**Final Project – Title, Scope, and Members**

**Tentative Title**

Why Weak Passwords Still Put Cybersecurity at Risk

**Scope of the Project**

This project focuses on the problem of weak and reused passwords. Many people continue to use simple passwords like “123456” or reuse the same password for multiple accounts. This practice creates a major security risk because attackers can easily exploit weak credentials through brute-force attacks, credential stuffing, and phishing-based password harvesting.

The project incorporates a simulated client–server environment within a virtual machine (VM) to represent real-world password vulnerabilities in a safe and controlled setting. The client system will simulate user authentication attempts, while the server will store user credentials. Controlled brute-force and dictionary attacks will be demonstrated to compare how quickly weak passwords can be cracked compared to strong ones.

In addition, the project will demonstrate how using secure password management tools (such as Bitwarden or KeePass) and implementing multi-factor authentication (MFA) can significantly reduce the success rate of password attacks.

The goal is to provide a realistic, hands-on demonstration of password vulnerabilities and show how modern tools and authentication practices enhance cybersecurity.

**Group Members**

Working individually.

**Data for the Project**

**Describe the data**  
This project utilizes a combination of publicly available datasets, industry reports, and simulated experimental results to analyze the risks associated with weak and reused passwords. The data sources include:

* Public password breach datasets such as the *RockYou* password list and *Have I Been Pwned* password statistics.
* Published cybersecurity reports and academic research focusing on password reuse, credential stuffing, and password strength analysis.
* Industry statistics from organizations such as the *Verizon Data Breach Investigations Report (DBIR)* and the *Ponemon Institute*, which provide quantitative insights into password-related breaches.
* Simulated experimental data from the virtual environment, including measurements of password-cracking attempts, success rates, and time required to compromise weak versus strong passwords.
* Case studies of real-world incidents where poor password practices led to unauthorized access or data breaches.

This combination of real-world and experimental data allows for both theoretical understanding and practical demonstration of password vulnerabilities. It provides a solid foundation for analyzing not only how weak passwords are exploited but also how implementing secure password managers, stronger password policies, and multi-factor authentication (MFA) can mitigate these risks.

**Ethical Considerations**

All data sets used in this project are publicly accessible and ethically sourced. Sensitive or personally identifiable data will not be used. Instead, the analysis will rely on aggregated statistics and safe, simulated experiments to maintain ethical and academic integrity.

**Links to Data Sources**

* Have I Been Pwned – Password Statistics:

<https://haveibeenpwned.com/Passwords>

* Verizon Data Breach Investigations Report (DBIR): <https://www.verizon.com/business/resources/reports/dbir/>

**Overview of the Project (Abstract)**

Weak and reused passwords continue to be one of the easiest entry points for attackers. Even with stronger technologies available, users still fall back on predictable credentials, which makes brute force and credential stuffing attacks highly effective. The goal of this project is to study why weak passwords remain common, how attackers exploit them, and what solutions can realistically improve security.

The project will use data from breach statistics, password studies, and security reports to show trends in password strength and reuse. The methodology includes analyzing datasets, reviewing reports like the Verizon DBIR, and studying recent incidents where poor password hygiene was the root cause.

Expected outcomes are:

* A clear explanation of the risks created by weak passwords.
* Insights into how attackers exploit them in real-world breaches.
* An evaluation of mitigation strategies such as password managers, MFA, and better user education.
* Actionable recommendations for individuals and organizations to reduce risks.

By focusing on both the human and technical sides of the problem, the project aims to present realistic steps toward stronger security.

**Timeline and Member Contribution**

Since this is an individual project, I am responsible for all stages. The weekly timeline is as follows:

* **Week of Sept 25 – Oct 1:** Gather and review data sources (breach datasets, security reports, case studies).
* **Week of Oct 2 – Oct 8:** Analyze data; draft the background and problem statement.
* **Week of Oct 9 – Oct 15:** Write analysis of attack methods and case studies.
* **Week of Oct 16 – Oct 22:** Draft solutions and recommendations section.
* **Week of Oct 23 – Oct 29:** Assemble the first full draft of the paper.
* **Week of Oct 30 – Nov 12:** Revise and polish; integrate feedback if any.
* **By Nov 28:** Upload project to GitHub repo and submit repo link.
* **By Dec 10:** Record and submit final video presentation explaining findings and recommendations.

**Member Contribution:**

All research, analysis, coding (if any), writing, and presentation work will be completed by me.