Types of attacks in the OSI model by layer

OSI model layer	Type of attack
Application layer	Exploit
Presentation layer	Phishing
Session layer	Hijacking
Transport layer	Reconnaissance / DoS
Network layer	Man-in-the-middle
Data link layer	Spoofing
Physical layer	Sniffing

Exploit on the application layer

An exploit on the application layer refers to a type of cyber-attack that targets vulnerabilities in software applications or services. This attack takes advantage of weaknesses in the design, coding, or configuration of the application itself.

Procedure for an application layer exploit:

1. Reconnaissance: The attacker gathers information about the target application, such as its version, underlying technologies, and potential vulnerabilities.
2. Vulnerability identification: The attacker identifies specific vulnerabilities in the application. This can be done through various means, including manual analysis, automated scanning tools, or by leveraging publicly known vulnerabilities.
3. Exploit development: Once vulnerabilities are identified, the attacker creates or obtains an exploit that can take advantage of the specific weakness. This could involve crafting malicious input or creating code that triggers a vulnerability.
4. Delivery: The attacker finds a way to deliver the exploit to the target application. This can be done through techniques like phishing emails, malicious links, compromised websites, or exploiting other vulnerabilities in the system.

5. Execution: The exploit is executed, taking advantage of the vulnerability within the application. This could result in various consequences, such as unauthorized access, data breaches, privilege escalation, or the execution of malicious code on the target system.
6. Persistence and control: If successful, the attacker may attempt to maintain access to the compromised system for further exploitation or to establish a foothold for future attacks.
7. Covering tracks: To avoid detection, the attacker may attempt to erase evidence of the attack, modify logs, or use other techniques to hide their presence.

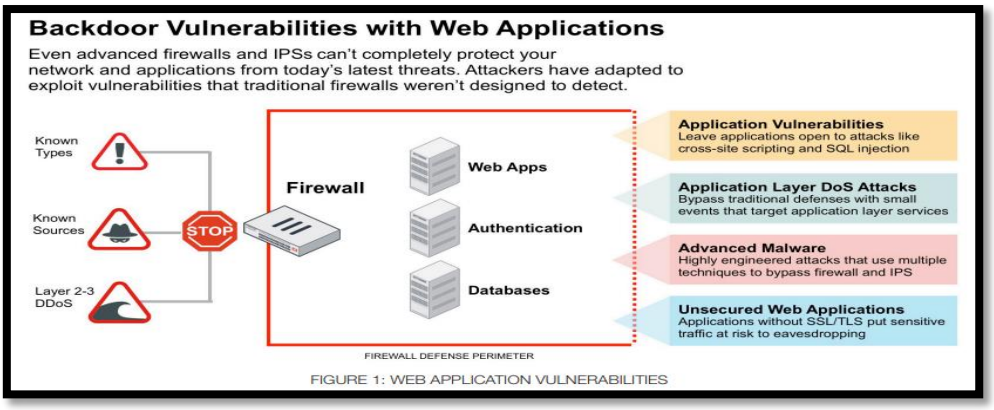


FIGURE 1: WEB APPLICATION VULNERABILITIES

Phishing attacks on the presentation layer

Phishing attacks on the presentation layer involve manipulating the visual elements presented to users, typically through email or websites, to deceive them into providing sensitive information or performing malicious actions. This type of attack aims to trick users into believing they are interacting with a legitimate source.

Procedure for a phishing attack on the presentation layer:

