

# 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

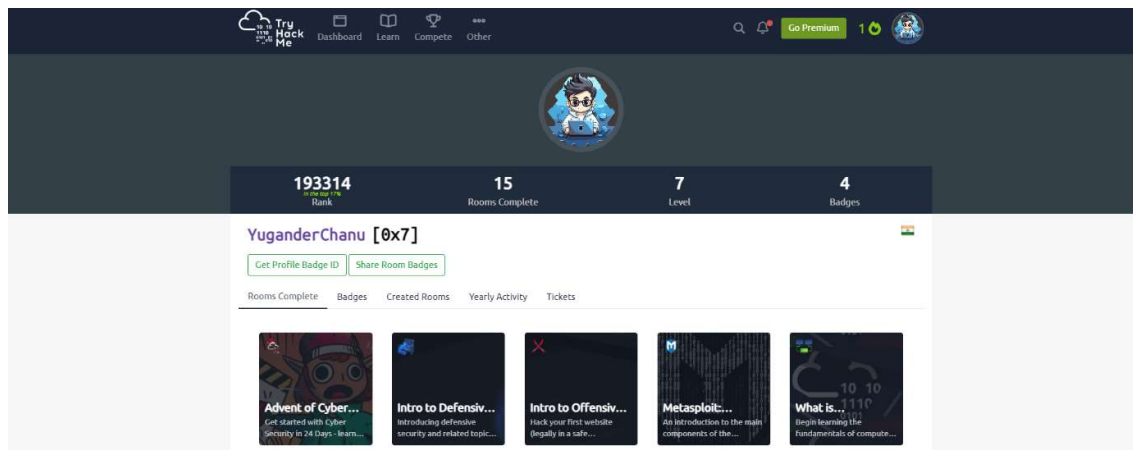
Before starting this internship, I had already completed several rooms on TryHackMe and HackTheBox. This prior experience gave me a solid foundation in cybersecurity principles and practical skills. During the internship, I continued to build on this knowledge by tackling new challenges and applying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

https://dnshumpster.com

NETZNER-AS

DNS Servers		
ns711.hostguy.com.	142.132.213.119	NETZNER-AS Germany
ns712.hostguy.com.	142.132.213.119	NETZNER-AS Germany

**MX Records** \*\* This is where email for the domain goes...

0 cyberscuredindia.com.	142.132.213.119	NETZNER-AS Germany
-------------------------	-----------------	-----------------------

**TXT Records** \*\* Find more hosts in Sender Policy Framework (SPF) configurations

```
*vwapfl ip4:142.132.213.119 ip4:116.202.193.189 *a *mx *ip4:88.99.193.171 -all*
```

**Host Records (A)** \*\* this data may not be current as it uses a static database (updated monthly)

cpas1.cyberscuredindia.com	142.132.213.119	NETZNER-AS Germany
cpcontacts.cyberscuredindia.com	142.132.213.119	NETZNER-AS Germany
webdisk.cyberscuredindia.com	142.132.213.119	NETZNER-AS Germany
webmail.cyberscuredindia.com	142.132.213.119	NETZNER-AS Germany

Download .xlsx of Hosts View Graph (beta)

Mapping the domain as ip:netzner-india.com

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

https://www.shodan.io/search?query=apache-servers

Shodan Maps Images Monitor Developer More...

SHODAN Explore Pricing apache Login

TOTAL RESULTS: 20,982

TOP COUNTRIES

United States	5,111
Korea, Republic of	2,724
Germany	1,525
Canada	1,513
France	1,014
More...	

