

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

TryHackMe

Dashboard Learn Compete Other

Access Machines Go Premium 1 U

Learn > Active Reconnaissance

Active Reconnaissance

Learn how to use simple tools such as traceroute, ping, telnet, and a web browser to gather information.

Easy 60 min

Share your achievement Start AttackBox Help Save Room 2818 Options

Room completed (100%)

- 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 shows the TryHackMe interface for the 'Passive Reconnaissance' room. The top navigation bar includes 'TryHackMe', 'Dashboard', 'Learn', 'Compete', and 'Other'. A red 'Access Machines' button, a search icon, a 'Go Premium' button, and a user profile icon are on the right. The room title 'Passive Reconnaissance' is displayed with a description: 'Learn about the essential tools for passive reconnaissance, such as whois, nslookup, and dig.' It is marked as 'Easy' and '60 min'. A green 'Share your achievement' button and a 'Start AttackBox' button are visible. The room status is 'Room completed (100%)'. A list of tasks is shown on the left, each with a green checkmark and a dropdown arrow:

- 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

The background image shows a server room with the text 'SCANNING FOR TARGET...' overlaid.

Result:

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