

Name: SASIKUMAR.B

Ex. No.: 3

Roll No:231901047

PASSIVE AND ACTIVE RECONNAISSANCE

Aim:

To do perform passive and active reconnaissance in TryHackMe platform.

Algorithm:

1. Access the Passive reconnaissance lab in TryHackMe platform using the link below-
<https://tryhackme.com/r/room/passiverecon>
2. Click Start AttackBox to run the instance of Kali Linux distribution.
3. Run whois command on the website tryhackme.com and gather information about it.
4. Find the IP address of tryhackme.com using nslookup and dig command.
5. Find out the subdomain of tryhackme.com using DNSDumpster command.
6. Run shodan.io to find out the details- IP address, Hosting Company, Geographical location and Server type and version.
7. Access the Active reconnaissance lab in TryHackMe platform using the link below-
<https://tryhackme.com/r/room/activerecon>
8. Click Start AttackBox to run the instance of Kalilinux distribution.
9. Perform active reconnaissance using the commands, traceroute, ping and netcat.

Output:

ACTIVE RECONNAISSANCE

The screenshot displays the TryHackMe 'Active Reconnaissance' room interface. At the top, there's a navigation bar with the TryHackMe logo and links to Dashboard, Learn, Compete, and Other. Below this, the room title 'Active Reconnaissance' is prominently displayed, along with a description: 'Learn how to use simple tools such as traceroute, ping, telnet, and a web browser to gather information.' The room is marked as 'Easy' and takes '60 min' to complete. A green bar at the bottom indicates 'Room completed (100%)'. Below this, a list of tasks is shown, each with a green checkmark indicating completion:

- Task 1 Introduction
- Task 2 Web Browser
- Task 3 Ping
- Task 4 Traceroute
- Task 5 Telnet
- Task 6 Netcat
- Task 7 Putting It All Together

PASSIVE RECONNAISSANCE

The screenshot displays the TryHackMe interface for the 'Passive Reconnaissance' room. The top navigation bar includes links to Dashboard, Learn, Compete, and Other, along with a 'Go Premium' button and a user profile icon. The room title 'Passive Reconnaissance' is prominently displayed, followed by a description: 'Learn about the essential tools for passive reconnaissance, such as whois, nslookup, and dig.' Below this, a green button 'Share your achievement' and a 'Start AttackBox' button are visible. A list of seven tasks is shown, each with a green checkmark indicating completion. The tasks are: Task 1 Introduction, Task 2 Passive Versus Active Recon, Task 3 Whois, Task 4 nslookup and dig, Task 5 DNSDumpster, Task 6 Shodan.io, and Task 7 Summary. A green bar at the bottom of the task list indicates 'Room completed (100%)'.

Learn > Passive Reconnaissance

Passive Reconnaissance

Learn about the essential tools for passive reconnaissance, such as whois, nslookup, and dig.

Easy 60 min

Share your achievement Start AttackBox Help Save Room 4159 Options

Room completed (100%)

- Task 1 Introduction
- Task 2 Passive Versus Active Recon
- Task 3 Whois
- Task 4 nslookup and dig
- Task 5 DNSDumpster
- Task 6 Shodan.io
- Task 7 Summary

Result:

Thus, the passive and active reconnaissance has been performed successfully in TryHackMe platform.