ROMA TRE
UNIVERSITÀ DEGLI STUDI

INGEGNERIA
CIVILE, INFORMATICA E DELLE TECNOLOGIE AERONAUTICHE

ADTViewer: un'interfaccia utente per l'analisi delle intrusioni informatiche

Relatore
Prof. Stefano Iannucci

Correlatore
Dott. Tommaso Caiazzi

Francesco Spezzano 534050

Anno Accademico 2023/2024

Introduzione

- Crescente rilevanza della cybersecurity nel contesto della digitalizzazione globale
- Espansione delle superfici di attacco a causa della crescente complessità dei sistemi informatici
- Necessità di sistemi avanzati per l'analisi e risposta tempestiva agli attacchi informatici

Introduzione

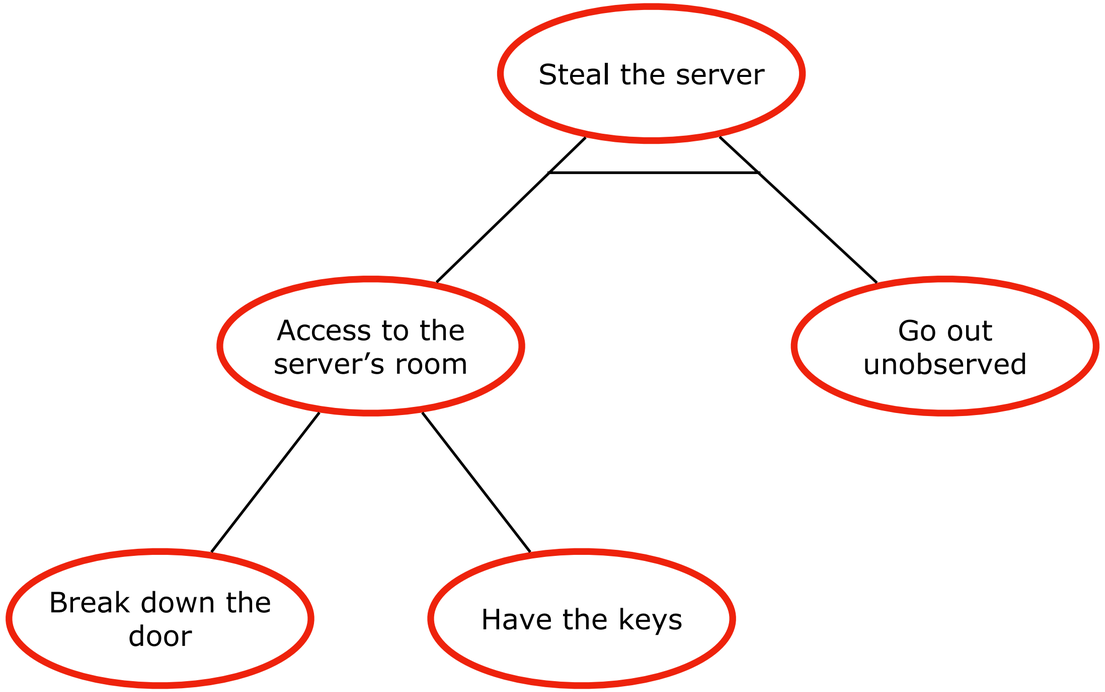
- Intrusion response: rilevare, mitigare e prevenire gli attacchi
  - Attack Trees e Attack Defense Trees
- Limitazioni degli strumenti esistenti (ADTool, PRISM-Games): staticità e complessità
- Necessità di una GUI per analizzare dinamicamente gli attacchi e le difese

Obiettivi della tesi

- Realizzazione di una GUI intuitiva per analisi dinamica degli Attack Defense Tree (ADT)
- Integrazione diretta con:
  - Framework PANACEA (analisi tramite PRISM-Games)
  - Soluzioni SIEM (es. Wazuh/OpenSearch)
- Sviluppo di un'architettura modulare e user-friendly per supportare esperti nella gestione interattiva delle minacce informatiche

