# DISCLAIMER

Il materiale contenuto nel drive è stato raccolto e richiesto tramite autorizzazione ai ragazzi frequentanti il corso di studi di Informatica dell'Università degli Studi di Salerno. Gli appunti e gli esercizi nascono da un uso e consumo degli autori che li hanno creati e risistemati per tanto non ci assumiamo la responsabilità di eventuali mancanze o difetti all'interno del materiale pubblicato.

Il materiale sarà modificato aggiungendo il logo dell'associazione, in tal caso questo possa recare problemi ad alcuni autori di materiale pubblicato, tale persona può contattarci in privato ed elimineremo o modificheremo il materiale in base alle sue preferenze.

Ringraziamo eventuali segnalazioni di errori così da poter modificare e fornire il miglior materiale possibile a supporto degli studenti.

CoScienze
Associazione

Alfonso Cannavale

## ALBERO DI ATTACCO

Le tipologie di vulnerabilità rispondono, di norma, alle seguenti domande:

- Sotto quali ipotesi si verificano?
- Quali conseguenze hanno?
- Come si possono mitigare?

Il *modo non corretto di agire* prevede di provare comandi a casaccio o copiare soluzioni messe a punto da altri, senza avere idea di cosa si stia facendo o utilizzare strumenti automatici di attacco, senza avere idea del loro funzionamento.
Il *modo corretto di agire*, invece, prevede la piena consapevolezza delle proprie azioni:

- conoscere tutti i dettagli dell'ambiente che si sta studiando;
- identificare tutti i modi possibili (plausibili ed improbabili) di condurre un attacco;
- provare l'attacco sui sistemi su cui si ha il permesso di operare;
- capire nel dettaglio modalità e conseguenze dell'attacco;
- capire come mitigare l'attacco.

L'**albero di attacco** è uno strumento utile per la conduzione ragionata di attività di attacco e rappresenta una **vista gerarchica** dei possibili attacchi ad un sistema, dove:

- ogni nodo dell'albero è un'azione;
- il nodo radice è l'azione finale dell'attacco;
- ciascun nodo foglia è un'azione iniziale dell'attacco;
- ciascun nodo intermedio rappresenta un'azione preliminare per poter svolgere l'azione rappresentata dal nodo padre.

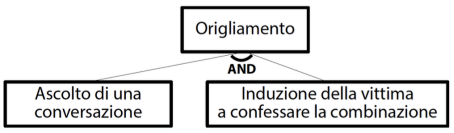
*Esempio:*

Supponiamo di voler aprire una cassaforte:

- Il ***nodo radice*** dell'albero rappresenta proprio l'obiettivo dell'attacco;
- La cassaforte può essere aperta se almeno una delle azioni rappresentate nei ***nodi foglia*** ha successo;
- Le ***azioni intermedie*** hanno bisogno, a loro volta, del successo di almeno un'altra azione preliminare. Alcune azioni necessitano l'esecuzione di più azioni preliminari, si modellano con un AND e un arco;
- Un ***possibile attacco*** è un OR di percorsi (incrocianti su un nodo AND) da nodi foglia al nodo radice.


Alcune azioni necessitano l'esecuzione di più azioni preliminari

- Si modellano con un AND e un arco




Una volta definito, l'albero d'attacco può essere arricchito con opportune **etichette** sui nodi, come: (i) fattibilità dell'azione (Possibile, Impossibile), (ii) costo dell'azione e (iii) probabilità di successo.

- Aggregando le etichette nel percorso da una foglia alla radice → è possibile ***stimare l'attacco***.