Introduction

Miyamoto Musashi's timeless strategy, "Know your enemy, know his sword," remains relevant in the digital age of cybersecurity. In the realm of red team operations, reconnaissance is crucial. It involves a preliminary survey or observation of a target without alerting them. This report delves into the various aspects of reconnaissance, focusing on passive techniques that gather information discreetly.

https://tryhackme.com/p/Damiano254

Task 1: Understanding Reconnaissance in Cybersecurity

Reconnaissance, or recon, is the first step in understanding a target's infrastructure and personnel. It is categorized into two primary types:

1. **Passive Reconnaissance**: Observing the target without direct interaction. It relies on publicly available information and is less likely to alert the target.

2. **Active Reconnaissance:** Involves direct interaction with the target to elicit responses, which can provide more detailed information but risks detection.

Covered Topics:

- Types of reconnaissance activities.
- WHOIS and DNS-based reconnaissance.
- Advanced searching techniques.
- Image-based searching.
- Google Hacking.
- Specialized search engines.
- Tools like Recon-ng and Maltego.

Task 2: Taxonomy of Reconnaissance

Reconnaissance is classified into passive and active, each with distinct characteristics:

- **Passive Recon:** Utilizes Open-Source Intelligence (OSINT) for information gathering without alerting the target. It includes analysing social media profiles, job posts, and domain information.
- **Active Recon:** Involves scanning and probing the target to observe responses, which can be external (outside the target's network) or internal (within the target's network).

Task 3: Built-in Tools for Reconnaissance

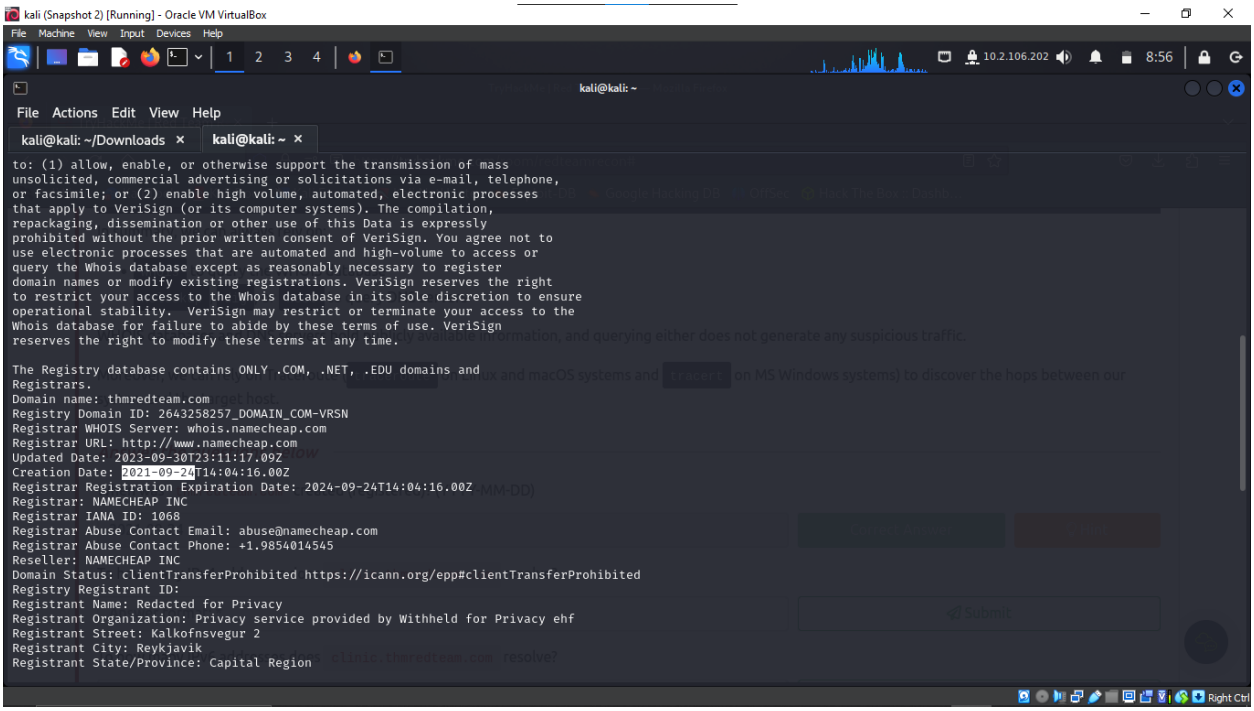
Several built-in tools aid in reconnaissance:

- **WHOIS**: Queries WHOIS databases for domain registration information.
- **dig, nslookup, host:** Tools for querying DNS records to find associated IP addresses and other DNS information.
- **traceroute/tracert:** Traces the packet's route from the source to the target, revealing the path and transit delays of packets.

