TryHackMe | OSI Model Room Writeup

Luc1f3r · Follow

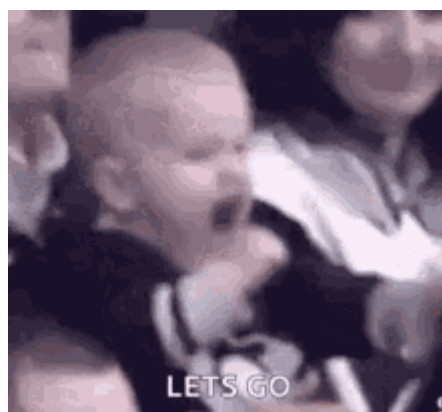10 min read · Oct 20, 2022

(▶) Listen   (⬆) Share   (•••) More

Hello Everyone,

This is the first blog I am writing and I am so excited.

This blog is a write-up on the room — OSI Model in the TryHackMe Platform. For those who are reading this, I think there is no need to tell what TryHackMe is. They are one of the best cyber security trainers who have 500+ rooms which teach us about different aspects of Cyber Security in a practical way.

Now about the OSI Model room, this room focus on a very specific part of the modern networking concept. This room explicitly covers the OSI Model that is followed in the transfer of data in a network. This is a subscriber-only room. I hope this blog helps you to gain more knowledge in this area.
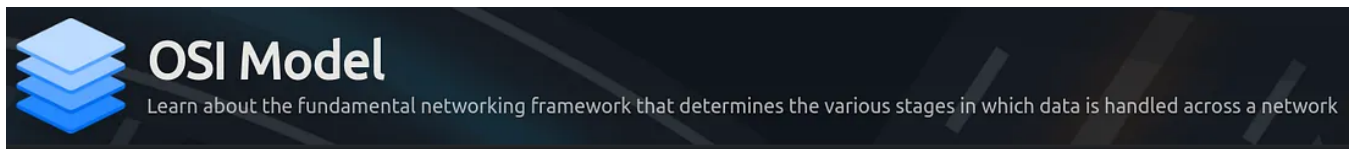
Task 1: What is OSI Model?

The **OSI** model (or **O**pen **S**ystems **I**nterconnection Model) is an absolute fundamental model used in networking. This critical model provides a framework dictating how all networked devices will send, receive and interpret data.

One of the main benefits of the OSI model is that devices can have different functions and designs on a network while communicating with other devices. Data sent across a network that follows the uniformity of the OSI model can be understood by other devices.

The OSI model consists of seven layers which are illustrated in the diagram below. Each layer has a different set of responsibilities and is arranged from Layer 7 to Layer 1.

At every individual layer that data travels through, specific processes take place, and pieces of information are added to this data, which is what we'll come to discuss in the upcoming tasks within this room. However, for now, we only need to understand that this process is called encapsulation and what the OSI model looks like in the diagram below:
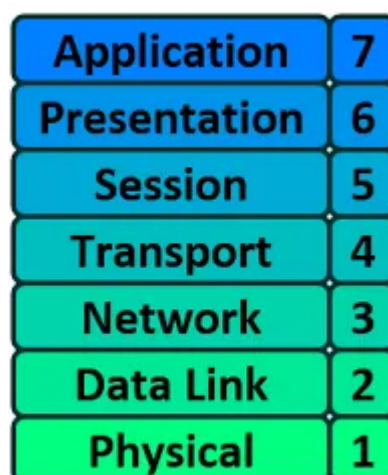
This is a very important concept in Networking Concepts. It is highly recommended to remember them in the order given.

Tip: Remember this sentence — **A**nxious **P**ale **C**easer **T**reated **N**ervous **D**runks **P**atiently. Now starting letter of each word resembles each layer.

Questions:

Q. What does the "OSI" in the "OSI Model" stand for?
Ans: **Open System Interconnection** — First line of the task

Q. How many layers (in digits) does the OSI model have?
Ans: **7** — Observed from the diagram

Q. What is the key term for when pieces of information get added to data?
Ans: **Encapsulation** — Combining Information

Task 2: Layer 7, Application

The application layer of the OSI model is the layer that you will be most familiar with. This familiarity is because the application layer is the layer in which protocols and rules are in place to determine how the user should interact with data sent or received.

