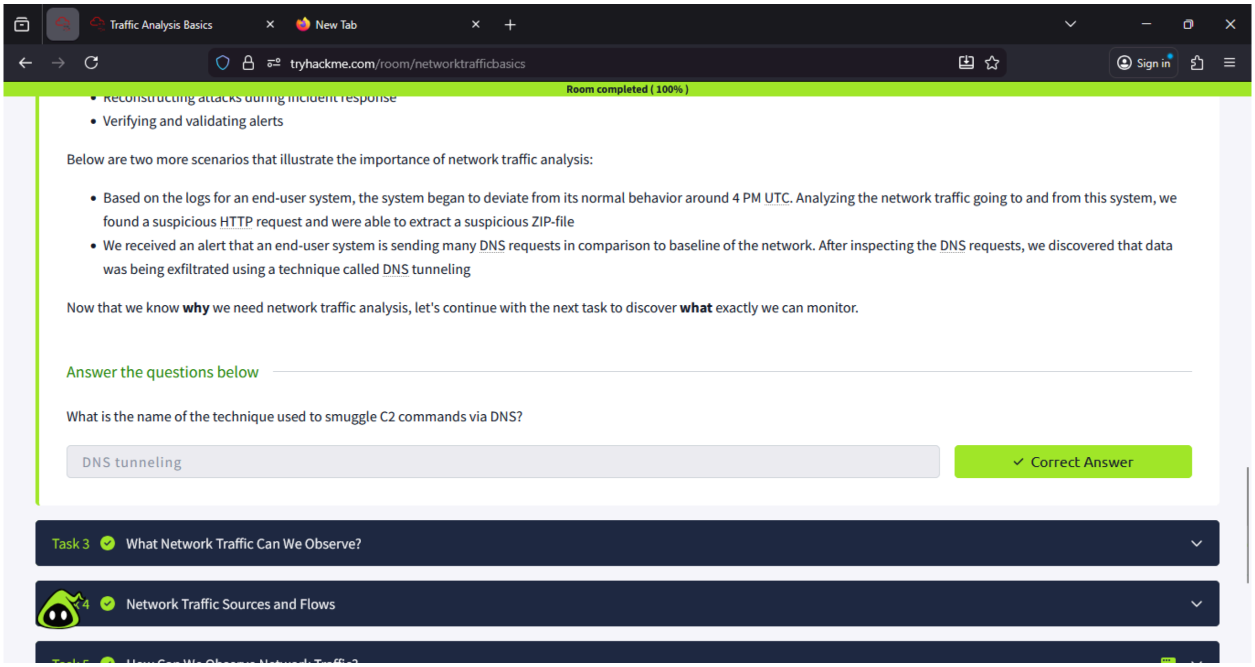
Network Traffic Basics



- Reconstructing attacks during incident response
- Verifying and validating alerts

Below are two more scenarios that illustrate the importance of network traffic analysis:

- Based on the logs for an end-user system, the system began to deviate from its normal behavior around 4 PM UTC. Analyzing the network traffic going to and from this system, we found a suspicious HTTP request and were able to extract a suspicious ZIP-file
- We received an alert that an end-user system is sending many DNS requests in comparison to baseline of the network. After inspecting the DNS requests, we discovered that data was being exfiltrated using a technique called DNS tunneling

Now that we know **why** we need network traffic analysis, let's continue with the next task to discover **what** exactly we can monitor.

Answer the questions below

What is the name of the technique used to smuggle C2 commands via DNS?

