could well happen when the data is transmitted by layer 1: the physical layer.

Layer 1 -- Physical:

The physical layer is right down to the hardware of the computer. This is where the electrical pulses that make up data transfer over a network are sent and received. It's the job of the physical layer to convert the binary data of the transmission into signals and transmit them across the network, as well as receiving incoming signals and converting them back into binary data.

For the "Which Layer" Questions below, answer using the layer number (1-7)

Answer the questions below

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

4 ✓ Correct Answer

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

2 ✓ Correct Answer

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

2 ✓ Correct Answer

Which layer transmits and receives data?

1 ✓ Correct Answer

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

6 ✓ Correct Answer

Which layer tracks communications between the host and receiving computers?

5 ✓ Correct Answer

Which layer accepts communication requests from applications?

7 ✓ Correct Answer

Which layer handles logical addressing?

3 ✓ Correct Answer

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

Segments ✓ Correct Answer

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

7 ✓ Correct Answer Hint

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

UDP ✓ Correct Answer

Task 3 Encapsulation

Task 4 ✓ The TCP/IP Model

Task 5 ✓ Networking Tools Ping

Task 6 ✓ Networking Tools Traceroute

Task 7 ✓ Networking Tools WHOIS

connection can be established using TCP.

History:

It's important to understand exactly *why* the TCP/IP and OSI models were originally created. To begin with there was no standardisation -- different manufacturers followed their own methodologies, and consequently systems made by different manufacturers were completely incompatible when it came to networking. The TCP/IP model was introduced by the American DoD in 1982 to provide a standard -- something for all of the different manufacturers to follow. This sorted out the inconsistency problems. Later the OSI model was also introduced by the International Organisation for Standardisation (ISO); however, it's mainly used as a more comprehensive guide for learning, as the TCP/IP model is still the standard upon which modern networking is based.

Answer the questions below

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

TCP/IP — ✓ Correct Answer

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

Transport — ✓ Correct Answer

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

Application — ✓ Correct Answer

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 — ✓ Correct Answer

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

Internet — ✓ Correct Answer

What kind of protocol is TCP?

Connection-based — ✓ Correct Answer — Hint

What is SYN short for?

Synchronise — ✓ Correct Answer — Hint

What is the second step of the three way handshake?

SYN/ACK — ✓ Correct Answer

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

ACK — ✓ Correct Answer

Task 5 ✓ Networking Tools Ping

Task 6 ✓ Networking Tools Traceroute

Task 7 ✓ Networking Tools WHOIS

Task 8 Networking Tools Dig

Task 9 ✓ Further Reading

Created by

Task 3 Encapsulation

Task 4 The TCP/IP Model

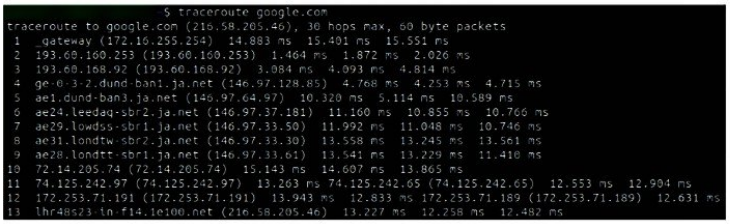
Task 5 Networking Tools Ping

Task 6 Networking Tools Traceroute

The logical follow-up to the ping command is 'traceroute'. Traceroute can be used to map the path your request takes as it heads to the target machine.

The internet is made up of many, many different servers and end-points, all networked up to each other. This means that, in order to get to the content you actually want, you first need to go through a bunch of other servers. Traceroute allows you to see each of these connections -- it allows you to see every intermediate step between your computer and the resource that you requested. The basic syntax for traceroute on Linux is this: `traceroute <destination>`

By default, the Windows traceroute utility (`tracert`) operates using the same ICMP protocol that ping utilises, and the Unix equivalent operates over UDP. This can be altered with switches in both instances.



You can see that it took 13 hops to get from my router (`_gateway`) to the Google server at 216.58.205.46

Now it's your turn. As with before, all questions about switches can be answered with the man page for traceroute (`man traceroute`).

Answer the questions below

Use traceroute on tryhackme.com
Can you see the path your request has taken?

