**Protocols and Networking**

It is essential for Cyber Security Professionals to have a solid understanding of how computers communicate. There is much more happening behind the scenes of computer networks than what can be observed when using applications.

**The OSI Model**

The OSI ("Open Systems Interconnection") model represents an easy and intuitive way to standardize the different parts required to communicate across networks.

The model makes it clear what is required to communicate on a network by splitting the requirements into multiple layers.

This is what the OSI Model looks like:

|  |  |
| --- | --- |
| **Layer** | **What it does** |
| 7 - Application | Where humans process data and information |
| 6 - Presentation | Ensures data is in a usable format |
| 5 - Session | Capable of maintaining connections |
| 4 - Transport | Data is forwarded to a service capable of handling requests |
| 3 - Network Layer | Responsible for which path packets should travel on a network |
| 2 - Data Link | Responsible for which physical devices packets should go to |
| 1 - Physical | The physical infrastructure to transport data |

The top 3 layers are typically implemented in software within the Operating System:

|  |  |
| --- | --- |
| **Layer** | **Where it is implemented** |
| 7 - Application | Software |
| 6 - Presentation | Software |
| 5 - Session | Software |

The bottom 3 layers are typically implemented in hardware within devices on the network, e.g. Switches, Routers and Firewalls:

|  |  |
| --- | --- |
| **Layer** | **Where it is implemented** |
| 3 - Network Layer | Hardware |
| 2 - Data Link | Hardware |
| 1 - Physical | Hardware |

Layer 4, the Transport layer, connects the software with the hardware layers.

SDN ("Software Defined Networking") is technology which allows more layers of the hardware to be implemented via software.

**Layer 7 - Application Layer**

The business logic and functionality of the application lies here. This is what the users use to interact with services across a network. Most developers create applications on the Application Layer.

Most of the applications you use are on the Application Layer, with the complexity of the other layers hidden.

Examples of Layer 7 Applications:

* HTTP ("Hypertext Transfer Protocol") - Enables us to access web applications
* FTP ("File Transfer Protocol") - Allows users to transfer files
* SNMP ("Simple Network Management Protocol") - Protocol to read and update network device configurations

There are many applications which uses these protocols like Google Chrome, Microsoft Skype and FileZilla.

You are accessing this class via Layer 7!

**Layer 6 - Presentation Layer**

Typically an unseen layer, but is responsible of adapting, transforming and translating data. This is to ensure the application and layers beneath can understand one another.

* Encoding Schemes used to represent text and data, for example ASCII(American Standard Code for Information Interchange) and UTF(Unicode Transformation Format).
* Encryption for services, for example SSL ("Secure Sockets Layer") and TLS ("Transport Security Layer")
* Compression, for example GZip in use in many implementations of HTTP.

**Layer 5 - Session Layer**

 This layer's responsibility is handling connections between the application and the layers below. It involves establishing, maintaining and terminating connections, otherwise referred to as sessions.

Common protocols which represent the Session Layer well are:

* SOCKS - A protocol for sending packets through a proxy server.
* NetBIOS - An older Windows protocol for establishing sessions and resolving names.
* SIP ("Session Initiation Protocol") - For engaging in VOIP ("Voice Over IP") communications

**Layer 4 - Transport**

The layer which allows applications to be represented on the network.

Some well known applications on this layer:

* TCP ("Transmission Control Protocol") - Used for many applications, ensuring stability, control of how much data can be sent at any given time, reliability and more.
* UDP ("User Datagram Protocol") - Lightweight and quick protocol use for many services.
* QUIC ("Quick UDP Internet Connections") - A protocol designed for faster connections and goes hand-in-hand with the version 2 of the HTTP protocol.

**Layer 3 - Network**

A layer responsible of routing packets between networks via routers.

On this layer, the following protocols reside:

* IP ("Internet Protocol") - Used everyday when accessing the Internet. Comes in two versions, IP version 4 and 6.
* ICMP ("Internet Control Message Protocol") - Used by network devices and network operators, to diagnose network connections or for devices to send and respond to error conditions and more.
* IPSec ("Internet Protocol Security") - Allows encrypted and secure connections between two network devices.

**Layer 2 - Link**

Link networks, as the name implies, consist of protocols designed to send packets through the actual links (physical connections) that network nodes are connected to. A simpler way of thinking of it is that the Link Layer is responsible for moving data from physical over to logical (to the network layer).

Protocols on this layer include:

* Ethernet - An essential protocol used by most operating systems when connecting to networks using a physical cable.
* Wi-Fi ("Wireless Fidelity") - For accessing networks via radio signals. It uses a family of protocols called IEEE 802.11.xx
* NDP ("Neighbor Discovery Protocol") - IP version 6(IPv6) uses this protocol on the Link Layer to gather information required to communicate via IPv6

**Layer 1 - Physical**

Physical layer represents the signaling which allows bits and bytes to transfer between a physical medium. It can be transferred via radio or signals over a cable, using electrical signals or light, for example fiber.

Examples of the Physical Layer protocols includes:

* CAN Bus ("Controller Area Network") - Used in microcontrollers and other devices to communicate to other similar devices, not involving a computer. Often used in ICS ("Industrial Control Systems").
* Ethernet Physical Layer - Used by Ethernet on the physical layer to send signals with speeds up to many gigabits of traffic per second.
* Bluetooth Physical Layer - Bluetooth also has its own specifications on how radio signals should be sent and received.