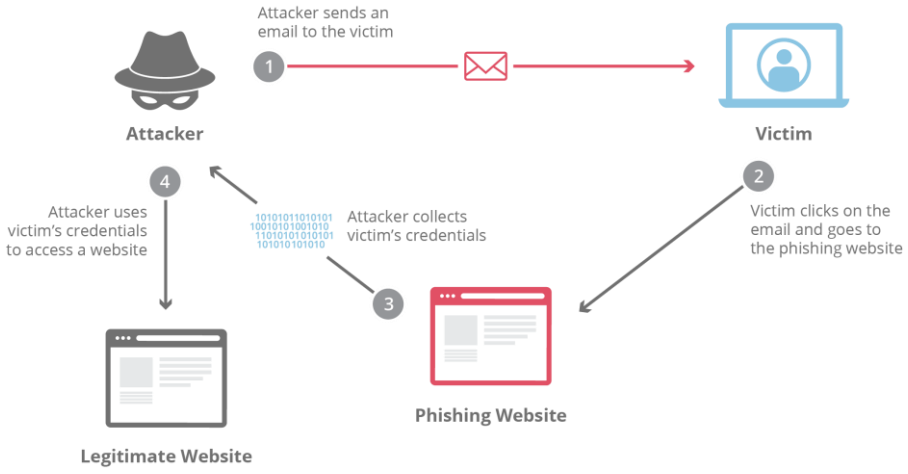
1. Preparation: The attacker selects a target audience and determines the goal of the phishing attack, such as stealing login credentials, financial information, or spreading malware.
2. Spoofing: The attacker creates a deceptive email or website that imitates a trusted entity, such as a well-known company, financial institution, or government agency. They use social engineering techniques to make the communication appear legitimate, often including official logos, email addresses, or website designs.

3. Delivery: The attacker sends out phishing emails or lures victims to visit the spoofed website. They may use tactics like urgency, fear, or incentives to entice users into taking action, such as clicking a link, downloading an attachment, or entering personal information.

4. Deception: When the victim interacts with the phishing email or website, they are presented with a fraudulent interface that closely mimics the legitimate source. The attacker may request sensitive information like usernames, passwords, credit card details, or ask the victim to perform certain actions that benefit the attacker.

5. Information Harvesting: As victims unwittingly provide their sensitive information or perform requested actions, the attacker captures and collects the data for their malicious purposes. This can include using the stolen credentials for unauthorized access, identity theft, or selling the information on the black market.

6. Covering tracks: To avoid detection, the attacker may try to erase traces of their activity, remove the phishing infrastructure, or use anonymization techniques to hide their identity and location.



Hijacking attacks on the session layer

Hijacking attacks on the session layer involve unauthorized interception or manipulation of established communication sessions between two parties. These attacks aim to gain control over an ongoing session, allowing the attacker to eavesdrop on sensitive information, inject malicious content, or impersonate one of the parties involved.

Procedure for a hijacking attack on the session layer:

1. Session establishment: The legitimate parties initiate a session by establishing a connection and exchanging session-specific information, such as session IDs, cookies, or tokens.

2. Session monitoring: The attacker monitors the communication channels to identify sessions of interest. They may employ techniques like sniffing network traffic or exploiting vulnerabilities in the underlying protocols.

3. Session hijack: Once a target session is identified, the attacker attempts to hijack it by either:

    a. Session hijacking: The attacker intercepts and steals the session-specific information, such as session IDs or cookies, from the legitimate user. This can be done through techniques like session side jacking, where the attacker captures the session data over an insecure network.
    b. Session replay: The attacker captures a legitimate session and replays it to gain unauthorized access to the system. This involves reusing captured session data, such as session IDs, to impersonate the legitimate user.
    c. Man-in-the-Middle (MitM): The attacker positions themselves between the legitimate parties, intercepting and altering the communication. This allows them to eavesdrop on sensitive information, modify data in transit, or inject malicious content.

4. Exploitation: With control over the session, the attacker can perform various malicious actions, such as accessing sensitive data, modifying transactions, executing unauthorized commands, or injecting malware into the session.

5. Persistence and control: If the attacker's objective is to maintain control over the compromised session, they may employ techniques like session fixation, where they force the legitimate user to use a session ID controlled by the attacker.

6. Covering tracks: To avoid detection, the attacker may attempt to erase evidence of their presence, modify logs, or use encryption and anonymization techniques to

conceal their activities.

Reconnaissance on the transport layer

Reconnaissance on the transport layer refers to the process of gathering information about network communication patterns, protocols, and vulnerabilities to potentially exploit or compromise the transport layer of a network.

