**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.

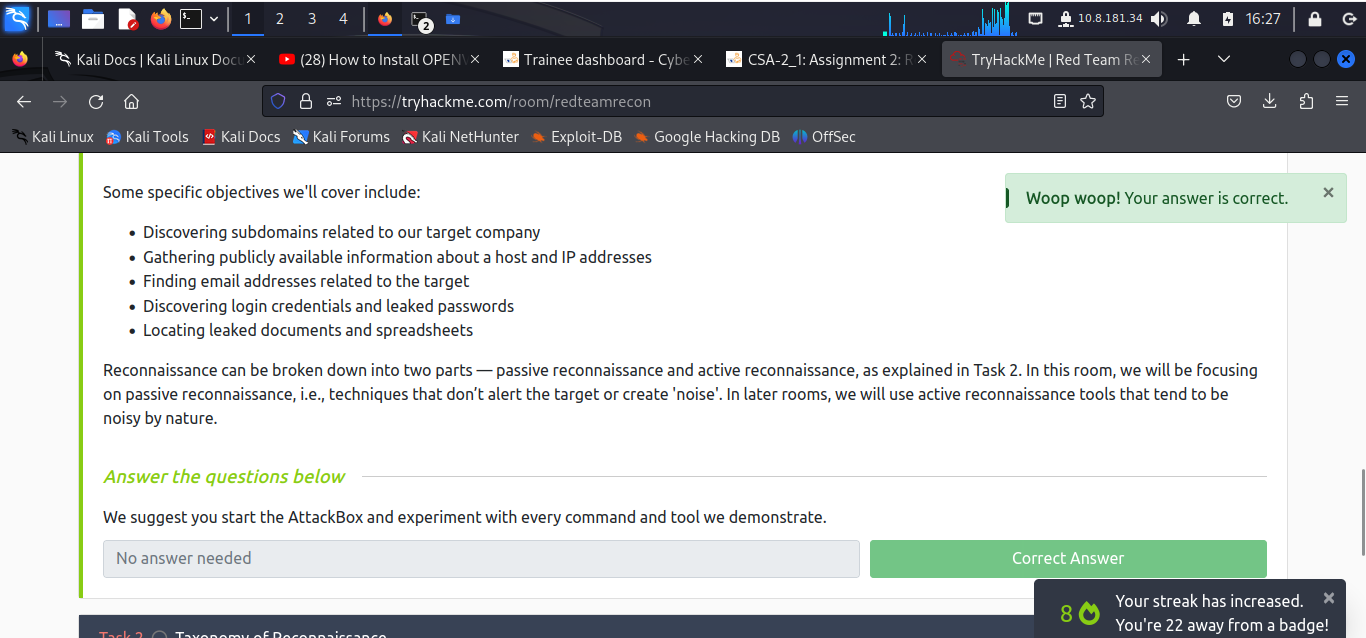
Before proceeding, what is Recon? Reconnaissance (recon) can be defined as a preliminary survey or observation of your target (client) without alerting them to your activities.

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***



***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.

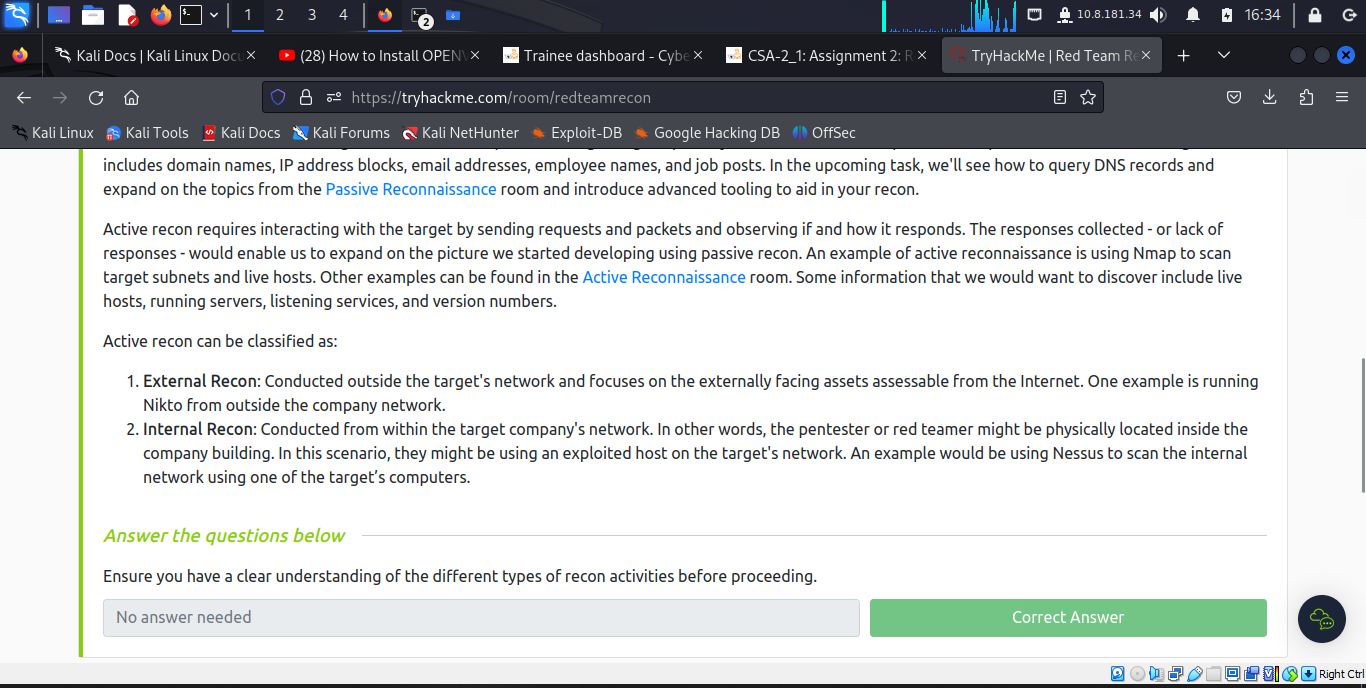
Passive recon doesn't require interacting with the target and relies on publicly available information that is collected and maintained by a third party.

