Exam Report: 6.8.7 Practice Questions

Date: 1/21/2020 8:33:18 pm
Time Spent: 8:32

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 67%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: 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?

○ Port scanner

● ~~Network-based IDS~~

○ VPN concentrator

○ Protocol analyzer

➡ ○ Host-based IDS

Explanation

A *host-based* IDS is installed on a single host and monitors all traffic coming in to 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 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

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_02]

Question 2: Correct

What do host-based intrusion detection systems often rely upon to perform detection activities?

○ Remote monitoring tools

○ Network traffic

○ External sensors

➡ ● Host system auditing capabilities

Explanation

A host-based IDS often relies upon the host system's auditing capabilities to perform detection activities. The host-based IDS uses the logs of the local system to search for attack or intrusion activities. Host-based IDS does not analyze network traffic, use external sensors, or rely upon remote monitoring tools.

References

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_05]

Question 3: Correct

Which actions can a typical passive intrusion detection system (IDS) take when it detects an attack? (Select two.)

➡ ☑ An alert is generated and delivered via email, the console, or an SNMP trap.

□ The IDS configuration is changed dynamically, and the source IP address is banned.

□ LAN-side clients are halted and removed from the domain.

➡ ☑ The IDS logs all pertinent data about the intrusion.

Explanation

The main functions of a passive IDS are to log suspicious activity and generate alerts if an attack is deemed to be severe. Additional functionality can be achieved by using a more advanced type of IDS called an active IDS. An active IDS can automate responses that may include dynamic policy adjustment and reconfiguration of supporting network devices to block the offending traffic.

References

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_06]

Question 4: Correct

Network-based intrusion detection is most suited to detect and prevent which types of attacks?

○ Application implementation flaws

○ Buffer overflow exploitation of software

➡ ● Bandwidth-based denial of service

○ Brute force password attack

Explanation

Network-based intrusion detection systems are best suited to detect and prevent bandwidth-based denial of service attacks. This type of attack manipulates network traffic in such a way that network-based IDS can easily detect it.

The other forms of attack are content-specific and directed at a host. For this reason. these attacks are not easily detected by a network-based IDS.

References

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_08]

Question 5: Correct

Which of the following activities are considered passive in regards to the function of an intrusion detection system? (Choose two.)

➡ ☑ Monitoring the audit trails on a server

□ Transmitting FIN or RES packets to an external host

➡ ☑ Listening to network traffic

☐ Disconnecting a port being used by a zombie

Explanation

Passive IDS is a form of IDS that takes no noticeable action on the network. Passive IDS systems are undetectable by intruders. Passive IDS systems can monitor audit trails or listen to network traffic in real time.

Active IDS functions are those that interact with the network and generate detectible events. Such events can include disconnecting ports or transmitting FIN or RES packets to attackers.

References

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_09]

Question 6: Correct

Which of the following devices can monitor a network and detect potential security attacks?

○ Load balancer

○ DNS server

➡ ● IDS

○ CSU/DSU

○ Proxy

Explanation

An intrusion detection system (IDS) is a special network device that can detect attacks and suspicious activity.

A proxy server is a type of firewall that can filter based on upper-layer data. A CSU/DSU is a device that converts the signal received from the WAN provider into a signal that can be used by equipment at the customer site. A DNS server provides IP address-to-host name resolution. *Load balancing* configures a group of servers in a logical group called a *server farm*. Incoming requests to the group are distributed to individual members within the group.

References

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_17]

Question 7: Incorrect

Which of the following are security devices that perform stateful inspection of packet data and look for patterns that indicate malicious code? (Select two.)

➡ ☑ IDS

☐ ACL

☑ ~~Firewall~~

☐ VPN

➡ ☐ IPS

Explanation

An intrusion detection system (IDS) and an intrusion prevention system (IPS) are devices that scan packet contents looking for patterns that match known malicious attacks. Signature files identify the patterns of all known attacks. When a packet matches the pattern indicated in the signature file, the packet can be dropped or an alert can be sent.

