



## TASK 2: ACTIVE & PASSIVE RECONNAISSANCE

### WHAT IS RECONNAISSANCE?

Reconnaissance, often called "recon" in cybersecurity and intelligence fields, refers to the initial phase of gathering information about a target. The goal is to collect data that can help reveal potential weaknesses or vulnerabilities in systems, networks, or applications. Reconnaissance is critical for both attackers and defenders: attackers use it to understand and exploit possible entry points, while defenders use it to identify and mitigate potential threats.

---

### What is the difference between Active and Passive Recon?

Reconnaissance typically involves two main types: **Passive Recon** and **Active Recon**.

#### **Passive reconnaissance:**

It includes gathering data without direct interaction with the target, such as researching public records, analyzing social media, or studying network information from external sources.

#### **Active reconnaissance:**

On the other hand, involves directly engaging with the target through actions like pinging servers, scanning ports, or using automated tools to gather technical details.

By performing reconnaissance, security professionals can better understand their environment and strengthen defenses, reducing the risk of successful attacks.

---

### Tools used for Active and Passive Recon?

Active and passive reconnaissance rely on specialized tools to gather information about a target, each suited to either direct or indirect methods of data collection.

#### **Passive Reconnaissance Tools**

Passive reconnaissance involves gathering information without interacting directly with the target, helping to avoid detection. Common tools include:

- OSINT Framework: A collection of tools that help locate public data, from social media profiles to geolocation data, useful in building a profile without alerting the target.
- Shodan: A search engine for internet-connected devices, revealing information about devices on a network, such as routers or cameras, without direct access.

- Maltego: A data visualization tool that maps relationships between entities, like people and organizations, which is useful in examining public connections.

### Active Reconnaissance Tools

Active reconnaissance involves direct engagement with a target, making it more detectable but often more detailed. Popular active recon tools include:

- Nmap: A network scanner used to detect live hosts, open ports, services, and operating systems on a network.
- Metasploit: A framework that automates the discovery of vulnerabilities and offers tools for testing them.
- Wireshark: A packet analyzer that captures and inspects data packets traveling over a network, helping to uncover information like communication patterns or protocols.

Both passive and active recon tools are essential for developing a comprehensive view of potential vulnerabilities, aiding both security professionals and ethical hackers in their assessments.



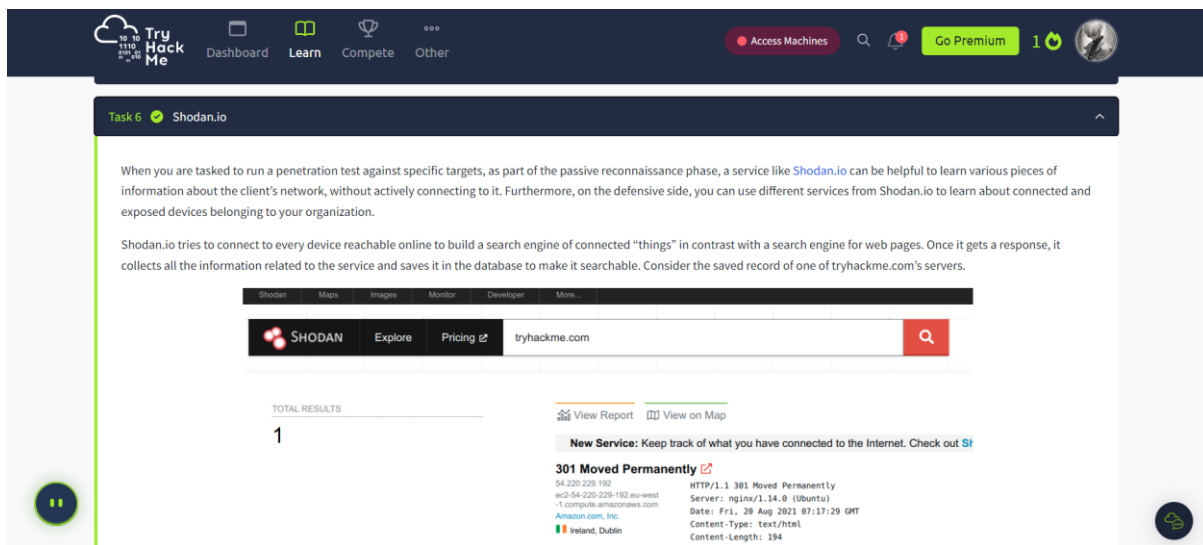
**PASSIVE RECON TOOL**



**ACTIVE RECON TOOL**

EYEQ DOT NET

## Passive Reconnaissance on TryHackMe:



**Task 6** ✔ Shodan.io

When you are tasked to run a penetration test against specific targets, as part of the passive reconnaissance phase, a service like [Shodan.io](#) can be helpful to learn various pieces of information about the client's network, without actively connecting to it. Furthermore, on the defensive side, you can use different services from Shodan.io to learn about connected and exposed devices belonging to your organization.

