A REPORT ON OSI Model

-Team Euphorbia

INDEX

1. Introduction

Open Systems Interconnection Model (OSI Model) is a conceptual model which was first defined in raw form in Washington, D.C., in February 1978 by French software engineer Hubert Zimmermann, and the refined but still draft standard was published by the ISO in 1980. It had two major components: an abstract model of networking, called the Basic Reference Model or seven-layer model, and a set of specific protocols. The OSI reference model was a major advance in the standardization of network concepts as although not a standard itself, it was a framework in which future standards could be defined.

It was made by an industry effort that attempted to get industry participants to agree on common network standards to provide multi-vendor interoperability as it was common for large networks to support multiple network protocol suites, with many devices unable to interoperate with other devices because a lack of common protocols.

The OSI protocol suite was considered by many as too complicated and inefficient and to a large extent unimplementable. Due to this, the TCP/IP model of 5 layers was picked up for practical implementation. It didn't help that the TCP/IP model provided independent implementations of simplified protocols making it easier to apply practically.

This doesn't mean that the OSI model is not used nowadays at all. Due to being a detailed model, it is still used by users and operators to determine the required hardware and software to build their network, understand and communicate the process followed by components communicating across a network, Perform troubleshooting, by identifying which network layer is causing an issue and focusing efforts on that layer.

2. Overview of the OSI Model

2.1. Application Layer:

- The top layer of the OSI model is the Application layer.
- It does not refer to the actual applications that users run it just provides the framework that the actual applications run on top of it.
- In simple words to know what the application layer does, for example, a user wanted to use a web browser like Firefox, Chrome, etc. to open an FTP session and transfer a file. In this particular case, the application layer would define the file transfer protocol. This protocol is not directly accessible to the end user. The end user must still use an application that is designed to interact with the file transfer protocol. In this case, Internet Explorer would be that application.
- Some protocol of FPT are: telnet, DNS, DHCP, FTP, SNMOP, HTTP, NFS etc.

2.2. Presentation Layer:

- The presentation layer takes the data that is provided by the application layer and converts it into a standard format that the other layers can understand.
- Likewise, this layer converts the inbound data that is received from the session layer into something that the application layer can understand.
- Also, it does Encryption and decryption of data, and compression for bandwidth management of data while handling the data.
- In order for network communications to function properly, the data needs to be structured in a standard way because applications handle data differently from one another. So this layer is necessary.

2.3. Session Layer:

- Once the data has been put into the correct format, the sending host must establish a session with the receiving host. This is where the session layer comes into play.
- It is mainly responsible for establishing, maintaining, and eventually terminating the session with the remote host with token management.
- The interesting thing about the session layer is that it is more closely related to the application layer than it is to the physical layer because sessions are established between applications.
- If a user is running multiple applications, several of those applications may have established sessions with remote resources at any time.

- Some session layer protocols are PPTP: Point-to-Point Tunneling Protocol, RPC: Remote Procedure Call Protocol, RTCP: Real-time Transport Control Protocol, SCP: Session Control Protocol, SDP: Session Description Protocol, etc.

2.4. Transport Layer:

- The Transport layer is responsible for maintaining flow control and congestion control using TCP (Transmission Control Protocol).
- An operating system allows users to run multiple applications simultaneously and it is therefore possible that multiple applications may need to communicate over the network simultaneously so this layer takes the data from each application, and integrates it all into a single stream i.e., segment (which is also data unit in this layer).
- This layer is also responsible for providing error checking and performing data recovery when necessary.
- The transport Layer is responsible for ensuring that all of the data is sent from sending host to the receiving host.
- Apart from that Best-effort delivery of segments with no guarantees on ordering, integrity, reliability, and with no congestion and flow control is done by User Datagram Protocol (UDP).

