

Exercise-3
PASSIVE AND ACTIVE RECONNAISSANCE

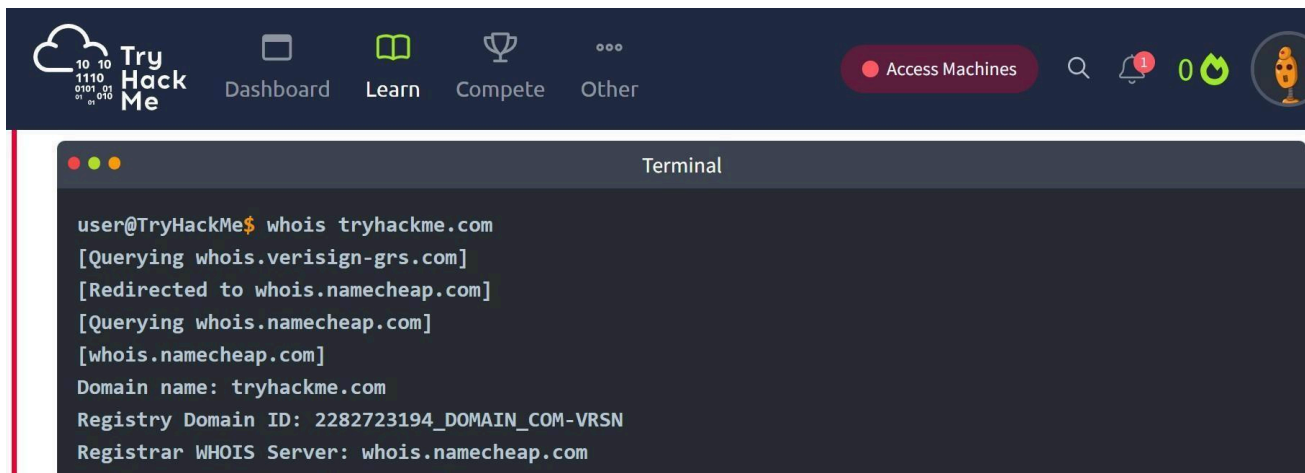
Aim:

To do perform passive and active reconnaissance in TryHackMe platform.

Algorithm:

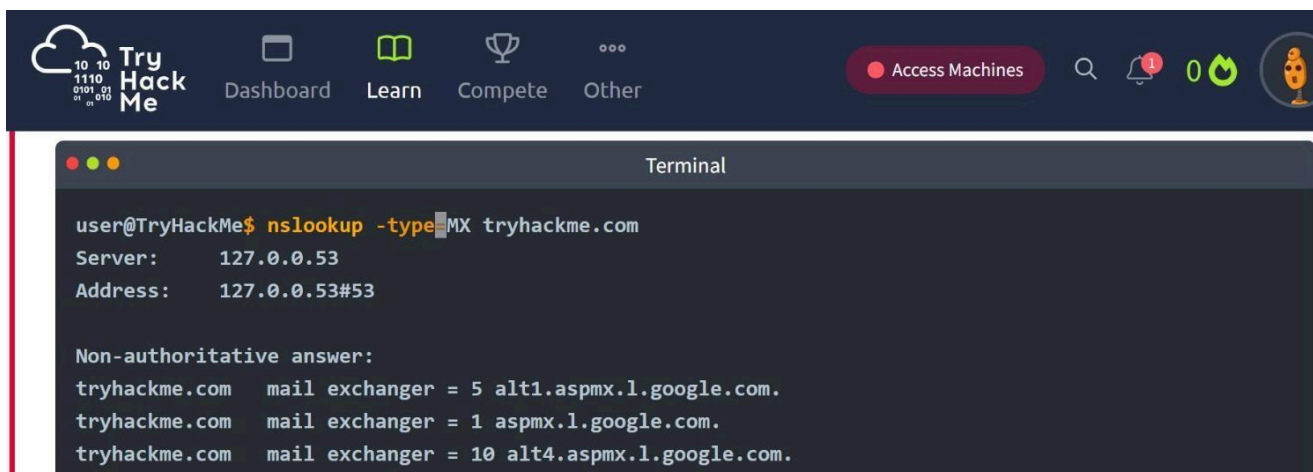
1. Access the Passive reconnaissance lab in TryHackMe platform using the link below- <https://tryhackme.com/r/room/passiverecon>
2. Click Start AttackBox to run the instance of Kali Linux distribution.
3. Run whois command on the website tryhackme.com and gather information about it.
4. Find the IP address 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 shows the TryHackMe dashboard with a terminal window open. The terminal displays the output of the `whois tryhackme.com` command. The output indicates that the domain is registered with Verisign, has been redirected to Namecheap, and provides details about the domain name, registry ID, and registrar.

