Weekly challenge 2

Quiz • 50 min

Try again once you are ready

Grade received 67.50%

Latest Submission Grade 67.50%

To pass 80% or higher

Try again

Review Learning Objectives

1. Why is network traffic monitoring important in cybersecurity? Select two answers. **0.5 / 1 point**

- [x] It helps identify deviations from expected traffic flows.

  Correct

- [x] It provides a method of classifying critical assets.

  This should not be selected
  Please review the video on network traffic.

- [x] It helps detect network intrusions and attacks.

  Correct Like Dislike Report an issue

- [x] It provides a method to encrypt communications.

  This should not be selected
  Please review the video on network traffic.

2. What tactic do malicious actors use to maintain and expand unauthorized access into a network? **1 / 1 point**

- ( ) Exfiltration
- (•) Lateral movement
- ( ) Phishing
- ( ) Data size reduction

Correct

3. Fill in the blank: The transmission of data between devices on a network is governed by a set of standards known as _____. **1 / 1 point**

- (•) protocols
- ( ) ports
- ( ) payloads
- ( ) headers

Correct

4. Do packet capture files provide detailed snapshots of network communications? **1 / 1 point**

- (•) Yes. Packet capture files provide information about network data packets that were intercepted from a network interface.
- ( ) No. Packet capture files do not contain detailed information about network data packets.
- ( ) Maybe. The amount of detailed information packet captures contain depends on the type of network interface that is used.

Correct

5. Fill in the blank: tcpdump is a network protocol analyzer that uses a(n) _____ interface. **1 / 1 point**

- ( ) internet
- ( ) graphical user
- (•) command-line
- ( ) Linux

Correct

6. Which layer of the TCP/IP model is responsible for accepting and delivering packets in a network? **0 / 1 point**

- ( ) Transport
- ( ) Application
- (•) Network Access
- ( ) Internet

Incorrect
Please review the video on IP headers.

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

- [x] Type of Service

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

- [x] Identification

  Correct

- [x] Flags

  Correct

- [x] Fragment Offset

  Correct

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

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

Correct

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

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

Incorrect
Please review the video on tcpdump.

10. Examine the following tcpdump output: **0.5 / 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
```

Which protocols are being used? Select two answers.

- [x] `UDP`

  This should not be selected
  Please review the video on tcpdump.

- [x] `TOS`

  This should not be selected
  Please review the video on tcpdump.

- [x] `TCP`

  Correct

- [x] `IP`

  Correct