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.



***Task 3: Built-in Tools***

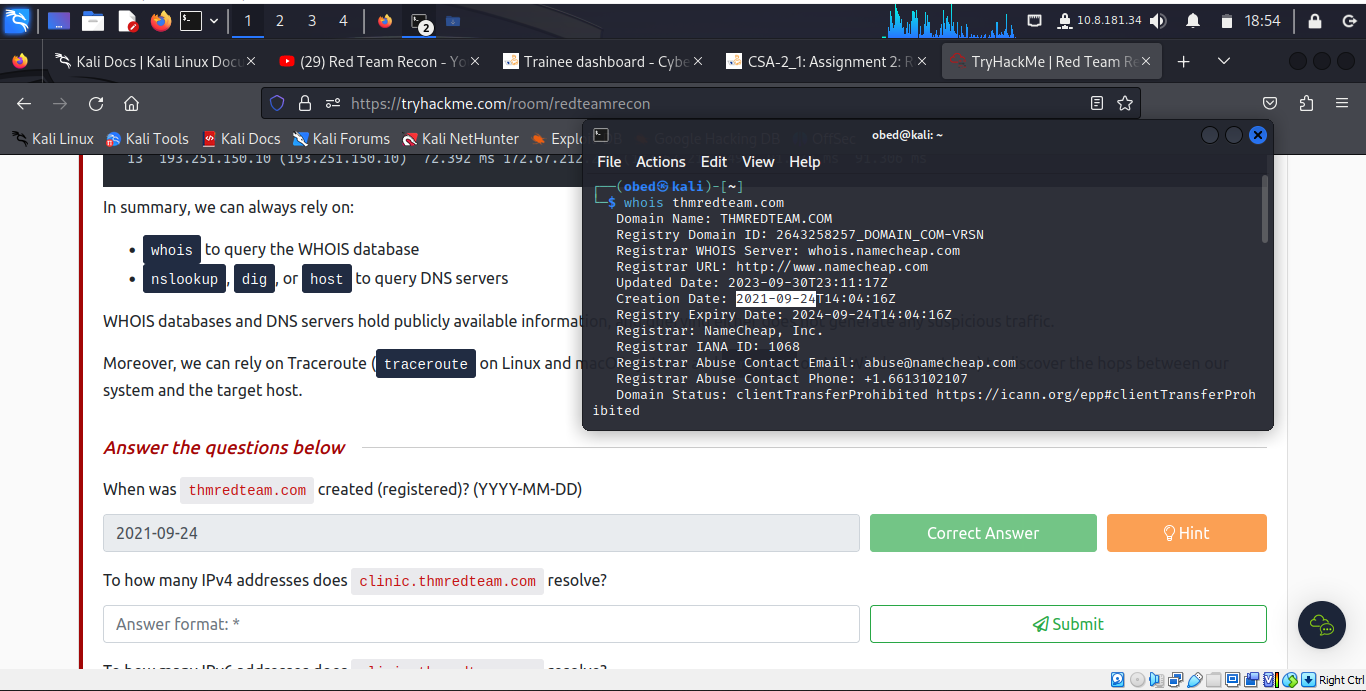
The learner, through this sub-task grasps the knowledge around whois; dig, nslookup, host; and traceroute/tracert.

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

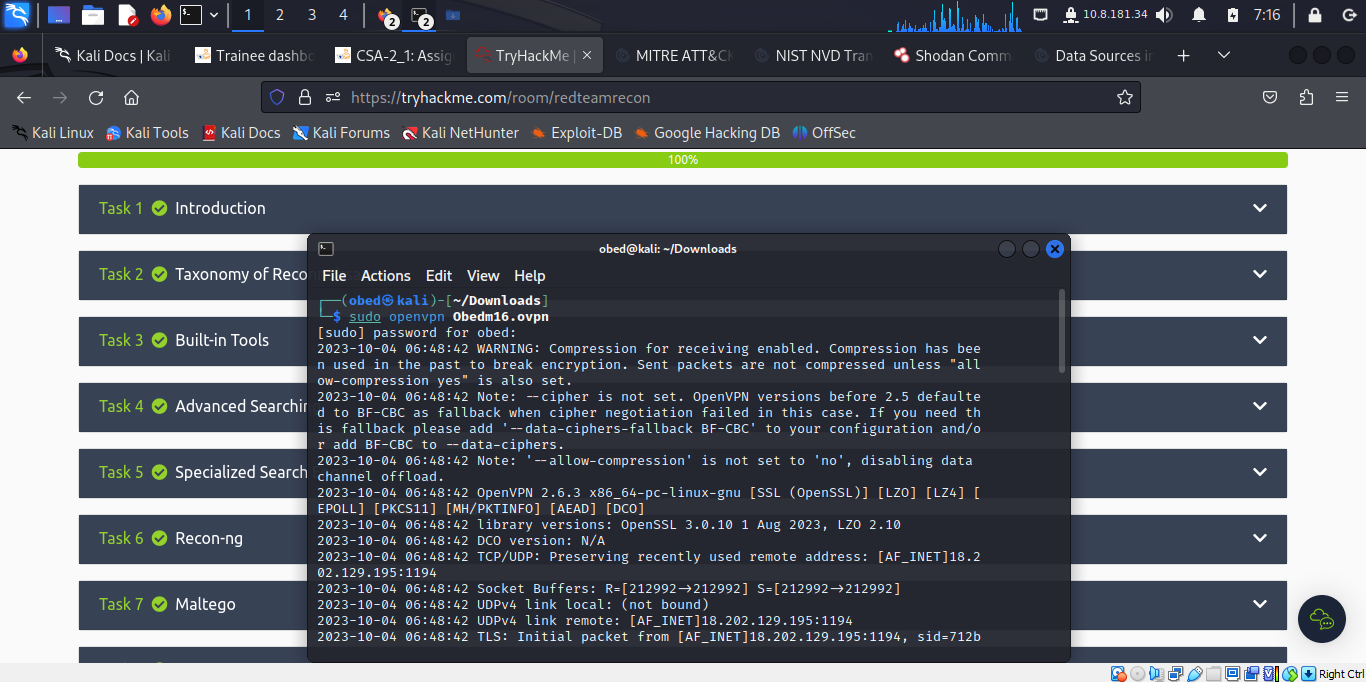
Another concept is traceroute, or on MS Windows systems, tracert. As the name indicates, it traces the route taken by the packets from our system to the target host.

