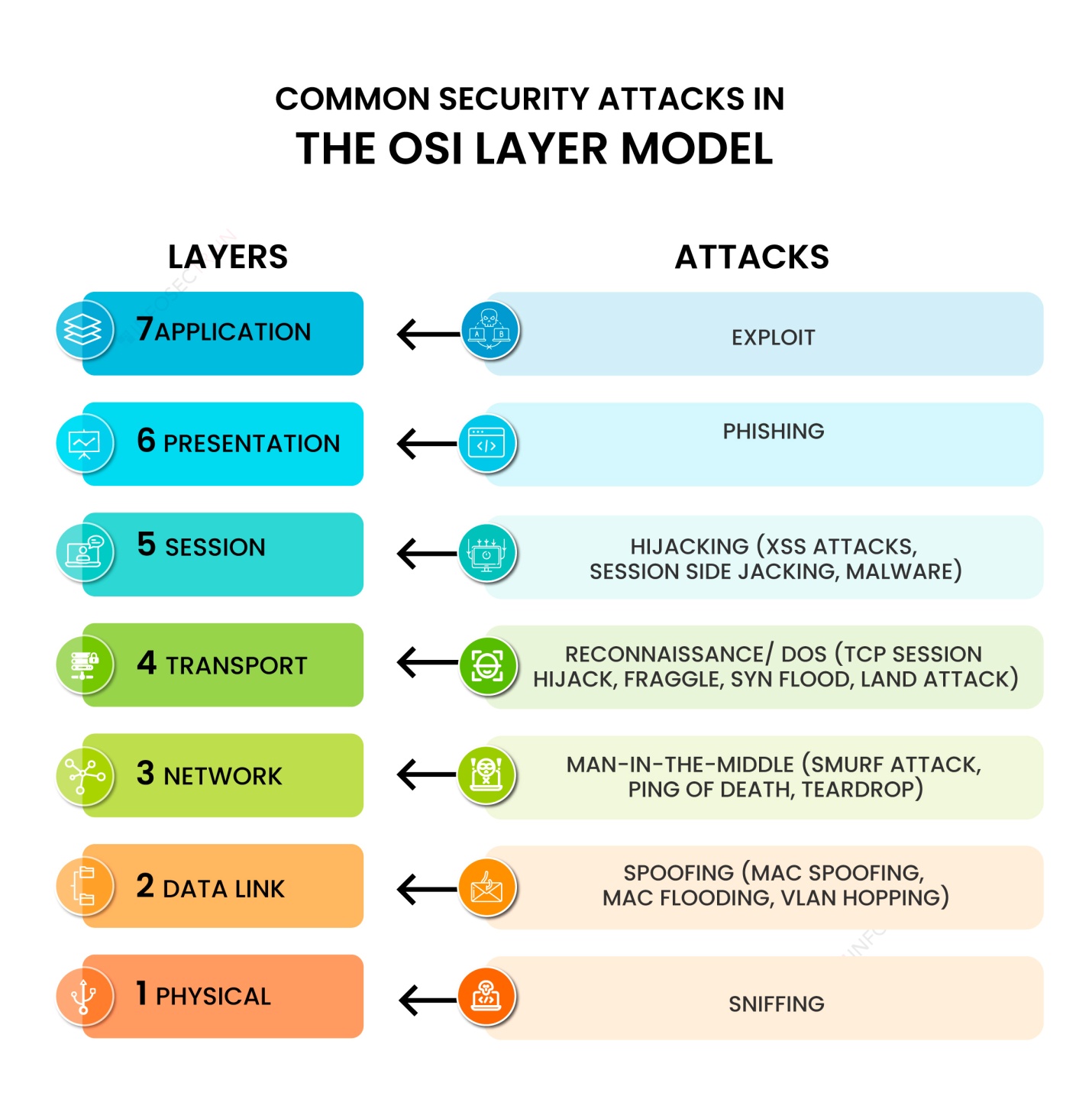
Name: A.G.Kathiresan

Group Task 2

OSI layer

Attacks targeting different layers of the OSI (Open Systems Interconnection) model can compromise network security and have varying impacts on the overall system. Here's a breakdown of how attacks at different layers can affect network security and the system in depth:

**1. Application layer**

The application layer is the closest to users in the OSI layer model and establishes the communication between the user and applications with which they interact individually. The common security attack on this layer is an exploit.

