NAME :- Saurav Gajanan Patil

Gmail Id :- sauravpatil0506@gail.com

College :- NDMVP's KBTCOE,Nashik

- **Active Reconnaissance:**

  So , at starting the lab tells details like what is active reconnaissance and its tools . so for active reconnaissance we nned to have some contact to target like if we have to open a door we have to check the kry hole properly or lock properly by making contact with it.

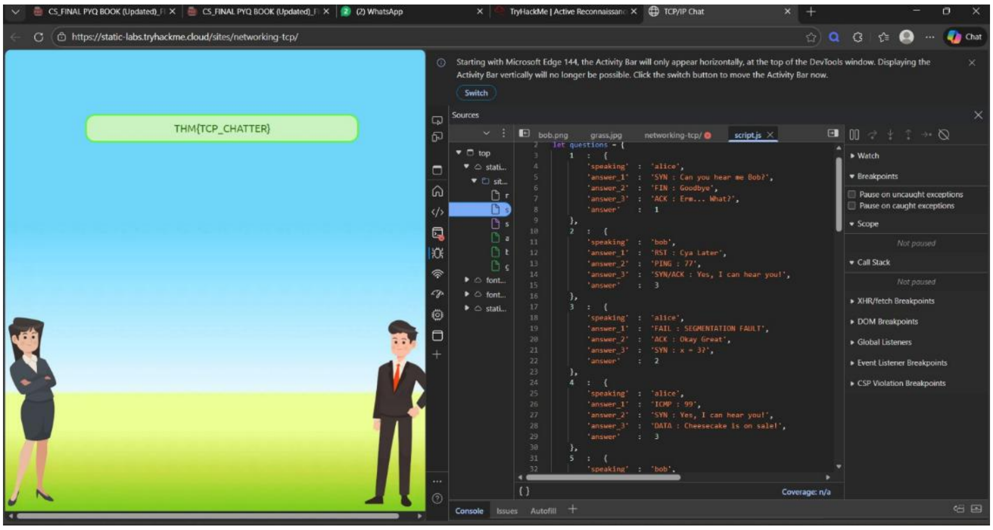
  In this room we use many tools for active reconnaissance like.

  - Browser developer Option
  - Ping
  - telnet
  - netcat
  - traceroute

so , lets deep dive in tools to get more details about it and how they works,

1) **Browser developer option:-**

   So first lets know how to open this in linux or windows , By clicking Ctrl+Shift+I so it opens a inspect window by which we can inspect a webpage on which we has opened the inspect window it shows details like , source codes ,files, images used in webpage , networks etc. lets go though the webpage provided in the task on the room

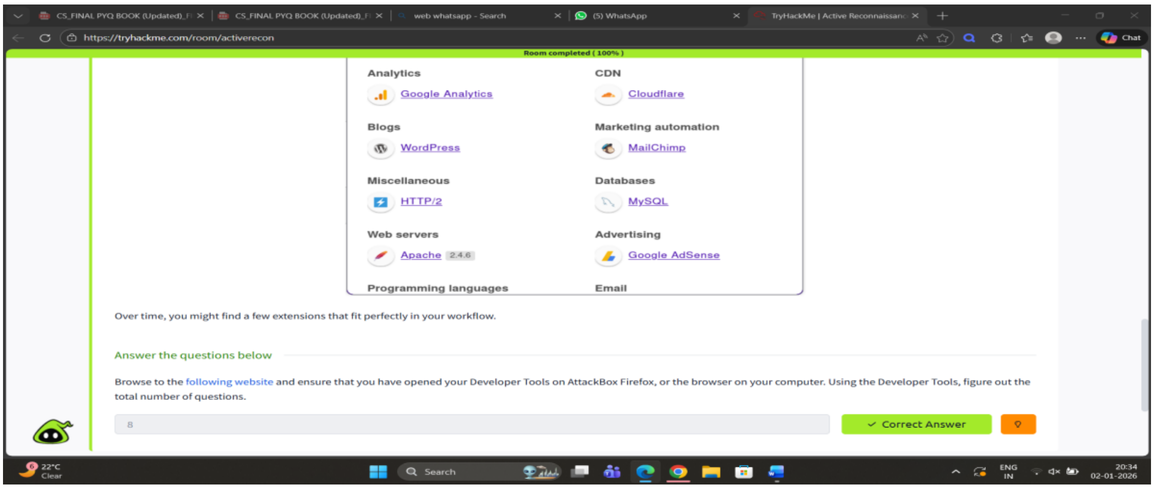


THM{TCP_CHATTER}

Starting with Microsoft Edge 144, the Activity Bar will only appear horizontally, at the top of the DevTools window. Displaying the Activity Bar vertically will no longer be possible. Click the switch button to move the Activity Bar now.

```
let questions = {
    1   :   {
        'speaking'  :  'alice',
        'answer_1'  :  'SYN : Can you hear me Bob?',
        'answer_2'  :  'FIN : Goodbye',
        'answer_3'  :  'ACK : Erm... What?',
        'answer'    :  1
    },
    2   :   {
        'speaking'  :  'bob',
        'answer_1'  :  'RST : Cya Later',
        'answer_2'  :  'PING : 77',
        'answer_3'  :  'SYN/ACK : Yes, I can hear you!',
        'answer'    :  3
    },
    3   :   {
        'speaking'  :  'alice',
        'answer_1'  :  'FAIL : SEGMENTATION FAULT',
        'answer_2'  :  'ACK : Okay Great',
        'answer_3'  :  'SYN : x = 3?',
        'answer'    :  2
    },
    4   :   {
        'speaking'  :  'alice',
        'answer_1'  :  'ICMP : 99',
        'answer_2'  :  'SYN : Yes, I can hear you!',
        'answer_3'  :  'DATA : Cheesecake is on sale!',
        'answer'    :  3
    },
    5   :   {
        'speaking'  :  'bob',
```

So as in above pic we can see a webpage alice is asking some questions to bob and each question have 3 options so to slect correct answers we have check the code of the site i.e script in this webpage so we will get the correct answers for each so we open inspect window and check the file in source option so , there script.js is present in which we can see the questions with options and correct answer is given so by solving this at end we will get the flag THM{TCP_CHAPTER} which is the end we have to get .so by this inspecter window we can check codes and styles data and



Room completed (100%)

Analytics	CDN
Google Analytics	Cloudflare
Blogs	**Marketing automation**
WordPress	MailChimp
Miscellaneous	**Databases**
HTTP/2	MySQL
Web servers	**Advertising**
Apache 2.4.6	Google AdSense
Programming languages	**Email**

Over time, you might find a few extensions that fit perfectly in your workflow.

Answer the questions below

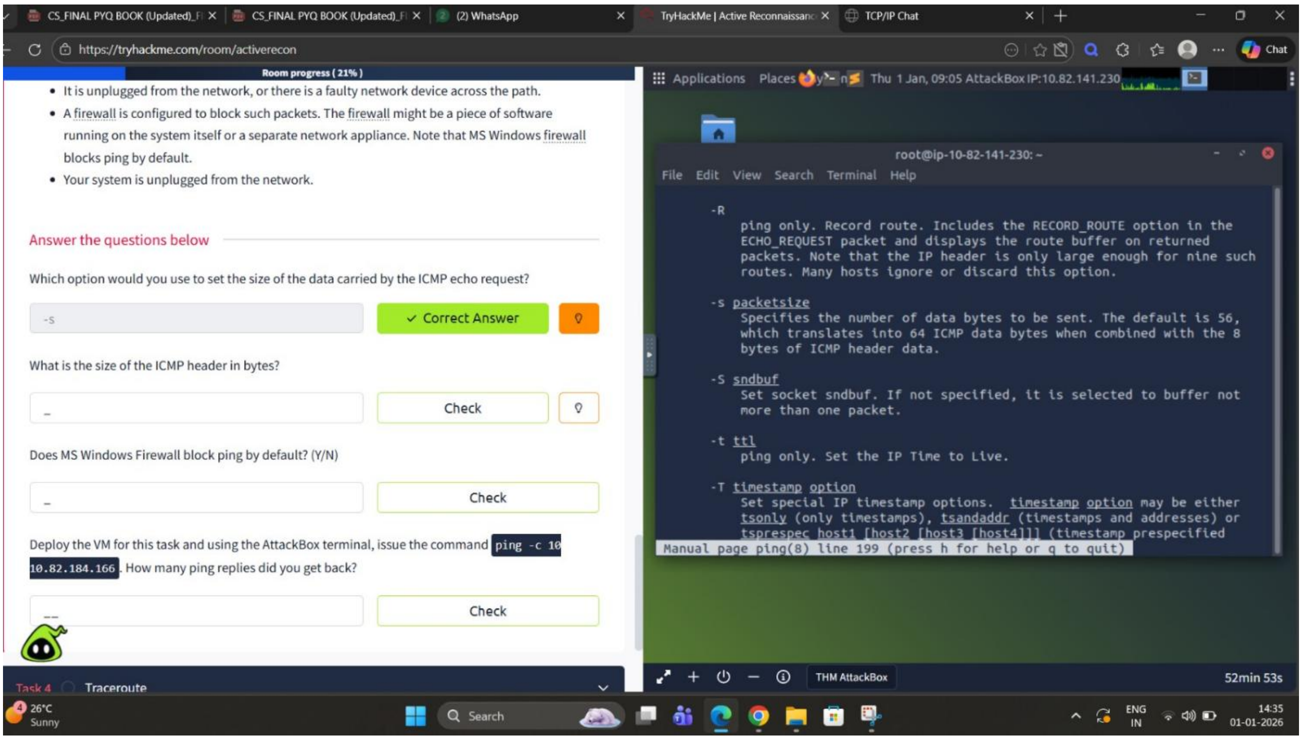
Browse to the following website and ensure that you have opened your Developer Tools on AttackBox Firefox, or the browser on your computer. Using the Developer Tools, figure out the total number of questions.

