Past-paper walk-through

Detecting Network Attacks ▪ 3.5

eXercise

Questions in this set

- 2026 Q13 ▪ 1 mark
- 2026 Q14 ▪ 1 mark
- 2026 Q22 ▪ 1 mark

Question 13

2026 ▪ Q13 ▪ 1 mark

The network administrator for a manufacturing facility has implemented a signature-based network detection system. Which of the following is a potential impact of using this network detection method instead of anomaly-based detection? **[1]**

A More false negative alerts

B Higher operating costs

C Slower detection time

D More alert fatigue

Solution 13

A More false negative alerts ✓

B Higher operating costs

C Slower detection time

D More alert fatigue

Answer: **A**

Question 14

2026 ▪ Q14 ▪ 1 mark

Consider the following lines from a log file: 2025-09-25 08:01:14 ARP Reply: 192.168.1.13 is-at 00:01:5e:00:fc:16; 2025-09-25 09:14:15 ARP Reply: 192.168.1.13 is-at 00:3b:cc:5e:ee:01. Which of the following attack types is indicated in the log file? **[1]**

A ARP poisoning attack

B DNS poisoning attack

C Evil-twin attack

D MAC flooding attack

Question 14

```
2025-09-25 08:01:14 ARP Reply: 192.168.1.13 is-at 00:01:5e:00:fc:16
2025-09-25 09:14:15 ARP Reply: 192.168.1.13 is-at 00:3b:cc:5e:ee:01
```

Solution 14

A ARP poisoning attack ✓

B DNS poisoning attack

C Evil-twin attack

D MAC flooding attack

Answer: **A**

Question 22

2026 ▪ Q22 ▪ 1 mark

A hospital's security manager has implemented an automated network security tool that: analyzes network traffic for signs of malicious activity so the team can spot threats; generates an alert when suspicious or malicious traffic is detected; but does not take direct action to block or stop the traffic itself, because the hospital wants administrators to decide how to respond. Which of the following security systems did the security manager implement? **[1]**

A Data loss prevention system

B Network intrusion prevention system

C Network intrusion detection system

D Security information and event management system

Solution 22

A Data loss prevention system

B Network intrusion prevention system

C Network intrusion detection system ✅

D Security information and event management system

Answer: **C**