

Lab Report No.1

Footprinting and Reconnaissance

Ethical Hacking

Submitted By: Raghad Alharthi 2210003220

Section: CS Group no. 2

Contents

Room: Red Team Recon.....	3
Task 3:	3
Q1:.....	3
Q2 & Q3:.....	3
Task 4:	3
Q1:.....	3
Q2:.....	4
Task 5:	4
Q1:.....	4
Task 6:	5
Q1:.....	5
Q2:.....	5
Q3:.....	5
Q4:.....	6
Task 7:	6
Q1:.....	6
Q2:.....	7
Room: Passive Reconnaissance.....	8
Task 2:	8
All Questions:	8
Task 3:	8
Q1:.....	8
Q2:.....	9
Q3:.....	9
Task 4:	9
Q1:.....	9
Task 5:	10
Q1:.....	10

Task 6:	10
Q1:.....	10
Q2:.....	11
Q3:.....	11
Room: Active Reconnaissance	12
Task 2:	12
Q1:.....	12
Task 3:	12
Q1:.....	12
Q2:.....	13
Q3:.....	13
Q4:.....	13
Task 4:	14
Q1:.....	14
Q2:.....	14
Q3:.....	15
Q4:.....	15
Task 5:	15
Q1:.....	15
Q2:.....	15
Task 6:	16
Q1:.....	16

Room: Red Team Recon

Task 3:

Q1:

Room progress (6%)

WHOIS databases and DNS servers hold publicly available information, and querying either does not generate any suspicious traffic.

Moreover, we can rely on Traceroute (`tracert` on Linux and macOS systems and `tracert` on MS Windows systems) to discover the hops between our system and the target host.

Answer the questions below

When was `thmredteam.com` created (registered)? (YYYY-MM-DD)

2021-09-24 ✓ Correct Answer 🔍 Hint

To how many IPv4 addresses does `clinic.thmredteam.com` resolve?

```
root@ip-10-10-255-5:~  
File Edit View Search Terminal Help  
root@ip-10-10-255-5:~# whois thmredteam.com  
Domain Name: THMREDTEAM.COM  
Registry Domain ID: 2643258257_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.namecheap.com  
Registrar URL: http://www.namecheap.com  
Updated Date: 2024-09-17T15:52:57Z  
Creation Date: 2021-09-24T14:04:16Z  
Registry Expiry Date: 2025-09-24T14:04:16Z  
Registrar: NameCheap, Inc.  
Registrar IANA ID: 1068  
Registrar Abuse Contact Email: abuse@namecheap.com  
Registrar Abuse Contact Phone: +1.6613102107  
Domain Status: clientTransferProhibited https://icann.org/epp#cli  
ntTransferProhibited  
Name Server: KIP.NS.CLOUDFLARE.COM  
Name Server: UMA.NS.CLOUDFLARE.COM
```

Q2 & Q3:

To how many IPv4 addresses does `clinic.thmredteam.com` resolve?

2 ✓ Correct Answer

To how many IPv6 addresses does `clinic.thmredteam.com` resolve?

2 ✓ Correct Answer

```
root@ip-10-10-255-5:~# ^C  
root@ip-10-10-255-5:~# nslookup clinic.thmredteam.com  
Server: 127.0.0.53  
Address: 127.0.0.53#53  
  
Non-authoritative answer:  
Name: clinic.thmredteam.com  
Address: 104.21.93.169  
Name: clinic.thmredteam.com  
Address: 172.67.212.249  
Name: clinic.thmredteam.com  
Address: 2606:4700:3034::6815:5da9  
Name: clinic.thmredteam.com  
Address: 2606:4700:3034::ac43:d4f9
```

Task 4:

Q1:

OSINT filetype:pdf	Find files of type <code>PDF</code> related to a certain term.
salary site:blog.tryhackme.com	Limit search results to a specific site.

combining these two queries.

Answer: filetype:xls site: clinic.thmredteam.com

How would you search using Google for `xls` indexed for `http://clinic.thmredteam.com`?

filetype:xls site:clinic.thmredteam.com ✓ Correct Answer 🔍 Hint

How would you search using Google for files with the word `passwords` for `http://clinic.thmredteam.com`?

Submit

filetype:xls site:clinic.thmredteam.com

Your search - `filetype:xls site:clinic.thmredteam.com` - did not match any documents.