Questions and Answers

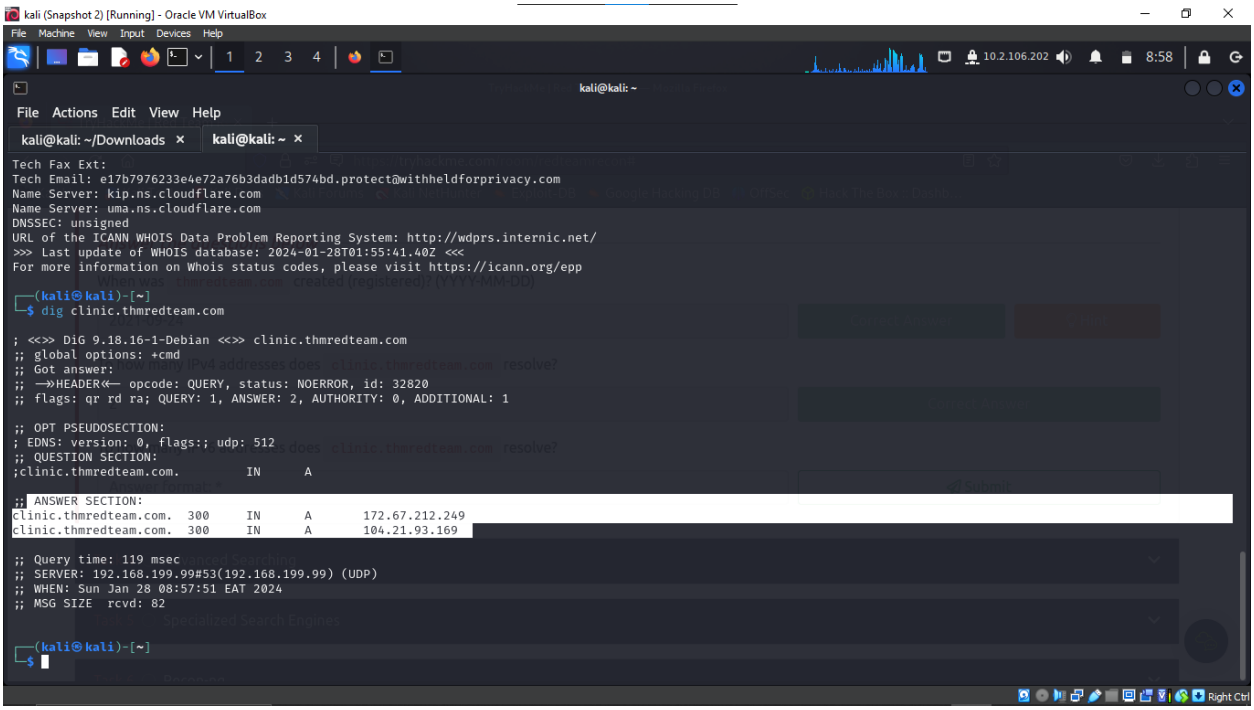
When was thmredteam.com created (registered)?