8

So the question in the lab ask how many total number of questions are there so by inspecting we can see there 8 questions in script.js so correct answer is 8 . by this way we can solve this first lesson now move on next lesson

2)Ping:-

ping is a tool we can use to check if we are connected to the system or not we can ping the ip address of the system and our system will send packets to the system if we recive all sent packets then we are connected . so in this lap they have also given some commands like ping -n 11 <host-ip> we can use this to send 11 packets by using -n we can tell how many no. of packets we want to send . to see whole manual to check which commands are used for what purpose in ping we can use simple command like **man ping** linux to open whole manual. Lets move forward to questions



CS_FINAL PYQ BOOK (Updated)_F
CS_FINAL PYQ BOOK (Updated)_F
(2) WhatsApp
TryHackMe | Active Reconnaissanc
TCP/IP Chat
https://tryhackme.com/room/activerecon
Chat
Room progress (21%)
Applications
Places
Thu 1 Jan, 09:05 AttackBox IP:10.82.141.230
root@ip-10-82-141-230: ~
File Edit View Search Terminal Help
THM AttackBox
52min 53s
Task 4 Traceroute
26°C
Sunny
Search
ENG
IN
14:35
01-01-2026

- It is unplugged from the network, or there is a faulty network device across the path.
- 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.
- Your system is unplugged from the network.

Answer the questions below

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

-s ✓ Correct Answer

What is the size of the ICMP header in bytes?

_ Check

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

_ Check

Deploy the VM for this task and using the AttackBox terminal, issue the command `ping -c 10 10.82.184.166`. How many ping replies did you get back?

__ Check

```
       -R
           ping only. Record route. Includes the RECORD_ROUTE option in the
           ECHO_REQUEST packet and displays the route buffer on returned
           packets. Note that the IP header is only large enough for nine such
           routes. Many hosts ignore or discard this option.

       -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.

       -S sndbuf
           Set socket sndbuf. If not specified, it is selected to buffer not
           more than one packet.

       -t ttl
           ping only. Set the IP Time to Live.

       -T timestamp option
           Set special IP timestamp options.  timestamp option may be either
           tsonly (only timestamps), tsandaddr (timestamps and addresses) or
           tsprespec host1 [host2 [host3 [host4]]] (timestamp prespecified
 Manual page ping(8) line 199 (press h for help or q to quit)
```

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

-> so , the answer is -s as we see in manual opened in the above picture that -s is use to specify the number of data bytes to be sent so the correct answer is -s.

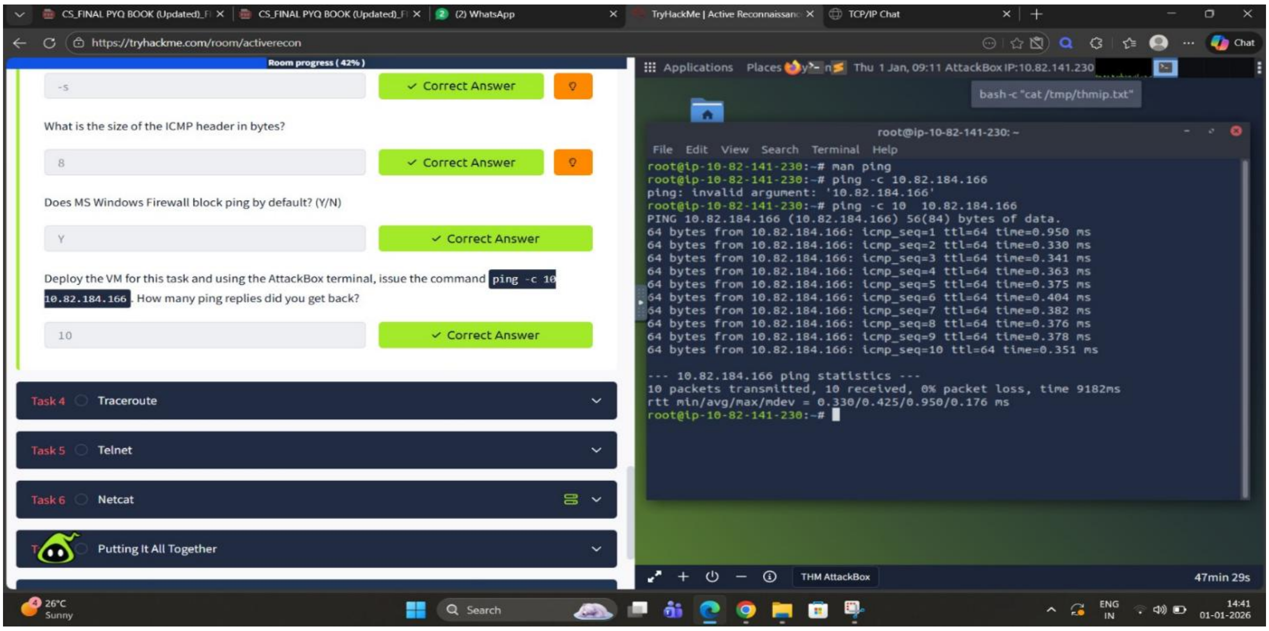
2. What is the size of the ICMP header in bytes?
-> in manual under command **-s packetsize** we see the last line mention ICMP header size as 8 bytes.

So, the correct answer is 8.

3) Does MS Windows Firewall block ping by default? (Y/N)
-> Y(yes), MS Windows Firewall blocks ping it is given in the lesson while teaching , but if tried to run ping on windows termial it blocks it so yes MS Windows Firewalls blocks ping.

4) Deploy the VM for this task and using the AttackBox terminal, issue the command ping -c 10 10.82.184.166. How many ping replies did you get back?

-> so in below window we can see we have opend attackbox and has runed ping -c 10 10.82.184.166 and it has pinged 10 times the ip so the correct answer is 10 also at end we can see it is written on terminal that 10 packets transmited,10 recived.



CS_FINAL PYQ BOOK (Updated)_F
CS_FINAL PYQ BOOK (Updated)_F
(2) WhatsApp
TryHackMe | Active Reconnaissanc
TCP/IP Chat
https://tryhackme.com/room/activerecon
Room progress (42%)
✓ Correct Answer
Task 4 Traceroute
Task 5 Telnet
Task 6 Netcat
Putting It All Together
Applications
Places
Thu 1 Jan, 09:11 AttackBox IP:10.82.141.230
bash -c "cat /tmp/thmip.txt"
root@ip-10-82-141-230: ~
File Edit View Search Terminal Help
THM AttackBox
47min 29s
26°C Sunny
Search
ENG IN
14:41 01-01-2026

[redacted]

-s

What is the size of the ICMP header in bytes?

8

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

Y

Deploy the VM for this task and using the AttackBox terminal, issue the command `ping -c 10 10.82.184.166`. How many ping replies did you get back?

