**Ex. No.: 3** **Date:**

## PASSIVE AND ACTIVE RECONNAISSANCE

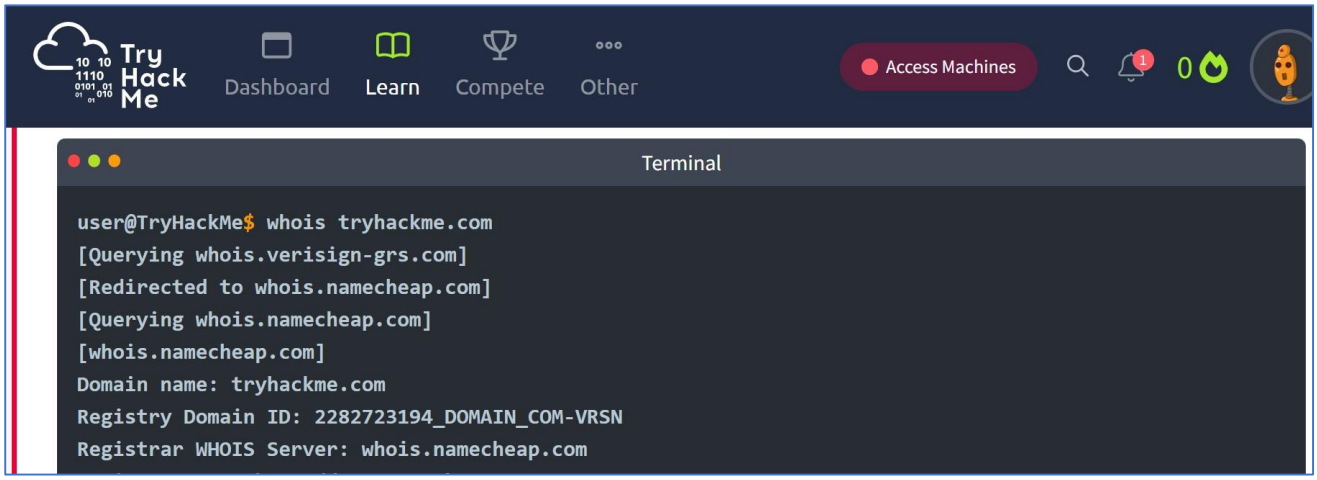
**Aim:**

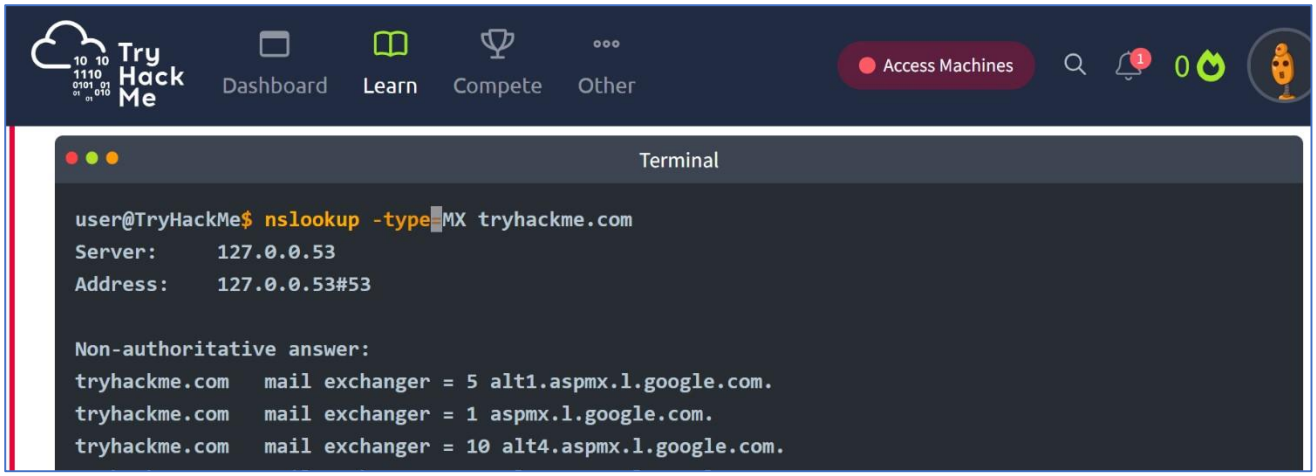
To do perform passive and active reconnaissance in TryHackMe platform.

