LONG TERM INTERNSHIP- CYBER SECURITY

Smart Internz

Technology stack: Cyber security with IBM Qradar

Project title: threat intelligence-strategies for proactive cyber defense

Team id: LTVIP2024TMID14858

Team size: 5

Team leader: Reddy.Hema Latha

Team member: sheik.vaheeda

Register number:SBAP0014869n

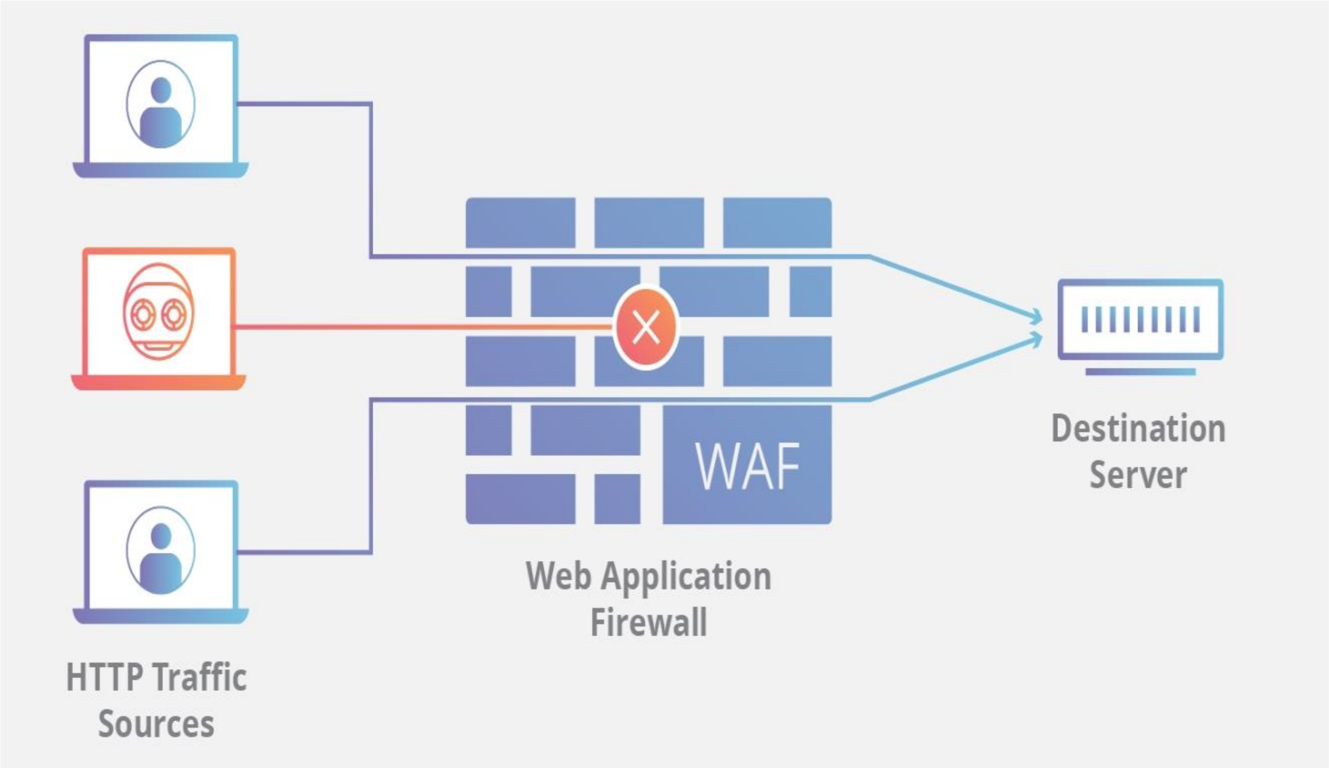
MY TASK

DEFEENSE MECHANISM DESIGN AND IMPLEMENTATION

Defence mechanismsIn recent years, there have been developments through various means for defending a vehicle against vulnerabilities and attacks. Defense mechanisms can be categorized into three groups such as Authentication and Encryption, Malware and Intrusion Detection, and Software Vulnerability.