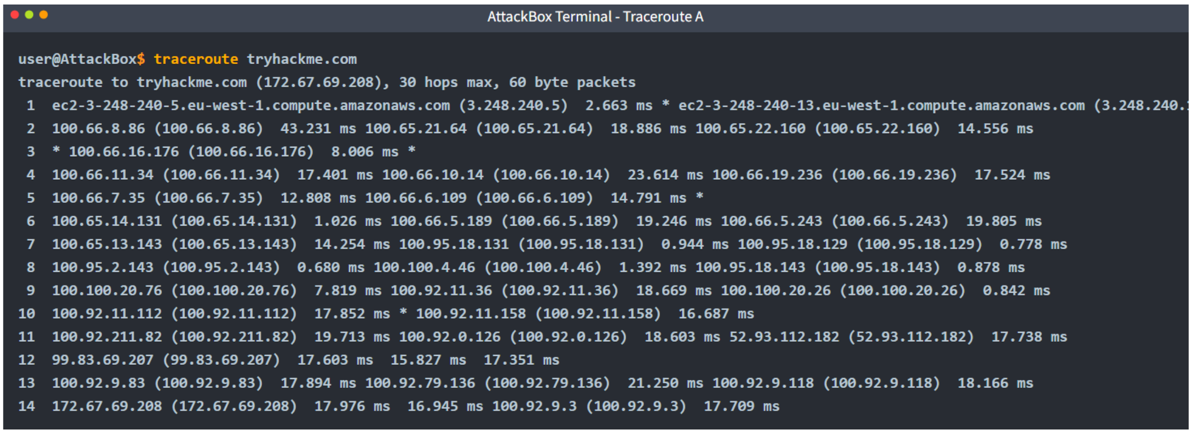
10

```
root@ip-10-82-141-230:~# man ping
root@ip-10-82-141-230:~# ping -c 10.82.184.166
ping: invalid argument: '10.82.184.166'
root@ip-10-82-141-230:~# ping -c 10  10.82.184.166
PING 10.82.184.166 (10.82.184.166) 56(84) bytes of data.
64 bytes from 10.82.184.166: icmp_seq=1 ttl=64 time=0.950 ms
64 bytes from 10.82.184.166: icmp_seq=2 ttl=64 time=0.330 ms
64 bytes from 10.82.184.166: icmp_seq=3 ttl=64 time=0.341 ms
64 bytes from 10.82.184.166: icmp_seq=4 ttl=64 time=0.363 ms
64 bytes from 10.82.184.166: icmp_seq=5 ttl=64 time=0.375 ms
64 bytes from 10.82.184.166: icmp_seq=6 ttl=64 time=0.404 ms
64 bytes from 10.82.184.166: icmp_seq=7 ttl=64 time=0.382 ms
64 bytes from 10.82.184.166: icmp_seq=8 ttl=64 time=0.376 ms
64 bytes from 10.82.184.166: icmp_seq=9 ttl=64 time=0.378 ms
64 bytes from 10.82.184.166: icmp_seq=10 ttl=64 time=0.351 ms

--- 10.82.184.166 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9182ms
rtt min/avg/max/mdev = 0.330/0.425/0.950/0.176 ms
root@ip-10-82-141-230:~# 
```

So with this first lesson ha ended lets move forward to next lesson.

3) traceroute:-

So , first check what traceroute helps in , by using traceroute we can see how many routers are there between host and server , so basically it find the ip address of the routers intermediate between host and servers or two connected hosts. By using command **traceroute server_ip** as given in below picture lets go by picture and question in the lesson to get better understanding.

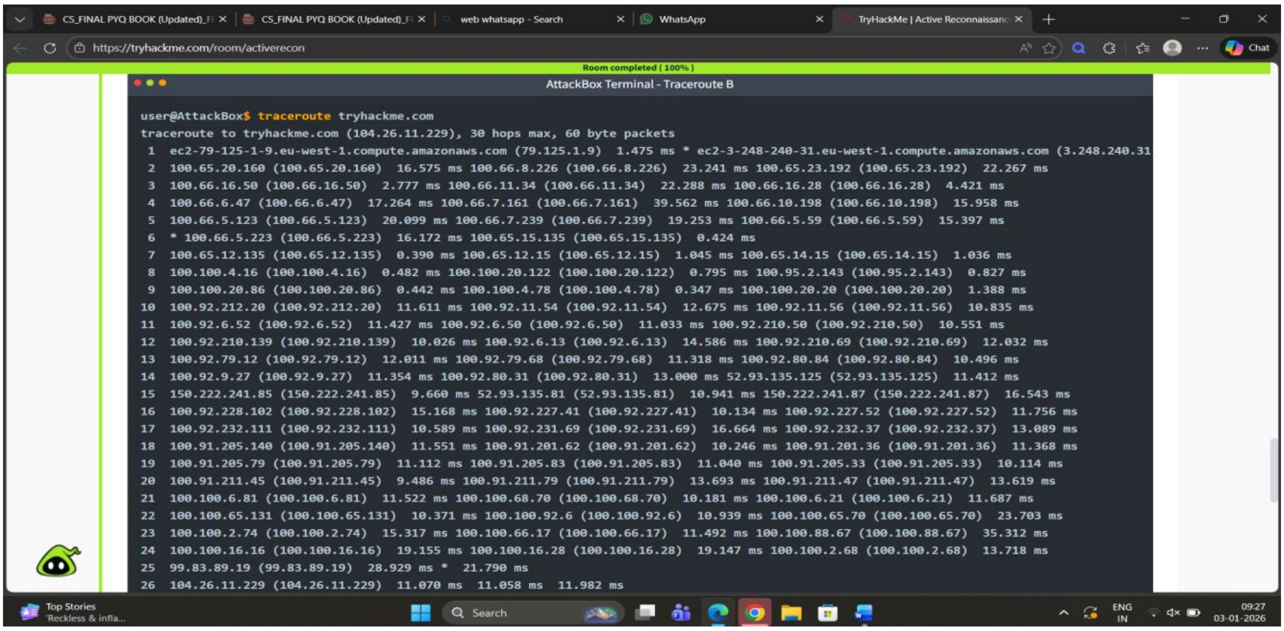


AttackBox Terminal - Traceroute A

```
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.
 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
 5  100.66.7.35 (100.66.7.35)  12.808 ms 100.66.6.109 (100.66.6.109)  14.791 ms *
 6  100.65.14.131 (100.65.14.131)  1.026 ms 100.66.5.189 (100.66.5.189)  19.246 ms 100.66.5.243 (100.66.5.243)  19.805 ms
 7  100.65.13.143 (100.65.13.143)  14.254 ms 100.95.18.131 (100.95.18.131)  0.944 ms 100.95.18.129 (100.95.18.129)  0.778 ms
 8  100.95.2.143 (100.95.2.143)  0.680 ms 100.100.4.46 (100.100.4.46)  1.392 ms 100.95.18.143 (100.95.18.143)  0.878 ms
 9  100.100.20.76 (100.100.20.76)  7.819 ms 100.92.11.36 (100.92.11.36)  18.669 ms 100.100.20.26 (100.100.20.26)  0.842 ms
10  100.92.11.112 (100.92.11.112)  17.852 ms * 100.92.11.158 (100.92.11.158)  16.687 ms
11  100.92.211.82 (100.92.211.82)  19.713 ms 100.92.0.126 (100.92.0.126)  18.603 ms 52.93.112.182 (52.93.112.182)  17.738 ms
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 ms 100.92.9.118 (100.92.9.118)  18.166 ms
14  172.67.69.208 (172.67.69.208)  17.976 ms  16.945 ms 100.92.9.3 (100.92.9.3)  17.709 ms
```

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

-> above image show the traceroute A in which we can see the last ip as the last router ip before reaching tryhackme.com and in above image it is **172.67.69.208** so it's the correct answer.


CS_FINAL PYQ BOOK (Updated)_F
CS_FINAL PYQ BOOK (Updated)_F
web whatsapp - Search
WhatsApp
TryHackMe | Active Reconnaissanc
https://tryhackme.com/room/activerecon
Chat
Room completed (100%)
AttackBox Terminal - Traceroute B
Top Stories
'Reckless & infla...
Search
ENG
IN
09:27
03-01-2026

