Relatório Acadêmico: Password Vaults (Gerenciadores de Senhas)

Instituto Federal de Santa Catarina (IFSC) – Campus São José
Curso: Analise e Desenvolvimento de Sistemas – ADS (Noturno)
Disciplina: Segurança de Informação
Alunos(a): Jessé Ricardo Rogério & Kauê dos Santos Rocha
Professor(a): Emerson Ribeiro de Mello
Data: 12/06/2025

Introdução

A segurança digital é um dos pilares da proteção de dados na era da informação. Com o aumento de vazamentos e ataques cibernéticos, a utilização de *password vaults* (ou gerenciadores de senhas) tornou-se essencial para mitigar riscos como *phishing*, *credential stuffing* e *keyloggers*. Este relatório explora os conceitos, tipos, benefícios e desafios dessas ferramentas, além de apresentar um estudo de caso real e atividade prática.

1.1 Objetivos

- Explicar o funcionamento técnico dos "*password vaults"*.
- Comparar os diferentes tipos disponíveis (locais, em nuvem, navegadores e de *hardware*).
- Analisar vulnerabilidade e um caso real de vulnerabilidade (LastPass, 2022).
- Fornecer orientações para uso seguro & uso de *vaults.*

1.2 Justificativa

A reutilização de senhas e a adoção de credenciais fracas são práticas comuns que comprometem a segurança. *Password vaults* resolvem esses problemas ao centralizar o armazenamento de senhas com criptografia robusta, garantindo praticidade sem sacrificar a proteção, utilizando apenas uma senha mestre.

Fundamentação Teórica

2.1 Armazenamento Criptográfico

- **Criptografia AES-256:** Padrão avançado para encriptação dos dados.
- **Armazenamento:** Bancos de dados locais ou em nuvem (sempre criptografados).

2.2 Senha Mestra (Master Password)

• Única senha necessária para acessar o cofre. (*master password*)

- **Proteções:**
- *Hashing* (PBKDF2, Argon2, bcrypt) para prevenir ataques de força bruta.
- *Zero-Knowledge Proof*: O provedor não tem acesso à senha mestra, apenas tem acesso a dados criptografados.

•2.3 Autenticação Multi-Fator (MFA/2FA)

• Adiciona uma camada extra de segurança (ex.: token via app, biometria, sms).

2.4 Geração de Senhas Aleatórias

• Cria senhas complexas (20+ caracteres) com alta entropia (PRNG/CSPRNG).

Tipos de Password Vaults

Tipo	Exemplos	Vantagens	Desvantagens
Local	KeePass, Bitwarden	Controle total, imune a vazamentos	Sem sincronização, backup manual
Nuvem	LastPass, 1Password	Sincronização automática	Risco de vazamento em nuvem
Navegador	Google Password Manager	Integração fácil com navegadores	Criptografia menos robusta
Hardware	YubiKey, Trezor	Resistente a malware	Custo elevado, perda física

---

Metodologia

Este relatório baseia-se em:

- **Revisão bibliográfica:** Fontes como OWASP, Wikipedia e manuais técnicos.
- **Estudo de caso:** Análise do vazamento do LastPass (2022).
- **Demonstração prática:** Configuração básica de um *password vault* (Bitwarden).

Caso Real: LastPass (2022)

5.1 O Ataque

• Explorou um engenheiro com 2FA desativado.

• Vazamento de *vaults* parcialmente descriptografados.

5.2 Lições Aprendidas

• 2FA obrigatório para todos os usuários.

• Senha mestra forte (mínimo 12 caracteres com símbolos).

• Segurança baseasse também em falhas individuais – Engenharia Social

---

Atividades Práticas (Espaço Reservado)

Instruções - https://github.com/jesse-rr/Webrepo/blob/main/README.md

---

Conclusão

Password vaults são ferramentas indispensáveis para segurança digital, principalmente para desenvolvimento e/ou senhas mais fortes, mas exigem:

• Senha mestra complexa e única.

• Habilitar 2FA sempre que possível.

• Escolher provedores confiáveis com criptografia desejável.

Embora não sejam imunes a falhas, sua adoção reduz significativamente riscos associados a senhas fracas e reutilizadas.

Referências

• **OWASP.** *Password Storage Cheat Sheet*. Disponível em: https://cheatsheetseries.owasp.org/.

• **Wikipedia.** *Password Manager*. Disponível em: https://en.wikipedia.org/wiki/Password_manager.

• **1Password.** *Enterprise Password Vaults Guide*. Disponível em: https://blog.1password.com/enterprise-password-vaults-guide/.