Everyday applications such as email clients, browsers, or file server browsing software such as FileZilla provide a friendly, **G**raphical **U**ser **I**nterface (**GUI**) for users to interact with data sent or received. Other protocols include **DNS** (**D**omain **N**ame **S**ystem), which is how website addresses are translated into IP addresses.

Questions:

Q. What is the name of this Layer?
Ans. **Application**

Q. What is the technical term that is given to the name of the software that users interact with?
Ans. **Graphical User Interface** — Given in the material

Task 3: Layer 6, Presentataion

Layer 6 of the OSI model is the layer in which standardisation starts to take place. Because software developers can develop any software such as an email client differently, the data still needs to be handled in the same way — no matter how the software works.

This layer acts as a translator for data to and from the application layer (layer 7). The receiving computer will also understand data sent to a computer in one format destined for another format. For example, when you send an email, the other user may have another email client to you, but the contents of the email will still need to display the same.

Security features such as data encryption (like HTTPS when visiting a secure site) occur at this layer.

Questions:

Q. What is the name of this Layer?
Ans. **Presentation**

Q. What is the main purpose that this Layer acts as?
Ans. **Translator**

Task 4: Layer 5, Session
Once data has been correctly translated or formatted from the presentation layer (layer 6), the session layer (layer 5) will begin to create a connection to the other computer that the data is destined for. When a connection is established, a session is created. Whilst this connection is active, so is the session.

The session layer (layer 5) synchronises the two computers to ensure that they are on the same page before data is sent and received. Once these checks are in place, the session layer will begin to divide up the data sent into smaller chunks of data and begin to send these chunks (packets) one at a time. This dividing up is beneficial because if the connection is lost, only the chunks that weren't yet sent will have to be sent again — not the entire piece of the data (think of it as loading a save file in a video game).

What is worth noting is that **sessions are unique** — meaning that data cannot travel over different sessions, but in fact, only across each session instead.

Questions:

Q. What is the name of this Layer?
Ans. **Session**

Q. What is the technical term for when a connection is successfully established?
Ans. **Session**

Q. What is the technical term for "small chunks of data"?
Ans. **Packets**

Task 5: Layer 4, Transport

Layer 4 of the OSI model plays a vital part in transmitting data across a network and can be a little bit difficult to grasp. When data is sent between devices, it follows one of two different protocols that are decided based on several factors:

- TCP

- UDP

Let's begin with TCP. The **T**ransmission **C**ontrol **P**rotocol (**TCP**). Potentially hinted by the name, this protocol is designed with reliability and guarantee in mind. This protocol reserves a constant connection between the two devices for the amount of time it takes for the data to be sent and received.

Not only this, but TCP incorporates error checking into its design. Error checking is how TCP can guarantee that data sent from the small chunks in the session layer (layer 5) has then been received and reassembled in the same order.

Let's summarise the advantages and disadvantages of TCP in the table below:

Advantages of TCP	Disadvantages of TCP
Guarantees the accuracy of data.	Requires a reliable connection between the two devices. If one small chunk of data is not received, then the entire chunk of data cannot be used.
Capable of synchronising two devices to prevent each other from being flooded with data.	A slow connection can bottleneck another device as the connection will be reserved on the receiving computer the whole time.
Performs a lot more processes for reliability.	TCP is significantly slower than UDP because more work has to be done by the devices using this protocol.

TCP is used for situations such as file sharing, internet browsing or sending an email. This usage is because these services require the data to be accurate and complete (no good having half a file!).