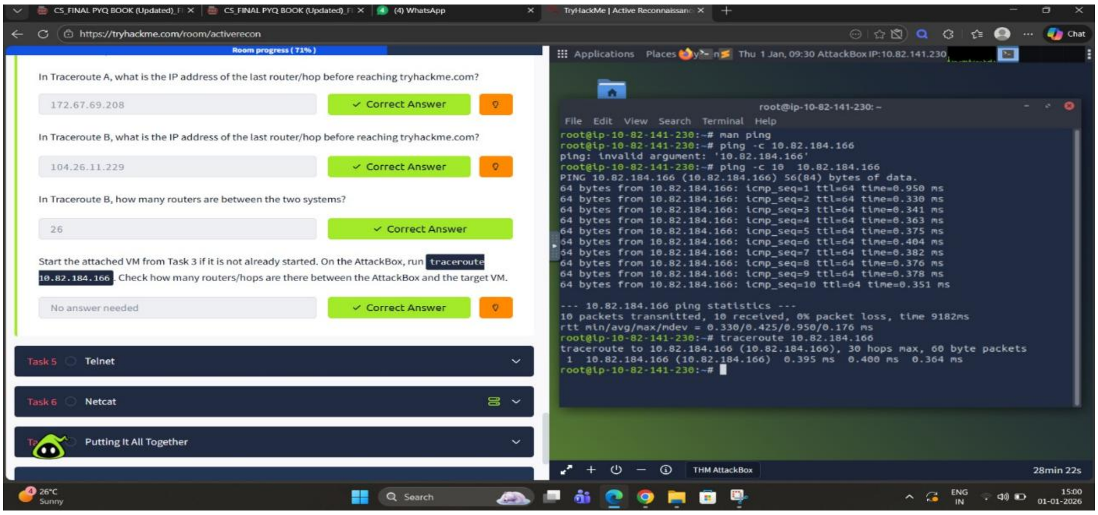
```
user@AttackBox$ traceroute tryhackme.com
traceroute to tryhackme.com (104.26.11.229), 30 hops max, 60 byte packets
 1  ec2-79-125-1-9.eu-west-1.compute.amazonaws.com (79.125.1.9)  1.475 ms * ec2-3-248-240-31.eu-west-1.compute.amazonaws.com (3.248.240.31
 2  100.65.20.160 (100.65.20.160)  16.575 ms 100.66.8.226 (100.66.8.226)  23.241 ms 100.65.23.192 (100.65.23.192)  22.267 ms
 3  100.66.16.50 (100.66.16.50)  2.777 ms 100.66.11.34 (100.66.11.34)  22.288 ms 100.66.16.28 (100.66.16.28)  4.421 ms
 4  100.66.6.47 (100.66.6.47)  17.264 ms 100.66.7.161 (100.66.7.161)  39.562 ms 100.66.10.198 (100.66.10.198)  15.958 ms
 5  100.66.5.123 (100.66.5.123)  20.099 ms 100.66.7.239 (100.66.7.239)  19.253 ms 100.66.5.59 (100.66.5.59)  15.397 ms
 6  * 100.66.5.223 (100.66.5.223)  16.172 ms 100.65.15.135 (100.65.15.135)  0.424 ms
 7  100.65.12.135 (100.65.12.135)  0.390 ms 100.65.12.15 (100.65.12.15)  1.045 ms 100.65.14.15 (100.65.14.15)  1.036 ms
 8  100.100.4.16 (100.100.4.16)  0.482 ms 100.100.20.122 (100.100.20.122)  0.795 ms 100.95.2.143 (100.95.2.143)  0.827 ms
 9  100.100.20.86 (100.100.20.86)  0.442 ms 100.100.4.78 (100.100.4.78)  0.347 ms 100.100.20.20 (100.100.20.20)  1.388 ms
10  100.92.212.20 (100.92.212.20)  11.611 ms 100.92.11.54 (100.92.11.54)  12.675 ms 100.92.11.56 (100.92.11.56)  10.835 ms
11  100.92.6.52 (100.92.6.52)  11.427 ms 100.92.6.50 (100.92.6.50)  11.033 ms 100.92.210.50 (100.92.210.50)  10.551 ms
12  100.92.210.139 (100.92.210.139)  10.026 ms 100.92.6.13 (100.92.6.13)  14.586 ms 100.92.210.69 (100.92.210.69)  12.032 ms
13  100.92.79.12 (100.92.79.12)  12.011 ms 100.92.79.68 (100.92.79.68)  11.318 ms 100.92.80.84 (100.92.80.84)  10.496 ms
14  100.92.9.27 (100.92.9.27)  11.354 ms 100.92.80.31 (100.92.80.31)  13.000 ms 52.93.135.125 (52.93.135.125)  11.412 ms
15  150.222.241.85 (150.222.241.85)  9.660 ms 52.93.135.81 (52.93.135.81)  10.941 ms 150.222.241.87 (150.222.241.87)  16.543 ms
16  100.92.228.102 (100.92.228.102)  15.168 ms 100.92.227.41 (100.92.227.41)  10.134 ms 100.92.227.52 (100.92.227.52)  11.756 ms
17  100.92.232.111 (100.92.232.111)  10.589 ms 100.92.231.69 (100.92.231.69)  16.664 ms 100.92.232.37 (100.92.232.37)  13.089 ms
18  100.91.205.140 (100.91.205.140)  11.551 ms 100.91.201.62 (100.91.201.62)  10.246 ms 100.91.201.36 (100.91.201.36)  11.368 ms
19  100.91.205.79 (100.91.205.79)  11.112 ms 100.91.205.83 (100.91.205.83)  11.040 ms 100.91.205.33 (100.91.205.33)  10.114 ms
20  100.91.211.45 (100.91.211.45)  9.486 ms 100.91.211.79 (100.91.211.79)  13.693 ms 100.91.211.47 (100.91.211.47)  13.619 ms
21  100.100.6.81 (100.100.6.81)  11.522 ms 100.100.68.70 (100.100.68.70)  10.181 ms 100.100.6.21 (100.100.6.21)  11.687 ms
22  100.100.65.131 (100.100.65.131)  10.371 ms 100.100.92.6 (100.100.92.6)  10.939 ms 100.100.65.70 (100.100.65.70)  23.703 ms
23  100.100.2.74 (100.100.2.74)  15.317 ms 100.100.66.17 (100.100.66.17)  11.492 ms 100.100.88.67 (100.100.88.67)  35.312 ms
24  100.100.16.16 (100.100.16.16)  19.155 ms 100.100.16.28 (100.100.16.28)  19.147 ms 100.100.2.68 (100.100.2.68)  13.718 ms
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
```

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

-> so , like traceroute A , we have to see the ip address of last router in the Traceroute B and here it is **104.26.11.229** so it is tge correct answer .

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

-> so , here they has asked how many routers are between two systems in tarcerouteB so we can see there are 26 result present on the traceroute b terminal i.e 26 ip addresses , so these are of routers therefore , there are 26 routers in between so **26** is the correct answer.



CS_FINAL PYQ BOOK (Updated)_F
CS_FINAL PYQ BOOK (Updated)_F
(4) WhatsApp
TryHackMe | Active Reconnaissanc
https://tryhackme.com/room/activerecon
Room progress (71%)
Applications
Places
Thu 1 Jan, 09:30 AttackBox IP:10.82.141.230
Chat
THM AttackBox
28min 22s
26°C
Sunny
Search
ENG
IN
15:00
01-01-2026

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

172.67.69.208 ✓ Correct Answer

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

104.26.11.229 ✓ Correct Answer

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

26 ✓ Correct Answer

Start the attached VM from Task 3 if it is not already started. On the AttackBox, run `traceroute 10.82.184.166`. Check how many routers/hops are there between the AttackBox and the target VM.

No answer needed ✓ Correct Answer

Task 5 Telnet

Task 6 Netcat

Putting It All Together

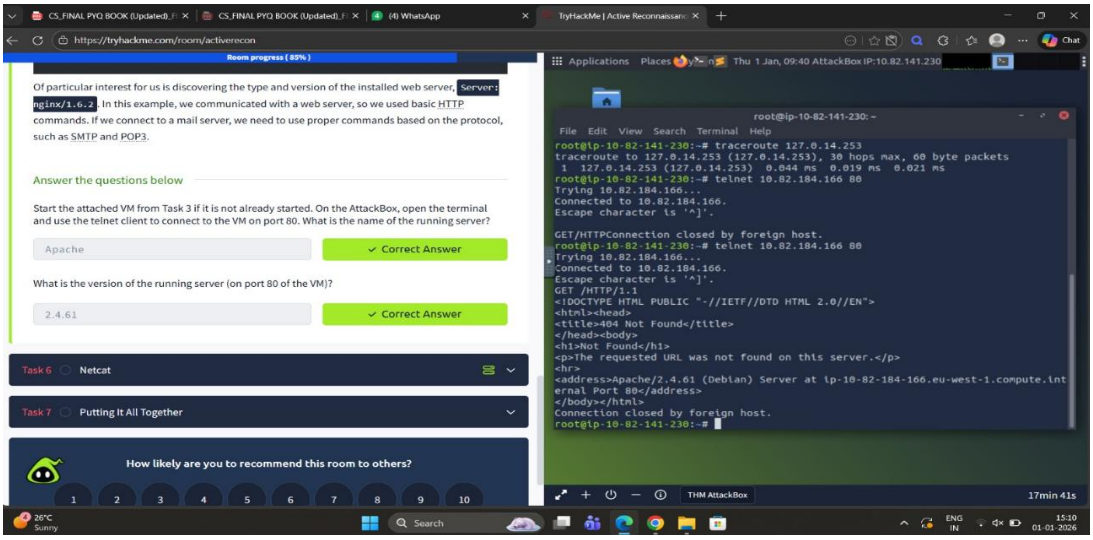
```
root@ip-10-82-141-230: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-82-141-230:~# man ping
root@ip-10-82-141-230:~# ping -c 10.82.184.166
ping: invalid argument: '10.82.184.166'
root@ip-10-82-141-230:~# ping -c 10  10.82.184.166
PING 10.82.184.166 (10.82.184.166) 56(84) bytes of data.
64 bytes from 10.82.184.166: icmp_seq=1 ttl=64 time=0.950 ms
64 bytes from 10.82.184.166: icmp_seq=2 ttl=64 time=0.330 ms
64 bytes from 10.82.184.166: icmp_seq=3 ttl=64 time=0.341 ms
64 bytes from 10.82.184.166: icmp_seq=4 ttl=64 time=0.363 ms
64 bytes from 10.82.184.166: icmp_seq=5 ttl=64 time=0.375 ms
64 bytes from 10.82.184.166: icmp_seq=6 ttl=64 time=0.404 ms
64 bytes from 10.82.184.166: icmp_seq=7 ttl=64 time=0.382 ms
64 bytes from 10.82.184.166: icmp_seq=8 ttl=64 time=0.376 ms
64 bytes from 10.82.184.166: icmp_seq=9 ttl=64 time=0.378 ms
64 bytes from 10.82.184.166: icmp_seq=10 ttl=64 time=0.351 ms

--- 10.82.184.166 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9182ms
rtt min/avg/max/mdev = 0.330/0.425/0.950/0.176 ms
root@ip-10-82-141-230:~# traceroute 10.82.184.166
traceroute to 10.82.184.166 (10.82.184.166), 30 hops max, 60 byte packets
 1  10.82.184.166 (10.82.184.166)  0.395 ms  0.400 ms  0.364 ms
root@ip-10-82-141-230:~# █
```

