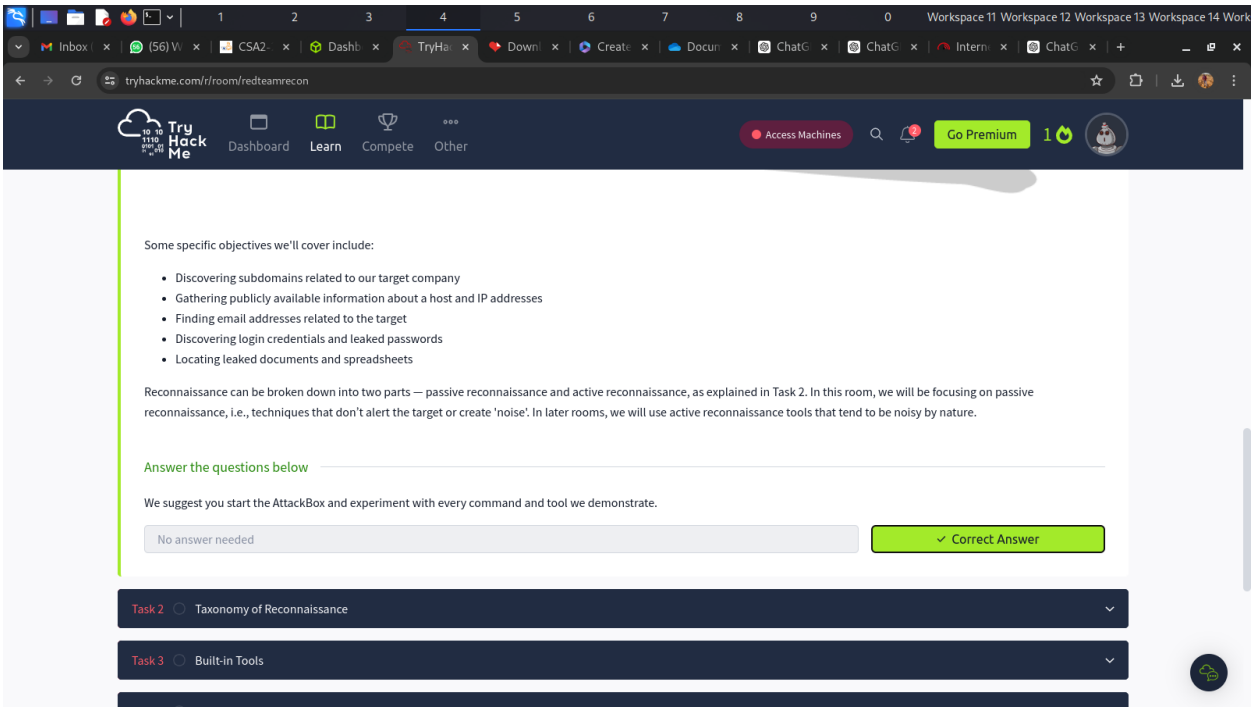
cs-sa07-24019
John_Mbithi_Mutave

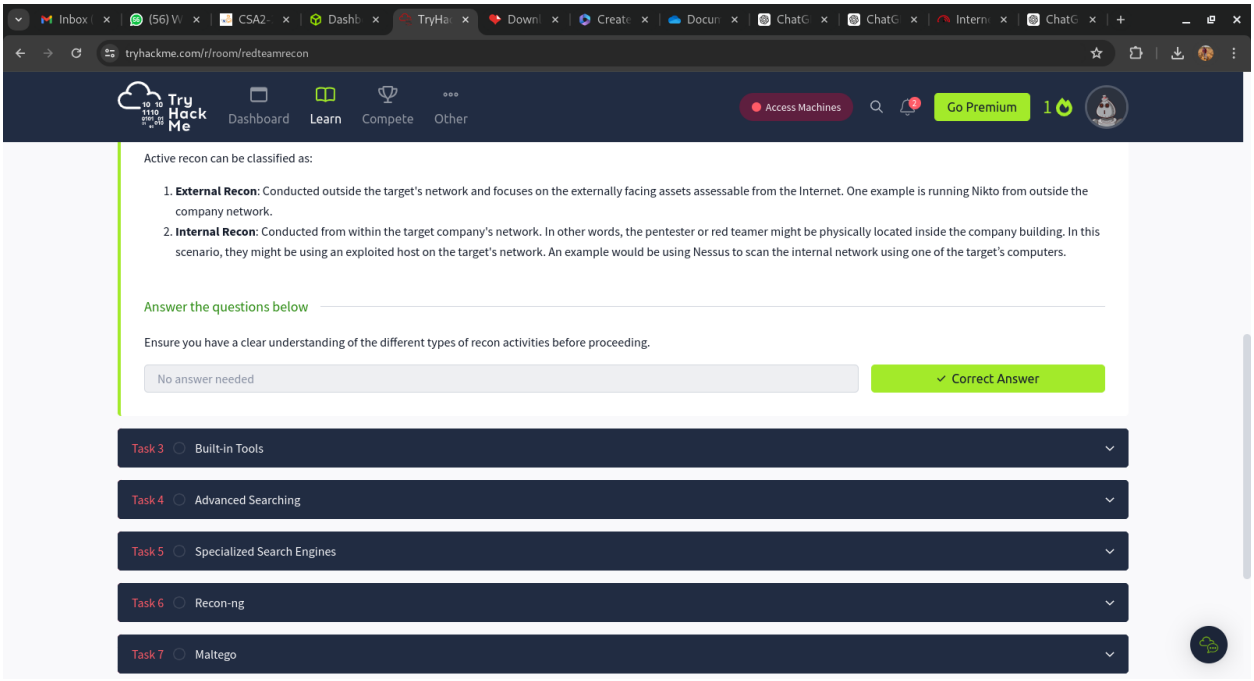
