Security Fundamentals

Physical security

Deterrents

Security controls that act as deterrents include warning signs and barbed wire. Their purpose is to deter potential attackers and make them less likely to attempt to gain entry.

- **Warning Signs:** Signs such as “DO NOT ENTER” and “You Are Trespassing” can be enough to make people turn around, as they have been informed that any further activity may be illegal.
- **Fences:** This creates a barrier that can’t be climbed over and requires more effort for attackers to bypass, slowing them down, and giving more time for them to be detected.
- **Guard Dogs:** Security dogs that are trained to bark and cause distress are a strong deterrent.
- **Security Lighting:** Lighting is used to prevent low visibility areas caused by darkness, which could allow an intruder to bypass security controls such as CCTV and Security Guards.
- **CCTV Cameras:** If individuals believe they are being filmed (even if the cameras do not work) then this is likely to deter them from conducting any illegal or malicious activity, as there may be recorded evidence of them conducting a crime.

Monitoring controls

These controls, such as CCTV cameras and intrusion detection systems are implemented to provide real-time monitoring and give security personnel the ability to detect and respond to intruders or insider threats.

- **CCTV:** Closed-circuit television allows monitoring from multiple interconnected cameras.
- **Security Guards:** There needs to be a team that is trained in their use and maintenance so they can fully utilize the security controls and respond to incidents.
- **Intrusion Detection Systems:** These systems have several different triggers that can generate alerts or set off alarms, including thermal (heat) detection, sound detection, and movement detection.

Access controls

Access controls are used to prevent unauthorized people from accessing specific sections of a building or area

- **Electronic Doors:** These secure doors should be used throughout the facility, to limit the areas that a person can access, based on their role.
- **Turnstiles/Gates:** This efficient control is very common in office buildings and requires employees to tap their ID pass on a reader, which will unlock the gate and allow them to pass through.

- **Mantraps:** These are a slow but effective security control, where an individual wanting to access a protected area must go through an initial door into a holding room, where they are inspected from a window or camera before the second door is unlocked.

Endpoint Security

Host Intrusion Detection

Host intrusion detection systems, also known as HIDS, is software installed on an endpoint that allows for the detection of suspicious or malicious activity using rules which are checked against activity to see if it matches any known malicious patterns.

Host Intrusion Prevention

Host intrusion prevention systems, also known as HIPS, is software installed on an endpoint that works similarly to HIDS but is able to take autonomous actions to defend systems once the malicious activity has been detected instead of just alerting human analysts .

Anti-Virus Solutions

This is a fundamental security control that works to detect and remove known malware that is present on the system.

- **Signature-based**
  The AV solution will use signatures which are specific patterns of activity to identify previously documented malware, either removing the file, generating an alert, or quarantining the malware.
- **Behavior-based**
  This type of unconventional AV works to identify suspicious behavior by creating a baseline of "normal" activity and working to identify any deviations or anomalies that don't fit the baseline, as these could indicate suspicious or malicious activity.

Log Monitoring

Endpoints can be configured to send logs to a centralized location, a SIEM platform, where this data is aggregated, normalized, and matched against a number of rules designed to detect and flag suspicious or unusual activity so it can be investigated by security analysts.

Endpoint Detection and Response

EDR agents are pieces of software that sit silently on endpoints and provide logging, monitoring, and reactive capabilities.

Vulnerability Scanning

Routine vulnerability scans should be conducted against endpoints to detect misconfigurations, security flaws, and vulnerabilities that could be exploited by an attacker to gain access to a system, execute malicious code, or cause a denial of service.

- External scans
- Internal scan

Compliance Scanning

Some compliance frameworks require endpoints to meet a minimum standard of security, and vulnerability scanners will often have profiles or pre-set setting configurations to look specifically for details that the compliance framework covers, allowing defenders to see if any systems do not meet the requirements.

Email security

Spam Filter

A spam filter is a piece of software that scans incoming emails to see if they have telltale signs of spam or malicious emails and prevents them from being delivered to employee mailboxes so that they don't fill up with junk or dangerous messages.

Data Loss Prevention

Data loss prevention (DLP) or data leak prevention is a security control that works to prevent sensitive business or personal information from leaving the organization in an unauthorized manner.

Email Scanning

Typically phishing emails will contain either a malicious URL or a malicious attachment (or both), and specially designed scanners will read the email header and body, and work to identify malicious indicators either using patterns or signatures, or blacklists that include lists of known malicious email senders, file hashes, and domain names.

