Question 1
Why is network traffic monitoring important in cybersecurity? Select two answers. 1 / 1 point
It helps detect network intrusions and attacks.
Correct
It provides a method to encrypt communications.
It provides a method of classifying critical assets.
It helps identify deviations from expected traffic flows.
Correct

Question 2
Which of the following behaviors may suggest an ongoing data exfiltration attack? Select two answers. 1 / 1 point
Multiple successful multi-factor authentication logins
Outbound network traffic to an unauthorized file hosting service
Correct
Network performance issues
Unexpected modifications to files containing sensitive data
Correct

Question 3
What information do packet headers contain? Select three answers. 1 / 1 point
Protocols
Correct
Payload data
IP addresses
Correct
Ports
Correct

Question 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

Question 5
Fill in the blank: tcpdump is a network protocol analyzer that uses a(n) _____ interface. 1 / 1 point
Linux
graphical user
command-line
internet
Correct

Question 6
Which layer of the TCP/IP model is responsible for accepting and delivering packets in a network? 1 / 1 point
Application
Transport
Internet
Network Access
Correct

Question 7
Which IPv4 header fields involve fragmentation? Select three answers.1 / 1 point
Flags
Correct
Identification
Correct
Fragment Offset
Correct
Type of Service

Question 8
What is the process of breaking down packets known as? 1 / 1 point
Flags
Fragmentation
Checksum
Fragment Offset
Correct

Question 9
Which tcpdump option applies verbosity? 1 / 1 point
-i
-c
-v
-n
Correct

Question 10
Examine the following tcpdump output:
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. 1 / 1 point
UDP
TOS
TCP
Correct
IP
Correct