4)Start the attached VM from Task 3 if it is not already started. On the AttackBox, run `traceroute  10.82.184.166`. Check how many routers/hops are there between the AttackBox and the target VM.
-> so we have to start attackbox for this task they does not want any answer just want that we should try it once practically so open attackbox and run command **traceroute 10.82.184.166** after that we gwt only one output so there is only one intermediate router present in between as we can see in above picture.

4) <u>Telnet :-</u>

so by telnet we can connect to any running services by tcp protocol and can listen and exchange messages until it uses encryption , therefore it is not secure and not used more enough so, we have ssh (secure shell protocol) which is secure and used ore by everyone then telnet because it uses encryption so if any user try to get data it will be in encrypted form and not as it is like telnet . telnet works on port 23 .

so lets see question in the lesson



CS_FINAL PYQ BOOK (Updated)_F
CS_FINAL PYQ BOOK (Updated)_F
(4) WhatsApp
TryHackMe | Active Reconnaissanc
https://tryhackme.com/room/activerecon
Room progress (85%)
Applications
Places
Thu 1 Jan, 09:40 AttackBox IP:10.82.141.230
Chat
THM AttackBox
17min 41s
26°C
Sunny
Search
ENG
IN
15:10
01-01-2026

Of particular interest for us is discovering the type and version of the installed web server, `Server: nginx/1.6.2`. In this example, we communicated with a web server, so we used basic HTTP commands. If we connect to a mail server, we need to use proper commands based on the protocol, such as SMTP and POP3.

Answer the questions below

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

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

2.4.61 ✓ Correct Answer

Task 6 Netcat

Task 7 Putting It All Together

How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9 10

```
root@ip-10-82-141-230: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-82-141-230:~# traceroute 127.0.14.253
traceroute to 127.0.14.253 (127.0.14.253), 30 hops max, 60 byte packets
 1  127.0.14.253 (127.0.14.253)  0.044 ms  0.019 ms  0.021 ms
root@ip-10-82-141-230:~# telnet 10.82.184.166 80
Trying 10.82.184.166...
Connected to 10.82.184.166.
Escape character is '^]'.

GET/HTTPConnection closed by foreign host.
root@ip-10-82-141-230:~# telnet 10.82.184.166 80
Trying 10.82.184.166...
Connected to 10.82.184.166.
Escape character is '^]'.
GET /HTTP/1.1
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.61 (Debian) Server at ip-10-82-184-166.eu-west-1.compute.int
ernal Port 80</address>
</body></html>
Connection closed by foreign host.
root@ip-10-82-141-230:~# █
```

1) 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?
-> so we have to oprn a terminal on attackbox and have to connect to port 80 and have to check the running server so lets do it
so to connect on port 80 we should type command **"telnet 10.82.184.166 80** " so here 10.82.184.166 is the ip address of the machine and 80 in the last the port number . after running this press enter and type **GET /HTTP/1.1** we use this because we are connecting to the http server so by using this we can get the data after that we the data where we can see the server is **Apache 2.4.61 (Debian)** so the server is Apache (for refrence see above image).

2)What is the version of the running server (on port 80 of the VM)?
-> so , as I say we can see srever **Apache 2.4.61 (Debian)** here **2.4.61** is the version of the running server.

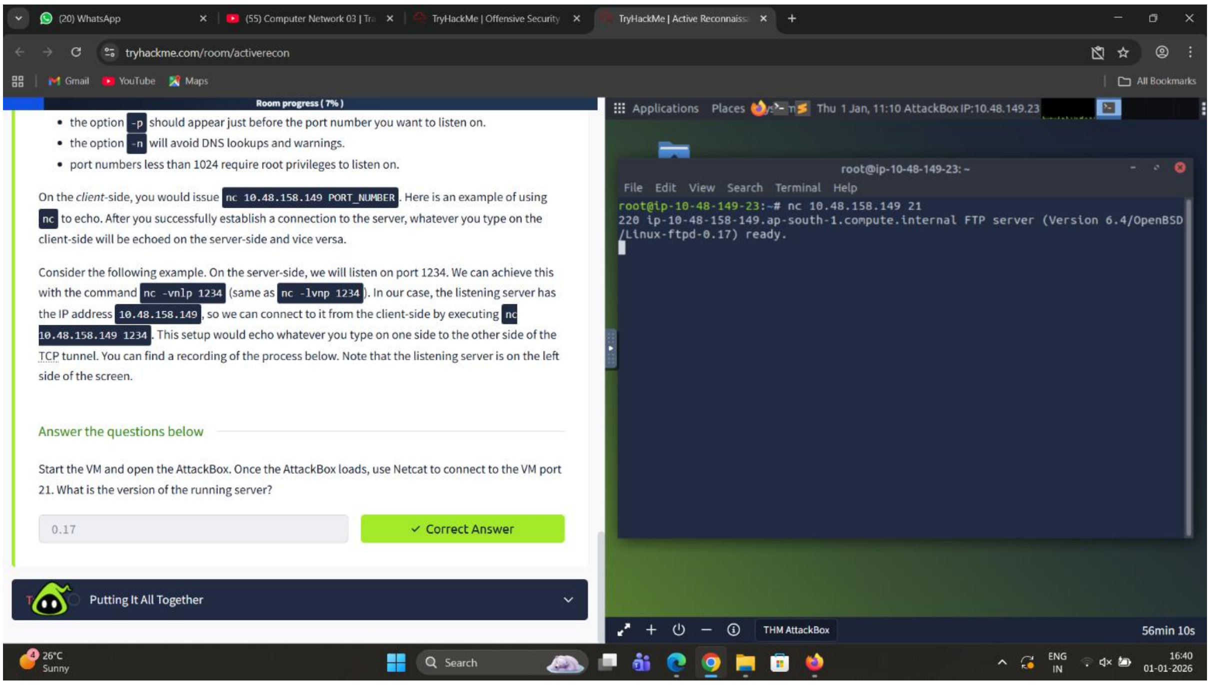
5) <u>Netcat</u> :-

Netcat (nc) is a tool which we can use as client or server on tcp and udp ports because it works for both and it can listen on ports so , it is like telnet , so to listen first we need to connect so we connect like **nc 10.82.184.166 80 (i.e nc machine_ip port) ,** it is similar to telnet after that we have to use GET line to listen on the port as GET/HTTP/1.1 after that press shift + enter . when we want to listen on server side we can give command nc -vnlp 2345 to listen on port 2345 . and to listen on client-side we can give command nc machine_ip 2345 to listen on port 2345 on client-side. There are many options available on netcat like

-l	Listen mode
-p	Specify the Port number
-n	Numeric only; no resolution of hostnames via DNS
-v	Verbose output (optional, yet useful to discover any b
-vv	Very Verbose (optional)
-k	Keep listening after client disconnects

- Make sure that, the option -p should appear just before the port number you want to listen on.
- Also we need root privilages to listen on ports lets than 1024.