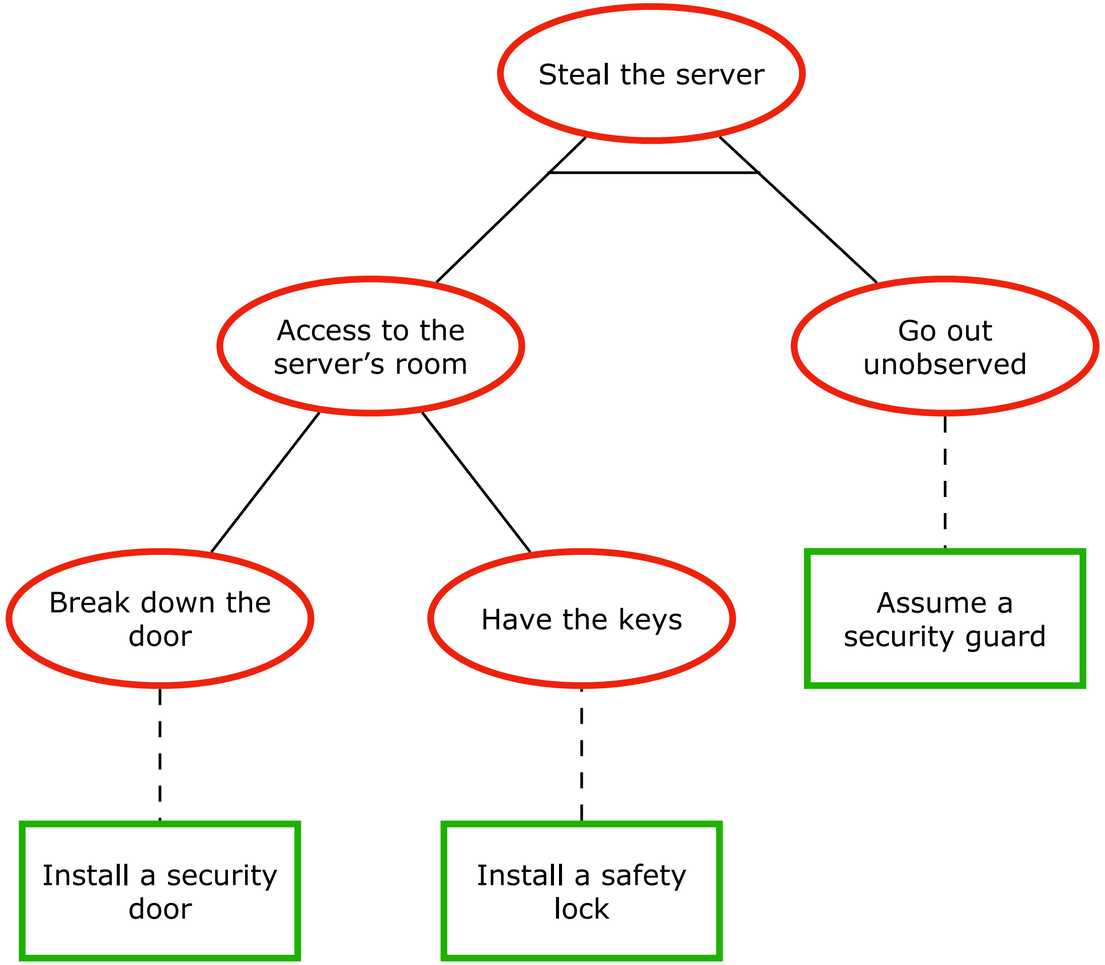
Attack Trees e Attack Defense Trees

- **Attack Trees** (AT)
  - Rappresentazione gerarchica delle strategie di attacco
  - Identificazione di percorsi e vulnerabilità
- Struttura degli Attack Trees:
  - **Nodo Radice**: obiettivo dell'attaccante
  - **Nodi Intermedi**: condizioni intermedie
  - **Nodi Foglia**: azioni elementari



Attack Trees e Attack Defense Trees

- **Attack Defense Trees** (ADT)
  - Estensione degli AT con contromisure difensive
  - Rappresentazione dinamiche di attacco-difesa per analisi di strategie ottimali



ADTViewer: panoramica e caratteristiche

- ADTViewer è un plugin per OpenSearch Dashboards sviluppato per:
  - **Visualizzare** dinamicamente ADT
  - **Analizzare** strategie ottimali calcolate da PANACEA
  - **Integrarsi** facilmente con sistemi SIEM come Wazuh/OpenSearch
  - Architettura user-friendly e modulare

