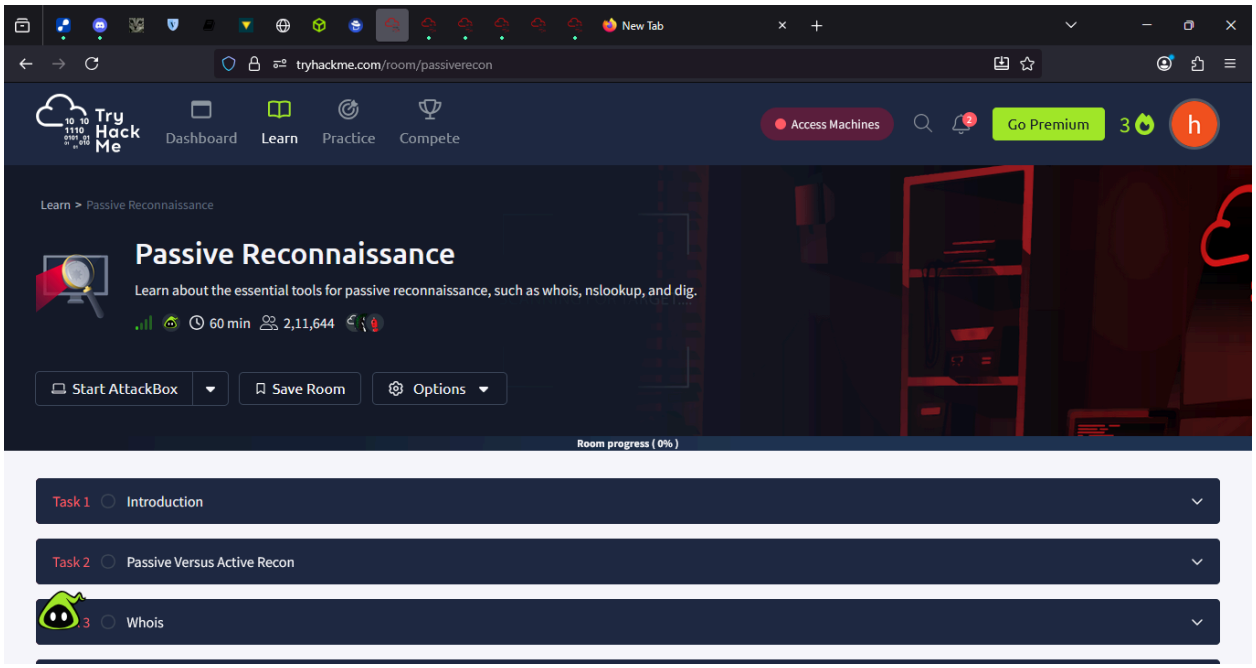
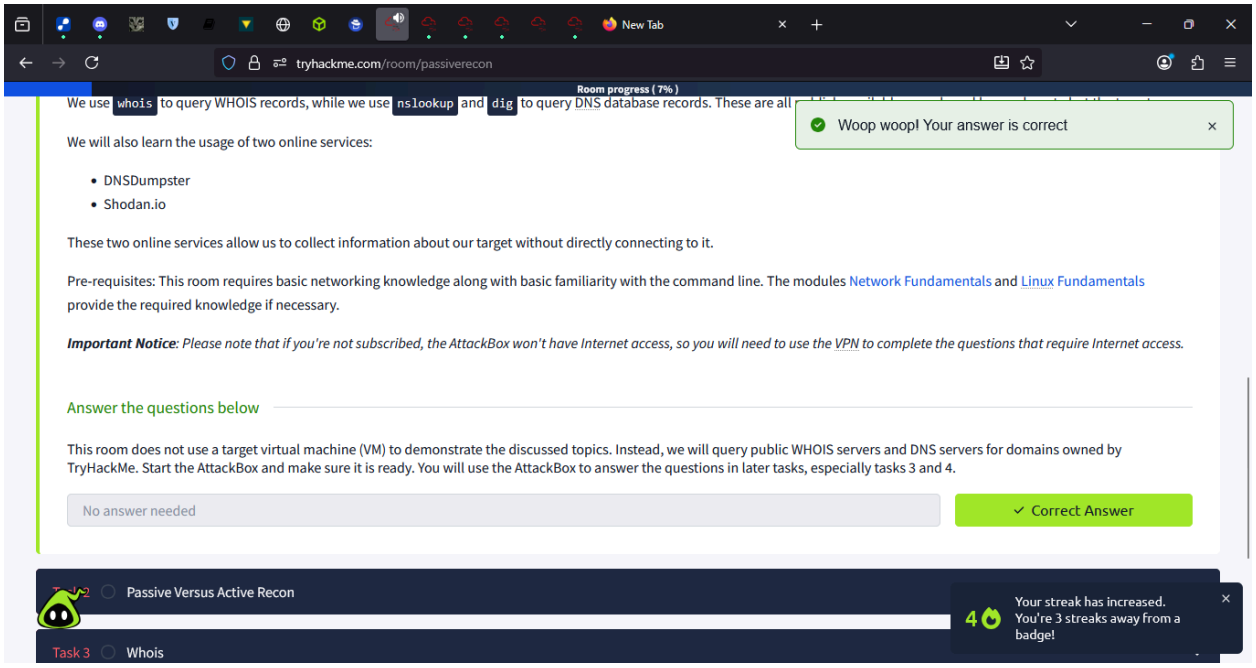
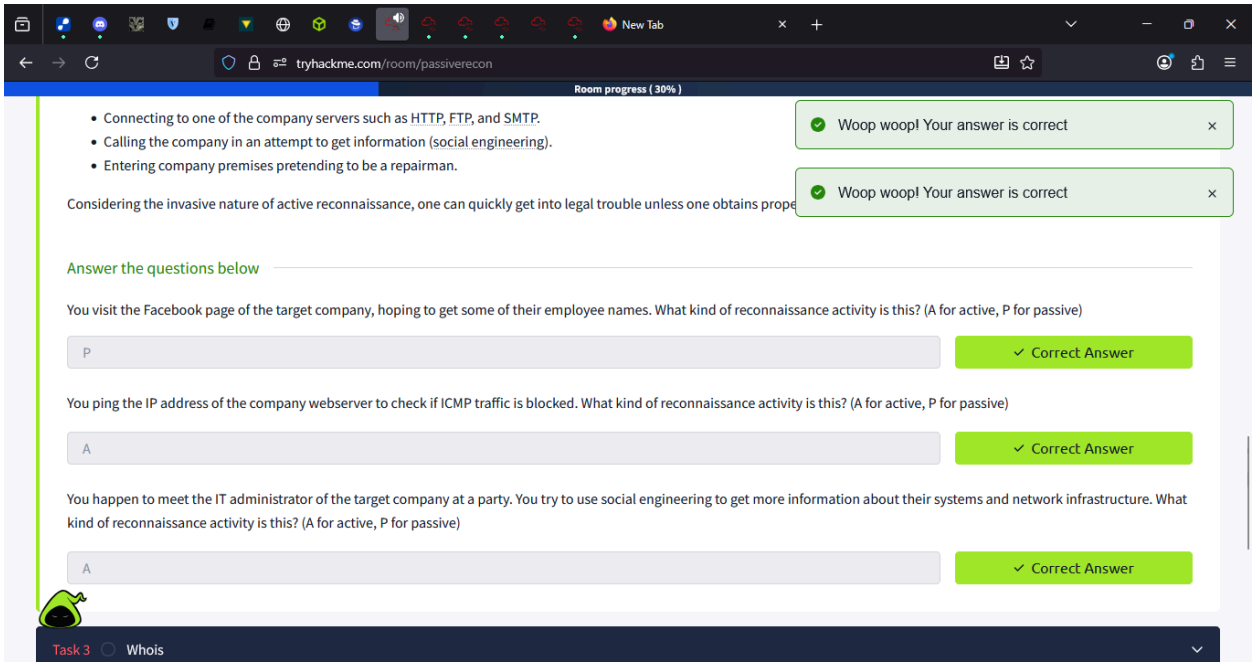
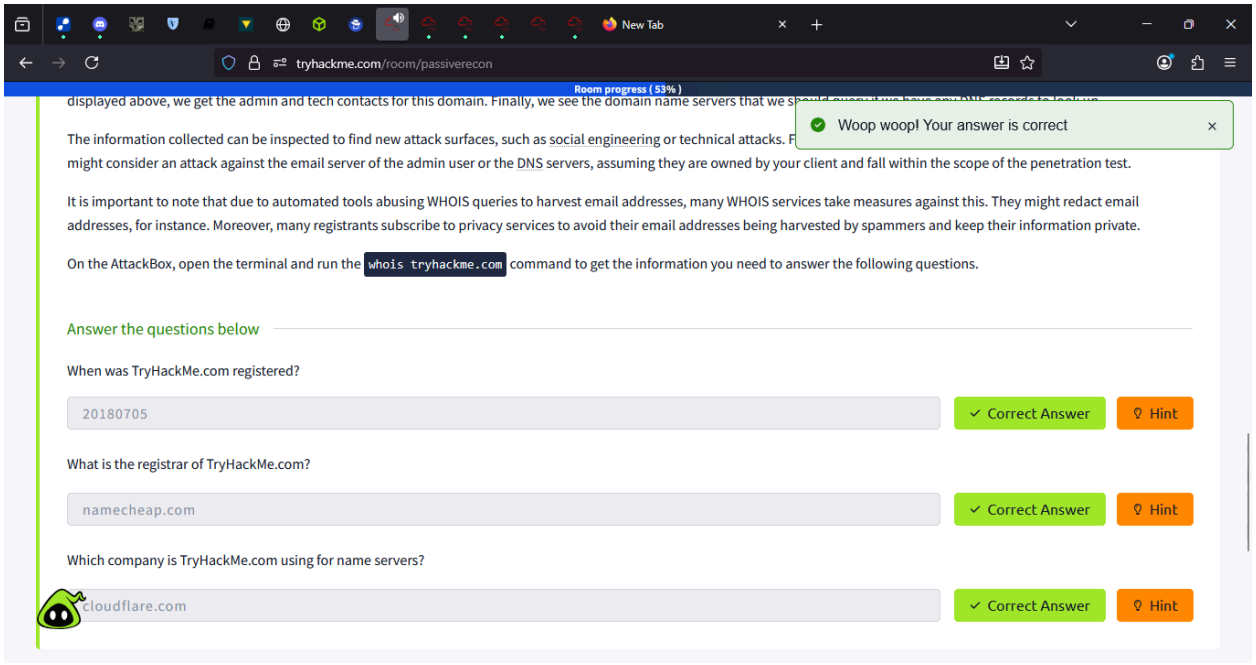
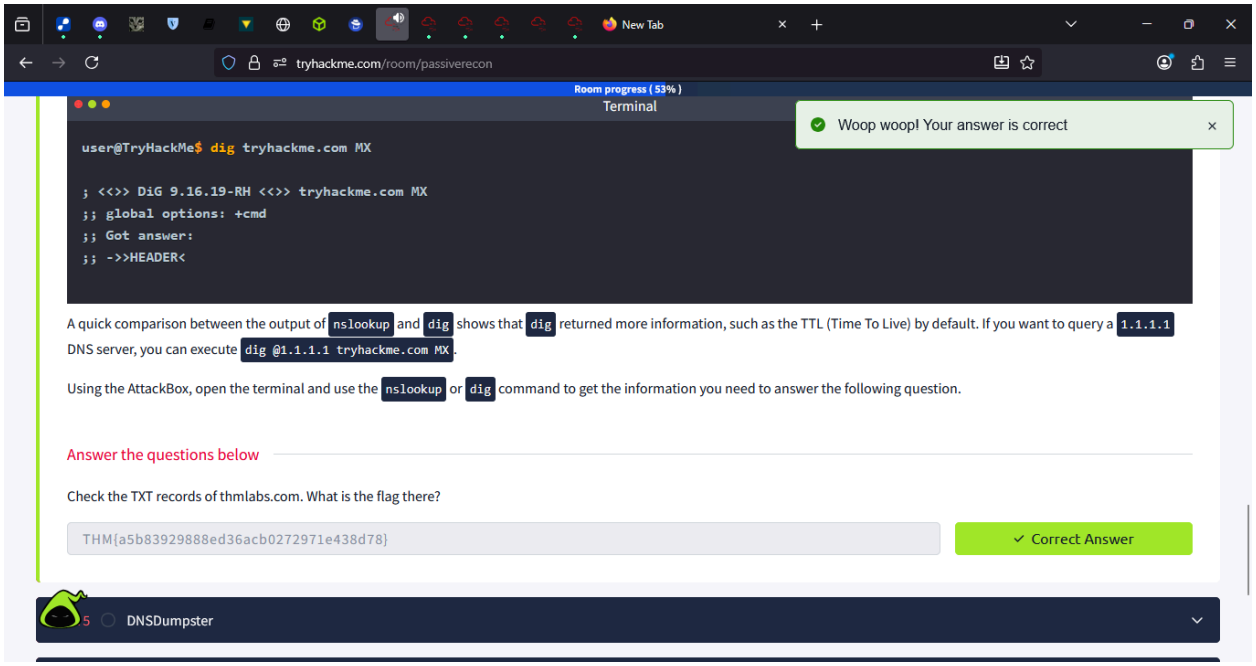
Passive Reconnaissance

