Web Security+Firewalls

Web Security:

SQL Injection:

An attacker can manipulate an SQL query via the input data from the client, forcing the SQL server to execute an unintended operation constructed using an untrusted input.

Cross-site scripting XSS

An attacker sends input JavaScript tags to a web application. When this input is returned to the user unsanitized, the user's browser would execute it. XSS can be as simple as crafting a link and persuading a user to click on it. The script could post the user's cookies to the attacker when they load the webpage.

XSS Types:

- Reflected XSS - Where the malicious script comes from the current HTTP request
- Stored XSS - Where the malicious script comes from the website's database
- DOM-Based XSS - Where the vulnerability exists in client-side code rather than server-side code

Firewalls:

A firewall is a device that filters traffic between a protected network and a less trustworthy network. Usually, a firewall runs on a separate device and acts as a single point through which all traffic is channelled. Firewall code usually runs on a proprietary minimized operating system limiting security problems.

- "That which is not expressly forbidden is permitted" - default permit
- "That which is not expressly permitted is forbidden" - default deny

Capabilities:

- The focal point for monitoring traffic
- Central point for access control
- Limits the damage a network security problem can do to the overall network

Incapabilities:

- Protects against malicious insiders
- Protect a connection that doesn't go through it
- Protect against new threats
- Protect against viruses/trojans

Firewall Goals:

- All traffic from inside to outside and vice versa, must pass through the firewall. All other traffic is blocked.
- Only authorized traffic, as defined by the local security policy is allowed to pass.
- The firewall itself is immune to penetration.

Only authorized traffic as defined by the local security policy will be allowed to pass through the firewalls. It's assumed that the firewall itself is immune to penetration.

Enforcing Policy:

- Service Control - Determines the types of internet services that can be accessed
- Direction Control - Determines the direction in which particular service requests are allowed (Upload/Download)
- User Control - Controls access to a service according to which user is attempting to access it. IP-based filtering or authentication with IPsec.

Firewall Types:

- Packet filtering - Network Layer - IP
- Circuit level gateway - Transport Layer - TCP
- Stateful inspection firewall
- Application level gateway

Packet Filtering:

Controls access to packets on the basis of packet address (source/destination) or specific protocol type such as HTTP web traffic. Packet filtering is stateless and very fast. However it doesn't support advanced user authentication schemes, and it cannot block specific application commands. It also lacks upper-layer functionality. Packet filtering can be easily bypassed using IP spoofing.

Application Level Gateway:

Also known as an application proxy, they act as a relay of application-level traffic rather than trying to deal with all the possible combinations of addresses and protocols that are forbidden at the IP level, the application-level gateway needs only scrutinize a few allowable applications. A prime disadvantage is that it adds significant overhead to the network as it splices the connections forwarding input and outward traffic. It filters traffic at the application layer specific to applications which are configured. It offers a higher level of network security.

Stateful Inspection:

It maintains the state information from one packet to another on the input stream. A stateful inspection firewall will track the sequence of packets and conditions from one packet to another.

Circuit Level Gateway:

A circuit-level gateway does not permit an end-to-end TCP connection, the security function consists of determining which connections will be allowed. It can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications.

Intrusion Detection Systems:

An IDS is a device that typically is a separate computer that monitors activity to identify malicious or suspicious events.

IDS Functions:

- Monitoring users and system activity
- Auditing system configuration for vulnerabilities and misconfigurations
- Assessing the integrity of critical systems
- Recognising known attack patterns
- Identifying abnormal activity through statistical analysis

Types of IDS

- Signature-Based - IDS use simpling pattern matching to detect known attacks
- Heuristic - Use statistical analysis to detect abnormal behaviours.

IDS Methods:

- Filter packet headers
- Filter packet content
- Maintain connection state
- Use complex, multipacket signatures
- Filter in realtime
- Use optimal sliding time window size to match signatures.

Intrusion Prevention System = Intrusion Detection System + Firewall