Weekly challenge 2

Quiz • 50 min

Try again once you are ready

Grade received 65%
Latest Submission Grade 65%
To pass 80% or higher
Try again

Review Learning Objectives

Submit your assignment
Try again

Due Jun 18, 11:59 PM +08 Attempts 3 every 24 hours

Receive grade

Your grade 65%
To Pass 80% or higher

View Feedback
We keep your highest score

Like Dislike Report an issue

1. Fill in the blank: _____ describes the amount of data that moves across a network. **1 / 1 point**

- Data exfiltration
- Network data
- Traffic flow
- Network traffic

Correct

2. Which of the following behaviors may suggest an ongoing data exfiltration attack? Select two answers. **0.5 / 1 point**

- [x] Unexpected modifications to files containing sensitive data

  Correct

- [x] Multiple successful multi-factor authentication logins

  This should not be selected
  Please review the video on data exfiltration.

- [x] Network performance issues

  This should not be selected
  Please review the video on data exfiltration.

- [x] Outbound network traffic to an unauthorized file hosting service

  Correct

3. What information do packet headers contain? Select three answers. **0.75 / 1 point**

- [x] IP addresses

  Correct

- [x] Payload data

  This should not be selected
  Please review the video on packet captures.

- [x] Protocols

  Correct

- [x] Ports

  Correct

4. The practice of capturing and inspecting network data packets that are transmitted across a network is known as _____. **0 / 1 point**

- (•) port sniffing
- ( ) protocol capture
- ( ) packet sniffing
- ( ) packet capture

Incorrect
Please review the video on packet captures.

5. Network protocol analyzer tools are available to be used with which of the following? Select two answers. **0.5 / 1 point**

- [x] Graphical user interface

  Correct

- [x] Network interface card

  This should not be selected
  Please review the video on packet analysis.

- [x] Internet protocol

  This should not be selected
  Please review the video on packet analysis.

- [x] Command-line interface

  Correct

6. Which protocol version is considered the foundation for all internet communications? **1 / 1 point**

- ( ) HTTP
- (•) IPv4
- ( ) UDP
- ( ) ICMP

Correct

7. Which IPv4 header fields involve fragmentation? Select three answers. **0.75 / 1 point**

- [x] Identification

  Correct

- [x] Type of Service

  This should not be selected
  Please review the video on IP headers.

- [x] Flags

  Correct

- [x] Fragment Offset

  Correct

8. Which IPv4 field uses a value to represent a standard, like TCP? **1 / 1 point**

- ( ) Version
- (•) Protocol
- ( ) Total Length
- ( ) Type of Service

Correct

9. Which tcpdump command outputs detailed packet information? **0 / 1 point**

- (•) `sudo tcpdump -v any -i`
- ( ) `sudo tcpdump -i any -c 100`
- ( ) `sudo tcpdump -i any -n`
- ( ) `sudo tcpdump -i any -v`

Incorrect
Please review the video on tcpdump.

10. Examine the following tcpdump output: **1 / 1 point**

```
22:00:19.538395 IP (tos 0x10, ttl 64, id 33842, offset 0, flags [P], proto TCP
(6), length 196) 198.168.105.1.41012 > 198.111.123.1.61012: Flags [P.], cksum
0x50af (correct), seq 169, ack 187, win 501, length 42
```

What is the value of the Type of Service field?

- (•) `0x10`
- ( ) `0x50af`
- ( ) `6`
- ( ) `501`

Correct