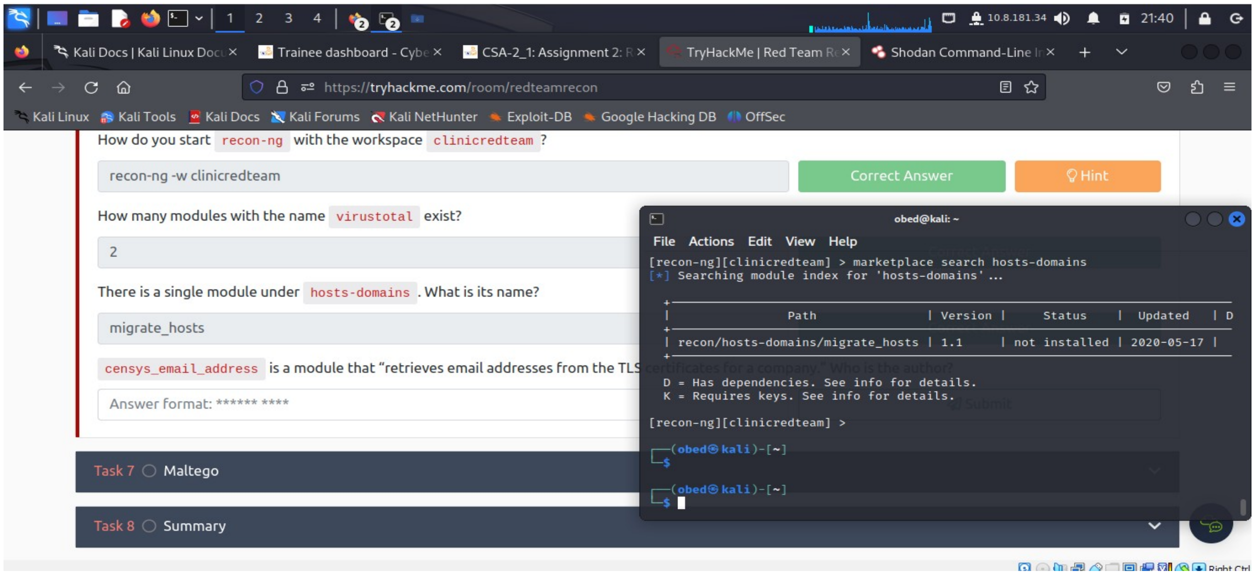
Task 6 ○ Recon-ng

Task 7 ○ Maltego

Task 6: Recon-ng

Recon-ng is a framework that helps automate the OSINT work. 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 task, we will demonstrate using Recon-ng in the terminal.

Recon-ng can be used to find various bits and pieces of information that can aid in an operation or OSINT task. All the data collected is automatically 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.



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_hosts

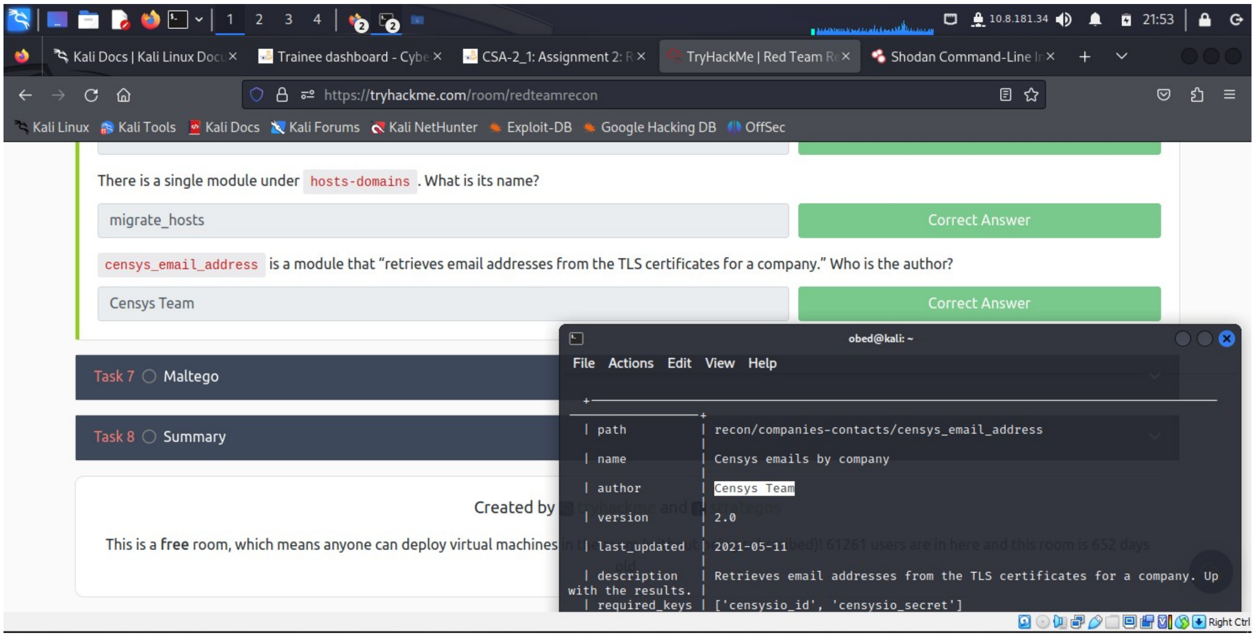
`censys_email_address` is a module that "retrieves email addresses from the TLS certificates for a company." Who is the author?

