IPS Introduction

1. Which of the following is true of an IDS?

A. Uses inline mode
B. Implements blocking to stop an attacker
C. Uses IP logging to send alerts
D. Only supports signatures to look for an attack

2. What IPS/IDS implementation uses templates and rules to find attacks?

A. Profiles
B. Signatures
C. Protocol analysis
D. Policies

3. What is not an action an IDS or IPS can typically take when an attack is detected?

A. TCP reset
B. IP logging
C. Produce an alert
D. Rate-limit traffic

4. What are the two kinds of interfaces found on an IDS/IPS? (Choose two.)

A. Command-and-control
B. Blocking
C. Reset
D. Monitoring

Answers

1.
- ☑ **B.** An IDS can use blocking to drop packets from an attacker, where the IDS logs in to an intermediate device to set up a blocking function.
- ☒ **A** is true of an IPS. **C** captures packets. An IDS can support other implementations other than signatures, like profiles, making **D** incorrect.

2.
- ☑ **B.** A signature is basically a simplified profile (template) that looks for certain items that are construed to be part of an attack.
- ☒ **A** examines traffic activity and compares it to a file of previously captured packets. **C** looks at traffic and compares it to protocol or application standards, like RFCs. **D** compares traffic to white and/or black lists to determine if the traffic constitutes an attack.

3.
- ☑ **D.** An IPS/IDS typically will not rate-limit traffic as an action when an attack is detected—an IDS can't do this, since traffic doesn't flow through it.
- ☒ **A**, **B**, and **C** are actions that an IDS or IPS can typically take.

4.
- ☑ **A** and **D.** A network IPS/IDS has two kinds of interfaces: command-and-control and monitoring.
- ☒ **B** is found on an intermediate device. **C** is an uncommon type of interface to be found on a sensor.

Signatures

5. A _____ signature examines many packets to determine if an attack is occurring. ?

A. Context
B. Content
C. Atomic
D. Compound

6. What alarm type indicates that an attack was not detected? ?

A. False positive
B. False negative
C. True positive
D. True negative

7. Cisco primarily relies on what technology on their network-based sensor solutions to detect and prevent attacks? ?

A. Signatures
B. Profiles
C. Protocol analysis
D. Policies

Answers

5.
- ☑ **D.** A compound signature examines many packets to determine if an attack is occurring.
- ☒ **A** examines just header information in a packet. **B** examines header and payload information. **C** looks for an attack in a single packet.

6.
- ☑ **B.** A false negative is where an attack occurs, but the IPS/IDS solution doesn't see it as an attack.
- ☒ **A** is where normal traffic triggers an alarm. **C** is where an attack occurred and an alarm was triggered. **D** is where the IPS/IDS solution sees normal traffic and doesn't trigger an alarm.

7.
- ☑ **A.** Cisco primarily relies on signatures on their network-based sensor solutions to detect and prevent attacks.
- ☒ Cisco supports **B**, **C**, and **D**, but primarily relies on signatures.

Cisco IPS Products

8. What SME would look for application-layer attacks? ?

A. Atomic
B. Flood
C. Service
D. String

9. What protocol does SDEE use to send alarms between a sensor and a management station? ?

A. SSH
B. SNMP
C. HTTP
D. HTTPS

10. What method does a management station typically use to obtain alerts from a sensor when using SDEE?

A. Syslog
B. SNMP
C. Subscription
D. Active/reset

Answers

8.
- ☑ **C.** The Service SME looks for application-layer attacks.
- ☒ **A** looks for attacks in a single packet. **B** uses compound implementations to look for flood DoS attacks. **D** uses regular expression strings to look for attacks.

9.
- ☑ **D.** SDEE uses HTTPS (SSL) to send alarms between a sensor and a management station.
- ☒ **A**, **B**, and **C** are not used by SDEE.

10.
- ☑ **C.** A management station opens up a subscription to an IPS sensor and pulls the alarms from it.
- ☒ **A** and **B** are alternatives to SDEE. **D** is a nonexistent term.