Firewalls use an access control list (ACL) to filter packets based on the packet header information. Firewalls can filter packets based on port, protocol, or IP address. A virtual private network (VPN) is an encrypted communication channel established between two entities to exchange data over an unsecured network.

References

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_18]

▼ Question 8: Incorrect

You have configured an NIDS to monitor network traffic. Which of the following describes harmless traffic that has been identified as a potential attack by the NIDS device?

➡ ○ False positive

○ Negative

○ Positive

● ~~False negative~~

Explanation

False positive traffic assessment means that the system identified harmless traffic as offensive and generated an alarm or stopped the traffic.

Negative traffic assessment means that the system deemed the traffic harmless and let it pass. False negative traffic assessment means that harmful traffic was allowed to pass without any alerts being generated or any actions being taken to prevent or stop it. This is the worst possible action by an IDS. Positive traffic assessment means that the system detected an attack and the appropriate alarms and notifications were generated or the correct actions were performed to prevent or stop the attack.

References

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_20]

▼ Question 9: Correct

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

○ Malicious traffic not being identified

○ The source address matching the destination address

➡ ● Legitimate traffic being flagged as malicious

○ Malicious traffic masquerading as legitimate traffic

○ The source address identifying a non-existent host

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

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_21]

▼ Question 10: Correct

Which of the following devices is capable of detecting and responding to security threats?

➡ ● IPS

○ IDS

○ DNS server

○ Multi-layer switch

Explanation

An intrusion prevention system (IPS) can detect and respond to security events. An IPS differs from an IDS because it can respond to security threats, not just detect them.

A DNS server provides IP address-to-host name resolution. A multi-layer switch uses an ASIC module to switch packets based on packet or data content instead of using the CPU and software.

References

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_23]

▼ **Question 11:** Correct

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

○ IDS

○ Packet sniffer

➡ ● IPS

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 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

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_24]

▼ **Question 12:** Correct

Network-based intrusion detection is most suited to detect and prevent which types of attacks?

○ Brute force password attack

○ Buffer overflow exploitation of software

➡ ● Bandwidth-based denial of service

○ Application implementation flaw

Explanation

Network-based intrusion detection systems are best suited to detect and prevent bandwidth-based denial of service attacks. This type of attack manipulates network traffic in such a way that network-based IDS can easily detect it.

The other forms of attack are content-specific and directed against a host. For this reason, they are not easily detected by network-based IDS.

References

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_28]

Question 13: Incorrect

A honeypot is used for which purpose?

➡ ○ To delay intruders in order to gather auditing data

○ To prevent sensitive data from being accessed

○ To disable an intruder's system

● ~~To entrap intruders~~

Explanation

A honeypot is used to delay intruders in order to gather auditing data. A honeypot is a fake network or system that hosts false information but responds as a real system should. Honeypots usually entice intruders to spend considerable time on the system and allows extensive logging of the intruder's activities. A honeypot often allows companies to discover and even prosecute intruders.

Honeypots should not be used to entrap intruders. Entrapment is an illegal activity. Honeypots are not direct countermeasures to preventing unwanted access. Rather, they are an enticement to prevent intruders from getting into the private network in the first place. Honeypots rarely take offensive action against intruders. They may prevent malicious activities from being launched by an intruder, but they do not direct attacks at the intruder.

References

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_29]

Question 14: 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 will analyze 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 a stateful firewall in front of the web server~~

○ Install an anti-malware scanner on the web server

○ Implement an application-aware IDS in front of the web server

○ Implement a packet-filtering firewall in front of the web server

➡ ○ Implement an application-aware IPS 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

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_31]

▼ **Question 15:** Correct

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

○ The system identified harmless traffic as offensive and generated an alarm.

➡ ● The system identified harmful traffic as harmless and allowed it to pass without generating any alerts.

○ The system correctly deemed harmless traffic as inoffensive and let it pass.

○ The system detected a valid attack and the appropriate alarms and notifications were generated.

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

LabSim for Security Pro, Section 6.8.
[All Questions SecPro2017_v6.exm INTRUSION_DETECT_PREV_26]