**Attack: Exploit**

Exploit means taking advantage of a software vulnerability. An exploit in the application layer refers to a type of cyber attack that targets vulnerabilities in software applications. These attacks take advantage of bugs or weaknesses in the code of the application to gain unauthorized access or perform malicious actions. This indicates that the target of an attack includes a software vulnerability that allows attackers to build the means to access and exploit it. Without employing an exploit, attackers can take down a website or important system by using DoS (Denial-of-Service) or DDoS (Distributed Denial-of-Service) cyberattacks. Many exploits are designed to enable super user-level access to a victim system.

**2. Presentation layer**

The presentation layer specifies the two devices’ encoding, encryption, and compression methods for proper communication. Anything sent from the application layer is received by the presentation layer, which is transformed into a format suitable for transmission via the session layer. Phishing is one of the common security attacks carried out by attackers in this layer.

**Attack: Phishing attack**

Phishing attacks in the presentation layer comprise using social engineering tactics to trick users into providing personal and sensitive information or clicking on a malicious link. This is often done by creating fake websites or email messages that appear to be from a legitimate source. This attack aims to steal sensitive information such as login credentials and credit card information or install malware on the victim’s system by disguising the attack as a legitimate request.

**3. Session layer**

The session layer establishes communication channels between devices, known as sessions. It starts sessions, keeps them open and effective while data is transferred, and closes them after communication is completed. Hijacking is one of the common security attacks that occurs in this layer.

**Attack: Hijacking**

Hijacking in the session layer occurs when an attacker intercepts and takes control of an established communication session between two parties. This can be carried out by exploiting vulnerabilities in the protocol used to establish the session or using the tools to intercept and manipulate network traffic. Once the attackers hijack the session, they can access sensitive information or gain unauthorized access. There are two types of session hijacking:

* **Active session hijacking**: In this, the attacker takes control of an active user session on a network and intercepts and alters network traffic in real time.
* **Passive session hijacking**: In this, attackers monitor network traffic and wait for users to log into a website; at that point, the attackers take over the session.

**4. Transport layer**

The transport layer performs flow control, transmitting data at a frequency corresponding to the receiving device’s connection speed and error control, determining whether data was received wrongly and requesting it if necessary. The most common security attack that is carried out in this layer is reconnaissance.

**Attack: Reconnaissance**

A reconnaissance attack in the transport layer typically involves an attacker attempting to gather information about a target system or network by actively probing the transport layer protocols, such as TCP or UDP. This can include techniques such as port scanning, which involves sending messages to various ports on the target system to determine which ports are open and potentially vulnerable to attack. Additionally, an attacker may use tools such as packet sniffers to capture and monitor network traffic to gather information.

**5. Network layer**

There are two primary jobs that the network layer does. One breaks up the segments into network packets and then puts the packets back together at the other end. The other is sending packets through a physical network by finding the best route. One of the most common security attacks in this layer is a man-in-the-middle attack.

**Attack: Man-in-the-Middle (MITM) attack**

In the network layer, a man-in-the-middle attack occurs when an attacker intercepts and modifies communication between two parties without their knowledge. The attackers become a man in the middle of the communication, able to read, modify, or inject new information into the communication. Attackers also intercept and alter communication by manipulating the routing of packets between the two sources. This can be done by using a technique such as ARP spoofing, where attackers send fake ARP messages to a target system, tricking it into sending packets to the attacker’s device instead of the intended source.

**6. Data link layer**

The data link layer establishes and terminates communication between two technically connected network nodes. It divides packets into frames and transmits them from source to destination. In this layer, attackers use spoofing attacks to target the network system.

**Attack: Spoofing attack**

A spoofing attack in the data link layer occurs when an attacker alters a device’s Media Access Control (MAC) address to impersonate another device in the network. This can allow the attackers to gain access to network resources or intercept and modify network traffic intended for the legitimate source. There are different ways that attackers carry out MAC spoofing.

* Address Resolution Protocol (ARP) spoofing
* DHCP spoofing
* MAC flooding

**7. Physical layer**

The physical layer is responsible for adequately connecting network nodes via wired or wireless means. Sniffing is the most common security attack used by attackers to target the data link layer.

**Attack: Sniffing attacks**

A sniffing attack in the data link layer occurs when an attacker captures and analyzes network traffic to gather sensitive information. This is done using a packet sniffer tool, which captures and decodes all the packets passing through a particular network segment. Sniffing attacks steal sensitive information such as login details, credit card numbers, and other personal and sensitive information.

2.TWO REAL WORLD CASE STUDIES OF THE OSI LAYER ATTACKS:

1. Mirai Botnet (Data Link Layer and Network Layer Attack):

The Mirai botnet was a large-scale IoT (Internet of Things) botnet that emerged in 2016. It targeted vulnerable IoT devices, such as cameras and routers, to carry out distributed denial-of-service (DDoS) attacks. Mirai infected devices by exploiting weak default passwords and known vulnerabilities.