Security Awareness Training

Security awareness training should be a mandatory program that new employees must complete, as well as be completed routinely by all employees, with time frames often dictated under different compliance frameworks.

Network Security

Network Intrusion Detection (NIDS)

Network intrusion detection systems, also known as NIDS, can come in the form of software or physical devices that tap monitor network traffic in order to generate alerts for human analysts to investigate

- Inline
- Network trap
- Passive

Network Intrusion Prevention (HIPS)

Whilst similar to NIDS, network intrusion prevention systems, or NIPS, are able to automatically take defensive actions based on the activity that has been identified

Firewalls

Firewalls are used to separate parts of a network to create private zones by restricting the traffic that can come in or go out.

Log monitoring

Network devices can generate logs, and these logs can be sent to a SIEM platform. By having logs come from systems across the environment, the SIEM is able to provide a dashboard that analysts can utilize to monitor activity and respond to alerts that are generated when suspicious or malicious traffic is detected.

Network Access Control

Network Access Control (NAC) can work to prevent rogue or non-compliant devices from connecting to a private network.

AAA Control Methods

Authentication

This involves using some form of verification to confirm that the identity is correct.

- Something you know
- Something you have
- Something you are

Authorization

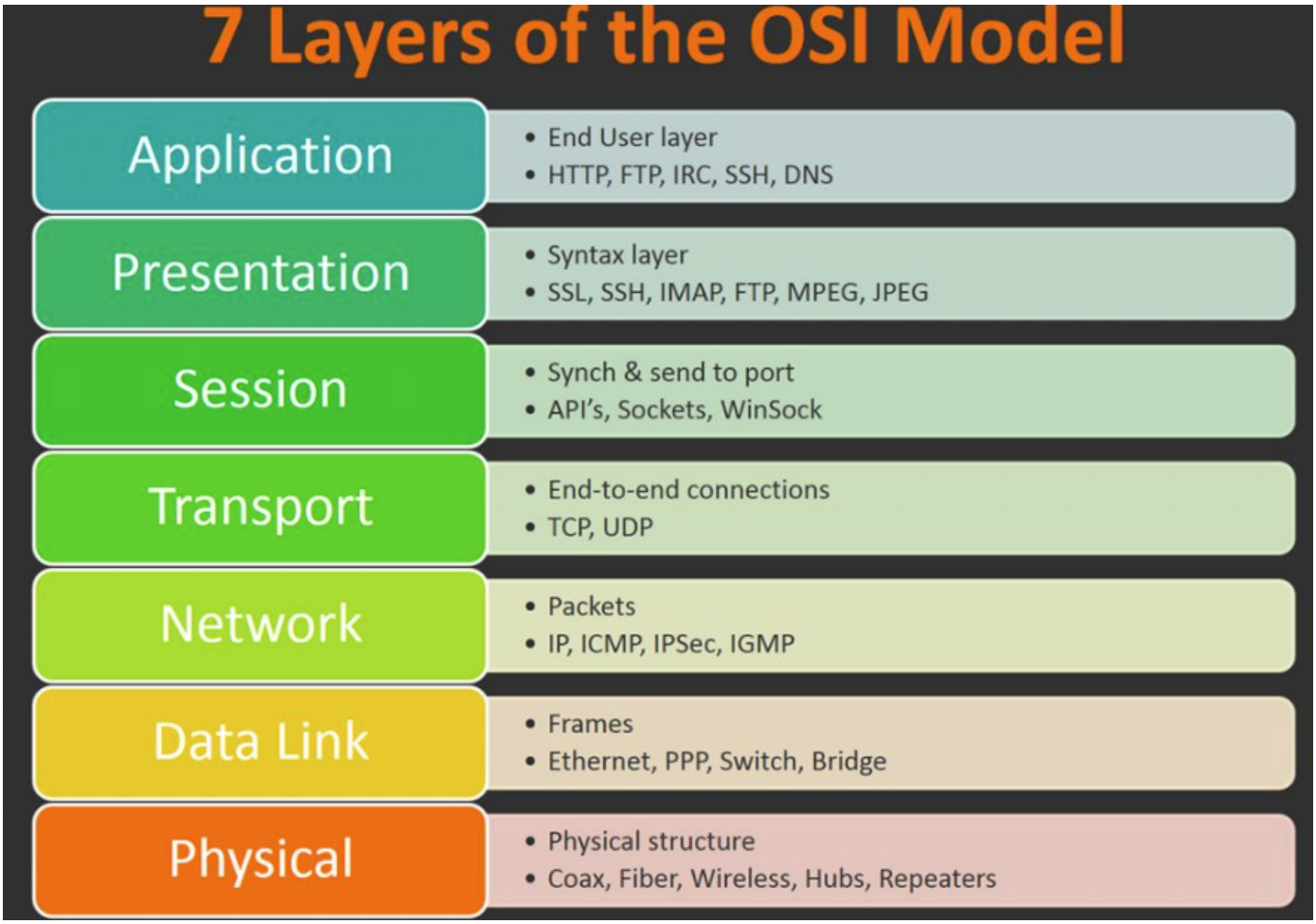
Authorization is all about what the authenticated user is permitted to do.