Shodan.io tries to connect to every device reachable online to build a search engine of connected "things" in contrast with a search engine for web pages. Once it gets a response, it collects all the information related to the service and saves it in the database to make it searchable. Consider the saved record of one of tryhackme.com's servers.

Shodan Maps Images Monitor Developer More

SHODAN

Explore

Pricing

tryhackme.com

Q

TOTAL RESULTS

1

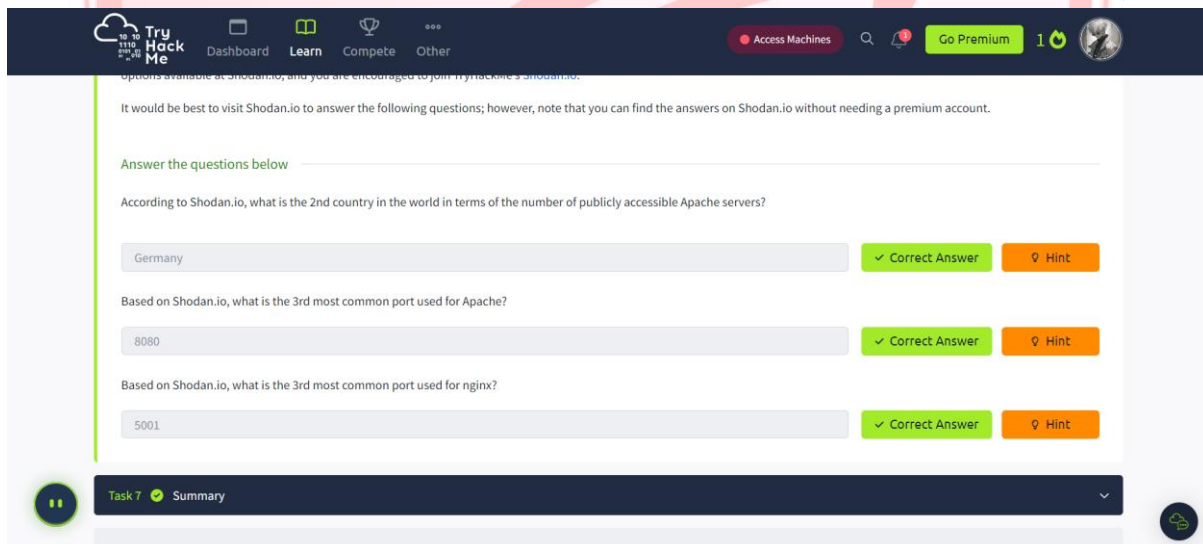
View Report

View on Map

New Service: Keep track of what you have connected to the Internet. Check out [SI](#)

301 Moved Permanently

54.220.228.192 HTTP/1.1 301 Moved Permanently  
ec2-54-220-229-192.eu-west-1.compute.amazonaws.com Server: nginx/1.14.0 (Ubuntu)  
Amazon.com, Inc. Date: Fri, 20 Aug 2021 07:17:29 GMT  
Content-Type: text/html  
Content-Length: 194  
Connection: keep-alive



**Task 7** ✔ Summary

Options available at Shodan.io, and you are encouraged to join TryHackMe's [Shodan.io](#).

It would be best to visit Shodan.io to answer the following questions; however, note that you can find the answers on Shodan.io without needing a premium account.

Answer the questions below

According to Shodan.io, what is the 2nd country in the world in terms of the number of publicly accessible Apache servers?

Germany

✔ Correct Answer

Hint

Based on Shodan.io, what is the 3rd most common port used for Apache?

8080

✔ Correct Answer

Hint

Based on Shodan.io, what is the 3rd most common port used for nginx?

5001

✔ Correct Answer

Hint

## References:

<https://chatgpt.com>

<https://www.google.co.in>

TryHackMe | Cyber Security Training