No answer needed — ✓ Correct Answer

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

-i — ✓ Correct Answer — Hint

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

-T — ✓ Correct Answer

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

Internet — ✓ Correct Answer

Task 7 Networking Tools WHOIS

Task 8 Networking Tools Dig

Task 9 Further Reading

Created by

MuirlandOracle

Room Type	Users In Room	Created
Free Room. Anyone can deploy virtual machines in the room (without being subscribed)	409,094	1646 days ago

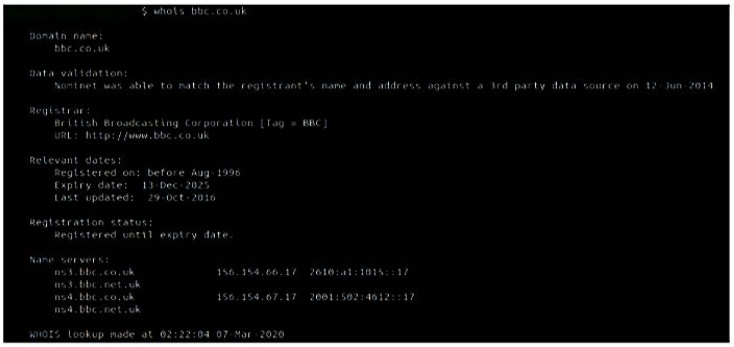
Enter whois.

Whois essentially allows you to query who a domain name is registered to. In Europe personal details are redacted; however, elsewhere you can potentially get a great deal of information from a whois search.

For Free Users using the AttackBox, there is a web version of the whois tool.

(Note: You may need to install whois before using it. On Debian based systems this can be done with `sudo apt update && sudo apt-get install whois`*)*

Whois lookups are very easy to perform. Just use `whois <domain>` to get a list of available information about the domain registration:



This is comparatively a very small amount of information as can often be found. Notice that we've got the domain name, the company that registered the domain, the last renewal, and when it's next due, and a bunch of information about nameservers (which we'll look at in the next task).

Your Turn

Answer the questions below

Perform a whois search on `facebook.com`

No answer needed — ✓ Correct Answer

What is the registrant postal code for facebook.com?

94025 — ✓ Correct Answer

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

29/03/1997 — ✓ Correct Answer

Perform a whois search on `microsoft.com`

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

No answer needed — ✓ Correct Answer

Which city is the registrant based in?

Redmond — ✓ Correct Answer

[OSINT] What is the name of the golf course that is near the registrant address for microsoft.com?

Bellevue Golf Course — ✓ Correct Answer

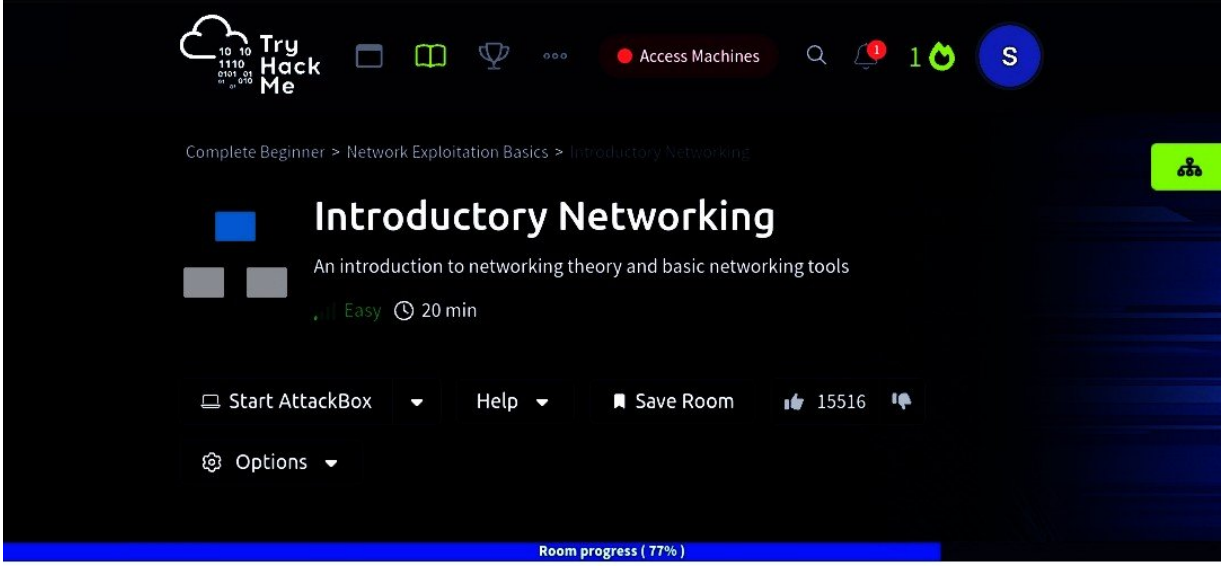
What is the registered Tech Email for microsoft.com?

msnhst@microsoft.com — ✓ Correct Answer

Task 8 Networking Tools Dig

Task 9 Further Reading

Created by



Task 1 Introduction

Task 2 The OSI Model: An Overview

Task 3 Encapsulation

Task 4 The TCP/IP Model

Task 5 Networking Tools Ping

Task 6 Networking Tools Traceroute

Task 7 Networking Tools WHOIS

Task 8 Networking Tools Dig

Task 9 Further Reading

Created by

MuirlandOracle

Room Type	Users In Room	Created
Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	409,094	1646 days ago