Suggestions:

- Make sure that all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

Q2:

filetype:xls site:clinic.thmredteam.com

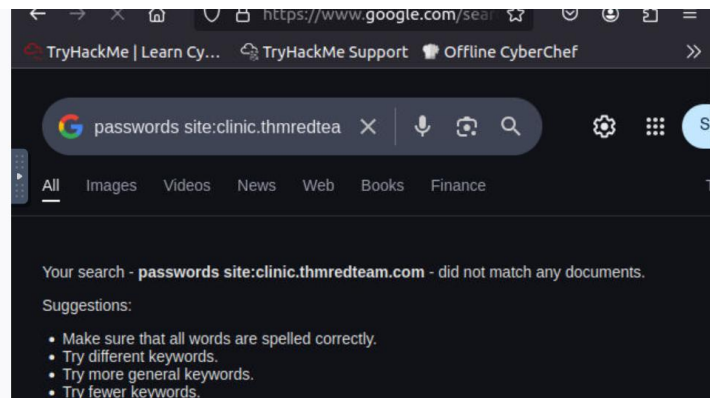
✓ Correct Answer ? Hint

How would you search using Google for files with the word **passwords** for http://clinic.thmredteam.com?

passwords site:clinic.thmredteam.com

✓ Correct Answer

Task 5 ☒ Specialized Search Engines



Task 5:

Q1:

Installing shodan:

```
root@ip-10-10-255-5:~# apt install python3-shodan
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed a
```

API key

443/tcp
|-- SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2
2086/tcp
2087/tcp
8080/tcp

Answer the questions below

What is the **shodan** command to get your Internet-facing IP address?

shodan myip ✓ Correct Answer ? Hint

Task 6 ☐ Recon-ng

https://cli.shodan.io

SHODAN

-- Diffie-Hellman Parameters:
Bits: 1024
Generator: 2
Fingerprint: RFC2409/Oakley Group 2

myip

Returns your Internet-facing IP address.

Example

```
$ shodan myip
199.30.49.210
```

```
root@ip-10-10-144-98:~# shodan init ZoHcxnNWmN7Fzxfi6ktBS0w5tzwOHj1Z
Successfully initialized
root@ip-10-10-144-98:~# shodan myip
3.255.131.165
```

Task 6:

Q1:

Answer the questions below

How do you start recon-ng with the workspace clinicredteam?

recon-ng -w clinicredteam

✓ Correct Answer

 Hint

How many modules with the name `virustotal` exist?

—

```
root@ip-10-10-255-5:~# recon-ng -w clinciredteam
```

```
[*] Your version of Recon-ng does not match the latest release.
[*] Please consider updating before further use.
Remote version: 5.1.2
Local version: 0
```

Q2:

How many modules with the name `virustotal` exist?

2

✓ Correct Answer

```
[recon-ng][climacris] > marketplace search virustotal
Searching module index for 'virustotal'...
```

Path	Version	Status	Updated	D	K
recon/hosts-hosts/virustotal	1.0	not installed	2019-06-24		*
recon/netblocks-hosts/virustotal	1.0	not installed	2019-06-24		*

Q3:

There is a single module under `hosts-domains`. What is its name?

migrate_hosts

✓ Correct Answer

```
recon-ng[clinicredteam] > marketplace search hosts-domains
Searching module index for 'hosts-domains'...
```

Path	Version	Status	Updated	D	K
recon/hosts-domains/migrate_hosts	1.1	not installed	2020-05-17		

Q4:

`censys_email_address` is a module that “retrieves email addresses from the TLS certificates for a company.” Who is the author?

Censys Inc

✓ Correct Answer

```
[recon-ng][clinicredteam] > marketplace info censys_email_address
+-----+
| path          | recon/companies-contacts/censys_email_address |
| name          | Censys - Emails by Company                    |
| author        | Censys, Inc. <support@censys.io>              |
| version       | 2.1                                            |
| last_updated  | 2022-01-31                                    |
| description   | Retrieves email addresses from the TLS certificates.leaf_data.subject.email_address' field and updates the 'contacts' table with the results. |
| required_keys | ['censysio_id', 'censysio_secret']            |
| dependencies  | ['censys>=2.1.2']                            |
| files         | []                                             |
| status        | not installed                                |
+-----+
```

Task 7:

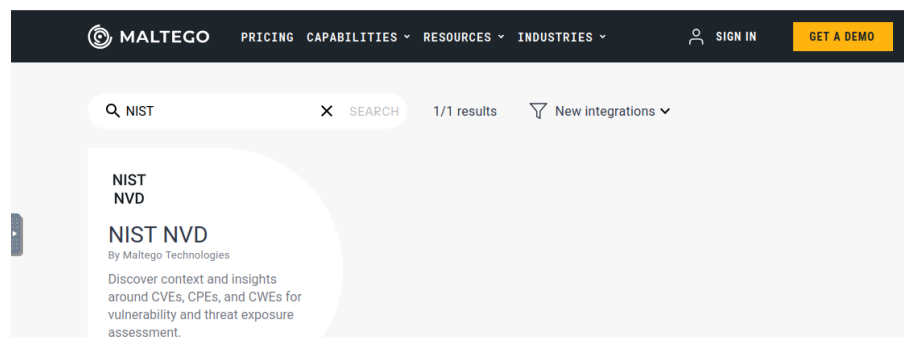
Q1:

What is the name of the transform that queries NIST’s National Vulnerability Database?

NIST NVD

✓ Correct Answer

💡 Hint



Q2:

What is the name of the project that offers a transform based on ATT&CK?

MISP Project

✓ Correct Answer

💡 Hint

★ > Transform Hub > Data Categories - Malware

ATT&CK - MISP

By MISP Project

Query MISP threat sharing instances and other MISP events, attributes, objects, tags, and galaxies.

Malware

TTPs

Incident Response

Threat Hunting



Room: Passive Reconnaissance

Task 2:

All Questions:

You visit the Facebook page of the target company, hoping to get some of their employee names. What kind of reconnaissance activity is this? (A for active, P for passive)

P

✓ Correct Answer

You ping the IP address of the company webserver to check if ICMP traffic is blocked. What kind of reconnaissance activity is this? (A for active, P for passive)

A

✓ Correct Answer

You happen to meet the IT administrator of the target company at a party. You try to use social engineering to get more information about their systems and network infrastructure. What kind of reconnaissance activity is this? (A for active, P for passive)

A

✓ Correct Answer

Task 3:

Q1:

When was TryHackMe.com registered?

20180705

✓ Correct Answer

🔍 Hint

```
root@ip-10-10-144-98:~# 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: 2021-05-01T19:43:23Z
Creation Date: 2018-07-05T19:46:15Z
Registry Expiry Date: 2027-07-05T19:46:15Z
Registrar: NameCheap, Inc.
```

Q2:

What is the registrar of TryHackMe.com?

✓ Correct Answer

🔍 Hint

```
root@ip-10-10-144-98:~# 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: 2021-05-01T19:43:23Z
```

Q3:

Which company is TryHackMe.com using for name servers?

✓ Correct Answer

🔍 Hint

```
Name Server: KIP.NS.CLOUDFLARE.COM
Name Server: UMA.NS.CLOUDFLARE.COM
```

Task 4:

Q1:

Check the TXT records of thmlabs.com. What is the flag there?

✓ Correct Answer

```
root@ip-10-10-144-98:~# nslookup -type=TXT thmlabs.com 1.1.1.1
Server:          1.1.1.1
Address:         1.1.1.1#53

Non-authoritative answer:
thmlabs.com      text = "THM{a5b83929888ed36acb0272971e438d78}"
```

Task 5:

Q1:

Lookup tryhackme.com on DNSDumpster. What is one interesting subdomain that you would discover in addition to www and blog?

remote

✓ Correct Answer

A Records (subdomains from dataset)				
Host	IP	ASN	ASN Name	Open Services
blog.tryhackme.com	104.22.55.228	ASN:13335 104.22.48.0/20	CLOUDFLARENET	http: cloudflare title: Direct IP tech: Cloudflare http8080: cloudfl title: Direct IP tech: Cloudflare
insights-proxy- worker.tryhackme.com	104.22.55.228	ASN:13335 104.22.48.0/20	CLOUDFLARENET	http: cloudflare title: Direct IP tech: Cloudflare http8080: cloudfl title: Direct IP tech: Cloudflare
remote.tryhackme.com	104.22.55.228	ASN:13335 104.22.48.0/20	CLOUDFLARENET	http: cloudflare title: Direct IP tech: Cloudflare http8080: cloudfl title: Direct IP

Task 6:

Q1:

According to Shodan.io, what is the 2nd country in the world in terms of the number of publicly accessible Apache servers?

