Comprehensive Analysis Of Attack On the OSI Model: Case Studies and Report.

By Team Fressia:

I. Overview:

OSI model :

- Stands for open system interconnection.
- It is a conceptual framework which helps in understanding the working of network protocols.
- It contains 7 layers namely : Physical, Data link, Network, Transport, Session, Presentation, Application .
- It was developed by ISO in 1970s.
- Each layer serves specific functions identical to them only.
- The data is passed down and up in layers.
- Common protocols associated with each layer include Ethernet, IP, TCP, HTTP, and more

Each layer and its working :

1. **Physical layer:**
    - It transmits raw bits over physical medium .
    - It also converts electrical, optical signals to digital signals and vice versa.
    - Ethernet is a protocol used for setting up LAN.
    - Wi-fi is a wireless communication standard that enables devices to connect to a network without physical cables.
    - Physical layer also performs multiplexing
    - Also performs error detection and correction.
    - Devices: NIC Card, Hubs, Repeater.
    - Physical media types used are Twisted Pair, Fiber Optic, Coaxial Cable, Wireless.
    -

2. **Data Link Layer:**
    - Responsible for error-free transmission of data frames over a physical link.
    - Provides logical addressing through MAC (Media Access Control) addresses.
    - Performs framing, flow control, and error detection.
    - Protocols: Ethernet (IEEE 802.3), Point-to-Point Protocol (PPP).
    - Techniques: Media access control, framing, error detection.
    - Devices: Network Interface Card (NIC), switches, bridges.

3. Network Layer:

- Handles logical addressing and routing of data packets across different networks.
- Translates logical IP addresses to physical MAC addresses.
- Determines the best path for data delivery using routing algorithms.
- Protocols: Internet Protocol (IP), Internet Control Message Protocol (ICMP).
- Techniques: Logical addressing, routing.
- Devices: Routers, Layer 3 switches.

4. Transport Layer:

- Ensures reliable, end-to-end data delivery and error recovery.
- Divides data into smaller segments and reassembles them at the destination.
- Manages flow control and congestion control.
- Protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP).
- Techniques: Segmentation, error recovery, flow control.
- Devices: Gateways, firewalls.

5. **Session Layer:**

- Establishes, manages, and terminates communication sessions between applications.
- Synchronizes dialogue and supports session checkpointing and recovery.
- Handles session establishment, authentication, and termination.
- Protocols: Remote Procedure Call (RPC), NetBIOS.
- Techniques: Session establishment, synchronization.
- Devices: Not applicable (software layer).

6. Presentation Layer:

- Focuses on data representation and encryption for application-layer compatibility.
- Translates data formats between different systems.
- Handles data compression and decompression.
- Protocols: JPEG (image compression), MPEG (video compression), SSL/TLS.
- Techniques: Data representation, encryption, compression.
- Devices: Not applicable (software layer).

7. Application Layer:

- Interacts directly with user applications and provides network services.
- Offers a wide range of services such as file transfer (FTP), email (SMTP, POP3, IMAP), and web browsing (HTTP).
- Supports application-specific protocols and data formats.
- Protocols: HTTP, SMTP, FTP, DNS.
- Techniques: Application-specific protocols, data formats.
- Devices: Not applicable (software layer).

These bullet points provide an overview of the remaining layers of the OSI model, their functions, associated protocols, techniques, and devices used.

Encapsulation:

- Encapsulation is the process of enclosing data and related information within a protocol-specific wrapper or
container for transmission over a network.

Protocol Data Unit(PDU):

- unit of data at each layer of the protocol (OSI & TCP/IP).

Encapsulation at layer's

1. Application Layer
   – Add application-specific data and headers.
   – Encapsulate the data into a message.
2. Transport Layer
   – Add transport layer header with source and destination port numbers.
   – Encapsulate the message into a segment or datagram.
3. **Network Layer**
   – Add network layer header with source and destination IP addresses.
   – Encapsulate the segment or datagram into a packet.
4. **Data Link Layer**
   – Add data link layer header and trailer with source and destination MAC addresses.
   – Encapsulate the packet into a frame.
5. **Physical Layer**
   – Convert the frame into a stream of bits.
   – Transmit the bits over the physical medium.

