cs-sa07-24019
John_Mbithi_Mutave

Passive Recon

- This module covers:
- Passive Reconnaissance
- Active Reconnaissance
- Nmap Live Host Discovery
- Nmap Basic Port Scans
- Nmap Advanced Port Scans
- Nmap Post Port Scans
- Protocols and Servers
- Protocols and Servers 2
- Network Security Challenge

In this room, I have learned d passive reconnaissance and active reconnaissance, focusing on essential tools related to passive reconnaissance. I have learned three command-line tools:

- **whois** to query WHOIS servers
- **nslookup** to query DNS servers
- **dig** to query DNS servers

We use **whois** to query WHOIS records, while we use **nslookup** and **dig** to query DNS database records.

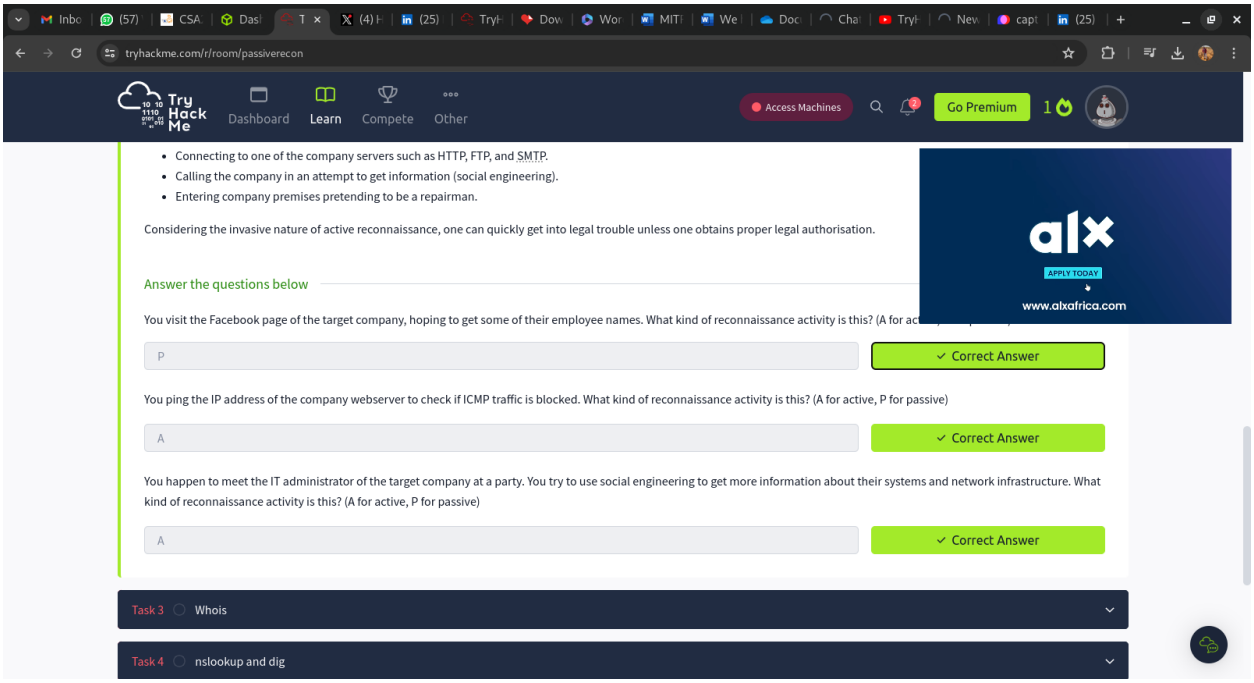
I have also learned the usage of two online services:

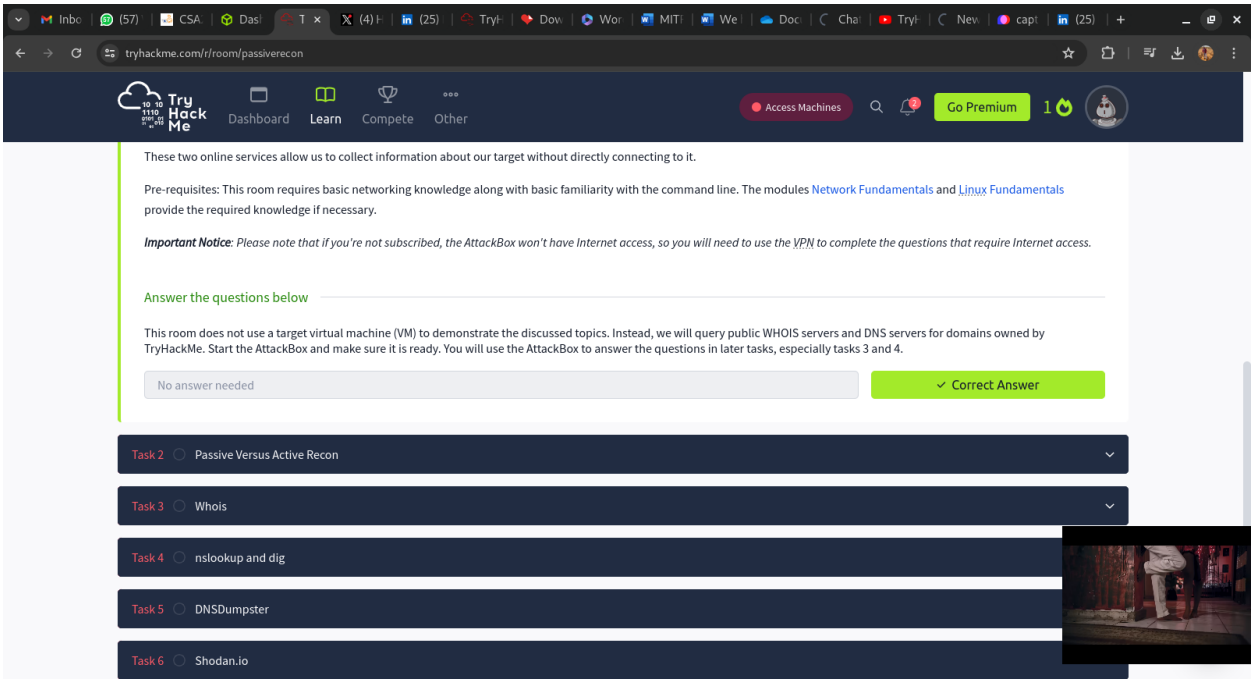
- DNSDumpster
- Shodan.io

cs-sa07-24019
John_Mbithi_Mutave

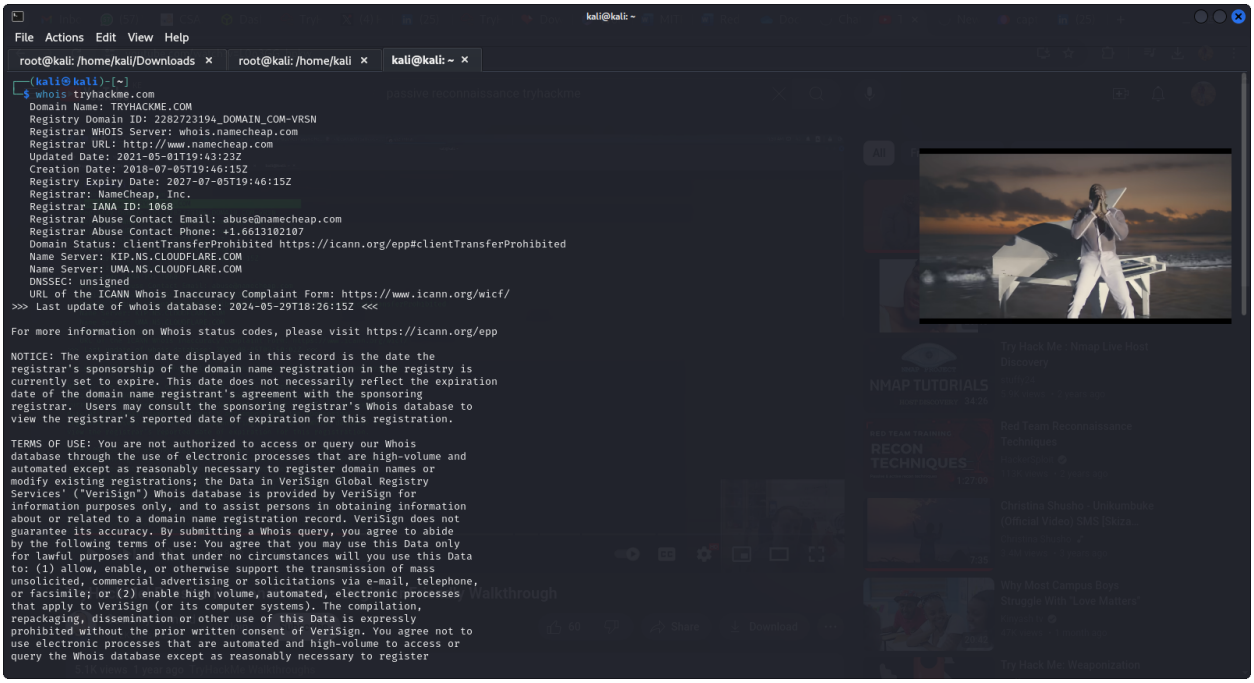
Purpose	Commandline Example
Lookup WHOIS record	**whois tryhackme.com**
Lookup DNS A records	**nslookup -type=A tryhackme.com**
Lookup DNS MX records at DNS server	**nslookup -type=MX tryhackme.com 1.1.1.1**
Lookup DNS TXT records	**nslookup -type=TXT tryhackme.com**
Lookup DNS A records	**dig tryhackme.com A**
Lookup DNS MX records at DNS server	**dig @1.1.1.1 tryhackme.com MX**
Lookup DNS TXT records	**dig tryhackme.com TXT**

