Internship Project Report

Name: Chanakya Marode

Internship Title: Cybersecurity Intern – Elevate Labs

Abstract

TraceForge is a PowerShell-based cybersecurity tool built to automate different security analysis tasks. It includes modules for system log collection, log analysis, firewall auditing, steganography detection, and secure file storage. The framework is made to help users and security analysts easily identify suspicious system activities, hidden files, or weak configurations. Each module is designed to run independently or together, giving clear and simple results without needing deep technical knowledge.

Introduction

In today's world, where security threats are increasing every day, checking system logs and auditing manually can be difficult and time-consuming. TraceForge was built to make this process easier and faster.

It works as an all-in-one automation tool that can collect logs from the system, analyze them, check firewall configurations, detect hidden data in files, and also allow users to securely store or encrypt their files and folders.

The goal was to create something that looks clean, works fast, and can help both beginners and professionals understand what's happening inside a system without much effort.

Tools and Technologies Used

- **Programming Language:** PowerShell
- **Platform:** Windows OS
- **Libraries/Utilities:** JSON handling, AI-based log analysis support
- **Version Control:** GitHub repository for project management and collaboration
- **Modules:** LogCollector, LogAnalyzer, FirewallAuditor, StegaTool, SecureFileStorage

Steps Involved in Implementation

1. Planned and designed a clean modular folder structure for easy management.
2. Developed main modules:

- **LogCollector** for gathering system logs.
- **LogAnalyzer** for analyzing collected data.
- **FirewallAuditor** for checking firewall settings and risks.
- **StegaTool** for finding hidden data in images or files.
- **SecureFileStorage** for encrypting and decrypting files or folders.

3. Created a main launcher `TraceForge.ps1` for user-friendly navigation between modules.
4. Implemented automatic output generation with organized timestamps.
5. Added configuration support for trusted setups.
6. Fully tested the tool on different Windows environments to ensure stability.

Results

The final TraceForge tool successfully automates system scanning and security checks. It collects logs, analyzes suspicious patterns, checks firewall configurations, finds hidden data through steganography analysis, and secures files with encryption.

All the results are saved in structured folders, making it easy for users to view and store reports. The tool provides accurate and easy-to-understand outputs without needing advanced technical knowledge.

Conclusion

TraceForge is a complete and practical tool that brings automation into core cybersecurity tasks. It helps users save time while improving visibility and control over system data. Its modular structure makes it easy to maintain and expand in the future. With everything running automatically, TraceForge shows how simple scripts can perform advanced security operations efficiently.

Future Scope

In future versions, TraceForge can include:

- **Phishing Simulation Module** for user awareness training.
- **Smarter AI-based log analysis** for deeper anomaly detection and prediction.
- **Improved visualization** for scan results using graphical reports.