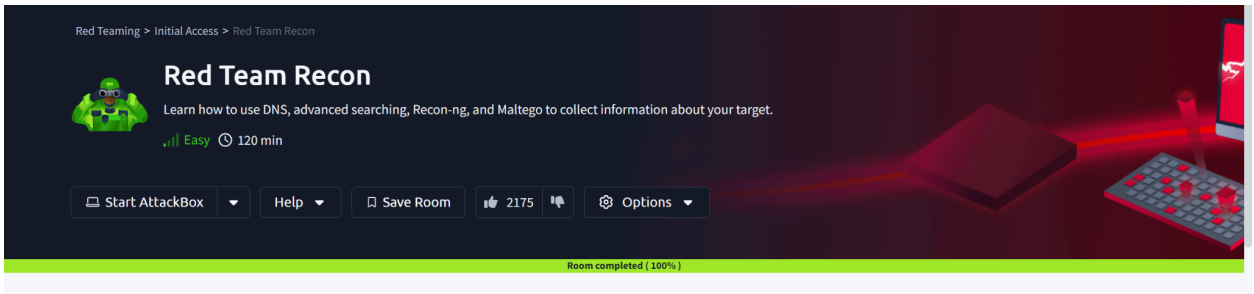
RED TEAM RECON

ASSIGNMENT REPORT



Peter Kinyumu,
cs-sa07-24067,
May 22nd, 2024.

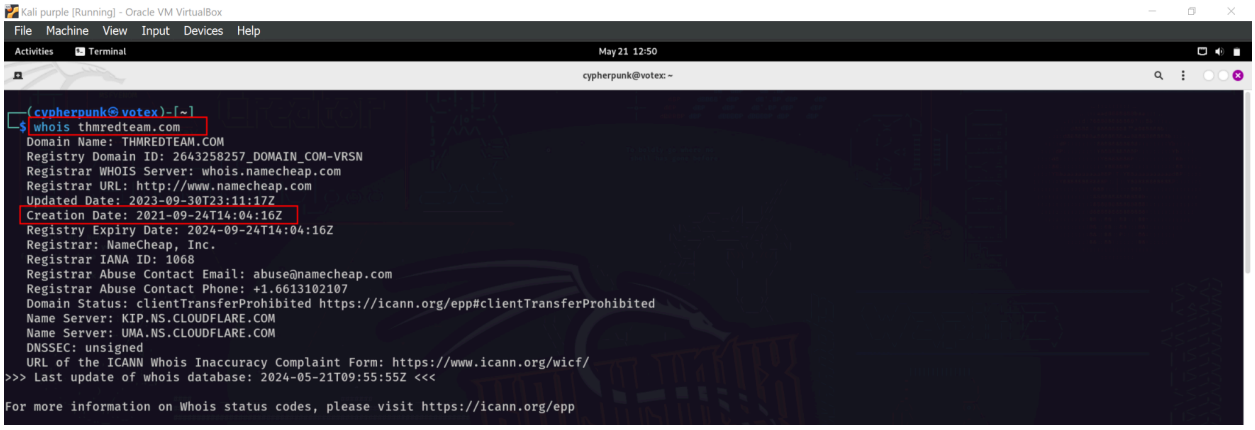
1. INTRODUCTION

This room teaches about reconnaissance; the preliminary survey of your target without alerting them to your activities. It covers tools that can help gather more information about your target such as the **whois** command to get the WHOIS records like domain registration details, Google Dorking, **nslookup**, **dig**, **host** for DNS records extractions, **recon-ng** and **Maltego**.