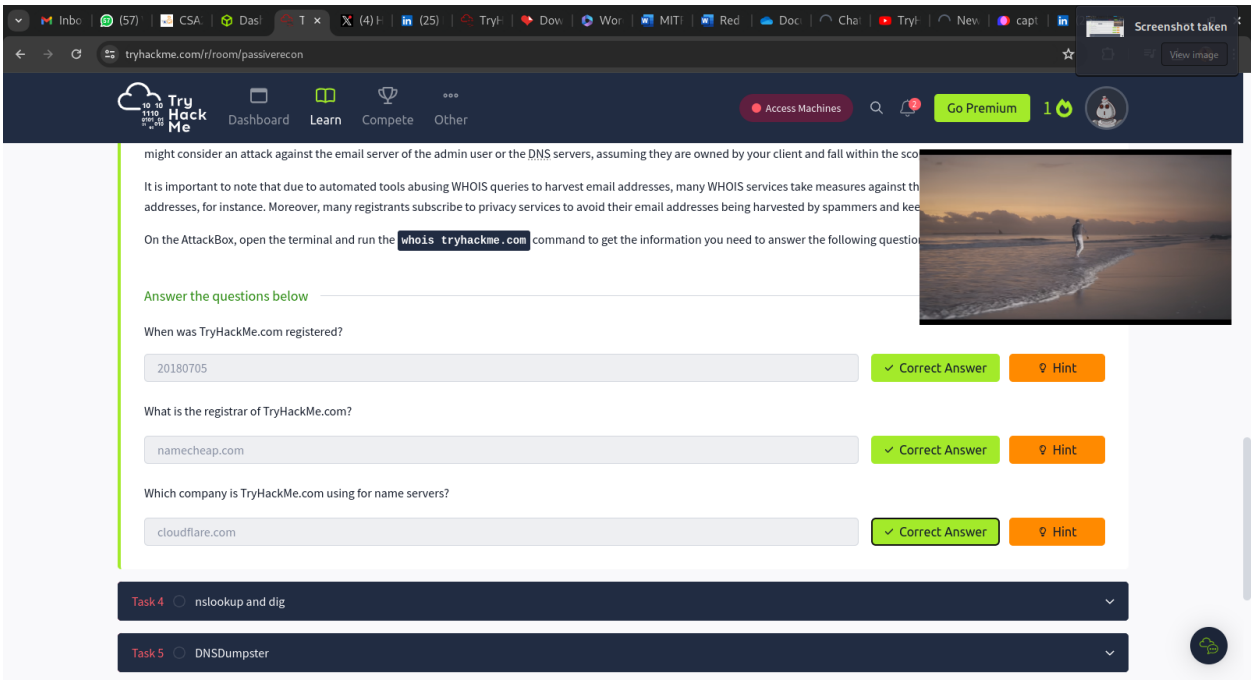
cs-sa07-24019
John_Mbithi_Mutave



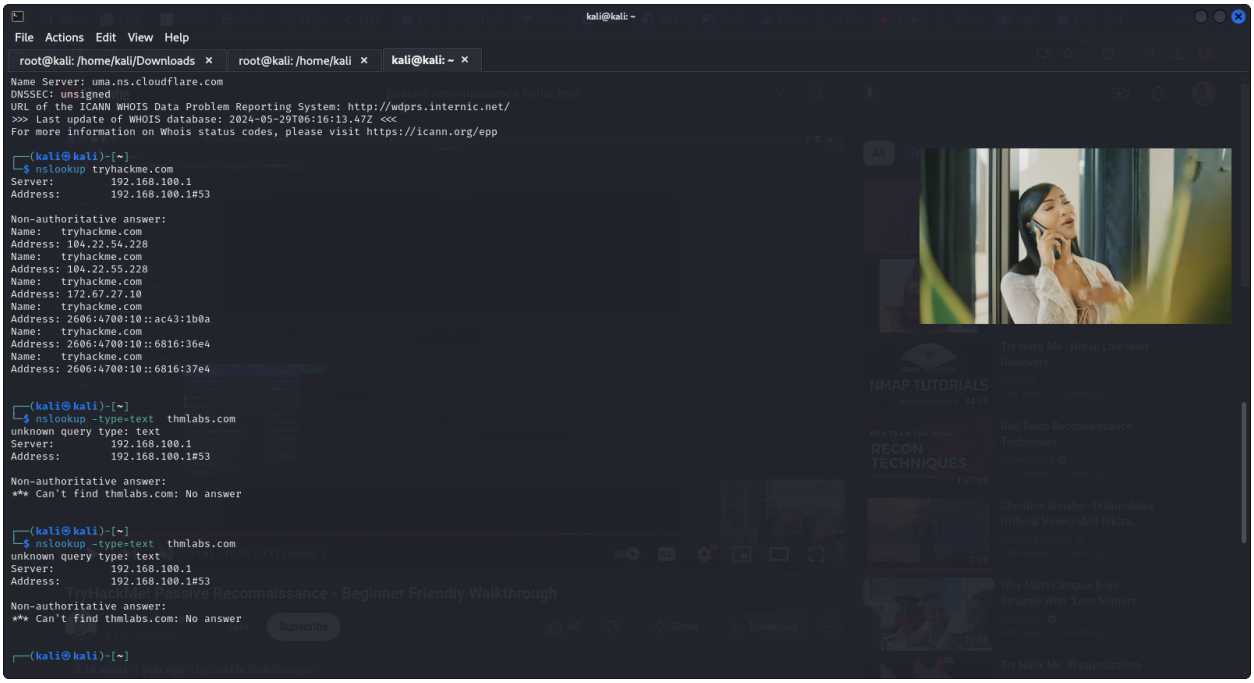


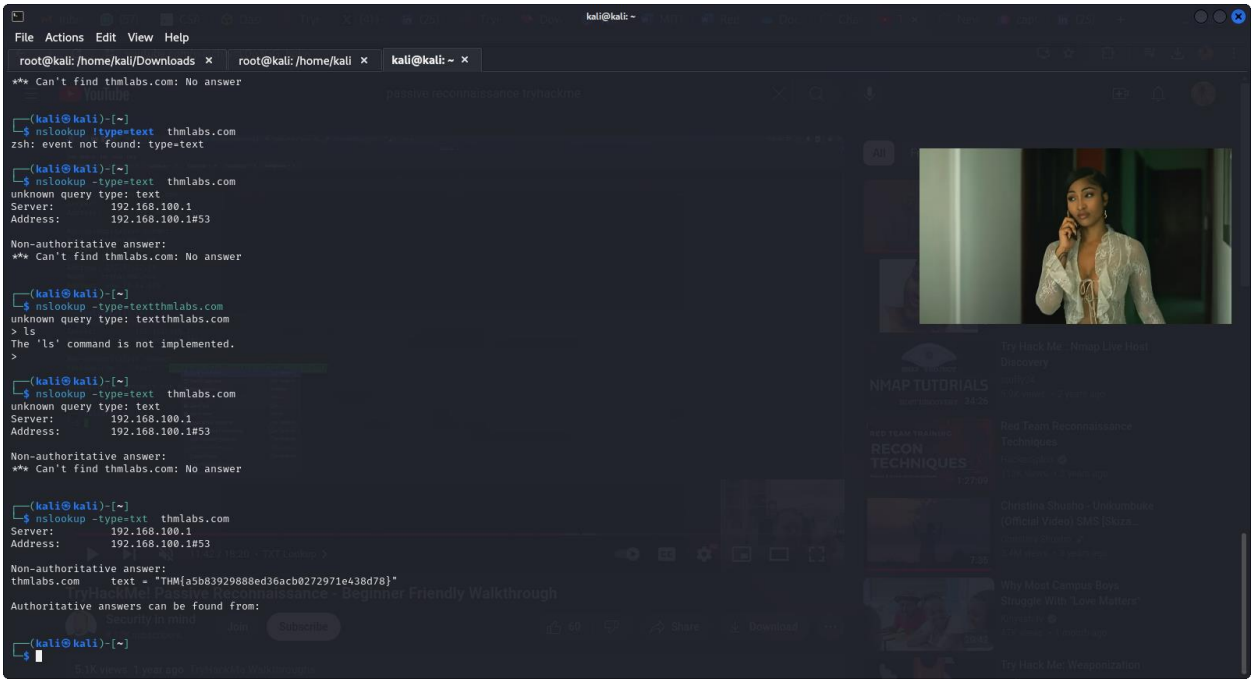
cs-sa07-24019
John_Mbithi_Mutave



