Summary: Intrusion Detection Systems and Analysis of Detected Attacks

Analyzed Dataset----- Thursday_Morning_Working_Hours.csv

An **Intrusion Detection System (IDS)** is a critical component of modern cybersecurity infrastructure. It monitors system or network activity for signs of malicious behavior or policy violations. The primary objective of an IDS is to detect and alert administrators of any suspicious activities that may indicate the presence of a security threat. IDSs do not typically prevent attacks by themselves but serve as an early warning mechanism that helps in mitigating risks before they escalate into serious breaches.

There are two main types of IDS: **Signature-Based IDS** and **Anomaly-Based IDS**.

Signature-Based IDS functions similarly to antivirus software. It detects intrusions by comparing incoming traffic patterns against a database of known attack signatures. This approach is highly effective in identifying known threats with high accuracy and low false positive rates. However, it has a major limitation: it cannot detect new or unknown threats that do not match existing signatures. Therefore, it requires constant updates to remain effective.

Anomaly-Based IDS, on the other hand, uses machine learning or statistical models to define "normal" behavior within a system or network. Any deviation from this normal behavior is flagged as a potential intrusion. This approach excels at detecting zero-day attacks or previously unknown threats. However, it can produce a high number of false positives, especially if the system is not properly trained or if the baseline of "normal behavior" is not well defined.

In the analysis of the dataset provided, three specific types of attacks were identified: **SQL Injection (SQLi), Cross-Site Scripting (XSS),** and **HTTPS Brute-Force attacks**.

SQL Injection is one of the most common and dangerous web application attacks. It involves injecting malicious SQL code into input fields with the goal of manipulating backend database queries. This can lead to unauthorized data access, data modification, or even deletion. For example, by entering `' OR '1'='1` into a login form, an attacker can bypass authentication and gain administrative access.

Cross-Site Scripting (XSS) is a type of code injection attack where an attacker injects malicious scripts, usually JavaScript, into trusted websites. When other users load the affected web page, the malicious script executes in their browsers. This can result in session hijacking, credential theft, and other forms of user exploitation. XSS attacks target the users rather than the server directly, making them dangerous and often difficult to detect.

HTTPS Brute-Force Attack is a form of credential attack where an attacker repeatedly attempts to guess usernames and passwords over a secure HTTPS connection. Despite the encryption, if rate-limiting or strong password policies are not enforced, attackers can automate login attempts using dictionary or credential stuffing techniques, leading to unauthorized access.

In conclusion, **IDSs are essential tools** in detecting and responding to various forms of cyber threats. Signature-based systems provide precision for known attacks, while anomaly-based systems offer adaptability to new threats. A **hybrid IDS** combining both methods offers a comprehensive defense mechanism. The detection of SQLi, XSS, and brute-force attacks in the dataset illustrates the diversity of threats faced by systems today and highlights the importance of robust detection.