Malware Types

- Virus
    - Definition:
        - A type of malware that installs itself on your computer, which can start to corrupt various parts of the machine, including files, documents, or applications/programs.
- Worm
    - Definition:
        - A self-replicating malware that does not require human interaction to begin infecting the original host machine and spread to other computers or networks without the need for user interaction.
    -
- Trojan Horse (Trojan)
    - Definition:
        - A type of malware that hides itself within legitimate software on the host machine or within files on the machine to avoid being detected before it can execute its malicious code when activated. It is also worth noting that Trojans are not self-replicating types of malware.
- Ransomware
    - Definition:
        - A type of malware that locks down a device until a predefined/specified ransom has been paid. If the demand is not met, there is the possibility that the attacker could delete information/data/files from the infected machine/network or keep them encrypted permanently.
- Spyware
    - Definition:
        - Malware that is on your end-device that monitors user activity on a given device and records it for later use/analysis
- Adware
    - Definition:
        - A type of malware that is invasive in nature and can display unwanted advertisements on your device, impacting system performance or overall user experience.
- Rootkit
    - Definition:
        - Malware that is inserted into a workstation, granting the attacker root/administrative access and privileges, is also malware that hides itself, making it very hard to detect.
- Keylogger
    - Definition:
        - Malware on your computer that tracks and logs the keystrokes a person takes, and allows the attacker to review a log of the keystrokes afterwards

- Botnet Malware
    - Definition:
        - A kind of malware that affects a large number of computers that, once activated, can be utilized at once to achieve the goal of the malicious attackers, such as a DOS/DDOS (Denial-of-Service/Distributed Denial-of-Service) attack, which can be used to make services or servers unresponsive due to all the traffic being sent to the target at one time.
- Fileless Malware
    - Definition:
        - Malware on your computer that is not associated with any files, making it potentially much more challenging to detect. It hides itself within legitimate tools on the machine or runs within the RAM rather than being stored within a file.

Authentication Methods

- Password-Based Authentication
    - Password-based authentication requires a user to enter a known password into a workstation or device to gain access.
- Multi-Factor Authentication
    - Multi-Factor Authentication requires a user to utilize multiple types of authentication to prove their identity and gain access. These can be, but are not limited to:
        - Something you know (password)
        - Something you are (fingerprint or retina)
        - Something you have (physical token, phone, badge)
- Biometric Authentication
    - Biometric Authentication uses unique physical characteristics, such as fingerprints or retina scans, to verify someone's identity and grant access.
- Single-Factor Authentication
    - Single-factor authentication requires a user to use just one method of authentication to prove their identity.
- Two-Factor Authentication
    - Two-factor authentication requires a user to utilize exactly two different methods of authentication to prove their identity and gain access.
- Token-Based Authentication
    - Token-based authentication requires a user to use a physical or digital token to authenticate their identity. This is done by using something that you have, such as a physical key token or an OTP (one-time password).
- Certificate-Based Authentication
    - Certificate-Based Authentication requires that a user have a digital certificate signed by a trusted third-party certificate authority installed on their machine to verify the user or machine as a trusted one.

CIA Triad

- The CIA Triad is a fundamental security model that guides security decisions and informs the development of security policies.

- Confidentiality
    - Ensuring that data remains secure and private from unauthorized access.
- Availability
    - Ensuring that data, as well as systems/services, remain accessible at all times or as much as possible.
- Integrity
    - Ensuring that data remains accurate, complete, and unaltered from any unauthorized users or processes.

Common Attacks

- Phishing
    - A method that attackers will use to gain confidential information or credentials from users by using email or other methods. These methods, such as emails, will be formatted to appear genuine or legitimate, typically seeming to come from a higher-level official or a trusted external party.
- Brute Force Attack
    - A type of attack that attempts to gain access to a server or system by trying many possible combinations of credentials until it finally works or is stopped.
- Denial-of-Service Attacks
    - A type of attack that seeks to target a system or server and try to knock it offline by flooding it with a massive amount of requests that, in the end, overload the system and cause it to either crash or completely halt.
- Distributed Denial-of-Service Attacks
    - This type of attack is similar to a Denial-of-Service attack, but is on a much larger scale. This attack will utilize a wide array of compromised machines and, once activated, will leverage these machines to target the victim's system or server.
- Man-in-the-Middle (MitM) Attack
    - A type of attack in which the attacker will place themselves between the user and the system or server that they are trying to access. The attacker will intercept or alter any information sent back and forth between the user and server, which can include PII (Personally Identifying Information) or user credentials.
- Password Spraying
    - This is a type of attack in which attackers attempt to use a small number of commonly known passwords across multiple user accounts, hoping that some users have weak or easily guessed credentials.
- Malware Infection

    - A type of attack in which an attacker installs malicious software on a system or server that impacts confidentiality, integrity, or availability.
- Social Engineering
    - A type of attack in which the attacker will attempt to utilize or trick a user into giving them access or information. This can be achieved through a piggybacking/tailgating attempt, which allows the attacker to gain access to the building, or by using phishing/vishing to trick the user into divulging sensitive information over email or a phone call.

