**Attack Surface**

The network attack surface refer to all the points at which a threat actor could gain access to hosts and services.  
  
Using the OSI model we can analyze the potential attack surface:

* Layer 1/2 - allows the attacker to connect to wall ports or wireless networks and communicate with hosts within the same broadcast domain
* Layer 3 - allows the attacker to obtain a valid network address possibly by spoofing and communicate with hosts in other zones
* Layer 4/7 - allows the attacker to establish connections to TCP or UDP ports and communicate with application layer protocols and services.

Each layer requires its own type of security controls to prevent, detect, and correct attacks. Provisioning multiple control categories and functions to enforce multiple layers of protection is referred to as ***defense in depth***.

Security controls deployed to the network perimeter are designed to prevent external hosts from launching attacks at any network layer. The division of the private network into segregated zones is designed to mitigate risks from internal hosts that have either been compromised or that have been connected without authorization.

Typical weaknesses in a network include:

* Single points of failure
* Complex dependencies
* Availability over confidentiality and integrity
* Lack of documentation
* Over dependence on perimeter security