Corvit System Multan

Report

Muhammad Fatiq

Supervisor: Muhammad Bilal

SIEM

SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations.

SIEM systems help enterprise security teams detect user behavior anomalies and use artificial intelligence (AI) to automate many of the manual processes associated with threat detection and incident response.

Wazuh:

Purpose: Wazuh is a security monitoring platform that provides log analysis, intrusion detection, vulnerability detection, and compliance monitoring.

Features: It offers capabilities like file integrity monitoring, log data analysis, and real-time alerts. Wazuh is often used in conjunction with other tools, such as the Elastic Stack (Elasticsearch, Logstash, Kibana) for enhanced analysis and visualization.

Snort:

Purpose: Snort is an open-source network intrusion detection system (NIDS) that monitors network traffic for suspicious activity.

Features: It can perform real-time packet logging and analysis, detect a variety of attacks (like buffer overflows, port scans, and attacks on network services), and is highly configurable with custom rule sets.

Security Onion:

Purpose: Security Onion is a Linux distribution for intrusion detection, network security monitoring, and log management. It combines multiple open-source tools into a single platform.

Features: It integrates tools like Snort (or Suricata), Wazuh, Zeek (formerly known as Bro), the Elastic Stack, and others to provide comprehensive security monitoring, analysis, and visualization. It's designed to be a complete solution for security monitoring and incident response.

CCMP (Counter Mode with Cipher Block Chaining MessageAuthentication Code Protocol):

- **Purpose**: CCMP is an encryption protocol used in wireless networks toprovide data confidentiality, integrity, and authentication. It's part of theWPA2 (Wi-Fi Protected Access II) security standard.
- **Features**: CCMP uses the AES (Advanced Encryption Standard) cipherin counter mode for encryption and CBC-MAC (Cipher Block Chaining

  Message Authentication Code) for message integrity. It provides strongsecurity compared to older protocols like WEP.

GCM (Galois/Counter Mode):

- **Purpose**: GCM is an encryption mode that combines the AES cipherwith a Galois field multiplication for both encryption and integrity.
- **Features**: GCM provides authenticated encryption with associated data (AEAD). It offers both confidentiality (through AES encryption) and data integrity/authentication (through Galois field multiplication). It is widely used in modern cryptographic protocols due to its efficiency and securityproperties.

AES (Advanced Encryption Standard):

- **Purpose**: AES is a symmetric encryption algorithm widely used acrossvarious applications to secure data.
- **Features**: AES supports key sizes of 128, 192, or 256 bits and operateson blocks of 128 bits. It's known for its strength and efficiency and is used in a wide range of security protocols and applications, including
  CCMP and GCM.

WiFi SLAX:

- **Purpose**: It seems like "WiFi SLAX" might be a typo or misinterpretation. However, SLAX is a lightweight Linux distribution andmight be used in some security contexts, but it’s not directly related to Wi-Fi encryption.
- **Features**: If you meant something else, please provide more context,and I’d be happy to help clarify.

AJAX SPIDER:

- **Purpose**: This term might refer to a web spider or crawler that handlesAJAX (Asynchronous JavaScript and XML) content.
- **Features**: AJAX is used to load web content dynamically without refreshing the page. An AJAX spider would be designed to understandand index web content that is dynamically loaded via JavaScript, which

  can be challenging for traditional crawlers. It could be a part of a webscraping tool or security scanner.

sql injection types and their difference

1. In-band SQLi (Classic)2.Inferential SQLi (Blind)
3. Out-of-band SQLi.

In-band SQL Injection :

In-band SQL Injection is the most common and easy-to-exploit of SQL Injection attacks. In-band SQL Injection occurs when an attacker is able touse the same communication channel to both launch the attack and gatherresults.

Inferential SQLi (Blind SQLi)

Inferential SQL Injection, unlike in-band SQLi, may take longer for an attacker to exploit, however, it is just as dangerous as any other form of SQL Injection. In an inferential SQLi attack, no data is actually transferred via the web application and the attacker would not be able to see the result of an attack in-band (which is why such attacks are commonly referred to as "blind SQL Injection attacks").

Out-of-band SQLi

Out-of-band SQL Injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band SQL Injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.

Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).