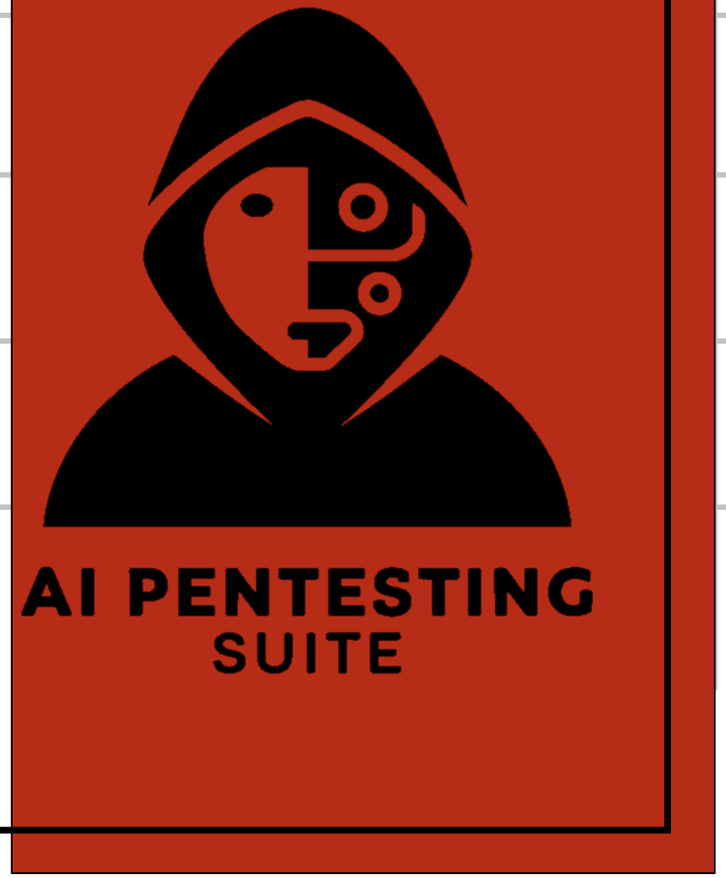
Alessandro Luppino



AI-Based Penetration Testing Suite

Un assistente per il lavoro di penetration testing, in grado di riconoscere vulnerabilità e fornire supporto.

SLIDES

TABLE OF CONTENTS

INTRODUZIONE

Il progetto si propone di sviluppare un sistema automatizzato per la rilevazione di vulnerabilità in infrastrutture IT, utilizzando un modello di intelligenza artificiale. In questa prima fase, il focus sarà sullo sviluppo di un modulo AI capace di analizzare i risultati prodotti da strumenti di scansione come Nmap, OpenVAS, e Nessus, per identificare e classificare automaticamente le vulnerabilità presenti.
Questo modulo rappresenta il cuore del sistema, e sarà la base per sviluppi futuri, come la generazione automatica di report e suggerimenti per vettori di attacco.

NOTA: i modelli, i dataset e i framework che verranno nominati in seguito sono provvisori e potrebbero subire dei cambiamenti nel corso del progetto come verrà approfondito nell’analisi dei rischi.

OBIETTIVI

ATTUALI

Creazione del Modulo di Rilevazione delle Vulnerabilità:

- Ricerca e preprocessing di dataset con CVE e vulnerabilità.
- Fine tuning di un modello precedentemente addestrato.
- Integrazione del modello con strumenti di scansione esistenti.
- Presentazione delle vulnerabilità all'utente con una breve descrizione e la loro gravità

Creare una base per moduli futuri

FUTURI

Modulo di Generazione Automatica di Report:

- Analizzare i risultati delle scansioni e generare report leggibili e dettagliati.

Modulo di Attacco:

- Suggerire exploit e tecniche di attacco specifiche per le vulnerabilità rilevate.

REQUISITI

FUNZIONALI

Input: Output da strumenti di scansione (file XML, JSON o testo da Nmap, Nessus, OpenVAS).

Elaborazione:
Parsing dell'output degli strumenti di scansione.
Classificazione delle vulnerabilità attraverso il modello AI addestrato.

Output:
Lista di vulnerabilità classificate con gravità e dettagli tecnici.

NON FUNZIONALI

Prestazioni: Il sistema deve processare i dati di una scansione standard in tempi ragionevoli.

Scalabilità: Deve essere facilmente estendibile per includere nuovi tipi di vulnerabilità e strumenti di scansione.

Usabilità: Output chiaro e facilmente leggibile, in particolare per pentester o analisti.