Benefits:

- Standardization: Ensures interoperability between different vendors' products.
- Modularity: Allows for easy development and modification of specific layers.
- Troubleshooting: Simplifies problem isolation and resolution.
- Protocol Development: Facilitates the creation of new protocols.
- Education and Understanding: Aids in comprehending network protocols and technologies.
- Comparison with TCP/IP: OSI model provides a comprehensive framework, better interoperability, modularity, troubleshooting, and protocol development support.

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.

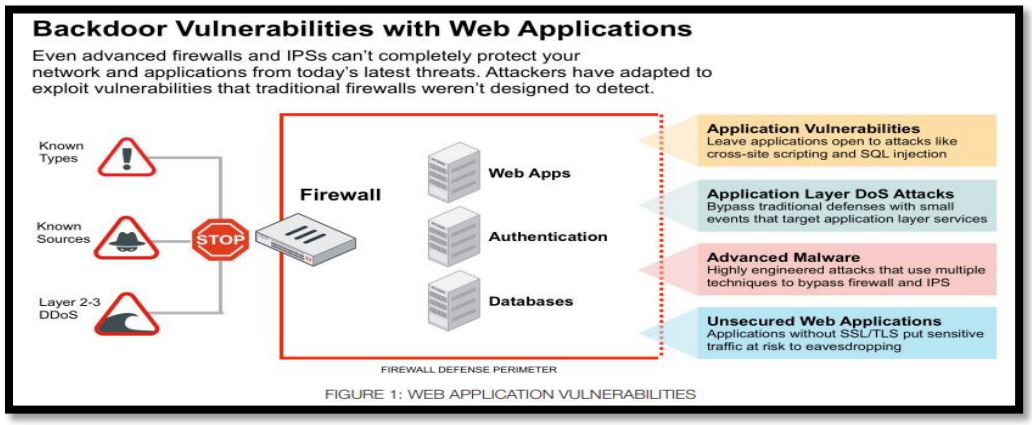


FIGURE 1: WEB APPLICATION VULNERABILITIES

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.

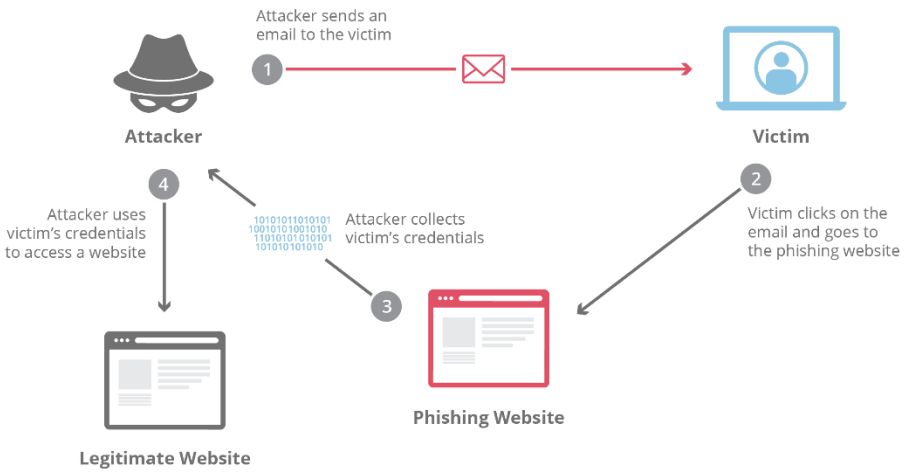
2. **Spoofing:** The attacker creates a deceptive email or website that imitates a trusted entity, such as a well-known company, financial institution, or government agency. They use social engineering techniques to make the communication appear legitimate, often including official logos, email addresses, 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.

