MINISTRY OF EDUCATION
IMAM ABDULRAHMAN BIN
FAISAL UNIVERSITY
COLLEGE OF COMPUTER SCIENCE
& INFORMATION TECHNOLOGY
Department of Computer Science

وزارة التعليم
جامعة الإمام
عبدالرحمن بن فيصل
كلية علوم الحاسب
وتقنية المعلومات

IAU
جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

Lab Report No.1

Footprinting and Reconnaissance

Ethical Hacking

Submitted By: Raghad Alharthi 2210003220

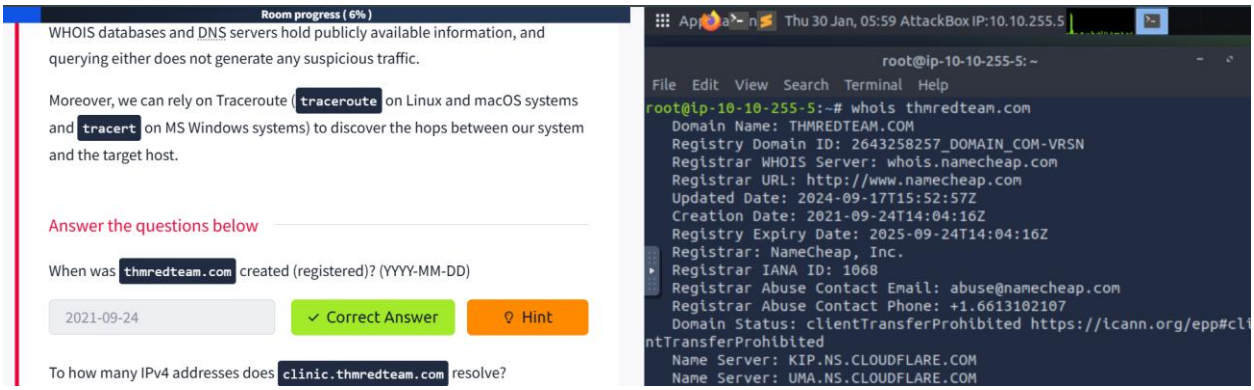
Section: CS Group no. 2

Contents

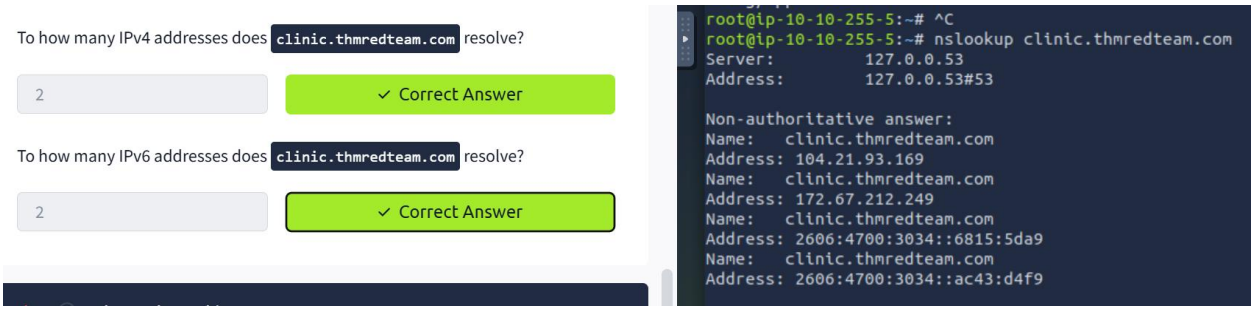
Room: Red Team Recon

Task 3:

Q1:



Q2 & Q3:



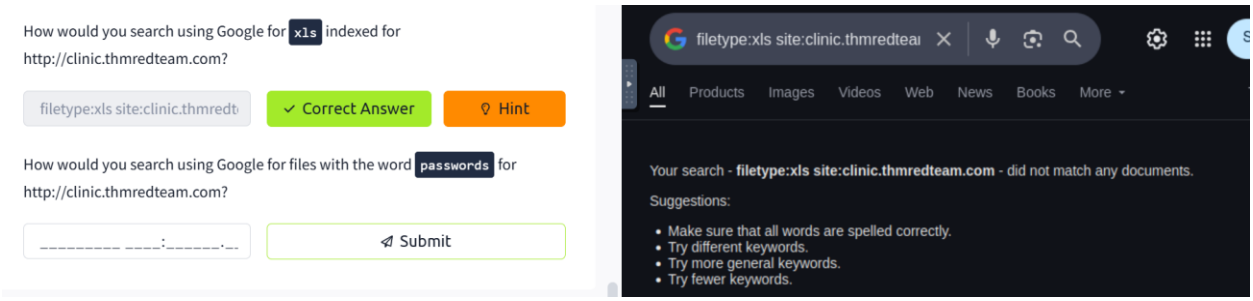
Task 4:

Q1:

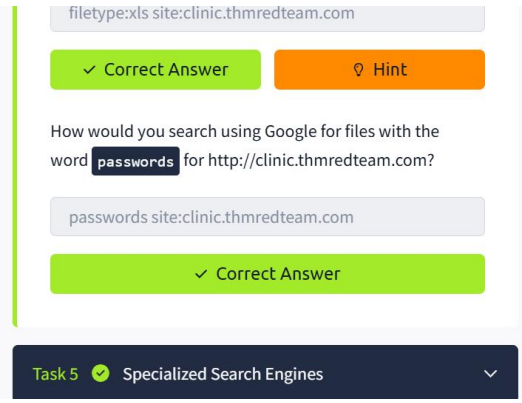
OSINT filetype:pdf	Find files of type PDF related to a certain term.
salary site:blog.tryhackme.com	Limit search results to a specific site.

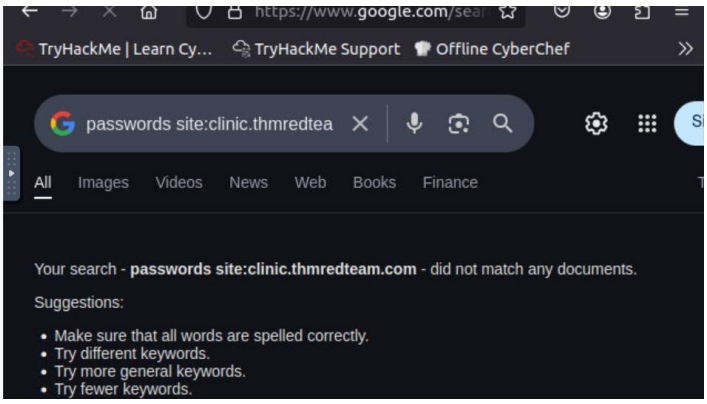
combining these two queries.

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



Q2:

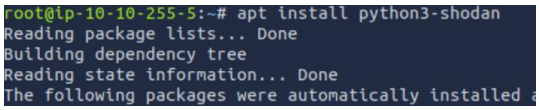




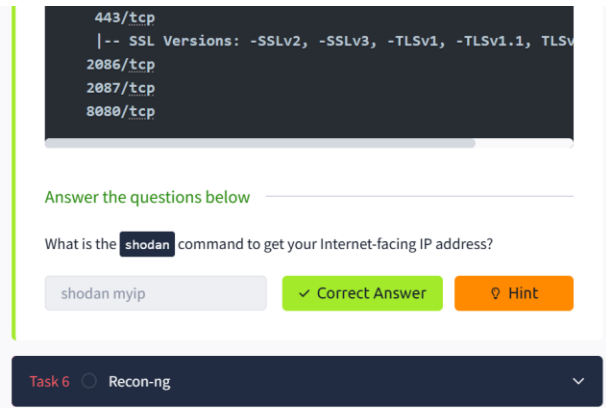
Task 5:

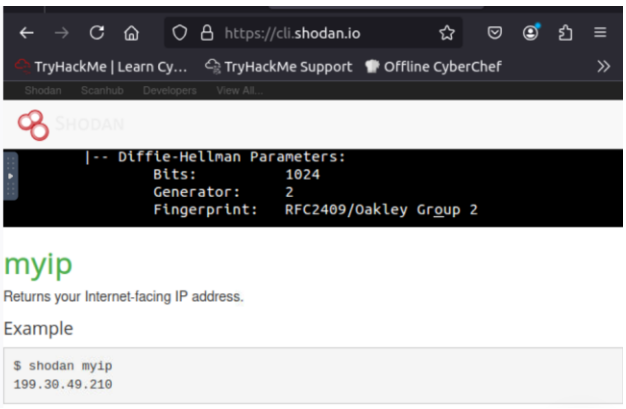
Q1:

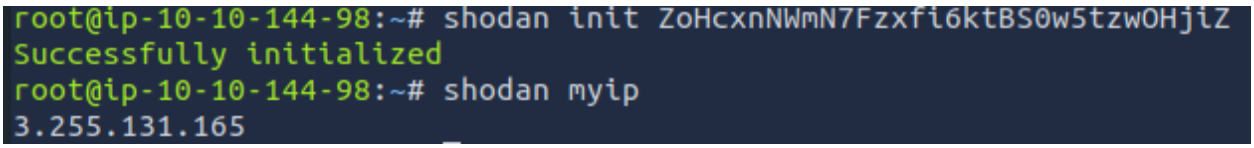
Installing shodan:



API key







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?

Q2:

How many modules with the name `virustotal` exist?