Answer: 2021-09-24



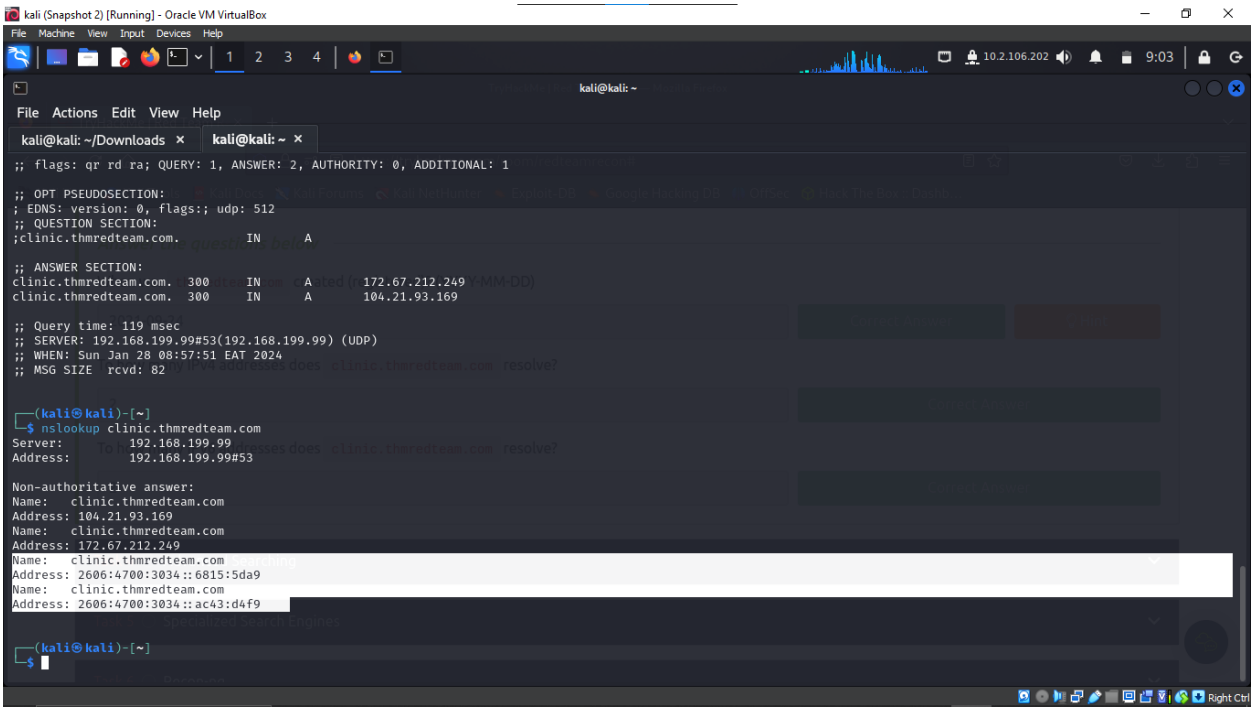
To how many IPv4 addresses does clinic.thmredteam.com resolve?

Answer: 2



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

Answer: 2



Task 4: Advanced Searching

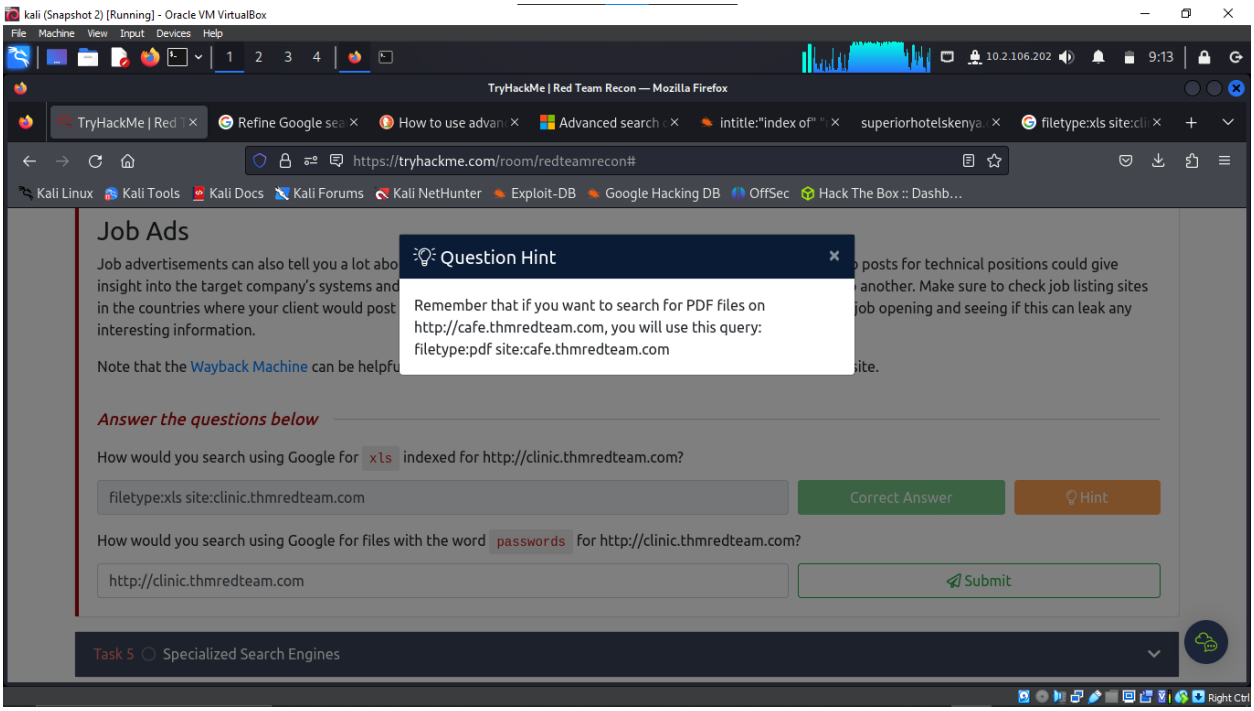
Efficient use of search engines is a key skill in reconnaissance:

- **Search Modifiers:** Techniques like using quotes for exact phrases, filetype for specific file types, site for limiting to a specific domain, and others enhance search precision.
- **Confidential Information:** Search engines can inadvertently index sensitive data, which can be discovered using advanced search techniques.

Questions and Answers

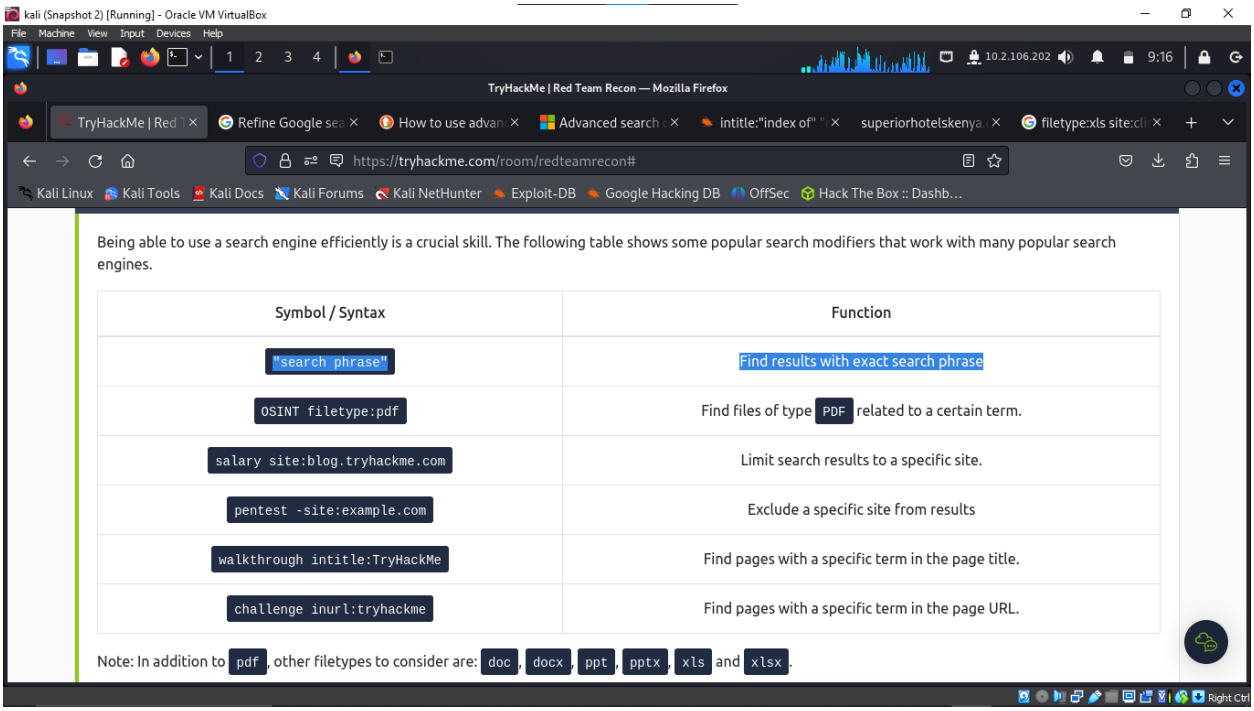
How would you search using Google for xls indexed for http://clinic.thmredteam.com?

