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.

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.

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.

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.

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.

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.

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.

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.

References:

1. Network Security: Threats and Impact on Network Performance:

www.researchgate.net/publication/266680981\_Network\_Security\_Threats\_and\_Impact\_on\_Network\_Performance

2. A Study on Network Security Attacks and Their Impacts on Networks:

www.researchgate.net/publication/305295380\_A\_Study\_on\_Network\_Security\_Attacks\_and\_Their\_Impacts\_on\_Networks

3. Network Security Threats, Attacks, and Their Countermeasures

ieeexplore.ieee.org/document/7045434