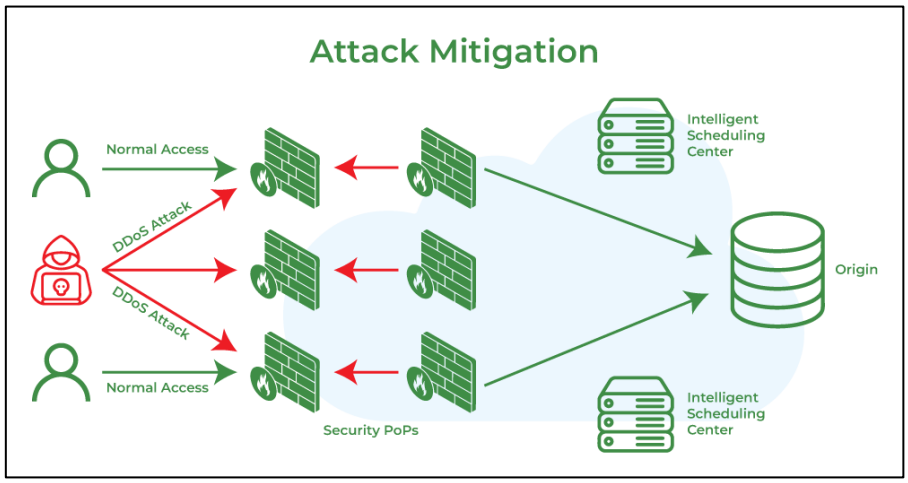
Attack Mitigation

Attack Mitigation is a process of monitoring the vulnerabilities in your system to stop the threat from penetrating the network. It is a good practice, but it should not be mistaken for security measures. It's important to prevent attacks right at their onset by using an appropriate measure, which is also referred to as defense in ethical hacking. This will reduce the number of successful attacks over time without sacrificing network security should something go wrong with your defenses while you're performing mitigation processes. It is not just about preventing potential attacks, but also preventing incidents. This can be achieved by identifying the vulnerabilities that can have negative effects on your business and working to mitigate the risks.



Vulnerability: A vulnerability refers to a weakness or inadvertent error in your system that allows outsiders such as hackers to gain access to your system without you being aware. A hacking attempt is called an attack if it breaks down security measures and causes damage or threat to an organization's data and intellectual property.

Mitigation: Mitigation refers to the process of removing or blocking access from a source with malicious intent, usually by using appropriate control systems. Using mitigation of existing vulnerabilities prevents future instances of attacks from occurring in normal conditions. Attack Mitigation in Ethical Hacking is an ongoing process to ensure the protection of our system from acts of malicious intent.

Steps of Mitigation of a cyberattack:

- **Authentication:** Authentication is the process of determining whether someone is who they claim to be. As you can see from the following diagram, authentication removes access from an attacker only after the attack has been detected by an IDS/IPS, and only when it's known that access was gained inappropriately. Attackers typically follow this path. They scan your network in order to find IPs with vulnerabilities.
- Next, they'll attempt to gain unauthorized access by exploiting those vulnerabilities
- Then they'll use techniques like Credential Harvesters or Phishing to gain access to sensitive information
- Finally, they'll use that sensitive information to compromise your systems (or your clients' systems).

Access Control in Computer Network

Access control is a method of limiting access to a system or to physical or virtual resources. It is a process by which users can access and are granted certain prerogative to systems, resources or information. Access control is a security technique that has control over who can view different aspects, what can be viewed and who can use resources in a computing environment. It is a fundamental concept in security that reduces risk to the business or organization. To establish a secure system, electronic access control systems are used that depend on user credentials, access card readers, auditing and reports to track employee access to restricted business locations and areas. These systems include access control panels to prohibit entry to sensitive areas like alarms and lock down areas to prevent unauthorized access or operations. Access control systems perform identification, authentication, and authorization of users and entities by evaluating required login credentials that may include passwords, pins, bio-metric scans or other authentication factors. There is multi-factor authentication which requires two or more authentication factors which is often an important part of the layered defense to protect access control systems.

Authentication Factors:

- Password or PIN
- Bio-metric measurement (fingerprint & retina scan)
- Card or Key

For computer security, access control include the authorization, authentication and audit of the entity trying to gain access. Access control models have a subject and an object.

The Subject-the human user-is the one trying to gain access to the object-usually the software. In computer systems, an access control list contains a list of permissions and the users to whom these permissions apply.

Authentication Mechanism:

1. Two-factor authentication
2. Multi factor authentication
3. one-time password

4. Three-factor authentication
5. Bio metrics
6. Hard Tokens
7. Soft Tokens

Different access control models are used depending on the compliance requirements and the security levels of information technology that is to be protected. Basically access control is of 2 types:

1. **Physical Access Control:** Physical access control restricts entry to campuses, buildings, rooms and physical IT assets.
2. **Logical Access Control:** Logical access control limits connections to computer networks, system files and data.

Access Control Models:

1. **Attribute-based Access Control (ABAC):** In this model, access is granted or declined by evaluating a set of rules, policies, and relationships using the attributes of users, systems and environmental conditions.
2. **Discretionary Access Control (DAC):** In DAC, the owner of data determines who can access specific resources.
3. **History-Based Access Control (HBAC):** Access is granted or declined by evaluating the history of activities of the inquiring party that includes behavior, the time between requests and content of requests.
4. **Identity-Based Access Control (IBAC):** By using this model network administrators can more effectively manage activity and access based on individual requirements.
5. **Mandatory Access Control (MAC):** A control model in which access rights are regulated by a central authority based on multiple levels of security. Security Enhanced Linux is implemented using MAC on the Linux operating system.
6. **Organization-Based Access control (OrBAC):** This model allows the policy designer to define a security policy independently of the implementation.

7. **Role-Based Access Control (RBAC):** RBAC allows access based on the job title. RBAC eliminates discretion on a large scale when providing access to objects. For example, there should not be permissions for human resources specialist to create network accounts.
8. **Rule-Based Access Control (RAC):** RAC method is largely context based. Example of this would be only allowing students to use the labs during a certain time of day.