Tecnologie e architettura del sistema

- Frontend
  - **React** (Interattività e modularità)
  - **D3** (Visualizzazione interattiva degli ADT)
- Backend e Data Layer
  - **OpenSearch** (Integrazione SIEM e log management)
  - **PostgreSQL** (Gestione strutturata di alberi e policy)
- Containerizzazione
  - **Docker** (Deployment e orchestrazione servizi)

Workflow: caricamento e visualizzazione ADT

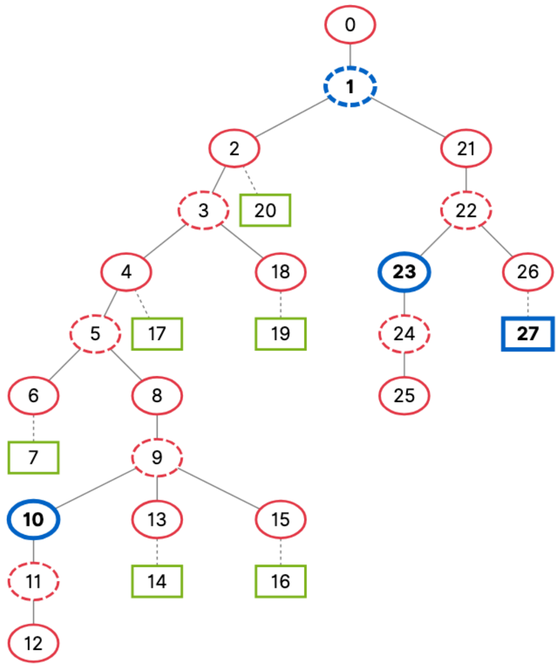
- **Caricamento** semplice e immediato di ADT da file XML
- **Visualizzazione** interattiva e dinamica degli ADT
- Calcolo automatico delle **policy ottimali** tramite PANACEA (PRISM-Games)

Workflow: caricamento e visualizzazione ADT

ADT Manager | adt_nuovo_250217_1004.json | adt_nuovo_250217_1004.json

Attack Tree

State: **0**



Tree Manager

Node Info | States Visualizer | Actions Manager

Show all nodes

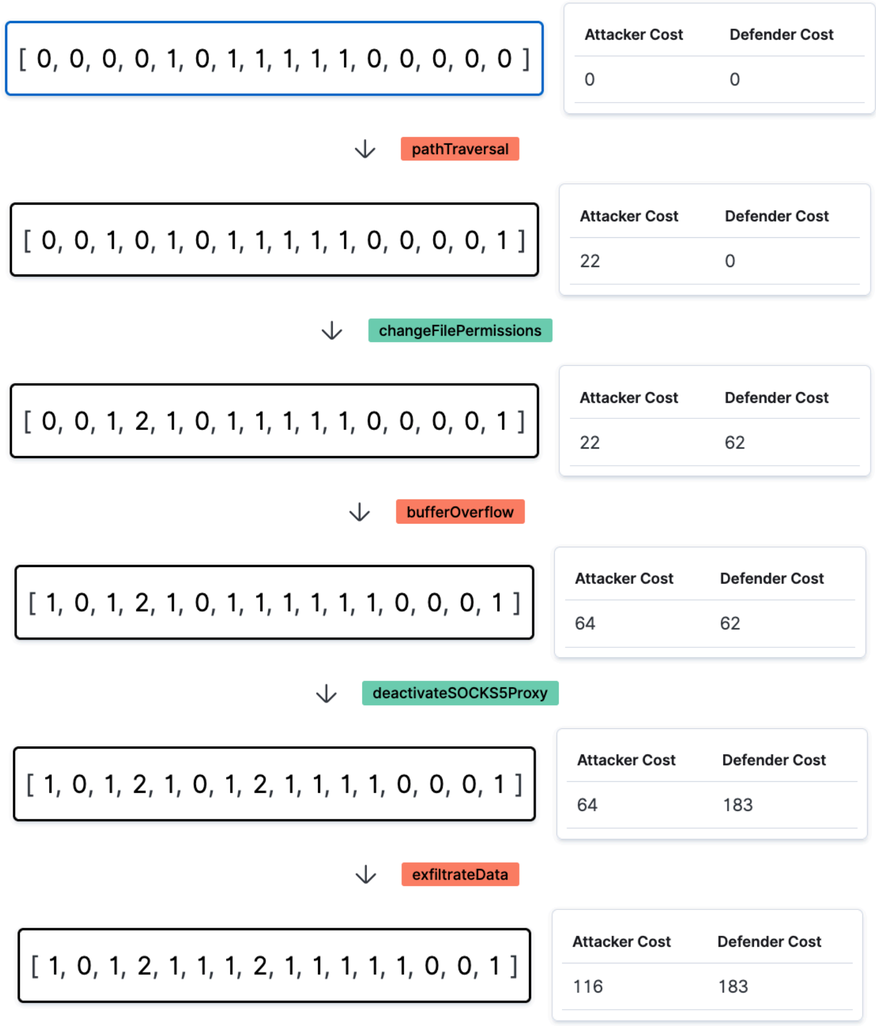
ID	Name	Type	Action	Role
1	Exfiltrate Data	Action	exfiltrateData	Attacker
10	Web Recon Succesful	Attribute	N/A	N/A
23	Web Recon Succesful	Attribute	N/A	N/A
27	Deactivate S O C K S5 Proxy	Action	deactivateSOCKS5Proxy	Defender