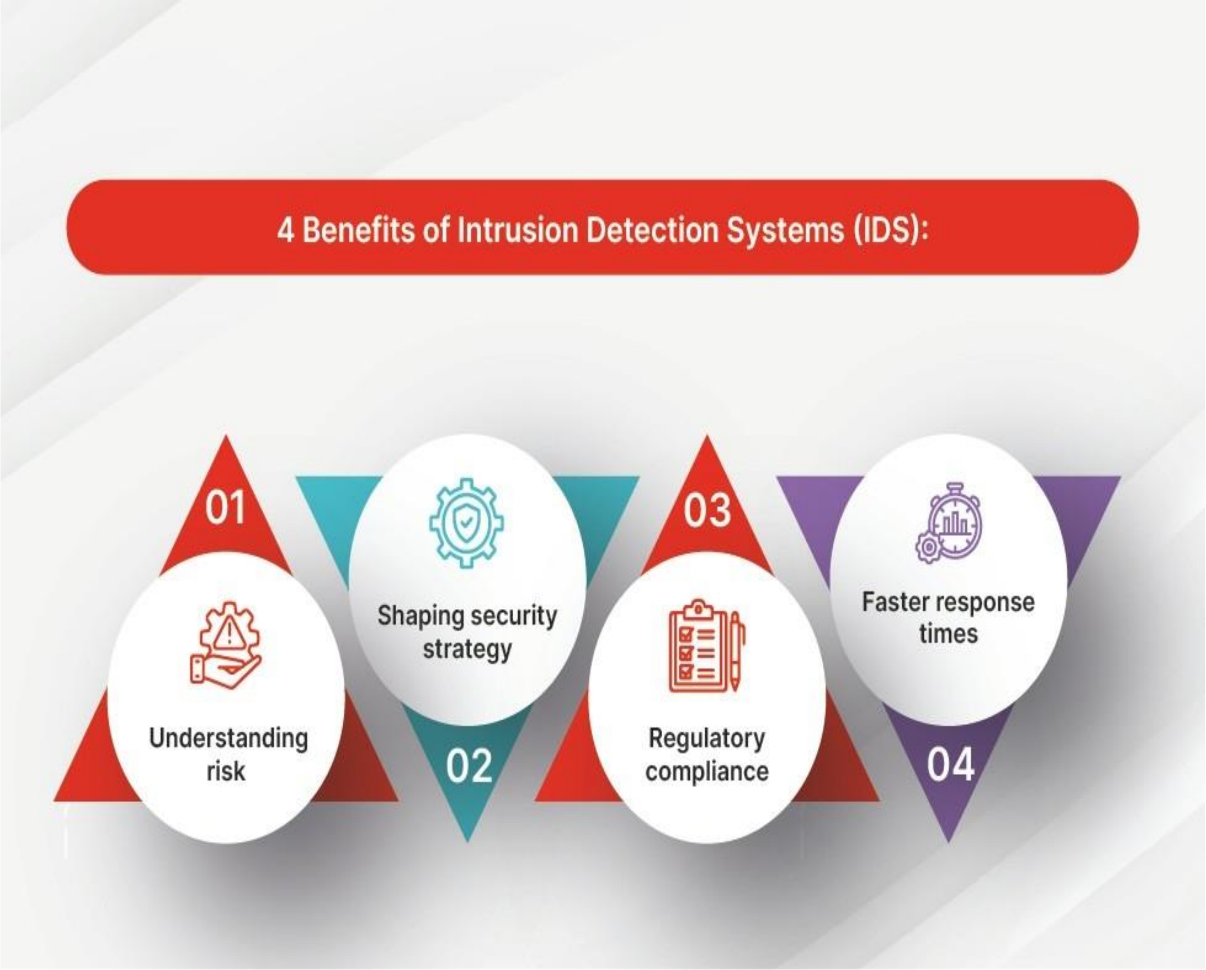
Technical defense can be encryption,firewall,anti malware and intrusion detection.

INTEGRATING WAFs and IDS



A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.

There are three primary types of WWAFs a cloud based WAF,software based WAF,hard ware based WAF.


4 Benefits of Intrusion Detection Systems (IDS):
01
Understanding risk
02
Shaping security strategy
03
Regulatory compliance
04
Faster response times

An intrusion detection system (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate threat.

DEPLOYING SSL/TLS ENCRYPTION AND SECURE COMMUNICATION PROTOCOLS

Secure Sockets Layer (SSL) is a communication protocol, or set of rules, that creates a secure connection between two devices or applications on a network. It’s important to establish trust and authenticate the other party before you share credentials or data over the internet. SSL is technology your applications or browsers may have used to create a secure, encrypted communication channel over any network. However, SSL is an older technology that contains some security flaws. Transport Layer Security (TLS) is the upgraded version of SSL that fixes existing SSL vulnerabilities. TLS authenticates more efficiently and continues to support encrypted communication channels.

SSL ensures the data that is transferred between a client and a server remains private. This protocol enables the client to authenticate the identity of the server.