Basic Network Security Concepts

- These are foundational concepts used to secure computer networks.

- Firewall
    - A firewall is a device or software that sits between the outside world and your network, controlling what traffic is allowed to flow in and out. It improves security by monitoring incoming and outgoing connections and allowing or denying access based on a set of predefined rules.
- Virtual Private Network (VPN)
    - A VPN is like a secure tunnel that allows you to connect to a private network, such as a corporate network, from a remote location. It protects data by encrypting the connection between the user and the desired network.
- Encryption
    - Encryption protects data by converting it into a secure format that unauthorized users cannot read. Depending on the type of encryption used, either the same key (symmetric encryption) or two different keys (asymmetric encryption) are used to encrypt and decrypt the data.
- Network Segmentation
    - Network segmentation divides a network into smaller, isolated segments, rather than maintaining it as a single, extensive network. This enhances security by restricting access to resources and making it more difficult for attackers or malware to move between different parts of the network.
- Intrusion Detection System (IDS)
    - An IDS monitors network traffic for suspicious activity or anomalies. When something unusual is detected, it generates an alert for IT or security personnel to investigate.
- Intrusion Prevention System (IPS)
    - An IPS monitors network traffic and actively blocks malicious activity based on predefined rules. In addition to stopping threats, it generates alerts that allow security personnel to review the incident.
- Least Privilege
    - The principle of least privilege states that users should only be given the access necessary to perform their job. Limiting access reduces the risk of misuse, mistakes, or security breaches.

- Secure Protocol (HTTPS, SSH)
    - Secure protocols, such as HTTPS, SSH, and SFTP, are enhanced, encrypted versions of older protocols like HTTP, Telnet, and FTP. They help protect data during transmission by preventing unauthorized access or interception.

Defensive Security Concepts

- Defensive security concepts focus on protecting systems, networks, and data from attacks and minimizing potential damage.
- Access Control
    - Access control or access control lists are created and maintained by an organization to provide and distribute access to services and resources to users while also restricting other users from accessing those same resources. This minimizes the chance of misuse or unauthorized access, as the access control limits users to having access only to what they need.
- Security Awareness Training
    - Security awareness training is a crucial initiative that can be implemented within an organization to educate and train users on recognizing various types of attacks and intrusion methods, as well as the proper response protocols to follow in the event of malicious activity or an incident.
- Patch Management
    - Proper patch management keeps your organization safe and secure by ensuring that all operating systems, services, and applications being utilized within your organization are up-to-date and have any known vulnerabilities remediated before attackers can exploit them.
- Antivirus / Anti-Malware
    - Antivirus and anti-malware software are installed on user devices to protect them from malicious software being installed or files being downloaded, which can corrupt and expose the device and organization to breaches.
- Logging and Monitoring
    - Logging and monitoring allow organizations to observe activity on networks and servers by recording events in log files. These logs can be reviewed later to determine whether malicious activity occurred, where it happened, and how it impacted systems. This information enables technicians to understand incidents better and respond more effectively.
- Backups and Recovery
    - Backups and recovery involve creating copies of data and system configurations at specific points in time. These backups allow organizations to restore systems after an incident, such as malware infections or data loss, by reverting to a known safe state.
- Incident Response
    - An incident response plan is a documented set of steps an organization follows when a security incident occurs. It typically includes investigation, containment,

recovery, and a post-incident review to understand what happened and how similar incidents can be prevented in the future.

Threat vs Vulnerability vs Risk

- These concepts are used to understand what can cause harm, identify weaknesses, and assess the likelihood of damage occurring.
- Threat
    - A threat is any **potential cause of harm** to a system, network, or organization. This can include attackers, malware, natural disasters, or accidental human actions.
- Vulnerability
    - A vulnerability is a **weakness** in a system, network, application, or process that **can be exploited by a threat** to gain unauthorized access or cause damage.
- Risk
    - Risk is the **likelihood** that a **threat will exploit a vulnerability** and the **potential impact** or damage that could result from that exploitation.
- Example of how they all connect
    - Example 1:
        - Someone attempting to harm you is a **threat**
        - You being unprepared or out of shape is a **vulnerability**
        - The possibility of you being injured is the **risk**
    - Example 2:
        - A hacker attempting to break into a system is a **threat**
        - The weak or reused password on an account is a **vulnerability**
        - The possibility of the account being compromised and data being stolen is the **risk**