Affidabilità: Deve fornire risultati accurati in termini di gravità delle vulnerabilità rilevate.

TECNICI

Modello AI: RoBERTa.

Linguaggi e Framework: Python, Hugging Face, PyTorch.

Integrazioni: Nmap, Nessus, OpenVAS.

Dataset: CVE, Exploit-DB.

ANALISI DEI RISCHI

RISCHIO	PROBABILITA’	IMPATTO	MITIGAZIONE
Dataset non formattato correttamente	Bassa	Alto	Effettuare un pre processamento accurato e testandolo con dataset più piccoli.
Problemi durante il fine tuning del modello AI	Alta	Medio	Testare con piccoli dataset prima di addestrare sul dataset completo.
Costi elevati di calcolo per l'addestramento	Media	Basso	Effettuare test iniziali con output da Nmap e OpenVAS per validare l'integrazione.
Difficoltà di integrazione con strumenti di scansione	Bassa	Basso	Utilizzare versioni ridotte del modello AI come DistilBERT.
Tempi di sviluppo eccessivi	Media	Alto	Seguire strettamente la pianificazione del diagramma di Gantt.

COCOMO

EARLY DESIGN

Size Stimata = 3.5 KLOC

B = 1.1

M = PERS * RPCX * RUSE * PDIF * PREX * FCIL * SCED

A = 2.94

Valori Scelti:

PERS = 0.86 (high)

RPCX = 1.00 (nominal)

RUSE = 0.94 (low)

PDIF = 1.00 (nominal)

PREX = 1.00 (nominal)

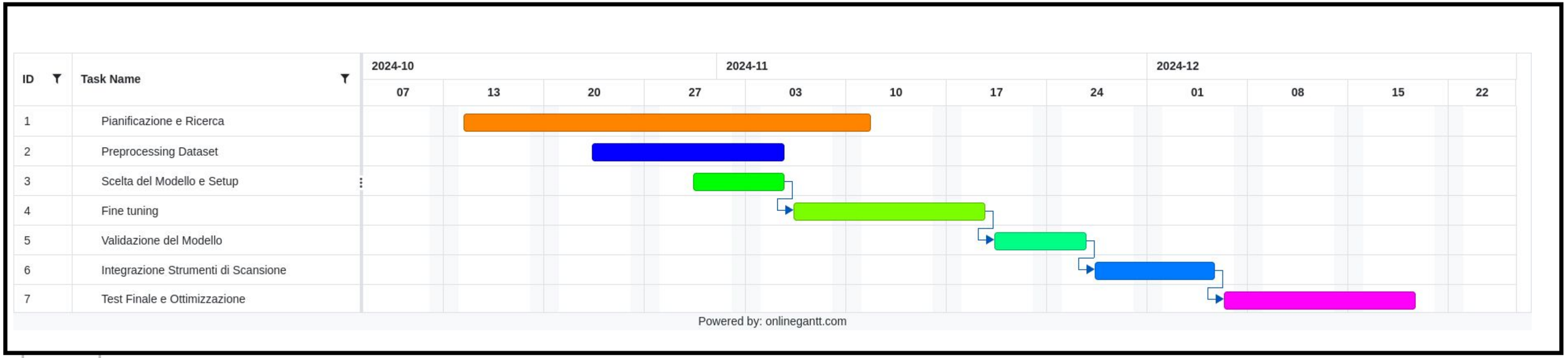
FCIL = 0.91 (high)

SCED = 1.00 (nominal)

$PM = A * Size^{B} * M = 7,25657025$

NOTA: La stima iniziale potrebbe non riflettere accuratamente le condizioni effettive del progetto. Ad esempio, alcuni fattori come la complessità del prodotto o le tempistiche richieste potrebbero essere stati sovrastimati. È possibile che alcune delle variabili considerate nel modello non rispecchino pienamente la natura specifica del progetto che sto affrontando. Inoltre, l'uso di strumenti o tecniche che semplificano il processo potrebbe non essere stato adeguatamente considerato nella stima. Per questo motivo, anche se la stima suggerisce un tempo maggiore, ritengo sia possibile completarlo comunque entro la scadenza.

GANTT


ID
Task Name
2024-10
2024-11
2024-12
07
13
20
27
03
10
17
24
01
08
15
22
1 Pianificazione e Ricerca
2 Preprocessing Dataset
3 Scelta del Modello e Setup
4 Fine tuning
5 Validazione del Modello
6 Integrazione Strumenti di Scansione
7 Test Finale e Ottimizzazione
Powered by: onlinegantt.com

FINE

Grazie per l’attenzione!