

Ex. No.: 3

PASSIVE AND ACTIVE RECONNAISSANCE

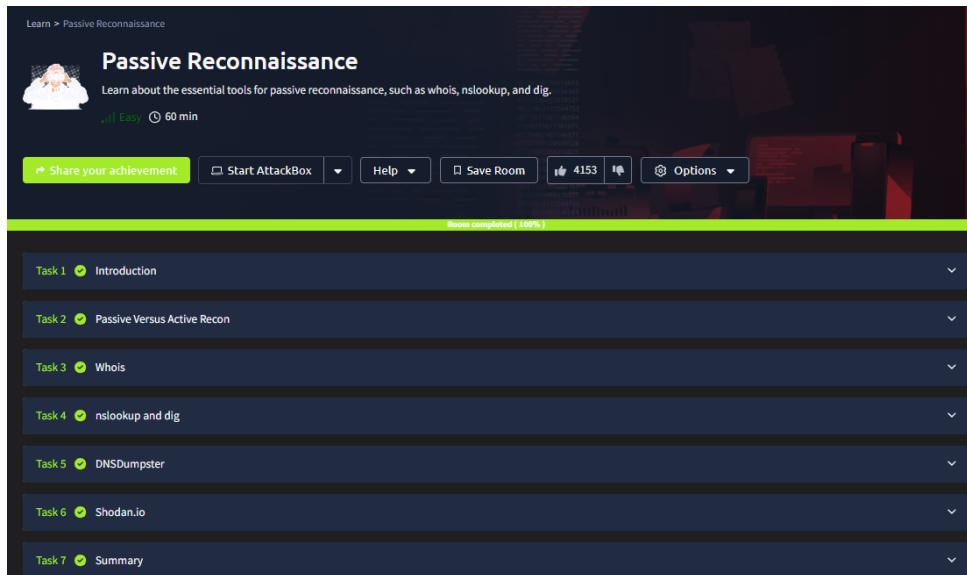
Aim:

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:



```

zsh: corrupt history file /home/kali/.zsh_history
[~] 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: 2014-05-01T09:43:23Z
Creation Date: 2012-07-05T19:46:15Z
Expiration Date: 2017-07-05T19:46:15Z
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: K1P.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: 2023-06-22T12:34:14Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide

```

SHODAN | Maps | Images | Monitor | Developer | More... |

SHODAN Explore Pricing tryhackme.com

TOTAL RESULTS 1

[View Report](#) [View on Map](#)

New Service: Keep track of what you have connected to the Internet. Check out [Shodan New Service](#)

301 Moved Permanently

54.220.228.192

HTTP/1.1 301 Moved Permanently

Server: nginx/1.14.8 (Ubuntu)

Host: ec2-54-220-228-192.eu-west-1.compute.amazonaws.com

Date: Fri, 20 Aug 2021 07:17:29 GMT

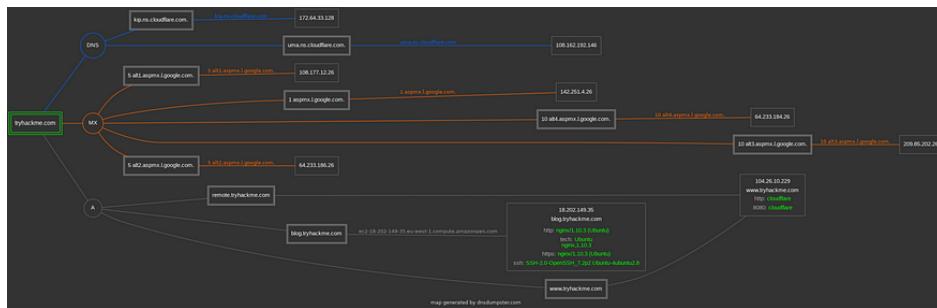
Content-Type: text/html

Content-Length: 194

Connection: keep-alive

Location: https://54.220.228.192/

X-Frame-Options: ALLOW-FROM https://tryhackme.com



Active Reconnaissance

Learn how to use simple tools such as traceroute, ping, telnet, and a web browser to gather information.

Full Easy 60 min

Share your achievement Start AttackBox Help Save Room Options 2814

Rooms completed (100%)

Task 1 ✓ Introduction

Task 2 ✓ Web Browser

Task 3 ✓ Ping

Task 4 ✓ Traceroute

Task 5 ✓ Telnet

Task 6 ✓ Netcat

Task 7 ✓ Putting It All Together

The image shows three screenshots of the TryHackMe platform interface. The top two screenshots show terminal sessions on the 'Pente' machine. The left terminal session shows a netcat listener on port 80, receiving a connection from 'pentester@TryHackMe'. The response includes headers for HTTP/1.1, Server (nginx/1.6.2), Date (Tue, 17 Aug 2021 11:39:49 GMT), Content-Type (text/html), and Content-Length (967). The right terminal session shows a user performing a DNS query with 'dig' for 'tryhackme.com' MX records, receiving a response with global options and an answer section. The bottom screenshot shows the 'AttackBox' terminal with a traceroute command to 'tryhackme.com', displaying the path through various IP addresses and their latencies.

```

pentester@TryHackMe$ nc MACHINE_IP 80
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: 967

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)  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

```

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