PROJECT REPORT

On

PASSWORD ANALYSIS (CYBER SECURITY)

(B.Tech CSE 3rd Semester Mini project)

2023-2024

Submitted to:

Dr. Susheela

(CC-CSE-F2-3rd Sem)

Submitted by:

Mr. Sarang Negi

Roll. No: 2219563

B.Tech CSE

Section-F2 (3rdSem)

Session: 2023-2024

DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

GRAPHIC ERA HILL UNVERSITY, DEHRADUN

CERTIFICATE

Certified that Mr. Sarang Negi (Roll No.- 2219563) has developed mini project on "PASSWORD ANALYSIS (Cyber Security)" for the CS 3rd Semester Mini Project Lab in Graphic Era Hill University, Dehradun. The project carried out by Students is their own work as best of my knowledge.

Dr. Susheela

Class Co-ordinator

CSE-F2-3rd Sem

(CSE Department) GEHU Dehradun

ACKNOWLEDGMENT

I would like to express my sincere gratitude to my mentor, Dr. Susheela for their guidance and support throughout this project. Dr. Susheela was always available to answer my questions and provide me with feedback. I am grateful for their patience and encouragement.

I would also like to thank my classmates for their support. We worked together to overcome challenges and to achieve our goals. We shared resources and ideas, and we helped each other to stay on track. I am grateful for their friendship and support.

Finally, I would like to thank my family and friends for their love and support. They encouraged me to pursue my goals and to never give up. I could not have completed this project without them.

Mr. Sarang Negi

Roll No.- 2219563

CSE-F2-3rd Sem

Session: 2023-2024

GEHU, Dehradun

Table of contents :-

1. **INTRODUCTION TO CYBER SECURITY**
2. **TYPES OF CYBER SECURITY**
3. **PASSWORD ANALYSIS IN CYBER SECURITY**
4. **ROLE OF PASSWORD ANALYSIS IN CUBER SECURITY**
5. **ALGORITHM FOR CODE**

INTRODUCTION

Cybersecurity refers to any technology, measure or practice for preventing cyberattacks or mitigating their impact. Cybersecurity aims to protect individuals' and organizations' systems, applications, computing devices, sensitive data and financial assets against simple and annoying computer viruses, sophisticated and costly ransomware attacks, and everything in between.

Types of cyber security :-

A strong cybersecurity strategy protects all relevant IT infrastructure layers or domains against cyberthreats and cybercrime.Critical infrastructure security protects the computer systems, applications, networks, data and digital assets that a society depends on for national security, economic health and public safety.

Network security :

Network security prevents unauthorized access to network resources, and detects and stops cyberattacks and network security breaches in progress—while at the same time ensuring that authorized users have secure access to the network resources they need, when they need them.

Endpoint security :

Endpoints—servers, desktops, laptops, mobile devices—remain the primary entry point for cyberattacks. Endpoint security protects these devices and their users against attacks, and also protects the network against adversaries who leverage endpoints to launch attacks.

Application security :

Application security protects applications running onpremises and in the cloud, preventing unauthorized access to and use of applications and related data, *and* preventing flaws or vulnerabilities in application design that hackers can use to infiltrate the network. Modern application development methods—i.e. DevOps and DevSecOps—build security and security testing into the development process.

Cloud security :

Cloud security secures an organization's cloud-based services and assets—applications, data, storage, development tools, virtual servers and cloud infrastructure. Generally speaking, cloud security operates on the shared responsibility model: the cloud provider is responsible for securing the services they deliver and the infrastructure used to deliver them, while the customer is responsible for protecting their data, code and other assets they store or run in the cloud. The details vary depending on the cloud services used.

Information security :

Information security (InfoSec) pertains to protection of all an organization's important information—digital files and data, paper documents, physical media, even human speech—against unauthorized access, disclosure, use or alteration. Data security, the protection of digital information, is a subset of information security and the focus of most cybersecurity-related InfoSec measures.

Mobile security :

Mobile security encompasses a number of disciplines and technolgies specific to smartphones and mobile devices, including mobile application management (MAM) and enterprise mobility management (EMM). More recently, mobile security is available as part of unified endpoint management (UEM) solutions that enable configuration and security management for all endpoints—not just mobile devices but desktop, laptops, and more) from a single console.

Password Analysis in Cyber Security

What is password?

-> A password is a secret word or phrase or code that you need to know in order to have access to a place or system. In technical terms, it is a series of letters or numbers that you must type into a computer or computer system in order to be able to use it. A password is a real-life implementation of challenge-response authentication (a set of protocols to protect digital assets and data).

Password Management

-> Since passwords are meant to keep the files and data secret and safe so it is prevented the unauthorized access, password management refers to the practices and set of rules or principles or standards that out must follow or at least try to seek help from in order to be a good/strong password and along with its storage and management for the future requirements.

Role Of Password Analysis In Cyber Security :-

->Password analysis plays a crucial role in cybersecurity by assessing and enhancing the strength of passwords used to protect sensitive information. It involves evaluating factors such as complexity, length, and uniqueness to identify vulnerabilities. Strong passwords are a fundamental defense against unauthorized access, reducing the risk of data breaches and unauthorized system access. Regular analysis helps organizations identify weak passwords and enforce stronger authentication measures, contributing to overall cybersecurity resilience.

ALGORITHM FOR PASSWORD ANALYSIS CODE :

1.Include necessary header files:

-> Include the <iostream> and <cctype> header files for input/output operations and character classification.

2. Use the standard namespace:

-> Declare the usage of the standard namespace.

3. Define a function to check the length of the password: -> Create a function checkLength that takes a password and a minimum length as parameters, returning a boolean indicating whether the password meets the length requirement.

4. Define a function to check the complexity of the password: -> Create a function checkComplexity that takes a password as a parameter and checks for the presence of uppercase, lowercase, digit, and special characters.

5. Define a function to analyze the password:

-> Create a function passwordAnalysis that takes a password as a parameter.

-> Set a minimum length requirement.

-> Check the length and complexity of the password using the previously defined functions.

-> Print appropriate messages based on the analysis results.

6. Implement the main function:

-> Inside the main function:

-> Declare a string variable userPassword to store the user's input.

-> Prompt the user to enter their password.

-> Read the user's input and call the passwordAnalysis function with the entered password.

7. Return from main:

-> End the program by returning 0.

CODE:

```
#include <iostream>
#include <cctype> /* Defines various functions to classify and transform
characters */
 using namespace std
;
 bool checkLength(const string& password, int minLength)
{     return password.length() >= minLength;
}  bool checkComplexity(const string& password) {     bool
hasUppercase = false, hasLowercase = false, hasDigit = false,
hasSpecial = false;     for (char ch : password) {         if
(isupper(ch)) {             hasUppercase = true;         } else if
(islower(ch)) {             hasLowercase = true;         } else if
(isdigit(ch)) {             hasDigit = true;
        } else {
hasSpecial = true;
        }     }     return hasUppercase && hasLowercase &&
hasDigit && hasSpecial;
}  void passwordAnalysis(const string& password) {
int minLength = 8; // Minimum length required     bool
lengthCheck = checkLength(password, minLength);
bool complexityCheck = checkComplexity(password);
if (lengthCheck && complexityCheck) {         cout <<
"Strong password!" << endl;
```

```
    } else if (lengthCheck || complexityCheck) {
cout << "Moderate password." << endl;
    } else {         cout << "Weak password!" << endl << "Enter a
strong password use numbers,and special characters - " << endl;
       } }
int main()
 {     string userPassword;
cout << "Enter your password: ";
cin >> userPassword;
passwordAnalysis(userPassword);
return 0;
}
```