Khaula Molapo

Computer Security Week 10

1.

Rule 1

Rule:
alert tcp any any -> any 80 (msg:"SQL Injection Attempt"; content:"' or 1=1--"; nocase; sid:1000001; rev:1;)
This Snort rule detects basic SQL injection attacks. It looks for the common malicious string ' or 1=1-- in network traffic going to port 80 (HTTP). Attackers often use this string to trick a website's database into giving unauthorized access or data.

Action (alert): tells Snort to send an alert when it matches.
Protocol (tcp): checks TCP traffic.
Ports (any -> any 80): traffic going to web servers.
Content: searches for the SQL injection pattern.
nocase: makes the search case-insensitive.
If a hacker tries to log in with this trick, Snort catches it and warns administrators. This rule helps detect common database hacking attempts early.

Rule 2

Rule:
alert icmp any any -> any any (msg:"ICMP Ping Sweep Detected"; itype:8; detection_filter:track by_src, count 5, seconds 2; sid:1000002; rev:1;)
This rule detects a ping sweep — when someone sends multiple ICMP echo requests (pings) to find active hosts on a network. Attackers use this to map targets before launching attacks.

Action (alert): generates a warning.
Protocol (icmp): monitors ping requests.
itype:8: specifies ICMP echo requests.
detection_filter: limits how many requests trigger an alert. If one IP sends 5 pings within 2 seconds, Snort raises a warning.

This logic helps detect scanning behavior quickly. It prevents false alarms from normal pings but flags suspicious fast scans. It's simple but effective in identifying reconnaissance attacks before bigger ones happen.

Rule 3

Rule:
alert tcp any any -> any 21 (msg:"FTP Brute Force Attempt"; flow:to_server,established; content:"530 Login incorrect"; detection_filter:track by_src, count 5, seconds 10;

sid:1000003; rev:1;)
This rule detects FTP brute force attacks, where an attacker tries multiple passwords quickly. It looks for repeated "530 Login incorrect" responses from an FTP server.

Action (alert): raises an alert.
Protocol (tcp): monitors TCP traffic.
Port 21: is for FTP services.
Flow: checks data from client to server.
Content: looks for failed login messages.
Detection filter: triggers if 5 failed attempts come from the same IP in 10 seconds.

This is a smart way to catch password guessing attacks without false alarms. It helps network admins act before the attacker finds a working password and gains access.

2. HIDS vs. NIDS Analysis

Feature	HIDS (Host-Based IDS)	NIDS (Network-Based IDS)	
Scope	Monitors a single host or device	Monitors entire network traffic	
Data Source	Analyzes system logs, files, and local activity	Analyzes network packets	
Visibility	Sees encrypted and local user actions	Sees overall network behavior	
Installation	Installed on each host	Deployed at network entry/exit points	
Detection Speed	Slightly slower, analyzes logs	Faster, analyzes real-time packets	
Cost	Cheaper for small systems	Can be expensive for large networks	
Maintenance	Needs updates per host	Centralized management	
Best For	Detecting insider or file-level threats	Detecting external or network threats	
Limitation	Limited to one host	Struggles with encrypted traffic	
False Positives	Fewer due to detailed context	More due to broad monitoring	

For a small e-commerce business, deploying a Network Intrusion Detection System (NIDS) should be the first priority. NIDS monitors all incoming and outgoing network traffic in real-time, which is vital for protecting a web server that handles customer data, transactions, and payments. It can detect suspicious connections, SQL injections, denial-of-service attacks, and unauthorized access attempts before they reach the web application or

database.

HIDS, while useful, works best for detecting local file changes or insider threats, which are less common for small businesses compared to external cyberattacks. Since e-commerce websites are often targeted through their network interfaces, NIDS gives wider coverage and faster detection.

NIDS tools like Snort or Suricata can monitor live traffic, log malicious attempts, and alert administrators immediately. They are easier to manage centrally and can grow with the company's needs.

Once the NIDS is running smoothly, the business can later add HIDS to servers for deeper protection. But as a first step, focusing on NIDS helps stop network-level attacks early — the most common threat for small online businesses.

3. The Target Breach (400 words)

In 2013, Target Corporation suffered one of the largest retail data breaches in history. Cybercriminals stole payment information from about 40 million customers. The attackers entered Target's network through a third-party HVAC vendor with weak security. Once inside, they installed malware on Target's point-of-sale (POS) systems to collect customer card data as transactions happened.

Target had a FireEye intrusion detection system (IDS) in place, which successfully detected the malicious activity and even sent multiple alerts to the company's security team. Unfortunately, these alerts were ignored or not escalated properly. This was the key failure — not a lack of technology, but a failure in response.

The IDS identified unusual behavior, such as data being sent to unknown servers in other countries. If the team had investigated the alerts in time, the breach could have been stopped or minimized. Instead, the attackers continued to exfiltrate data for weeks before being discovered.

This case shows that even the best IDS system is useless without a strong incident response process. Security tools can only alert; humans must act. Organizations must have well-trained teams, alert prioritization, and automated responses for critical events.

After the breach, Target upgraded its monitoring, added real-time alerting, and restructured its security operations center. The incident remains a powerful lesson that IDS effectiveness depends not only on detection accuracy but also on timely and decisive human action.