2.5. Network Layer:

- The Network Layer is responsible for determining how the data will reach the recipient.
- In simple words, it creates logical paths, known as virtual circuits, between the source and destination hosts.
- This layer handles things like addressing, routing, and logical protocols.
- The Network Layer is also responsible for its own error handling and packet sequencing and congestion control.
- The amount of data that must be transmitted often exceeds the maximum packet size I.e. MTU(maximum transmission unit). Therefore, the data is fragmented into multiple packets. When this happens, the Network Layer assigns each packet a sequence number. When the data is received by the remote host, that device's Network layer examines the sequence numbers of the inbound packets and uses the sequence number to reassemble the data and to figure out if any packets are missing.
- Data units in this layer are called call a Packet.

2.6. Data Link Layer:

- The data link layer can be sub-divided into two other layers:
- Media Access Control (MAC) layer,
- The MAC layer basically establishes the computer's identity on the network, via its MAC address.
- A MAC address is the address that is assigned to a network adapter at the hardware level

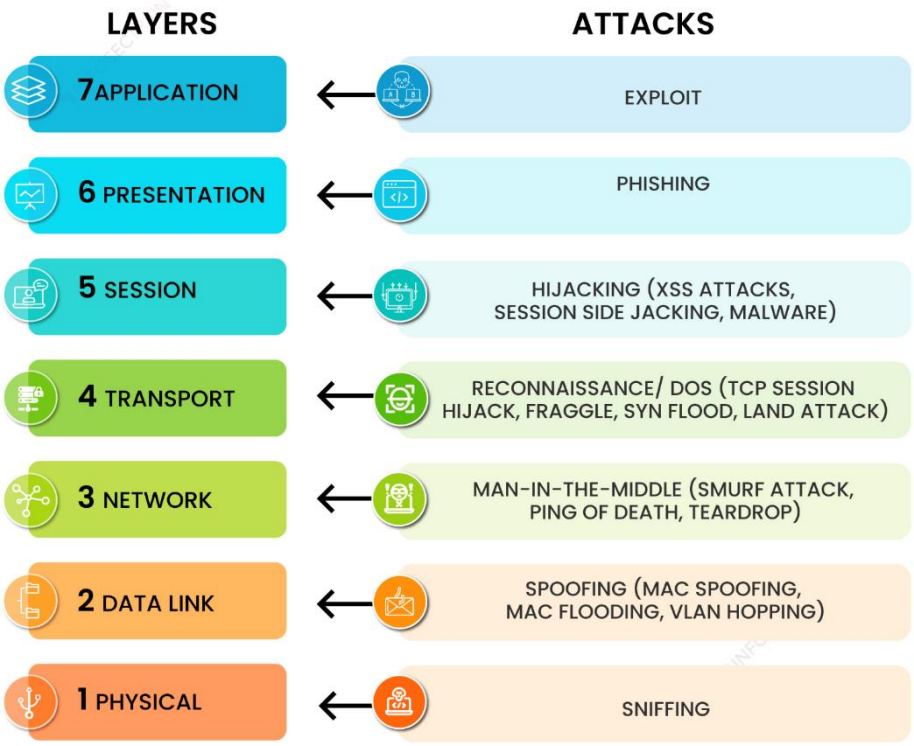
- Which is used while sending and receiving a data frame(which is the data unit of this layer) and also checks for chances of collision occurrence.
-
- Logical Link Control (LLC) layer
- The LLC layer controls frame synchronization, and flow control multiplexing of the L3 protocol and provides a degree of error checking.

2.7. Physical Layer:

- The physical layer of the OSI model refers to the actual hardware specifications or characteristics such as timing and voltage.
- The physical layer defines the means of transmitting raw bits rather than logical data packets over a physical link connecting network nodes.
- The physical layer provides an electrical, mechanical, and procedural interface to the transmission medium.
- The shapes and properties of the electrical connectors, the frequencies to broadcast on, the modulation scheme to use, and similar low-level parameters, are specified here.

3. Analysis of attack each layer

Attacks can occur at any layer some of the most common attacks at each layer are as follows:



3.1. Physical Layer:

- Denial of service (DoS) attacks: These attacks attempt to disrupt the physical layer by disabling network devices or interrupting the flow of data.
- Eavesdropping: It involves capturing and monitoring data as it travels across the physical layer.
- Man-in-the-middle (MitM) attack: This attack involves an attacker inserting themselves between two communicating parties and intercepting their data.