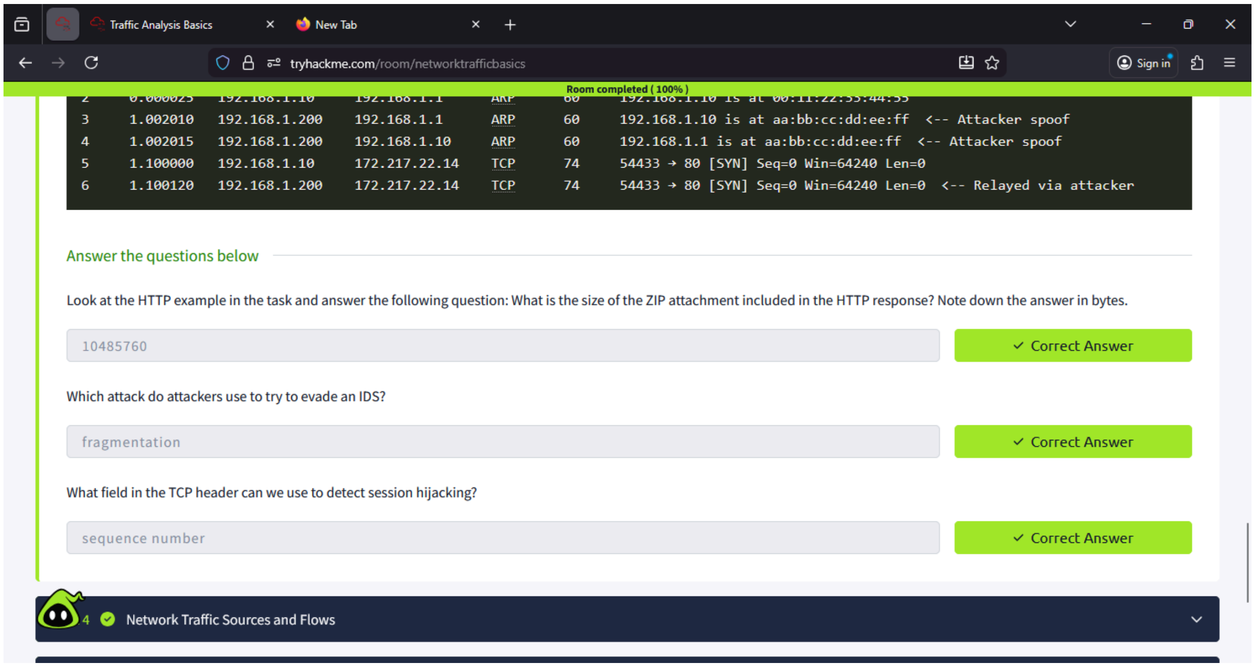
DNS tunneling

✓ Correct Answer

Task 3 ✓ What Network Traffic Can We Observe?

4 ✓ Network Traffic Sources and Flows

Task 5 ✓ How Can We Observe Network Traffic?



```
2    0.000025   192.168.1.10    192.168.1.1     ARP    60    192.168.1.10 is at 00:11:22:33:44:55
3    1.002010   192.168.1.200   192.168.1.1     ARP    60    192.168.1.10 is at aa:bb:cc:dd:ee:ff  <-- Attacker spoof
4    1.002015   192.168.1.200   192.168.1.10    ARP    60    192.168.1.1 is at aa:bb:cc:dd:ee:ff  <-- Attacker spoof
5    1.100000   192.168.1.10    172.217.22.14   TCP    74    54433 → 80 [SYN] Seq=0 Win=64240 Len=0
6    1.100120   192.168.1.200   172.217.22.14   TCP    74    54433 → 80 [SYN] Seq=0 Win=64240 Len=0  <-- Relayed via attacker
```

Answer the questions below

Look at the HTTP example in the task and answer the following question: What is the size of the ZIP attachment included in the HTTP response? Note down the answer in bytes.

10485760

✓ Correct Answer

Which attack do attackers use to try to evade an IDS?