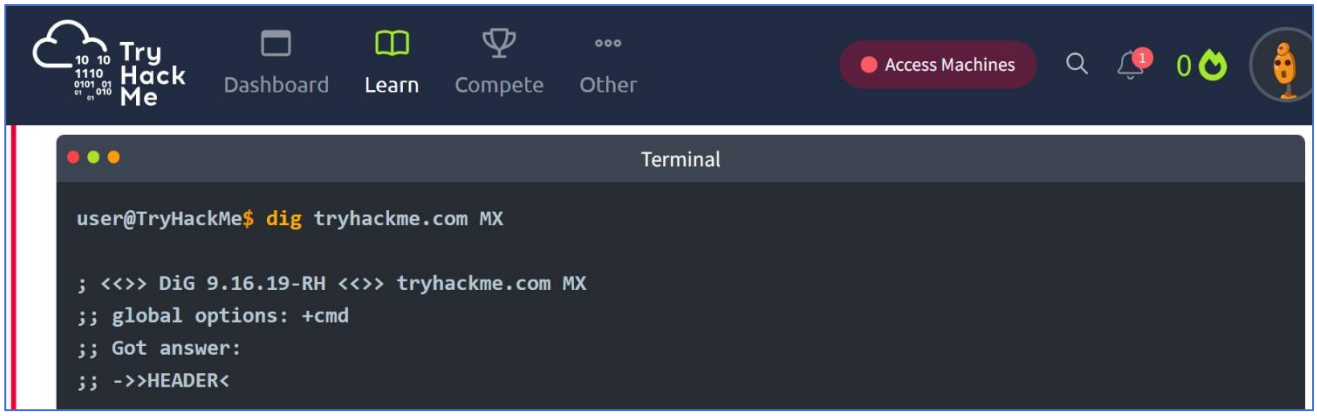
**Algorithm:**

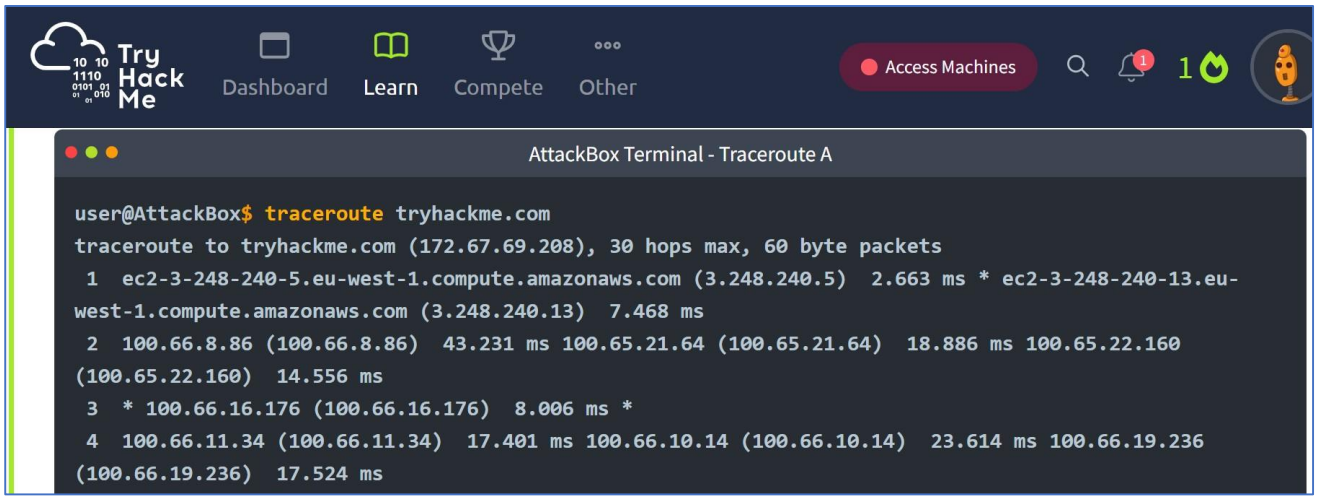
1. Access the Passive reconnaissance lab in TryHackMe platform using the link below- https://tryhackme.com/r/room/passiverecon
2. Click Start AttackBox to run the instance of Kali Linux distribution.
3. Run whois command on the website tryhackme.com and gather information about it.
4. Find the IP address 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.

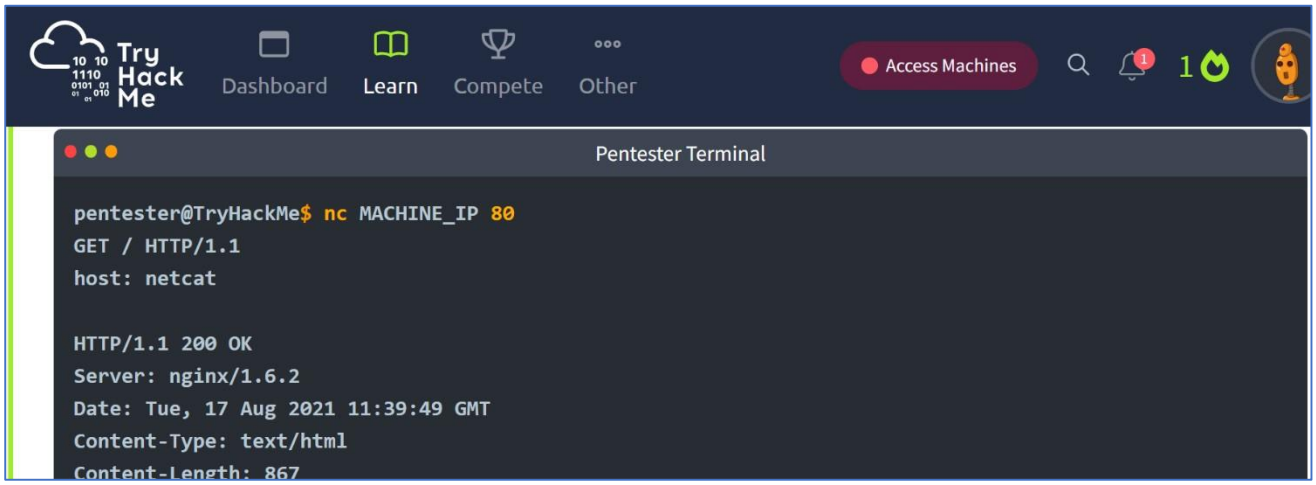
**Output:**


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Terminal
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


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Terminal
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.


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Terminal
user@TryHackMe$ dig tryhackme.com MX
; <<>> DiG 9.16.19-RH <<>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<




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