Procedure for reconnaissance on the transport layer:

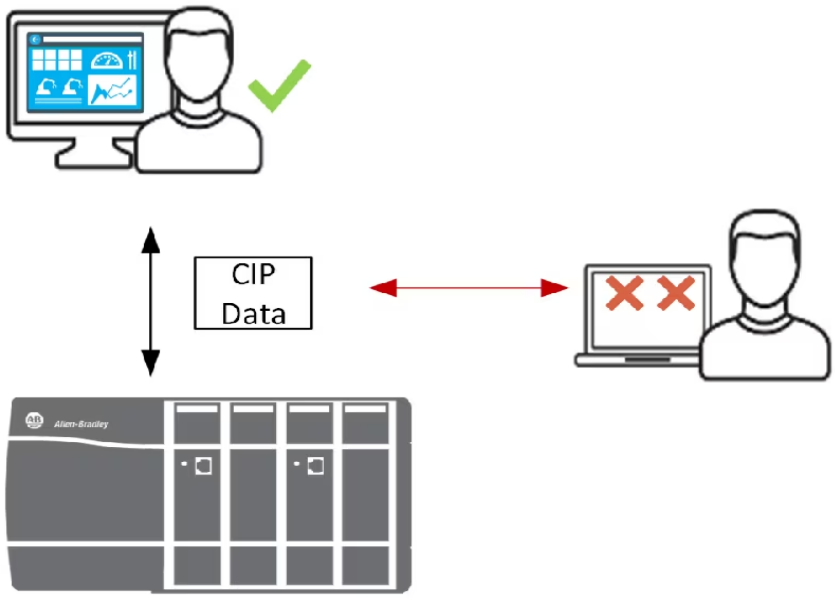
1. Network scanning: The attacker conducts network scanning using tools like port scanners to identify active systems, open ports, and services running on those ports. This helps in mapping the network infrastructure and identifying potential targets.

2. Port and service enumeration: Once the open ports are identified, the attacker performs port and service enumeration to determine the specific protocols and services running on those ports. This can provide valuable information about potential vulnerabilities or weaknesses associated with specific protocols.

3. Traffic analysis: The attacker captures and analyses network traffic to gain insights into the communication patterns, protocols in use, and potential vulnerabilities. This can involve techniques like packet sniffing or network monitoring to intercept and analyse the data packets flowing through the network.

4. Protocol analysis: The attacker analyses the behaviour, security mechanisms, and potential vulnerabilities of specific transport layer protocols, such as TCP (Transmission Control Protocol) or UDP (User Datagram Protocol). They may study protocol specifications, known vulnerabilities, or publicly available information to identify weaknesses that can be exploited.

5. Vulnerability identification: Based on the gathered information from network scanning, port enumeration, traffic analysis, and protocol analysis, the attacker identifies potential vulnerabilities or weaknesses in the transport layer. These vulnerabilities can include misconfigurations, outdated protocols, weak encryption, or improper handling of network traffic.
6. Exploitation: Once vulnerabilities are identified, the attacker may attempt to exploit them to gain unauthorized access, perform packet manipulation, conduct denial-of-service attacks, or intercept sensitive data flowing through the network.
7. Covering tracks: To avoid detection, the attacker may attempt to erase evidence of their reconnaissance activities, modify logs, or use techniques to hide their presence, such as anonymization or encryption.



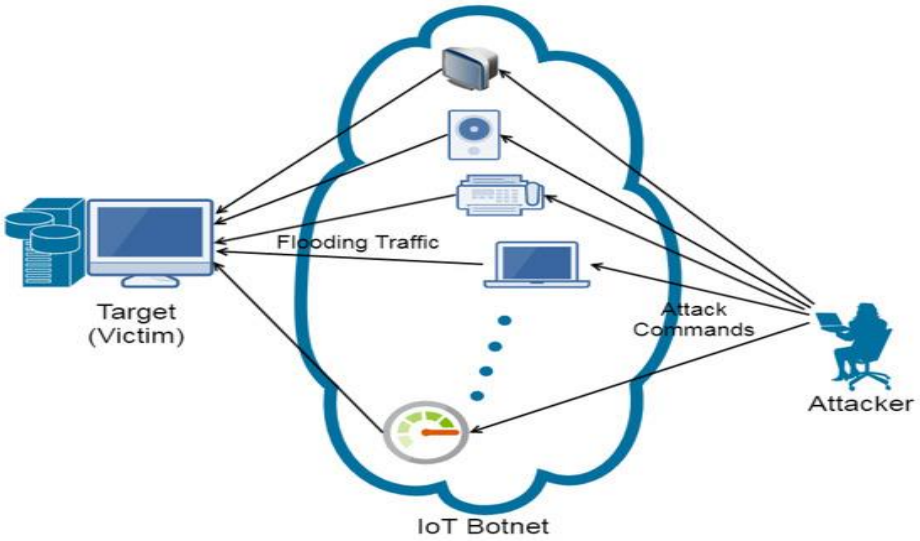
DoS attacks on the transport layer

Denial-of-Service (DoS) attacks on the transport layer aim to disrupt or disable network services by overwhelming or exploiting vulnerabilities in the underlying transport layer protocols. These attacks render the targeted system or network unable to respond to legitimate requests.

