Internship Assignment Report: Cyber Security and Digital Forensics

Assignment 3: Reconnaissance

- **TryHackMe Rooms:**
  - Passive Reconnaissance

Assignment Overview

- Welcome to my internship assignment report! This document highlights the cybersecurity and digital forensics challenges I've tackled as part of my Cyber Security and Digital Forensics internship with **CyberSecured India**. The focus of this report is on Passive Reconnaissance, and it includes practical exercises completed on **TryHackMe**.
- Through these assignments, I've had the opportunity to apply theoretical knowledge in real-world scenarios, hone my problem-solving skills, and gain hands-on experience with essential cybersecurity concepts. Each section will walk you through the tasks I've completed, showcasing the steps I took, the tools I used, and the insights I gained along the way.

Background and Prior Experience

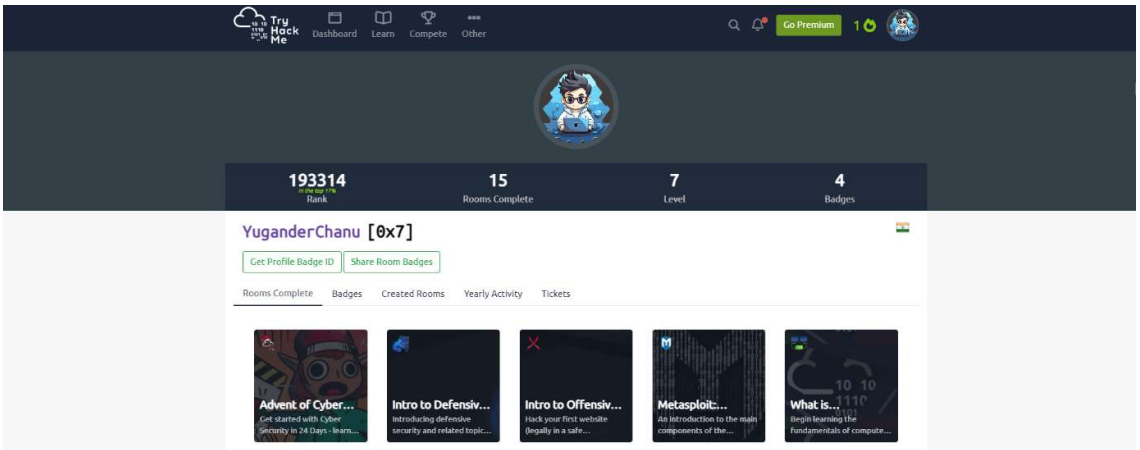
Before starting this internship, I had already completed several rooms on TryHackMe and HackTheBox. This prior experience gave me a solid foundation in cybersecurity principles and practical skills. During the internship, I continued to build on this knowledge by tackling new challenges and applying what I had previously learned in more complex scenarios.

About Me

- **Name:** Yugander Chanupalli
- **Position:** Cyber Security and Digital Forensics
- **Organization:** CyberSecured India
- **Email:** yugander9010@gmail.com
- **Submission Date:** 12/09/2024

TryHackMe

TryHackMe Account Picture:



Passive Reconnaissance

Overview:

In the "Passive Reconnaissance" room on TryHackMe, I got hands-on experience with tools and techniques used to gather information about targets without making direct contact. This room was all about exploring how to use command-line tools and publicly available services to collect data stealthily. What’s cool is that these tools can provide a massive amount of information once you know how to use them and interpret the results effectively.

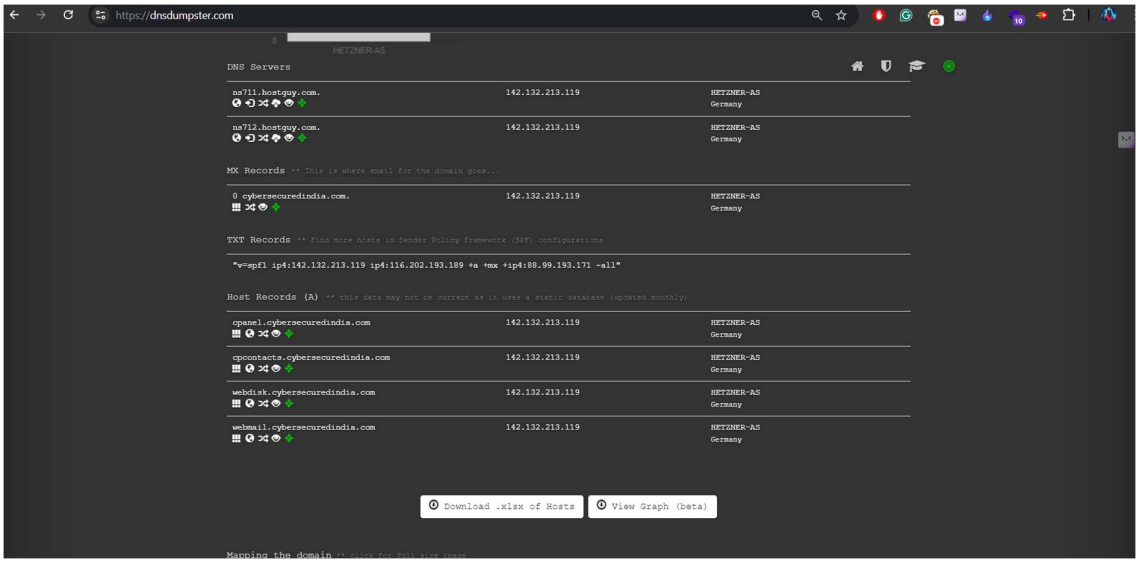
Key Tools and Techniques Learned:

Throughout this room, I focused on several command-line tools and online services that are essential for passive reconnaissance:

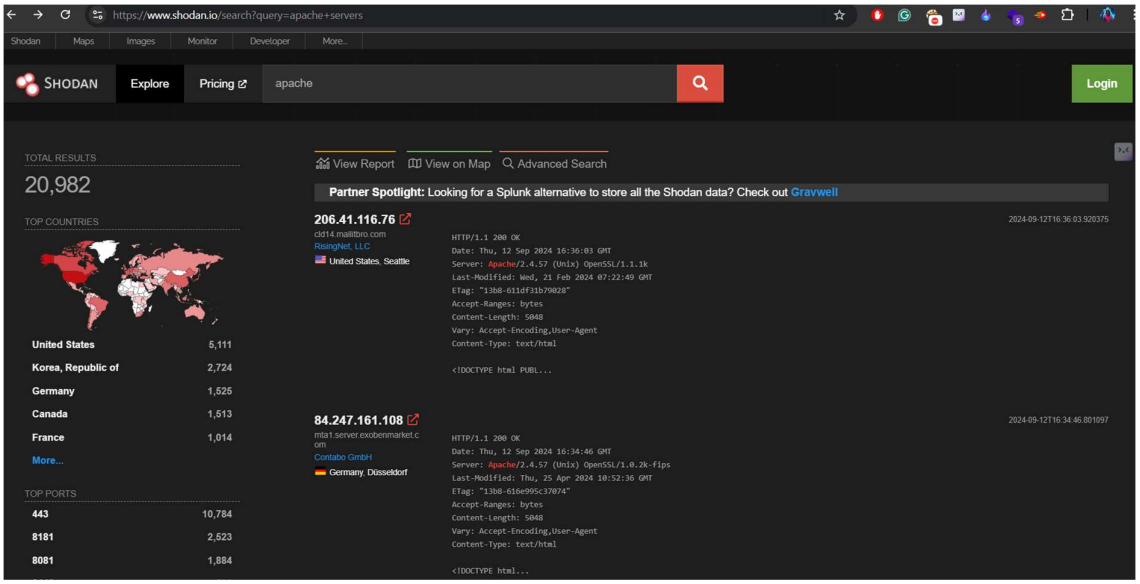
- **Command-line Tools:**
  - **whois:** This tool is like a treasure map for domain registration details. Running a simple whois tryhackme.com command can tell you a lot about who owns a domain, when it was registered, and when it might expire.
  - **nslookup:** I learned how to use nslookup to find different DNS records like A, MX, and TXT. For example, using nslookup -type=A tryhackme.com helped me find the IP addresses tied to the domain. It's quite powerful for getting quick insights.
  - **dig:** This tool is like nslookup but more advanced and flexible. Commands like dig tryhackme.com A and dig @1.1.1.1 tryhackme.com MX allowed me to get deeper into DNS querying. It's pretty handy when you need more control and detail in your queries.
- **Public Services:**
  - **DNSDumpster:** A fantastic tool for visualizing and mapping a domain's infrastructure. It helped me see subdomains and how they connect, which is super useful for understanding a target's broader digital landscape.
  - **Shodan.io:** This is basically a search engine for internet-connected devices. It's incredible what kind of exposed services and devices you can find with a bit of searching. It really shows the importance of securing everything that's connected to the web.

Proof of concept:

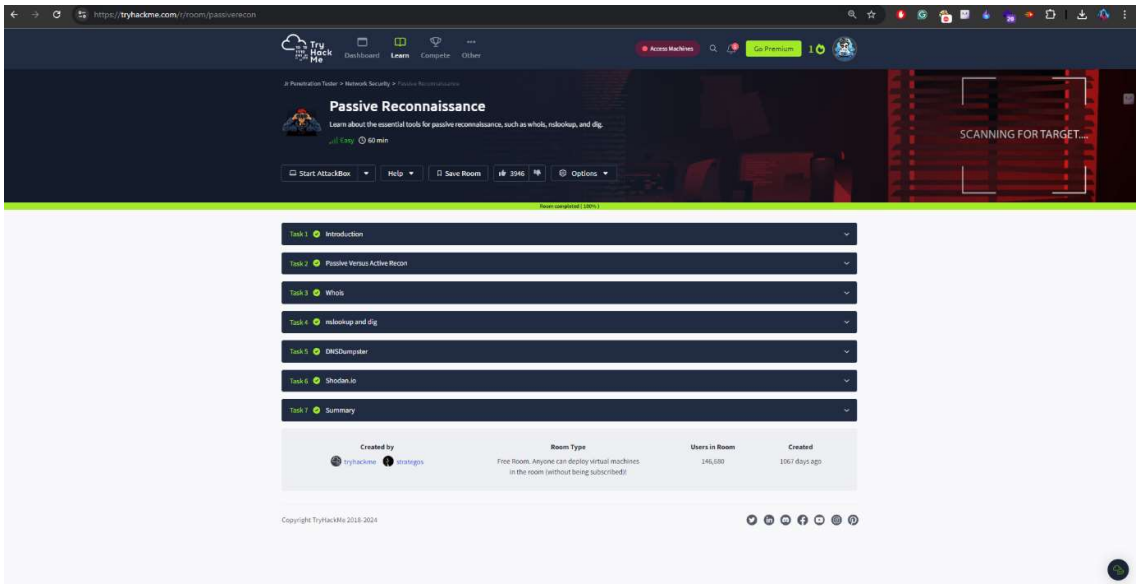
I understood the concept by completing using the publicly available tools. Below image demonstrates the using of dnsdumpster.com to find all domain information about cybersecuredindia.com.



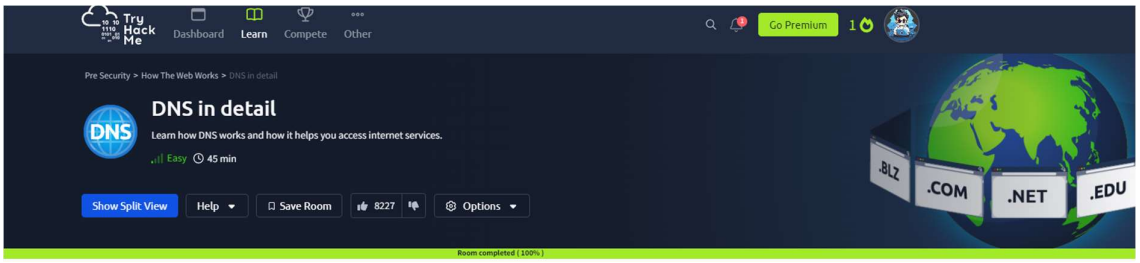
And also,working with shodan helped me to understand the details of devices which are alive on internet.

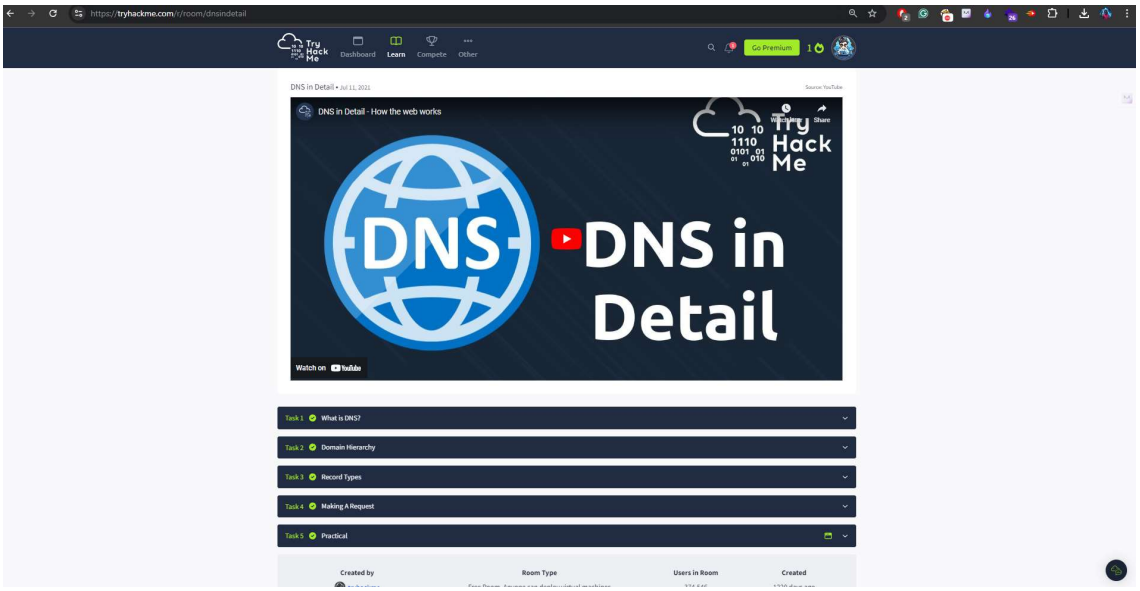


Finally, completed the all tasks that are related to this room helped me to understand the use of reconnaissance importance.



During the completion of this room I also did another room which explains the concepts of DNS and its working.





This room explained me how the dns works on internet and also what are the records that are most important for pentesters to find sensitive vulnerabilities.