Answer: filetype:xls site: clinic.thmredteam.com



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

Answer: passwords site: clinic.thmredteam.com



Task 5: Specialized Search Engines

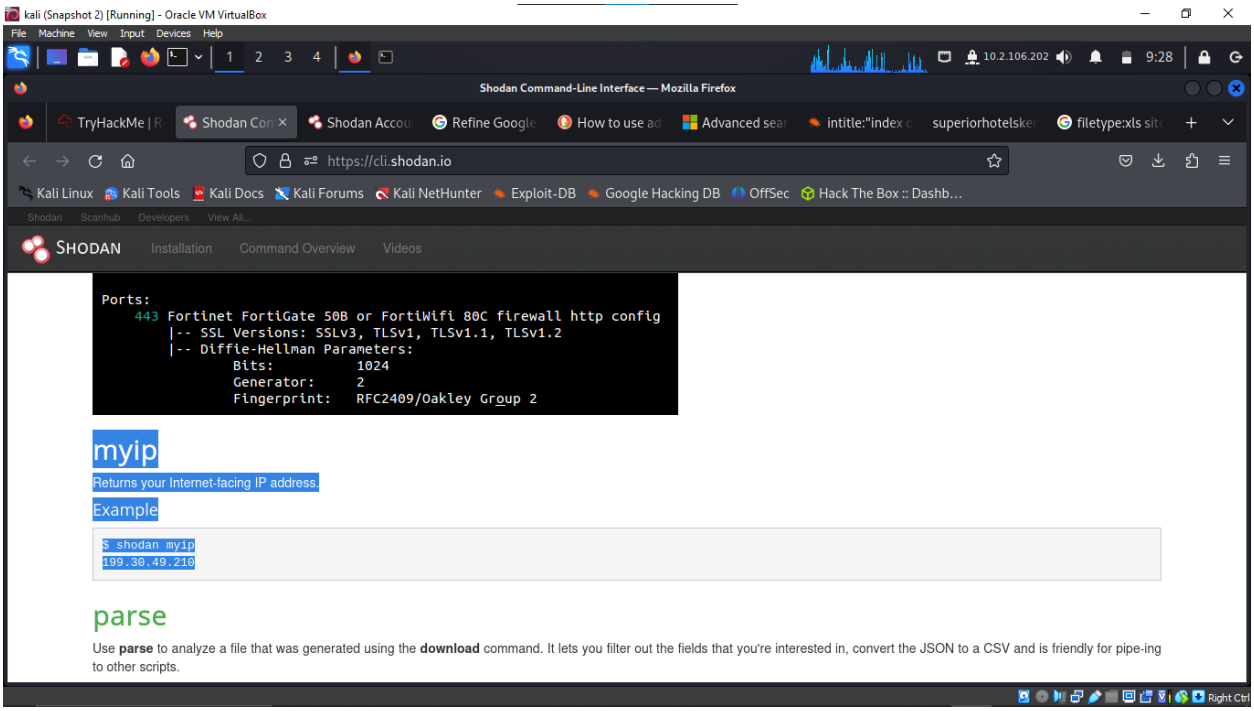
Beyond standard tools, specialized search engines provide advanced functionalities:

- **WHOIS and DNS Related:** Services like WHOIS history and advanced DNS services offer detailed insights into domain histories and DNS records.
- **Censys and Shodan:** Platforms that provide comprehensive data about domains and IP addresses, including their geographical locations, open ports, and associated organizations.