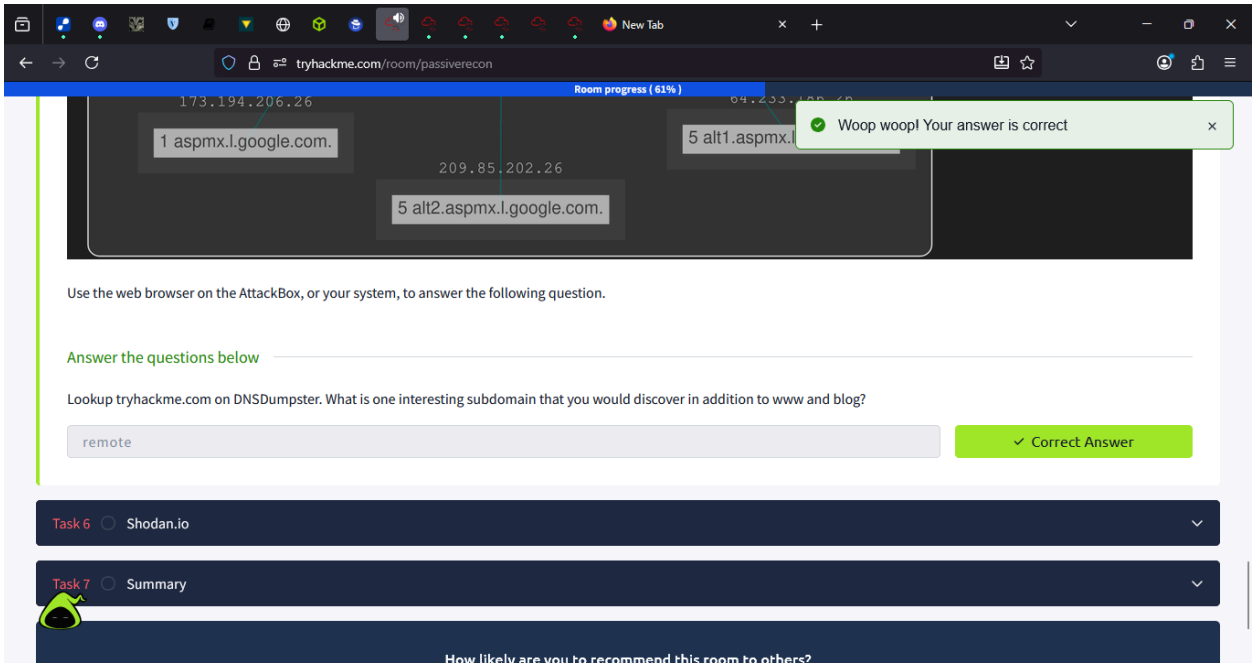


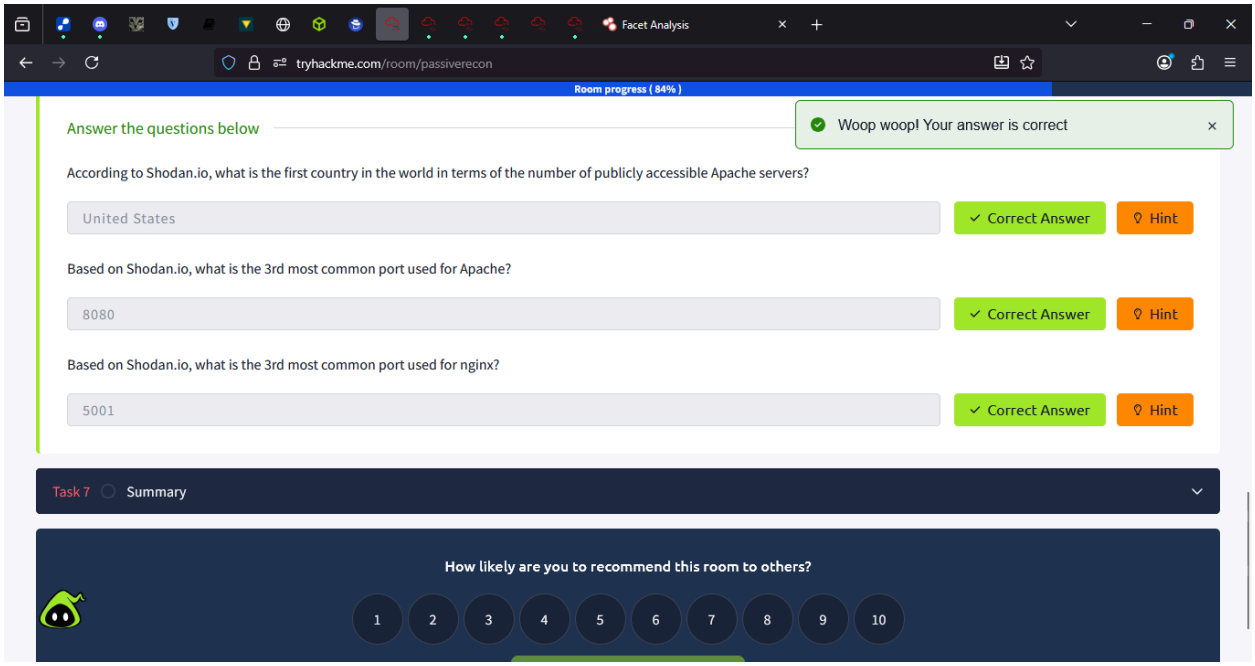


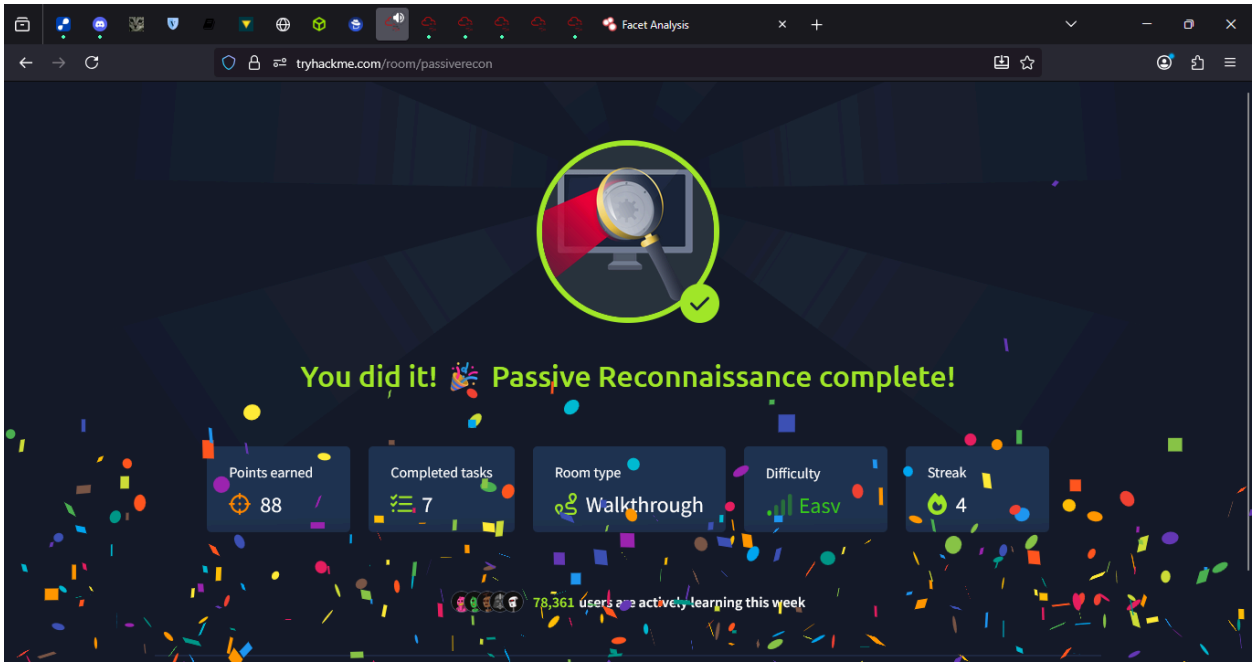

New Tab
tryhackme.com/room/passiverecon
Room progress (30%)
Woop woop! Your answer is correct
Woop woop! Your answer is correct