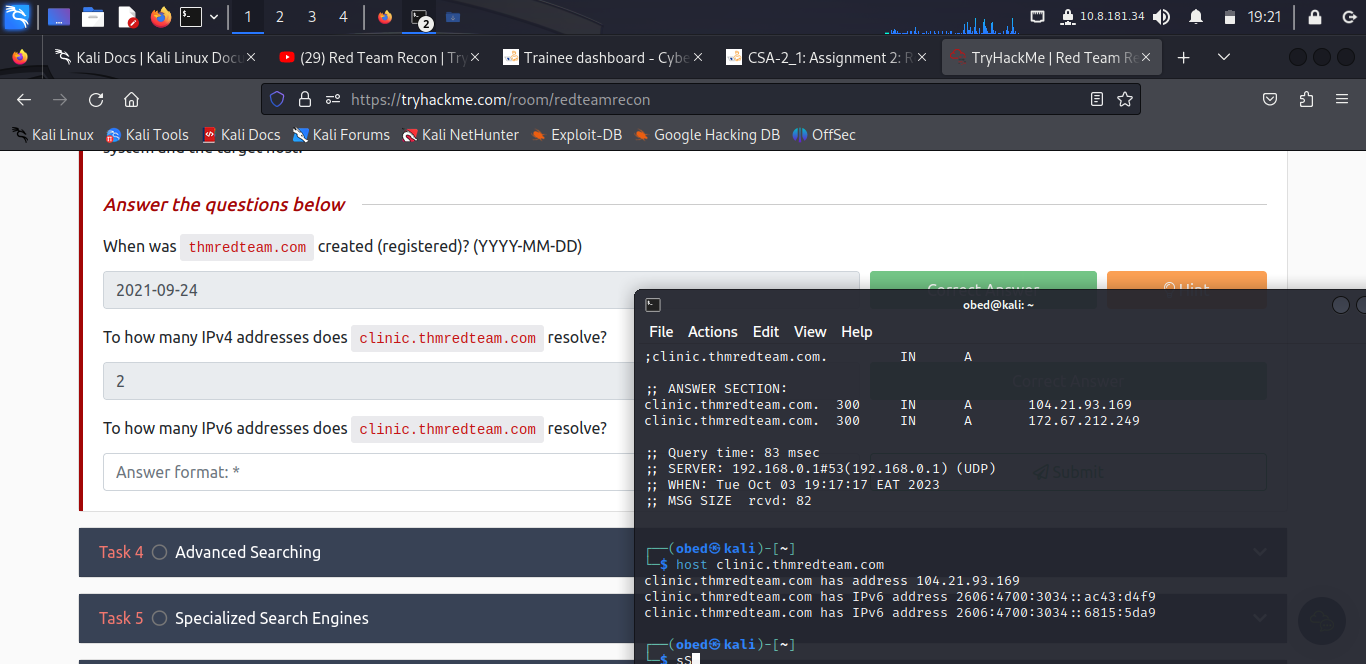
WHOIS is a request and response protocol that follows the [RFC 3912](https://www.ietf.org/rfc/rfc3912.txt) specification. A WHOIS server listens on TCP port 43 for incoming requests. The domain registrar is responsible for maintaining the WHOIS records for the domain names it is leasing. whois will query the WHOIS server to provide all saved records. In the following example, we can see whois provides us with:

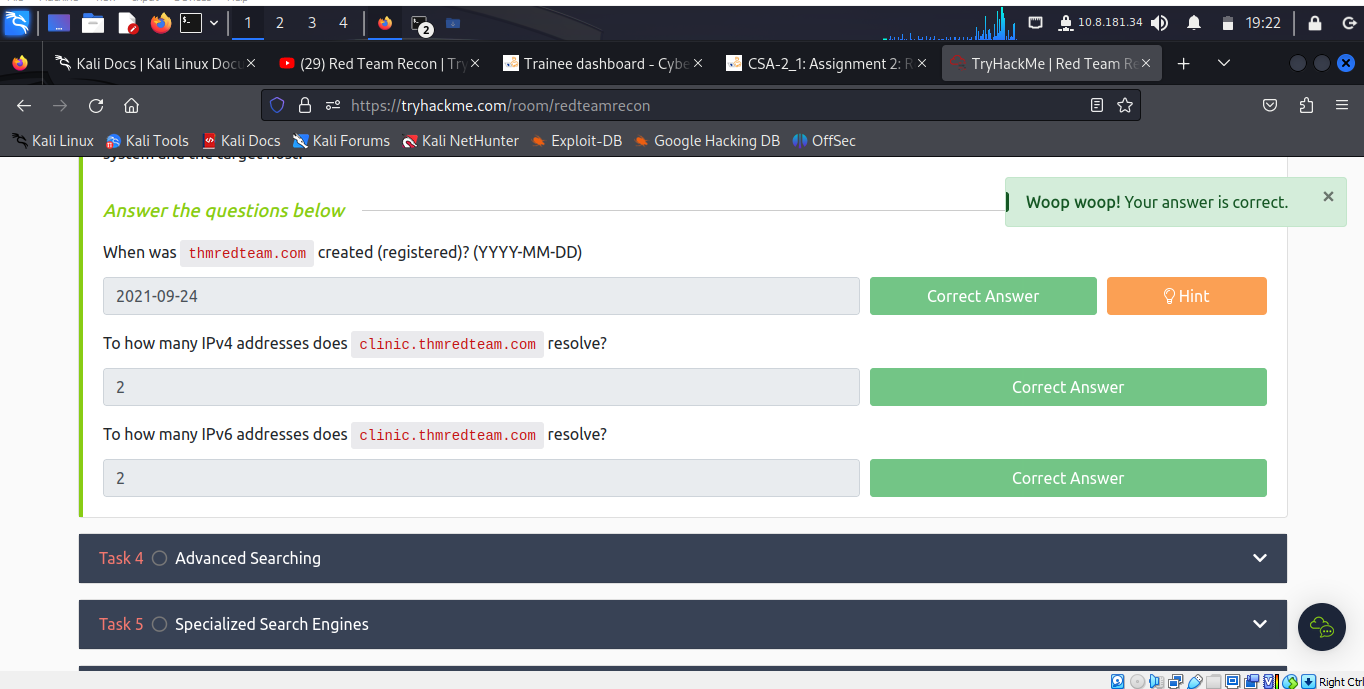
* Registrar WHOIS server
* Registrar URL
* Record creation date
* Record update date
* Registrant contact info and address (unless withheld for privacy)
* Admin contact info and address (unless withheld for privacy)
* Tech contact info and address (unless withheld for privacy)