Answer format: ****** ****

Task 7 ○ Maltego

Task 8 ○ Summary

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

  +-----------------------------------------------------------------------------
  |                Path                | Version |     Status    |  Updated   | D
  +-----------------------------------------------------------------------------
  | 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] >

┌──(obed㉿kali)-[~]
└─$

┌──(obed㉿kali)-[~]
└─$ 
```



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

Task 8 ○ Summary

Created by

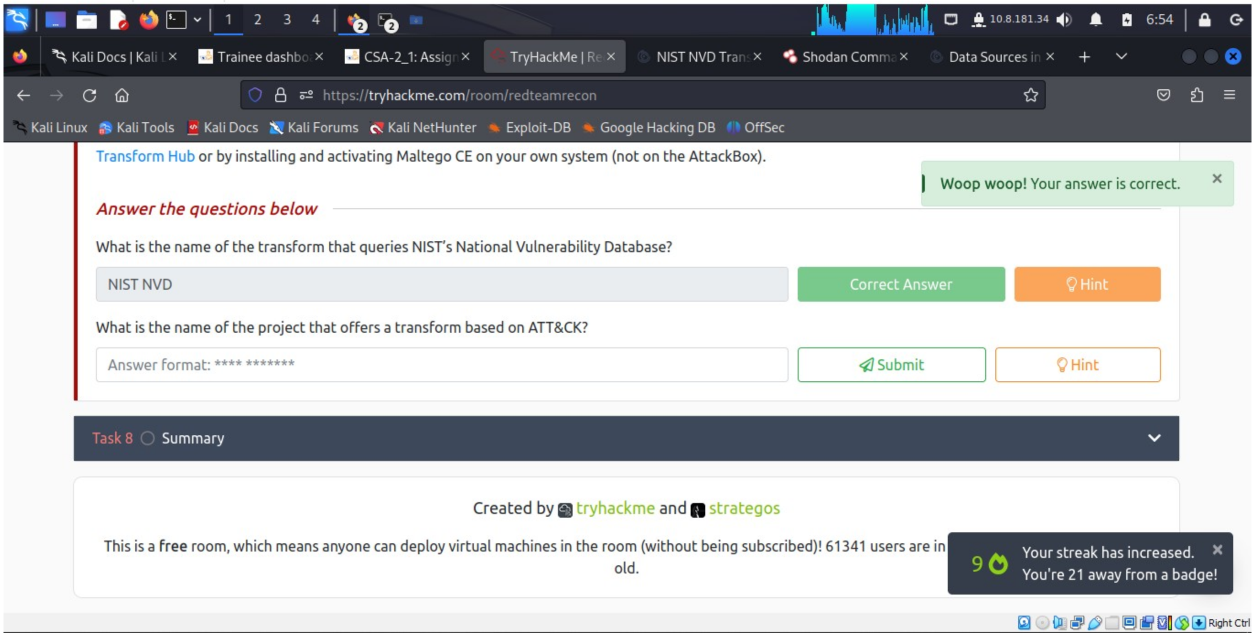
This is a free room, which means anyone can deploy virtual machines