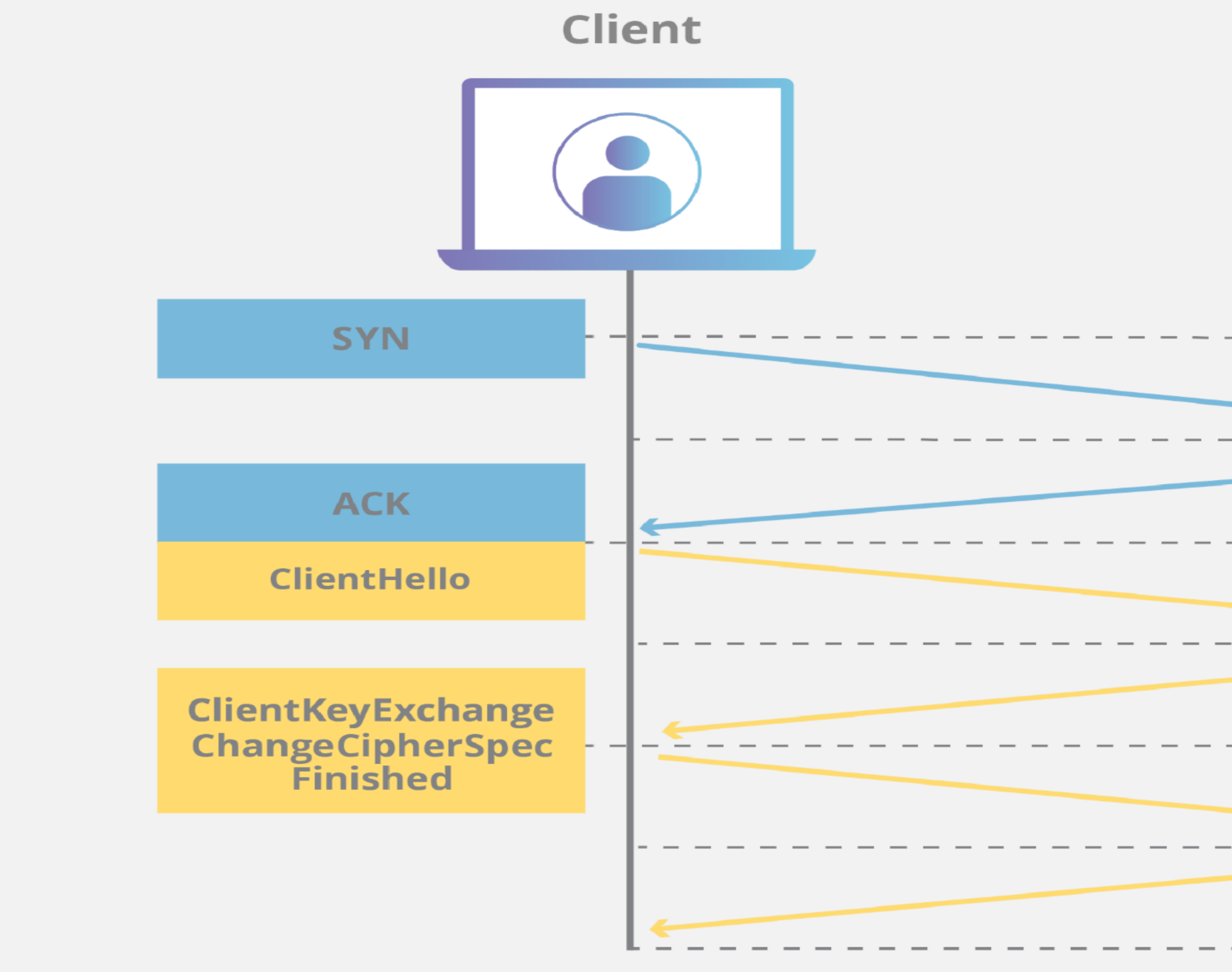
TLS(transport layer security) is a security protocol that provides privacy and integrity for internet communications.Implementing tls is a standard practice for building secure web apps.

What does TLS do?

Encryption: Hides the data being transferred from third parties

Authentication: Ensures that the parties exchanging information

Are who they claim to be



Integrity: Verifies that the data has not been forged or tampered with.

Configuring access control and user permissions:

Access control is an essential element of security that determines who is allowed to access certain data, apps and resources and in what circumstances.

User permissions part of the overall user management process are access granted to users to specific resources such as files ,applications, networks or devices

User permissions can also specify

The type of access: for example a user might be allowed to read data without modifying it or be allowed to read and right data.

Specific functions a user can access :for example most systems have an administrative role that allows users to change configuration

CONCLUSION

Mastering web security equips organisations with the knowledge and tools necessary to fortify their websites against cyber Threats safeguard sensitive data and maintain trust with users in an increasingly digital world.