fragmentation

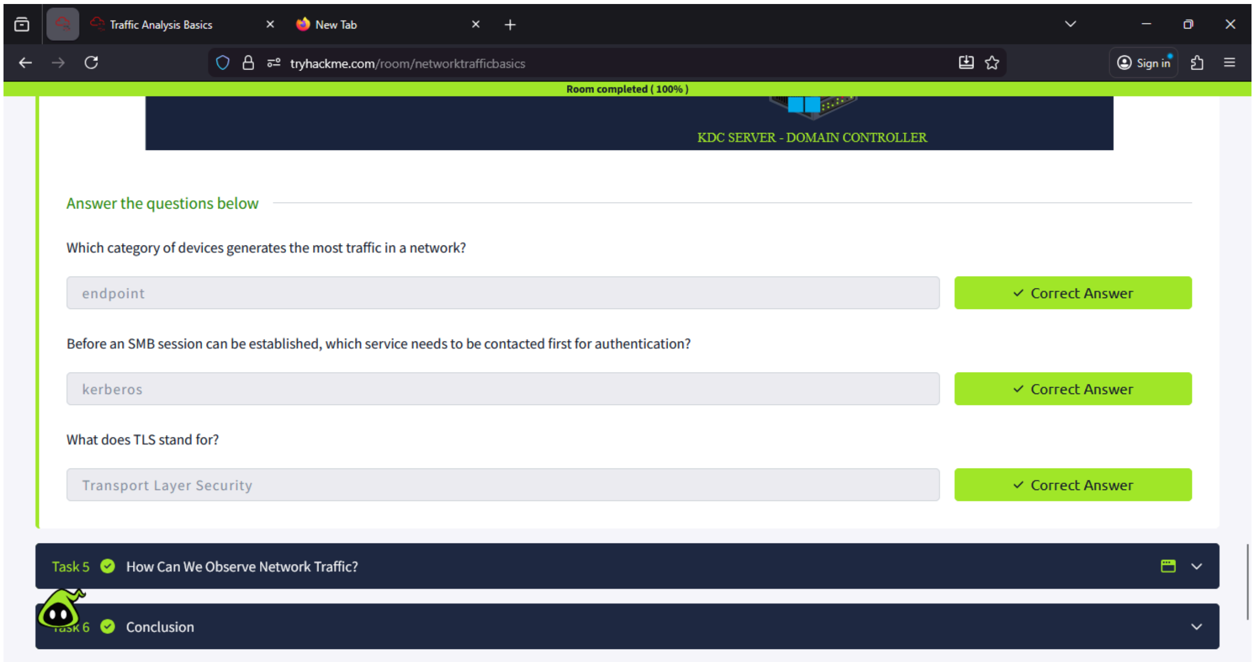
✓ Correct Answer

What field in the TCP header can we use to detect session hijacking?

sequence number

✓ Correct Answer

4 ✓ Network Traffic Sources and Flows



Traffic Analysis Basics
New Tab
tryhackme.com/room/networktrafficbasics
Sign in
Room completed (100%)
KDC SERVER - DOMAIN CONTROLLER

Answer the questions below

Which category of devices generates the most traffic in a network?

endpoint

✓ Correct Answer

Before an SMB session can be established, which service needs to be contacted first for authentication?

kerberos

✓ Correct Answer

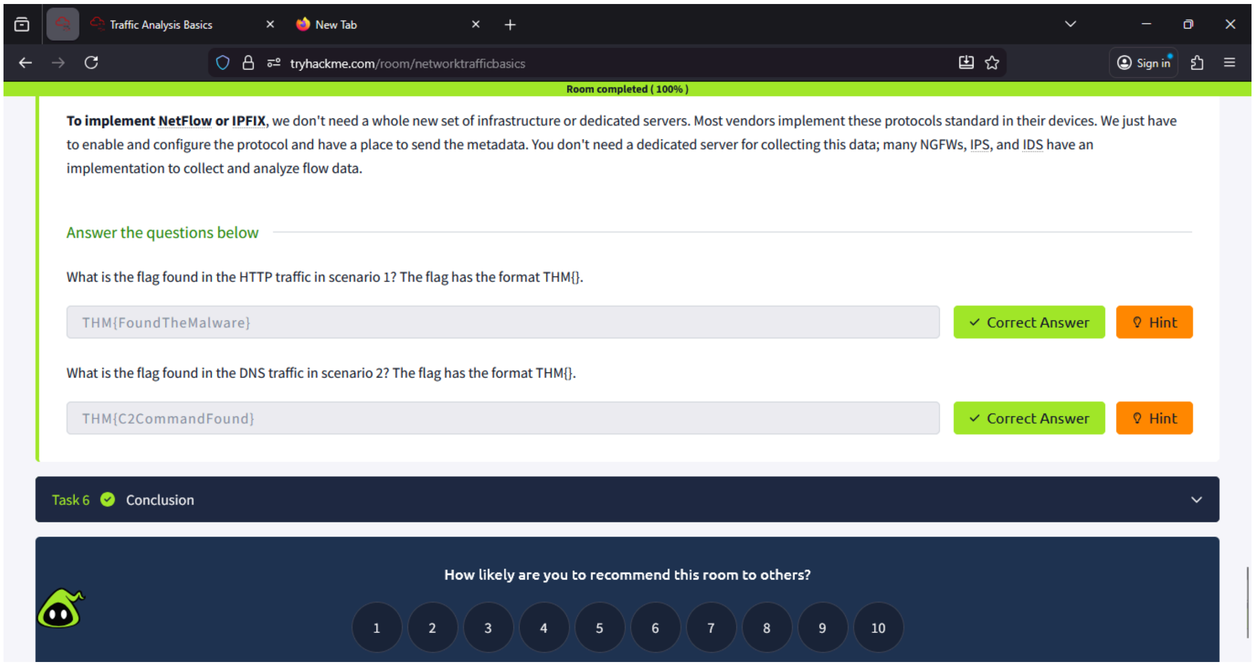
What does TLS stand for?

