Slide 1: Relevância do Tema & Contexto

1. **Problema**

• Senhas fracas e reutilização de credenciais = vazamentos

• Múltiplas senhas = difícil de gerenciar/lembrar

2. **Solução** → *Password Vault*

3. **Importância**

• Reduz phishing, credential stuffing, keyloggers

• Permite senhas complexas sem necessidade de memorização

Slide 2: Principais Conceitos

1. **Armazenamento Criptográfico**

• Criptografia AES-256

• Banco de dados local ou em nuvem (sempre encriptado)

2. **Senha Mestra (Master Password)**

• Única senha (perdeu = perdeu tudo)

• Provedor só armazena dados criptografados (senhas exceto master)

• Chave mestra fica no cliente (browser/SO/diretório do app)

• Hashing (PBKDF2, Argon2, bcrypt) → Previne força bruta

• Zero-Knowledge Proof → Provedor não acessa senha mestra

3. **Autenticação Multi-Fator (MFA/2FA)**

• Reduz phishing e keyloggers

4. **Geração de Senhas Aleatórias**

• 20+ caracteres com símbolos e números

• Alta entropia (PRNG/CSPRNG)

• Elimina reutilização entre serviços

Slide 3: Tipos - Prós e Contras

1. **Locais (Offline)**

• *Exemplos*: KeePass, Bitwarden (self-host)

• **Prós**: Controle total, imune a vazamentos em nuvem

• **Contras**: Sem sincronização, backup manual obrigatório

2. **Nuvem**

• *Exemplos*: LastPass, 1Password

• **Prós**: Sincronização, monitoramento de vazamentos

• **Contras**: Risco de vazamento, dependência do provedor

3. **Navegadores**

• *Exemplos*: Google Password Manager, Firefox Lockwise

• **Prós**: Conveniente (preenchimento automático)

• **Contras**: Criptografia fraca, vulnerável a malware

4. **Hardware**

• *Exemplos*: Trezor, YubiKey

• **Prós**: Resistente a malware, ideal para 2FA

• **Contras**: Custo alto, perda = necessidade de backup

Slide 4: Caso Real - LastPass (2022)

• Ataque explorou engenheiro com **2FA desativado**

• Vazamento de vaults parcialmente descriptografados

• **Lição**: 2FA obrigatório + senha mestra forte são críticos

---

Slide 5: Demonstração Prática

Slide 6: Conclusão

• Elimina necessidade de memorizar senhas sem perder segurança

• Senha mestra é o elo mais fraco → deve ser forte e única

• AES-256 + 2FA essenciais para mitigar riscos

• **Não é perfeito mas é bom.**

Slide 7: Referências

OWASP Cheat Sheet - https://cheatsheetseries.owasp.org/ (Boas praticas & comparativos de segurança)

Wikipedia Password Managers - https://en.wikipedia.org/wiki/Password_manager (Tipos, usos, exemplos)

1Password Enterprise Guide - https://blog.1password.com/enterprise-password-vaults-guide/ (Como funciona em empresas grandes)

Deepseek (LLM) – Erros de Português e formatação do relatório. Possíveis ideias de atividades praticas.