In the diagram below, we can see how a picture of a dog is broken down into small pieces of data (known as packets) from the "web server", where the "computer" re-constructs the picture of the dog into the correct order.
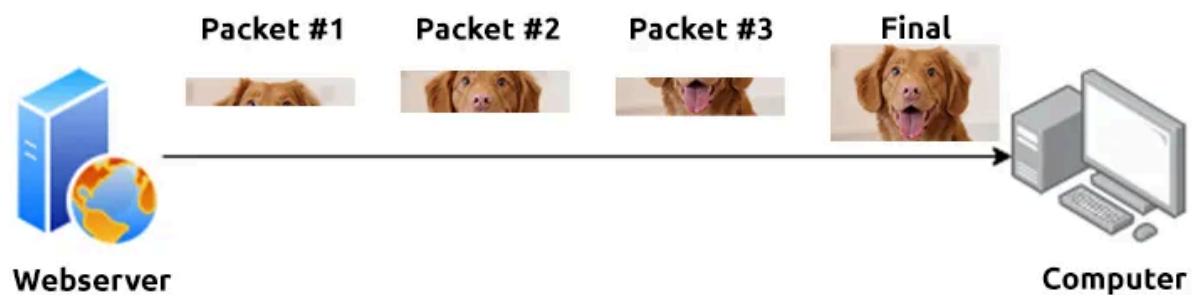
Now let's move on to the **User Datagram Protocol** (or **UDP** for short). This protocol is not nearly as advanced as its brother — the TCP protocol. It doesn't boast the many features offered by TCP, such as error checking and reliability. In fact, any data that gets sent via UDP is sent to the computer whether it gets there or not. There is no synchronisation between the two devices or guarantee; just hope for the best, and fingers crossed.

Whilst this sounds disadvantageous, it does have its merits, which we'll layout in the table below:

Advantages of UDP	Disadvantages of UDP
UDP is much faster than TCP.	UDP doesn't care if the data is received.
UDP leaves the application layer (user software) to decide if there is any control over how quickly packets are sent.	It is quite flexible to software developers in this sense.
UDP does not reserve a continuous connection on a device as TCP does.	This means that unstable connections result in a terrible experience for the user.

Using the same example as before, we can now see that only Packets #1 and #3 have been received by the "Computer", meaning that half of the image is missing.
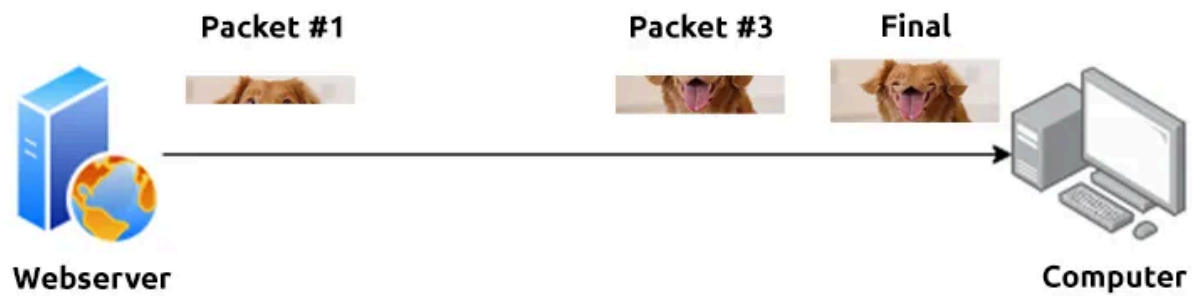
UDP is useful in situations where there are small pieces of data being sent. For example, protocols used for discovering devices or larger files such as video streaming (where it is okay if some part of the video is pixelated. Pixels are just lost pieces of data!)

Questions:

Q. What is the name of this Layer?
Ans. **Transport**

Q. What does TCP stand for?
Ans. **Transmission Control Protocol**

Q. What does UDP stand for?
Ans. **User Datagram Protocol**

Q. What protocol guarantees the accuracy of data?
Ans. **TCP**

Q. What protocol doesn't care if data is received or not by the other device?
Ans. **UDP**

Q. What protocol would an application such as an email client use?
Ans. **TCP**

Q. What protocol would an application that downloads files use?
Ans. **TCP**

Q. What protocol would an application that streams video use?
Ans. **UDP**

Task 6: Layer 3, Network

The third layer of the OSI model (network layer) is where the magic of routing & re-assembly of data takes place (from these small chunks to the larger chunk). Firstly, routing simply determines the most optimal path in which these chunks of data should be sent.

