1. **Introduction**

The topics that we're going to cover in this room are:

* The OSI Model
* The TCP/IP Model
* How these models look in practice
* An introduction to basic networking tools

1. **The OSI Model: An Overview**

Which layer would choose to send data over TCP or UDP?

4

Which layer checks received information to make sure that it hasn't been corrupted?

2

In which layer would data be formatted in preparation for transmission?

2

Which layer transmits and receives data?

1

Which layer encrypts, compresses, or otherwise transforms the initial data to give it a standardised format?

6

Which layer tracks communications between the host and receiving computers?

5

Which layer accepts communication requests from applications?

7

Which layer handles logical addressing?

3

When sending data over TCP, what would you call the "bite-sized" pieces of data?

Segments

[Research] Which layer would the FTP protocol communicate with?

7

Which transport layer protocol would be best suited to transmit a live video?

UDP

1. **Encapsulation (Đóng gói)**

How would you refer to data at layer 2 of the encapsulation process (with the OSI model)?

Frames

How would you refer to data at layer 4 of the encapsulation process (with the OSI model), if the UDP protocol has been selected?

Datagrams

What process would a computer perform on a received message?

De-encapsulation

Which is the only layer of the OSI model to add a trailer during encapsulation?

Data Link

Does encapsulation provide an extra layer of security (Aye/Nay)?

Aye

1. **The TCP/IP Model**

Which model was introduced first, OSI or TCP/IP?

TCP/IP

Which layer of the TCP/IP model covers the functionality of the Transport layer of the OSI model (Full Name)?

Transport

Which layer of the TCP/IP model covers the functionality of the Session layer of the OSI model (Full Name)?

Application

The Network Interface layer of the TCP/IP model covers the functionality of two layers in the OSI model. These layers are Data Link, and?.. (Full Name)?

Physical

Which layer of the TCP/IP model handles the functionality of the OSI network layer?

Internet

What kind of protocol is TCP?

Connection-based

What is SYN short for?

Synchronise

What is the second step of the three way handshake?

SYN/ACK

What is the short name for the "Acknowledgement" segment in the three-way handshake?

ACK

1. **Ping**

What command would you use to ping the bbc.co.uk website?

ping bbc.co.uk

Ping muirlandoracle.co.uk

What is the IPv4 address?

217.160.0.152

What switch lets you change the interval of sent ping requests?

-i

What switch would allow you to restrict requests to IPv4?

-4

What switch would give you a more verbose output?

-v

1. **Traceroute**

Use traceroute on tryhackme.com

Can you see the path your request has taken?

No answer needed

What switch would you use to specify an interface when using Traceroute?

-i

What switch would you use if you wanted to use TCP SYN requests when tracing the route?

-T

[Lateral Thinking] Which layer of the TCP/IP model will traceroute run on by default (Windows)?

Internet

1. **Whois**

**Perform a whois search on facebook.com**

No answer needed

What is the registrant postal code for facebook.com?

94025

When was the facebook.com domain first registered (Format: DD/MM/YYYY)?

29/03/1997

**Perform a whois search on microsoft.com**

(Note: Please ensure you have read the task above before attempting the next questions.)

No answer needed

Which city is the registrant based in?

Redmond

[OSINT] What is the name of the golf course that is near the registrant address for microsoft.com? 🡪 tìm trên Google Maps

Bellevue Golf Course

What is the registered Tech Email for microsoft.com?

msnhst@microsoft.com

1. **Dig**

What is DNS short for?

Domain Name System

What is the first type of DNS server your computer would query when you search for a domain?

Recursive

What type of DNS server contains records specific to domain extensions (i.e. .com, .co.uk\*, etc)\*? Use the long version of the name.

Top-Level Domain

Where is the very first place your computer would look to find the IP address of a domain?

Hosts File

[Research] Google runs two public DNS servers. One of them can be queried with the IP 8.8.8.8, what is the IP address of the other one?

8.8.4.4

If a DNS query has a TTL of 24 hours, what number would the dig query show?

86400

1. **Further Reading**

Additionally, if you want to expand your knowledge of networking theory, the [CISCO Self Study Guide by Steve McQuerry](https://www.amazon.co.uk/Interconnecting-Cisco-Network-Devices-ICND1/dp/1587054620/ref=sr_1_1?keywords=Interconnecting+Cisco+Network+Devices%2C+Part+1&qid=1583683766&sr=8-1) is a great resource to work from.