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’.

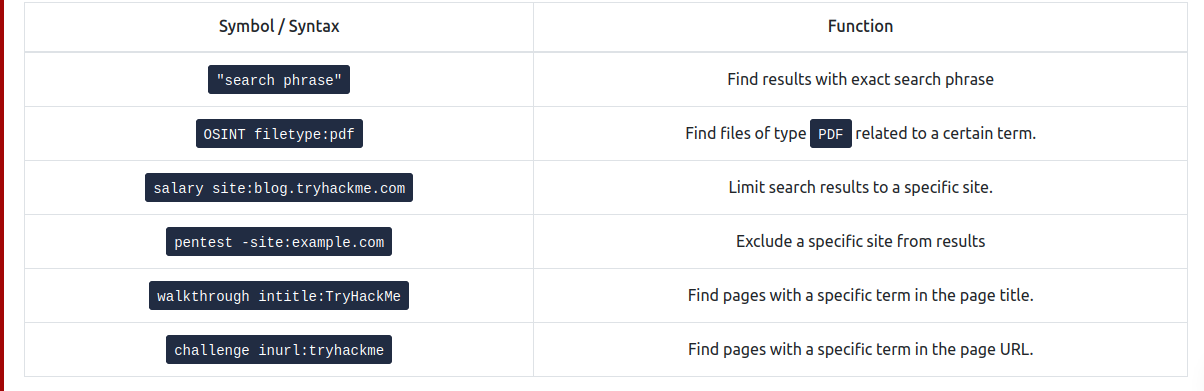






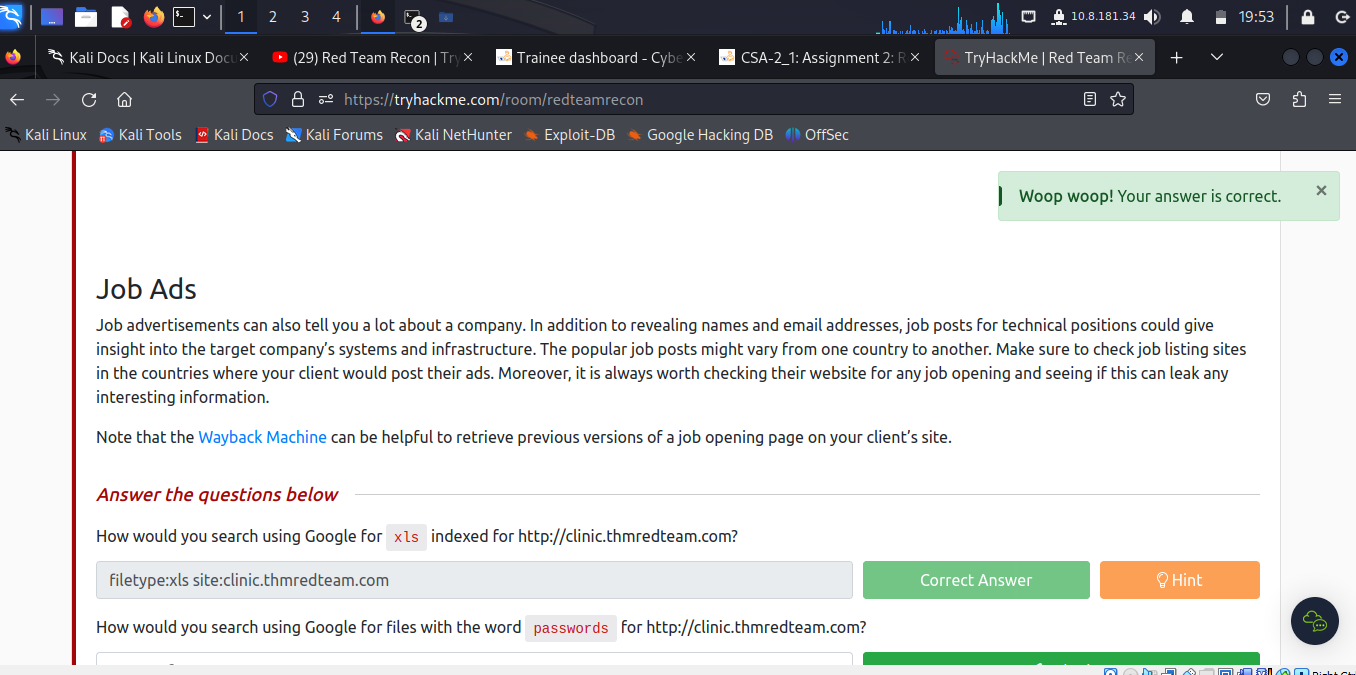
***Task 4: Advanced Searching***

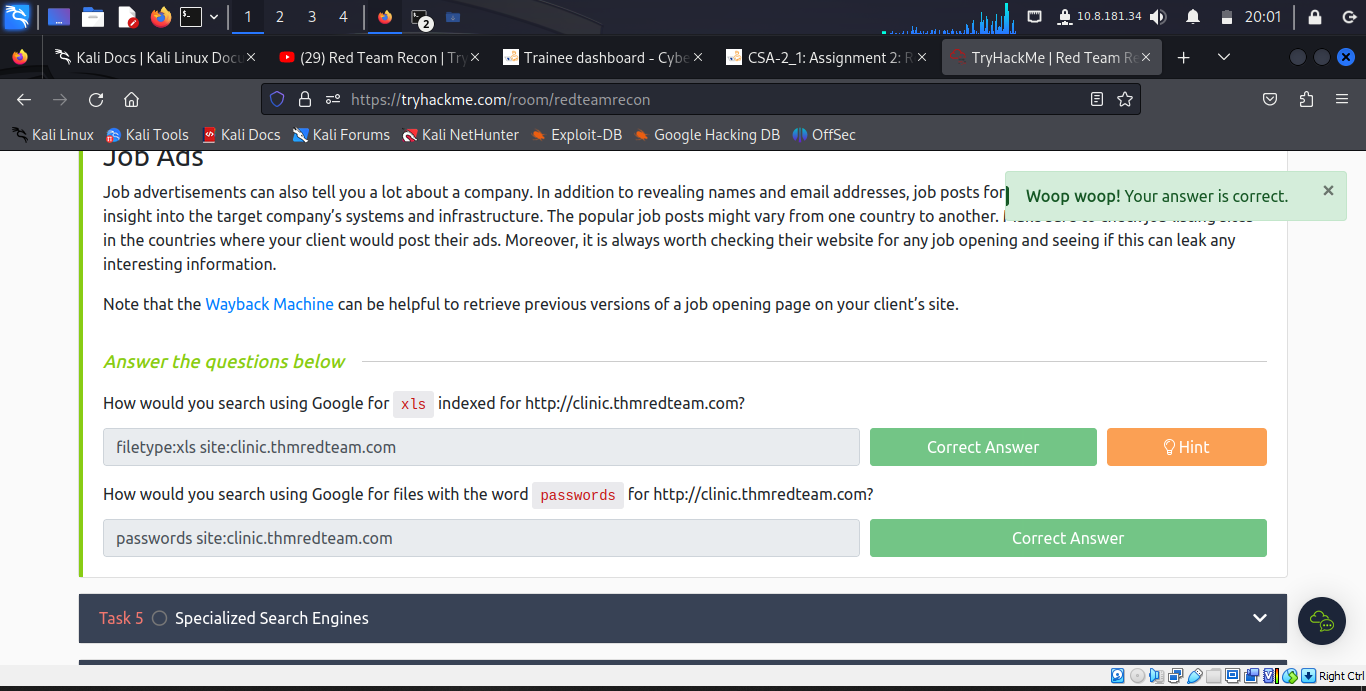
Being able to use a search engine efficiently is a crucial