Whilst some protocols at this layer determine exactly what is the "optimal" path that data should take to reach a device, we should only know about their existence at this stage of the networking module. Briefly, these protocols include **OSPF** (**O**pen **S**hortest **P**ath **F**irst) and **RIP** (**R**outing **I**nformation **P**rotocol). The factors that decide what route is taken is decided by the following:

- What path is the shortest? I.e. has the least amount of devices that the packet needs to travel across.

- What path is the most reliable? I.e. have packets been lost on that path before?

- Which path has the faster physical connection? I.e. is one path using a copper connection (slower) or a fibre (considerably faster)?

At this layer, everything is dealt with via IP addresses such as 192.168.1.100. Devices such as routers capable of delivering packets using IP addresses are known as Layer 3 devices — because they are capable of working at the third layer of the OSI model.
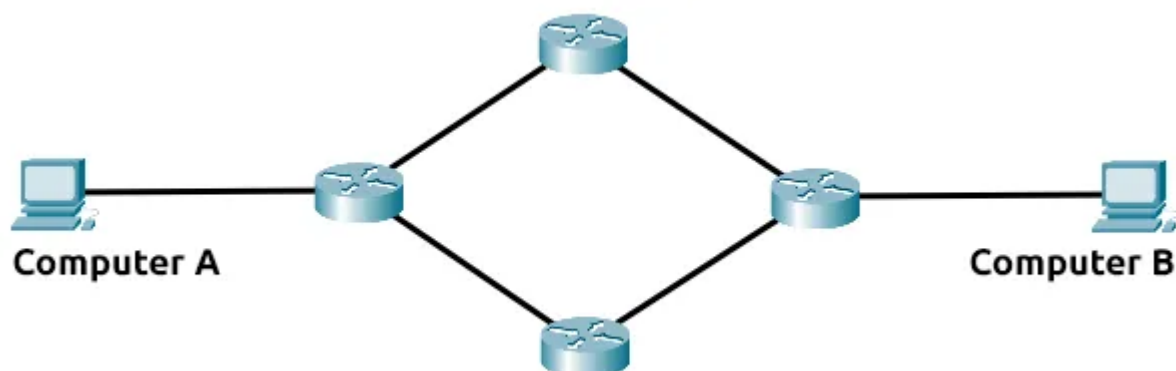
Questions:

Q. What is the name of this Layer?
Ans. **Network**

Q. Will packets take the most optimal route across a network? (Y/N)
Ans. **Y**

Q. What does the acronym "OSPF" stand for?

Ans. **Open Shortest Path First**

Q. What does the acronym "RIP" stand for?

Ans. **Routing Information Protocol**

Q. What types of addresses are dealt with at this layer?

Ans. **IP Addresses**

Task 7: Layer 2, Data Link

The data link layer focuses on the physical addressing of the transmission. It receives a packet from the network layer (including the IP address for the remote computer) and adds in the physical **MAC** (**M**edia **A**ccess **C**ontrol) address of the receiving endpoint. Inside every network-enabled computer is a Network Interface Card (**NIC**) which comes with a unique MAC address to identify it.

MAC addresses are set by the manufacturer and literally burnt into the card; they can't be changed — although they can be spoofed. When information is sent across a network, it's actually the physical address that is used to identify where exactly to send the information.

Additionally, it's also the job of the data link layer to present the data in a format suitable for transmission.

Questions:

Q. What is the name of this Layer?

Ans. **Data Link**

Q. What is the name of the piece of hardware that all networked devices come with?

Ans. **Network Interface Card**

Task 8: Layer 1, Physical

This layer is one of the easiest layers to grasp. Put simply, this layer references the physical components of the hardware used in networking and is the lowest layer that you will find. Devices use electrical signals to transfer data between each other in a binary numbering system (1's and 0's).