Transport Layer Security

✓ Correct Answer

Task 5 How Can We Observe Network Traffic?

Task 6 Conclusion



To implement NetFlow or IPFIX, we don't need a whole new set of infrastructure or dedicated servers. Most vendors implement these protocols standard in their devices. We just have to enable and configure the protocol and have a place to send the metadata. You don't need a dedicated server for collecting this data; many NGFWs, IPS, and IDS have an implementation to collect and analyze flow data.

Answer the questions below

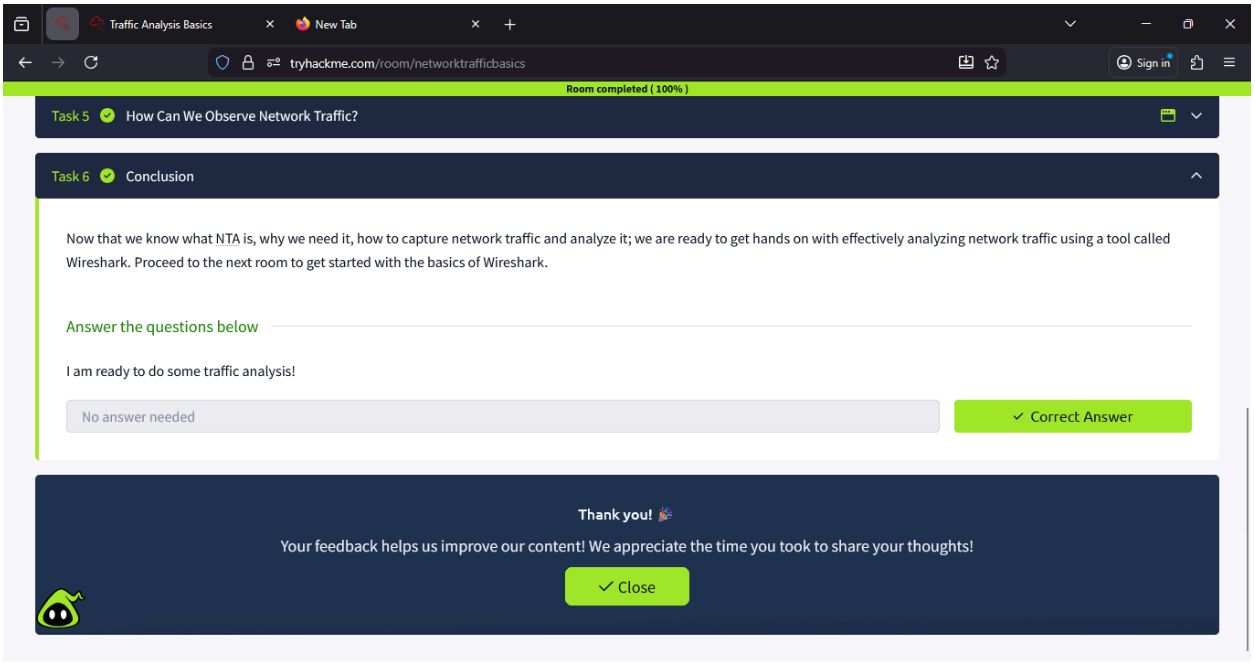
What is the flag found in the HTTP traffic in scenario 1? The flag has the format THM{}.

