Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/11/2022 8:05:14 pm • Time spent: 03:59

Score: 60% Passing Score: 80%

Question 1: ✓ Correct

You are concerned about protecting your network from network-based attacks on the internet. Specifically, you are concerned about attacks that have not yet been identified or that do not have prescribed protections.

Which type of device should you use?

- ○ Signature-based IDS
- ○ Host-based firewall
- ➡ ● Anomaly-based IDS
- ○ Network-based firewall
- ○ Antivirus scanner

EXPLANATION

An anomaly-based intrusion detection system (IDS) can recognize and respond to some unknown attacks. Signature recognition, also referred to as pattern matching or dictionary recognition, looks for patterns in network traffic and compares them to known attack patterns called signatures. Signature-based recognition cannot detect unknown attacks. This system can only detect attacks identified by published signature files.

Antivirus software is a form of signature-based IDS. A network-based firewall filters packets for a network, while a host-based firewall filters packets for a host. Firewalls are typically configured using access control lists that identify specific traffic as allowed or denied.

REFERENCES

11.3.2 IDS Facts

q_ids_anomaly_secp7.question.fex

Question 2: ✓ Correct

Which of the following describes the worst possible action by an IDS?

- ● The system identified harmful traffic as harmless and allowed it to pass without generating any alerts.
- ○ The system detected a valid attack and the appropriate alarms and notifications were generated.
- ○ The system correctly deemed harmless traffic as inoffensive and let it pass.
- ○ The system identified harmless traffic as offensive and generated an alarm.

EXPLANATION

The worst possible action an IDS can perform is identifying harmful traffic as harmless and allowing it to pass without generating any alerts. This condition is known as a false negative.

Positive traffic assessment means that the system detected a valid attack and the appropriate alarms and notifications were generated. Negative traffic assessment means that the system correctly deemed harmless traffic as inoffensive and let it pass. False positive traffic assessment means that the system identified harmless traffic as offensive and triggered an alarm.

REFERENCES

11.3.2 IDS Facts

q_ids_false_neg_secp7.question.fex

▾ Question 3: ✓ Correct

Which of the following describes a false positive when using an IPS device?

○ The source address matching the destination address

➡ ● Legitimate traffic being flagged as malicious

○ Malicious traffic not being identified

○ The source address identifying a non-existent host

○ Malicious traffic masquerading as legitimate traffic

EXPLANATION

On an intrusion prevention system (IPS), a positive match occurs when traffic matches the signature that identifies malicious traffic. A false positive occurs when legitimate traffic is identified as malicious traffic. This situation is undesirable, as it often results in legitimate traffic being rejected. Good IPS signature files result in low false positive rates.

A false negative occurs when malicious traffic is not identified and is, therefore, allowed.

Spoofing is the technique of falsifying the source address in a packet.

REFERENCES

11.3.2 IDS Facts

q_ids_false_pos_02_secp7.question.fex

Question 4: ✗ Incorrect

As a security precaution, you have implemented IPsec that is used between any two devices on your network. IPsec provides encryption for traffic between devices.

You would like to implement a solution that can scan the contents of the encrypted traffic to prevent any malicious attacks.

Which solution should you implement?

- ○ Protocol analyzer
- ● ~~Network-based IDS~~
- ○ Port scanner
- ➡ ○ Host-based IDS
- ○ VPN concentrator

EXPLANATION

A host-based IDS is installed on a single host and monitors all traffic coming into the host. A host-based IDS can analyze encrypted traffic because the host operating system decrypts that traffic as it is received.

A network-based IDS is a dedicated device installed on the network. It analyzes all traffic on the network. It cannot analyze encrypted traffic because the packet contents are encrypted so that only the recipient can read the packet contents.

A protocol analyzer examines packets on the network, but it cannot look at the contents of encrypted packets. A port scanner probes a device to identify open protocol ports. A VPN concentrator is a device used to establish remote access VPN connections.

REFERENCES

11.3.2 IDS Facts

q_ids_host_01_secp7.question.fex

Question 5: ✓ Correct

What is the most common form of host-based IDS that employs signature or pattern-matching detection methods?

- ○ Firewalls
- ○ Motion detectors
- ○ Honeypots
- ➡ ● Antivirus software

EXPLANATION

Antivirus software using signatures is the most commonly deployed form of a host-based IDS.

REFERENCES

11.3.2 IDS Facts

q_ids_host_03_secp7.question.fex

Question 6: ✕ Incorrect

An active IDS system often performs which of the following actions? (Select two.)

□ Traps and delays the intruder until the authorities arrive.

➡ ☑ Performs reverse lookups to identify an intruder.

☑ ~~Cannot be detected on the network because it takes no detectable actions.~~

□ Requests a second logon test for users performing abnormal activities.