```
obed@kali: ~
 | 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. Up
with the results. |
 | required_keys | ['censysio_id', 'censysio_secret']
```

Task 7: 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.

The information collected in Maltego 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.



Transform Hub or by installing and activating Maltego CE on your own system (not on the AttackBox).

Woop woop! Your answer is correct.

Answer the questions below

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

NIST NVD

Correct Answer

Hint

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

Answer format: **** *******

Submit

Hint

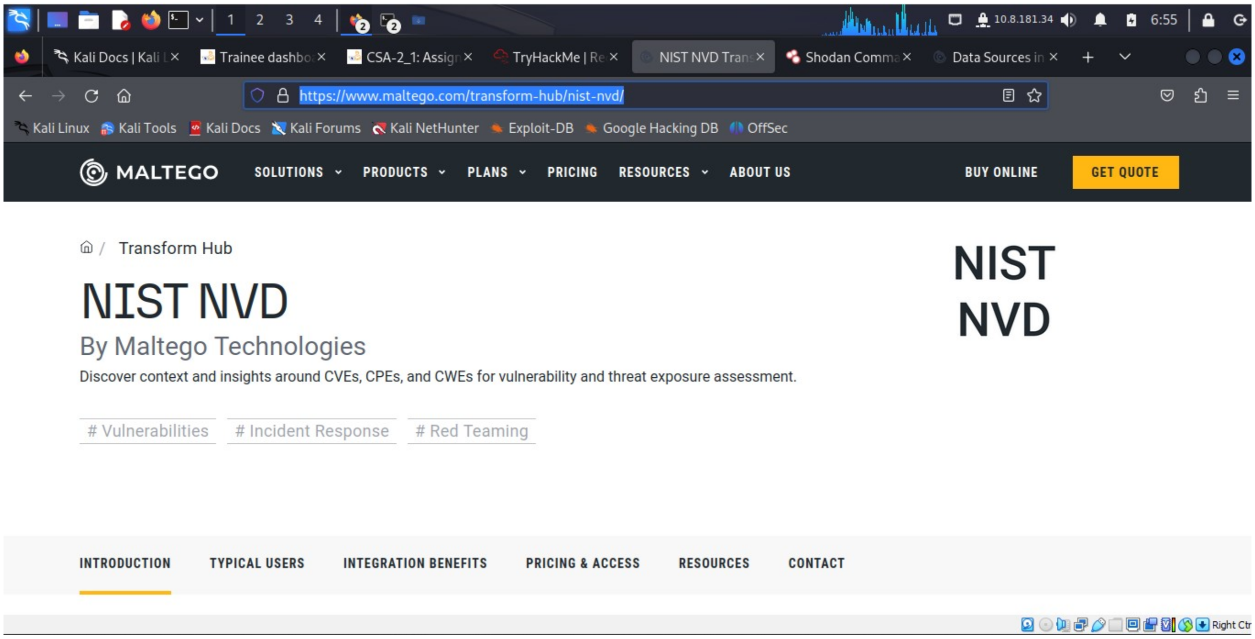
Task 8 ○ Summary

Created by tryhackme and strategos

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 61341 users are in old.

9 Your streak has increased. You're 21 away from a badge!

The above result is achieved by only visiting the Maltego official website and learn resources available, as it can be seen below.



Transform Hub

NIST NVD

By Maltego Technologies

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

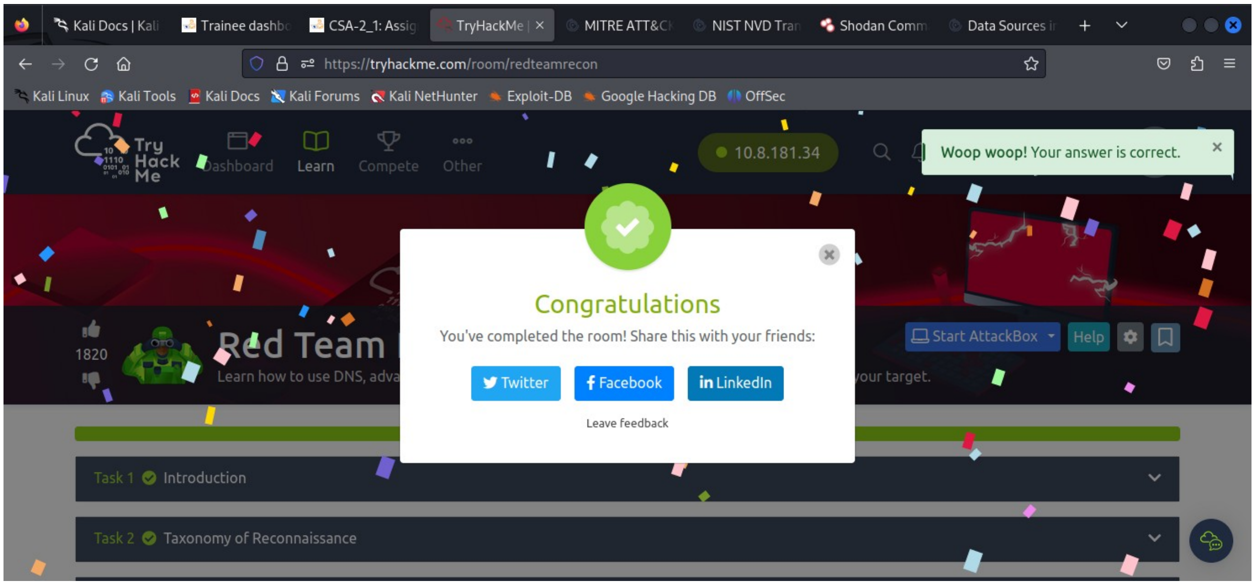
Vulnerabilities # Incident Response # Red Teaming

NIST NVD

Task 8: Summary

This activity reminds the learner on how to know about the "enemy" or where to initiate the attack session.

In the cyber warfare era; in addition to the learner knowing red team skillset and capabilities, they need to gain as much information about the target as possible.



Woop woop! Your answer is correct.

Congratulations

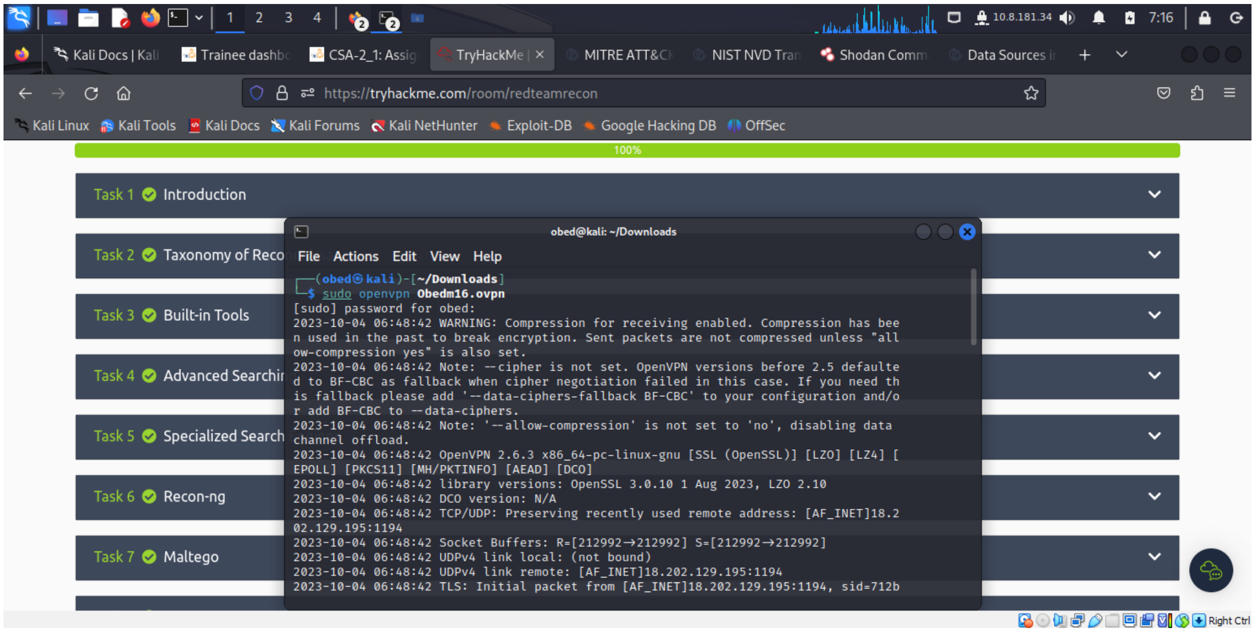
You've completed the room! Share this with your friends:

Red Team

Learn how to use DNS, adva ... our target.

Task 1 Introduction

Task 2 Taxonomy of Reconnaissance



