Text

Description automatically generated with medium confidence

Temasek Polytechnic School of Informatics and IT

Diploma in

Cyber Security and Digital Forensics

AY 22/23 Semester

Major Project Documentation

Project Title:

Automated Auditing Tool for Linux 1

Submitted To:

Mr Simon

Submitted By:

Nur Hidayah, 2004679C

Lee Leng Han, 2002073A

Saihu Dawood, 2002866H

Shania Tay, 2002100B

Supervisor:

Mr Simon

Table of Contents

[Project overview 2](#_Toc1298144525)

[Background of our project: 3](#_Toc1625550102)

[Problem statement: 3](#_Toc1240711765)

[Our Project Vision: 3](#_Toc850700102)

[Our Tool Functionalities: 3](#_Toc234005605)

[User Guide: 3](#_Toc826583271)

[How to start? 4](#_Toc580277902)

[CentOS 8 Virtual Machine 4](#_Toc156114545)

[Ubuntu 20.04 Virtual Machine 4](#_Toc1628676072)

[Debian 10 Virtual Machine 4](#_Toc473648945)

[Recommended Usage: 4](#_Toc1142901913)

[Downloads and modules needed for the audit tool: 4](#_Toc984458364)

[APPENDIX A (Nur Hidayah) 4](#_Toc1736903931)

[APPENDIX B (Leng Han) 5](#_Toc1629773928)

[APPENDIX C (Saihu Dawood) 6](#_Toc1129195714)

[APPENDIX D (Shania Tay) 7](#_Toc1995039641)

# Project overview

## Background of our project:

Our team was given the responsibility of developing a Linux Automated Audit application that would have the fundamental capabilities of scanning the complete operating system and reporting the results and necessary corrections.

## Problem statement:

Manual auditing to date is a bothersome task for auditors and possesses a significant number of disadvantages which includes:

* Manual Auditing is a time-consuming and tedious task
* Manual auditing can bring about accuracy problems such as human errors
* Manual audits in comparison with automated audits are inconsistent

Problems auditors face:

* Audit data would need to be manually collected, updated, and maintained.
* Audit commands to be manually typed out, checked, and verified

It is an extremely inefficient process where large amounts of time and energy would be wasted to carry out these manual audits.

## Our Project Vision:

We have thus decided to make and create a reliable automated Linux audit tool that is in line and compliant with current industrial standards, with security checks built in accordance with CIS benchmarks and standards. The tool can run extensive scans through the systems to support system hardening and to reduce security risk.

## Our Tool Functionalities:

1. Fully automated audits for Linux in accordance with the latest version of the CIS Benchmark
2. Remediation measures of failed benchmark components to aid in security hardening
3. Pie Chart/ Excel/ MySQL summary for audit results
4. Search Function for audit results
5. Filter Function for audit results
6. Language Translation for audit results
7. Compatible with 3 different Linux Distributions. (Ubuntu, Debian and CentOS)

# User Guide:

## How to start?

### CentOS 8 Virtual Machine

* Import and download all files and scripts from Github created ( <https://github.com/shersho/majorprj5> )
* Run command **‘python3 start.py’** to start the automated audit tool

### Ubuntu 20.04 Virtual Machine

### Debian 10 Virtual Machine

## Recommended Usage:

* Run the audit button before any other functionalities for the most accurate and up to date audit results.
* Ensure audit functionality chosen are ran to completion before starting another functionality

## Downloads and modules needed for the audit tool:

|  |  |
| --- | --- |
| **Modules needed** | **Commands for installation** |
| Python Version 3.6 | yum install python36 |
| Python3 Tkinter | yum install python3-tkinter |
| Python3 Pip | yum install python3-pip  Python3 -m pip install –upgrade pip |
| Python Tkinter Module matplotlib | Pip install matplotlib |
| Python Tkinter Module googletrans | Pip install googletrans==3.1.0a0 |
| Python Tkinter Module textblob | Pip install textblob |
| Mysql server | sudo apt install mysql-server |
| LibreOffice | Install latest version on the Internet |

# APPENDIX A (Nur Hidayah)

# APPENDIX B (Leng Han)

# APPENDIX C (Saihu Dawood)

# APPENDIX D (Shania Tay)