The Open Systems Interconnection (OSI) model is a conceptual framework that defines the functions of a network into seven layers. Each layer plays a specific role in transmitting and receiving data.

Unfortunately, attackers can target vulnerabilities at various layers of the OSI model.

We need security at each layer of OSI model for protecting CIA of the system.

Network security includes information security and computer security. It also requires firewall for protecting systems or data from being attacked and hacked.

Cybersecurity threats exist at all OSI-ISO model layers beginning at Layer 7 – the Application Layer because that’s the place where users begin by interfacing to the network.

In the table, some common attacks that occur at different layers are shown

|  |  |  |
| --- | --- | --- |
| LAYERS | TYPES OF ATTACKS | IMPACT OF ATTACK |
| Application Layer | possible exploits at the Application Layer include viruses, worms, phishing, key loggers, backdoors, program logic flaws, bugs, and trojan horses. | No user is able to access the network resources |
| Presentation Layer | **SSL Hijacking,** Phishing | Affected systems stop accepting SSL requests and automatically restarts |
| Session Layer | **Session Hijacking, MITM Attack** | **Disable Management operations** |
| Transport Layer | Reconnaissance | Connection limits of hosts |
| Network Layer | **man-in-the-middle** | **Affects the network BW and overloads the firewall** |
| Data Link Layer | IP spoofing, ARP spoofing | Disrupts the flow of data across all the ports |
| Physical Layer | Sniffing | Disconnection of links, data destroyed, access control,Environmental issues |