Assessing the Security and Privacy of Detack EPAS, a Password Security Assessment System

REIT7841 Project Proposal

Student Name: Subhav Batra

Student ID: 48773203

Date: 26/03/2025

Introduction

In the modern cybersecurity landscape, password security remains a critical challenge for organizations worldwide. Despite advancements in technology, weak password practices continue to be a leading cause of data breaches. Traditional authentication mechanisms are increasingly vulnerable to attacks such as phishing, brute force, and credential stuffing. With organizations facing growing pressures to comply with stringent regulations such as GDPR (General Data Protection Regulation) and PCI-DSS (Payment Card Industry Data Security Standard), there is an urgent need for enhanced security measures, particularly in password authentication systems.

This research focuses on integrating robust password authentication with Blue Team strategies to strengthen data protection and ensure regulatory compliance. The goal is to explore how Blue Teams, through continuous monitoring and proactive security measures, can enhance password security systems and safeguard sensitive data. By combining theory and practical security strategies, this study aims to bridge the gap between theoretical security practices and real-world defence operations.

Problem Statement

Despite the increasing reliance on digital data, organizations often fail to adequately protect sensitive information due to weaknesses in password authentication systems. These systems are prone to common vulnerabilities, such as weak or reused passwords, making them susceptible to various attacks. Additionally, organizations often overlook the strategic role of Blue Teams in strengthening password systems and ensuring compliance with privacy and data protection regulations.

The lack of integration between password authentication mechanisms and Blue Team operations means that organizations are less prepared to respond to breaches involving compromised credentials. Furthermore, maintaining compliance with regulations without robust password policies and monitoring is a significant challenge for organizations. Thus, this research seeks to investigate how a combination of secure password protocols and Blue Team strategies can reduce vulnerabilities, improve incident response, and support regulatory compliance.

Research Objectives

1. Adopting and implementing the password assessment system for ASOC system.
2. To analyse the vulnerabilities in current password authentication systems and explore best practices for robust authentication mechanisms.
3. To examine the role of Blue Teams in cybersecurity, focusing on their role in password protection and ensuring regulatory compliance.
4. To develop a framework for integrating password authentication strategies with Blue Team operations to enhance data protection and compliance.
5. To assess the effectiveness of the proposed framework in identifying and mitigating password-related security breaches.

Literature Review

The literature surrounding password authentication systems and their integration with Blue Team strategies is rich, yet fragmented. Below are some key papers and findings that inform this research:

- **"The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes"** (Bonneau et al., 2012):
  This paper discusses the various weaknesses of password-based systems and the challenges of transitioning to alternative authentication methods. It highlights issues such as user behaviour, password reuse, and weak password creation, which remain prominent in today's systems. The authors emphasize that multi-factor authentication (MFA) can significantly improve security, but its adoption is hindered by user convenience and implementation challenges.
- **"Improving Organizational Password Policy Compliance via Open-Source Tools"** (Christopher M. Frenz, IEEE 2011)
  Frenz (2011) explores how open-source tools can be leveraged to enhance password policy compliance within organizations. The study introduces two key applications: a CGI server-based random password generator and a password complexity filter. These tools collectively address password security at both the creation and enforcement stages, ensuring that organizations can enforce robust password policies effectively.

The study emphasizes the importance of customizable security solutions in mitigating weak password practices.