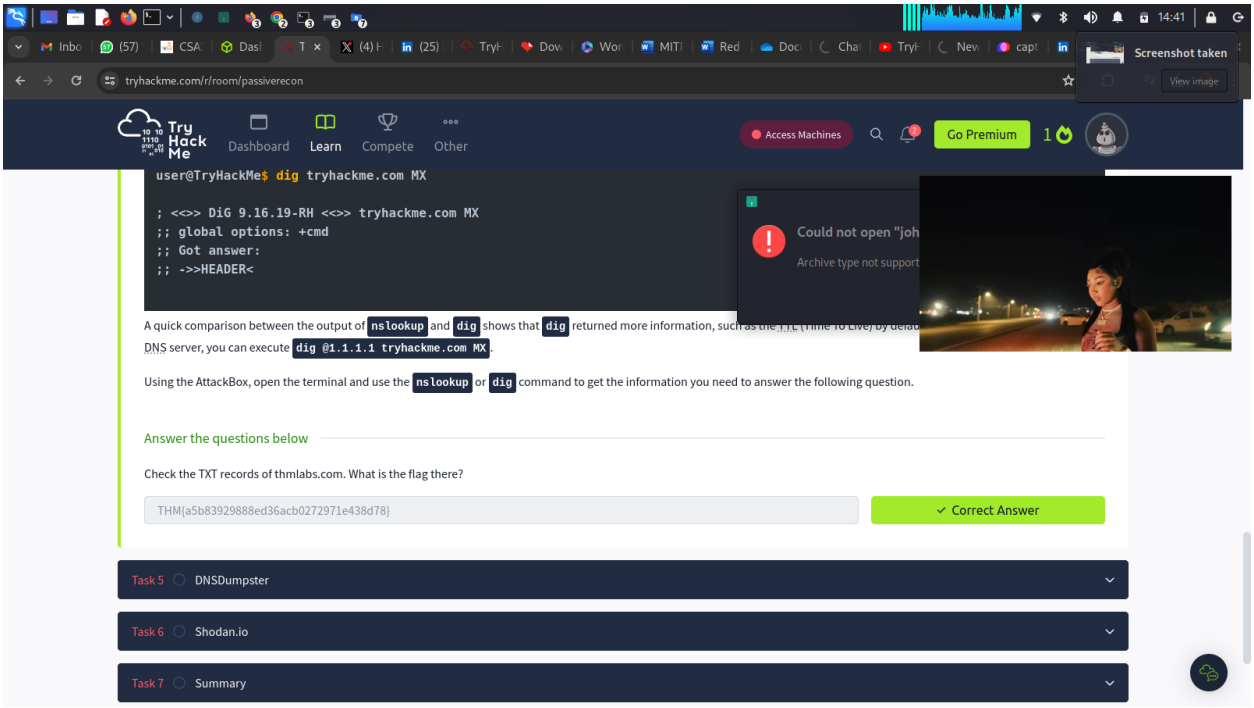


cs-sa07-24019
John_Mbithi_Mutave

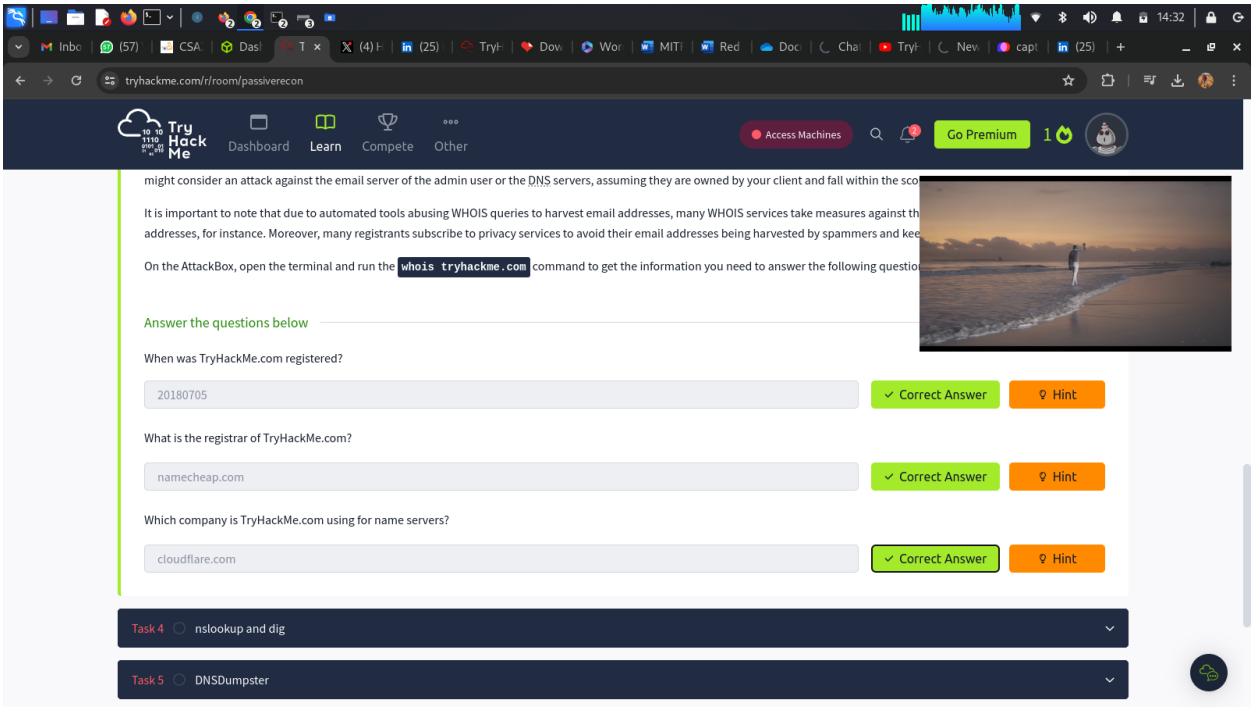


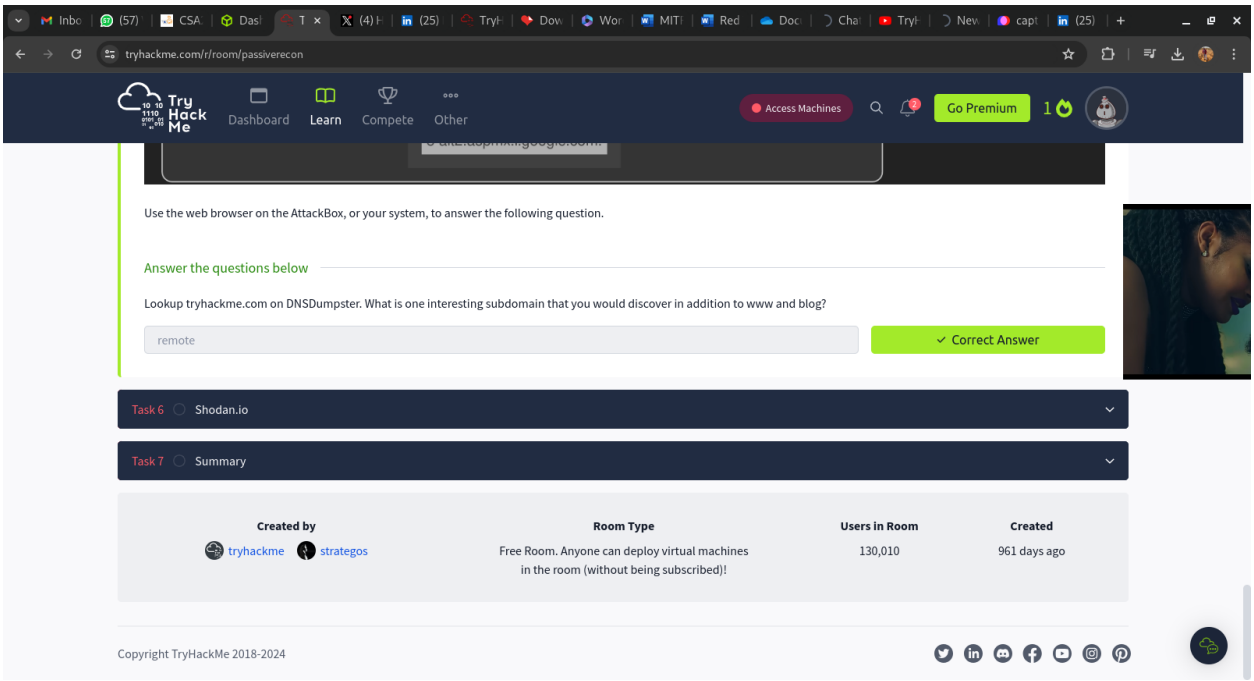


cs-sa07-24019
John_Mbithi_Mutave

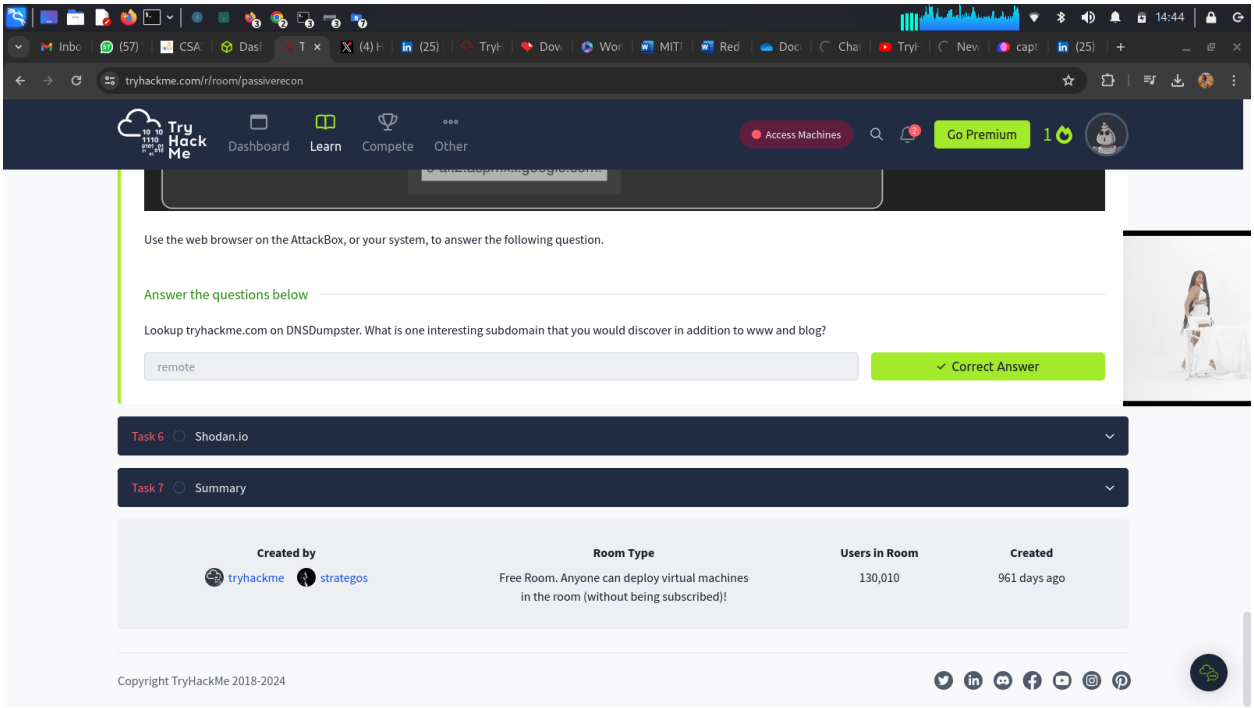


