IBM Innovation Center for Education

PHEMESOFT Software That Matters

TRUSTED DELIVERY PARTNER for IBM ICE

THE YENEPOYA INSTITUTE OF ARTS SCIENCE COMMERCE AND MANAGEMENT
(a constituent unit of Yenepoya Deemed to be University)

Password Cracking Resistance Analyzer
PROJECT SYNOPSIS

MASTER OF COMPUTER SCIENCE AND APPLICATIONS

SUBMITTED BY :

Ahamed Salim PS	24MCA202
Nandana PS	24MCA216
Suparna P	24MCA221

GUIDED BY:
MR. SHASHANK

IBM Innovation Center for Education

TITLE PAGE

1. Name of the student: Ahamed salim ps

2. Class Roll No. 24MCA202

3. Campus ID: 35466

4. Present official Address: YIASCM Blamatta, Mangalore
575002

5. Email: 35466@yenepoya.edu.in

6. Phone No. +91 7736907547

7. Branch: Computer Science

8. Batch: 2024-2026

9. Proposed Topic: Password Cracking Resistance Analyzer

IBM Innovation Center for Education

PHEMESOF Software Th

TRUSTED DELIVERY PARTNER f

TABLE OF CONTENTS

1.1 Introduction

The **Automated Intrusion Detection System (IDS)** is designed to monitor and analyze network traffic for potential security threats. Using packet sniffing techniques and firewall integration, the system detects suspicious activities such as DDoS attacks, port scans, unauthorized access attempts**,** and malware propagation in real-time.

By leveraging advanced detection mechanisms, including signature-based and behavioural anomaly detection**,** the IDS ensures strong network security and mitigates threats before they cause damage.

1.2 Key Features

Real-time Traffic Monitoring – Continuously analyzes incoming network packets. **Intrusion Detection & Alerts** – Detects high-volume requests, port scans, and unauthorized access attempts.

Firewall Integration – Automatically blocks malicious IPs using Windows Firewall (netsh) or Linux (iptables**) .**

Custom Detection Rules – Implements specific rules for DDoS, brute-force attacks, and suspicious activity**.**

Logging & Reporting – Stores detected threats in structured logs for further analysis.

Machine Learning Integration – Enhances detection accuracy by learning attack patterns over time.

User-Friendly GUI – Designed with Tkinter for managing intrusion events interactively.

1.3 Technology Stack

Frontend:

Tkinter: Allows users to view threats, manage logs, and configure detection settings.

Backend:

Scapy – Handles packet sniffing and network analysis.

Windows Firewall (`netsh`) / Linux (`iptables`) – Automates intruder blocking.

Nmap – Assists in network scanning and threat identification**.**

SQLMap – Detects and mitigates SQL injection vulnerabilities**.**

CVE Integration – Fetches real-time vulnerability data to strengthen security measures.

1.4 Specialized Field: Cybersecurity and Ethical Hacking

This project falls under the domain of cybersecurity and ethical hacking, ensuring networks remain secure from external attacks, internal threats, and automated exploits. The IDS helps organizations mitigate security risks proactively, preventing unauthorized access and data breaches.

2.1 Methodology

The development of the Password Cracking Resistance Analyzer follows a structured methodology to simulate realistic password cracking scenarios and ensure accurate evaluation of password strength and resistance.

2.2 Requirement Analysis & Tool Selection

Define functionalities including password strength testing, entropy calculation, and simulated attacks.

Research and integrate cracking tools like Hashcat and John the Ripper with Python APIs.

Ensure the system supports various operating environments (Windows/Linux) for testing purposes.

2.3 System Architecture and Design

Design a modular framework combining rule-based and attack-based analysis of passwords.

Define interaction between GUI and backend password cracking simulation tools.

2.4 Frontend Development (Tkinter)

Develop an intuitive GUI for inputting and testing passwords.

Allow users to set custom password policies and view resistance scores.

2.5 Backend Integration

Implement password testing modules with predefined cracking dictionaries and brute-force settings.

Integrate password scoring mechanisms based on NIST guidelines

Provide improvement suggestions based on real-world cracking patterns and ML-based predictions.

2.6 Final Testing and Documentation

Validate cracking simulations across different password complexities and lengths

Ensure efficient computation and avoid excessive CPU usage during brute-force simulations

Generate comprehensive password resistance analysis reports for user guidance.

3.1 Facilities required for proposed work

The development of the Password Cracking Resistance Analyzer requires the following tools and environments.

3.2 Development Environment

Python 3.12: The primary programming language for building the front-end (Tkinter) and integrating the backend tools.

Tkinter: Built-in Python library for developing the graphical user interface (GUI).

IDE VSCode: To write, test, and debug Python code efficiently.

3.3 Detection & Mitigation Tools

John the Ripper: A popular open-source password cracking tool used to simulate real-world attack scenarios and evaluate password strength.

Hashcat: A powerful GPU-based password recovery tool that simulates brute-force and dictionary attacks efficiently.

CrackLib: A library used to prevent users from choosing passwords that are easily guessed or found in dictionaries.

Zxcvbn: A password strength estimator that provides feedback and strength scores based on common user behaviors and patterns.

3.4 Testing and Deployment

VirtualBox: for setting up virtual machines that simulate target environments for penetration testing.

Operating Systems:

Kali Linux: Used to test password cracking resistance using tools like John the Ripper and Hashcat.

Windows: For testing the compatibility of the tool across platforms and development of front-end.

3.5 Reporting Tools

PDF and HTML Libraries: Libraries like ReportLab and WeasyPrint are used to export detailed password analysis and resistance reports.