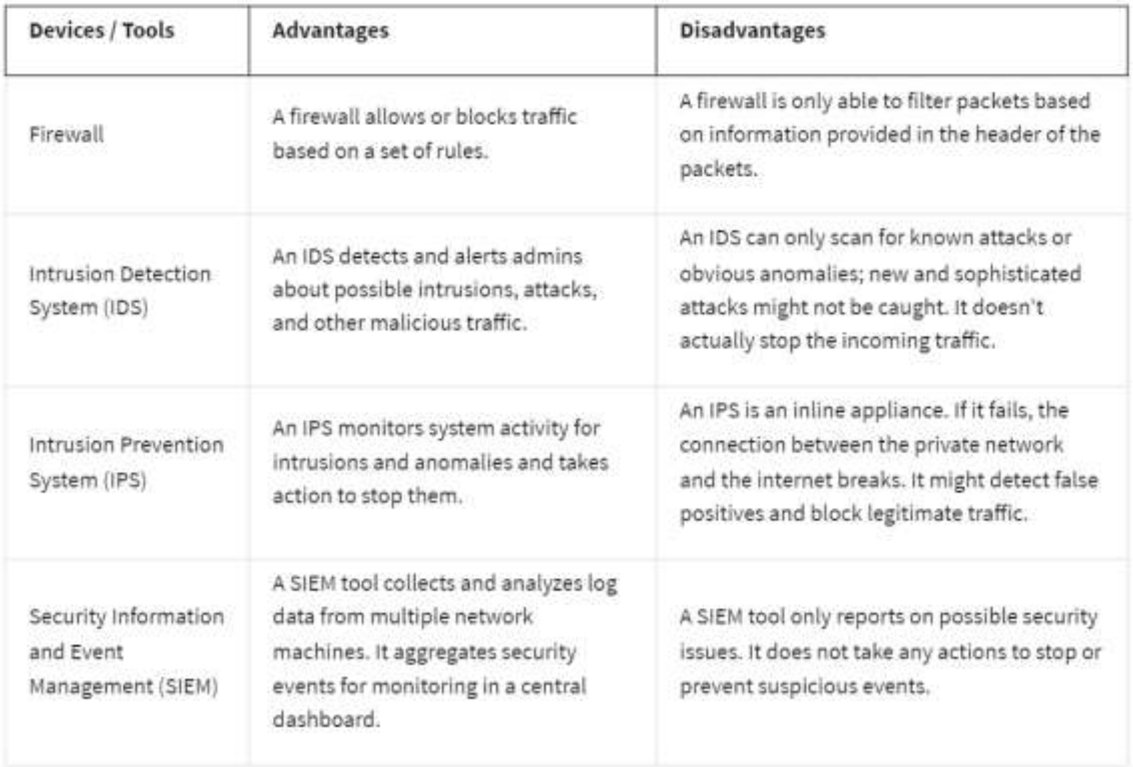
- Security hardening: The process of strengthening a system to reduce its vulnerabilities and attack surface
- Patch update: A software and operating system update that addresses security vulnerabilities within a program or product
- Baseline configuration (baseline image): A documented set of specifications within a system that is used as a basis for future builds, releases, and updates
- Multi-factor authentication (MFA): A security measure which requires a user to verify their identity in two or more ways to access a system or network
- Network log analysis: The process of examining network logs to identify events of interest
- Penetration testing (pen test): A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes
- Principle of least privilege: Access and authorization to information only last long enough to complete a task



Devices / Tools	Advantages	Disadvantages
Firewall	A firewall allows or blocks traffic based on a set of rules.	A firewall is only able to filter packets based on information provided in the header of the packets.
Intrusion Detection System (IDS)	An IDS detects and alerts admins about possible intrusions, attacks, and other malicious traffic.	An IDS can only scan for known attacks or obvious anomalies; new and sophisticated attacks might not be caught. It doesn't actually stop the incoming traffic.
Intrusion Prevention System (IPS)	An IPS monitors system activity for intrusions and anomalies and takes action to stop them.	An IPS is an inline appliance. If it fails, the connection between the private network and the internet breaks. It might detect false positives and block legitimate traffic.
Security Information and Event Management (SIEM)	A SIEM tool collects and analyzes log data from multiple network machines. It aggregates security events for monitoring in a central dashboard.	A SIEM tool only reports on possible security issues. It does not take any actions to stop or prevent suspicious events.

Created By: Abdelrahim Alsadiq

- **A brute force attack is a trial-and-error process of discovering private information. There are different types of brute force attacks that malicious actors use to guess passwords, including:**
  - Simple brute force attacks. When attackers try to guess a user's login credentials, it's considered a simple brute force attack.
  - Dictionary attacks when attackers use a list of commonly used passwords and stolen credentials from previous breaches to access a system.
- **Some common measures organizations use to prevent brute force attacks and similar attacks from occurring include:**
  - **Salting and hashing:**
    - Hashing converts information into a unique value that can then be used to determine its integrity. It is a one-way function, meaning it is impossible to decrypt and obtain the original text
    - Salting adds random characters to hashed passwords. This increases the length and complexity of hash values, making them more secure.
  - **Multi-factor authentication (MFA)**
  - **CAPTCHA and reCAPTCHA**
  - **Password policies**: Organizations use password policies to standardize good password practices throughout the business.