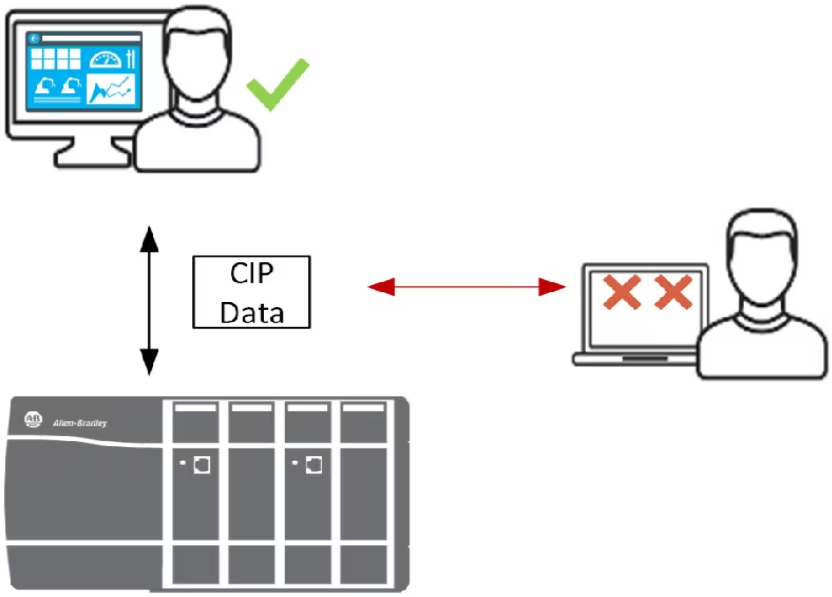
3. **Traffic analysis:** The attacker captures and analyses network traffic to gain insights into the communication patterns, protocols in use, and potential vulnerabilities. This can involve techniques like packet sniffing or network monitoring to intercept and analyse the data packets flowing through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

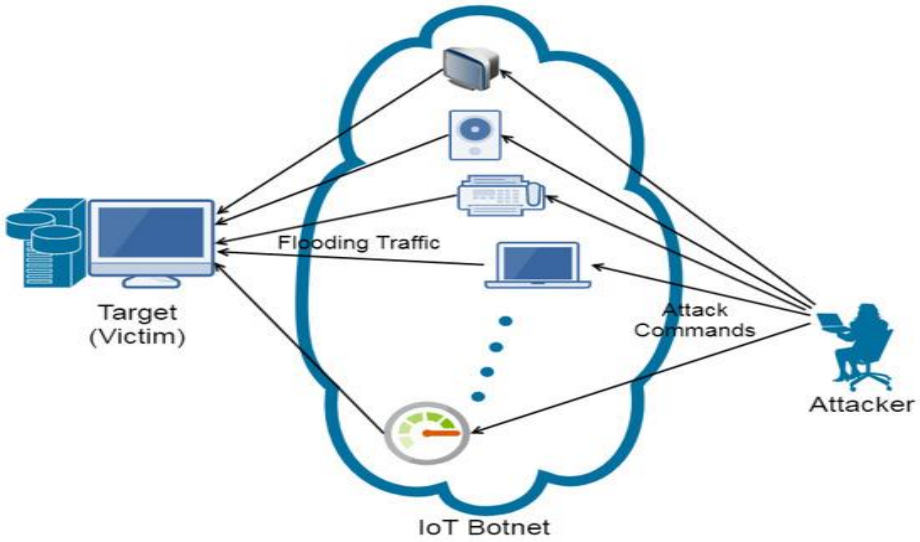
a. **SYN flood:** The attacker sends a large number of TCP SYN requests to the target, exhausting its resources and preventing it from establishing new connections.
b. **UDP flood:** The attacker sends a flood of UDP packets to the target, consuming its bandwidth and causing the target to expend resources 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.