Germany

✓ Correct Answer

💡 Hint

SHODAN

Explore

Downloads

Pricing

public accessible Apache servers

TOTAL RESULTS

191

View Report

View on Map

Advanced Search

Product Spotlight: We've Launched a new API for Fast Vuln

187.84.58.246

187-84-58-246.bom

mtempo.inf.br

BRASIL TECPAR |

AMIGO | AVATO

Brazil, Tupandi

HTTP/1.1 200 OK

Date: Tue, 04 Feb 2025 06:11:53 GMT

Server: Apache

X-Frame-Options: SAMEORIGIN

Last-Modified: Mon, 16 Mar 2020 14:42:27 GMT

Etag: "b03-5a0f9d3fd4a98"

Accept-Ranges: bytes

Content-Length: 2819

Vary: Accept-Encoding

Content-Type: text/html

TOP COUNTRIES

Brazil	189
Germany	1

Q2:

Based on Shodan.io, what is the 3rd most common port used for Apache?

✓ Correct Answer

🔍 Hint

TOP PORTS	
80	6,960,888
443	5,918,214
8080	348,713
5006	160,751
8081	155,012

Q3:

Based on Shodan.io, what is the 3rd most common port used for nginx?

✓ Correct Answer

🔍 Hint

TOP PORTS	
80	11,228,910
443	9,012,198
5001	702,466
5000	641,700
8888	473,313

Room: Active Reconnaissance

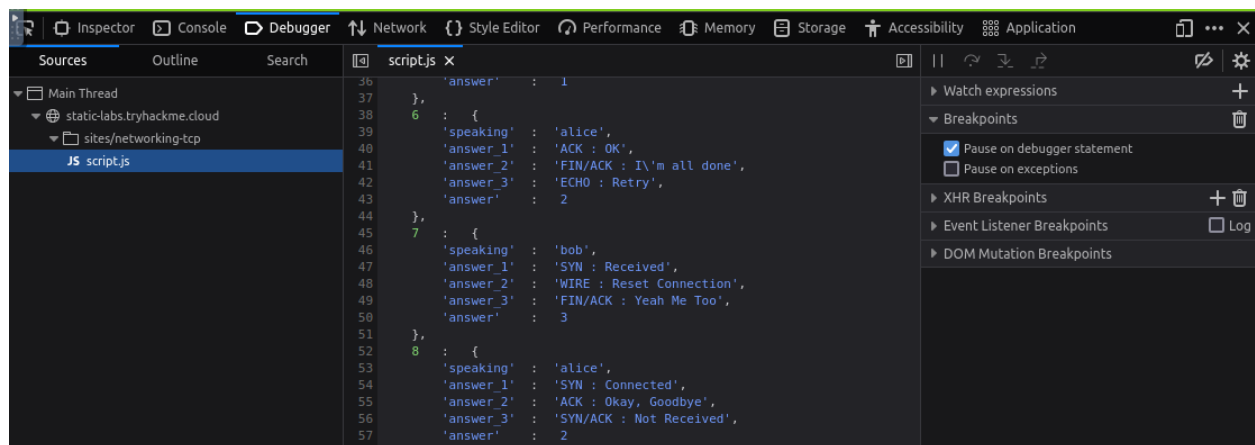
Task 2:

Q1:

Browse to the [following website](#) and ensure that you have opened your Developer Tools on AttackBox Firefox, or the browser on your computer. Using the Developer Tools, figure out the total number of questions.

✓ Correct Answer

💡 Hint



Task 3:

Q1:

Which option would you use to set the size of the data carried by the ICMP echo request?

✓ Correct Answer

💡 Hint

Using command: man ping

```
-s packetsize  
Specifies the number of data bytes to be sent. The default is 56,  
which translates into 64 ICMP data bytes when combined with the 8  
bytes of ICMP header data.
```

Q2:

What is the size of the ICMP header in bytes?

8

✓ Correct Answer

🔍 Hint

Also using man ping:

ICMP PACKET DETAILS

An IP header without options is 20 bytes. An ICMP ECHO_REQUEST packet contains an additional 8 bytes worth of ICMP header followed by an arbitrary amount of data. When a `packetsize` is given, this indicated the size of this extra piece of data (the default is 56). Thus the amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space (the ICMP header).

