IT Security Foundations: Network Security

Key Terms:

- **Access Control List (ACL):** A list of rules that specifies which users or systems are granted or denied access to a particular object or system resource
- **Advanced threat management:** Devices that have additional features such as AI, and reputation-based monitoring to defend against threats that use known and unknown attack vectors
- **Egress filtering:** Prevents certain packets from leaving the network
- **Firewall:** A hardware or software-based method to control incoming and outgoing traffic and is based on a set of rules that either permit or deny traffic on a network or host
- **Hardware firewalls:** Firewalls that prevent unauthorized network access by filtering traffic and can provide varying levels of protection and performance
- **High-end hardware firewalls:** Dedicated appliances that provide enhanced performance and protect the edge and critical infrastructure environments without reducing network performance
- **Honeypot:** A system set up to lure a would-be attacker, to observe their behavior
- **Ingress filtering:** Prevents attack packets such as malware from entering the protected network
- **Intrusion detection and prevention systems:** Sensors that monitor ingress and egress traffic using deep packet inspection and a combination of signature and heuristic-based analysis for unusual or suspicious data or activities
- **Intrusion detection system:** A device that sits out-of-band and passively monitors network traffic for malicious activity; if detected, it will log information about the activity and report an attack
- **Intrusion prevention system:** A device that sits in-band and actively monitors network traffic for malicious activity; if detected, it blocks the attack and logs information about the activity
- **Personal firewalls:** Software firewalls are used on laptops or desktops that support stateful inspection and network address translation, and allow users to set rules for specific applications

- **Proxy server:** A web server that acts as a gateway between a client application, for example, a browser and the real server
- **Router firewall:** A physical device controls incoming and outgoing network traffic based on predetermined security rules and uses network address translation to mask private IP addresses
- **Unified threat management (UTM):** Next-generation firewalls that combine firewall capabilities with intrusion prevention, antivirus, antispyware, data loss prevention, and content filtering features

Chapter Links

- Sample attack logs: https://ossec-docs.readthedocs.io/en/latest/docs/log_samples/misc/attacks.html
- Project Honeypot collects data about spammers and spambots: https://www.projecthoneypot.org/index.php
- Learn more about applications associated with port 6000 by visiting: https://www.speedguide.net/port.php?port=6000
- Discover what applications are associated with port 8585 by visiting: https://www.speedguide.net/port.php?port=8585
- View possible indicators of compromise (IOCs) found within a packet capture at VirusTotal.com: https://www.virustotal.com/gui/file/fc31b3b15bc7f704056adc94bc16c63aba4143ac6f535e5d86c2204e221066b4/details
- A great deal of information can be obtained by investigating data found in a honeypot. The following outlines the different types of data you can find: https://isc.sans.edu/forums/diary/CSAM+Web+Honeypot+Logs/16718
- Many times, malicious actors will use common usernames and passwords to gain access to a system. Read more here: https://isc.sans.edu/forums/diary/Honey+Pot+Entertainment+SSH/19121
- Learn more about Cerber ransomware by visiting: https://www.avast.com/c-cerber