TOP PORTS

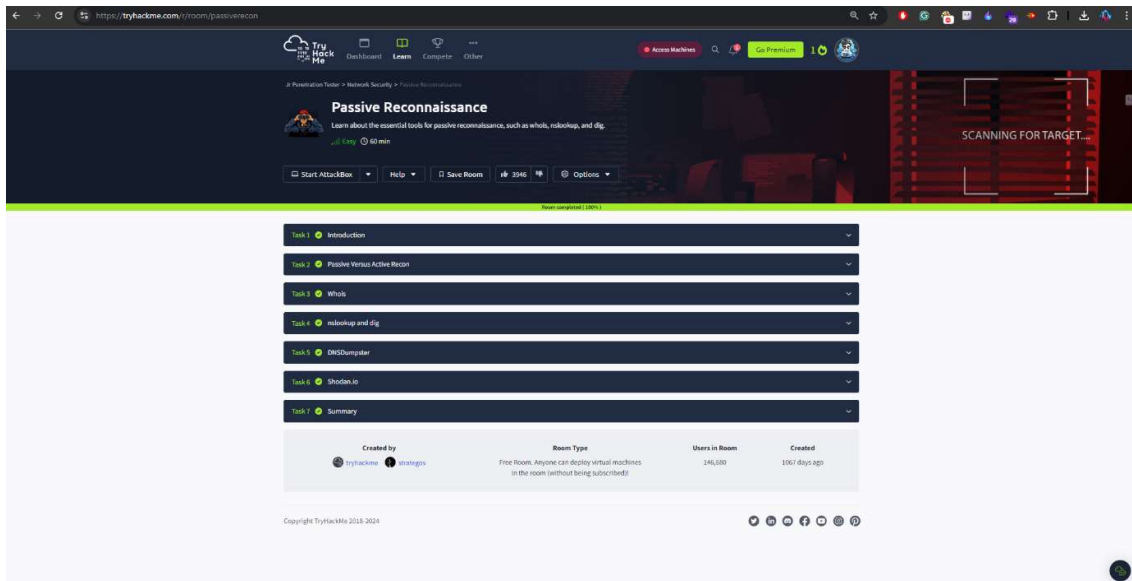
443	10,784
8181	2,523
8081	1,884

View Report View on Map Advanced Search

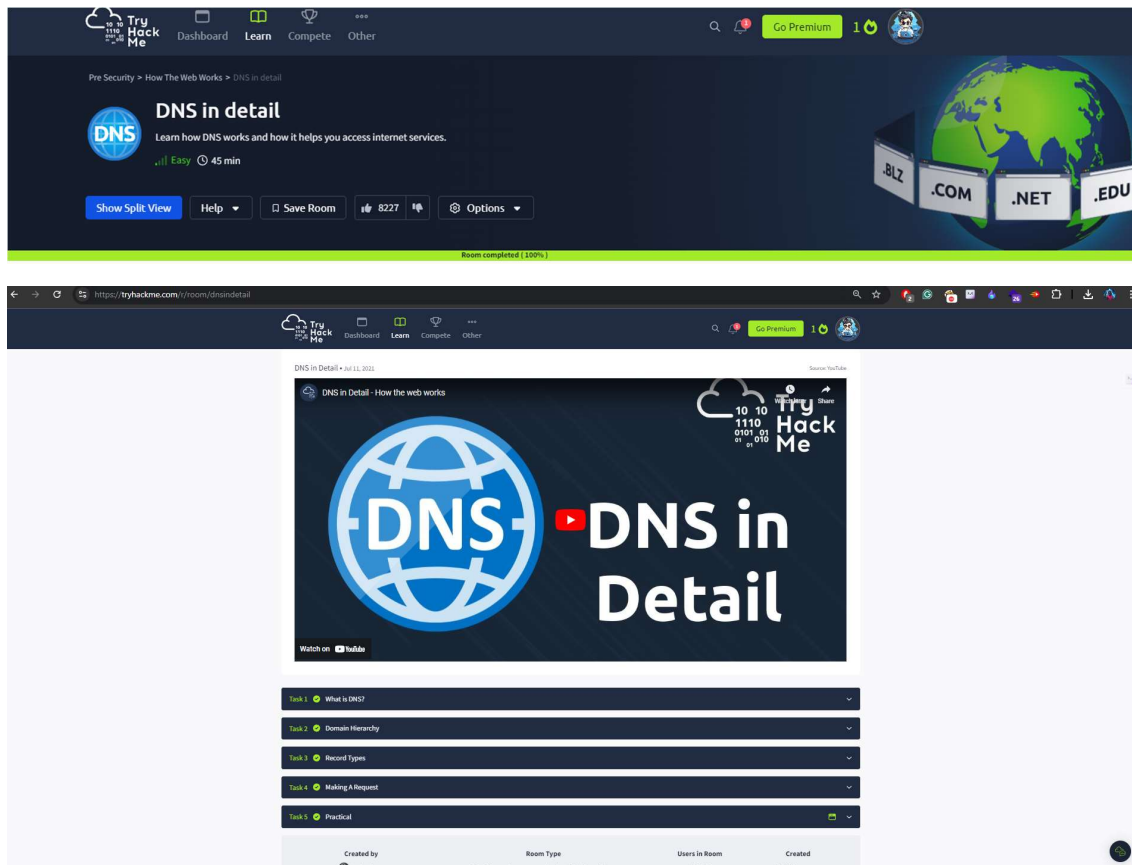
Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out [Gravwell](#)