Rows per page: 5

1

Workflow: gestione e ricalcolo policy

- Visualizzazione dettagliata e navigabile delle policy generate da PANACEA
- Possibilità di escludere azioni di attacco e ricalcolare automaticamente nuove policy
- Aggiornamento interattivo e visivo degli alberi e delle policy dopo modifiche



Workflow: gestione e ricalcolo policy

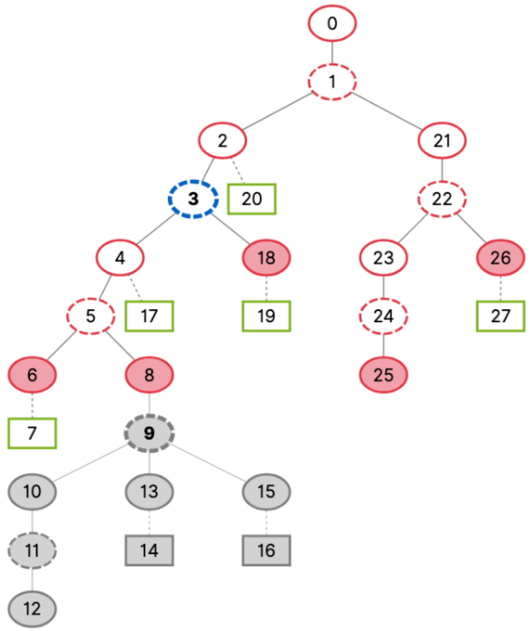
ADT Manager

adt_nuovo_policy_250219_2019.json

adt_nuovo_250219_2019.json

Attack Tree

State: **0**



Tree Manager

Node Info | States Visualizer | Actions Manager

Show all available actions

Role	Action	Monetary Cost	Time	Flag
Attacker	webRecon	5	1	
Attacker	**getLoginData**	10	2	
Attacker	**pathTraversal**	20	2	
Defender	UpdateApache	20	20	