For example, ethernet cables connecting devices, such as in the diagram below:

Questions:

Q. What is the name of this Layer?
Ans. **Physical**

Q. What is the name of the numbering system that is both 0's and 1's?
Ans. **Binary**

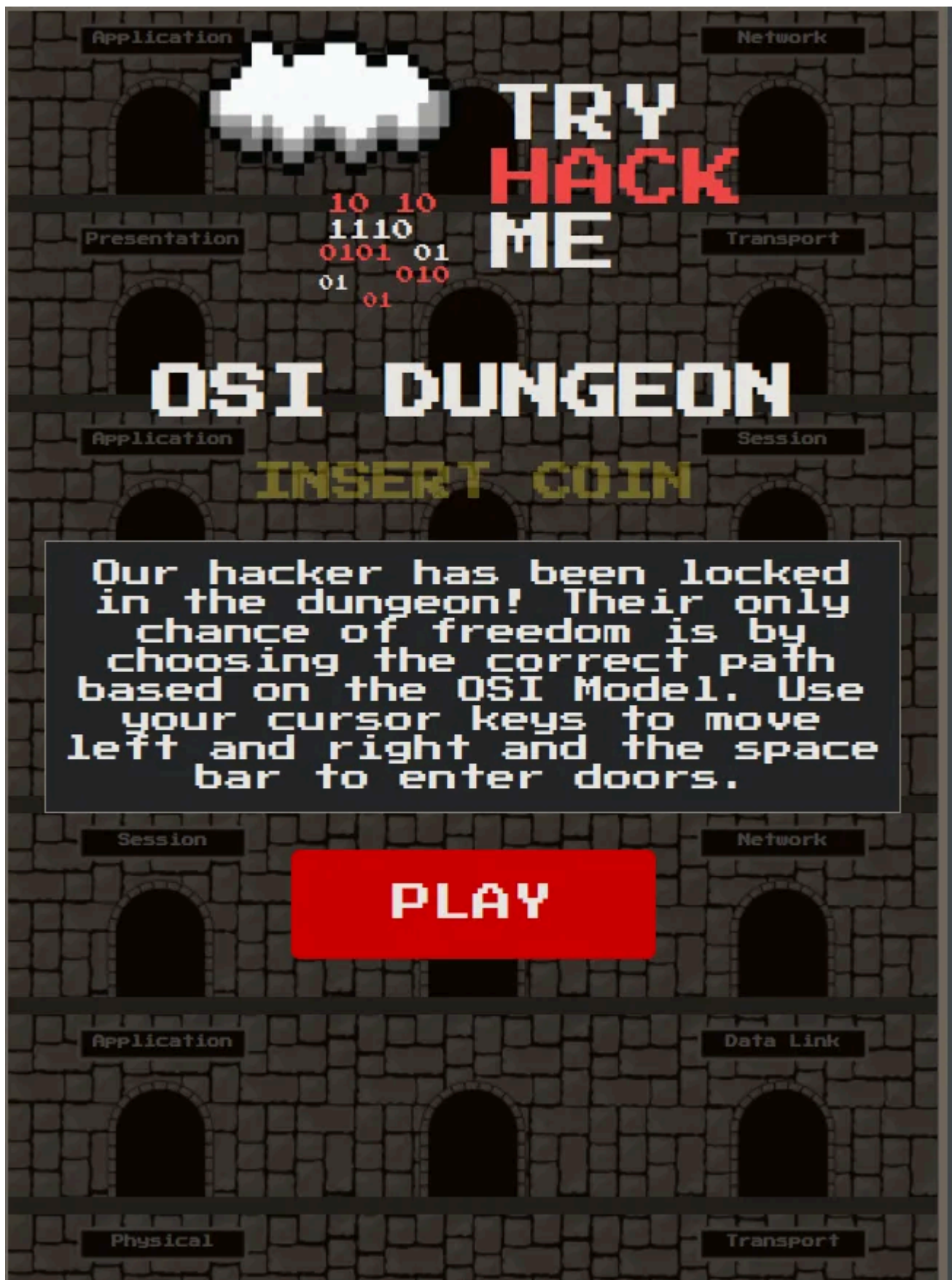Q. What is the name of the cables that are used to connect devices?
Ans. **Ethernet Cables**

Task 9: Practical — OSI Game
Can you escape the OSI dungeon? Climb the levels in the correct order to escape the dungeon and reveal the flag! (Can you beat our staff's high score of 19 seconds?)

