2.1.5 Attack and Defense Strategy Overview

Understanding the methodology behind common attacks can help you better defend your assets.

This lesson covers the following topics:

- Attack strategies
- Defense methodologies

Attack Strategies

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

Strategy	Description
Perform reconnaissance	*Reconnaissance* is the process of gathering information about an organization, including: - System hardware information - Network configuration - Individual user information
Use social engineering	*Social engineering* is the process of manipulating others into providing sensitive information. Social engineering tactics include: - Intimidation - Sympathy
Use technical approaches	A *technical* approach to obtaining information includes using software or utilities to find vulnerabilities in a system. Methods often used by hackers are: - Port scan - Ping sweep
Breach the system	A *breach* is the penetration of system defenses. It is often achieved by using information gathered by through reconnaissance.
Escalate privileges	*Escalating privileges* is a primary objective of an attacker. Once an attacker has breached the system, obtaining higher privileges allows the attacker to access more information and gain greater control within 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 computers	*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 vulnerabilities	An *exploitation* takes advantage of known vulnerabilities in software and systems. Once a vulnerability has been exploited, an attacker can often: - Steal information - Deny services

	- Crash systems - Modify/alter information

Defense methodologies

General defense methodologies include the following items:

Methodology	Description
Layering	*Layering* involves implementing multiple security strategies to protect the same asset. *Defense in depth* or *security in depth* is based on the premise that no single layer is completely effective in securing 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 jobs and nothing more. When assigning privileges, be aware that it is often easier to give a user more access when it is needed than to take away privileges that have already been granted.
Variety	Defensive layers should incorporate a variety of methods. Implementing multiple layers of the same defense does not provide adequate protection against attacks.
Randomness	*Randomness* in security is the constant change in personal habits and passwords to prevent predictable behavior.
Simplicity	Security measures should provide protection, but not be so complex that it is difficult to understand and use them.