Questions and Answers

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

Answer: shodan myip

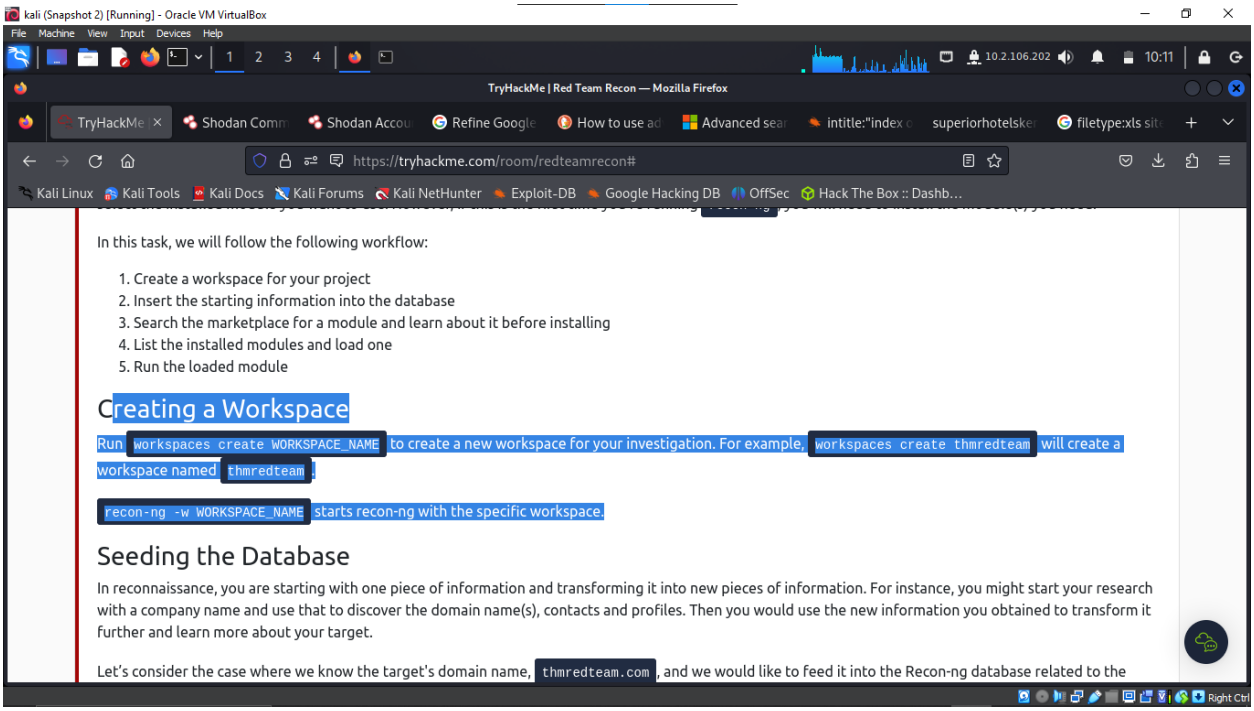


Task 6: Recon-ng

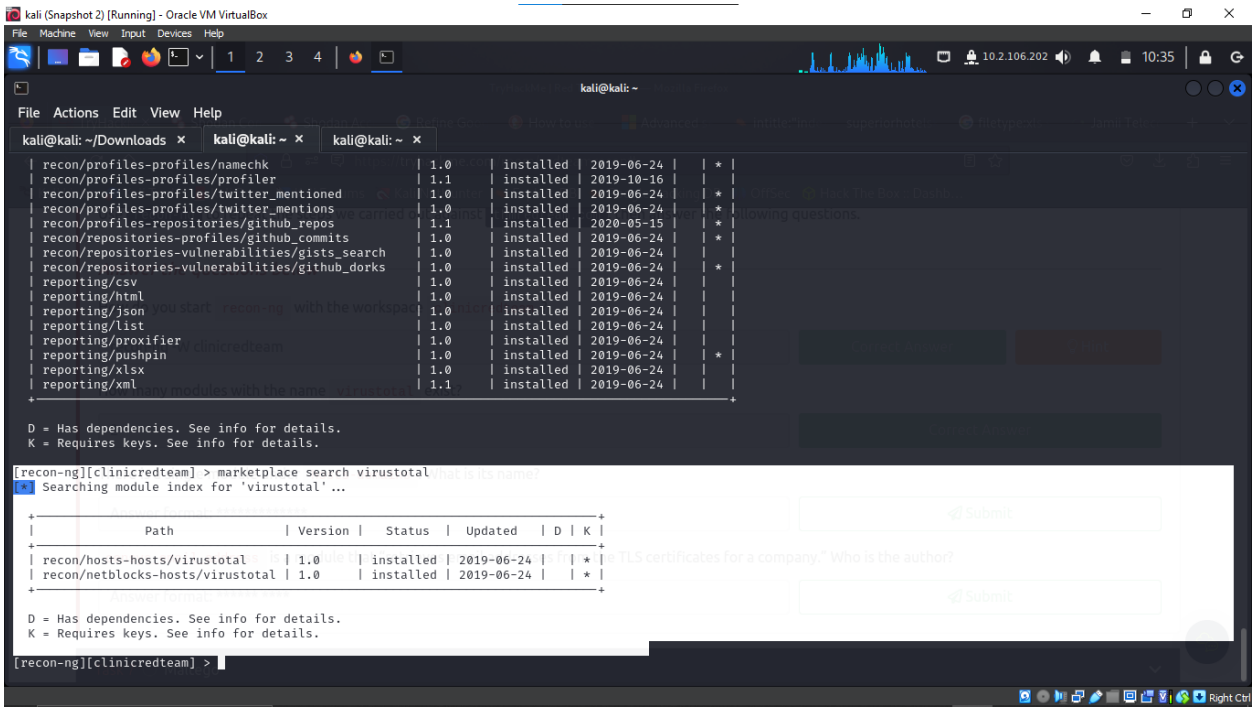
Recon-ng is a powerful framework that automates OSINT tasks. It uses various modules to gather and transform information into actionable intelligence. Key steps include creating a workspace, seeding the database with initial information, and utilizing modules to gather more data.