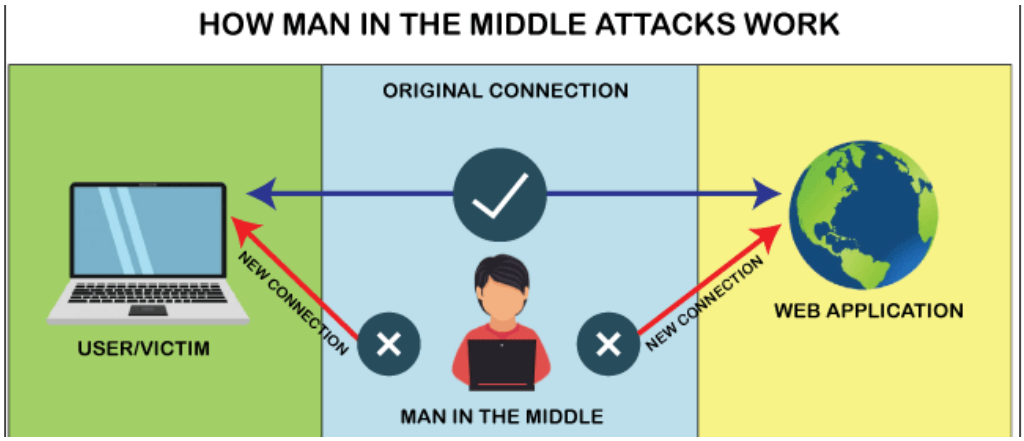
3. **Eavesdropping:** As the network traffic flows through the attacker's device, they intercept and capture the data packets, allowing them to eavesdrop on the communication between the legitimate parties. This can include capturing sensitive information like usernames, passwords, or other confidential 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.

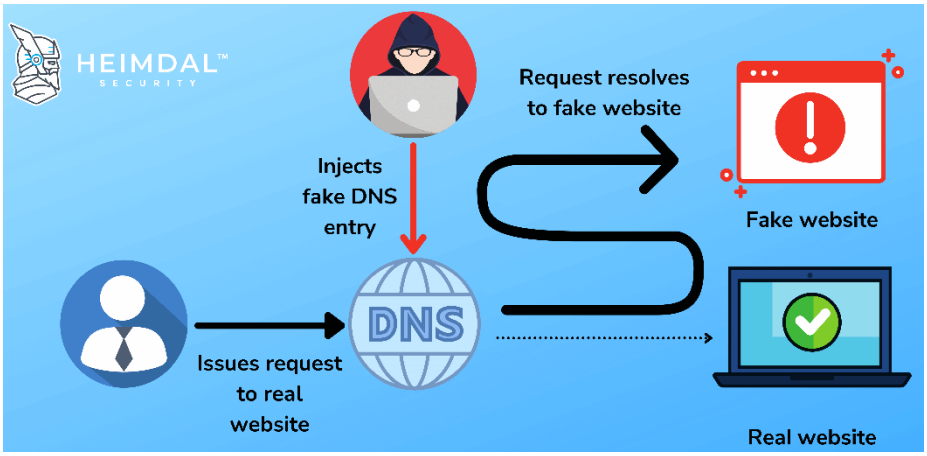
3. Address caching: Once the attacker successfully spoofs the MAC or ARP cache, they intercept and capture network traffic intended for the legitimate device. This allows them to eavesdrop on the communication or manipulate the data being transmitted.

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.