skill. In this module the learner goes through popular search modifiers:



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.

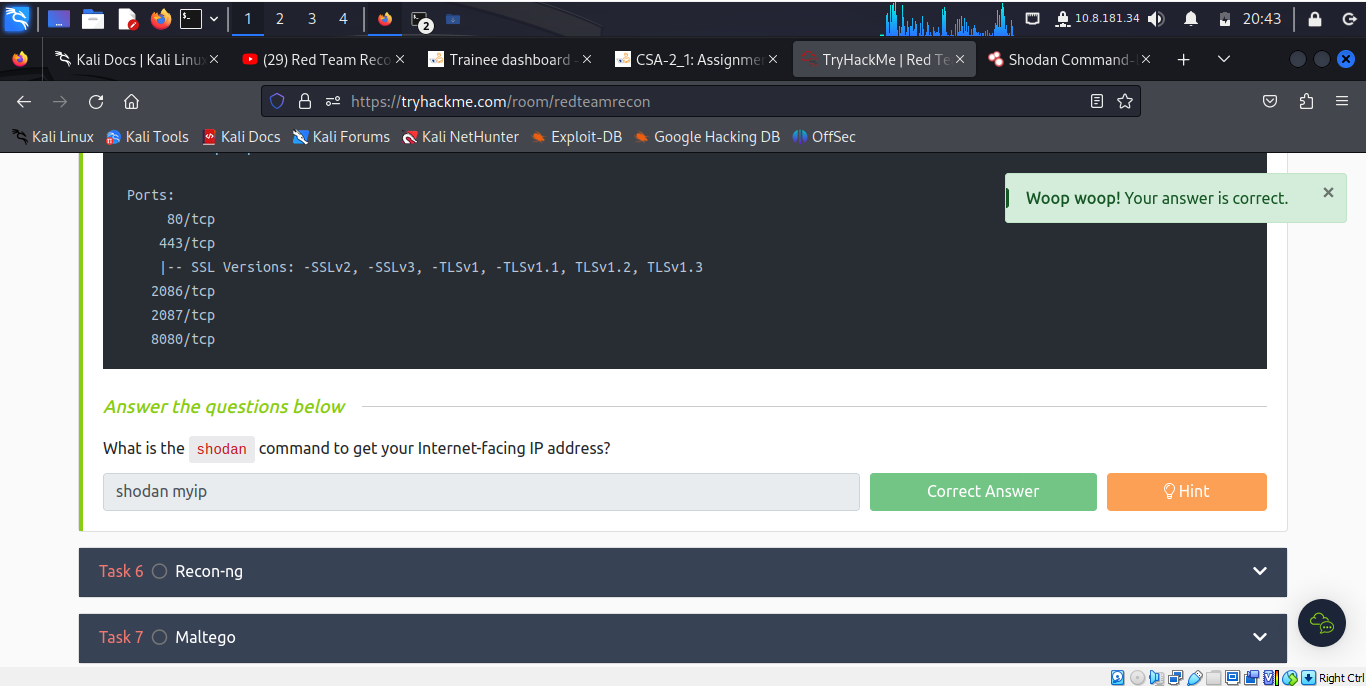




***Task 5: Specialized Search Engines***

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.

