**Introduction to IP 1.5:**

* IP can be seen as a road (Ethernet, DSL, Cable System) and IP is the truck
* OSI Layer 4 refers to the transport layer
* Multiplexing is using many different applications at the same time over the same network
* UDP is referred as unreliable, as there is no error recovery, retransmissions, and no confirmation that it was transferred, with no flow control to go faster or slower
* TCP and UDP ports can be any number between 0 and 65,535
* Port numbers are for communication and not for security
* Web server – tcp/80, VoIP server – udp/5004 and Email server – tcp/143

**Networking Devices 2.1:**

* A switch has bridging done in hardware with application specific integrated circuits with OSI layer 2 rating
* Switches can have multiple ports and features at the core of an enterprise network with 100s to 1000s of connections and can be powered over PoE (power over ethernet)
* Routers route traffic between IP subnets, considered OSI layer 3 switches. Switch at layer 2, router at layer 3. Routers can connect LANS to WANS
* Access points are not wireless routers and can provide an access point in a single device
* Access points are OSI layer 2 devices
* Cable modems are broadband and transmit across multiple frequencies of different traffic types. Data on the cable network is called DOCSIS (Data over cable service interface specification)

**Plans and procedures 3.2:**

* The only constant is change (in IT)
* Changes are the most common risks in the enterprise and occurs very frequently. Can often be overlooked or ignored. Changes require clear policies such as frequency, duration, installation process, and fallback procedures
* There are many different kinds of security incidents, such as phishing attempts, malware, and DDoS attacks that cause outages and downtime.
* Disposal of desktops, laptops, tablets, and mobile devices is important to the system life cycle to the proper handling and disposal of data

**Social Engineering 4.2**

* Denial of service force a service to fail by overloading the service, take advantage of design failure or vulnerabilities (which is why it’s important to patch) and can cause a system to be unavailable
* On-path attacks (man in the middle attack) works by having an attacker redirect the traffic as you’re sending information back and forth to another devices. ARP poisoning is when an attacker spoofs their MAC address in the middle of the conversation
* VLAN hopping is when attackers move from one VLAN to another without going through a router through switch spoofing and double tacking

**Software Tools 5.3:**

* Wireless networks are incredibly easy to monitor, and some network drivers won’t capture wireless information. They may need specialized adapters/chipsets and drivers to view wireless0specific information such as signal-to-noise ratio, channel information, etc.
* Speed test sites allow for bandwidth testing to transfer a file and measure the throughput and provide useful pre- and post- change analysis
* IP ports scanners scan for IP addresses and open ports with operating systems, services, etc. and allow to pick a range of IP addresses to see who responds to the scan. It also allows to visually map the network and gather information on each device