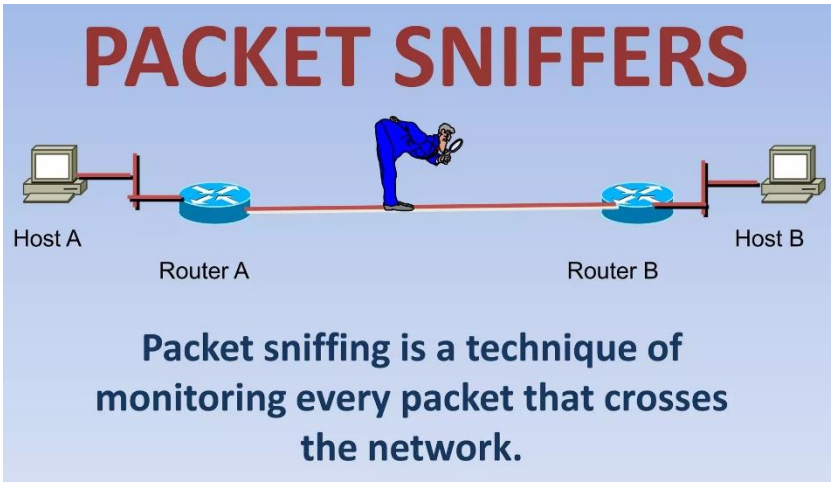


Sniffing attacks on the physical layer

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.



II. Case Study of Attacks On OSI MODEL:

The Stuxnet worm attack, discovered in 2010, targeted supervisory control and data acquisition (SCADA) systems, specifically those used in Iran's nuclear facilities. This sophisticated attack aimed to disrupt and sabotage the operation of Iran's uranium enrichment centrifuges.

Impact of Stuxnet worm attack:

- The Stuxnet worm attack had far-reaching consequences, demonstrating the potential for cyberattacks to disrupt critical infrastructure systems.
- It specifically targeted SCADA systems, which are responsible for monitoring and controlling industrial processes.
- The attack compromised multiple layers of the OSI model, resulting in physical damage and operational disruption.

Consequences of Stuxnet worm attack:

- Physical Damage: Stuxnet targeted the physical layer (Layer 1) by exploiting zero-day vulnerabilities in Microsoft Windows to gain access to the target systems.
- Operational Disruption: Stuxnet impacted the data link layer (Layer 2) by tampering with the communication protocols used by the SCADA systems.
- Exploiting Software Vulnerabilities: Stuxnet exploited vulnerabilities in the application layer (Layer 7) by using malicious code hidden within infected files.

Countermeasures To Prevent Stuxnet Worm Attack:

- Patch Management: Regularly applying security patches and updates to all software and operating systems can mitigate the risk of vulnerabilities being exploited by attackers.
- Network Segmentation and Access Control: Implementing this helps isolate critical infrastructure systems from external networks and other less critical systems.
- Intrusion Detection and Prevention Systems: Employing these systems at various layers of the network infrastructure can help identify and block malicious activities.
- Security Awareness and Training: Training SCADA operators, system administrators, and personnel on secure practices.
- Recognizing and responding to potential cyber threats, can enhance the overall security posture.
- Education on phishing attacks, social engineering techniques, and safe computing practices helps mitigate the risk of human error leading to successful attacks.

Case Study 2 : SQL Injection Attack:

SQL injection is a type of attack that targets the application layer (Layer 7) of the OSI model. It takes advantage of vulnerabilities in web applications that do not properly validate and sanitize user input before interacting with a database.

Impact Of SQL Injection Attack:

- In 2013, the retail giant Target fell victim to a massive data breach that compromised the personal and financial information of approximately 40 million customers.

- The attack exploited a vulnerability in Target's web application, which allowed the attackers to inject malicious SQL (Structured Query Language) code into the application's input fields.
- Through this SQL injection attack, the hackers gained unauthorized access to the customer database and exfiltrated sensitive information.

Consequences Of SQL Injection Attack:

- Data Manipulation: Malicious SQL statements can modify, delete, or insert data into the application's database, leading to data corruption or unauthorized modifications.
- Unauthorized Data Access: Attackers can bypass authentication mechanisms, retrieve sensitive information from databases, or gain unauthorized access to user accounts.
- Denial of Service: Attackers may exploit SQL injection vulnerabilities to perform resource-intensive queries, causing excessive server load and potential denial of service for legitimate users.
- Information Leakage: Error messages or debug information generated by the application during an SQL injection attack can reveal sensitive database structure, table names, or even administrator credentials, aiding future attacks.

