

Name: MOHAMED ARSATH A

Ex. No.: 3

Roll No:231901030

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

PASSIVE RECONNAISSANCE

The screenshot shows the TryHackMe interface for the 'Passive Reconnaissance' room. The top navigation bar includes the TryHackMe logo, a menu with 'Dashboard', 'Learn', 'Compete', and 'Other', and user options like 'Access Machines', 'Go Premium', and a profile icon. The room title 'Passive Reconnaissance' is prominently displayed, along with a description: 'Learn about the essential tools for passive reconnaissance, such as whois, nslookup, and dig.' It is marked as 'Easy' and takes '60 min'. A progress bar at the top indicates 'Room completed (100%)'. Below the title, there are buttons for 'Share your achievement', 'Start AttackBox', 'Help', 'Save Room', and a '4158' likes count. A list of seven tasks is shown, each with a green checkmark indicating completion: 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. The background features a dark theme with a red and black grid pattern and the text 'SCANNING FOR TARGET...'. A play button icon is visible in the bottom left corner.

TryHackMe

Dashboard Learn Compete Other

Access Machines Go Premium 1

CompTIA Pentest+ > Information Gathering and Vulnerability Scanning > 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 4158 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.