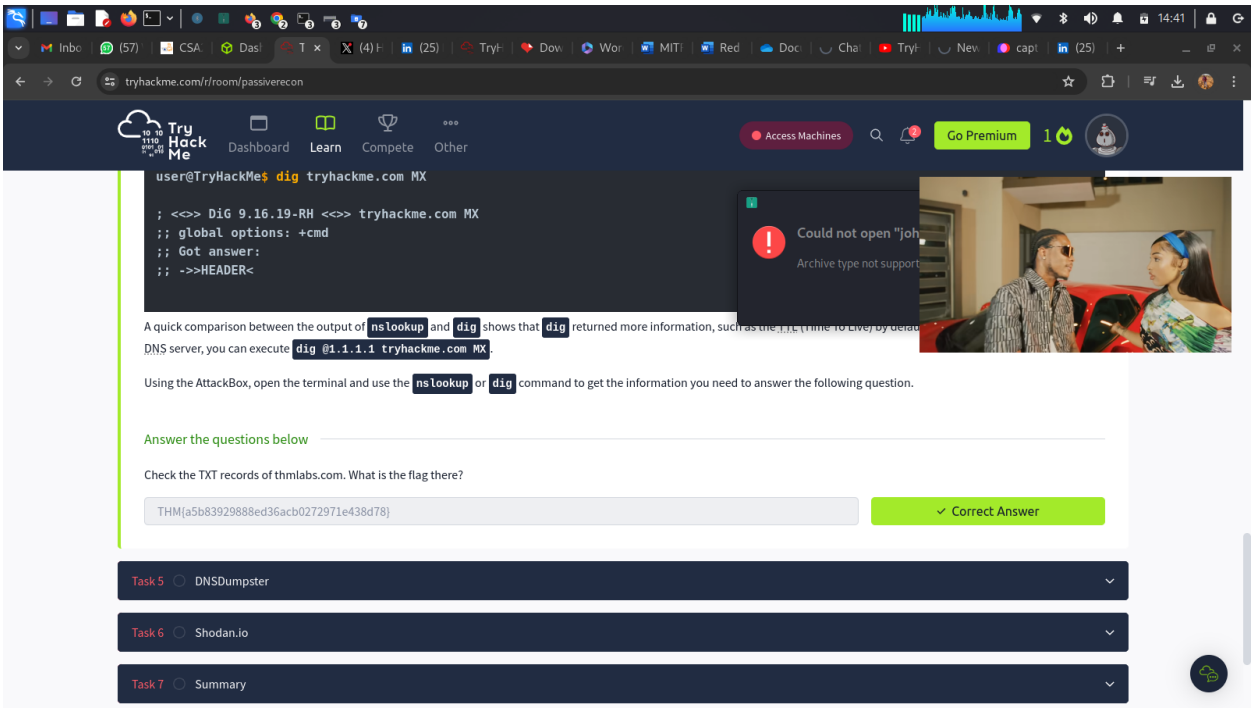
cs-sa07-24019
John_Mbithi_Mutave



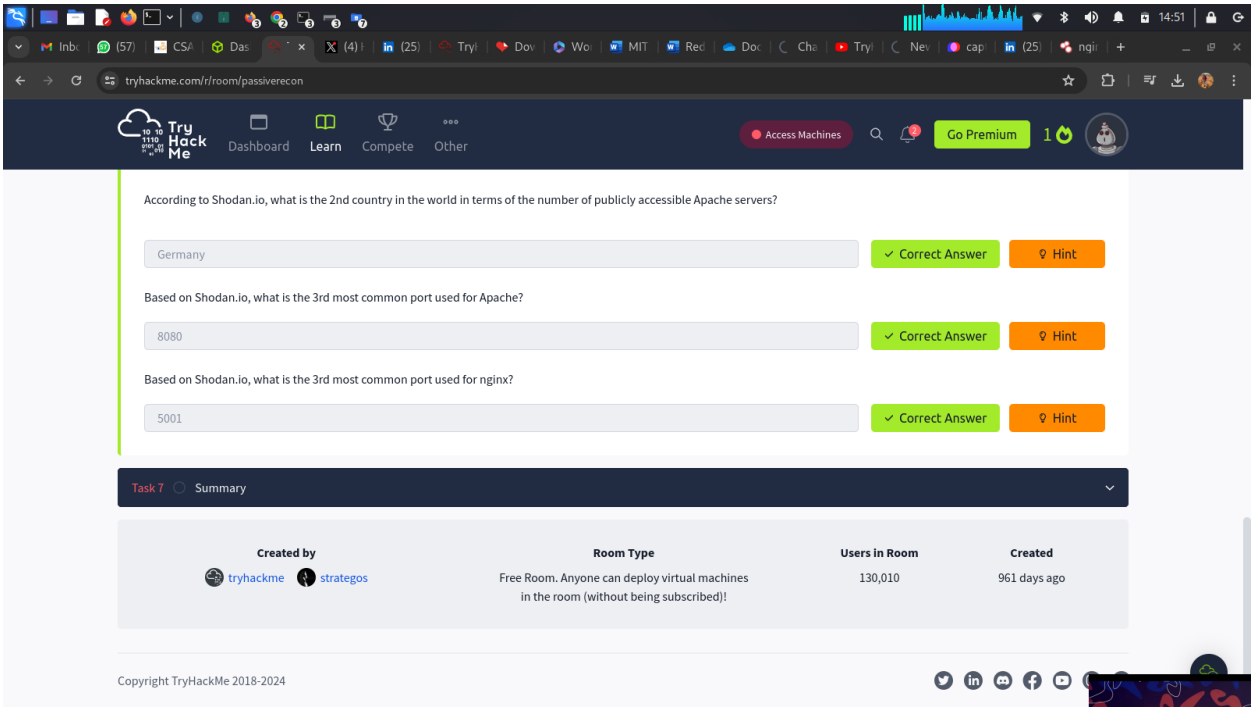


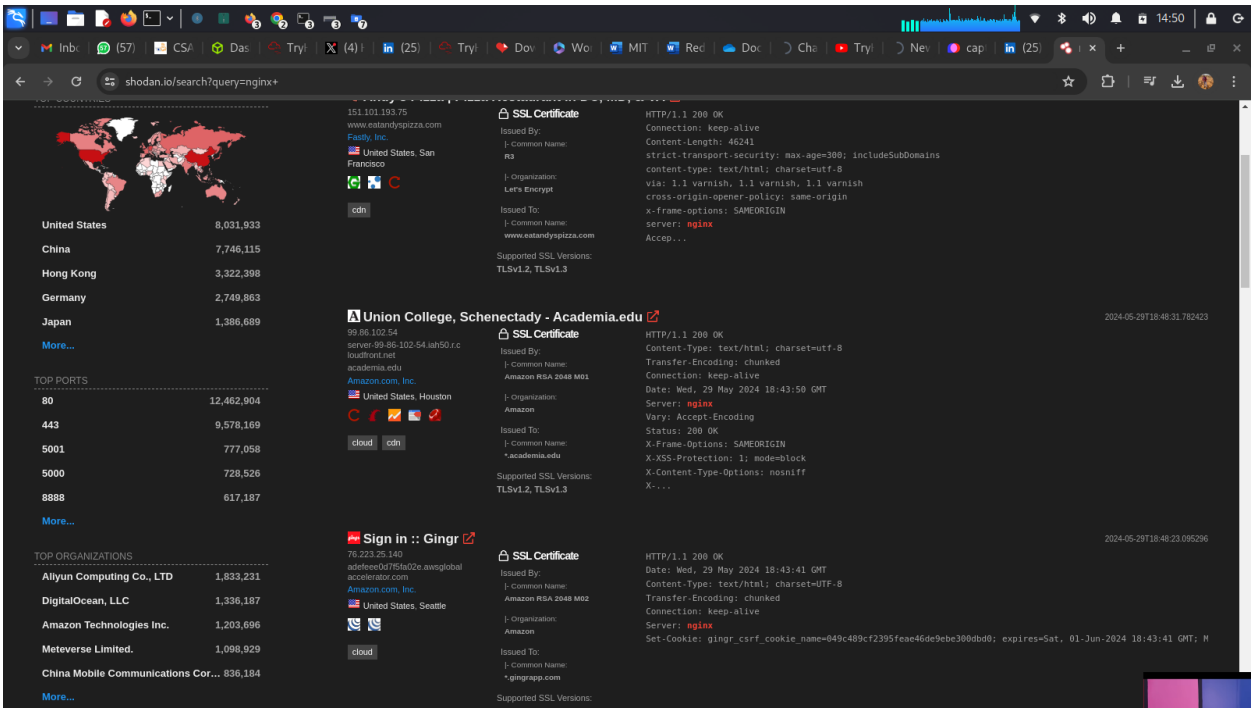
cs-sa07-24019
John_Mbithi_Mutave