Countermeasures to Prevent SQL Injection Attack:

- Input Validation and Sanitization: Implement strict input validation to ensure that user input conforms to expected formats and rejects any malicious characters. Sanitize input by encoding or escaping special characters before using them in SQL queries.
- Parameterized Queries or Prepared Statements: These techniques ensure that input is treated as data rather than executable SQL, mitigating the risk of SQL injection.
- Principle of Least Privilege: Limiting access privileges reduces the potential damage an attacker can cause if an SQL injection vulnerability is exploited.
- Secure Coding Practices: Implement secure coding practices, such as using built-in security libraries, and regularly updating software dependencies, to minimize the risk of introducing SQL injection vulnerabilities.
- Regular Security Testing: Perform regular security testing, including vulnerability assessments and penetration testing, to identify and address any SQL injection vulnerabilities in the application.

Type of Attack	Layer of OSI	Impact	Consequences	Counter measures	Year of attack	Impacted organization
Fiber Optic Cable Cut	Physical	Disruption of network connectivity	Loss of data transmission, service unavailability	Implementation of backup communication channels	2019	Multiple
MAC Address Spoofing	Data Link	Unauthorized network access, interception of traffic	Data compromise, network disruption	Port security measures, MAC address filtering, network access control, IEEE 802.1X	2014	Iran Nuclear
SYN Flood Attack	Transport	Server resource exhaustion, denial of service	Service unavailability, financial losses	Intrusion Prevention Systems (IPS)	2018	GitHub
SQL Injection	Application	Unauthorized data access, data modification	Compromised data integrity, unauthorized access	Input validation and sanitization	2017	Equifax
Session Hijacking	Session	Unauthorized session control, data interception	Data compromise, unauthorized access, impersonation	Secure session management	2015	Sony play station network

III. Mitigation and Strategies on OSI Model Attack:

Application Layer

- **Attack vectors**: distributed denial-of-service attacks (DDoS) attacks, HTTP floods, SQL injections, cross-site scripting, parameter tampering, and Slowloris attacks. Other exploits include viruses, worms, phishing, key loggers, backdoors, program logic flaws, bugs, and trojan horses.

- **Mitigation:** have an arsenal of security protections, such as web application firewalls (WAFs), secure web gateway services. This layer is the hardest to defend as the application is accessible only over Port 80 (HTTP) or Port 443 (HTTPS). Keep yourself acquainted with the Application Monitoring to detect zero-day vulnerabilities.

Presentation Layer

- **Attack vectors**: SSL hijacking, encryption downgrade attacks, decryption attacks, encoding attacks, DDoS attacks

- **Mitigation:** offload the SSL from the origin infrastructure and inspecting the application traffic for signs of attack traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure.

Session Layer

- **Attack vectors**: Session hijacking attack, Man-in-the-Middle (MITM), Blind attack, Man-in-the-browser, SSH Sniffing

- **Mitigation:** Check for new updates or version upgrades with your hardware provider. Generally, these updates would carry a patch to nullify the threat.

Transport Layer

- **Attack vectors**: TCP Sequence prediction, SYN flood attack, TCP Session hijacking, UDP flood attack, UDP-based amplification attacks
- **Mitigation:** DDoS blackhole routing/filtering or commonly referred to as Blackholing is one of the mitigation scenarios typically used by ISP's.

Network Layer

- **Attack vectors**: IP Spoofing and jamming, ICMP attack, Smurf attack, Worm-hole, Blackhole attacks, Sybil attack, Packet sniffing, and selective forwarding attacks
- **Mitigation:** Ensure all security patches, packet filtering is kept enabled and any unused ports are blocked, unused services, and interfaces are disabled at the router operating system. Enable logging, place firewalls between your network and all untrusted networks and make sure that all switch traffic is encrypted.