Accountability

Accountability is the process of being able to identify what has happened and when which can be used as evidence during a security event or incident.

Networking

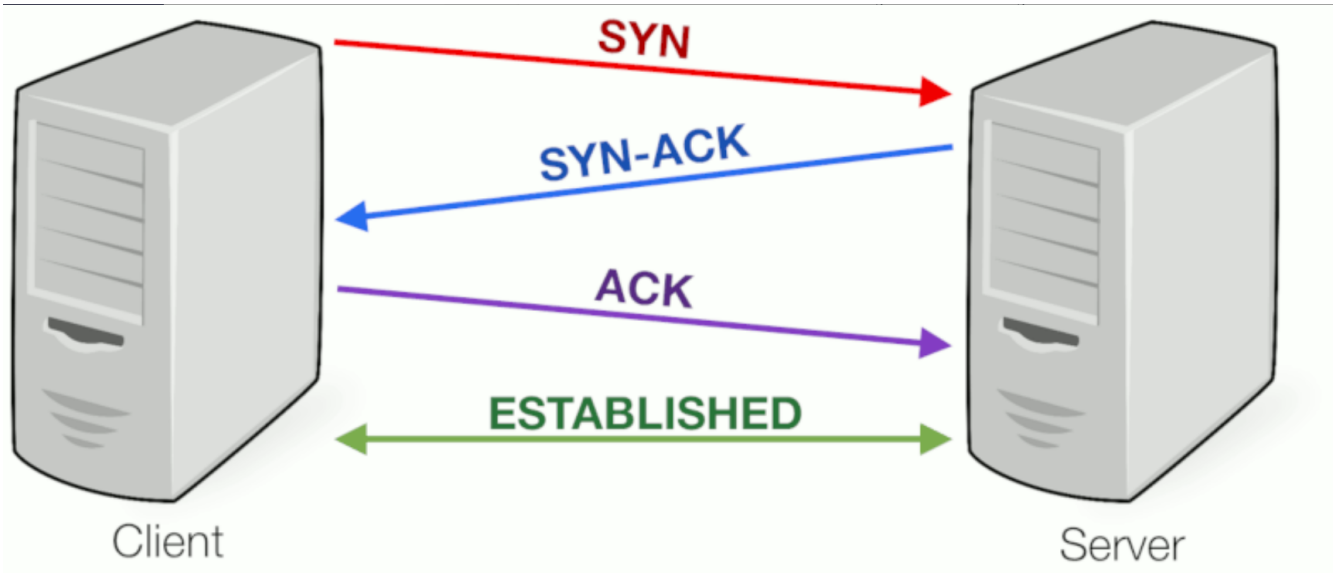
OSI model



Protocols

Transmission Control Protocol (TCP)

- Connection-oriented protocol
- Three-way handshake



User Datagram Protocol (UDP)

- UDP is connectionless
- UDP enables fast, delay-free communication

- UDP does not guarantee the security and integrity of the data

Internet Control Message Protocol (ICMP)

- Used by network devices to diagnose network communication issues
- Used to determine whether or not data is reaching its intended destination in a timely manner

Internet Protocol (IP)

- Provides an identity to a networked device on the internet
- Private IP Addresses -> used inside a network
- Public IP Addresses -> used on the outside of a network and are assigned by an ISP
- Static and Dynamic IPs -> both private IP addresses and public IP addresses are either dynamic or static, which means that, respectively, they either change or they don't.

Media Access Control (MAC)

- A hardware identification number that uniquely identifies each device on a network
- The MAC address is manufactured into every network card, such as an Ethernet card or Wi-Fi card, and therefore cannot be changed
- MAC addresses are made up of six two-digit hexadecimal numbers, separated by colons

Network devices

Switch

- A switch works as a smart version of a hub because it actually understands where to send data, instead of sending it to everyone.

Router

- A router is a network device that forwards data based on a logical address

Hub

- When a system sends data to the hub on one port, the hub will broadcast these to all other attached devices

Bridge

- A network bridge device works to connect separate networks to make them into one larger network.