3.2. Data Link Layer:

- Sniffing: In this it involves capturing and monitoring data as it travels across the data link layer.
- Frame modification: This attack involves modifying data frames as they travel across the data link layer.
- MAC flooding: It involves flooding a network with malicious MAC addresses, which can disrupt network traffic.

3.3. Network Layer:

- Routing attacks: In this attacker attempts to disrupt the routing of data packets across a network.
- Spoofing: This attack involves an attacker sending falsified data packets to a network, which can lead to data theft or denial of service.
- Man-in-the-middle (MitM) attack: This attack involves an attacker inserting themselves between two communicating parties and intercepting their data.

3.4. Transport Layer:

- Session hijacking: This attack involves an attacker taking over an existing session between two communicating parties.
- TCP/IP stack overflow: This attack involves exploiting a vulnerability in the TCP/IP stack to gain control of a system.
- SYN flood attack: This attack involves flooding a system with SYN packets, which can exhaust the system's resources and lead to a denial of service.

3.5. Session Layer:

- Session hijacking: This attack involves an attacker taking over an existing session between two communicating parties.
- Session replay: This attack involves an attacker capturing and replaying a session between two communicating parties.

3.4. Presentation Layer:

- Malformed data: This attack involves sending malformed data to a system, which can lead to system crashes or data corruption.
- Encryption attacks: These attacks attempt to break encryption used to protect data.
- Phishing attacks: These attacks involve sending fraudulent emails or text messages that appear to be from a legitimate source, to trick users into revealing sensitive information, often through fake websites or emails.

3.5. Application Layer:

- Injection attacks: These attacks involve injecting malicious code into a system through an application.
- Cross-site scripting (XSS) attacks: These attacks inject malicious code into websites to steal information or manipulate user interactions.

3.6. Mitigation Strategies:

There are a number of mitigation strategies that can be used to protect against attacks at each layer of

the OSI model. Some of the most common mitigation strategies include:

- Using firewalls and intrusion detection systems (IDSs): Firewalls and IDSs can be used to filter traffic and detect malicious activity.
- Encrypting data: Encrypting data can help to protect it from being intercepted and read by unauthorized parties.
- Using strong passwords and security best practices: Using strong passwords and following security best practices can help to protect systems from being compromised.
- Keeping software up to date: Keeping software up to date can help to protect systems from known vulnerabilities.

By implementing these mitigation strategies, organizations can help to protect their networks and data from a variety of attacks.

4. Impact On Network Security

The impact of network security can vary depending on the type of attack and the layer of the OSI model that it targets. For example, an attack on the physical layer could disrupt the entire network, while an attack on the application layer could compromise the confidentiality or integrity of sensitive data.

4.1 Physical Layer:

At the physical layer, there are various security threats to consider. Eavesdropping is a concern where an attacker intercepts data during transmission, potentially compromising sensitive information. Denial-of-service attacks can flood the network with excessive traffic, rendering it inaccessible to legitimate users. Another threat involves physical tampering with network devices, where attackers can physically damage the devices, disrupting network connectivity and traffic flow.

4.2 Data Link Layer:

In the Data Link layer, security risks arise that can compromise network integrity. MAC address spoofing occurs when an attacker falsifies the MAC address of a legitimate device, granting unauthorized access to the network. ARP poisoning involves manipulating the ARP cache of a device, redirecting traffic to unintended destinations. VLAN hopping is a vulnerability where attackers can maneuver between Virtual LANs (VLANs), potentially gaining unauthorized access to restricted resources.

4.3 Network Layer:

The Network layer faces its own set of security challenges. IP spoofing enables attackers to forge the IP address of a legitimate device, enabling impersonation and unauthorized access. DNS poisoning involves

corrupting the DNS cache of a device, causing it to direct users to incorrect IP addresses, leading to potential data breaches. Routing table attacks allow attackers to manipulate routing tables, diverting network traffic to unintended destinations, compromising data confidentiality and availability.