➡ □ Updates filters to block suspect traffic.

EXPLANATION

An active IDS performs behaviors that can be seen by anyone watching the network. Usually, these actions are necessary to block malicious activities or discover the identity of an intruder. Updating filters and performing reverse lookups are common behaviors of an active IDS.

No form of IDS requires users to perform a second logon based on questionable activities. There are some authentication systems, such as CHAP, that periodically re-authenticate, but that is done at random time intervals and is not visible to the user. A solution that serves to trap and delay the intruder until the authorities arrive describes a man trap (a physical security mechanism). However, this definition could be stretched to include honeypots and padded cells (logical or technical security mechanisms often used in conjunction with an IDS).

A passive IDS cannot be detected on the network because it takes no detectable actions.

REFERENCES

11.3.2 IDS Facts

q_ids_ids_03_secp7.question.fex

Question 7: ✕ Incorrect

You are concerned about attacks directed at your network firewall. You want to be able to identify and be notified of any attacks. In addition, you want the system to take immediate action to stop or prevent the attack, if possible.

Which tool should you use?

○ Port scanner

○ Packet sniffer

➡ ○ IPS

● ~~IDS~~

EXPLANATION

Use an intrusion prevention system (IPS) to both detect and respond to attacks.

An intrusion detection system (IDS) can detect attacks and send notifications, but it cannot respond to attacks.

Use a port scanner to check for open ports on a system or a firewall. Use a packet sniffer to examine packets on the network.

REFERENCES

11.3.2 IDS Facts

q_ids_ips_01_secp7.question.fex

Question 8: × Incorrect

Your organization uses a web server to host an e-commerce site.

Because this web server handles financial transactions, you are concerned that it could become a prime target for exploits. You want to implement a network security control that analyzes the contents of each packet going to or from the web server. The security control must be able to identify malicious payloads and block them.

What should you do?

- ● ~~Implement an application-aware IDS in front of the web server~~
- ➡ ○ Implement an application-aware IPS in front of the web server
- ○ Implement a stateful firewall in front of the web server
- ○ Install an anti-malware scanner on the web server
- ○ Implement a packet-filtering firewall in front of the web server

EXPLANATION

You should implement an application-aware IPS in front of the web server. Even though an application-aware IDS can analyze network packets to detect malicious payloads, only an application-aware IPS can both detect and block malicious packets. Because of this, an application-aware IPS would be the most appropriate choice.

Installing an anti-malware scanner on the web server itself is a good idea, but it can only detect malware after it has been installed on the server. Using a packet-filtering firewall or a stateful firewall is also a good security measure, but neither are capable of inspecting the contents of network packets. A packet-filtering firewall can only filter based on IP address, port, and protocol. A stateful firewall can only monitor the state of a TCP connection. These devices should be used in conjunction with an IDS or an IPS to protect a network.

REFERENCES

11.3.2 IDS Facts

q_ids_ips_03_secp7.question.fex

Question 9: ✓ Correct

Which IDS method searches for intrusion or attack attempts by recognizing patterns or identifying entities listed in a database?

○ Stateful-inspection-based IDS

○ Anomaly-analysis-based IDS

○ Heuristics-based IDS

➡ ● Signature-based IDS

EXPLANATION

A signature-based IDS, or pattern-matching-based IDS, is a detection system that searches for intrusion or attack attempts by recognizing patterns that are listed in a database.

A heuristics-based IDS is able to perform some level of intelligent statistical analysis of traffic to detect attacks. Anomaly-analysis-based IDSs look for changes in the normal patterns of traffic. Stateful-inspection-based IDSs search for attacks by inspecting packet contents and associating one packet with another. These searches look for attacks in overall data streams rather than individual packets.

REFERENCES

11.3.2 IDS Facts

q_ids_signature_01_secp7.question.fex

▼ **Question 10:** ✓ Correct

What does an IDS that uses signature recognition use to identify attacks?

○ Comparison of current statistics to past statistics

○ Exceeding threshold values

○ Statistical analysis to find unusual deviations

➡ ◉ Comparisons to known attack patterns

EXPLANATION

Signature recognition, also referred to as pattern matching, dictionary recognition, or misuse-detection (MD-IDS), looks for patterns in network traffic and compares them to known attack patterns called signatures.

Anomaly recognition, also referred to as behavior, heuristic, or statistical recognition, monitors traffic to define a standard activity pattern as normal. Clipping levels or thresholds are defined that identify deviations from the norm. When the threshold is reached, an alert is generated or an action is taken. Anomaly-based systems can recognize and respond to some unknown attacks (attacks that do not have a corresponding signature file).

REFERENCES

11.3.2 IDS Facts

q_ids_signature_02_secp7.question.fex