<p><b>206.41.116.76</b></p> <p>0814.netltd.com RisingNet, LLC United States, Seattle</p>	<p>HTTP/1.1 200 OK Date: Thu, 12 Sep 2024 16:36:03 GMT Server: Apache/2.4.57 (Ubuntu) OpenSSL/1.1.1k Last-Modified: Wed, 21 Feb 2024 07:22:49 GMT ETag: "110b-611df31b79028" Accept-Ranges: bytes Content-Length: 5848 Vary: Accept-Encoding, User-Agent Content-Type: text/html</p> <p>&lt;!DOCTYPE html PUBL...</p> <p>2024-09-12T16:36:03.520375</p>
<p><b>84.247.161.108</b></p> <p>mta1.server.exobrainmarket.com Conabo GmbH Germany, Düsseldorf</p>	<p>HTTP/1.1 200 OK Date: Thu, 12 Sep 2024 16:34:46 GMT Server: Apache/2.4.57 (Ubuntu) OpenSSL/1.0.2k-fips Last-Modified: Thu, 25 Apr 2024 10:52:36 GMT ETag: "110b-616995c37074" Accept-Ranges: bytes Content-Length: 5848 Vary: Accept-Encoding, User-Agent Content-Type: text/html</p> <p>&lt;!DOCTYPE html...</p> <p>2024-09-12T16:34:46.801997</p>

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.

Task 1: Practical

Using the website on the right, we can build requests to make DNS queries and view the results. The website will also show you the command you'll need to run on your own computer if you wished to make the requests yourself.

Answer the questions below

What is the CNAME of shop.website.thm?

shop.website.thm

Correct Answer

What is the value of the NS record of website.thm?

127.0.0.53

Correct Answer

What is the numerical priority value for the MX record?


10

Correct Answer

What is the IP address for the A record of www.website.thm?

10.10.10.10

Correct Answer

Created by:  aPhishme

Room Type: Free Room. Anyone can destroy virtual machines at the room (without being notified)

Users in Room: 214,345

Created: 1222 days ago

DNS Type: website.thm

Send DNS Request

Address: 127.0.0.53

Non-authoritative answer:

website.thm text = "TIM7812886899773549516C2E16D2948FFJ"

user@thm: ~\$ nslookup --type=MX website.thm

Server: 127.0.0.53

Address: 127.0.0.53

Non-authoritative answer:

website.thm mail exchanger = 10 alt4.aspmx.l.google.com

user@thm: ~\$ nslookup --type=A website.thm

Server: 127.0.0.53

Address: 127.0.0.53

Non-authoritative answer:

name: website.thm

Address: 10.10.10.10

user@thm: ~\$ nslookup website.thm