- **"Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines"** (Florence Mwagwabi, Tanya McGill, Michael Dixon, IEEE)
  Mwagwabi et al. (2014) examine the relationship between user perceptions of password security threats and compliance with organizational password guidelines. Using protection motivation theory, the study evaluates how security awareness training impacts user behaviour, highlighting that enhanced training programs can improve compliance. The findings suggest that organizations should focus on improving users' security coping appraisal to encourage stronger password practices.
- **"Towards Designing Effective Security Messages: Persuasive Password Guidelines"** (Nur Haryani Zakaria, Norliza Katuk, IEEE)
  Zakaria and Katuk (2013) explore the role of persuasive security messages in improving password guideline compliance. The study identifies human factors as the weakest link in security and highlights the need for better-designed security messages. Through a pilot study, the authors find that adding persuasive elements to password guidelines increases user motivation to create stronger passwords. Their findings suggest that organizations should focus on communication strategies that enhance security awareness and behavioural compliance.
- **"Deceptive Deletion Triggers Under Coercion"** (Lianying Zhao, Mohammad Mannan, IEEE Transactions on Information Forensics and Security)
  Zhao and Mannan (2016) examine the challenges of protecting password-protected encrypted data, particularly when users are coerced by adversaries. They propose a novel solution, Grace wipe, which allows users to fake compliance by entering a "deletion password" under duress, triggering the deletion of encryption keys and making the data inaccessible. This method leverages Trusted Platform Module (TPM) and trusted execution modes like Intel TXT to enable verifiable deletion. The research is crucial for high-stakes users, such as journalists or government agents, and offers a way to protect sensitive data under extreme circumstances, where traditional encryption methods fail.

- **"Killing the Password and Preserving Privacy with Device-Centric and Attribute-Based Authentication"** (Kostantinos Papadamou, Savvas Zannettou, Bogdan Chifor, Sorin Teican, George Gugulea, Alberto Caponi, IEEE Transactions on Information Forensics and Security)
  Papadamou et al. (2019) discuss the inherent weaknesses of traditional password-based authentication systems, highlighting issues such as poor security and lack of privacy. The authors propose a novel architecture that integrates device-centric and attribute-based authentication to replace traditional password methods, aiming for stronger security and improved user experience. Their approach ensures privacy-preserving access while supporting federated logins and identity profile management. The architecture is designed to comply with NIST assurance levels and offers solutions for account recovery in case of device loss. This research offers a promising alternative to the password system and improves usability while addressing privacy concerns.
- **"Development and Testing of a Core System for Red and Blue Scenario in Cyber Security Incidents"** (Cristian Chindrus, Constantin F. Caruntu, IEEE, 2022)
  Chindrus and Caruntu (2022) focus on the growing challenge of cyber-attacks and the importance of enhancing cyber security measures, especially considering the increasing digitalization of businesses. They explore the concept of the red and blue team exercises, a classic method in training security teams to respond to cyber incidents. However, they introduce an innovative approach combining both red and blue scenarios into a single framework to simulate real-life attacks. This system helps train cybersecurity teams more effectively, providing insights into hacker behaviour and enabling better coordination during actual incidents. The authors argue that this approach improves response time and overall understanding of cyber-attacks compared to traditional Red vs. Blue competitions.
- **"Enhancing Cyber Situational Awareness: A New Perspective of Password Auditing Tools"** (Eliana Stavrou, IEEE, 2018)
  Stavrou (2018) emphasizes the importance of password auditing in enhancing cyber situational awareness, especially for cybersecurity professionals who monitor and protect organizations' IT infrastructures. She highlights that password cracking, while a time-consuming process, is commonly used for auditing passwords. Existing password cracking tools, however, are limited in their ability to optimize the process

within a given evaluation timeframe. To address this gap, the paper advocates for the development of next-generation password auditing toolkits. These toolkits should incorporate holistic features that enhance password auditing effectiveness. Furthermore, Stavrou underscores the necessity of integrating password security policies that provide clear rules for constructing passwords. These tools, in conjunction with a robust policy framework, would enable defenders to proactively identify weak passwords, ultimately reducing the risk of data breaches and unauthorized access.

- **"Password Strength: An Empirical Analysis"** (Matteo Dell'Amico, Pietro Michiardi, Yves Roudier, IEEE, 2010)
  Dell'Amico, Michiardi, and Roudier (2010) explore the predictability of user-chosen passwords and how attackers can reduce the number of attempts needed to crack them using tools like dictionaries or probabilistic models. Their study aims to answer an important question: given a fixed number of guesses, what is the likelihood that an attacker will successfully break a password? Through empirical analysis of multiple datasets containing known passwords, they observe a “diminishing returns” phenomenon. While weak passwords are common, as the attack continues, the probability of success for the attacker diminishes exponentially. Even highly powerful attackers cannot guess a significant portion of passwords once an attack progresses. This research provides valuable insights for evaluating the effectiveness of user-chosen password authentication and offers a foundation for creating better proactive password checkers and security auditing tools.

