

PASSIVE AND ACTIVE RECONNAISSANCE

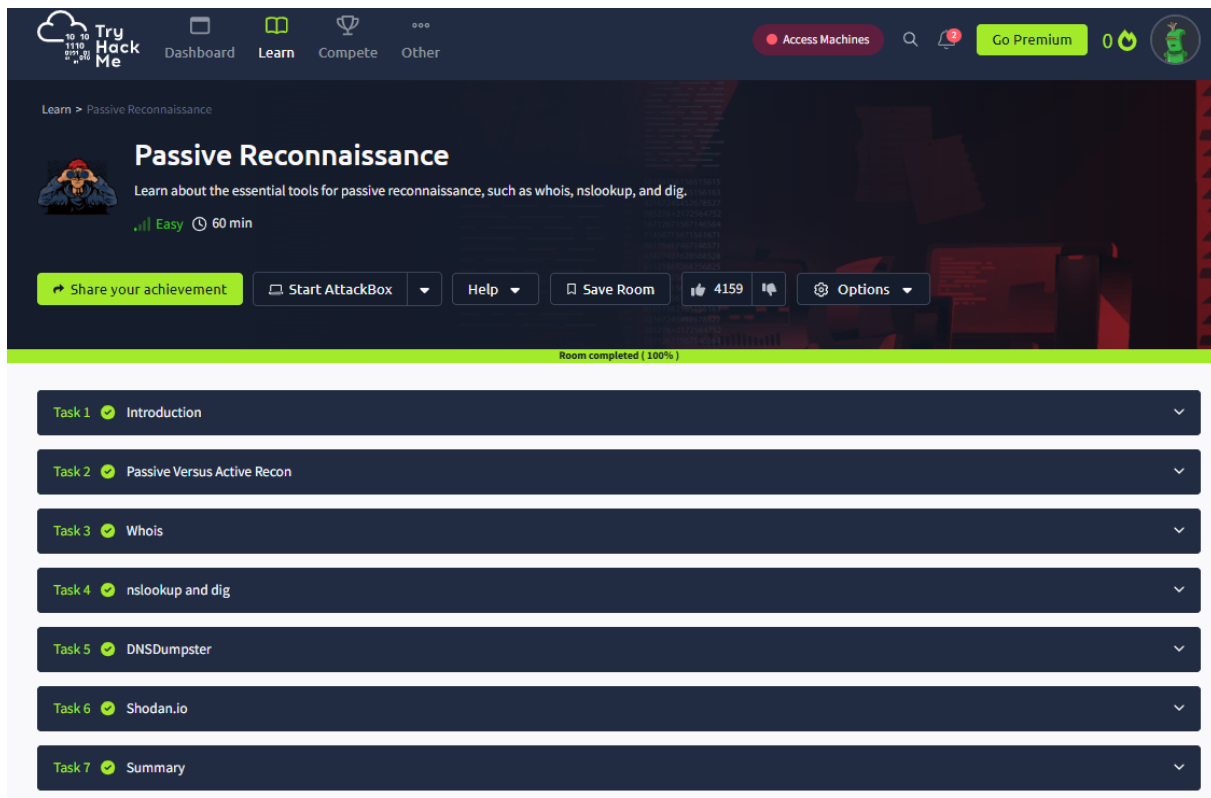
Aim:

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:



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 buttons for Access Machines, Go Premium, 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.' The difficulty level is 'Easy' and the estimated time is '60 min'. Below this, there are buttons for 'Share your achievement', 'Start AttackBox', 'Help', 'Save Room', a like count of 4159, and an 'Options' dropdown. A green bar at the bottom of the room header indicates 'Room completed (100%)'. The main content area lists seven tasks, all of which are marked as completed with green checkmarks:

- 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

Shodan
Maps
Images
Monitor
Developer
More...

SHODAN

Explore
Pricing

TOTAL RESULTS

1

View Report

View on Map

New Service: Keep track of what you have connected to the Internet. Check out S

301 Moved Permanently

54.220.229.192

HTTP/1.1 301 Moved Permanently

Server: nginx/1.14.0 (Ubuntu)

Date: Fri, 20 Aug 2021 07:17:29 GMT

Content-Type: text/html

Content-Length: 194

Location: https://54.220.229.192/

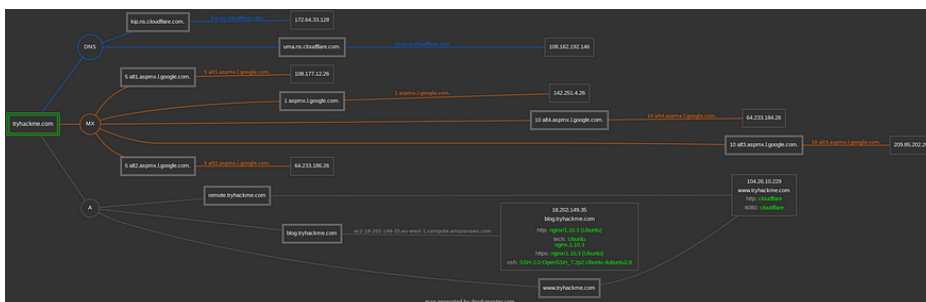
X-Frame-Options: ALLOW-FROM https://tryhackme.com


aws2-54-220-229-192.eu-west-1.compute.amazonaws.com

Amazon.com, Inc.

