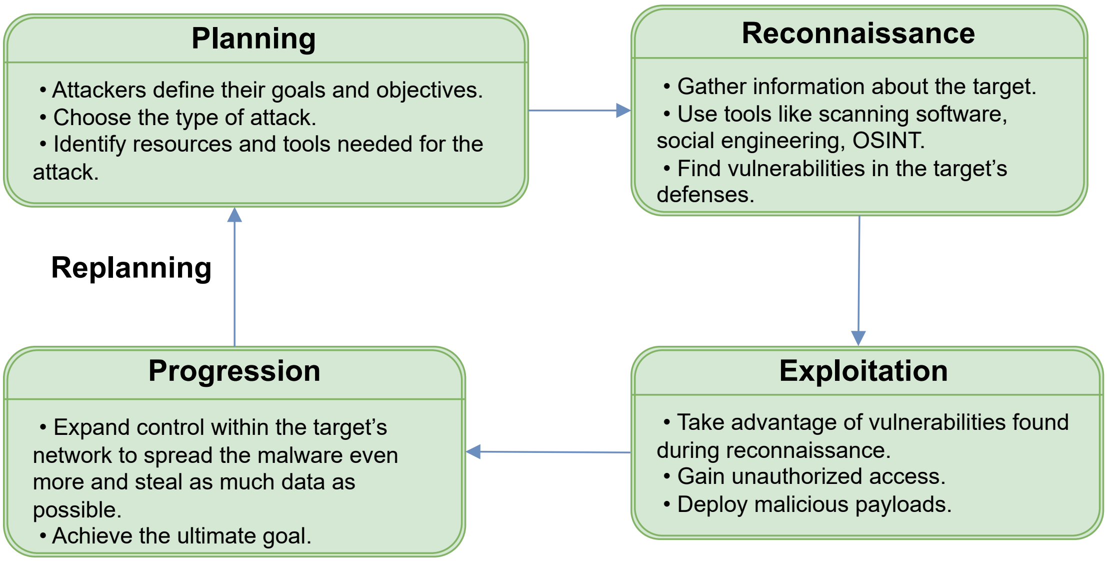
Chapter 1: Introduction

1 Steps Of An Attack


Planning
• Attackers define their goals and objectives.
• Choose the type of attack.
• Identify resources and tools needed for the attack.
Reconnaissance
• Gather information about the target.
• Use tools like scanning software, social engineering, OSINT.
• Find vulnerabilities in the target's defenses.
Exploitation
• Take advantage of vulnerabilities found during reconnaissance.
• Gain unauthorized access.
• Deploy malicious payloads.
Progression
• Expand control within the target's network to spread the malware even more and steal as much data as possible.
• Achieve the ultimate goal.
Replanning

2 Reasons for Poor Security

Reasons

- **Insufficient Budget**: Approximately $\frac{1}{4}$ of issues arise due to inadequate funding for cybersecurity initiatives and personnel.
- **Unqualified Personnel**: A lack of skilled and properly trained cybersecurity professionals.
- **Poor Administration**: Inefficient management and lack of synchronization in security policies and practices.

3 Impacts of a Cyberattack

Impacts

- **Data Breach**: Unauthorized access to sensitive client or organizational data. This may include encrypting data for ransom (ransomware), sharing confidential information, or selling it on the dark web.
- **Denial of Service (DoS)**: Disrupting or halting the services of an organization, making them inaccessible to users.
- **Financial Loss**: Hacking into bank accounts, demanding ransom (ransomware attacks), or causing service interruptions that result in revenue loss.
- **Damage to Reputation**: Eroding client trust or tarnishing someone's reputation by exposing compromised or sensitive data.
- **Loss of Clients**: Organizations may lose clients due to the exposure of sensitive information, compromised systems, server outages, and interruptions in services.

4 Information System

Definition

A set of active applications, services, and other components that allow for the management of informations. Vulnerabilities can affect all components of the information system (IS).

5 Responses to Cyberattacks

Responses

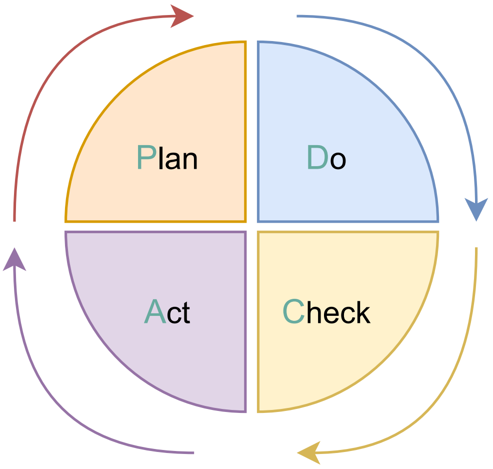
- **Reduce the Impact**: Taking measures to minimize the damage caused by the cyberattack, such as isolating affected systems, restoring backups, or limiting access.
- **Accept the Risk**: The least effective response, where no action is taken to counter the attack. This could include surrendering to attackers' demands, such as paying a ransom.
- **Refuse or Resolve the Risk**: Actively countering the attack by refusing to comply with attackers and taking corrective actions to fix vulnerabilities or breaches.
- **Transfer the Responsibility**: Shifting the burden of dealing with the cyberattack to a third party, such as an insurance provider or a managed cybersecurity service.

6 Steps For Protection (Deming's Wheel)

PDCA

The PDCA (Plan-Do-Check-Act) cycle is a continuous improvement process widely used in cybersecurity to ensure effective protection and adapt to evolving threats. Below are the four key steps:

- **Plan**: Identify goals, assess risks, and develop strategies to strengthen cybersecurity.
- **Do**: Implement the cybersecurity measures, like deploying firewalls and training staff.
- **Check**: Monitor and evaluate the effectiveness of security measures through audits and testing.
- **Act**: Address weaknesses and refine security measures to adapt to new threats.


Plan
Do
Act
Check