Q3:

Does MS Windows Firewall block ping by default? (Y/N)

Y

✓ Correct Answer

- A firewall is configured to block such packets. The firewall might be a piece of software running on the system itself or a separate network appliance. Note that MS Windows firewall blocks ping by default.

Q4:

Deploy the VM for this task and using the AttackBox terminal, issue the command `ping -c 10`

`MACHINE_IP`. How many ping replies did you get back?

10

✓ Correct Answer

```
root@ip-10-10-103-187:~# ping -c 10 10.10.103.187
PING 10.10.103.187 (10.10.103.187) 56(84) bytes of data.
64 bytes from 10.10.103.187: icmp_seq=1 ttl=64 time=0.058 ms
64 bytes from 10.10.103.187: icmp_seq=2 ttl=64 time=0.048 ms
64 bytes from 10.10.103.187: icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 10.10.103.187: icmp_seq=4 ttl=64 time=0.035 ms
64 bytes from 10.10.103.187: icmp_seq=5 ttl=64 time=0.043 ms
64 bytes from 10.10.103.187: icmp_seq=6 ttl=64 time=0.052 ms
64 bytes from 10.10.103.187: icmp_seq=7 ttl=64 time=0.051 ms
64 bytes from 10.10.103.187: icmp_seq=8 ttl=64 time=0.060 ms
64 bytes from 10.10.103.187: icmp_seq=9 ttl=64 time=0.033 ms
64 bytes from 10.10.103.187: icmp_seq=10 ttl=64 time=0.057 ms

--- 10.10.103.187 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9201ms
rtt min/avg/max/mdev = 0.033/0.048/0.060/0.008 ms
```

Task 4:

Q1:

In Traceroute A, what is the IP address of the last router/hop before reaching tryhackme.com?

172.67.69.208

✓ Correct Answer

💡 Hint

```
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 *
 2 100.66.8.86 (100.66.8.86) 43.231 ms 100.65.21.64 (100.65.21.64) 18.886 m
 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
 5 100.66.7.35 (100.66.7.35) 12.808 ms 100.66.6.109 (100.66.6.109) 14.791 m
 6 100.65.14.131 (100.65.14.131) 1.026 ms 100.66.5.189 (100.66.5.189) 19.24
 7 100.65.13.143 (100.65.13.143) 14.254 ms 100.95.18.131 (100.95.18.131) 0.
 8 100.95.2.143 (100.95.2.143) 0.680 ms 100.100.4.46 (100.100.4.46) 1.392 m
 9 100.100.20.76 (100.100.20.76) 7.819 ms 100.92.11.36 (100.92.11.36) 18.66
10 100.92.11.112 (100.92.11.112) 17.852 ms * 100.92.11.158 (100.92.11.158)
11 100.92.211.82 (100.92.211.82) 19.713 ms 100.92.0.126 (100.92.0.126) 18.6
12 99.83.69.207 (99.83.69.207) 17.603 ms 15.827 ms 17.351 ms
13 100.92.9.83 (100.92.9.83) 17.894 ms 100.92.79.136 (100.92.79.136) 21.250
14 172.67.69.208 (172.67.69.208) 17.976 ms 16.945 ms 100.92.9.3 (100.92.9.3
```

Q2:

In Traceroute B, what is the IP address of the last router/hop before reaching tryhackme.com?