Rows per page: 4

1 2 3 4

Export configuration

exclude_pathTraversal

Workflow: Analisi costi e confronto policy

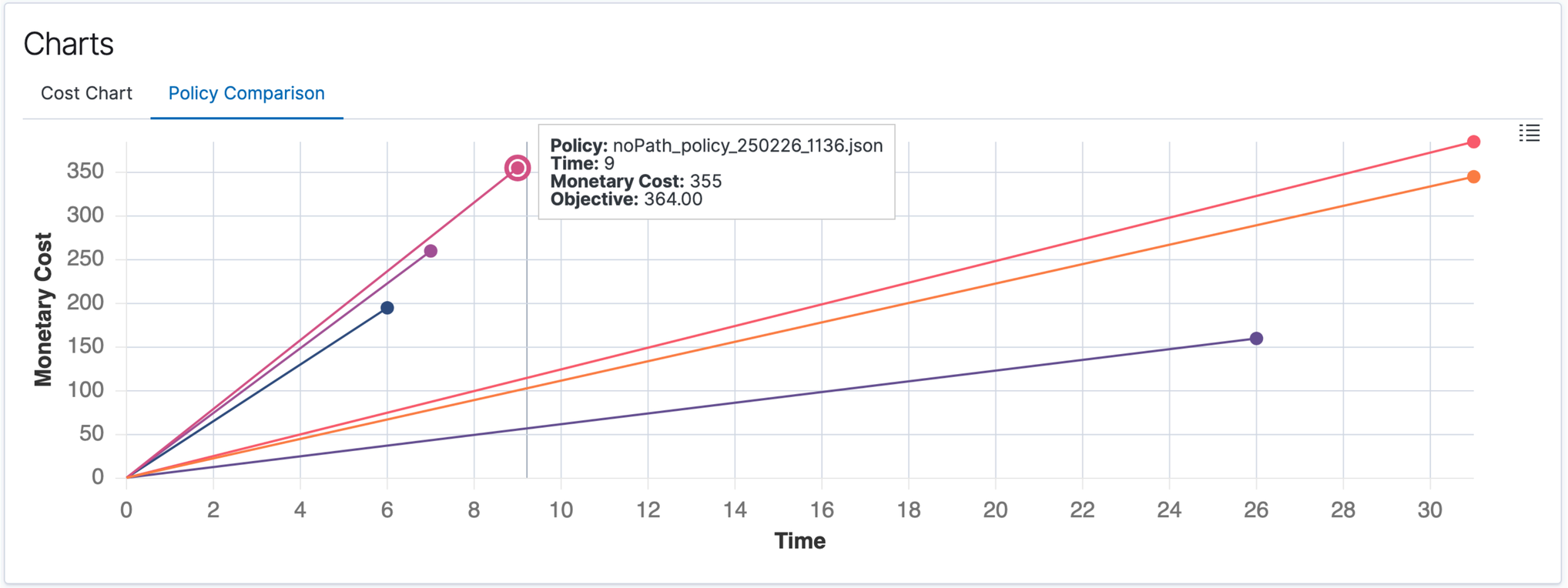
- **Grafici cumulativi** costi (Attaccante vs Difensore) per ogni policy
- **Confronto** diretto di più policy per analisi strategica delle contromisure

Workflow: Analisi costi e confronto policy

- **Grafici cumulativi** costi (Attaccante vs Difensore) per ogni policy
- **Confronto** diretto di più policy per analisi strategica delle contromisure

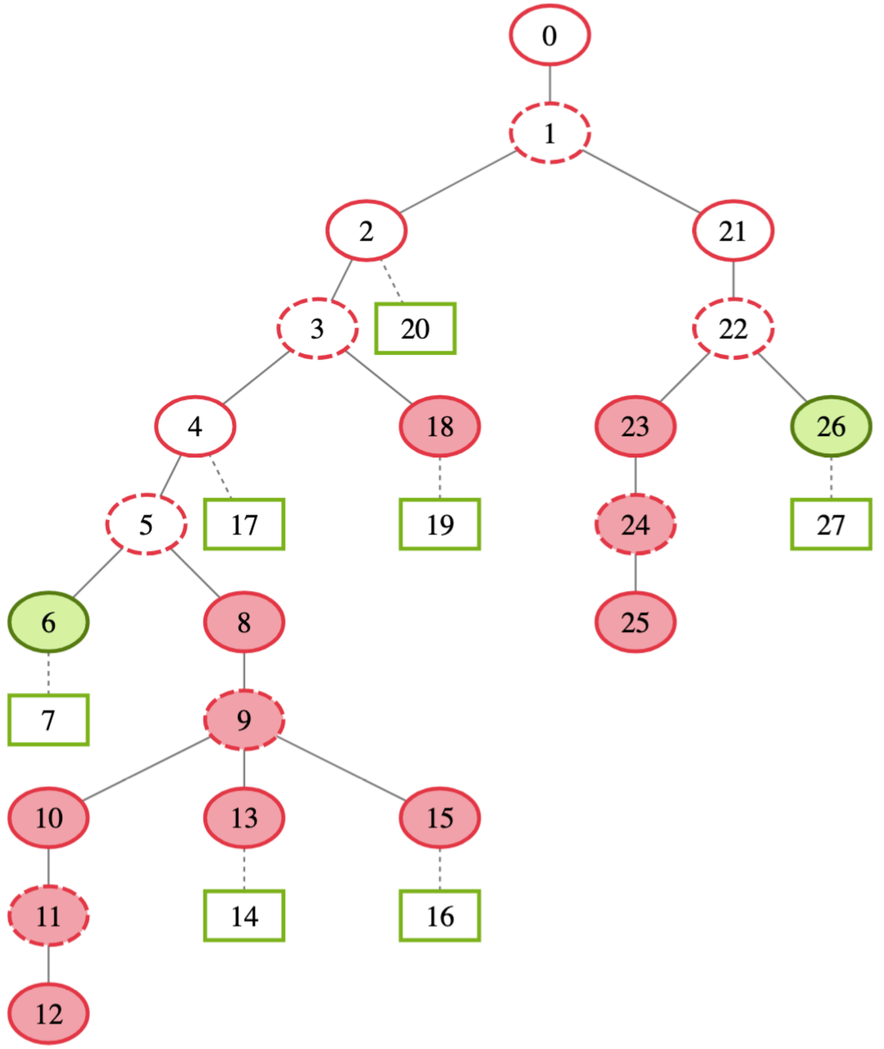
Workflow: Analisi costi e confronto policy