• Connecting to one of the company servers such as HTTP, FTP, and SMTP.
• Calling the company in an attempt to get information (social engineering).
• Entering company premises pretending to be a repairman.
Considering the invasive nature of active reconnaissance, one can quickly get into legal trouble unless one obtains prope
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

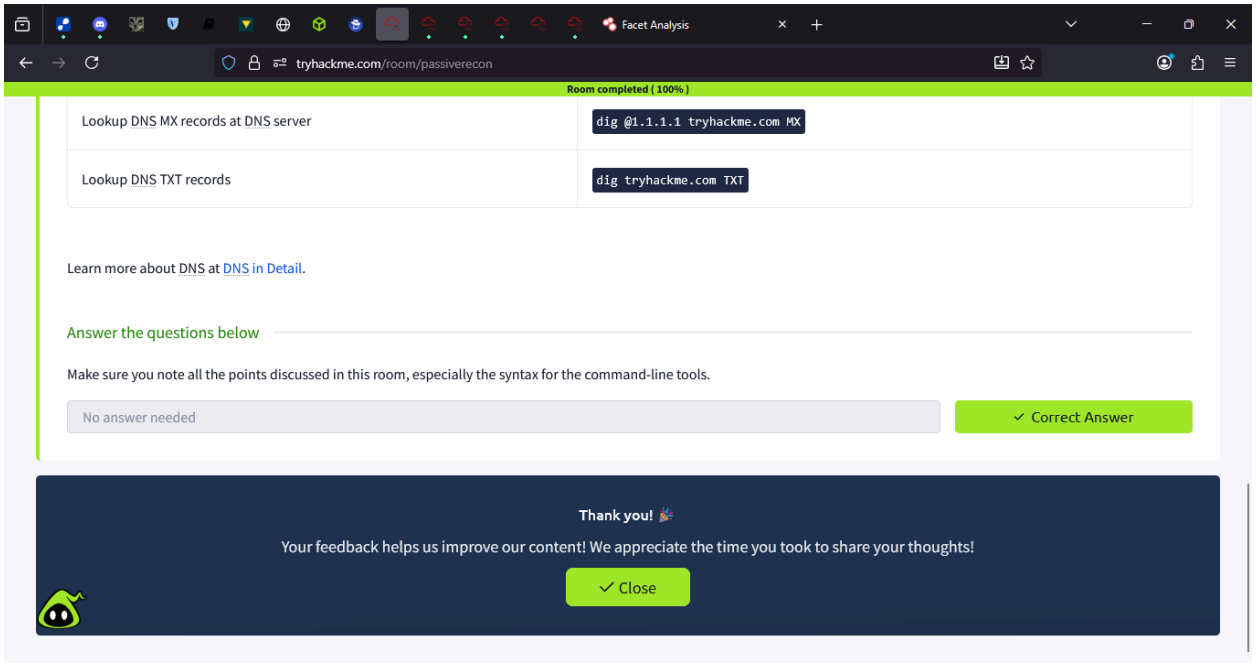

New Tab
tryhackme.com/room/passiverecon
Room progress (53%)
Woop woop! Your answer is correct
displayed above, we get the admin and tech contacts for this domain. Finally, we see the domain name servers that we
The information collected can be inspected to find new attack surfaces, such as social engineering or technical attacks. F
might consider an attack against the email server of the admin user or the DNS servers, assuming they are owned by your client and fall within the scope of the penetration test.
