Cybersecurity 101: Day 1.1 Cheatsheet

Key Terms

- **Cybersecurity**: The assessment of threats and the mitigation of risk.

  > **Example**: An organization is launching a new website and is concerned about attacks interrupting service due to system request overload (*denial of service, or *DoS** attacks). The security and IT organizations develop procedures to identify threats and protect applications and the network (e.g., packet monitoring and management, escalation management).

- **Threat assessment**: A structured process of identifying the risks posed to a group or system.

  > **Example**: The National Institute of Standards and Technology outlines structured processes and frameworks for identifying, estimating, and prioritizing risks to individual, organizational and operational assets. (*NIST Special Publication 800-30*)

- **Risk mitigation**: The process of reducing the impact of a negative event, and/or the likelihood that it will reoccur.

  > **Example**: Reducing the risks associated with signals from wireless access points that transmit beyond an organization's controlled boundaries. One mitigation action is to reduce the power of wireless transmissions so that signals are less likely to extend beyond the organization's physical perimeters.

- **Social engineering**: The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by gaining confidence and trust.

  > **Example**: An attacker calls and claims to be from your internet provider (this is an example of *vishing*, or *voice phishing*) and asks you questions about your account, aiming to trick you into giving account information or login credentials (*credential reuse*).

- **Phishing attack**: A technique for attempting to acquire sensitive data, such as credit card numbers, usernames, or passwords, through fraudulent solicitation (e.g., email). The

perpetrator pretends to be a reputable business or person.

> **Example**: During the World Cup in Russia, scammers sent out phishing emails to fans offering free trips, in order to access personal information.

- **Malware**: Hardware, software, or firmware meant to perform an unauthorized process that will compromise the confidentiality, integrity, or availability of a system (e.g., a virus, worm, Trojan horse, or other code-based entity that infects a host).

> **Example**: In May of 2017, the WannaCry worm spread rapidly across a number of computer networks, infecting Windows computers. It encrypts files on the machine's hard drive and demands a ransom payment in Bitcoin in exchange for decryption.

- **Man-in-middle attack (MitM)**: An attack where the adversary positions themself between the user and the system so that they can intercept and alter data traveling between them.

> **Example**: We download and update software daily. A remote hacker can use the lack of integrity verification (e.g., hash value) of downloads or update information to manipulate a software package with an MitM attack.

- **Packet sniffer**: Software that monitors network traffic on wired or wireless networks and captures packets. Packet sniffers are used by network managers to monitor and analyze traffic, but hackers also use them.

> **Example**: A user downloads a file from the internet. The file is a packet sniffer that, when installed on the network, can record and transmit any data to a hacker's command and control server.

- **Brute force attack**: An attack that involves trying all possible authentication combinations to find a match.

> **Example**: These attacks are often used for attacking authentication and discovering hidden content and pages within a web application. The brute force attack on Alibaba compromised 21 million user accounts using a database of 99 million usernames and passwords.

- **Code injection**: Type of attack that injects code that is then interpreted and executed by the target application.

> **Example**: HTML injections are used to change a website or to steal personal identifiable information (PII). HTML injections can occur via a website link, data, or input fields on web forms.

- **Keylogger**: A program designed to record which keys are pressed on your computer keyboard. It can obtain passwords or encryption keys and use these to bypass security measures.

  > **Example**: ZeuS/Zbot is a modular banking Trojan which uses keystroke logging to record credentials when a user visits a banking website.