4.4 Transport Layer:

The Transport layer is susceptible to specific security threats. Session hijacking occurs when an attacker seizes control of an ongoing session between two devices, potentially compromising communication privacy or taking over the session. TCP/IP fragmentation attacks involve fragmenting TCP/IP packets, making it difficult for the receiving device to reassemble them accurately, causing communication disruptions. SYN flooding is a type of DoS attack where a large volume of SYN packets overwhelms a device, rendering it unresponsive to legitimate requests.

4.5 Session Layer:

The Session layer is vulnerable to certain security risks. Session hijacking, similar to the Transport layer, involves an attacker seizing control of an established session between two devices, enabling eavesdropping or session manipulation. Man-in-the-middle attacks occur when an attacker intercepts and relays communication between two devices, potentially eavesdropping, altering data, or impersonating one of the parties involved.

4.6 Presentation Layer:

The Presentation layer faces security threats that impact data presentation and user interaction. Data tampering occurs when an attacker manipulates data as it is presented to the user, leading to the display of incorrect or malicious information. Cross-site scripting attacks involve injecting malicious code into a web page, which is executed when users access the page, potentially compromising their systems and data.

4.7 Application Layer:

The Application layer is the target of various security attacks. Malicious code attacks involve delivering harmful code to a user's device, which can be exploited to steal sensitive data or gain unauthorized control over the device. Phishing attacks employ deceptive emails or messages that appear to be from trustworthy sources, tricking users into divulging confidential information. Denial-of-service attacks overwhelm websites or services with excessive traffic, rendering them inaccessible to genuine users, causing disruptions and potential data breaches.

5. Mitigation Strategies

5.1 Physical Layer:

Attacks on the physical layer involve exploiting vulnerabilities in the physical infrastructure or communication medium. Here's a concise overview of how such attacks can occur:

1. Wiretapping: Attackers physically tap into a network cable or communication channel to intercept and listen to transmitted data.
2. Jamming: Attackers disrupt wireless signals by transmitting interfering signals on the same frequency, causing interference or blocking communication.
3. Physical Destruction: Attackers physically damage network infrastructure components, such as cutting cables or destroying devices, to disrupt connectivity.
4. Interference: Attackers exploit wireless vulnerabilities by transmitting signals that interfere with intended communication, causing packet loss or disruptions.
5. Denial of Service (DoS): Attackers overwhelm network devices with excessive traffic or requests, rendering them unable to function properly.
6. Man-in-the-Middle (MitM): Attackers insert themselves between communicating devices, intercepting and altering communication by placing rogue devices or compromising network hardware.
7. Physical Impersonation: Attackers physically impersonate legitimate devices or users by using fake credentials or mimicking authorized equipment, enabling unauthorized access or actions.

Physical layer attacks require physical proximity to the target infrastructure, making them more challenging to execute. Implementing physical security measures and protocols can help mitigate these risks.

5.2 Data Link Layer:

Attacks on the data link layer exploit vulnerabilities in network protocols and technologies at the point where adjacent devices connect. Here's a brief explanation of how these attacks occur:

1. MAC Address Spoofing: Attackers manipulate their MAC address to impersonate another device, gaining unauthorized access or disrupting communication.
2. ARP Spoofing/Cache Poisoning: Attackers send fake Address Resolution Protocol (ARP) messages to associate their MAC address with another device's IP address, allowing interception or modification of network traffic.
3. VLAN Hopping: Attackers exploit weaknesses in switch port trunking protocols to gain unauthorized access to different VLANs and intercept or modify traffic.
4. Spanning Tree Protocol (STP) Attacks: Attackers manipulate Spanning Tree Protocol implementations to create network loops, causing disruptions or facilitating eavesdropping.
5. MAC Layer Attacks: Attackers exhaust network bandwidth by continuously transmitting invalid frames, leading to denial of service conditions.
6. Ethernet Switch Attacks: Attackers exploit vulnerabilities in Ethernet switches to gain unauthorized access to traffic or compromise switch functionality.

Implementing security measures like authentication, encryption, and regular updates can help mitigate data link layer attacks.