Lets move towards question part



- the option `-p` should appear just before the port number you want to listen on.
- the option `-n` will avoid DNS lookups and warnings.
- port numbers less than 1024 require root privileges to listen on.

On the *client*-side, you would issue `nc 10.48.158.149 PORT_NUMBER`. Here is an example of using `nc` to echo. After you successfully establish a connection to the server, whatever you type on the client-side will be echoed on the server-side and vice versa.

Consider the following example. On the server-side, we will listen on port 1234. We can achieve this with the command `nc -vnlp 1234` (same as `nc -lvnp 1234`). In our case, the listening server has the IP address `10.48.158.149`, so we can connect to it from the client-side by executing `nc 10.48.158.149 1234`. This setup would echo whatever you type on one side to the other side of the TCP tunnel. You can find a recording of the process below. Note that the listening server is on the left side of the screen.

Answer the questions below

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-10-48-149-23:~# nc 10.48.158.149 21
220 ip-10-48-158-149.ap-south-1.compute.internal FTP server (Version 6.4/OpenBSD
/Linux-ftpd-0.17) ready.
```

1) 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?
   -> so , we have to see the version of server so we give command nc machine_ip port as in above image we have given in terminal nc 10.48.158.149 21 here 21 is port number where we have to see server version so the version we can see there is 0.17 don't misunderstood version 6.4 because it is a version of ftp server not main one the o.17 is the version of linux server which is what we needed so **0.17** is correct answer .

So , as thi our last lesson we conclude here the 1st lab of Active Reconnaissance and lets move towards next Passive Reconnaissance.

• Passive Reconnaissance:

At the beginning, the lab explains what passive reconnaissance is and the tools used for it. In passive reconnaissance, we do **not directly interact with the target**. Instead of touching or contacting it, we silently observe and collect publicly available information. You can think of it like **watching a house from a distance** to understand its structure, number of people, timing patterns, etc., without actually going near the door or touching the lock. So, everything is done quietly and indirectly.

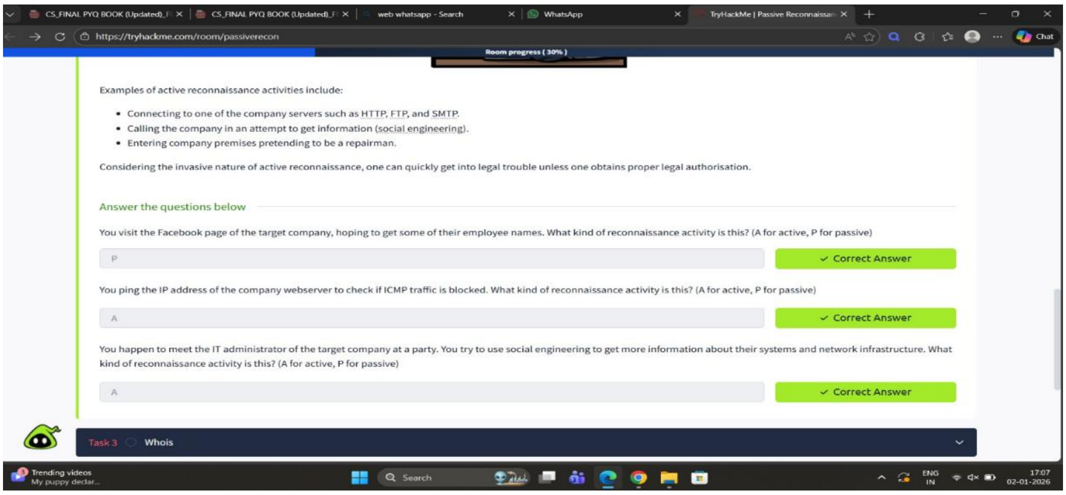
In this room, we use many tools and techniques for passive reconnaissance such as:

• **WHOIS Lookup**

• **nslookup/dig**
• **DNS Dumpster / Online DNS tools**

- **Shodan**

So, let’s dive deep into these tools to understand how they work and how they help us gather information **without alerting the target**.


CS_FINAL PYQ BOOK (Updated)_F
CS_FINAL PYQ BOOK (Updated)_F
web whatsapp - Search
WhatsApp
TryHackMe | Passive Reconnaissan
https://tryhackme.com/room/passiverecon
Chat
Room progress (30%)

Examples of active reconnaissance activities include:

- Connecting to one of the company servers such as HTTP, FTP, and SMTP.
- Calling the company in an attempt to get information (social engineering).
- Entering company premises pretending to be a repairman.

Considering the invasive nature of active reconnaissance, one can quickly get into legal trouble unless one obtains proper legal authorisation.

Answer the questions below

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 Whois

1) 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)

-> so the correct answer is P (Passive) because we are not directly contacting just getting information which is already present .

2) 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)

-> so the correct answer is A (Active) because we are pinging i.e aking contact with server which is active reconnaissance.

3) 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)

-> so the correct answer is A (Active) because we are making contact with peoples which also a part of active reconnaissance.

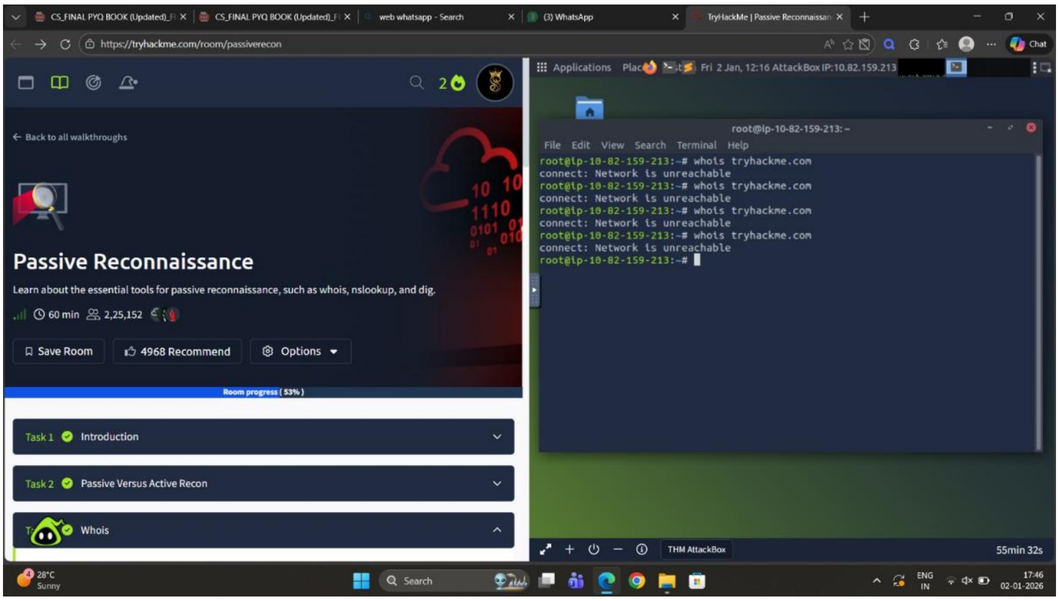
1) Whois :-

_It is a request and response protocol which works on tcp port 43 , it listens for incoming requests on that port it replies with various information related to the domain requested. such as

- Registrar: Via which registrar was the domain name registered?
- Contact info of registrant: Name, organization, address, phone, among other things. (unless made hidden via a privacy service)
- Creation, update, and expiration dates: When was the domain name first registered? When was it last updated? And when does it need to be renewed?

- Name Server: Which server to ask to resolve the domain name?

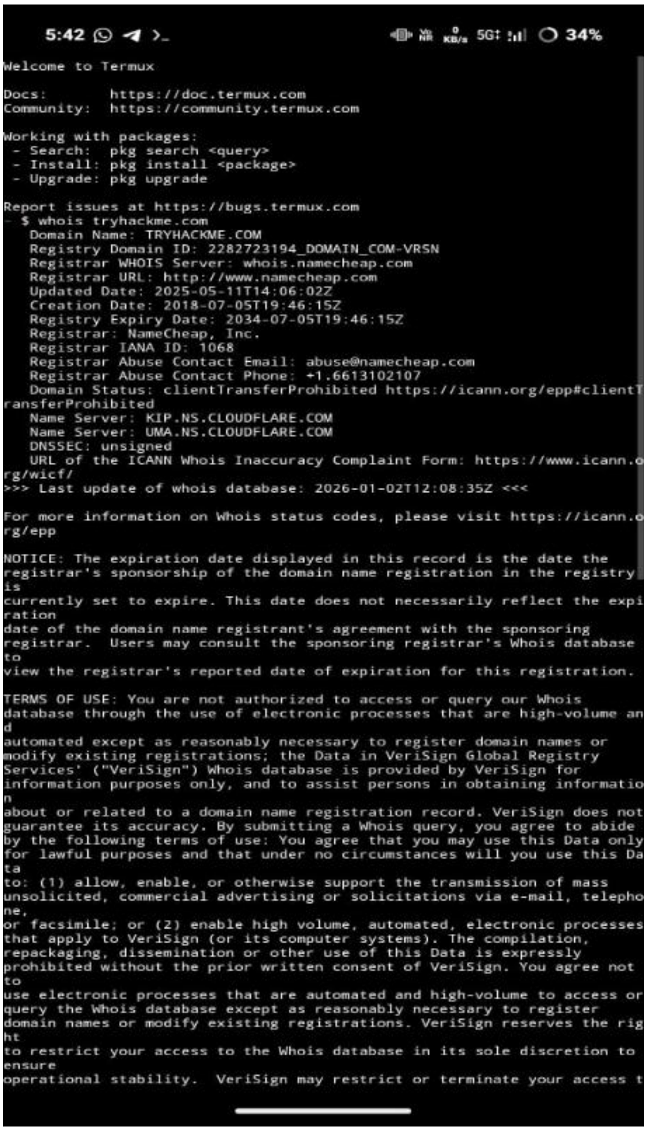
To get details of domain we just type **whois domain_name** and we will get above details .
lets go for the question of this lesson for better understanding:-



https://tryhackme.com/room/passiverecon
Back to all walkthroughs
Passive Reconnaissance
Learn about the essential tools for passive reconnaissance, such as whois, nslookup, and dig.
60 min
2,25,152
Save Room
4968 Recommend
Options
Room progress (53%)
Task 1 Introduction
Task 2 Passive Versus Active Recon
Whois
Applications
Fri 2 Jan, 12:16 AttackBox IP:10.82.159.213
root@ip-10-82-159-213: ~
File Edit View Search Terminal Help
THM AttackBox
55min 32s