Red Team Recon

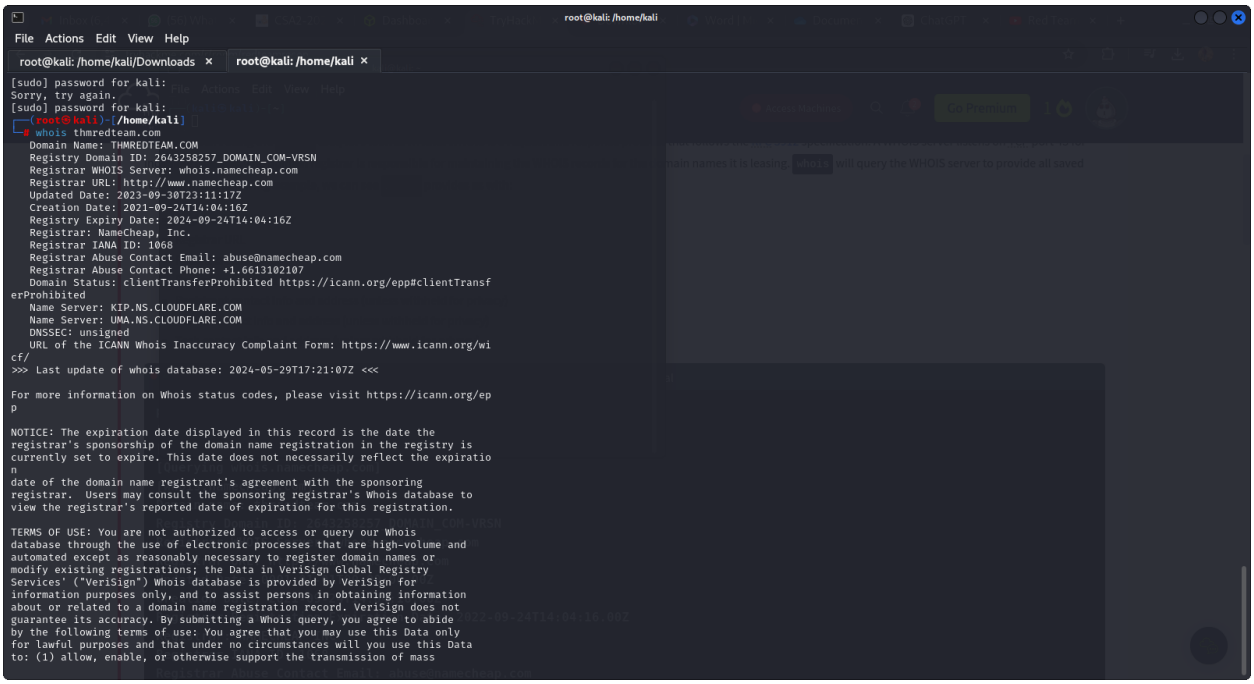
The tasks of this room cover the following topics:

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

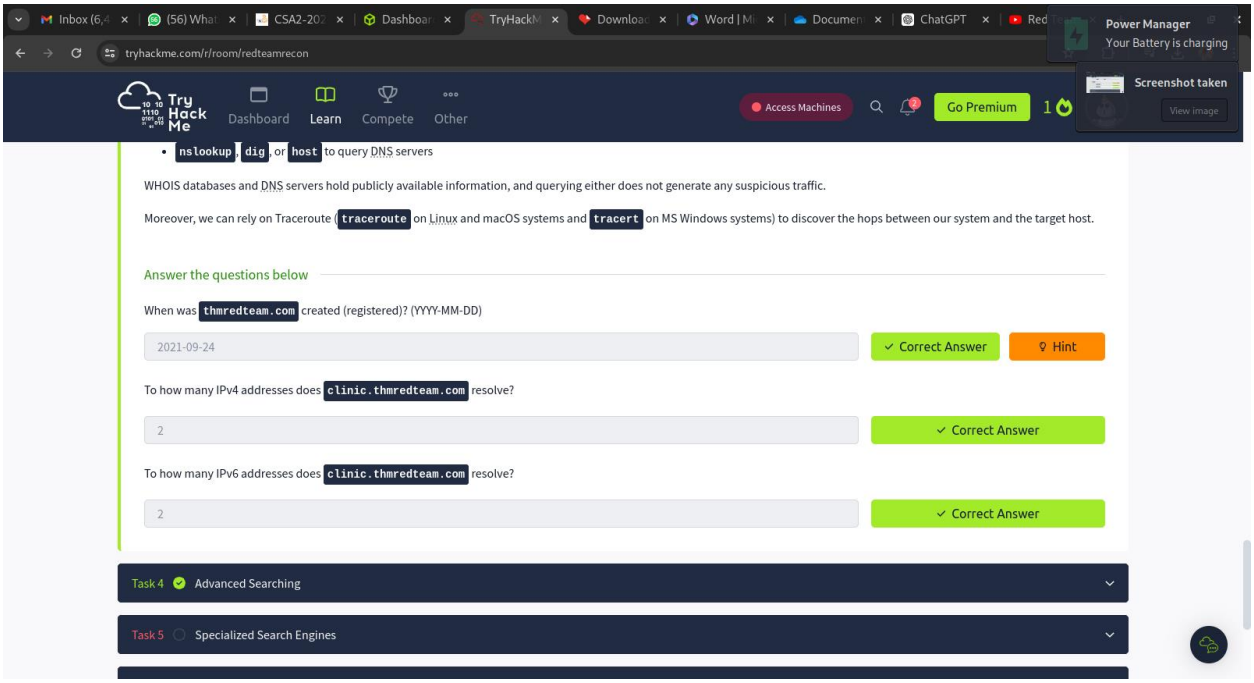


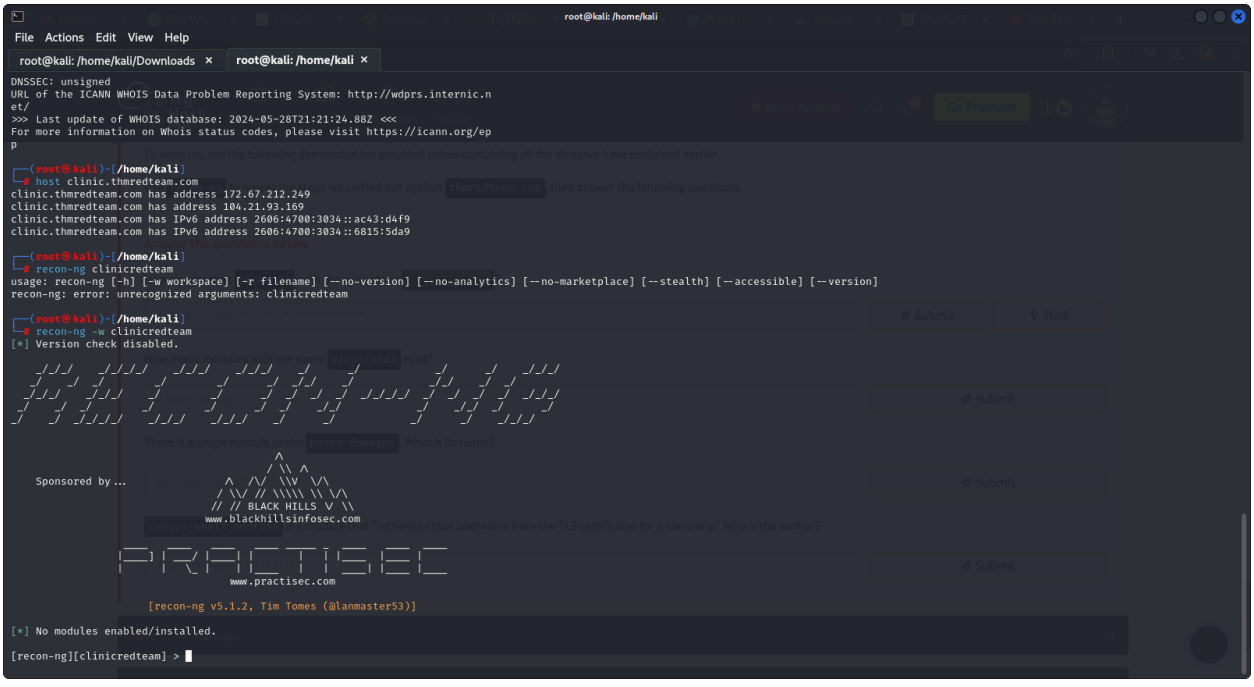
cs-sa07-24019
John_Mbithi_Mutave



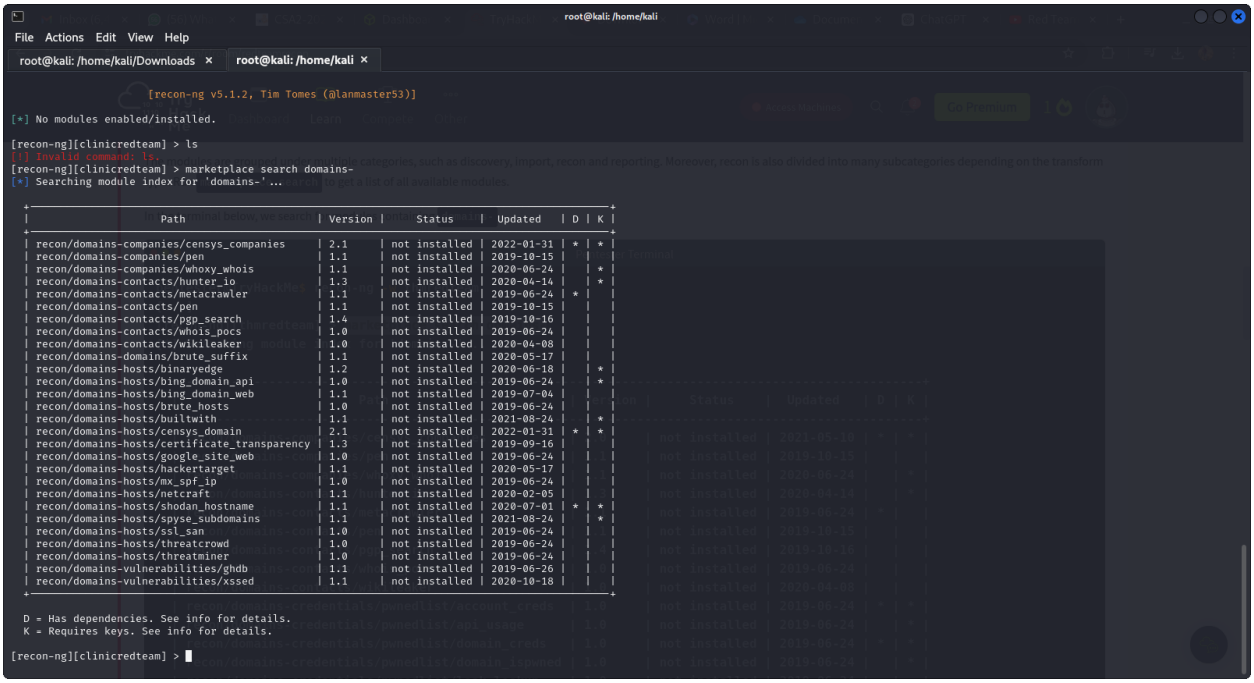


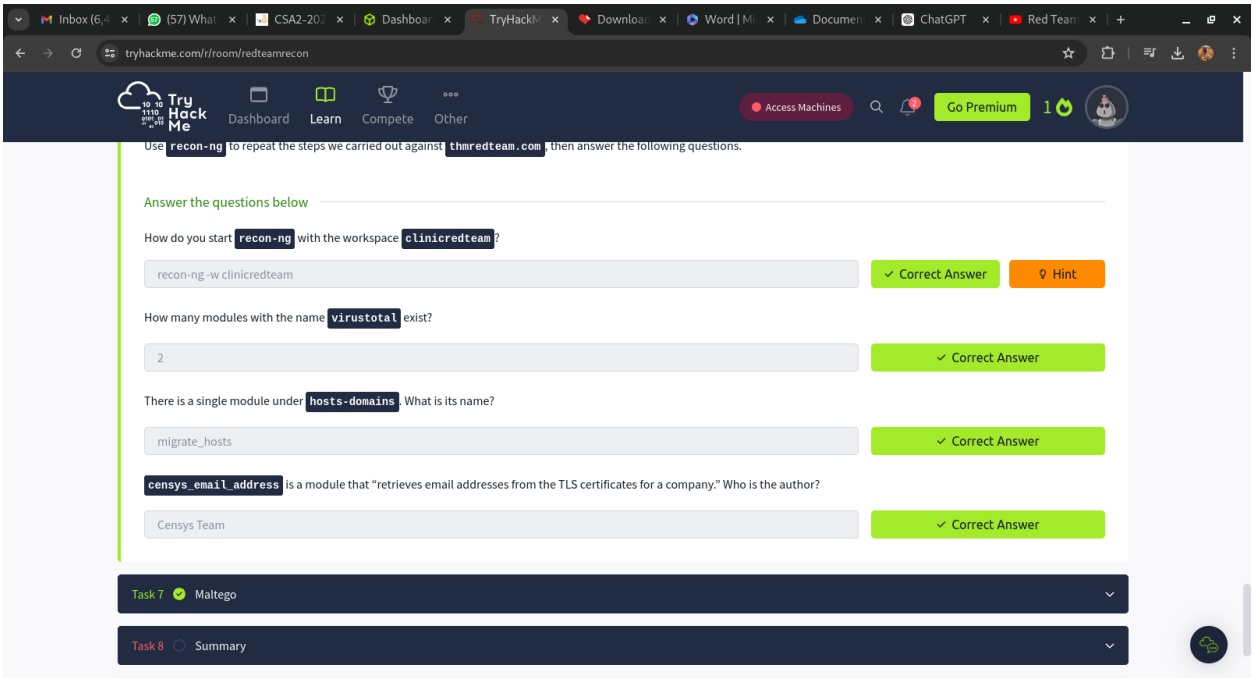
cs-sa07-24019