Click the "View Site" button on the right to start.

Site Home Screen Image:

This seems to very simple yet fun game in which the character gets to enter the rooms and exit out the other when entered correctly. The room order follows the OSI Model and the player must enter the rooms in the proper order (From Bottom To Top) to complete the challenge. Hope you find it fun.
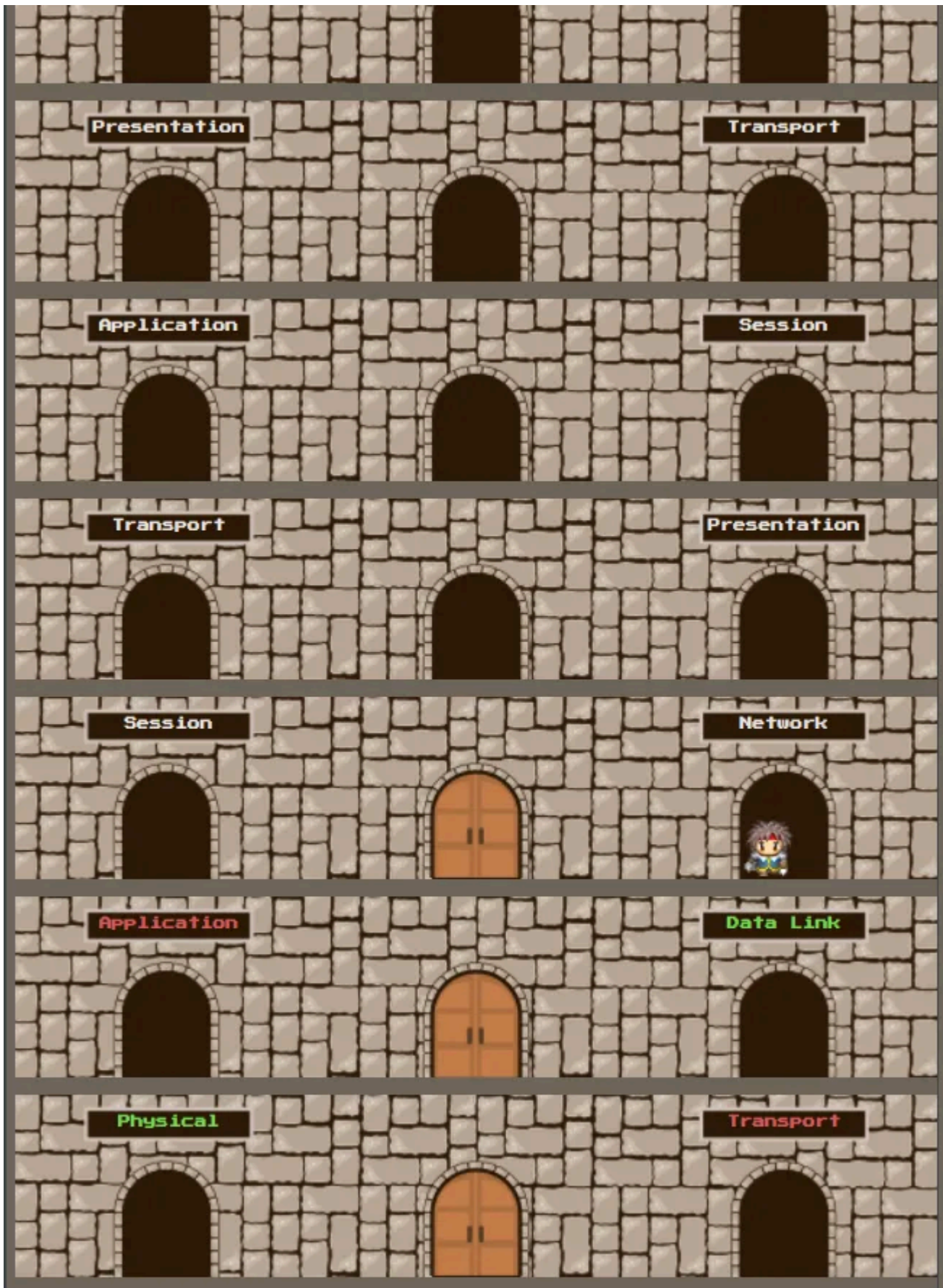
After successfully completing the challenge you will get the flag.
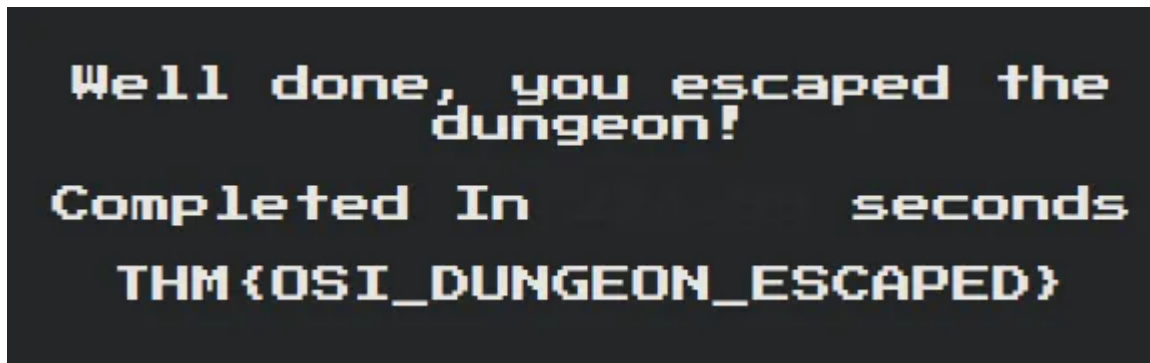
Submit the flag to complete the room.