```
root@ip-10-82-159-213:~# whois tryhackme.com
connect: Network is unreachable
root@ip-10-82-159-213:~# whois tryhackme.com
connect: Network is unreachable
root@ip-10-82-159-213:~# whois tryhackme.com
connect: Network is unreachable
root@ip-10-82-159-213:~# whois tryhackme.com
connect: Network is unreachable
root@ip-10-82-159-213:~# 
```

So I tried on the attackbox but it shows unreachable everytime I guess because it is not connected to internet as I don’t have premium so , for this specific task I moved to my termux on my smartphone , I am sharing image of the result I get



```
Welcome to Termux

Docs:       https://doc.termux.com
Community:  https://community.termux.com

Working with packages:
 - Search:  pkg search <query>
 - Install: pkg install <package>
 - Upgrade: pkg upgrade

Report issues at https://bugs.termux.com
~ $ 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: 2025-05-11T14:06:02Z
   Creation Date: 2018-07-05T19:46:15Z
   Registry Expiry Date: 2034-07-05T19:46:15Z
   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#clientT
ransferProhibited
   Name Server: KIP.NS.CLOUDFLARE.COM
   Name Server: UMA.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.o
rg/wicf/
>>> Last update of whois database: 2026-01-02T12:08:35Z <<<

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

NOTICE: 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 expi
ration
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 an
d
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 informatio
n
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Da
ta
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telepho
ne,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not
to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the rig
ht
to restrict your access to the Whois database in its sole discretion to
ensure
operational stability.  VeriSign may restrict or terminate your access t
```

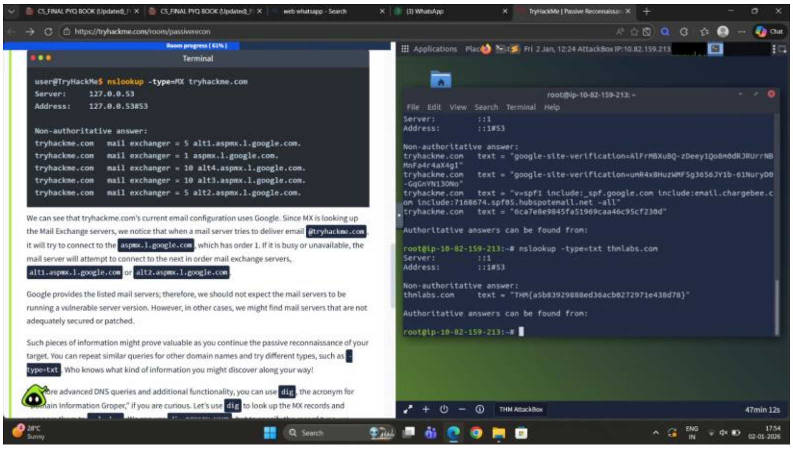
1) When was TryHackMe.com registered?
   -> so in above image we can see the creation date as 2018-07-05 so it is the answer for the question (note:- type answer a yyyymmdd)
2) What is the registrar of TryHackMe.com?
   -> so , we can see the registrar as Namecheap so the correct answer is namecheap.com
3) Which company is TryHackMe.com using for name servers?
   -> we can see name server there so they are using cloudflare.com as name server

2)<u>Nslookup/dig :-</u>

So , by using nslookuo and dig we can find the ip adresses of dns servers and also we can see different files like txt or mx files there are many options available to see such as

A	IPv4 Addresses
AAAA	IPv6 Addresses
CNAME	Canonical Name
MX	Mail Servers
SOA	Start of Authority
TXT	TXT Records

For ex:- nslookup type=A domain_name it gives ipv4 address ans if we use type = AAAA it gives ipv6 adress , txt gives Txt records ,etc.
same as nslookup , dig also give same thing but dig is more detailed tham nslookup and gives more info



```
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.
```

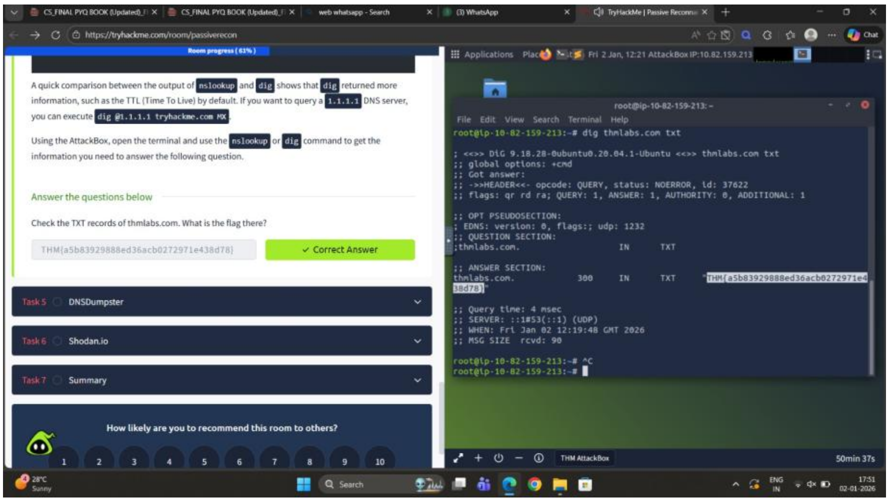
We can see that tryhackme.com's current email configuration uses Google. Since MX is looking up the Mail Exchange servers, we notice that when a mail server tries to deliver email `@tryhackme.com`, it will try to connect to the `aspmx.l.google.com`, which has order 1. If it is busy or unavailable, the mail server will attempt to connect to the next in order mail exchange servers, `alt1.aspmx.l.google.com` or `alt2.aspmx.l.google.com`.

Google provides the listed mail servers; therefore, we should not expect the mail servers to be running a vulnerable server version. However, in other cases, we might find mail servers that are not adequately secured or patched.

Such pieces of information might prove valuable as you continue the passive reconnaissance of your target. You can repeat similar queries for other domain names and try different types, such as `-type=txt`. Who knows what kind of information you might discover along your way!

re advanced DNS queries and additional functionality, you can use `dig`, the acronym for ain Information Groper," if you are curious. Let's use `dig` to look up the MX records and

```
Server:         ::1
Address:        ::1#53

Non-authoritative answer:
tryhackme.com   text = "google-site-verification=AlFrMBXuBQ-zDeey1Qo8m0dRJRUrrNB
MnFa4r4aX4gI"
tryhackme.com   text = "google-site-verification=umR4x8HuzWMF5g3656JY1b-61NuryD0
-GqGnYN13ONo"
tryhackme.com   text = "v=spf1 include:_spf.google.com include:email.chargebee.c
om include:7168674.spf05.hubspotemail.net -all"
tryhackme.com   text = "6ca7e8e9845fa51969caa46c95cf230d"

Authoritative answers can be found from:

root@ip-10-82-159-213:~# nslookup -type=txt thmlabs.com
Server:         ::1
Address:        ::1#53