2 ✓ Correct Answer

```
[recon-ng][clinicredteam] > 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 for a company. This module c
icates.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:

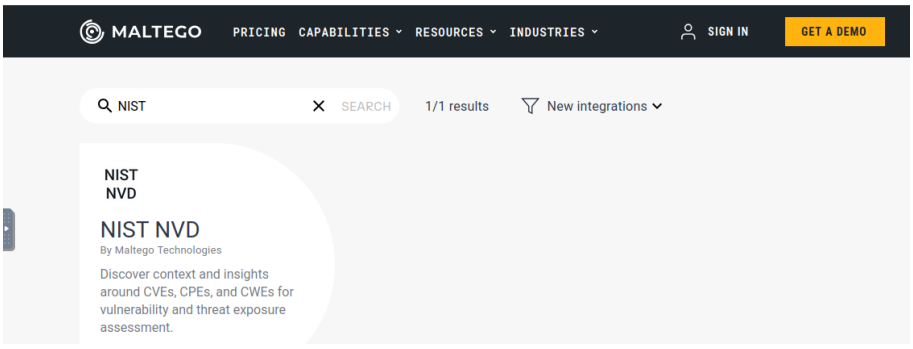
Q1:

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

NIST NVD

✓ Correct Answer

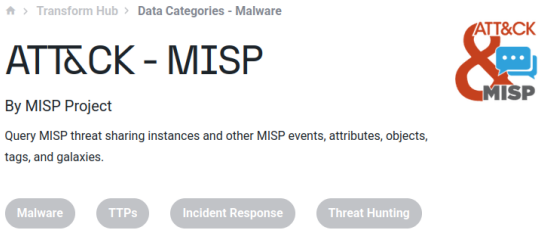
Hint



Q2:

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

MISP Project | ✓ Correct Answer | Hint



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?

namecheap.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?

cloudflare.com ✓ 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?

THM{a5b83929888ed36acb0272971e438d78} ✓ 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:

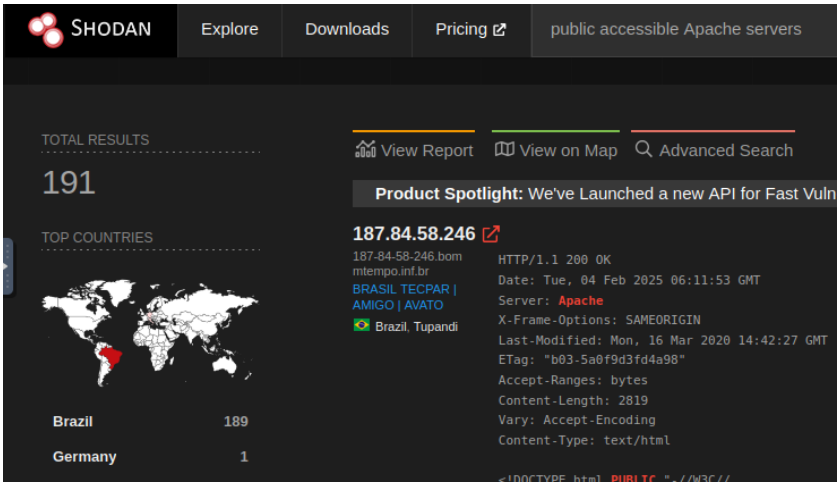
Q1:

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



Q2:

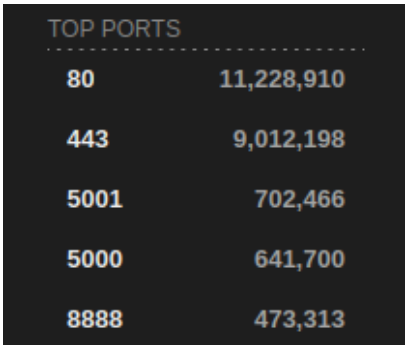
Based on Shodan.io, what is the 3rd most common port used for Apache?

8080 ✓ Correct Answer Hint

Q3:

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

5001 ✓ Correct Answer Hint



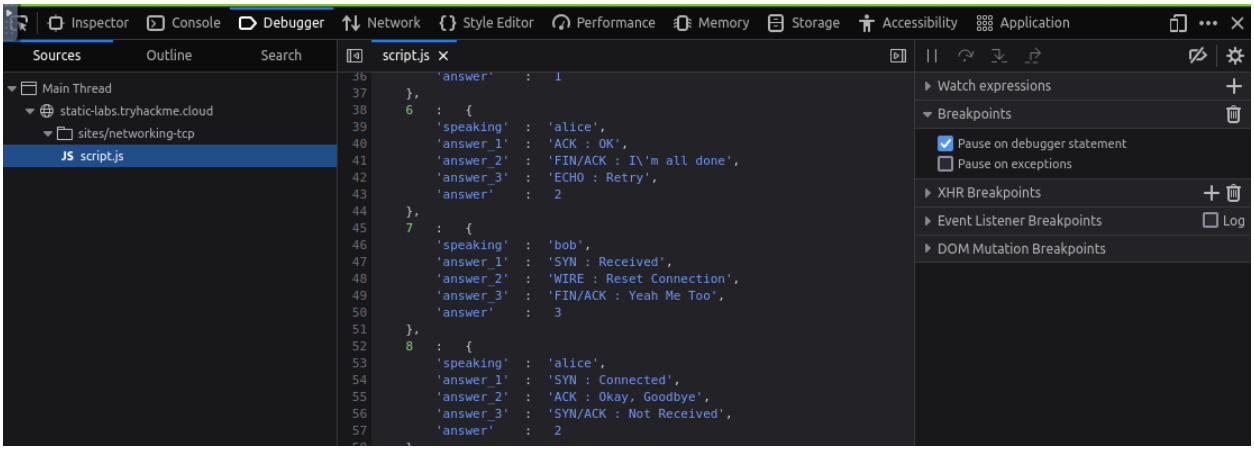
Room: Active Reconnaissance

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.

8 ✓ Correct Answer Hint



Task 3:

Q1:

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

-s ✓ 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
```

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: teltHTTP/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.