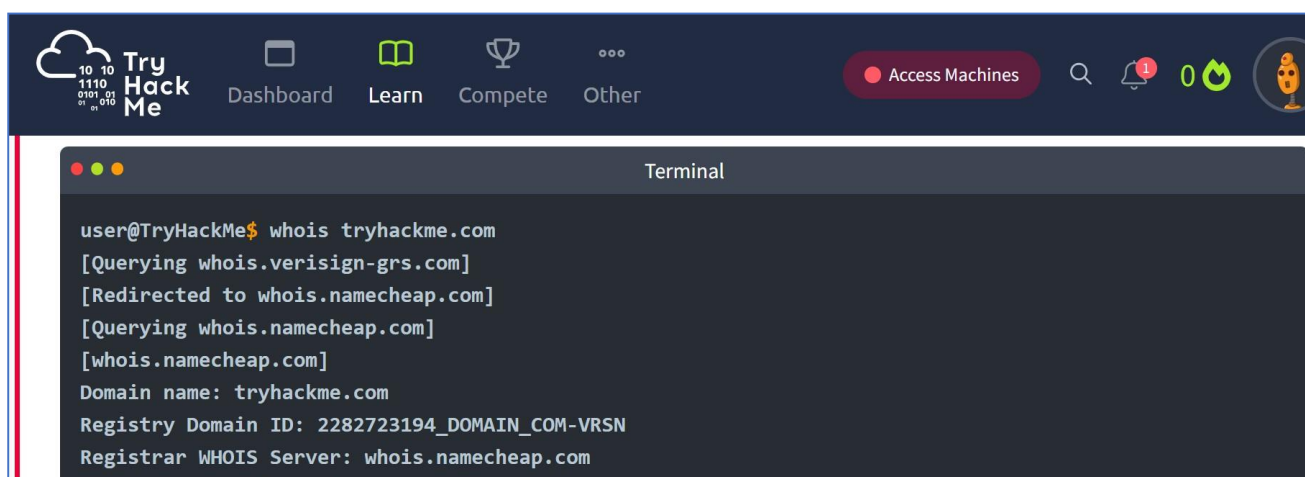


PASSIVE AND ACTIVE RECONNAISSANCE**Aim:**

To do perform passive and active reconnaissance in TryHackMe platform.

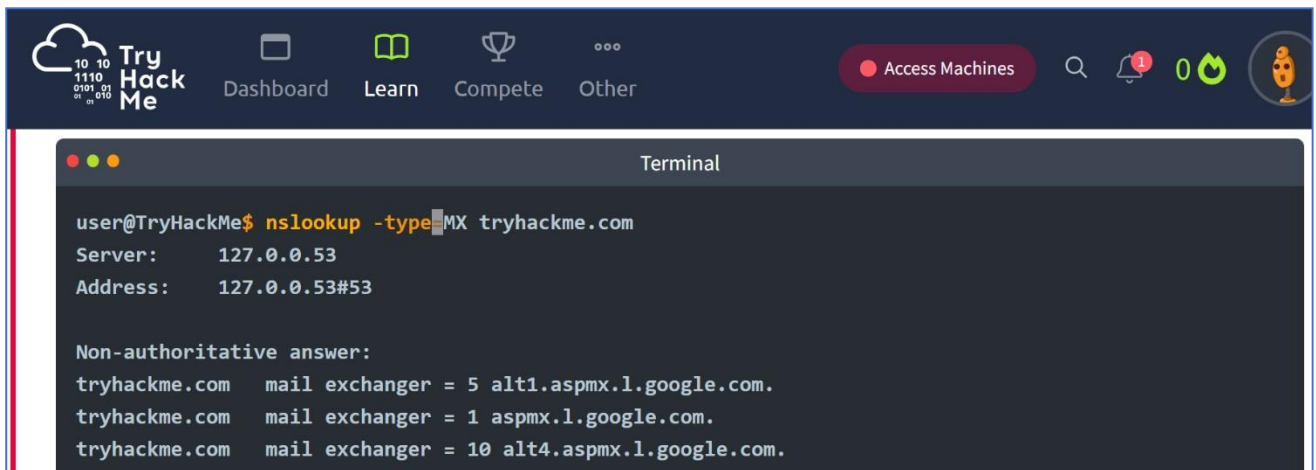
Algorithm:

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, showing domain information and redirection details.