Data Layer

- **Attack vectors**: ARP Spoofing, MAC cloning, DoS, Spanning tree attack, VLAN hopping, DHCP attacks
- **Mitigation:** configure their switches to limit the ports that can respond to DHCP requests, implement static ARP and install Intrusion Detection Systems (IDS). Allow discovered the MAC address to be authenticated against authentication, authorization and accounting (AAA) and subsequently filtered.

Physical Layer

- **Attack vectors**: Unauthorised access, data sniffing, physical damage
- **Mitigation:** Use defense-in-depth tactics, use access controls, accountability and auditing to track and control physical assets.

Being aware of the exploits and understanding the importance of the security issues is one of the first steps in the cybersecurity world. Please share your thoughts and pen down for further inputs.

Here are some mitigation strategies for each layer of the OSI model:

Physical Layer:

- Restrict physical access to networking devices and infrastructure to authorized personnel only.
- Implement security measures such as surveillance cameras, biometric access controls, and physical barriers to prevent unauthorized tampering.

Data Link Layer:

- Implement strong authentication mechanisms, such as MAC address filtering, to prevent unauthorized devices from accessing the network.
- Utilize encryption protocols like WPA2 or WPA3 to secure wireless communications.
- Enable port security features, such as limiting the number of MAC addresses allowed on a port, to prevent MAC spoofing attacks.

Network Layer:

- Implement network segmentation to separate critical resources and limit the potential impact of an attack.

- Configure access control lists (ACLs) and firewalls to control inbound and outbound traffic based on trusted sources, protocols, and ports.
- Utilize network address translation (NAT) to hide internal IP addresses from external networks.

Transport Layer:

- Implement Transport Layer Security (TLS) to encrypt data during transmission, ensuring confidentiality and integrity.
- Utilize firewalls to allow only trusted connections and block unauthorized access attempts.
- Implement session timeouts and connection limits to mitigate DoS (Denial of Service) attacks.

Session Layer:

- Implement strong authentication mechanisms to verify the identities of communicating entities.
- Utilize session encryption to protect the confidentiality and integrity of session data.

Presentation Layer:

- Implement secure coding practices to prevent common vulnerabilities, such as buffer overflows and injection attacks.
- Utilize encryption mechanisms, such as SSL/TLS, to secure data during presentation.

Application Layer:

- Keep software and applications up to date with the latest security patches.
- Implement secure coding practices and input validation to prevent common web application vulnerabilities, such as SQL injection and cross-site scripting (XSS).
- Utilize strong authentication and access control mechanisms to protect sensitive data.
- In addition to these strategies, it is important to regularly monitor network traffic, employ intrusion detection and prevention systems, and conduct security audits to identify and address potential vulnerabilities across the OSI model.

IV. Conclusion:

The Open Systems Interconnection (OSI) model is a conceptual framework that standardizes the functions of a communication system into seven layers. Each layer has a specific role and interacts with adjacent layers to ensure the proper transmission of data between network devices. While the OSI model itself is not directly attacked, the layers within the model can be targeted by various types of attacks. It's important to note that attacks can occur across multiple layers and may involve complex techniques that exploit vulnerabilities at different levels of the OSI model. Protecting a network requires implementing security measures at each layer and employing a defense-in-depth strategy to mitigate the risks associated with various attacks.

V. 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
- https://medium.com/codex/attack-vectors-w-r-t-osi-layers-7809a1e0a384
- Chatgpt
- https://www.secopsolution.com/blog/attacks-possibility-by-osi-layer-cyber-threat-intelligence#:~:text=Attacks%20are%20possible%20at%20each,weaknesses%20in%20the%20underlying%20protocols.
- https://www.infosectrain.com/blog/common-security-attacks-in-the-osi-layer-model/
- https://www.byos.io/blog/types-of-cyber-attacks-osi
- https://www.imperva.com/learn/application-security/osi-model/

THANK YOU