I hope you learnt about the OSI Model in networking and learnt different concepts related to that. I encourage you to use this blog as a reference and not the actual source for your answers. Thank you for your time. I will meet you with another interesting blog, until Keep Calm & Happy Hacking!

Tryhackme   Tryhackme Writeup   Osi Model   Networking   Writeup

Follow

Written by Luc1f3r

297 Followers · 28 Following

Responses (2)

What are your thoughts?

Respond

Samar
2 months ago

thank you for the help

👏   Reply

Mohdsm
11 months ago

helpful

👏   Reply

More from Luc1f3r

Luc1f3r
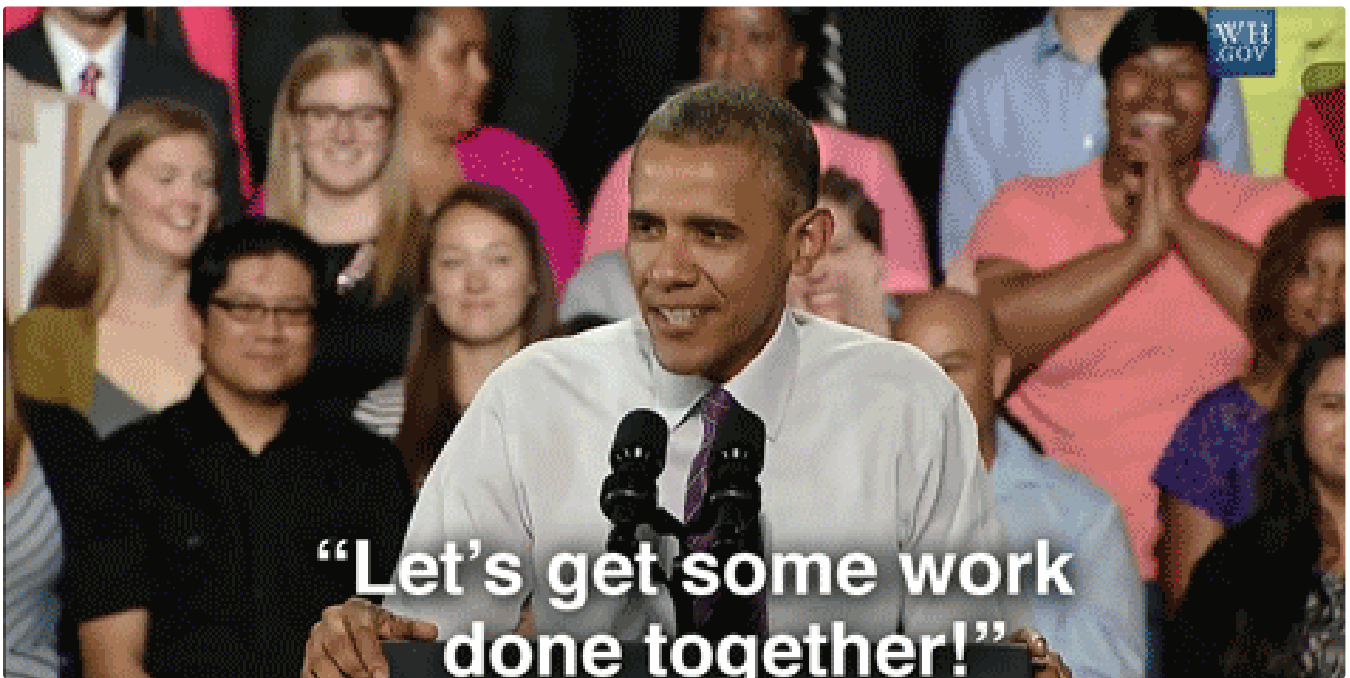
TryHackMe | Extending Your Network

Hey guys.... This is yet another write-up on a TryHackMe room — Extending your Network. This is going to be fundamental like the other rooms...

Oct 21, 2022

In The Gray Area by Luc1f3r

ChatGPT — Bug Bounty Recon Automation

In the past couple of weeks, OpenAI's ChatGPT has dominated the internet.

Jan 2, 2023   👏 570   💬 11

Luc1f3r

TryHackMe | How websites work Room Writeup

Hello everyone, Today I am writing this blog in another room in the amazing pathway — Pre security. In the previous Rooms, we saw...

Oct 22, 2022

ons: Program Misuse

rogram misuse in general?

e program in a setting that's cordor

Luc1f3r

[pwn.college] Program Misuse Notes