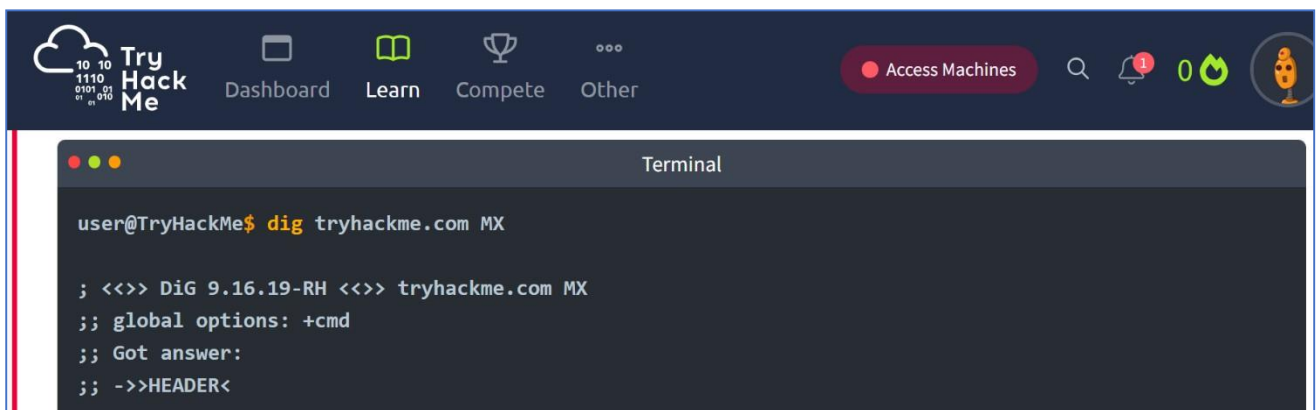
```
user@TryHackMe$ whois tryhackme.com
[Querying whois.verisign-grs.com]
[Redirected to whois.namecheap.com]
[Querying whois.namecheap.com]
[whois.namecheap.com]
Domain name: tryhackme.com
Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
```



The screenshot shows the TryHackMe dashboard at the top with navigation links: Dashboard, Learn, Compete, and Other. A red button labeled 'Access Machines' is on the right. Below the dashboard is a terminal window titled 'Terminal'. The terminal shows the command `nslookup -type=MX tryhackme.com` being executed. The output displays the server IP as 127.0.0.53 and the address as 127.0.0.53#53. It then lists non-authoritative answers for the MX records of tryhackme.com, showing three entries with their respective mail exchanger names and IP addresses.

