

PASSIVE AND ACTIVE RECONNAISSANCE

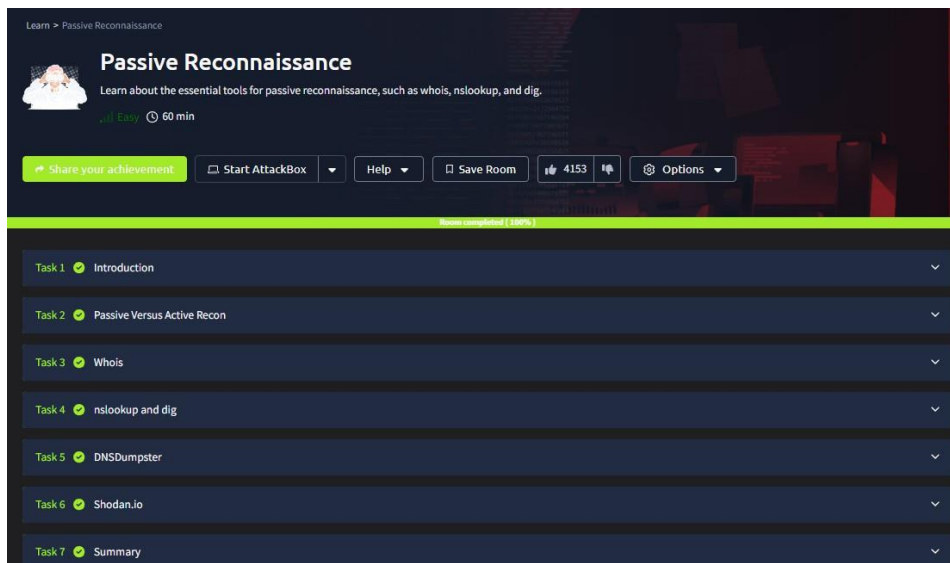
Aim:

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:



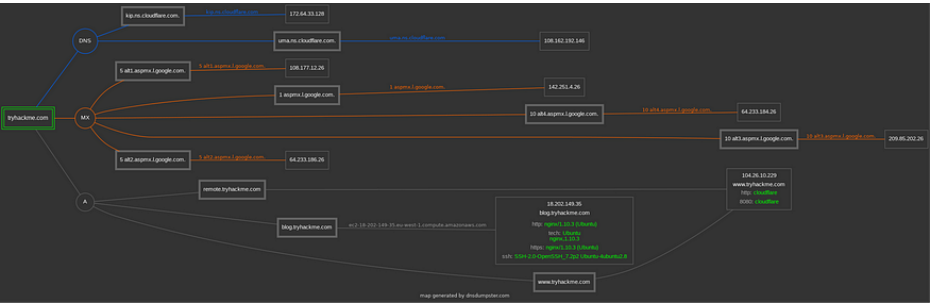
Name: VAISHAAL RAJHA T C G
231901502


```
hsh: 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: 2021-05-01T19:43:23Z
Creation Date: 2018-07-05T19:46:18Z
Registrar 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: +1.6633102107
Domain Status: clientTransferProhibited https://icann.org/epp/clientTransferProhibited
Name Server: KIP-NS.CLOUDFLARE.COM
Name Server: UMA-NS.CLOUDFLARE.COM
DNSSEC: unsigned
Last update 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
```






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

Name: VAISHAAL RAJHA T C G
231901502

The screenshot displays three terminal windows from the TryHackMe platform. The top-left window shows a netcat listener on MACHINE_IP 80, receiving an HTTP request from a host identified as netcat. The top-right window shows the output of the 'dig tryhackme.com MX' command, displaying DNS records for tryhackme.com. The bottom window, titled 'AttackBox Terminal - Traceroute A', shows the output of the 'traceroute tryhackme.com' command, detailing the network path and latency to tryhackme.com (172.67.69.208).

```
pentester@TryHackMe$ nc MACHINE_IP 80
GET / HTTP/1.1
host: netcat

HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 17 Aug 2021 11:39:49 GMT
Content-Type: text/html
Content-Length: 867

user@TryHackMe$ dig tryhackme.com MX
; <<> DiG 9.16.19-RH <<> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->HEADER<

user@AttackBox$ traceroute tryhackme.com
traceroute to tryhackme.com (172.67.69.208), 30 hops max, 60 byte packets
 1  ec2-3-248-240-5.eu-west-1.compute.amazonaws.com (3.248.240.5)  2.663 ms * ec2-3-248-240-13.eu-west-1.compute.amazonaws.com (3.248.240.13)  7.468 ms
 2  100.66.8.86 (100.66.8.86)  43.231 ms 100.65.21.64 (100.65.21.64)  18.886 ms 100.65.22.160 (100.65.22.160)  14.556 ms
 3  * 100.66.16.176 (100.66.16.176)  8.006 ms *
 4  100.66.11.34 (100.66.11.34)  17.401 ms 100.66.10.14 (100.66.10.14)  23.614 ms 100.66.19.236 (100.66.19.236)  17.524 ms
```

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