5.3 Network Layer:

Attacks at the OSI model's Network layer primarily entail exploiting flaws in network protocols and devices to interrupt or undermine network communication. IP spoofing, in which attackers forge the source IP address to fool network filters; ICMP attacks, in which attackers flood the network with ICMP packets to cause congestion or resource exhaustion; routing attacks, in which routing tables are manipulated to redirect traffic or spread incorrect routing information; DoS and DDoS attacks, which overwhelm network resources to render them inaccessible; and fragmentation attacks, which exploit IP packet fragmentation mechanisms.

5.4 Transport Layer:

Attacks against the Transport layer of the OSI model seek to exploit flaws in transport protocols in order to disrupt or undermine data flow. TCP/IP hijacking, in which attackers intercept and manipulate TCP/IP sessions to gain unauthorised access or steal data; SYN flooding, in which a server is overwhelmed with a high volume of SYN requests, rendering it unresponsive; port scanning, used to identify open ports and potential vulnerabilities on target systems; session hijacking, in which attackers take over a legitimate user's session to gain unauthorised access or manipulate data; and exploitation of vulnerabilities and man-in-the-middle attacks.

5.5 Presentation Layer:

Possible mitigation:

To mitigate, consider options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attack traffic or violations of policy at an application delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host.

The presentation layer adds a presentation header to the data packet that now consists of the application header as well as the original user data. The possible threats in this presentation layer are

- Encryption attacks
- SSL Hijacking
- Decryption downgrade attacks
- Man in the middle attack
- Encoding attacks

The mitigation for this layer is

- Update anti-virus database
- Verify links and sites
- Patch system updates

Update Anti-virus Database:

Ensure that the anti-virus software is regularly updated with the latest virus definitions and security patches.

Regularly schedule automatic updates or perform manual updates to ensure the anti-virus database can detect and protect against new threats.

Verify Links and Sites:

Be cautious when clicking on links in emails, social media, or websites. Verify the authenticity and legitimacy of links before accessing them.

Check for secure website indicators, such as HTTPS and a padlock symbol, to ensure the connection is encrypted and trustworthy.

Patch System Updates:

Keep the operating system, applications, and software up to date with the latest security patches and updates.

Regularly check for updates from official sources and apply them promptly to address known vulnerabilities.

5.6 Application Layer:

Possible mitigation:

Application monitoring is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero-day and application layers. Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDOS attacks.

The mitigations for this layer are

- Bug-Free Application
- Access control lists
- Firewalls
- Anti-virus
- Zero trust security

Bug-Free Application:

Developing and maintaining applications with strong emphasis on secure coding practices, adhering to established coding standards and best practices.

Regularly conducting code reviews and security testing (e.g., static analysis, dynamic analysis) to identify and address vulnerabilities and bugs in the application code.

Access Control Lists:

Implementing access control mechanisms, such as role-based access control (RBAC) or attribute-based access control (ABAC), to restrict and control user access to application resources.

Enforcing the principle of least privilege to ensure users have only the necessary permissions required to perform their tasks.

Firewalls:

Deploying firewalls at the network perimeter and within the internal network to monitor and control incoming and outgoing traffic to and from the application.

Configuring firewall rules to allow only necessary network traffic and blocking known malicious traffic

Anti-virus:

Implementing robust anti-virus and anti-malware solutions to detect and remove known malicious software from systems.

Keeping the antivirus software up to date with the latest virus definitions and regularly scanning systems for malware.

Zero Trust Security:

Adopting a Zero Trust security model that assumes no trust by default and verifies every user, device, and network resource attempting to access the application.

Implementing strong identity and access management (IAM) controls, network segmentation, and continuous authentication and authorization mechanisms.

6. Case Studies

Comprehensive Analysis of Attacks on the OSI Model: Case Studies and Report

6.1. Stuxnet:

The Stuxnet case study emphasizes the importance of defense-in-depth strategies, international collaboration, and information sharing to effectively combat cyber threats. Understanding Stuxnet's attack within the OSI model provides valuable insights into the multi-layered nature of advanced cyber-attacks, highlighting the need for comprehensive security measures across all layers of the model.