THM{FoundTheMalware}

What is the flag found in the DNS traffic in scenario 2? The flag has the format THM{}.

THM{C2CommandFound}

How likely are you to recommend this room to others?



Now that we know what NTA is, why we need it, how to capture network traffic and analyze it; we are ready to get hands on with effectively analyzing network traffic using a tool called Wireshark. Proceed to the next room to get started with the basics of Wireshark.

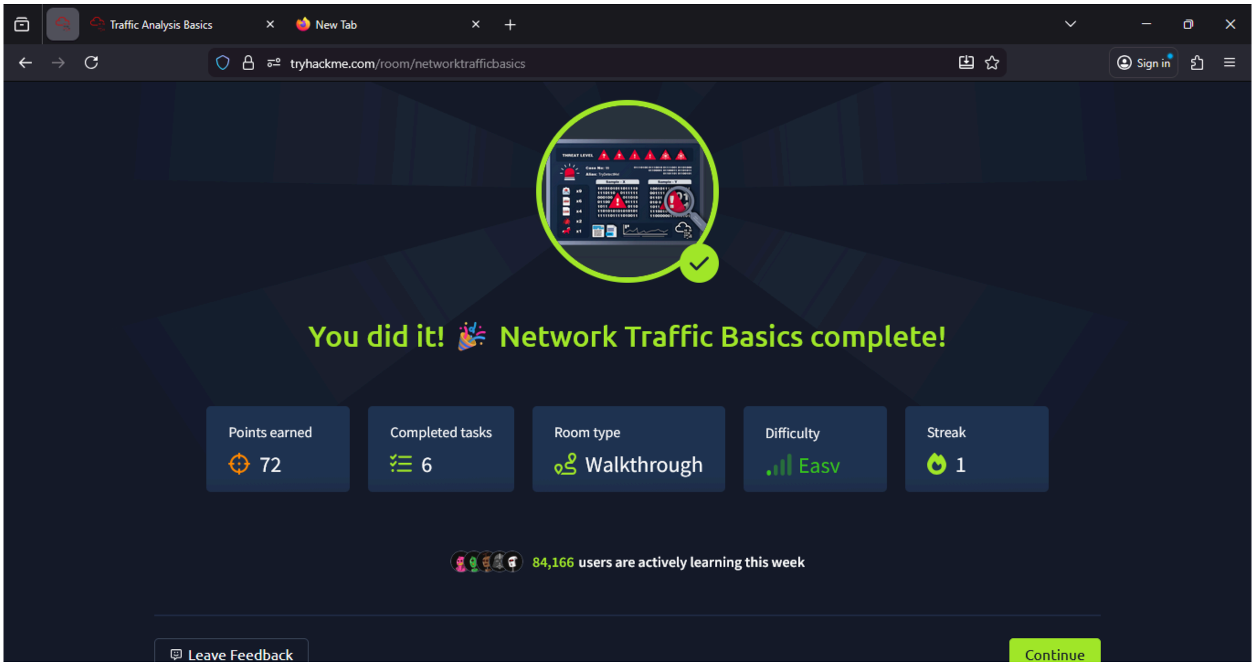
Answer the questions below

I am ready to do some traffic analysis!

No answer needed

Thank you! 🎉

Your feedback helps us improve our content! We appreciate the time you took to share your thoughts!



You did it! 🎉 Network Traffic Basics complete!

Points earned	Completed tasks	Room type	Difficulty	Streak
72	6	Walkthrough	Easy	1

84,166 users are actively learning this week