Procedure for a DoS attack on the transport layer:

1. Target selection: The attacker selects a specific target, such as a server, network infrastructure, or service, that relies on transport layer protocols like TCP or UDP.

2. Traffic flooding: The attacker initiates a massive influx of traffic towards the target, overwhelming its network resources or depleting its processing capabilities. This can be achieved through various means, including:
    a. SYN flood: The attacker sends a large number of TCP SYN requests to the target, exhausting its resources and preventing it from establishing new connections.
    b. UDP flood: The attacker sends a flood of UDP packets to the target, consuming its bandwidth and causing the target to expend resources processing the packets.
    c. Amplification attack: The attacker sends a small number of crafted requests to vulnerable servers or devices that, in turn, generate and amplify a much larger volume of traffic towards the target. This magnifies the impact of the attack.
3. Connection exhaustion: The attacker exploits vulnerabilities in the target's transport layer implementation to exhaust its connection resources. For example, they may send a series of malformed or maliciously crafted packets that consume the target's connection table or memory.
4. Protocol exploitation: The attacker identifies weaknesses or vulnerabilities in the target's transport layer protocols and exploits them to disrupt its normal operation. This can involve exploiting flaws in protocol handling, resource allocation, or congestion control mechanisms.
5. Service disruption: As the target becomes overwhelmed with the flood of traffic or resources are depleted, it becomes unable to handle legitimate requests, leading to service disruption or complete unavailability.
6. Mitigation evasion: The attacker may employ techniques like IP address spoofing, distributed attacks using a botnet, or employing reflection/amplification techniques to make it difficult for the target to block or filter the attack traffic.



Man-in-the-middle attacks on the network layer

Man-in-the-Middle (MitM) attacks on the network layer involve an attacker intercepting and manipulating the communication between two parties by positioning themselves between them. This allows the attacker to eavesdrop on the communication, modify data in transit, and potentially impersonate one or both parties involved.

Procedure for a Man-in-the-Middle attack on the network layer:

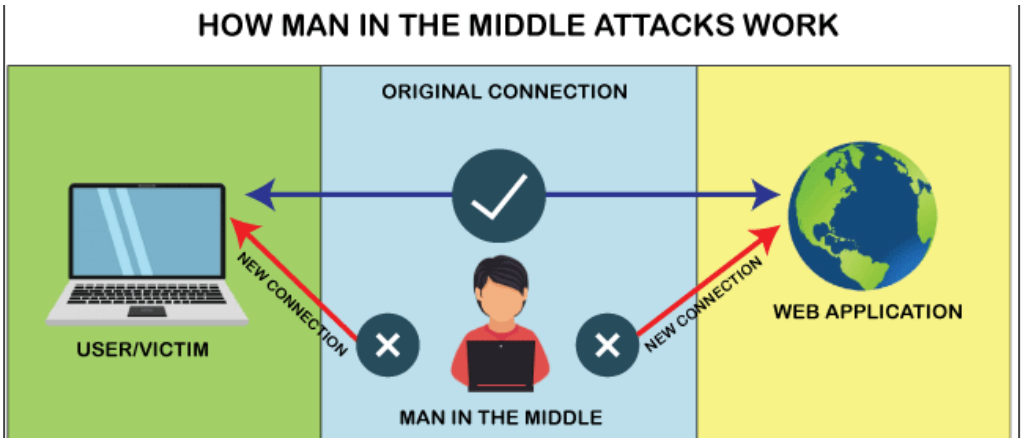
1. Network interception: The attacker positions themselves within the network infrastructure, typically by gaining unauthorized access to a network segment or by compromising an intermediate device, such as a router or switch.
2. ARP spoofing or DNS spoofing: The attacker may employ techniques like Address Resolution Protocol (ARP) spoofing or Domain Name System (DNS) spoofing to redirect network traffic through their own system. This involves tricking the legitimate parties into sending their traffic to the attacker's device, thinking it is a legitimate destination.
3. Eavesdropping: As the network traffic flows through the attacker's device, they intercept and capture the data packets, allowing them to eavesdrop on the communication between the legitimate parties. This can include capturing sensitive information like usernames, passwords, or other confidential data.
4. Data manipulation: With control over the intercepted network traffic, the attacker can modify the data packets before forwarding them to the intended recipient. This enables