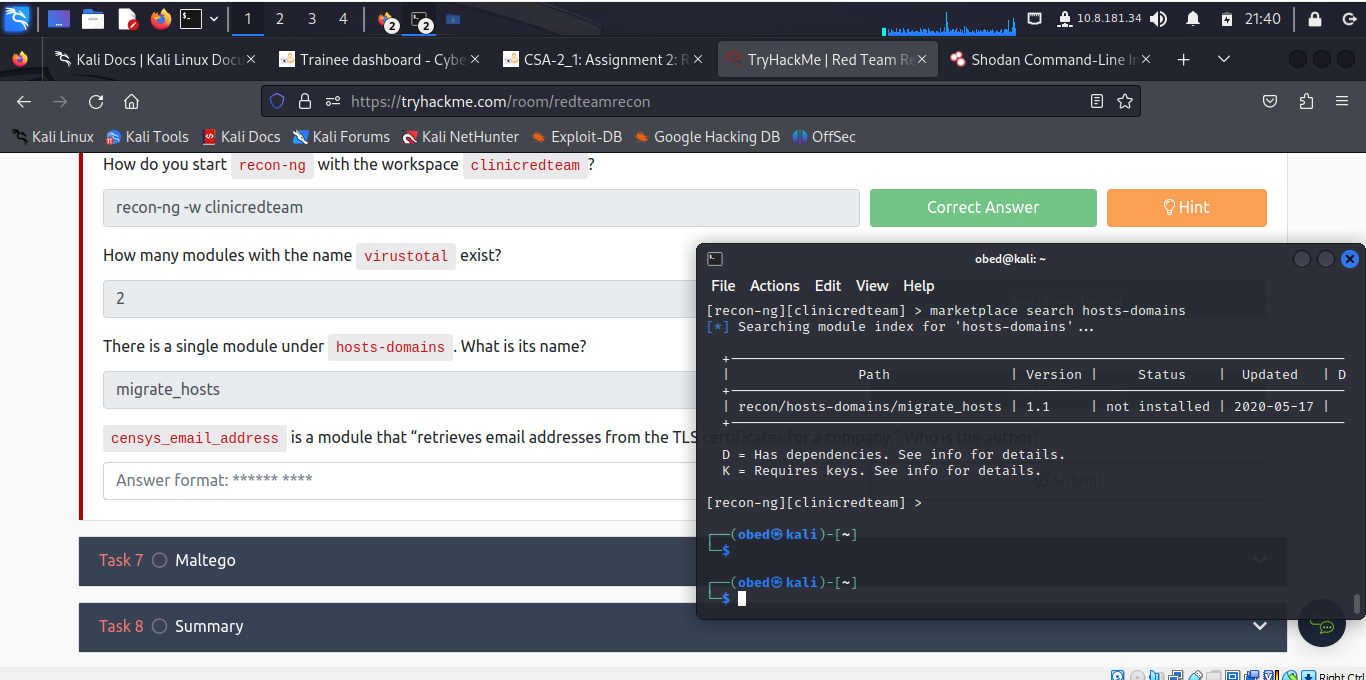
A handful of websites offer advanced DNS services that are free to use, these include ViewDNS.info (offers Reverse IP Lookup) and Threat Intelligence Platform (requires you to provide a domain name or an IP address, and it will launch a series of tests from malware checks to WHOIS and DNS queries).

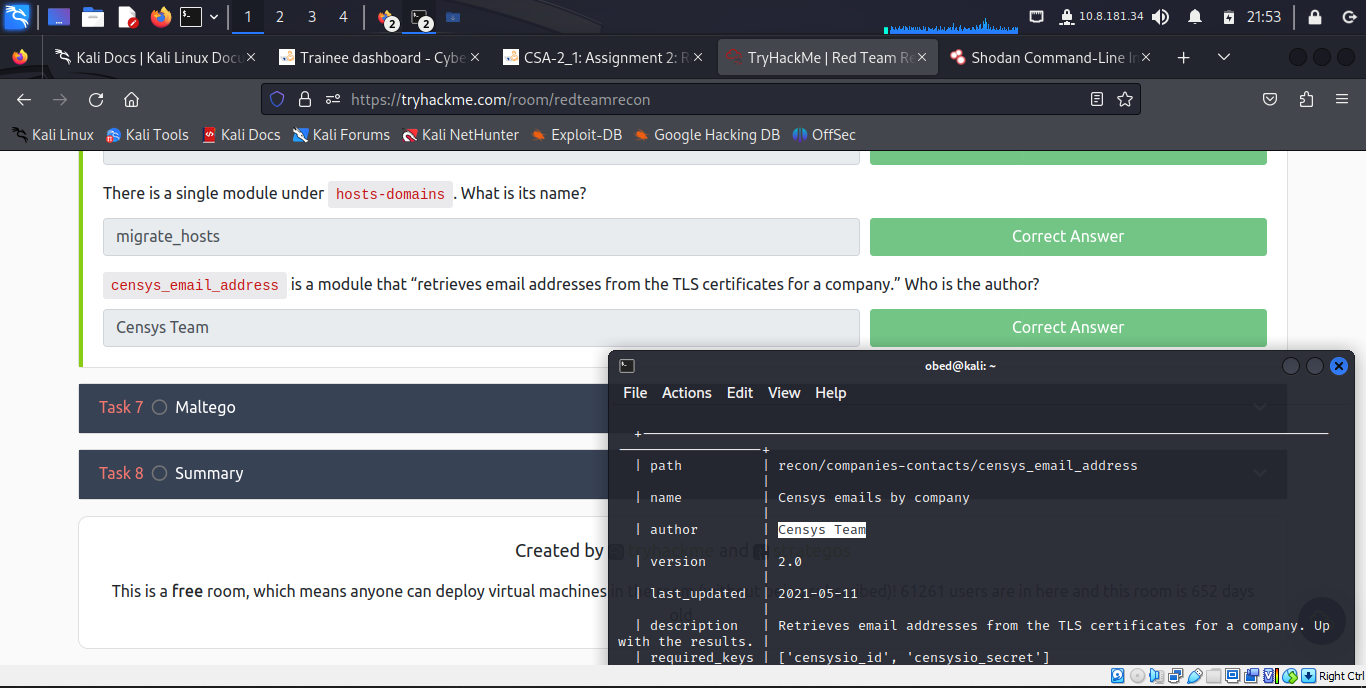


***Task 6: Recon-ng***

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.

