TryHackMe

Julien ROYON CHALENDARD

CTF :
Introductory Networking

Catégorie :
Network

2020

Sommaire

1 The OSI Model : An Overview

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

4

1.2 Which layer checks received packets to make sure that they haven't been corrupted ?

2

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

2

1.4 Which layer transmits and receives data ?

1

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

6

1.6 Which layer tracks communications between the host and receiving computers ?

5

1.7 Which layer accepts communication requests from applications ?

7

1.8 Which layer handles logical addressing ?

3

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

Segments

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

7

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

UDP

2 Encapsulation

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

Frames

2.2 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

2.3 What process would a computer perform on a received message ?

De-encapsulation

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

Data Link

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

Aye

3 The TCP/IP Model

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

TCP/IP

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

Transport

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

Application

3.4 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

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

Internet

3.6 What kind of protocol is TCP ?

Connection-based

3.7 What is SYN short for ?

Synchronise

3.8 What is the second step of the three way handshake ?

SYN/ACK

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

ACK

4 Wireshark

4.1 What is the protocol specified in the section of the request that's linked to the Application layer of the OSI and TCP/IP Models ?

Domain Name System

4.2 Which layer of the OSI model does the section that shows the IP address "172.16.16.77" link to (Name of the layer) ?

Network

4.3 In the section of the request that links to the Transport layer of the OSI and TCP/IP models, which protocol is specified ?

User Datagram Protocol

4.4 Over what medium has this request been made (linked to the Data Link layer of the OSI model) ?

Ethernet II

4.5 Which layer of the OSI model does the section that shows the number of bytes transferred (81) link to ?

Physical

4.6 [Research] Can you figure out what kind of address is shown in the layer linked to the Data Link layer of the OSI model ?

MAC

5 [Networking Tools] Ping

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

ping bbc.co.uk

5.2 What is the IP address ?

217.160.0.152

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

-i

5.4 What switch would allow you to restrict requests to IPV4 ?

-4

5.5 What switch would give you a more verbose output ?

-v

6 [Networking Tools] Traceroute

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

-i

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

-T

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

Internet

7 [Networking Tools] WHOIS

7.1 What is the registrant postal code for facebook.com ?

94025

7.2 When was the facebook.com domain first registered ?

29/03/1997

7.3 Which city is the registrant based in ?

Redmond

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

Bellevue Golf Course

7.5 What is the registered Tech Email for microsoft.com ?

msnhst@microsoft.com

8 [Networking Tools] Dig

8.1 What is DNS short for ?

Domain Name System

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

Recursive

8.3 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

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

Local Cache

8.5 [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

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

86400