- **Grafici cumulativi** costi (Attaccante vs Difensore) per ogni policy
- Confronto diretto di più policy per analisi strategica delle contromisure



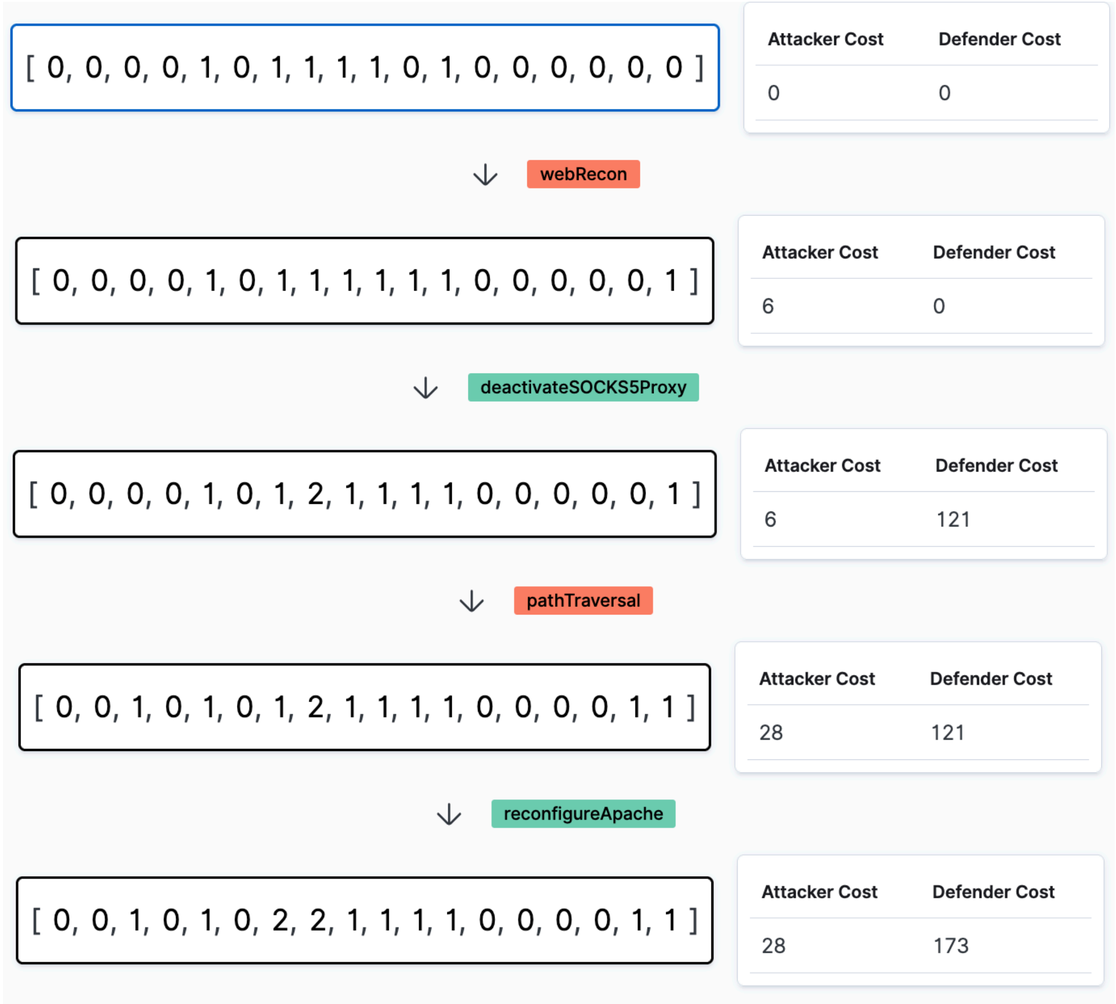
Case study 1: scenario non mitigato

