NATIONAL UNIVERSITY OF MODERN LANGUAGES
Faculty of Engineering and Computing
Department of Software Engineering

BSSE35-1-A-Mor

Semester Project
(Application of Info. & Comm. Techn.)

Project Title:

Cybersecurity and its Implementation.

Course Instructor:

Mr. Ahsan Arif (lecturer)

Group Members:

Jahanzaib

SP23870

Waleed Ahmed

SP23873

Fiza Tahir

SP23865

Sibgha Zameer

SP23863

Session:

Spring-2024

Importance of Cybersecurity and its Implementation.

Purpose/Problem Statement:

The main goal of our project is to develop an understanding of cybersecurity, cybercrimes, and mitigation strategies in the modern digital landscape. As cyber threats evolve, understanding risk assessment and mitigation strategies is crucial to protect sensitive information and prevent financial losses. According to a report by cybersecurity ventures, cybercrime is projected to cost the world $6 trillion dollar annually, up from $3 trillion in 2015[1]. This project addresses this need by exploring key concepts like CIA- data confidentiality, integrity, and availability [2] We will also analyze common types of cyber threats-ransomware, spyware [3], phishing, and malware[4] and how they effect our systems.

We will also design and implement a basic cybersecurity solution to protect personal devices and systems from common cyberthreats such as weak passwords, phishing attacks, unauthorized access, and outdated software.

Background:

This cybersecurity project aims to explore fundamental concepts in protecting digital assets from different cyber threats. It involves hands-on exercise in risk assessment, vulnerability analysis and implementing security measures.

In today's digital age, protecting personal and organizational data from cyber threats is paramount. However, many individuals and businesses remain vulnerable to common cybersecurity risks due to weak passwords, malware infections, and outdated software. This project aims to address these vulnerabilities by developing a simple yet effective cybersecurity solution. By focusing on detecting weak passwords, identifying malware threats, and reminding users of necessary software updates, this project seeks to enhance cybersecurity awareness and mitigate potential risks in digital environments. Through the implementation of automated tools and proactive measures, this project aims to empower users to safeguard their digital assets and minimize the likelihood of cyberattacks and breaches.

How it works?

It works by reminding the user after a set period that they are lacking certain security features which are essential for the safety of the user.

❖ Password Checker:

It works by detecting weak passwords when a user enters it and recommends stronger passwords. When a user enters a password, the software gives recommendations to the user based on the length of the password, the strength of the password depending on the use of special characters, upper case and lower-case characters and numerical values.

❖ Phishing Websites:

Phishing attacks work by taking a user to a false website and getting them to put sensitive information in the fields. The data gets stored using a database query language or in our case SQL. Once the data gets stored the opposers can use the data for malicious purposes like “Blackmailing, Selling the private data, Using the sensitive info to get access to user’s goods”.