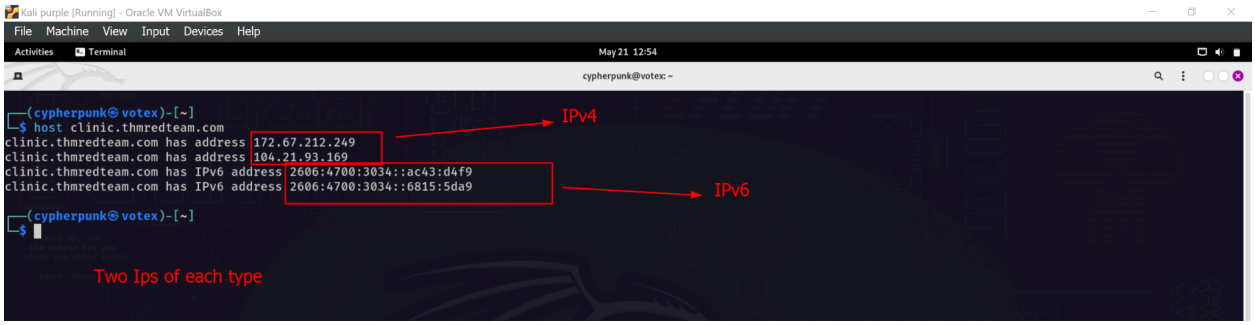
2. ANSWERS TO QUESTIONS

Built-in tools

a. **When was thmredteam.com created (registered)? (YYYY-MM-DD)**
   2021-09-24

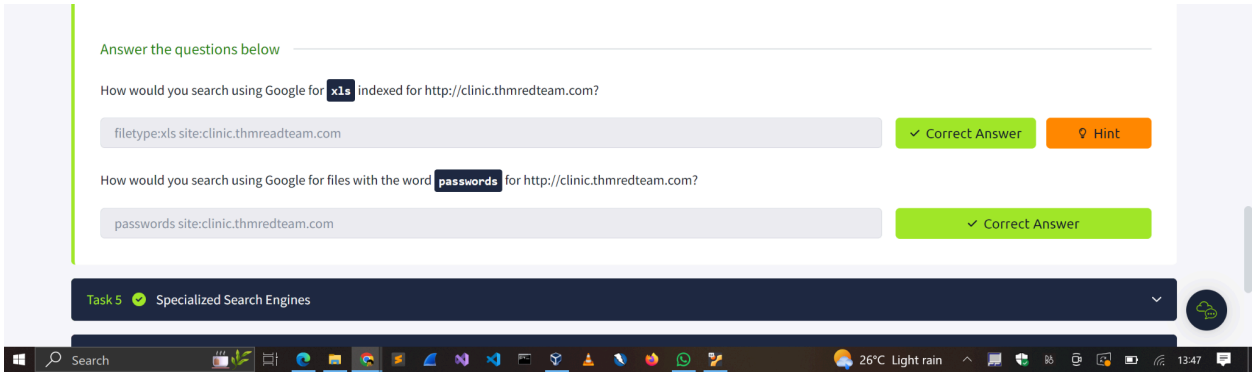


b. **To how many IPv4 addresses does clinic.thmredteam.com resolve?**
c. **To how many IPv6 addresses does clinic.thmredteam.com resolve?**



