1.3 Attack Trees

Attack Trees

Attack trees are a flowchart that show how an attacker might reach a goal, like a family tree of attacks. Key aspects include:

- Definition: A tree-like diagram that maps out different ways an attacker could achieve their goal.
- Structure:
  - Root: The top of the tree, showing the attacker's main goal
  - Branches: Different paths or methods branching down from the goal
  - Leaves: The bottom-most parts, showing specific actions an attacker might take
- Purpose:
  - Identify potential threats
  - Analyze possible attack paths
  - Prioritize security measures
- Benefits:
  - Provides a clear visual of possible attacks
  - Helps understand complex attack scenarios
  - Makes it easier to explain threats to non-technical people

Attack trees help security teams "see" potential threats, making it easier to plan comprehensive defenses.

Sample Attack Tree: Unauthorized Access to a Server

Here's a simplified attack tree for gaining unauthorized access to a server:

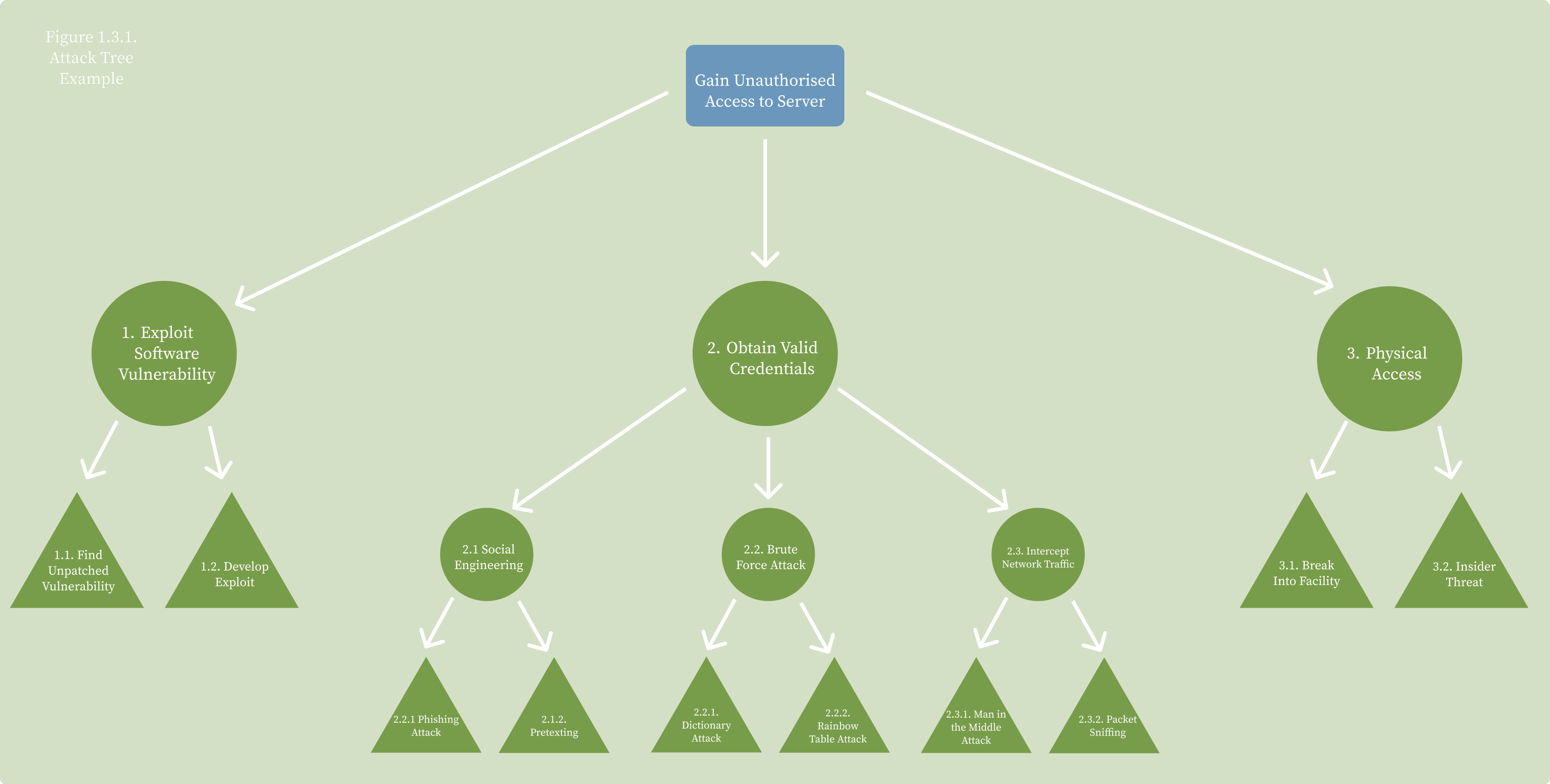
Figure 1.3.1. Attack Tree Example

Gain Unauthorised Access to Server
1. Exploit Software Vulnerability
2. Obtain Valid Credentials
3. Physical Access
1.1. Find Unpatched Vulnerability
1.2. Develop Exploit
2.1 Social Engineering
2.2. Brute Force Attack
2.3. Intercept Network Traffic
3.1. Break Into Facility
3.2. Insider Threat
2.2.1 Phishing Attack
2.1.2. Pretexting
2.2.1. Dictionary Attack
2.2.2. Rainbow Table Attack
2.3.1. Man in the Middle Attack
2.3.2. Packet Sniffing

This attack tree illustrates various paths an attacker might take to gain unauthorized access to a server. Each branch represents a different approach, with sub-branches detailing specific methods or steps within that approach.

This structure provides both a conceptual understanding of attack trees and a concrete example of how they are constructed and used in security analysis.