14.1.9 practice exam

Which of the following activities are considered passive in regards to the functioning of anintrusion detection system? (Select two.)Monitoring the audit trails on a server

Listening to network trafficAn active IDS system often performs which of the following actions? select twoUpdate filters to block suspect traffic

Perform reverse lookups to identify an intruderWhat does an IDS that uses signature recognition use for identifying attacks? Comparison to a database of know attacksWhich of the following are security devices that perform stageful inspections of packet data, looking for patterns that indicate malicious code? select twoIPS

IDSProperly configured passive IDS and system audit logs are an integral part of a comprehensive security plan. What step must be taken to ensure that the information is useful in maintaining a secure environment? Periodic reviews must be conducted to detect malicious activity or policy violations.

What security mechanism can be used to detect attacks originating on the Internet or from within an internal trusted subnet? IDSYou are connected 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 when poosible to stop or prevent the attacks.

Which tool should you use? IPSAs 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? Host based IDSYou are concerned about protecting your network from network-based attacks from the internet.

Specifically, you are concerned about zero day attacks (attacks that have not yet been identified or that do not have prescribed protections.)

Which type of device should you use? Anomaly based IDSIf maintaining confidentiality is of the utmost importance to your organization, what is the best response when an intruder is detected on your network? Disconnect the intruderYou have worked as a network Admin for a company for seven months. One day all picture files on the server become corrupted.

You discover that a user downloaded a virus from the internet onto his workstation, and it propagated to the server. You successfully restore all files from backup, but your boss adam at that this situation does not occur.

What should you do? Install a network virus detection software solution.

Which of the following actions should you take to reduce the attack surface of a server? Disable unused servicesYou want to make sure that a set of servers will only accept traffic for specific network services. You have verified that the servers are only running the necessary services, but you also want to make sure that the servers will not accept packets sent to those services.

Which tool should you use? Port scannerWhich of the following intrusion detection and prevention systems use fake resources to entice intruders by displaying a vulnerability, configuration flaw, or valuable data?

honeypotWhat does a tarpit specifically do to detect and prevent intrusion into your network? Answer connection requests in such a way that the attacking computer is stuck for a period of time ON14. 1. 9 PRACTICE EXAM SPECIFICALLY FOR YOUFOR ONLY$13. 90/PAGEOrder Now