Inland, Dublin

cloud





Dashboard

Learn


Complete

Other


Access Machines

Go Premium

0





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

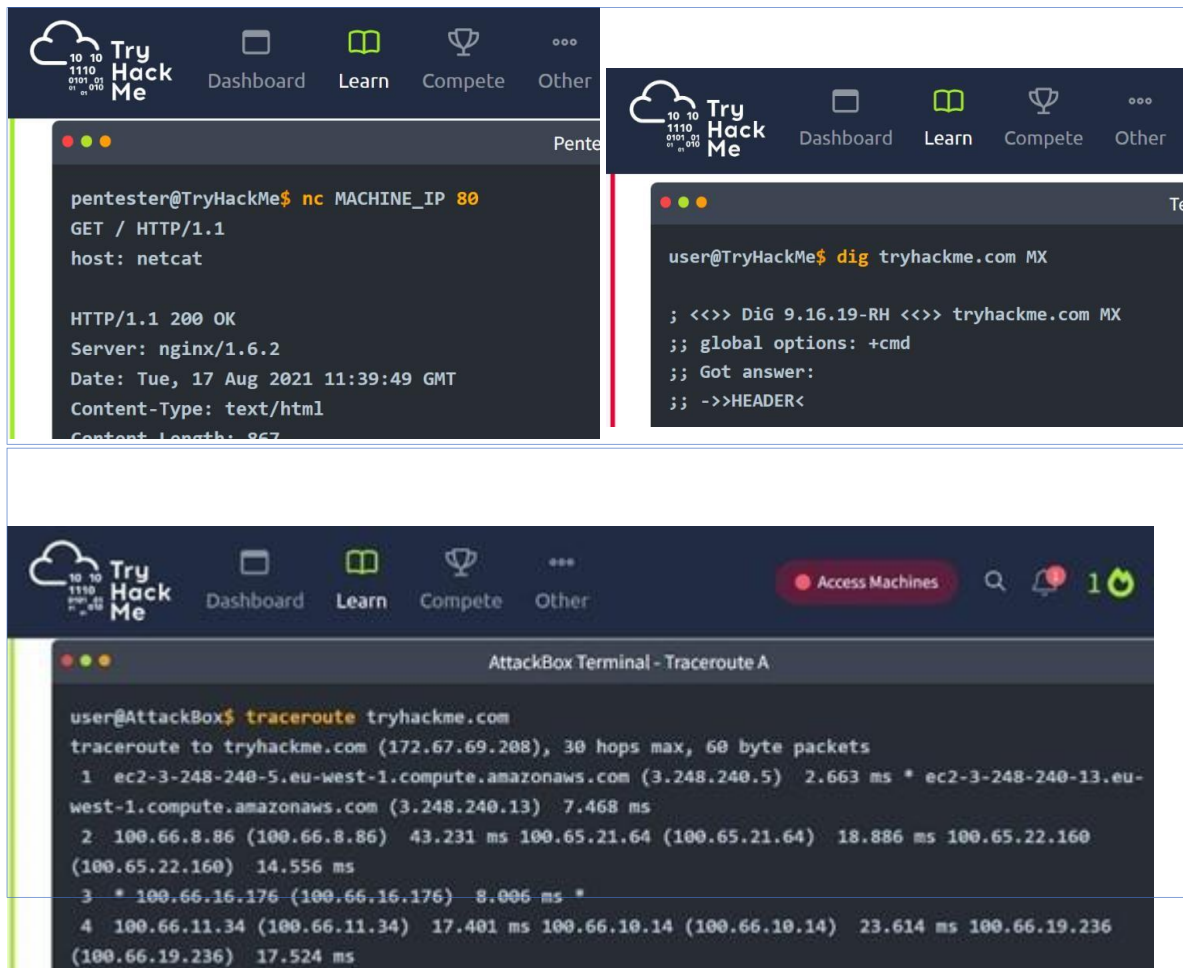
Task 3  Ping

Task 4  Traceroute

Task 5  Telnet

Task 6  Netcat

Task 7  Putting It All Together



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