Group Task :2

OS Layer 07

A Brief Overview

02

1.Sandip Narbat
2. Sai Kumar

Analyze a real world case study of an attacks on layer 7 (Application Layer) of the OSI model

Application Layer

Layer 7 of the OSI (Open Systems Interconnection) model is the Application layer. A network protocol stack's operations are described by the OSI model, a conceptual framework. It is broken down into seven layers, each of which is in charge of a different communication-related duty.

The OSI model's top layer, the Application layer, is in charge of giving user applications access to the network. Applications can use it to access network resources and services. This layer offers services including file transfer, email, online browsing, remote login, and network management while interacting directly with software programmer.

To establish communication between applications on various networked devices, the application layer employs a variety of protocols. At this layer, HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), and DNS (Domain Name System) are some of the regularly used protocols for online browsing, email delivery, file transfers, and name resolution.

Impact of attack on Application Layer:

A network or system may be significantly impacted by an attack on Layer 7, or the application layer, of the OSI model. Denial of service may occur as a result, making the programme slow or inaccessible to authorised users. The application may include vulnerabilities that can be used to gain access without authorization, disclose information, or cause data breaches. Attackers are able to modify data, impersonate users, and hijack user sessions. Phishing and social engineering, in which attackers trick users into giving over sensitive information, are other common uses of Layer 7 attacks. An organization's reputation and trustworthiness may be harmed by these attacks. Regular security testing, the installation of firewalls and intrusion prevention systems, the use of web application firewalls, and the promotion of secure coding techniques are examples of mitigation methods. Training in user awareness is essential to preventing falls.

Consequiences of attacks on Application layer:

- Service disruption: At the application layer, attackers can conduct Denial of Service (DoS) or Distributed Denial of Service (DDoS) assaults. This could slow down or render the application unavailable by flooding it with a large number of requests or malicious traffic. As a result, legitimate users are denied access to the service, which disrupts corporate operations.

- Data breaches: It occur as a result of attacks that target application layer flaws. Attackers may get unauthorised access to sensitive data, including personal information, financial information, or intellectual property, by taking advantage of flaws in the application's code or settings. The privacy and security of people or organisations may be jeopardised as a result of the theft or exposure of sensitive information.

- Unauthorized Access: Application-layer attacks can take advantage of flaws to obtain access to systems or user accounts without authorization. Attackers may get around authentication protocols, mess with session management, or take advantage of lax access limits. This may lead to data tampering, theft, or destruction that is not authorised, as well as unlawful acts taken on behalf of authorised users.

- Application Defacement: Some assaults try to alter the look or content of a website or an application. This can involve displaying false information, changing functionality, or replacing legitimate content with malicious or offensive stuff. Application defacement can harm a company's reputation, trustworthiness, and brand perception.

Countermeasures Employed :

- Frequent Security Assessments: To find and fix application layer vulnerabilities, conduct routine security assessments, such as vulnerability scanning and penetration testing. This aids in finding holes and fixing them before attackers take advantage of them.

- Secure Coding Techniques: Use secure coding techniques when developing applications. This entails employing safe development frameworks, doing code reviews, and adhering to secure coding standards. Techniques for output encoding, session management, and input validation can all be used to reduce typical security flaws. With web application firewalls (WAFs), you can defend against

- Install a web application firewall: To defend against common Layer 7 vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Before potential attacks reach the application, WAFs examine incoming traffic, weed out malicious requests, and block any such attempts.

- Use intrusion detection and prevention systems (IDPS): At the application layer to identify and prevent intrusions. These systems keep an eye on network activity, spot suspicious behaviour or well-known attack patterns, and take immediate preventative measures to thwart or lessen attacks.

THANK YOU