Network Security Basics

OSI Model

The OSI Model is a conceptual, implementation-neutral model that describes networking in seven separate layers, where each layer covers a set of functions and tasks.
This model helps us communicate while we do network troubleshooting and architecture.

TCP/IP Model

The TCP/IP Model is an implementation-specific networking model that revolves around the TCP protocol and IP addressing which anchor the Internet as we know it.
Its layers include:

- The Network Layer
- The Internet Layer
- The Transport Layer
- The Application Layer

OSI Layers

The OSI layers include: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

- The Physical layer includes physical technologies
- The Data Link layer includes data framing and local MAC addressing
- The Network layer includes connecting to the larger web and IP addressing
- The Transport layer includes protocols that make sure reliable delivery happens
- The Session layer authenticates and maintains communication over a period of time
- The Presentation layer en/decrypts and translates data into presentable form
- The Application layer includes all the applications we interact with that render data

Network Categories

Three broad categories of networks include:

- *Local Area Network (LAN)*, a smaller-sized network that connects multiple devices in a small area
- *Campus Area Network (CAN)*, a larger network that connects multiple computers and devices over a slightly larger area
- *Wide Area Network (WAN)*, the largest-sized network that connects multiple computers, over a geographically large area

The Internet is technically a WAN.

Network

A *network* is two or more computers or devices that are linked in order to share information.
Networking refers to a large set of standards and protocols that organize and regulate the sharing of information.

Network Protocols

A network protocol is a set of standards for Internet traffic.
Among them are the big transport protocols:

- TCP and UDP
- HTTP for web requests
- DNS to convert domain names to IP addresses
- IMAP/POP3 for email
- SSH
- FTP
- SMB for access to specific resources

Network Segmentation

Network Segmentation is the practice of breaking larger networks into smaller, functionally similar networks. This improves both security and performance.

Access Points

Access points are the systems and nodes used to distribute wireless signals.
If an attacker can physically hack an access point, they may be able to attack the users on the network! This is why you should be careful which access points you connect your devices to.

Wireless Security Standard

All wireless activity should be securely encrypted. Currently, the accepted standard for security is WPA2.

- WPA2-Personal will require a single password to access Wi-Fi
- WPA2-Enterprise will require multi-factor authentication