EyeQ Dot Net Pvt. Ltd.
LEARN FROM REAL HACKERS

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

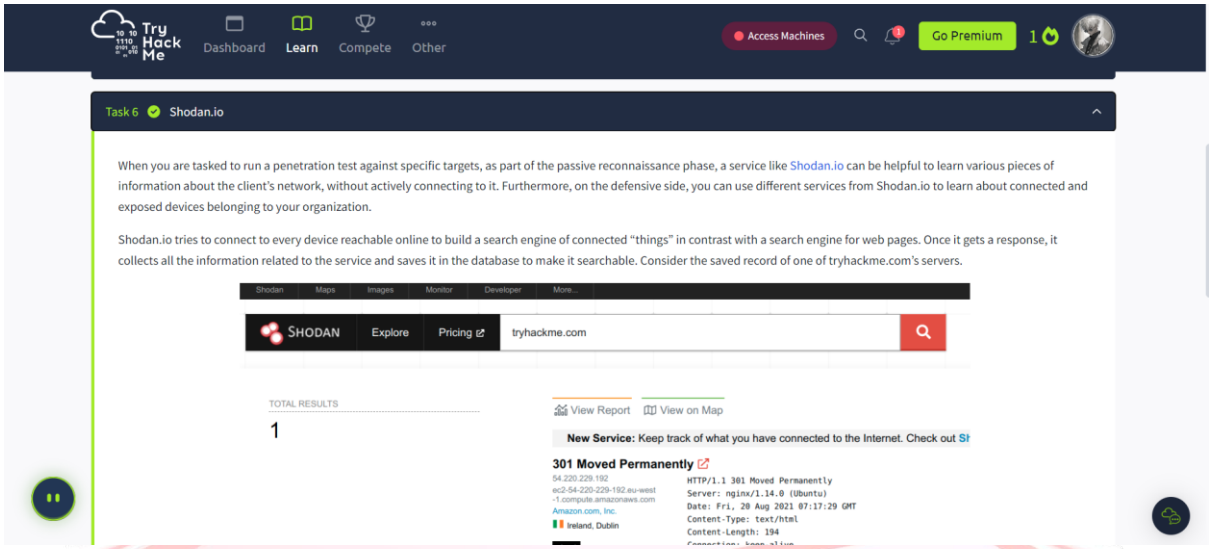
Active reconnaissance involves direct engagement with a target, making it more detectable but often more detailed. Popular active recon tools include:

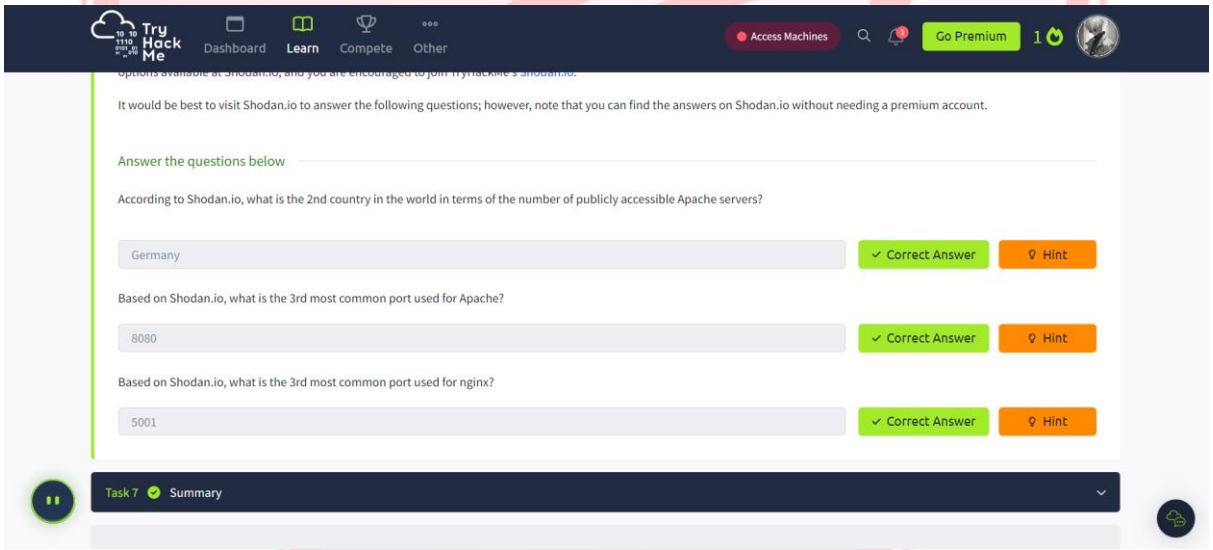
- Nmap: A network scanner used to detect live hosts, open ports, services, and operating systems on a network.
- Metasploit: A framework that automates the discovery of vulnerabilities and offers tools for testing them.
- Wireshark: A packet analyzer that captures and inspects data packets traveling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

Passive Reconnaissance on TryHackMe:





References:

https://chatgpt.com

https://www.google.co.in

TryHackMe | Cyber Security Training