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

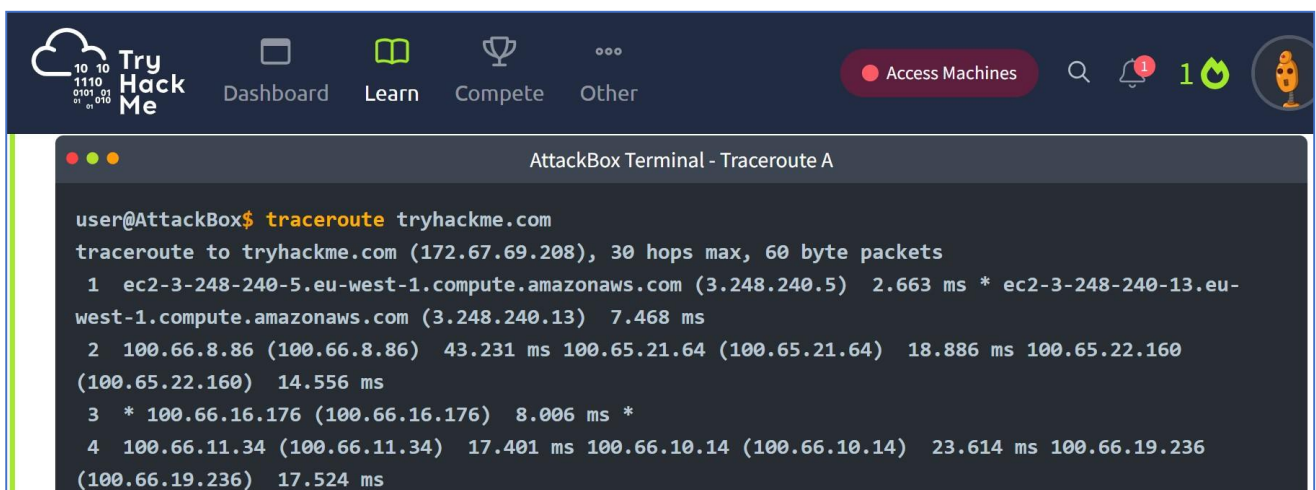
Non-authoritative answer:
tryhackme.com  mail exchanger = 5 alt1.aspmx.l.google.com.
tryhackme.com  mail exchanger = 1 aspmx.l.google.com.
tryhackme.com  mail exchanger = 10 alt4.aspmx.l.google.com.
```



This screenshot shows the TryHackMe dashboard with the same navigation links and 'Access Machines' button. The terminal window, titled 'Terminal', shows the command `dig tryhackme.com MX`. The output includes the DiG version (9.16.19-RH), global options (+cmd), and the start of the answer section, indicating that the header is being displayed.

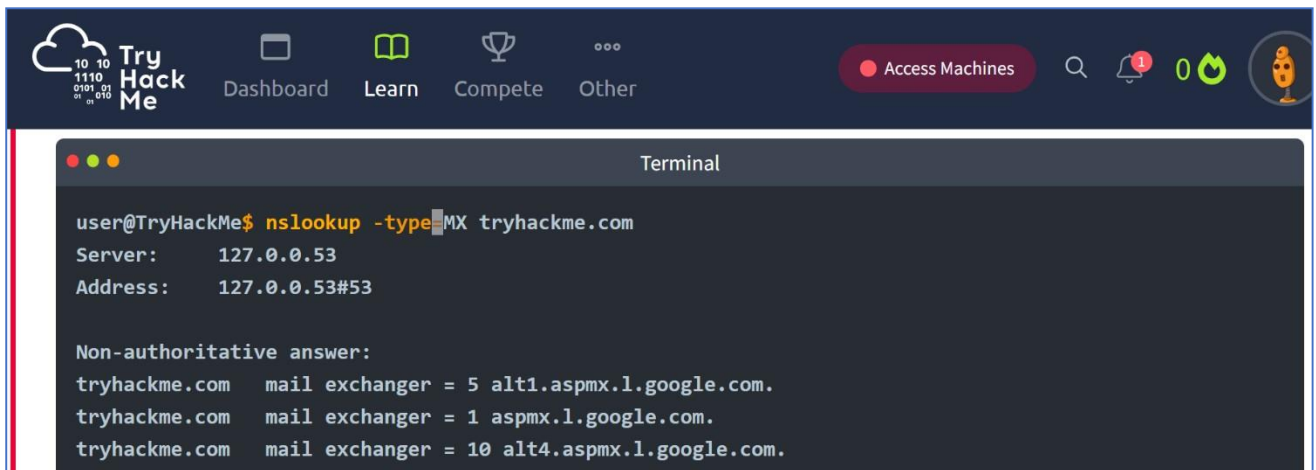
```
user@TryHackMe$ dig tryhackme.com MX

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



The screenshot displays the TryHackMe dashboard. The terminal window is titled 'AttackBox Terminal - Traceroute A'. It shows the command `traceroute tryhackme.com` being executed. The output provides a detailed traceroute from the user's location to tryhackme.com (172.67.69.208), showing 30 hops maximum and 60 byte packets. It lists the IP addresses of each hop along with the round-trip time in milliseconds.

```
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
```



The screenshot shows the TryHackMe dashboard with a terminal window open. The terminal displays the output of the command `nslookup -type=MX tryhackme.com`. The output shows the server IP as 127.0.0.53 and the address as 127.0.0.53#53. It also lists three mail exchangers for tryhackme.com: 5 alt1.aspmx.l.google.com., 1 aspmx.l.google.com., and 10 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.
```

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