Layer: Physical

Impact: Stuxnet caused centrifuges to malfunction in Iran's nuclear program, slowing down the production of enriched uranium.

Consequences: Stuxnet damaged the reputation of Iran's nuclear program and showed that the country's systems were vulnerable to attack.

Countermeasures: Patch Windows vulnerabilities promptly, use strong passwords and multi-factor authentication, keep SCADA systems up to date with the latest security patches, and implement intrusion detection systems to monitor for malicious activity.

6.2. Miral:

The Mirai botnet is an example of a network layer attack. Mirai infected IoT devices, such as routers and cameras, with malware. The malware then used the infected devices to launch a distributed denial-of-service (DDoS) attack against DynDNS, a domain name service provider. The attack caused widespread outages for websites and online services. The Mirai case study explores the Mirai botnet attack, a significant Distributed Denial of Service (DDoS) attack that targeted Internet of Things (IoT) devices. By analyzing Mirai within the framework of the OSI model, this study provides insights into the botnet's tactics, the layers it exploited, the impact it had on networks, and countermeasures to mitigate similar attacks.

The Mirai case study emphasizes the importance of securing IoT devices and addressing vulnerabilities in network protocols. It highlights the need for strong authentication, regular patching, network segmentation, and traffic monitoring as countermeasures against such botnet attacks.

Layer: Network

Impact: Mirai caused widespread outages for websites and online services.

Consequences: Mirai disrupted the services of major companies and showed that IoT devices are vulnerable to attack and can be used to launch large-scale DDoS attacks.

Countermeasures: Keep IoT devices up to date with the latest security patches, use strong passwords and multi-factor authentication, implement firewalls to block malicious traffic, and educate users about the risks of IoT security.

6.3. Heartbleed:

The Heartbleed attack was a security vulnerability in the OpenSSL cryptographic software library. The vulnerability allowed attackers to read the memory of a remote server, including sensitive information such as private keys and passwords. The Heartbleed attack exploited a vulnerability in the SSL/TLS protocol, which is used to secure communications between web servers and browsers
Layer: Transport
Impact: The Heartbleed attack was a major security breach that affected millions of websites and servers. The attack allowed attackers to steal sensitive information from a wide range of organizations, including government agencies, financial institutions, and businesses. Consequences: The consequences of the Heartbleed attack were significant. The attack led to the disclosure of sensitive information, including private keys and passwords. This information could be used by attackers to gain unauthorized access to computer systems and networks. The attack also damaged the reputation of OpenSSL and other security software vendors. Countermeasures: The Heartbleed vulnerability was patched in April 2014. However, the attack highlighted the need for organizations to implement strong security measures to protect their systems and networks. Some of the most effective countermeasures against the Heartbleed attack include:

- Keeping software up to date: Organizations should regularly update their software to ensure that they are using the latest security patches.
- Using strong passwords: Organizations should use strong passwords for all of their systems and networks.
- Encrypting sensitive data: Organizations should encrypt sensitive data, such as private keys and passwords.
- Educating employees about cybersecurity: Organizations should educate their employees about cybersecurity risks and how to protect themselves from attack.

7. Recommendation

- Implementing a multi-layered security: Implementing a multi-layered security plan that addresses threats and vulnerabilities at every OSI model tier is a good idea for organisations. This entails putting in place particular security controls and measures that are tailored to the traits and

dangers of each floor. Organisations may create a stronger and more reliable security posture with numerous levels of defence.

