241901025   DHARANI K

Ex.No: 3   **Date:15/08/2025**

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.

241901025　　　　　　　　　　　　　　　　　DHARANI K

Passive Reconnaissance

Learn about the essential tools for passive reconnaissance, such as whois, nslookup, and dig.

📶 😈 🕐 60 min 👥 218,167

| Share your achievement | 🖥 Start AttackBox | ▼ | 🔖 Save Room | 👍 4911 Recommend | ⚙ 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	⌄

```
┌──(JackSparrow💀Captain)-[~]
└─$ whois tryhackme.com
  Domain Name: TRYHACKME.COM
  Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
  Registrar WHOIS Server: whois.namecheap.com
  Registrar URL: http://www.namecheap.com
  Updated Date: 2025-05-11T14:06:02Z
  Creation Date: 2018-07-05T19:46:15Z
  Registry Expiry Date: 2034-07-05T19:46:15Z
  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: 2025-11-15T16:47:08Z <<<
```

```
┌──(JackSparrow💀Captain)-[~]
└─$ nslookup -type=MX tryhackme.com
Server:         10.255.255.254
Address:        10.255.255.254#53

Non-authoritative answer:
tryhackme.com   mail exchanger = 1 aspmx.l.google.com.
tryhackme.com   mail exchanger = 10 alt3.aspmx.l.google.com.
tryhackme.com   mail exchanger = 10 alt4.aspmx.l.google.com.
tryhackme.com   mail exchanger = 5 alt1.aspmx.l.google.com.
tryhackme.com   mail exchanger = 5 alt2.aspmx.l.google.com.

Authoritative answers can be found from:
```

```
┌──(JackSparrow☠Captain)-[~]
└─$ dig tryhackme.com MX

; <<>> DiG 9.20.11-4+b1-Debian <<>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11986
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;tryhackme.com.                 IN      MX

;; ANSWER SECTION:
tryhackme.com.          191     IN      MX      1 aspmx.l.google.com.
tryhackme.com.          191     IN      MX      10 alt3.aspmx.l.google.com.
tryhackme.com.          191     IN      MX      10 alt4.aspmx.l.google.com.
tryhackme.com.          191     IN      MX      5 alt1.aspmx.l.google.com.
tryhackme.com.          191     IN      MX      5 alt2.aspmx.l.google.com.

;; Query time: 39 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Sat Nov 15 22:20:16 IST 2025
;; MSG SIZE  rcvd: 157
```

RESULT:

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