Questions and Answers

- How do you start recon-ng with the workspace clinicredteam?
    - **Answer**: recon-ng -w clinicredteam



- How many modules with the name virustotal exist?
    - **Answer**: 2



- There is a single module under hosts-domains. What is its name?
    - **Answer**: migrate hosts

```
[recon-ng][clinicredteam] > marketplace search hosts_domains
[*] Searching module index for 'hosts_domains' ...
[!] No modules found.
Searches marketplace modules

Usage: marketplace search [<regex>]

[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     | installed | 2020-05-17 |   |   |
  +-------------------------------------------------------------------------------+

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

- Censys_email_address is a module that "retrieves email addresses from the TLS certificates for a company." Who is the author?
  - **Answer**: 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        | disabled                                                                                    |
  +-------------------------------------------------------------------------------------------------------------+
```

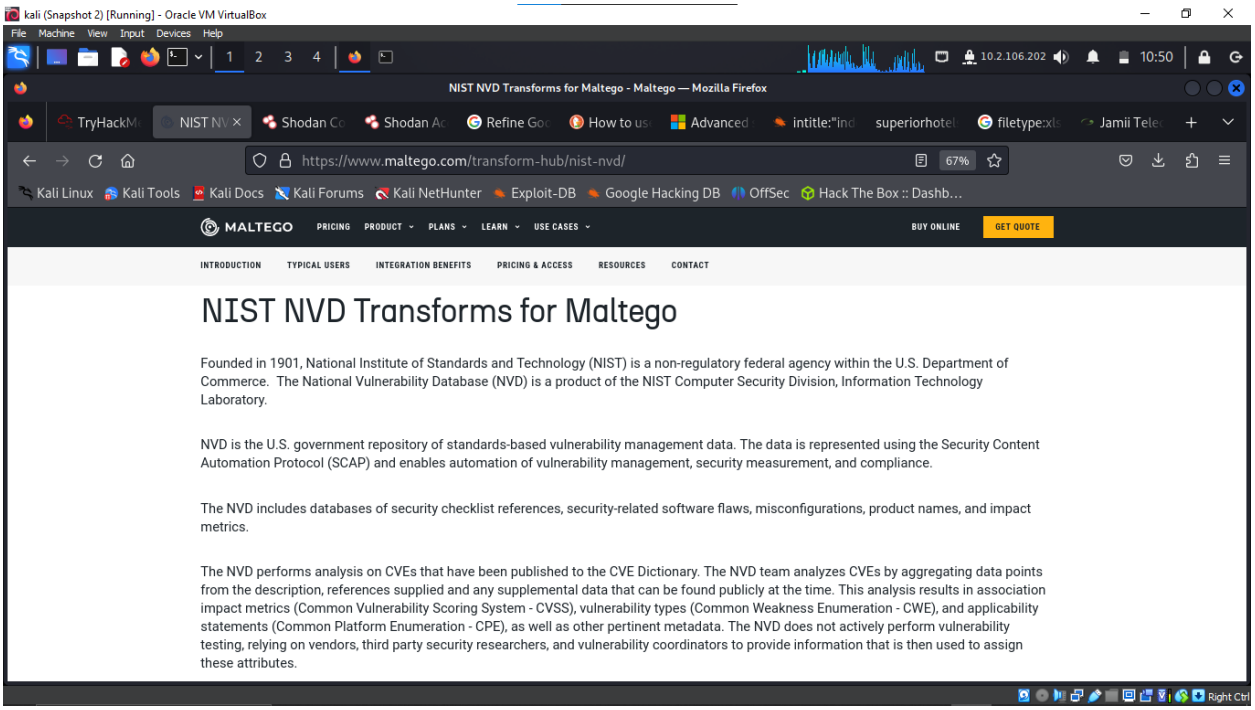
Task 7: Maltego

Maltego is a tool that combines mind-mapping with OSINT. It starts with a piece of information (like a domain or email address) and uses transforms to gather related data. Maltego is particularly effective in visualizing connections and gathering comprehensive intelligence.