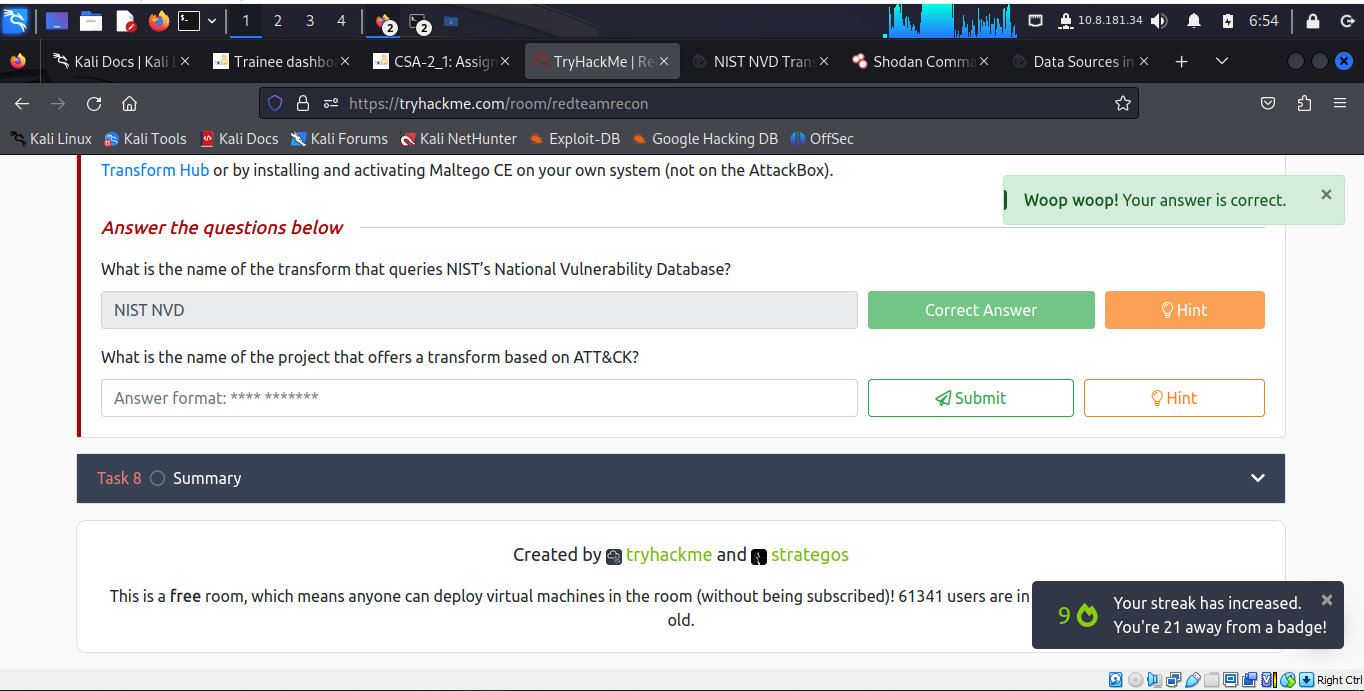




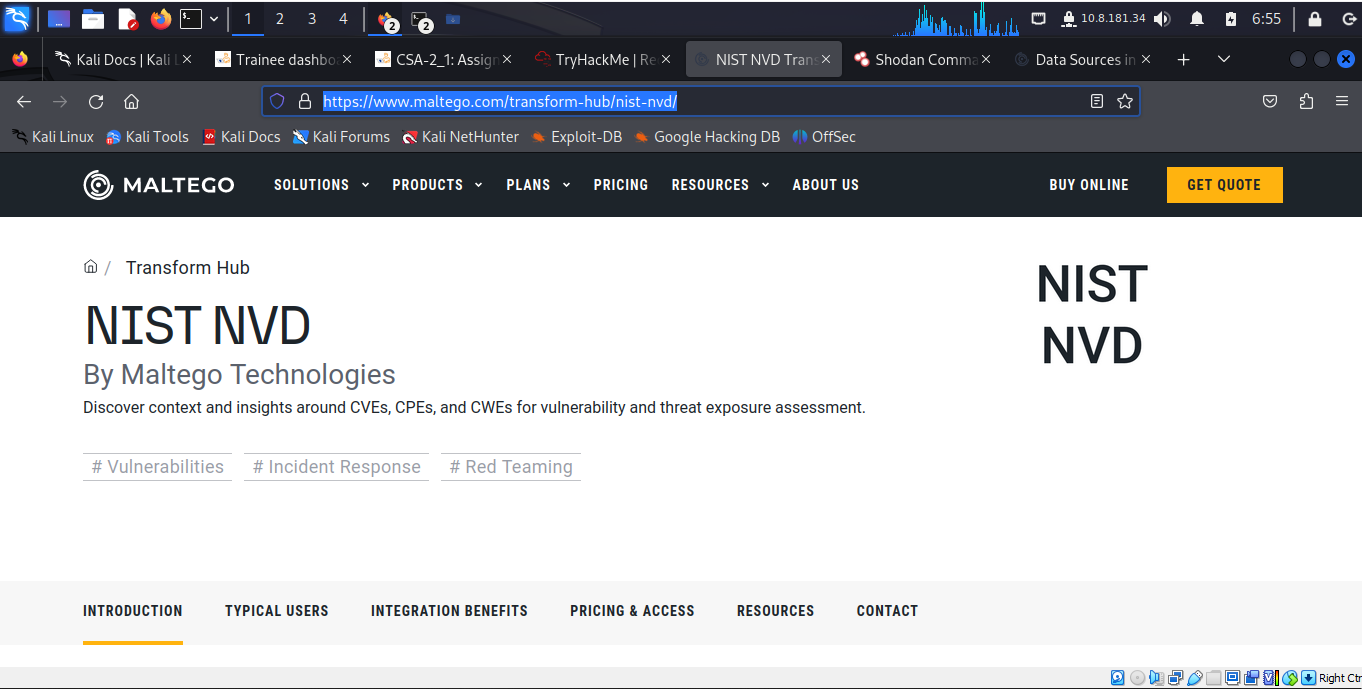
***Task 7: Maltego***

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.



