

NAME: THULASI.S
ROLL NO: 241901118

EXERCISE 3

PASSIVE AND ACTIVE RECONNAISSANCE

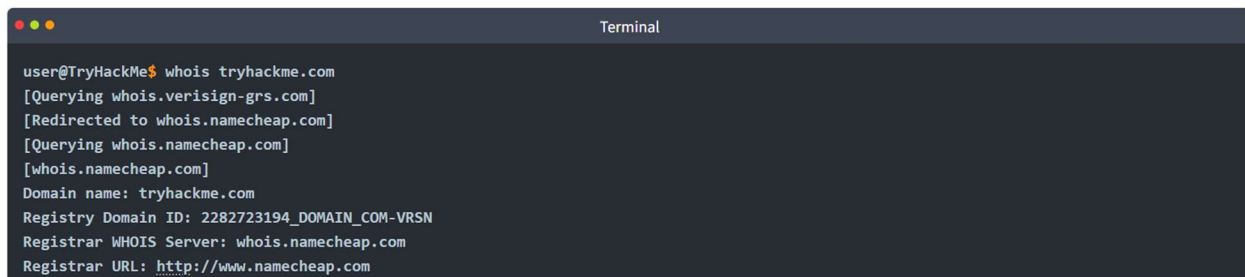
AIM:

To do perform passive and active reconnaissance in TryHackMe platform.

ALGORITHM:

1. Access the Passive reconnaissance lab in TryHackMe platform
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
8. Click Start AttackBox to run the instance of Kalilinux distribution.
9. Perform active reconnaissance using the commands, traceroute, ping and netcat.

OUTPUT:

A terminal window titled "Terminal" with a dark background and light text. It shows the execution of the 'whois' command for 'tryhackme.com'. The output indicates that the domain is registered with Namecheap, providing details like the Registry Domain ID, Registrar WHOIS Server, and Registrar URL.

```
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
Registrar URL: http://www.namecheap.com
```

```
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.
tryhackme.com mail exchanger = 10 alt3.aspmx.l.google.com.
tryhackme.com mail exchanger = 5 alt2.aspmx.l.google.com.
```

```
Terminal

user@TryHackMe$ dig tryhackme.com MX

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

```
AttackBox Terminal - Traceroute A

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) 2.556 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.