- Descrizione scenario: percorso di attacco senza restrizioni



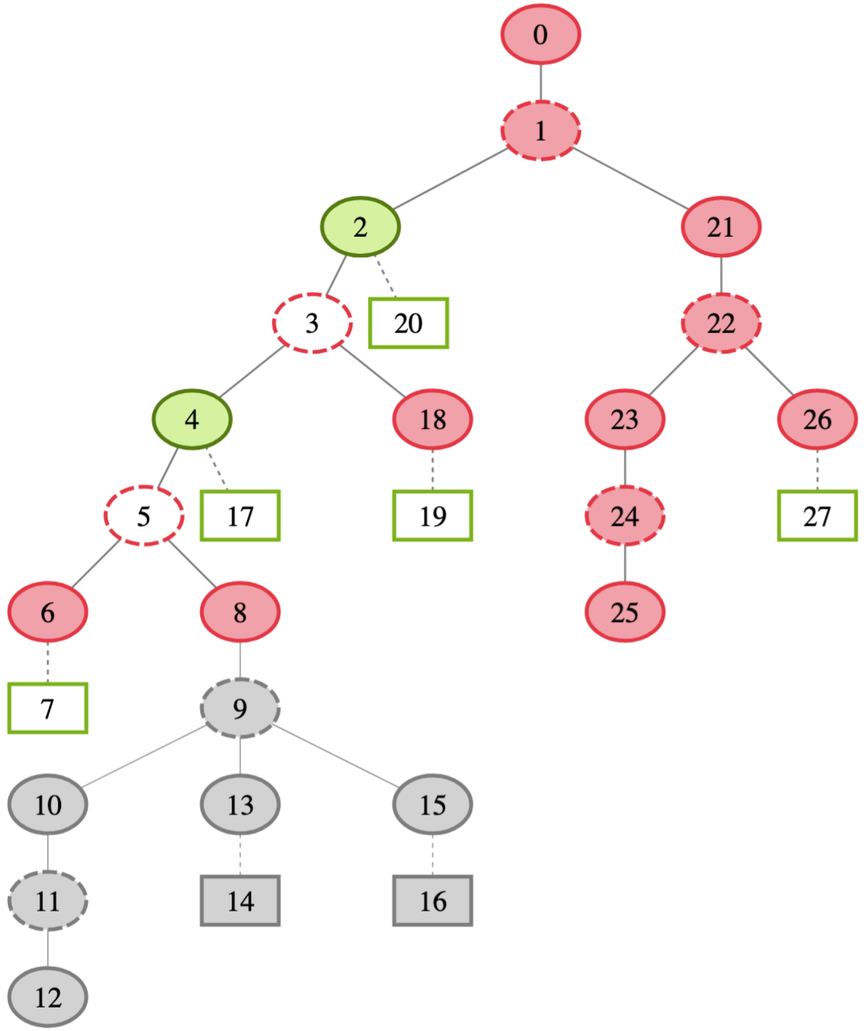
Case study 1: scenario non mitigato

- Descrizione scenario: percorso di attacco senza restrizioni
- Sequenza ottimale generata da PANACEA