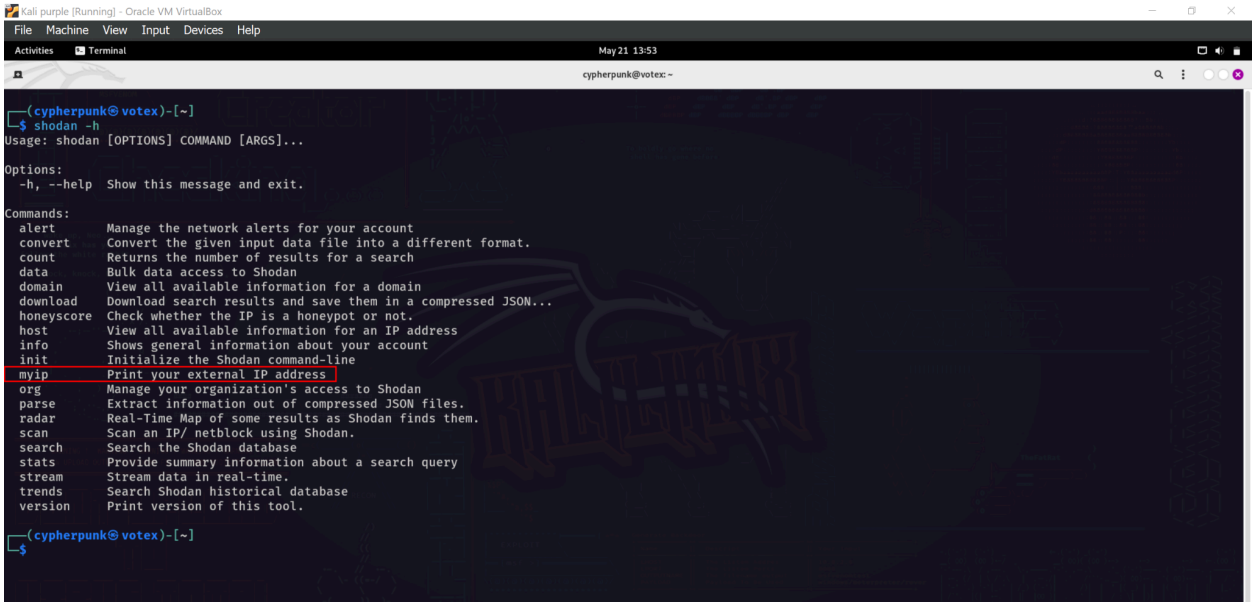
Advanced Searching

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



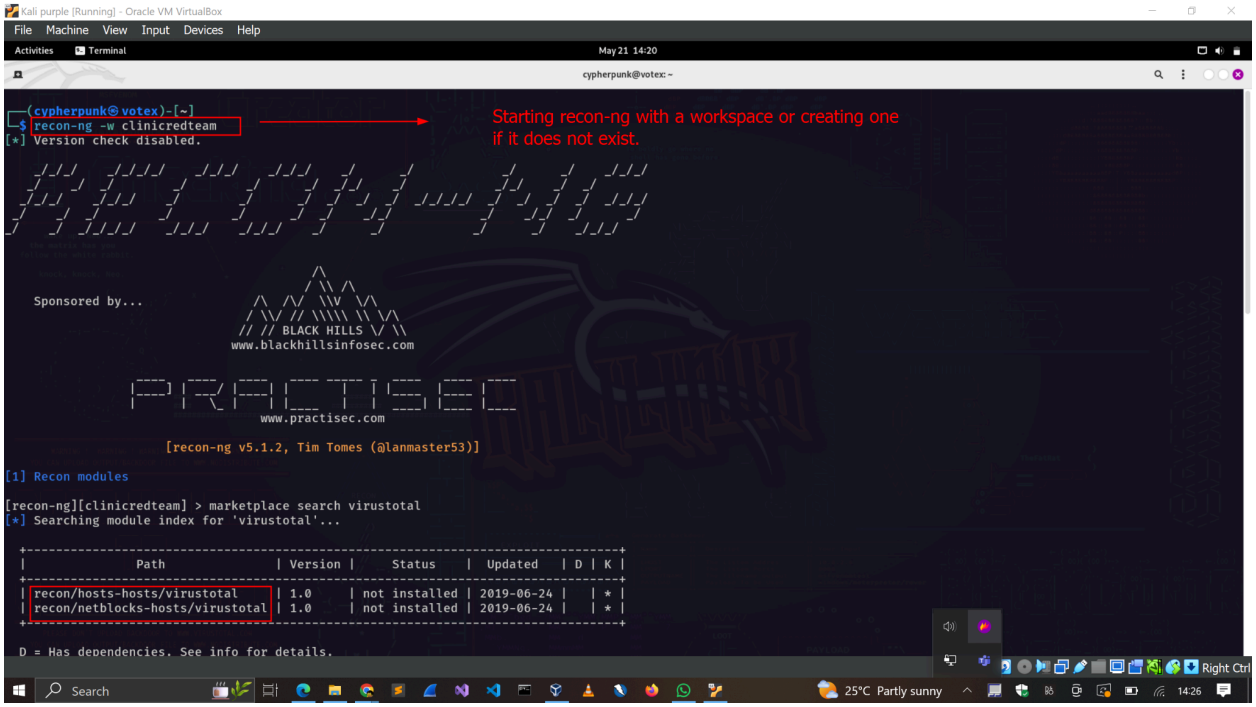
Shodan

a. **What is the shodan command to get your Internet-facing IP address?**
   shodan myip