Impact and Consequences:

Mirai's impact was widespread and had significant consequences. It harnessed the power of compromised IoT devices to launch massive DDoS attacks, disrupting critical services. One notable attack occurred in October 2016 when the Mirai botnet targeted Dyn, a major DNS service provider. The attack caused widespread outages, affecting popular websites like Twitter, GitHub, and Netflix.

Countermeasures:

- Manufacturers and users should ensure that IoT devices have strong, unique passwords and regularly update their firmware to patch known vulnerabilities.

- Network administrators should implement traffic filtering and anomaly detection mechanisms to identify and block malicious traffic associated with botnet activities.

- ISPs (Internet Service Providers) can employ network-level filtering to identify and block suspicious traffic originating from compromised IoT devices.

2. WannaCry Ransomware (Transport Layer and Application Layer Attack):

WannaCry is a notorious ransomware that emerged in May 2017. It exploited a vulnerability in the Windows SMB (Server Message Block) protocol, affecting computers running outdated versions of Windows operating systems.

Impact and Consequences:

WannaCry had a significant impact globally, affecting organizations in various sectors, including healthcare, finance, and government. The ransomware encrypted files on infected systems, making them inaccessible, and demanded ransom payments in Bitcoin for their release. It caused widespread disruption, with hospitals, banks, and businesses facing operational and financial challenges.

Countermeasures:

- Regular patching and updating of operating systems and software to address known vulnerabilities is crucial to prevent attacks like WannaCry.

- Employing effective endpoint protection solutions, including antivirus and anti-malware software, can help detect and mitigate ransomware threats.

- Implementing robust backup strategies, including offline and off-site backups, can help restore systems and data in case of a ransomware attack.

It's important to note that these case studies highlight the significance of proactive security measures, timely updates, and vulnerability management to mitigate the risks associated with attacks at different layers of the OSI model. Security awareness, user education, and industry collaboration also play vital roles in combating such threats effectively.

OSI ATTACKS AND ITS MITIGATION TECHNIQUES

1. Physical Layer Attacks:

- Attacks: Physical tampering, cable cutting, power supply disruption.

- Mitigation: Implement physical security measures like restricted access, surveillance systems, and tamper-evident seals. Redundant power supplies and backup connections can reduce the impact of disruptions.

2. Data Link Layer Attacks:

- Attacks: MAC address spoofing, ARP spoofing/poisoning.

- Mitigation: Implement port security mechanisms, such as MAC address filtering or port authentication protocols like IEEE 802.1X. Use tools like ARP spoofing detection or intrusion detection systems (IDS) to identify and prevent spoofing attempts.

3. Network Layer Attacks:

- Attacks: IP spoofing, ICMP attacks.

- Mitigation: Implement strong access control measures, including firewalls and intrusion prevention systems (IPS). Employ network traffic analysis tools to detect and prevent IP spoofing attempts. Configure routers and switches to drop suspicious ICMP packets.

4. Transport Layer Attacks:

- Attacks: SYN flood, TCP/IP hijacking.

- Mitigation: Implement SYN flood protection mechanisms like SYN cookies, rate limiting, or traffic shaping. Utilize secure transport protocols (e.g., TLS) for encrypted communication to prevent TCP/IP hijacking. Intrusion detection and prevention systems can help identify and block such attacks.

5. Session Layer Attacks:

- Attacks: Session hijacking.

- Mitigation: Implement session management techniques like session tokens, secure cookies, or session encryption. Employ strong authentication and authorization mechanisms to prevent unauthorized session hijacking. Use secure communication protocols (e.g., HTTPS) to protect session data in transit.

6. Presentation Layer Attacks:

- Attacks: Code injection.

- Mitigation: Implement input validation and output encoding techniques to prevent code injection attacks. Regularly update software and libraries to patch known vulnerabilities. Employ secure coding practices and web application firewalls (WAF) to detect and block malicious code injections.

7. Application Layer Attacks:

- Attacks: SQL injection, Cross-Site Scripting (XSS).

- Mitigation: Use parameterized queries or prepared statements to prevent SQL injection attacks. Implement input validation and output encoding techniques to mitigate XSS attacks. Employ web application firewalls (WAF) to detect and block such attacks.

Remember, defense-in-depth is crucial. Implement a combination of preventive measures, such as access controls, encryption, patch management, and network monitoring. Regular security assessments, employee education, and incident response planning are also essential to maintain robust network security.