John_Mbithi_Mutave



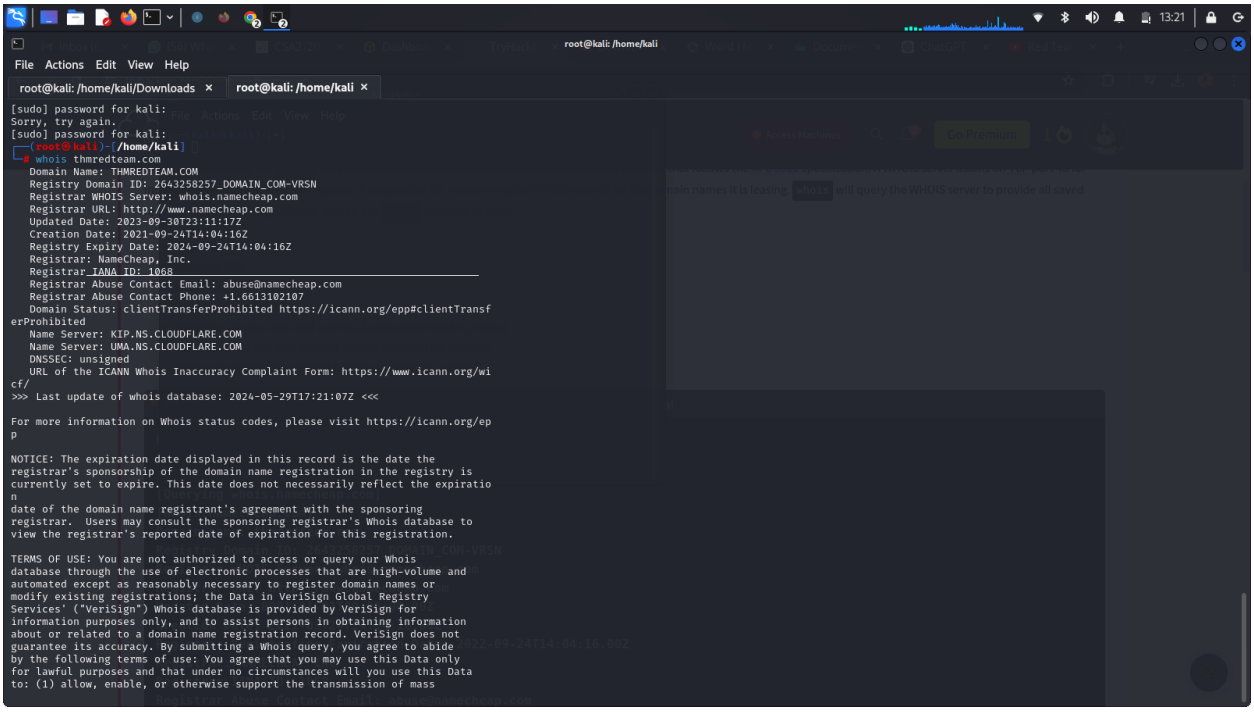


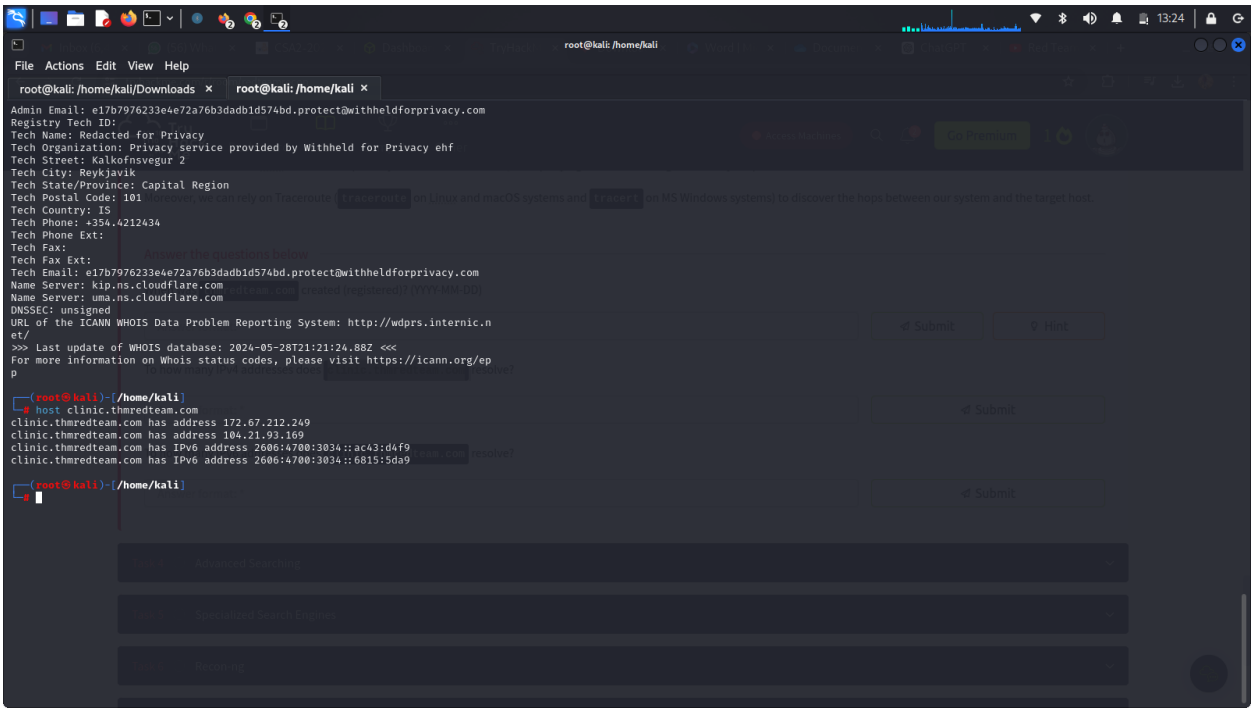
cs-sa07-24019
John_Mbithi_Mutave



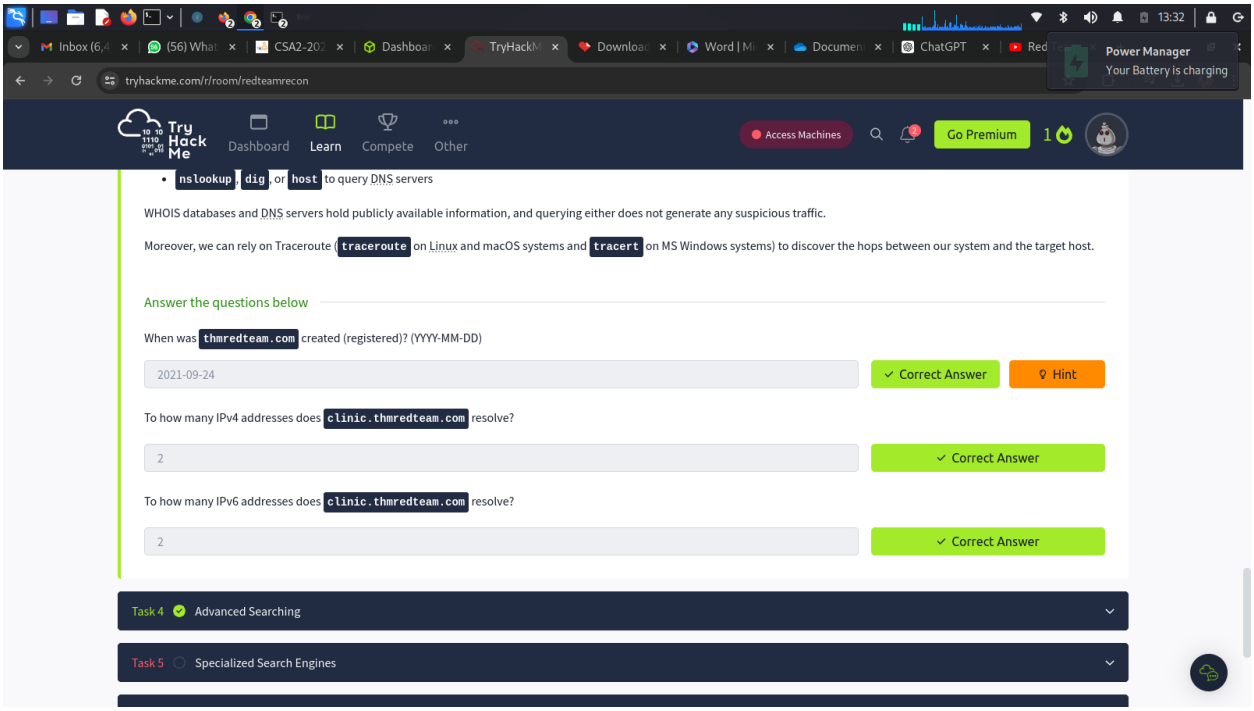


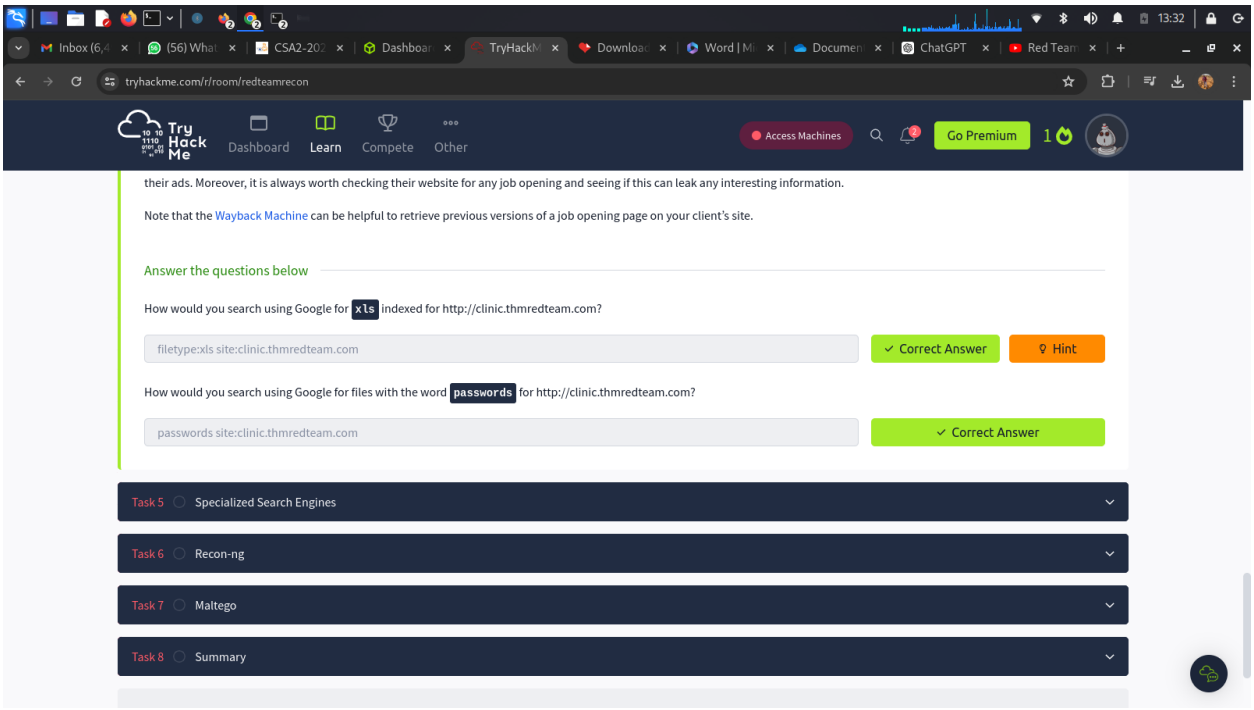
cs-sa07-24019
John_Mbithi_Mutave



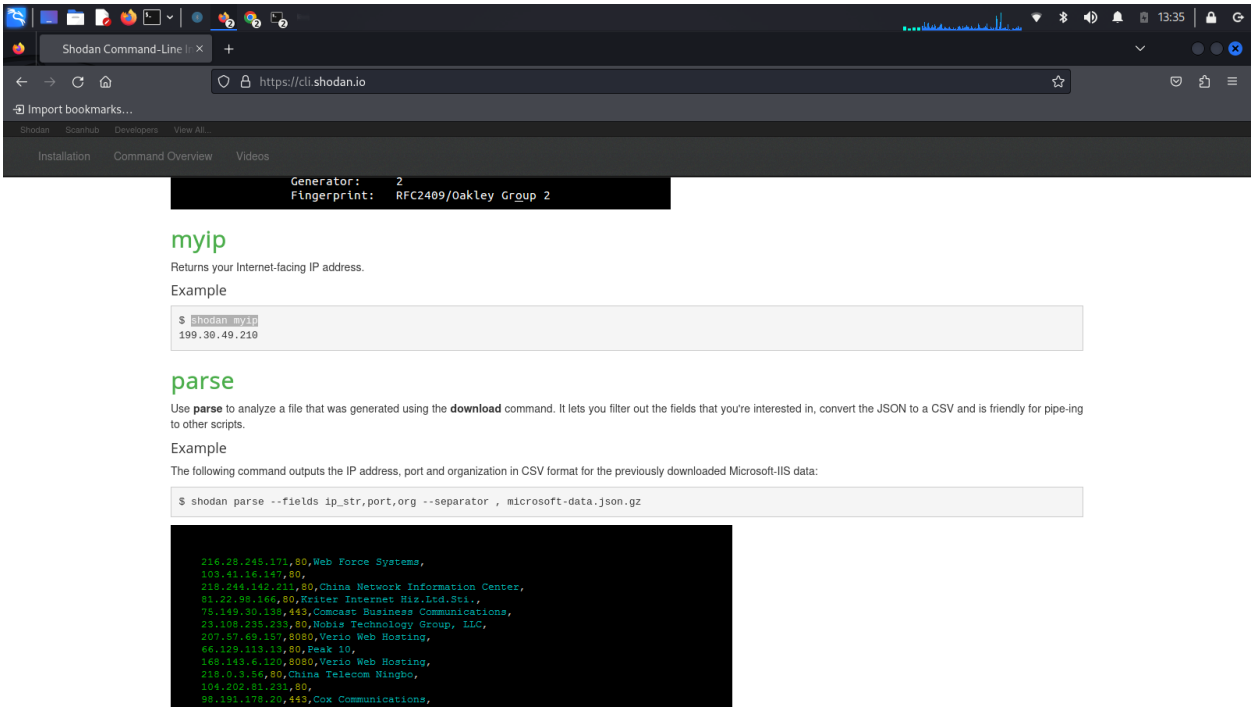