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

Authoritative answers can be found from:

root@ip-10-82-159-213:~# 
```



A quick comparison between the output of `nslookup` and `dig` shows that `dig` returned more information, such as the TTL (Time To Live) by default. If you want to query a `1.1.1.1` DNS server, you can execute `dig @1.1.1.1 tryhackme.com MX`.

Using the AttackBox, open the terminal and use the `nslookup` or `dig` command to get the information you need to answer the following question.

Answer the questions below

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

THM{a5b83929888ed36acb0272971e438d78}   ✓ Correct Answer

How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9 10

```
root@ip-10-82-159-213:~# dig thmlabs.com txt

; <<>> DiG 9.18.28-0ubuntu0.20.04.1-Ubuntu <<>> thmlabs.com txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37622
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;thmlabs.com.                   IN      TXT

;; ANSWER SECTION:
thmlabs.com.            300     IN      TXT     "THM{a5b83929888ed36acb0272971e4
38d78}"

;; Query time: 4 msec
;; SERVER: ::1#53(::1) (UDP)
;; WHEN: Fri Jan 02 12:19:48 GMT 2026
;; MSG SIZE  rcvd: 90

root@ip-10-82-159-213:~# ^C
root@ip-10-82-159-213:~# 
```

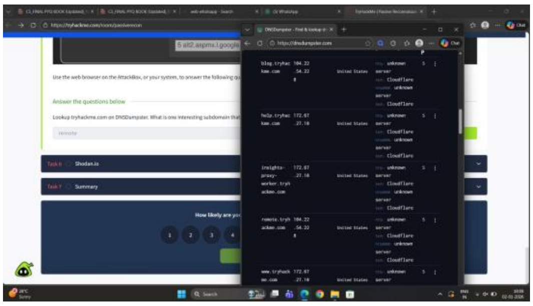
Check the TXT records of thmlabs.com. What is the flag there?
-> THM{a5b83929888ed36acb0272971e438d78}

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

->United States

Based on Shodan.io, what is the 3rd most common port used for Apache?
->8080

Based on Shodan.io, what is the 3rd most common port used for nginx?
-> 888



Use the web browser on the AttackBox, or your system, to answer the following qu

Answer the questions below

Lookup tryhackme.com on DNSDumpster. What is one interesting subdomain that

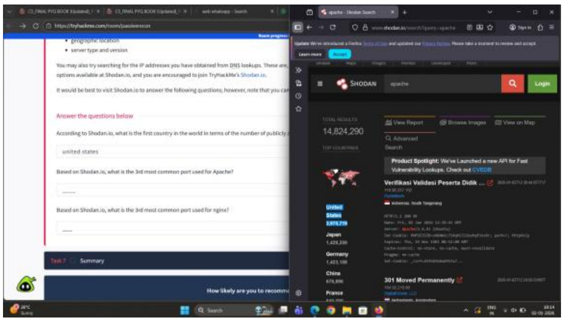
remote

Task 6 Shodan.io

Task 7 Summary

How likely are yo

```
blog.tryhac  104.22          United States  unknown    5
kme.com      .54.22                         server
             8                              Cloudflare
                                            unknown
                                            server
                                            Cloudflare
help.tryhac  172.67          United States  unknown    5
kme.com      .27.10                         server
                                            Cloudflare
                                            unknown
                                            server
                                            Cloudflare
insights-    172.67          United States  unknown    5
proxy-       .27.10                         server
worker.tryh                                 Cloudflare
ackme.com                                   unknown
                                            server
                                            Cloudflare
remote.tryh  104.22          United States  unknown    5
ackme.com    .54.22                         server
             8                              Cloudflare
                                            unknown
                                            server
                                            Cloudflare
www.tryhack  172.67          United States  unknown    5
me.com       .27.10                         server
```



- geographic location
- server type and version

You may also try searching for the IP addresses you have obtained from DNS lookups. These are, options available at Shodan.io, and you are encouraged to join TryHackMe's Shodan.io.

It would be best to visit Shodan.io to answer the following questions; however, note that you ca

Answer the questions below

According to Shodan.io, what is the first country in the world in terms of the number of publicly

united states

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

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

Task 7 Summary

How likely are you to recomm

SHODAN apache

TOTAL RESULTS 14,824,290

TOP COUNTRIES

United States

Japan 1,423,2[illegible]

Germany 1,423,1[illegible]

China 676,896

France

View Report Browse Images View on Map

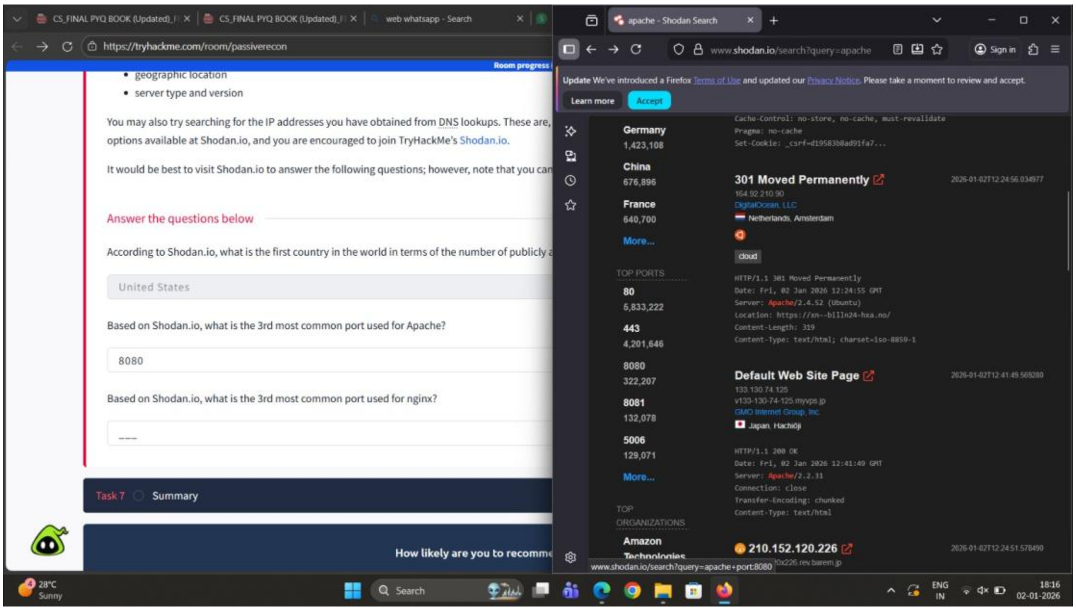
Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

Verifikasi Validasi Peserta Didik ...

Indonesia, South Tangerang

301 Moved Permanently



CS_FINAL PYQ BOOK (Updated)_!
CS_FINAL PYQ BOOK (Updated)_!
web whatsapp - Search
https://tryhackme.com/room/passiverecon
Room progress
apache - Shodan Search
www.shodan.io/search?query=apache
Sign in

- geographic location
- server type and version

You may also try searching for the IP addresses you have obtained from DNS lookups. These are, options available at Shodan.io, and you are encouraged to join TryHackMe's Shodan.io.

It would be best to visit Shodan.io to answer the following questions; however, note that you car

Answer the questions below

According to Shodan.io, what is the first country in the world in terms of the number of publicly a

United States

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

8080

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

Task 7 Summary

How likely are you to recomme

Update We've introduced a Firefox Terms of Use and updated our Privacy Notice. Please take a moment to review and accept.

Learn more Accept

Germany
1,423,108

China
676,896

France
640,700

More...

TOP PORTS

80
5,833,222

443
4,201,646

8080
322,207

8081
132,078

5006
129,071

More...

TOP ORGANIZATIONS

Amazon Technologies

```
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: _csrf=d19583b8ad91fa7...
```

301 Moved Permanently 2026-01-02T12:24:56.034977

164.92.210.90
DigitalOcean, LLC
Netherlands, Amsterdam

cloud

```
HTTP/1.1 301 Moved Permanently
Date: Fri, 02 Jan 2026 12:24:55 GMT
Server: Apache/2.4.52 (Ubuntu)
Location: https://xn--b11n24-hxa.no/
Content-Length: 319
Content-Type: text/html; charset=iso-8859-1
```

Default Web Site Page 2026-01-02T12:41:49.569280

133.130.74.125
v133-130-74-125.myvps.jp
GMO Internet Group, Inc.
Japan, Hachiōji

```
HTTP/1.1 200 OK
Date: Fri, 02 Jan 2026 12:41:49 GMT
Server: Apache/2.2.31
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html
```

210.152.120.226 2026-01-02T12:24:51.578490

www.shodan.io/search?query=apache+port:8080