Firewall

- A firewall is a network device that provides fundamental network security, by monitoring incoming and outgoing traffic and determining whether to allow or block it, based on rules.
- This allows us to create private networks, where only intended communications can come in, or out.

Command Line Tools

- **IP, or ipconfig (Windows)**
  Command-line tool that shows the current network configuration of the device that you are on.
- **Traceroute, or tracert (Windows)**
  Command-line tool that allows you to see the path that network packets take when going from one host to another.
- **Dig, or Nslookup (Windows and Linux)**
  Command-line tool that is used to query DNS servers for information about a specific domain.
- **Netstat (Windows and Linux)**
  Command-line tool that monitors the TCP and UDP connections on your host system.
- **Nmap (Network Mapper)**
  Tool for performing Network Discovery.

Ports and Services

In computer networking, a port is a communication endpoint. At the software level, a port identifies a specific process or a type of network service.

- Well-known ports range from 0 to 1023 (This is where some of the most common ports are.)
- Registered ports range from 1024 to 49151.
- Private ports range from 49152 to 65535. (These are typically used for "ephemeral" ports, which is the name given to the source port used by a client in a server-client communication. For example, if we're connecting to a web server on port 443 HTTPS (destination port) then our source port would be a random port between 49152 to 65535.)

Port 20, 21 - File Transfer Protocol (FTP)
Port 22 - Secure Shell (SSH)
Port 23 - Telnet
Port 25 - Simple Mail Transfer Protocol (SMTP)
Port 53 - Domain Name System (DNS)
Port 67, 68 - Dynamic Host Configuration Protocol (DHCP)
Port 80 - Hypertext Transfer Protocol (HTTP)
Port 443 - Hypertext Transfer Protocol Secure (HTTPS)
Port 514 - Syslog (UDP)

Risk
The possibility of a negative impact on practically anything.

Vulnerability
A weakness that can be exploited by a threat.

Risk Assessments
Risk assessments are conducted to identify and determine the impacts of risk, the likelihood and the consequences should a risk materialize.

Managing Risk

Policies

A policy is a plan of intent or course of action towards a particular domain. Policies are at the highest level, followed by procedures and standards, and then guidelines.

- Acceptable Use Policy (AUP)
- Service Level Agreement (SLA)
- Bring Your Own Device (BYOD)
- Memorandum of Understanding (MOU)

Compliance

- Compliance is defined as following rules and meeting requirements for specified frameworks.
- Organizations operating in different industries will have specific compliance frameworks that they need to comply with.
- For example, businesses that process or store data on citizens of the European Union (EU) will need to comply with the General Data Protection Regulation (GDPR), while organizations that process card payments will need to meet the requirements of the Payment Card Information Data Security Standard (PCI DSS).

The General Data Protection Regulation (GDPR)

A regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas, with the primary aim to give control to individuals over their personal data.

ISO 27001

An information security standard . Organizations that meet the requirements may be certified by an accredited certification body following the successful completion of an audit.

PCI DSS

A security standard for organizations that handle branded credit cards from the major card schemes.

The standard was created to increase controls around cardholder data to reduce credit card fraud.

HIPAA

A regulation intended to help covered entities and their business associates protect Electronic Protected Health Information (ePHI). HIPAA applies to companies that provide services that would use e-PHI such as suppliers or outsourced IT providers.The primary goal of HIPAA is to protect ePHI which includes, name, dates such as birth, admission, discharge, death, telephone number, SSN, photographs, address, etc. Companies under this regulation will need to implement technical and procedural controls to protect this information and perform risk analysis on risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.

Change Management

Change management is the process of ensuring that changes within an organization are planned, supported, well documented, and audit-able.

Patch Management

It involves the ability to deploy patches and security fixes to IT assets that require them, such as Windows updates to laptops and servers, and new versions of software such as web browsers.By deploying patches, an organization can remediate vulnerabilities that are present in older versions of software or the operating system and reduce the risk to the company.

- **Windows Server Update Services (WSUS)**
  WSUS enables IT teams to deploy the latest Microsoft product updates. You can use WSUS to fully manage the distribution of updates that are released through Microsoft Update to computers on your network.
- **Microsoft System Center Configuration Manager (SCCM)**
  Microsoft’s SCCM is a paid solution that acts as an asset inventory, assists in software installation, and deploys updates and security patches to systems across the network. SCCM uses Microsoft’s WSUS as we covered above to check for and install updates, however, it provides users with additional patch management control over when and how patches are applied.