```
┌──(obed㉿kali)-[~/Downloads]
└─$ sudo openvpn Obedm16.ovpn
[sudo] password for obed:
2023-10-04 06:48:42 WARNING: Compression for receiving enabled. Compression has bee
n used in the past to break encryption. Sent packets are not compressed unless "all
ow-compression yes" is also set.
2023-10-04 06:48:42 Note: --cipher is not set. OpenVPN versions before 2.5 defaulte
d to BF-CBC as fallback when cipher negotiation failed in this case. If you need th
is fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/o
r add BF-CBC to --data-ciphers.
2023-10-04 06:48:42 Note: '--allow-compression' is not set to 'no', disabling data
channel offload.
2023-10-04 06:48:42 OpenVPN 2.6.3 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [
EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2023-10-04 06:48:42 library versions: OpenSSL 3.0.10 1 Aug 2023, LZO 2.10
2023-10-04 06:48:42 DCO version: N/A
2023-10-04 06:48:42 TCP/UDP: Preserving recently used remote address: [AF_INET]18.2
02.129.195:1194
2023-10-04 06:48:42 Socket Buffers: R=[212992→212992] S=[212992→212992]
2023-10-04 06:48:42 UDPv4 link local: (not bound)
2023-10-04 06:48:42 UDPv4 link remote: [AF_INET]18.202.129.195:1194
2023-10-04 06:48:42 TLS: Initial packet from [AF_INET]18.202.129.195:1194, sid=712b
```

Conclusion