Attack tree has 2 elements:

* A root node is the goal of the overall attack
* A leaf node is a specific attack
* And / Or node represent different way to achieve the attack:
  + An and node means all sub-attacks must be achieved.
  + An or node means at least one attack must be achieved

Attack tree

1. Attack vector (paths which an attacker can exploit)
2. Attack surface

|  |  |
| --- | --- |
| Attack vector types | Attack surface examples |
| * Compromised Credentials * Weak Credentials * Insider Threats (Disgruntled employees or malicious insiders) * Missing or Poor Encryption * Misconfiguration * Ransomware * Phishing * Vulnerabilities * Brute Force * Distributed Denial of Service (DDoS) * SQL Injections * Trojans * Cross-Site Scripting (XSS) * Session Hijacking * Man-in-the-Middle Attacks * Third and Fourth-Party Vendors | * API endpoints * Web application * Network infrastructure * OS Settings * DNS server * Certificate server * Mobile client * 3rd party SW/Library * Data storage device * Application Framework * Kubernetes configuration * Docker configuration * Service configuration * Staff * Third-party software * Third-party vendors * Endpoints * Smartphones * Mobiles devices * Laptops * Desktops * Servers * Internet-of-Things (IoT) devices. |