It is important to note that due to automated tools abusing WHOIS queries to harvest email addresses, many WHOIS services take measures against this. They might redact email addresses, for instance. Moreover, many registrants subscribe to privacy services to avoid their email addresses being harvested by spammers and keep their information private.
On the AttackBox, open the terminal and run the whois tryhackme.com command to get the information you need to answer the following questions.
Answer the questions below
When was TryHackMe.com registered?
20180705
✓ Correct Answer
Hint
What is the registrar of TryHackMe.com?
namecheap.com
✓ Correct Answer
Hint
Which company is TryHackMe.com using for name servers?
cloudflare.com
✓ Correct Answer
Hint


New Tab
tryhackme.com/room/passiverecon
Room progress (53%)
Terminal
Woop woop! Your answer is correct
user@TryHackMe$ dig tryhackme.com MX
; <<>> DiG 9.16.19-RH <<>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<
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
DNSDumpster


New Tab
tryhackme.com/room/passiverecon
Room progress (61%)
173.194.206.26
1 aspmx.l.google.com.
209.85.202.26
5 alt2.aspmx.l.google.com.
Woop woop! Your answer is correct
Use the web browser on the AttackBox, or your system, to answer the following question.
Answer the questions below
Lookup tryhackme.com on DNSDumpster. What is one interesting subdomain that you would discover in addition to www and blog?
remote
Correct Answer
Task 6 Shodan.io
Task 7 Summary
How likely are you to recommend this room to others?


Facet Analysis
tryhackme.com/room/passiverecon
Room progress (84%)
Answer the questions below
Woop woop! Your answer is correct
According to Shodan.io, what is the first country in the world in terms of the number of publicly accessible Apache servers?
United States
Correct Answer
Hint
Based on Shodan.io, what is the 3rd most common port used for Apache?
8080
Correct Answer
Hint
Based on Shodan.io, what is the 3rd most common port used for nginx?
5001
Correct Answer
Hint
Task 7
Summary
How likely are you to recommend this room to others?
1
2
3
4
5
6
7
8
9
10


Facet Analysis
tryhackme.com/room/passiverecon
You did it! Passive Reconnaissance complete!
Points earned
88
Completed tasks
7
Room type
Walkthrough
Difficulty
Easy
Streak
4
78,361 users are actively learning this week


Facet Analysis
tryhackme.com/room/passiverecon
Room completed (100%)
Lookup DNS MX records at DNS server
dig @1.1.1.1 tryhackme.com MX
Lookup DNS TXT records
dig tryhackme.com TXT
Learn more about DNS at DNS in Detail.
Answer the questions below
Make sure you note all the points discussed in this room, especially the syntax for the command-line tools.
No answer needed
✓ Correct Answer
Thank you!
Your feedback helps us improve our content! We appreciate the time you took to share your thoughts!
✓ Close