- Regular Security Audits: Regularly carry out security audits To determine and evaluate the vulnerabilities of the network infrastructure, conduct routine thorough security audits. To find potential flaws and areas for improvement, these audits ought to involve code reviews, penetration testing, and vulnerability scans. Organisations can lower the risk of successful attacks by proactively discovering and addressing vulnerabilities.
- Enhanced access control: To prevent unauthorized access and reduce the risk of attack, deploy robust access control across your entire network architecture. This involves implementing strong authentication measures to ensure that users only have access to the resources they need for the job, such as multi-factor authentication and user-based access control. on role (RBAC).
- Use secure and encrypted communication methods: The data, network, and transport layers of the OSI model are particularly important places to apply encryption. Use TLS and IPSec or other secure communication protocols to protect the authenticity, confidentiality, and integrity of data. It prevents spying, tampering and unauthorized access to personal data.
- Promote information security awareness and training: Create a culture of security awareness among employees and conduct regular training on cybersecurity best practices. This includes training employees on the risks associated with OSI model attacks, phishing awareness, password hygiene, and safe use of network resources. By developing a security-aware workforce, organizations can significantly reduce the risk of a successful attack.
- Keep software and systems up-to-date: Install patches and updates for software, applications, and network equipment on a regular basis. This ensures quick remediation of known vulnerabilities and protects the system against new threats. Having a robust patch management process in place and staying up to date with the latest security updates is essential to maintaining a secure network environment.

8. Conclusion

In short, protecting against attacks on the OSI model requires a holistic and proactive approach to cybersecurity. By implementing the recommendations outlined above, organizations can significantly improve their defenses and reduce the risk of a successful attack.

The layered security approach provides multiple lines of defense, making it harder for an attacker to break into the network. By implementing layer-specific security controls and measures, organizations can address layer-specific vulnerabilities and mitigate the impact of attacks.

Regular security audits are essential to identify and address vulnerabilities in network infrastructure. Through vulnerability scanning, penetration testing, and code reviews, organizations can detect weaknesses and take action to strengthen their security defenses.

Powerful access control plays an important role in preventing unauthorized access to network resources. By implementing strong authentication mechanisms and using RBAC, organizations can ensure that only authorized users have access to sensitive information. Encryption and secure communication protocols protect the confidentiality, integrity, and authenticity of data in transit. By encrypting data at different layers of the OSI model and using secure protocols, organizations can protect against eavesdropping and unauthorized access. Security awareness and regular staff training are important. By educating employees about the risks associated with OSI attacks and promoting best practices, organizations can create a security-conscious workforce that works like an additional line of defense.

Regular patches and updates are essential to address known vulnerabilities and ensure systems are protected against emerging threats. By maintaining a robust patch management process and staying on top of security updates, organizations can reduce the attack surface and mitigate potential risks.

In short, a holistic approach that combines layered security, regular testing, robust access control, encryption, security awareness, and timely patching is essential for effective protection. against attacks on the OSI model. By implementing these recommendations, organizations can increase their cybersecurity and better protect their systems and data from potential attacks. However, it is important to note that security is an ongoing process and requires constant monitoring, tuning, and collaboration among all stakeholders to overcome emerging threats and vulnerabilities. . By prioritizing network security and implementing these recommendations, organizations can reduce the risks associated with OSI model attacks and maintain a secure and resilient network infrastructure.

9. References

1) OSI Model: What are the attacks on OSI Model?
(https://medium.com/@e.ahmadi/attacks-on-various-osi-model-layers-bd2fac5ab985)

2) What are the common security attacks on OSI Model?
(https://www.infosectrain.com/blog/common-security-attacks-in-the-osi-layer-model/)

3) What are threats and impact on Network perdormance?
(https://www.researchgate.net/publication/305295380_A_Study_on_Network_Security_Attacks_and_Their_Impacts_on_Networks)

4) Study on Network Security?
(https://blog.invgate.csom/iso-27001)

5) What is Heartbleed?
(https://en.wikipedia.org/wiki/Heartbleed)

6) What is OpenSSL?
(https://www.openssl.org/)

7) What is SSL/TLS?
(https://en.wikipedia.org/wiki/Heartbleed)

TEAM MEMBERS:

1. Jay
2. Niyati
3. Pawan
4. Aditya
5. Jiyanshu
6. Aasif
7. Mrunal
8. Piyush
9. Harsh
10. Prathamesh
11. Shubham
12. Ahmed
13. Ayaan
14. Prince
15. Kirti
16. Omkar
17. Sampada
18. Anubhav
19. Sakshi Jaiswal
20. Joseph