

Ex. No.: 3

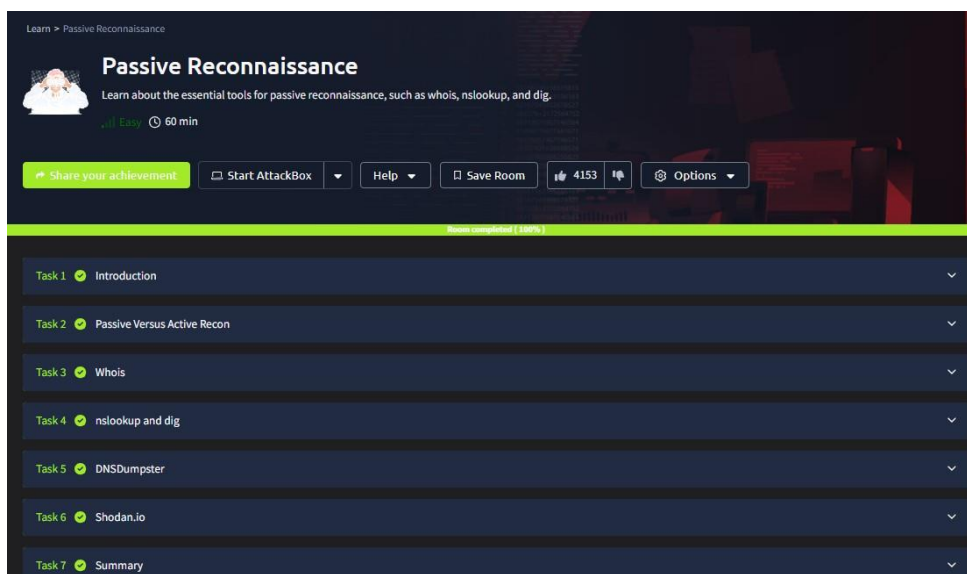
Date:20.08.2024

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:

CSE(Cyber Security) 2nd year

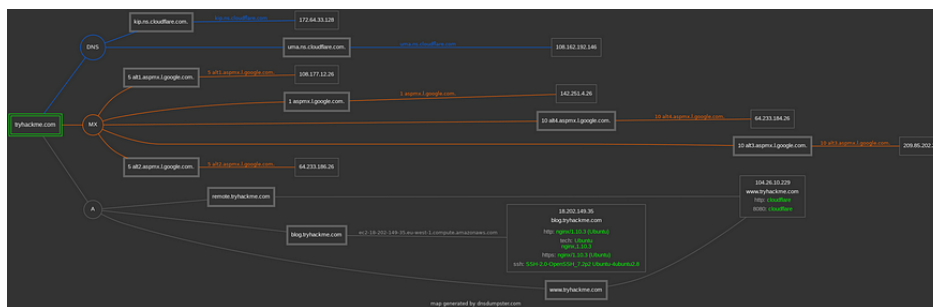
```
zsh: corrupt history file /home/kali/.zsh_history
❏ (kali@kali) ~
❏ whois tryhackme.com
Domain Name: TRYHACKME.COM
Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: https://www.namecheap.com
Updated Date: 2021-05-19T19:45:22Z
Creation Date: 2015-07-02T19:46:15Z
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: +1.681.929.8287
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
registrant'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 registrant'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, and by submitting a Whois query, you agree to abide
```

The screenshot shows the tryhackme website interface. At the top is a navigation bar with links: SHODAN, Maps, Images, Monitor, Developer, and More. Below this is a search bar containing the text 'tryhackme.com' and a magnifying glass icon. The main content area displays 'TOTAL RESULTS: 1'. A card for the first result is shown, titled 'New Service: Keep track of what you have connected to the Internet. Check out S...'. The result details include the title '301 Moved Permanently', the IP '54.220.229.192', and the server 'nginx/1.34.0 (Ubuntu)'. It also lists the date 'Fri, 20 Aug 2021 07:17:29 GMT', content type 'text/html', content length '394', connection 'keep-alive', location 'https://54.220.229.192/', and x-frame-options 'ALLOW-FROM https://tryhackme.com'. A 'cloud' icon is visible at the bottom left of the result card.





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](#)

👤 2814🔒

[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

▼

The image displays three screenshots of the TryHackMe platform interface, each showing a terminal window with different commands being executed.

Top Left Screenshot: The terminal window shows a netcat listener on MACHINE_IP 80. It receives an HTTP GET request from a host identified as netcat. The response is an HTTP 200 OK status from an nginx/1.6.2 server, dated Tue, 17 Aug 2021 11:39:49 GMT, with a content type of text/html and a content length of 957.

Top Right Screenshot: The terminal window shows a dig command being executed: `dig tryhackme.com MX`. The output indicates that the DNS record for tryhackme.com MX is 9.16.19-RH, and it shows the global options and the header of the response.

Bottom Screenshot: The terminal window shows a traceroute command being executed: `traceroute tryhackme.com`. The output shows the path from the user's machine to tryhackme.com (172.67.69.208), with 30 hops max and 60 byte packets. The path includes several hops through Amazon AWS infrastructure, with the final hop being 100.66.19.236.

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