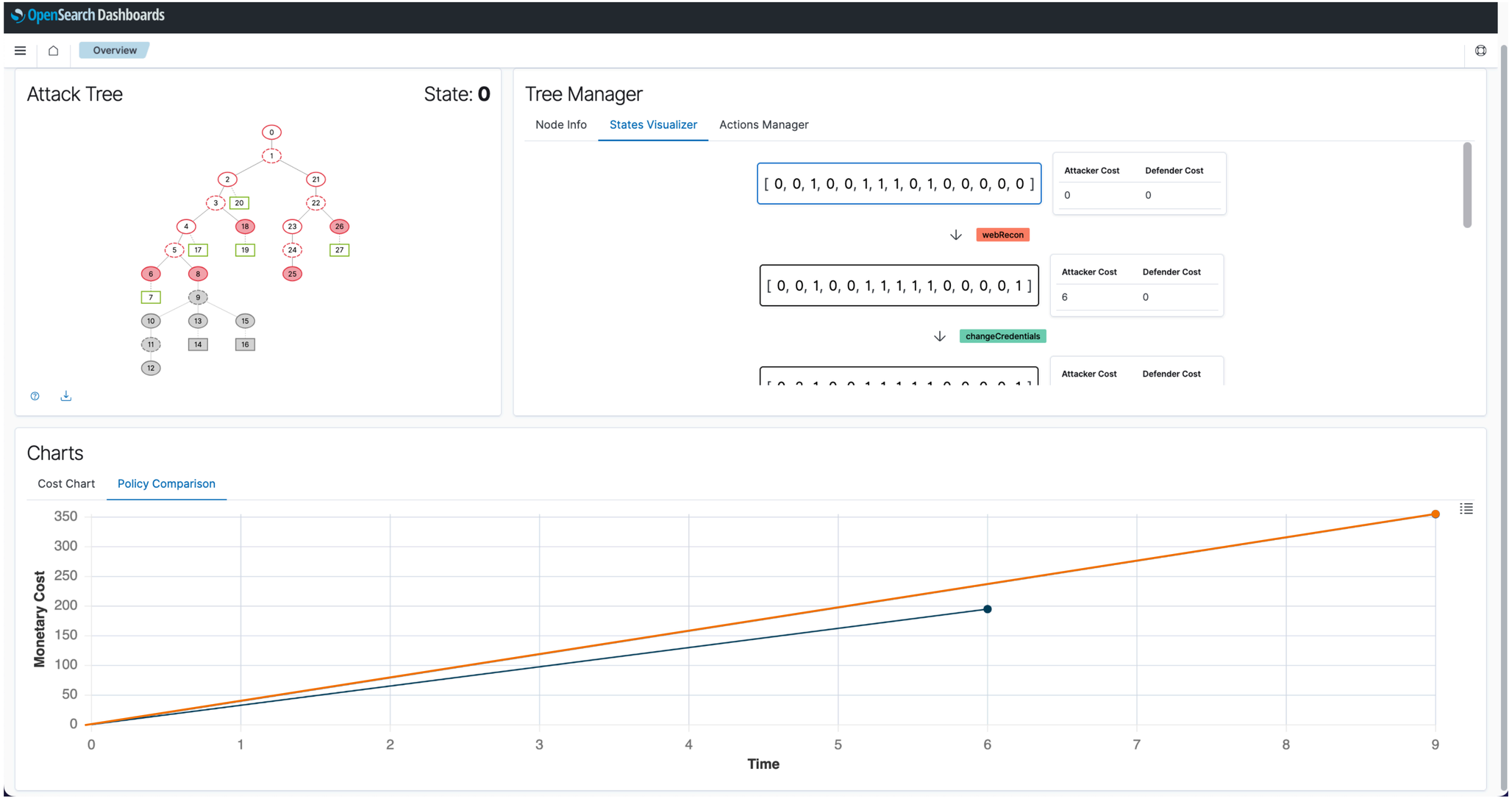


Case study 2: scenario mitigato

- Azione mitigante: esclusione “*pathTraversal*"
- Esclusione del sottoalbero radicato all’azione mitigante
- Nuova sequenza ottimale e analisi costi aggiornati



Confronto tra i due scenari



Conclusioni

- Risultati raggiunti:
  - Sviluppo di una GUI efficace per analisi interattiva
  - Miglioramento significativo nella comprensione e gestione dinamica delle minacce informatiche
- Suggerimenti per sviluppi futuri:
  - Integrazione Machine Learning
  - Ottimizzazione prestazioni (alberi molto grandi, PANACEA)

ROMA TRE
UNIVERSITÀ DEGLI STUDI

INGEGNERIA
CIVILE, INFORMATICA E DELLE TECNOLOGIE AERONAUTICHE

Grazie per l’attenzione!