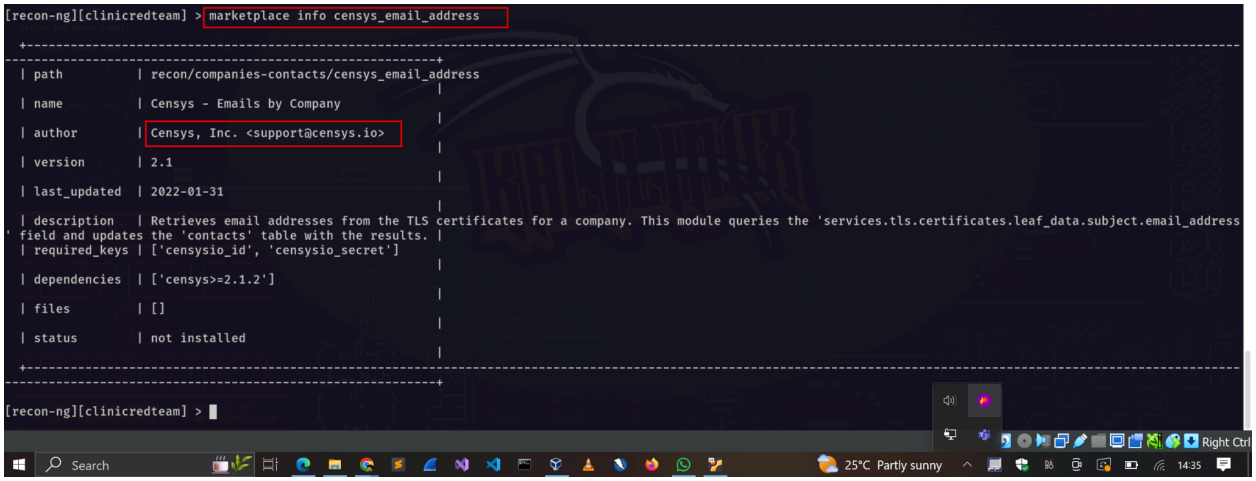
Recon-ng

a. **How do you start recon-ng with the workspace clinicredteam?**
b. **How many modules with the name virustotal exist?**
   Two modules exist with the name virustotal.



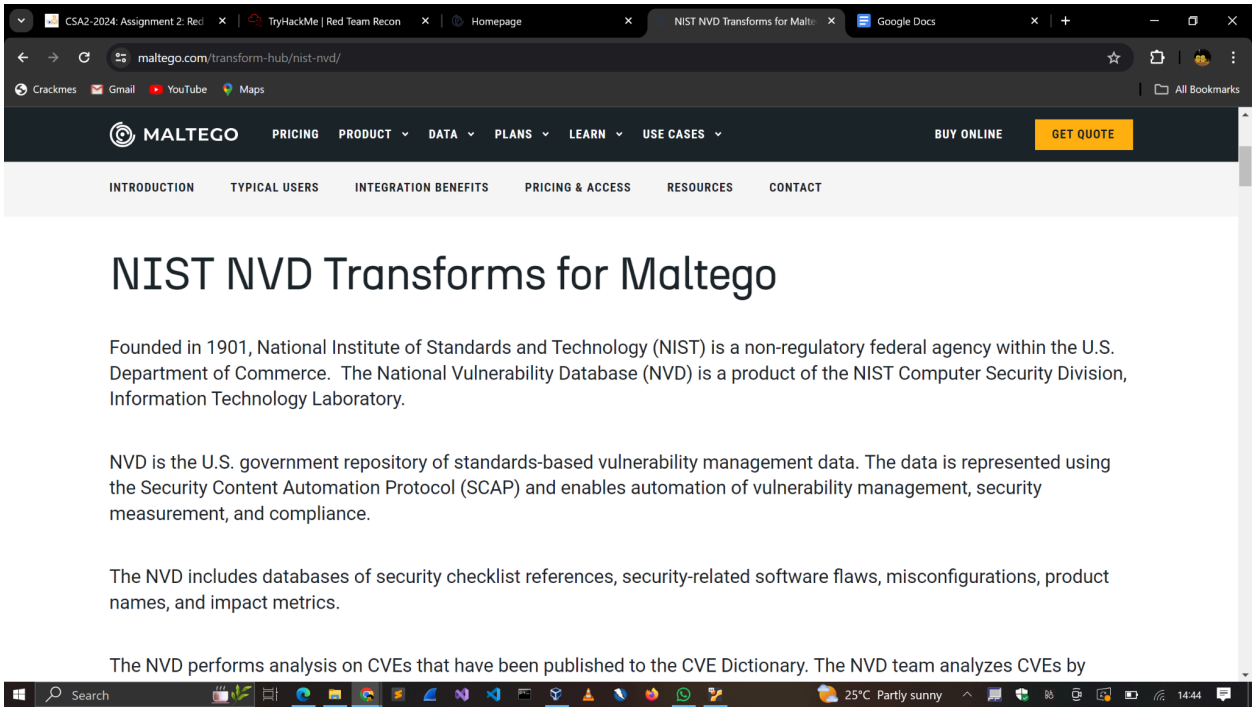
c. **There is a single module under hosts-domains. What is its name?**