104.26.11.229

✓ Correct Answer

💡 Hint

```
AttackBox Terminal - Traceroute B

user@AttackBox$ traceroute tryhackme.com
traceroute to tryhackme.com (104.26.11.229), 30 hops max, 60 byte packets
 1 ec2-79-125-1-9.eu-west-1.compute.amazonaws.com (79.125.1.9) 1.475 ms * ec
 2 100.65.20.160 (100.65.20.160) 16.575 ms 100.66.8.226 (100.66.8.226) 23.2
 3 100.66.16.50 (100.66.16.50) 2.777 ms 100.66.11.34 (100.66.11.34) 22.288
 4 100.66.6.47 (100.66.6.47) 17.264 ms 100.66.7.161 (100.66.7.161) 39.562 m
 5 100.66.5.123 (100.66.5.123) 20.099 ms 100.66.7.239 (100.66.7.239) 19.253
 6 * 100.66.5.223 (100.66.5.223) 16.172 ms 100.65.15.135 (100.65.15.135) 0.
 7 100.65.12.135 (100.65.12.135) 0.390 ms 100.65.12.15 (100.65.12.15) 1.045
 8 100.100.4.16 (100.100.4.16) 0.482 ms 100.100.20.122 (100.100.20.122) 0.7
 9 100.100.20.86 (100.100.20.86) 0.442 ms 100.100.4.78 (100.100.4.78) 0.347
10 100.92.212.20 (100.92.212.20) 11.611 ms 100.92.11.54 (100.92.11.54) 12.6
11 100.92.6.52 (100.92.6.52) 11.427 ms 100.92.6.50 (100.92.6.50) 11.033 ms
12 100.92.210.139 (100.92.210.139) 10.026 ms 100.92.6.13 (100.92.6.13) 14.5
13 100.92.79.12 (100.92.79.12) 12.011 ms 100.92.79.68 (100.92.79.68) 11.318
14 100.92.9.27 (100.92.9.27) 11.354 ms 100.92.80.31 (100.92.80.31) 13.000 m
15 150.222.241.85 (150.222.241.85) 9.660 ms 52.93.135.81 (52.93.135.81) 10.
16 100.92.228.102 (100.92.228.102) 15.168 ms 100.92.227.41 (100.92.227.41)
17 100.92.232.111 (100.92.232.111) 10.589 ms 100.92.231.69 (100.92.231.69)
18 100.91.205.140 (100.91.205.140) 11.551 ms 100.91.201.62 (100.91.201.62)
19 100.91.205.79 (100.91.205.79) 11.112 ms 100.91.205.83 (100.91.205.83) 11
20 100.91.211.45 (100.91.211.45) 9.486 ms 100.91.211.79 (100.91.211.79) 13.
21 100.100.6.81 (100.100.6.81) 11.522 ms 100.100.68.70 (100.100.68.70) 10.1
22 100.100.65.131 (100.100.65.131) 10.371 ms 100.100.92.6 (100.100.92.6) 10
23 100.100.2.74 (100.100.2.74) 15.317 ms 100.100.66.17 (100.100.66.17) 11.4
24 100.100.16.16 (100.100.16.16) 19.155 ms 100.100.16.28 (100.100.16.28) 19
25 99.83.89.19 (99.83.89.19) 28.929 ms * 21.790 ms
26 104.26.11.229 (104.26.11.229) 11.070 ms 11.058 ms 11.982 ms
```

Q3:

In Traceroute B, how many routers are between the two systems?

26

✓ Correct Answer

Q4:

```
root@ip-10-10-129-250:~# traceroute 10.10.140.133
traceroute to 10.10.140.133 (10.10.140.133), 30 hops max, 60 byte packets
 1  10.10.140.133 (10.10.140.133)  1.950 ms  1.866 ms  1.837 ms
root@ip-10-10-129-250:~#
```

Task 5:

Q1:

Start the attached VM from Task 3 if it is not already started. On the AttackBox, open the terminal and use the telnet client to connect to the VM on port 80. What is the name of the running server?

Apache

✓ Correct Answer

Q2:

What is the version of the running server (on port 80 of the VM)?

2.4.61

✓ Correct Answer

Command for both questions:

```
root@ip-10-10-129-250:~# telnet 10.10.114.128 80
Trying 10.10.114.128...
Connected to 10.10.114.128.
Escape character is '^]'.
GET / HTTP/1.1
host: telhHTTP/1.1 408 Request Timeout
Date: Tue, 04 Feb 2025 08:41:23 GMT
Server: Apache/2.4.61 (Debian)
```


Task 6:

Q1:

Start the VM and open the AttackBox. Once the AttackBox loads, use Netcat to connect to the VM port 21. What is the version of the running server?

0.17

✓ Correct Answer

```
root@ip-10-10-129-250:~# nc 10.10.251.158 21
220 ip-10-10-251-158.eu-west-1.compute.internal FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
```



Red Team Recon

Learn how to use DNS, advanced searching, Recon-ng, and Maltego to collect information about your target.



Passive Reconnaissance

Learn about the essential tools for passive reconnaissance, such as whois, nslookup, and dig.



Active Reconnaissance

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