Methodology

This research will adopt a mixed-methods approach combining qualitative and quantitative analysis. It will involve:

- Literature Review: Analysing existing studies and industry reports.
- Case Studies: Reviewing real-world incidents where password authentication failures led to security breaches and examining how Blue Teams responded.
- Proposed Framework: Designing a framework that integrates Blue Team operations with robust password authentication practices to enhance security and regulatory compliance.

Data will be collected through interviews with cybersecurity professionals and industry case studies, providing practical insights into the current state of password security and Blue Team operations.

Timeline

Activity	Duration
Literature Review	March 2025 - April 2025
Methodology Design	April 2025 - May 2025
Data Collection	May 2025 - June 2025
Data Analysis and Framework Development	June 2025 - August 2025
Drafting Thesis	August 2025 - November 2025
Final Review and Submission	November 2025

Conclusion

This research contributes to cybersecurity and privacy protection by proposing a robust password authentication framework tailored for blue team operations. By addressing security gaps in password management and aligning with compliance requirements, this study will offer practical recommendations for organizations to enhance data protection.

References

1. J. Bonneau et al., *"The Quest to Replace Passwords"* IEEE Security & Privacy, 2012.
2. C. M. Frenz, *"Improving Organizational Password Policy Compliance via Open-Source Tools,"* IEEE, 2011. [Online]. Available: IEEE Xplore.
3. F. Mwagwabi, T. McGill, and M. Dixon, *"Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines,"* 47th Hawaii International Conference on System Sciences, 2014. [Online]. Available: IEEE Xplore.
4. N. H. Zakaria and N. Katuk, *"Towards Designing Effective Security Messages: Persuasive Password Guidelines,"* 2013 International Conference on Information Security and Cyber Forensics, 2013. [Online]. Available: IEEE Xplore.
5. L. Zhao and M. Mannan, *"Deceptive Deletion Triggers Under Coercion,"* IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2672-2685, Dec. 2016. [Online]. Available: IEEE Xplore.
6. K. Papadamou et al., *"Killing the Password and Preserving Privacy With Device-Centric and Attribute-Based Authentication,"* IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2183-2193, Dec. 2019. [Online]. Available: IEEE Xplore.
7. C. Chindrus and C. F. Caruntu, *"Development and Testing of a Core System for Red and Blue Scenario in Cyber Security Incidents,"* 15th International Conference on Security of Information and Networks, Sousse, Tunisia, Nov. 2022. [Online]. Available: IEEE Xplore.
8. E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin, 2011. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
9. E. Stavrou, *"Enhancing Cyber Situational Awareness: A New Perspective of Password Auditing Tools,"* 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Glasgow, UK, Jun. 2018. [Online]. Available: IEEE Xplore.
10. M. Dell'Amico, P. Michiardi, and Y. Roudier, *"Password Strength: An Empirical Analysis,"* in Proc. 2010 IEEE INFOCOM, San Diego, CA, USA, Mar. 2010, pp. 1-9.

11. N. Gelernter, S. Kalma, B. Magnezi, and H. Porcilan, *"The Password Reset MitM Attack,"* in Proc. 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, May 2017, pp. 629-644. [Online]. Available: IEEE Xplore.
12. Y. Zhang, J. Wang, and X. Li, "A Survey of Machine Learning-Based Solutions for Phishing Website Detection," *Machine Learning and Knowledge Extraction*, vol. 3, no. 3, pp. 672–694, 2021. [Online]. Available: https://www.mdpi.com/2504-4990/3/3/34
13. OpenAI. (2025). ChatGPT (March 26 version) [Large language model]. https://chat.openai.com/