d. **censys_email_address is a module that "retrieves email addresses from the TLS certificates for a company." Who is the author? (Formart ****** ****)**

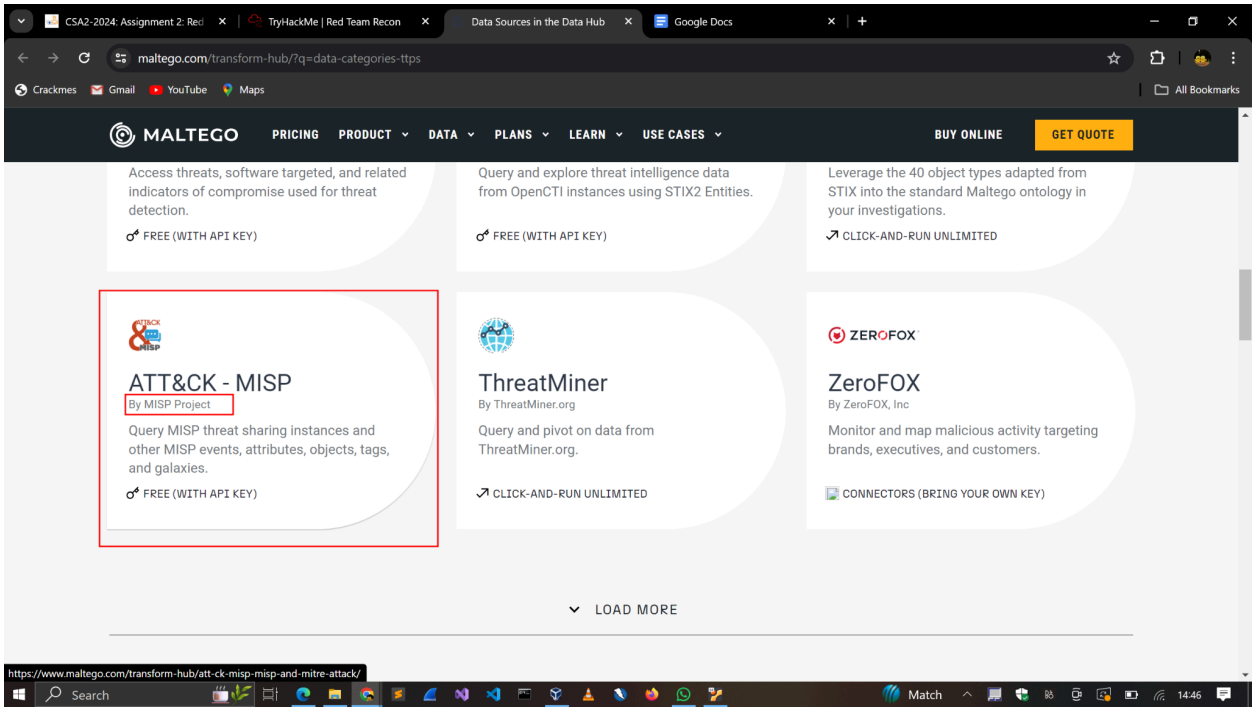


Maltego

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



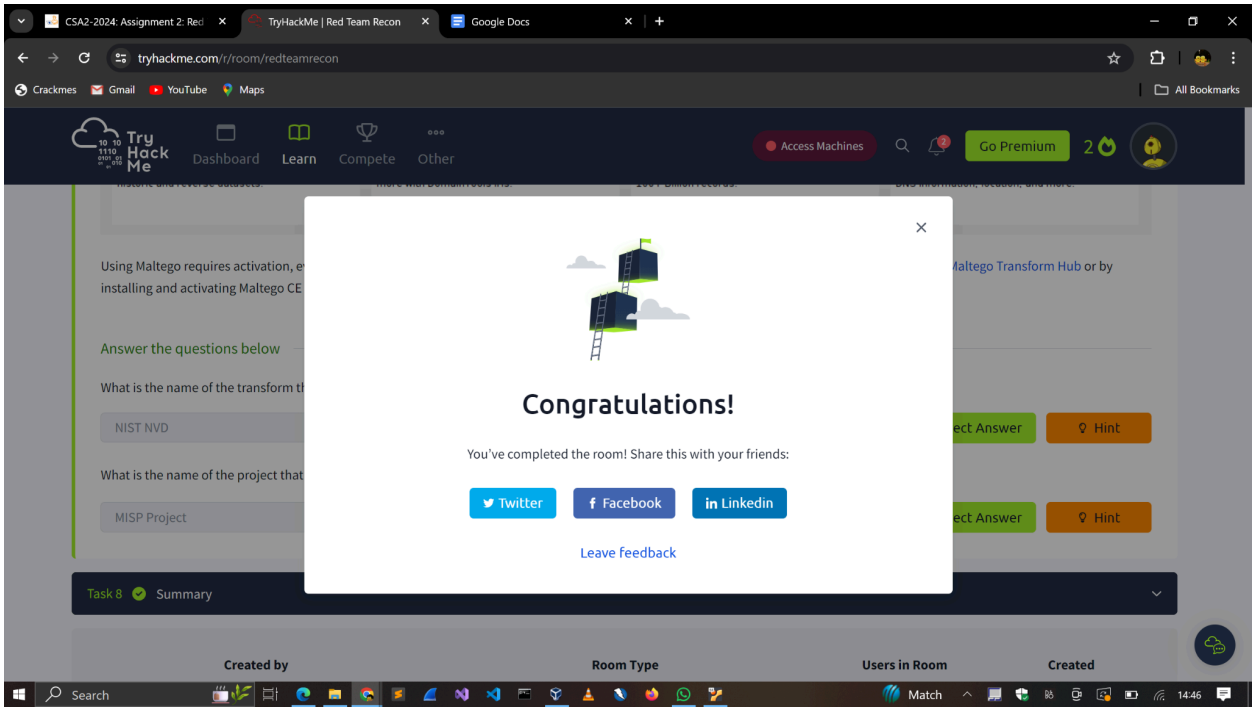
b. **What is the name of the project that offers a transform based on ATT&CK?**



3. MODULE COMPLETION

Below is the link to my THM profile, which displays completed rooms, including this room, Red Team Recon.

https://tryhackme.com/p/c1ph3rbnuk



4. CONCLUSION

I am excited to have learned alot about Reconnaissance and OSINT from this assignment. I learnt how to use the **whois** command to view domain registration details and WHOIS records. I have also learnt to extract DNS information using tools like **dig**, **nslookup**, and **host**. Additionally, i have learnt to perform advanced searching on Google with queries like **site:example.com**, **filetype:pdf**, etc. I have learnt how to use special search engines like ViewDNS.info, Shodan and Censys to gather more information about target IP addresses. Lastly, I have enjoyed using **recon-ng**, a framework that automates OSINT work.

I look forward to applying this knowledge on reconnaissance in my penetration testing process.