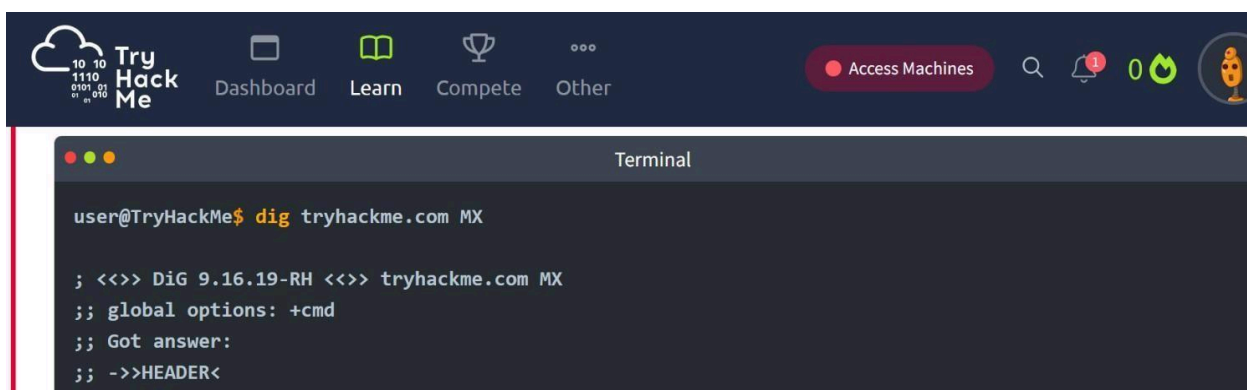
```
user@TryHackMe$ whois tryhackme.com
[Querying whois.verisign-grs.com]
[Redirected to whois.namecheap.com]
[Querying whois.namecheap.com]
[whois.namecheap.com]
Domain name: tryhackme.com
Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
```



The screenshot shows the TryHackMe dashboard with a terminal window open. The terminal displays the output of the `nslookup -type=MX tryhackme.com` command. The output shows the server address (127.0.0.53) and a non-authoritative answer listing three mail exchangers: alt1.aspmx.l.google.com, aspmx.l.google.com, and alt4.aspmx.l.google.com.

```
user@TryHackMe$ nslookup -type=MX tryhackme.com
Server:      127.0.0.53
Address:     127.0.0.53#53

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



The screenshot shows the TryHackMe dashboard with a terminal window open. The terminal displays the output of the `dig tryhackme.com MX` command. The output shows the command being executed, global options, and the start of the answer section.

```
user@TryHackMe$ dig tryhackme.com MX

; <<>> DiG 9.16.19-RH <<>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<
```

The screenshot shows the TryHackMe AttackBox interface. The top navigation bar includes the TryHackMe logo, a cloud icon, and links to Dashboard, Learn, Compete, and Other. A red button labeled 'Access Machines' is on the right. Below the navigation bar is a terminal window titled 'AttackBox Terminal - Traceroute A'. The terminal shows the command 'tracert tryhackme.com' being executed. The output displays the traceroute path from the user's machine to tryhackme.com (172.67.69.208), showing 30 hops max and 60 byte packets. The path includes several hops with IP addresses and round-trip times.

```
user@AttackBox$ tracert tryhackme.com
tracert 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
```

The screenshot shows the TryHackMe Pentester Terminal interface. The top navigation bar is identical to the previous screenshot. Below it is a terminal window titled 'Pentester Terminal'. The terminal shows a netcat listener on MACHINE_IP 80. It receives a connection from 10.10.10.10. The user enters 'GET / HTTP/1.1'. The terminal shows the response from the netcat server, including the host name 'netcat' and the HTTP status 'HTTP/1.1 200 OK'. The server information is displayed as 'Server: nginx/1.6.2', 'Date: Tue, 17 Aug 2021 11:39:49 GMT', 'Content-Type: text/html', and 'Content-Length: 867'.

```
pentester@TryHackMe$ nc MACHINE_IP 80
10.10.10.10
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
```

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