Quiz 9

Due Feb 24 at 11:59pm **Points** 15 **Questions** 8
Available Feb 23 at 12pm - Feb 24 at 11:59pm **Time Limit** 30 Minutes

Instructions

Quiz 9 covers MOs 1,2,3,5,6,7,8,9,10,13 in Module 5:

- MO 1. Define firewall policy and properties that firewall policies are based on (CO 1)
- MO 2. Identify the blacklist approach to creating firewall policies (CO 6)
- MO 3. Identify the whitelist approach to creating firewall policies (CO 6)
- MO4. Define a stateless firewall (CO 6)
- MO 5. Define a stateful firewall (CO 6)
- MO 6. Compare and contrast a stateless firewall and a stateful firewall (CO 6)
- MO 7. Define intrusion, intrusion detection, and intrusion prevention (CO 1)
- MO 8. Describe IDS components (CO 6)
- MO 9. Identify the automated attacks and threats that an IDS is designed to detect (CO 1)
- MO 10. Define the two types of mistakes that an IDS can make: false positive and false negative (CO 1)
- MO 13. Define the Base-Rate Fallacy (CO 1)

This quiz is no longer available as the course has been concluded.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	15 minutes	9 out of 15

Correct answers are hidden.

Score for this quiz: **9** out of 15
Submitted Feb 23 at 12:24pm
This attempt took 15 minutes.

Question 1	**2 / 2 pts**

Which option below might be classified as an intrusion?

- ARP spoofing
- Unauthorized access (misfeasor)
- Malware attack
- Denial-of-service attack
- All of the above

Question 2

2 / 2 pts

The following are possible outcomes of an IDS alarm except this one

- False positive
- True positive
- True negative
- Data breach
- False negative

Question 3

2 / 2 pts

What perform the same operations as packet filters, but also maintain state about the packets that have arrived?

- Stateful firewalls

- Virus
- Worm
- Backdoor
- User-level Rootkit

Incorrect

Question 4

0 / 2 pts

Which of the following is NOT true?

- An IDS can detect DNS cache poisoning attacks
- An IDS can make decision based on resource-usage information
- All firewalls maintain tables containing information on each active connection
- A firewall can make decision based on the source IP address

Question 5

1 / 1 pts

True or false: A **misfeasor** is a user who tries to block or cover up his actions by deleting audit files and/or system logs.

- True
- False

Incorrect

Question 6

0 / 2 pts

Which of the following is NOT true?

- Components of an IDS include IDS Sensors
- IPS stands for Intrusion Protection System
- **An ideal IDS should have both a high true-positive rate and a low false-negative rate**
- False-negative means that no alarm is sounded when there is an intrusion attack

Incorrect

Question 7

0 / 2 pts

True or false: Statistical Intrusion Detection can capture unknown or zero-day attacks.

- True
- **False**

Question 8

2 / 2 pts

Which of the following is NOT true about firewall policies (or rulesets)?

The blacklist approach specifies what kinds of packets should be dropped or rejected

They can be based on the source and destination IP addresses

The whitelist approach is more flexible (compared with the blacklist approach) in ensuring that service to the internal network is not disrupted by the firewall

The whitelist approach to defining a firewall ruleset is the default-deny policy

Quiz Score: **9** out of 15