2.1.5 Attack and Defense Strategy Overview

General attack strategies incorporate some or all of the techniques explained in the following table:

Step	Description
Reconnaissance	*Reconnaissance* is the process of gathering information about an organization, including: - System hardware information - Network configuration - Individual user information
Social Engineering	*Social engineering* is the process of manipulating others to give you sensitive information such as: - Intimidation - Sympathy
Technical	A *technical* approach is using software or utilities to find vulnerabilities in a system. - Port scan - Ping sweep
Breach	A *breach* is the penetration of system defenses, achieved through information gathered by reconnaissance to penetrate the system defenses and gain unauthorized access.
Escalate Privileges	*Escalating privileges* is one of the primary objectives of an attacker and can be achieved by configuring additional (escalated) rights to do more than just breaching the system.
Create a Backdoor	*Creating a backdoor* is an alternative method of accessing an application or operating system for troubleshooting. Hackers often create backdoors to exploit a system without being detected.
Stage	*Staging* a computer involves preparing it to perform additional tasks in the attack, such as installing software designed to attack other systems. This is an optional step.
Exploit	An *exploitation* takes advantage of known vulnerabilities in software and systems. Types of exploitation include: - Stealing information - Denying services - Crashing systems - Modifying/Altering information

General defense methodologies include the following items:

Item	Description
Layering	*Layering* involves implementing multiple security strategies to protect the same asset. *Defense in depth* or *security in depth* is the premise that no single layer is completely effective in securing the assets. The most secure system/network has many layers of security and eliminates single points of failure.
Principle of Least Privilege	The *principle of least privilege* states that users or groups are given only the access they need to do their job and nothing more. When assigning privileges, be aware that it is often easier to give a user more access when they need it than to take away privileges that have already been granted.
Variety	Defensive layers should have variety and be diverse; implementing multiple layers of the exact same defense does not provide adequate strength against attacks.
Randomness	*Randomness* in security is the constant change in personal habits and passwords to prevent anticipated events and exploitation.
Simplicity	Security measures should provide protection, but not be so complex that you do not understand and use them.