

Ex. No.: 3

Date:20.08.2024

PASSIVE AND ACTIVE RECONNAISSANCE

Aim:

To 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/t/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.

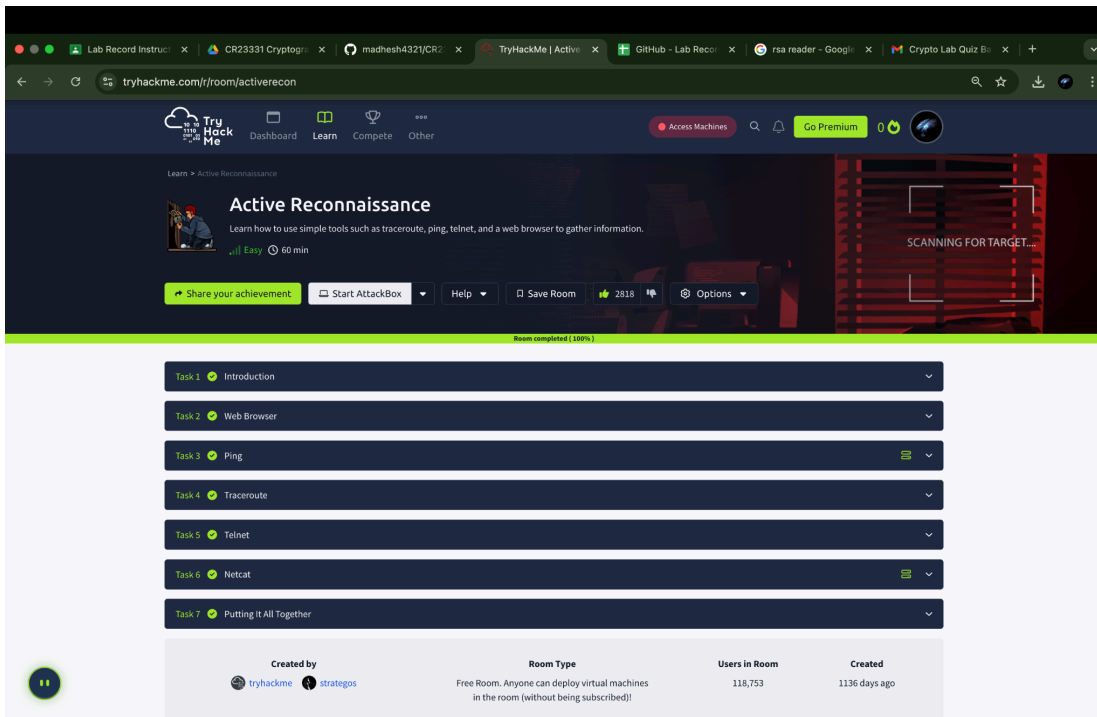
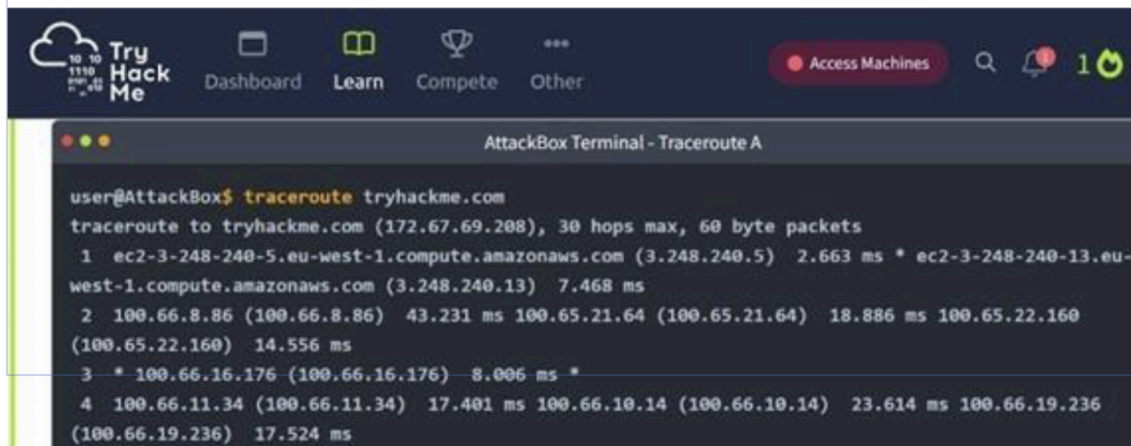
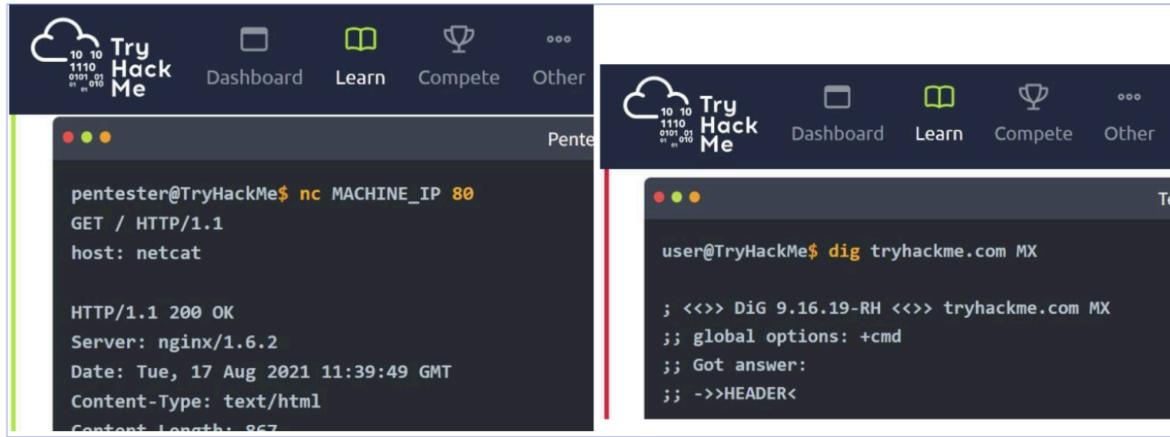
Output:

The screenshot shows the TryHackMe web interface for the 'Passive Reconnaissance' lab. The browser address bar displays 'tryhackme.com/t/room/passiverecon'. The page header includes navigation links like 'Dashboard', 'Learn', 'Compete', and 'Other', along with a 'Go Premium' button. The main content area features a 'Passive Reconnaissance' title, a brief description, and a 'Start AttackBox' button. Below this, a list of tasks is shown, all marked as completed (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

At the bottom, a table provides details about the room:

Created by	Room Type	Users in Room	Created
tryhackme strategos	Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)	159,791	1136 days ago



```

zsh: corrupt history file /home/kali/.zsh_history
kali@kali:~$ whois tryhackme.com
Domain Name: TRYHACKME.COM
Registry Domain ID: 2282723194 DOMAIN_COM-VKSW
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-05-03T19:43:12Z
Creation Date: 2018-07-05T19:46:15Z
Registry Expiry Date: 2027-07-05T19:46:15Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp/clientTransferProhibited
Name Server: KIP.NS.CLOUDFLARE.COM
Name Server: UMA.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-06-22T12:34:14Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide

```

Shodan Maps Images Monitor Developer More...

SHODAN Explore Pricing tryhackme

TOTAL RESULTS

1

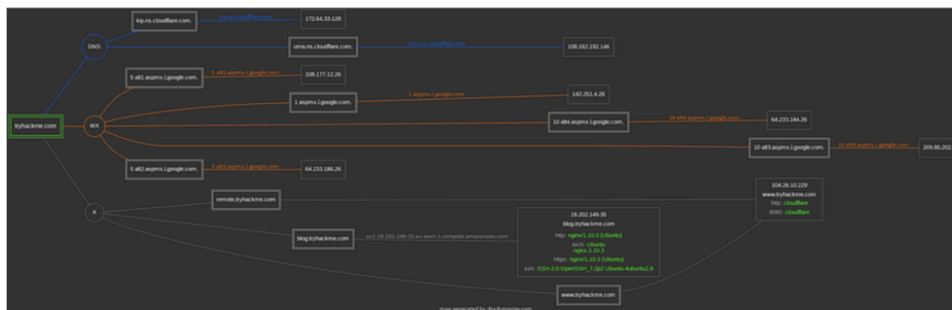
View Report View on Map

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

301 Moved Permanently

54.220.229.152
 eu2-04-220-229-152.eu-west-1.compute.amazonaws.com
 Amazon.com, Inc.
 Ireland, Dublin

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
 Connection: keep-alive
 Location: https://54.220.229.152/
 X-Frame-Options: ALLOW-FROM https://tryhackme.com



Result:

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