Questions and Answers

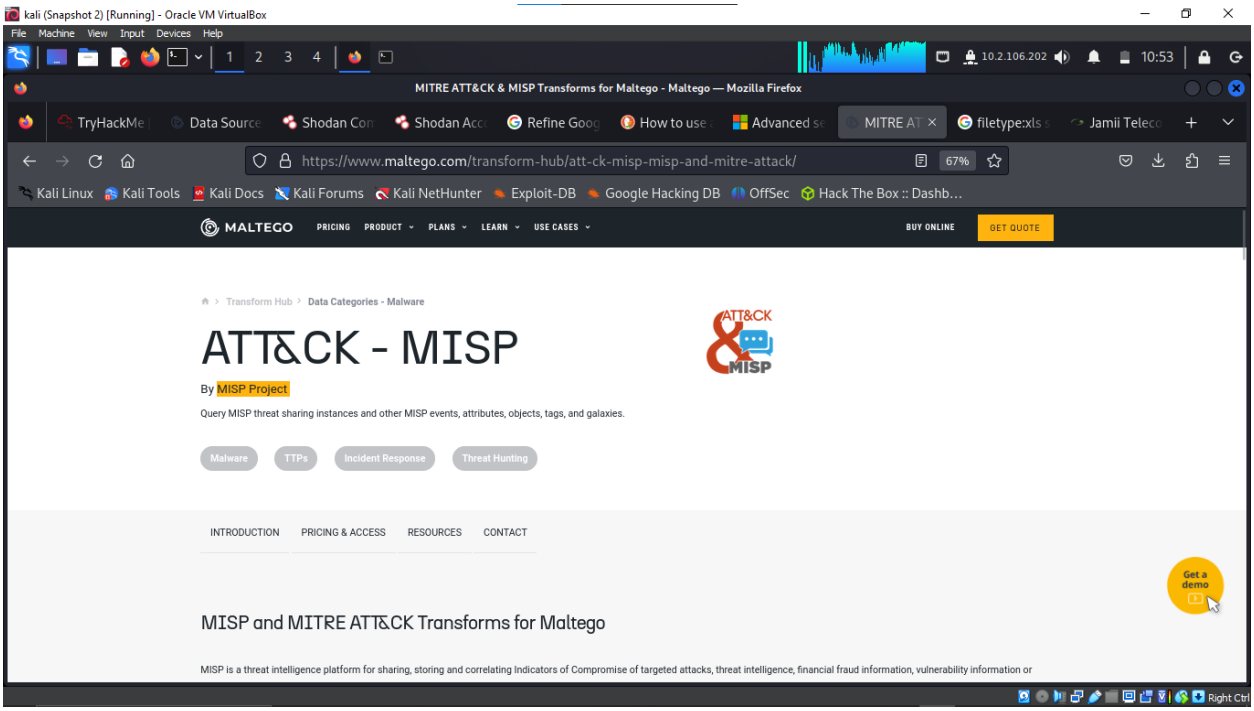
What is the name of the transform that queries NIST's National Vulnerability Database?

Answer: NIST NVD



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

Answer: MISP Project



Task 8: Summary

In the context of cyber warfare, knowing the enemy (the target) and oneself (red team capabilities) is crucial. Tools and techniques like WHOIS, DNS queries, advanced search engines, Recon-ng, and Maltego are essential in expanding knowledge about a target. This information aids in refining attack strategies and increasing the likelihood of a successful operation.

Conclusion

The different tools and techniques covered provide a foundational understanding necessary for advanced reconnaissance work in cybersecurity. Knowing as much as possible about the target enhances the effectiveness of subsequent attack phases, whether it's scanning for vulnerabilities or launching phishing campaigns. The essence of successful cyber operations lies in thorough and discreet reconnaissance, embodying Musashi's principle of understanding the enemy.