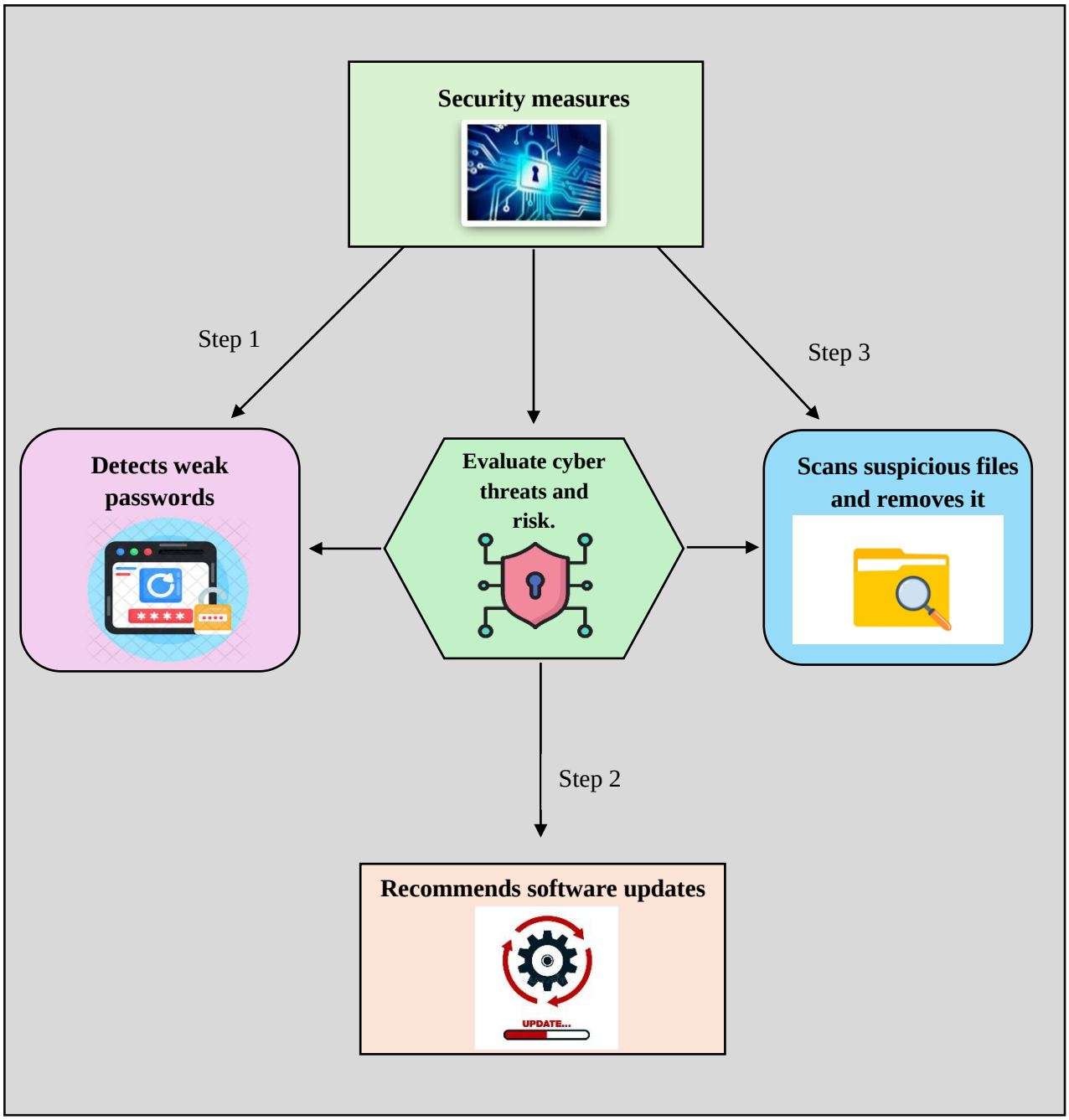
❖ Spyware Detection:

An antivirus software works by constantly scanning the user’s system for any malicious files or spywares. Which could normally be hidden from the user’s naked eye. And a virus scan could help bring the following hidden spywares to light and help eliminate them from a user’s system.

❖ Update Recommendations:

An update recommendation software mostly comes prebuild into OS these days, the main purpose of software’s is to remind the user after a set period that they are missing essential security updates.

System Model:



Language/Technologies used:

- ❖ Html-Language
- ❖ CSS
- ❖ Bootswatch
- ❖ Flask
- ❖ Jinja
- ❖ Sq lite 3
- ❖ Python

Includes:

- ➢ We used the following functions and iterables within these technologies:
  - ❖ Route
  - ❖ Redirects
  - ❖ Render_template
  - ❖ Flash
  - ❖ Jinja Syntax {% %}
  - ❖ SQL queries, such as (SELECT, UPDATE, INSERT, AND JOIN TABLES)

Note: Please do not alter the font size, font style, or formatting of this file. All data should be entered while maintaining the same formatting.

❖ References:

1. Morgan, S. (2019). 2019 Official Annual Cybercrime Report. Cybersecurity Ventures.
2. Ponemon Institute, 2020; ISO 27001, 2013.
3. "The hidden Dangers of spyware" By McAfee.
4. "Malware trends and tactics" by the Cybersecurity and Infrastructure Security Agency (CISA)

N	R	G	Doc.	Project