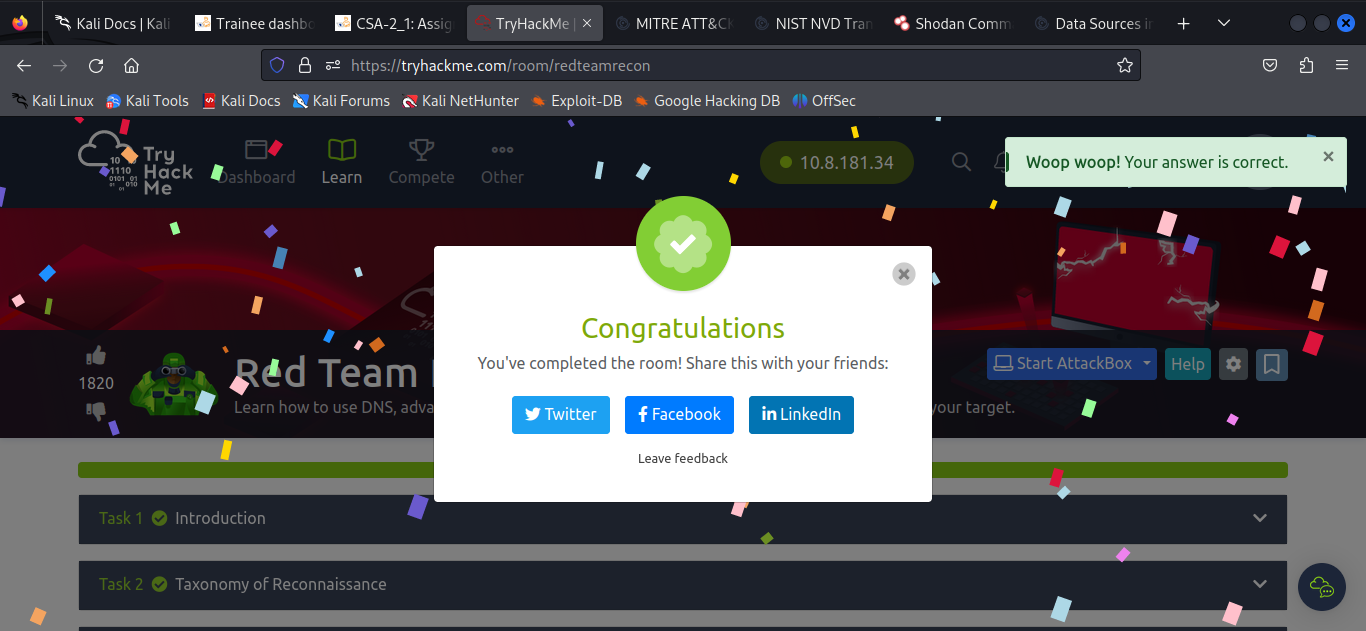
The above result is achieved by only visiting the Maltego official website and learn resources available, as it can be seen below.

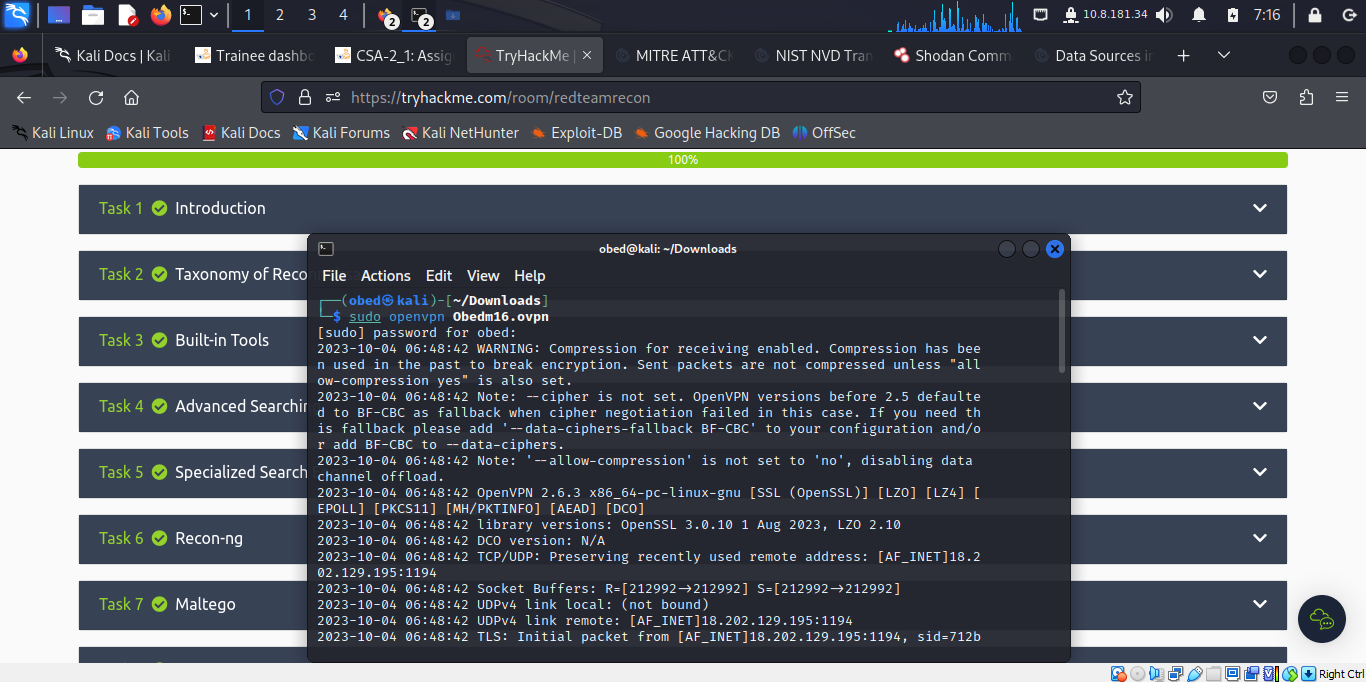


***Task 8: Summary***

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.





**Conclusion**