them to alter the content of the communication, inject malicious code, or execute other unauthorized actions.

5. Session hijacking: If the attacker successfully intercepts a session between the legitimate parties, they can hijack the session by stealing session-specific information (e.g., session cookies) or by taking over the session itself. This allows the attacker to gain unauthorized access to the session and potentially impersonate one of the parties.

6. Impersonation: In some cases, the attacker may impersonate one or both parties involved in the communication. By intercepting the traffic, they can forge responses to the legitimate parties, tricking them into believing they are communicating with the intended party when, in fact, they are communicating with the attacker.

7. Covering tracks: To avoid detection, the attacker may attempt to erase evidence of their presence, modify logs, or use techniques like encryption or anonymization to hide their activities and maintain persistence within the network.



Spoofing attacks on the data link layer

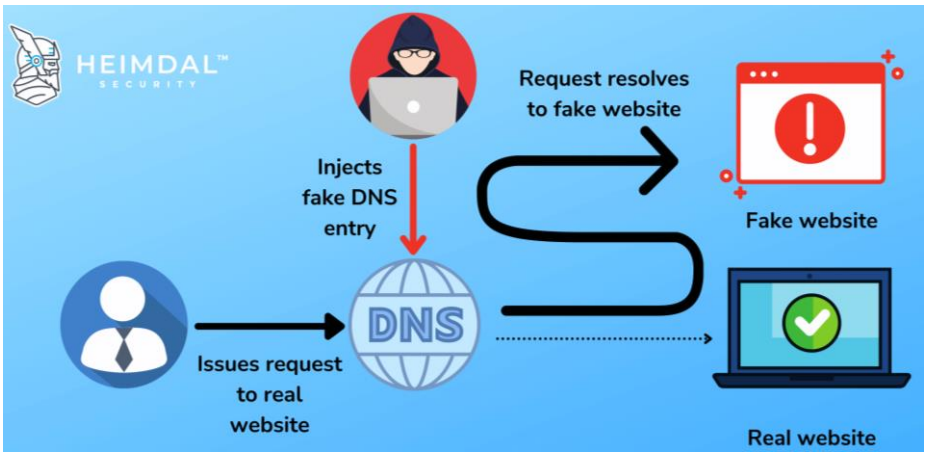
Spoofing attacks on the data link layer involve an attacker impersonating a legitimate device or manipulating data link layer protocols to deceive the network and gain unauthorized access or disrupt communication. These attacks exploit vulnerabilities in the data link layer to deceive network devices or compromise network integrity.

Procedure for a spoofing attack on the data link layer:

1. MAC address spoofing: The attacker spoofs the Media Access Control (MAC) address of their device to impersonate a legitimate device on the network. The MAC address is a unique identifier associated with the network interface card (NIC) of a device.
2. Address Resolution Protocol (ARP) spoofing: The attacker uses ARP spoofing techniques to manipulate the ARP cache of network devices. By sending fake ARP messages, the attacker associates their own MAC address with the IP address of a legitimate device, redirecting traffic intended for that device to their own system.
3. Address caching: Once the attacker successfully spoofs the MAC or ARP cache, they intercept and capture network traffic intended for the legitimate device. This allows them to eavesdrop on the communication or manipulate the data being transmitted.
4. Traffic interception or modification: With control over the network traffic, the attacker can intercept and inspect the data packets or modify them before forwarding them to the intended recipient. This can involve altering the content of the communication, injecting malicious code, or executing unauthorized actions.
5. Impersonation: By spoofing the MAC address or manipulating ARP, the attacker can impersonate a legitimate device on the network. This can enable them to gain unauthorized access to network resources, perform man-in-the-middle attacks, or conduct further exploits.
6. Disruption of network connectivity: The attacker can disrupt network connectivity by flooding the network with spoofed MAC or ARP messages, causing network devices to

update their ARP caches or MAC address tables with incorrect information. This can lead to communication failures or denial of service.