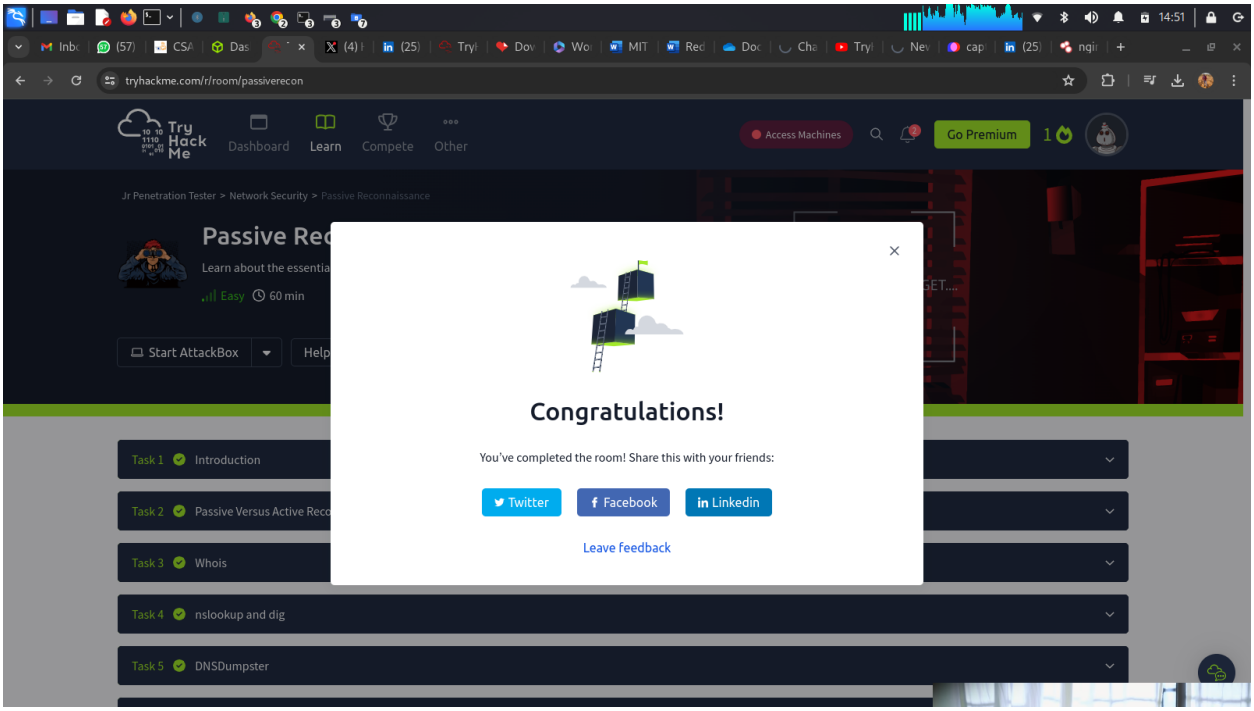


cs-sa07-24019
John_Mbithi_Mutave





cs-sa07-24019
John_Mbithi_Mutave



Shareable link - www.tryhackme.com/r/room/passiverecon

In this room, we focused on passive reconnaissance. In particular, we covered command-line tools, **whois**, **nslookup**, and **dig**. We also discussed two publicly available services DNSDumpster and Shodan.io. The power of such tools is that you can collect information about your targets without directly connecting to them. Moreover, the trove of information you may find using such tools can be massive once you master the search options and get used to reading the results.