Hello, I am happy to write to a blog on the pwn.college which is by far one the nicest resources to learn cybersecurity from. I started...

Dec 18, 2022 💬 1

See all from Luc1f3r

Recommended from Medium

Jawstar

Advent of Cyber 2024 {Day - 23} Tryhackme Answers

The Story

Dec 24, 2024

🌀 Trnty

TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

✦ Sep 7, 2024 · 👋 10

Lists

Business 101
25 stories · 1339 saves

Abhijeet Singh

Advent of Cyber 2024 [Day 3] Even if I wanted to go, their vulnerabilities wouldn't allow it.

So, Let's Start with the Questions. I hope you already read the story and all the given instructions —

⭐   Dec 4, 2024   👋 2

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Open in app ↗

Medium　🔍 Search　　　　　　🔔　👤

👤 Abhijeet Singh

Advent of Cyber 2024 [Day 6] If I can't find a nice malware to use, I'm not going.|

- Welcome to the Day 6 of the Advent of Cyber 2024 -

✦　Dec 7, 2024　　　　　　　　　　　　　　🔖⁺　•••

🏛 In System Weakness by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 11] Writeup with Answers | TryHackMe Walkthrough

If you'd like to WPA, press the star key!

✦   Dec 11, 2024   👋 855   💬 1   🔖⁺   •••

See more recommendations

Advent of Cyber 2024 [Day 11] Writeup with Answers | TryHackMe Walkthrough

If you'd like to WPA, press the star key!