7. Covering tracks: To avoid detection, the attacker may attempt to erase evidence of their activities, modify logs, or use techniques to hide their presence, such as MAC address randomization or encryption.



Sniffing attacks on the physical layer

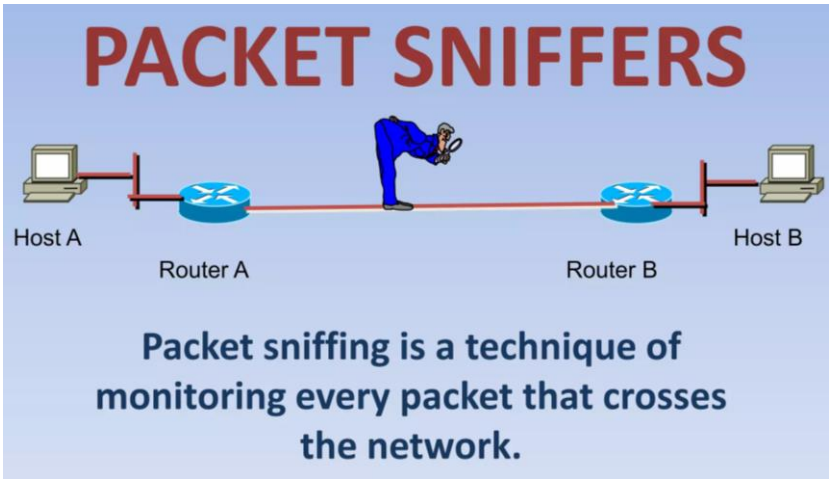
Spoofing attacks on the data link layer involve an attacker impersonating a legitimate device or manipulating data link layer protocols to deceive the network and gain unauthorized access or disrupt communication. These attacks exploit vulnerabilities in the data link layer to deceive network devices or compromise network integrity.

Procedure for a spoofing attack on the data link layer:

1. MAC address spoofing: The attacker spoofs the Media Access Control (MAC) address of their device to impersonate a legitimate device on the network. The MAC address is a unique identifier associated with the network interface card (NIC) of a device.
2. Address Resolution Protocol (ARP) spoofing: The attacker uses ARP spoofing techniques to manipulate the ARP cache of network devices. By sending fake ARP messages, the attacker associates their own MAC address with the IP address of a legitimate device, redirecting traffic intended for that device to their own system.
3. Address caching: Once the attacker successfully spoofs the MAC or ARP cache, they intercept and capture network traffic intended for the legitimate device. This allows them to eavesdrop on the communication or manipulate the data being transmitted.
4. Traffic interception or modification: With control over the network traffic, the attacker can intercept and inspect the data packets or modify them before forwarding them to

the intended recipient. This can involve altering the content of the communication, injecting malicious code, or executing unauthorized actions.

5. Impersonation: By spoofing the MAC address or manipulating ARP, the attacker can impersonate a legitimate device on the network. This can enable them to gain unauthorized access to network resources, perform man-in-the-middle attacks, or conduct further exploits.
6. Disruption of network connectivity: The attacker can disrupt network connectivity by flooding the network with spoofed MAC or ARP messages, causing network devices to update their ARP caches or MAC address tables with incorrect information. This can lead to communication failures or denial of service.
7. Covering tracks: To avoid detection, the attacker may attempt to erase evidence of their activities, modify logs, or use techniques to hide their presence, such as MAC address randomization or encryption.



REFERENCE:

https://medium.com/@e.ahmadi/attacks-on-various-osi-model-layers-bd2fac5ab985

https://www.semanticscholar.org/paper/Various-OSI-Layer-Attacks-and-Countermeasure-to-the-Kaur-Singh/b67469796cc7b90175544c45cc67ffa2593f677e

https://www.publications.scrs.in/uploads/final_menuscript/abe7e081dcdfc00ade4241a091b10607.pdf