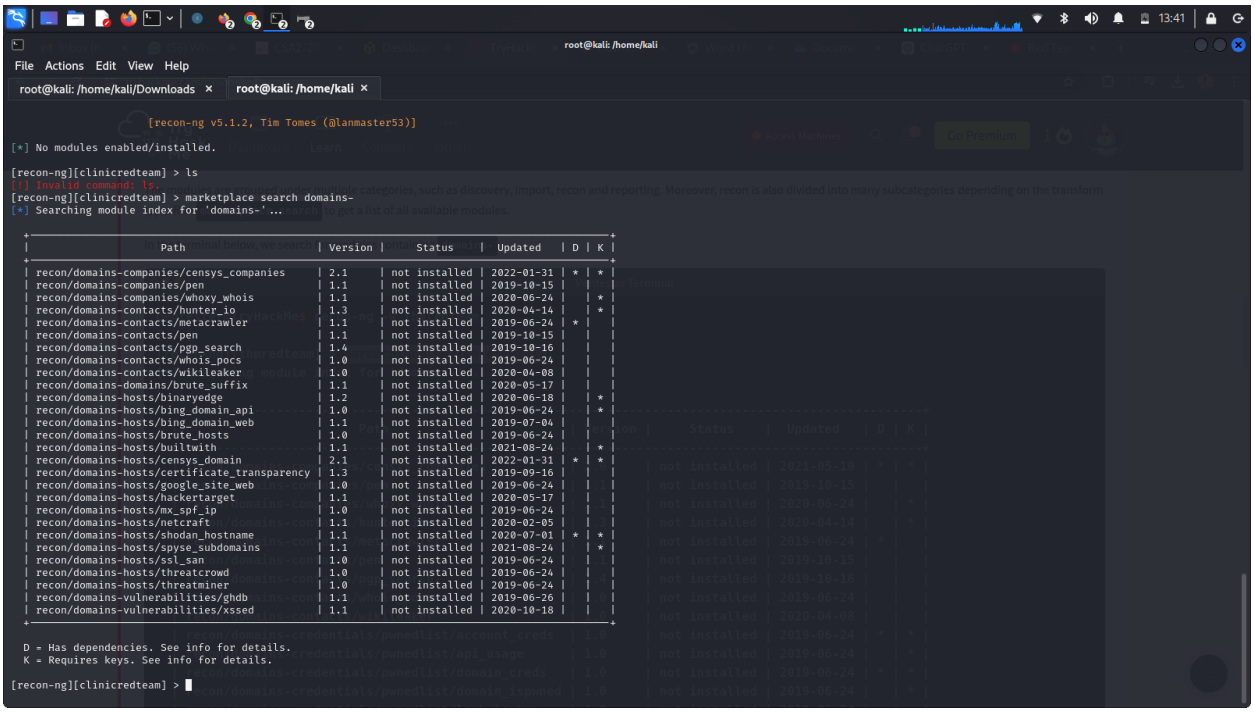
cs-sa07-24019
John_Mbithi_Mutave



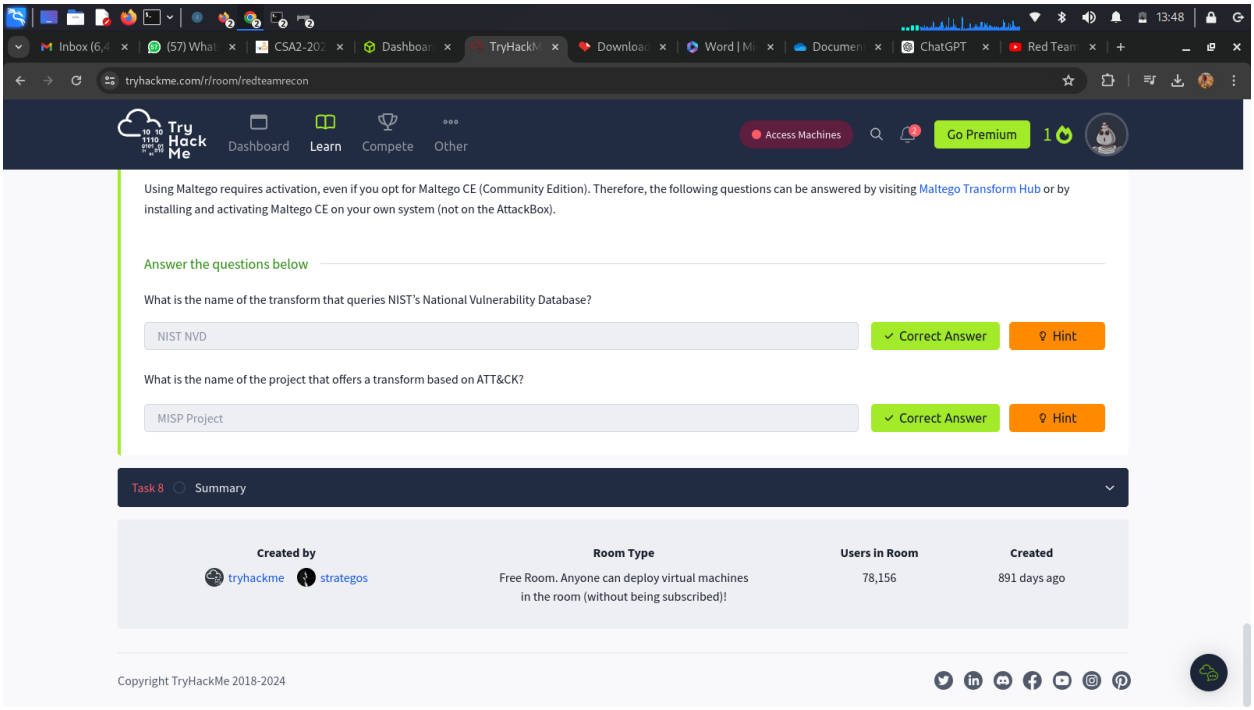


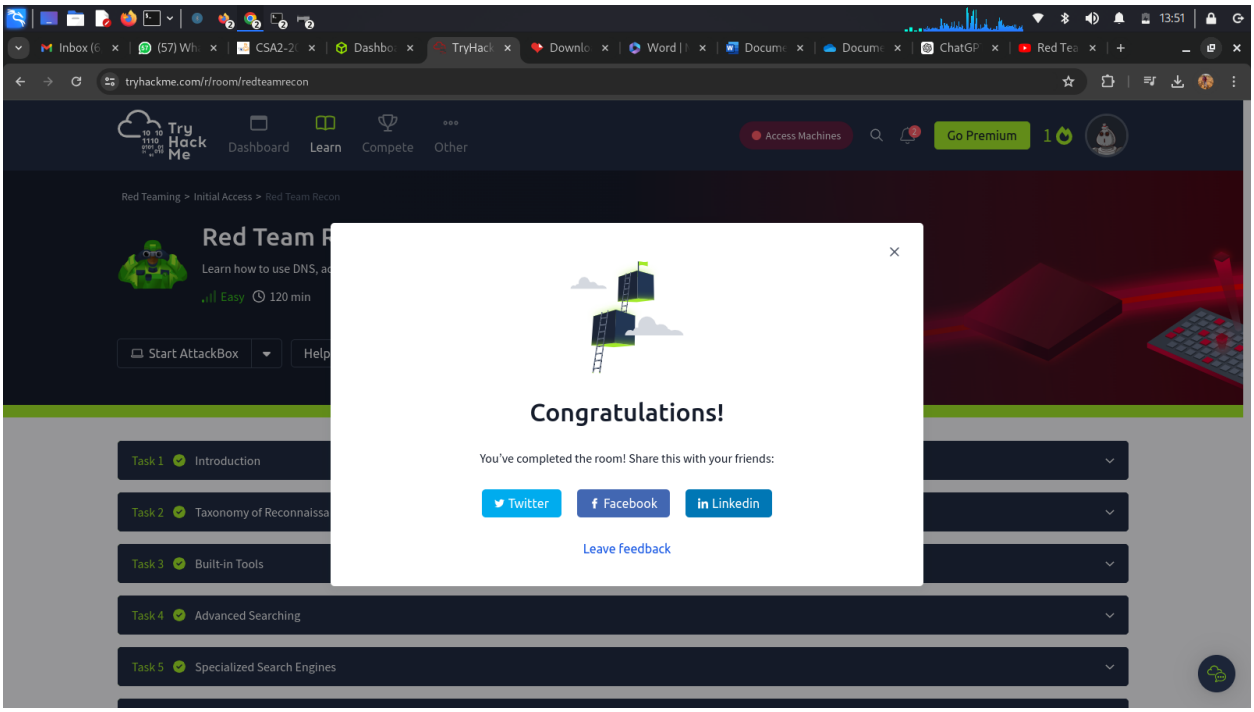
cs-sa07-24019
John_Mbithi_Mutave





cs-sa07-24019
John_Mbithi_Mutave





Shareable link: http://www.tryhackme.com/r/room/redteamrecon

Conclusion

We have reviewed essential built-in tools such as **whois**, **dig**, and **tracert**. Moreover, we explored the power of search engines to aid in our passive reconnaissance activities. Finally, we demonstrated two tools, Recon-ng and Maltego, that allow us to collect information from various sources and present them in one place.

The purpose is to expand our knowledge about the target and collect various information that can be leveraged in the subsequent attack phases. For instance, hosts that are discovered can be scanned and probed for vulnerabilities, while contact information and email addresses can be used to launch phishing campaigns efficiently. In brief, the more information we gather about the target, the more we can refine our attacks and increase our chances of success.