QUIZ:IDS\IPS

Total points 10/10

The respondent's email (**niyigabaclaujesus@gmail.com**) was recorded on submission of this form.

✓ What is the primary function of an Intrusion Detection System (IDS)? 1/1

- ○ a) Prevent network attacks
- ◉ b) Detect and alert about suspicious activity ✓
- ○ c) Block malicious traffic
- ○ d) Encrypt network communication

✓ Which mode of Snort allows it to actively block malicious traffic? * 1/1

- ○ a) Sniffer mode
- ○ b) Packet logger mode
- ○ c) Network intrusion detection mode
- ◉ d) Inline mode ✓

✓ What type of IDS/IPS detection technique relies on predefined attack patterns? *1/1

- (●) a) Signature-based detection ✓
- ( ) b) Anomaly-based detection
- ( ) c) Heuristic-based detection
- ( ) d) Behavior-based detection

✓ Which of the following is a common open-source IDS/IPS solution? * 1/1

- ( ) a) Norton Antivirus
- (●) b) Snort ✓
- ( ) c) Wireshark
- ( ) d) Windows Defender

✓ In which layer of the OSI model does Snort operate? * 1/1

- ( ) a) Application Layer
- ( ) b) Transport Layer
- (●) c) Network Layer ✓
- ( ) d) Data Link Layer

✓ An Intrusion Prevention System (IPS) only detects threats but does not take action. *1/1

- ○ True
- ◉ False ✓

✓ Snort can function as both an IDS and an IPS. * 1/1

- ◉ True ✓
- ○ False

✓ Anomaly-based IDS/IPS systems use predefined attack signatures to detect threats. *1/1

- ○ TRUE
- ◉ False ✓

✓ Snort can analyze and filter network packets based on custom rules. * 1/1

- ◉ True ✓
- ○ False

✓ A Host-based IDS (HIDS) monitors an entire network rather than individual devices. *1/1

- ○ True
- ◉ False ✓

This content is neither created nor endorsed by Google. - Terms of Service - Privacy Policy

Does this form look suspicious? Report

Google Forms