

QUESTION 215 (NEW)

Which of the following is a characteristic of a network-based intrusion detection system (IDS)?

- A. It monitors network traffic for suspicious activity.
 - B. It is installed on a host to monitor network traffic.
 - C. It is installed on a host to monitor system activity.
 - D. It monitors network traffic for suspicious activity and generates alerts.
- Correct Answer: D
- Explanation: A network-based intrusion detection system (IDS) is designed to monitor network traffic for suspicious activity and generate alerts. It is typically installed on a central location, such as a network switch or a dedicated server, and can monitor traffic across the entire network. This allows it to detect and alert on suspicious activity that may be occurring anywhere on the network. Option A is partially correct but lacks the alerting component. Option B describes a host-based IDS. Option C describes a host-based intrusion prevention system (IPS).