ARMAZENAMENTO SEGURO DE SENHAS

ANDERSON SILVA LIMA
WWW.LINKEDIN.COM/IN/LS-ANDERSON

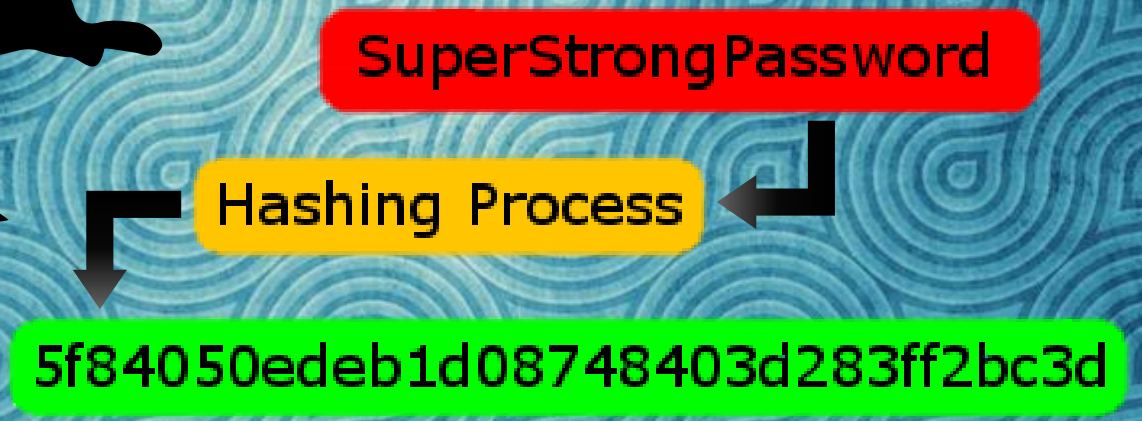
BLUETEAM COM ABORDAGEM OFENSIVA

A Defesa Cibernética com abordagem ofensiva consiste em analisar um cenário de ataque real ou simulado pensando como um atacante pensaria e como esse agente malicioso poderia comprometer um ambiente, assim, fortalecendo a segurança nos pontos identificados aumentando os esforços para um ataque obter sucesso.

PASSWORD HASHING

(...) é uma técnica utilizada em sistemas computacionais para ao invés de armazenar as senhas de usuários em texto plano é armazenado apenas a Hash dessas senhas no banco de dados. Essas Hashes são obtidas a partir de uma função de dispersão criptográfica (FDC).

MENEZES et al., 2001



CRYPTANALYSIS: ANÁLISE DE PADRÕES

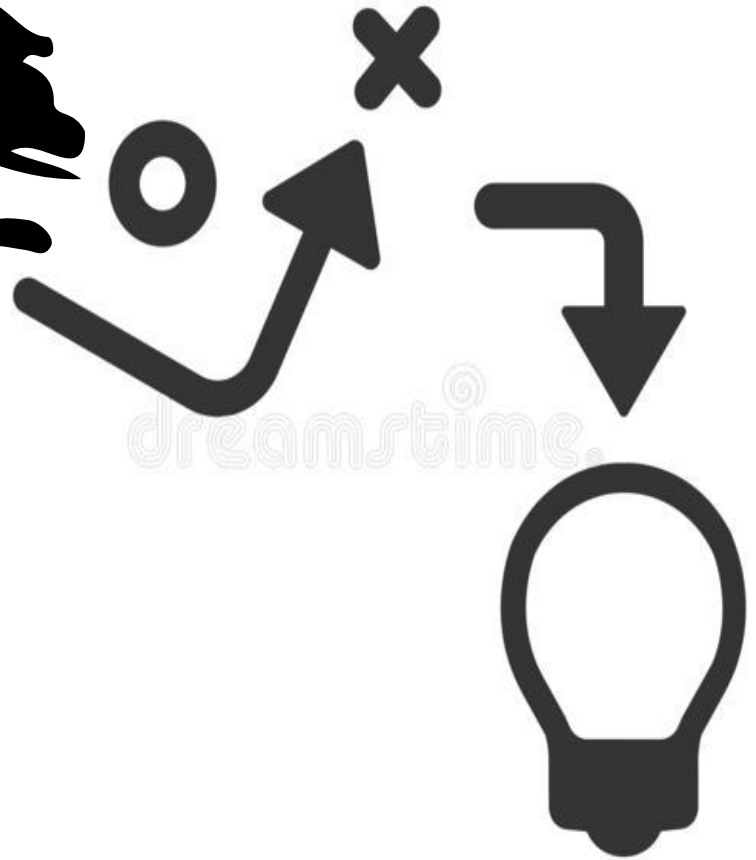
A partir de um conjunto de hashes de senhas um ator de ameaças analisa padrões identificando os seguintes pontos:

- Função Hash utilizada pela organização;
- Repetições de Hashes;
- Quantidade de repetições, pode indicar senha padrão;
- Possibilidade de Privilage Escalation;
- Lógica para composição de senhas;
- Nível de segurança no armazenamento de senhas.

CRYPTANALYSIS: ANÁLISE DE PADRÕES

Com essas informações em mãos é possível identificar:

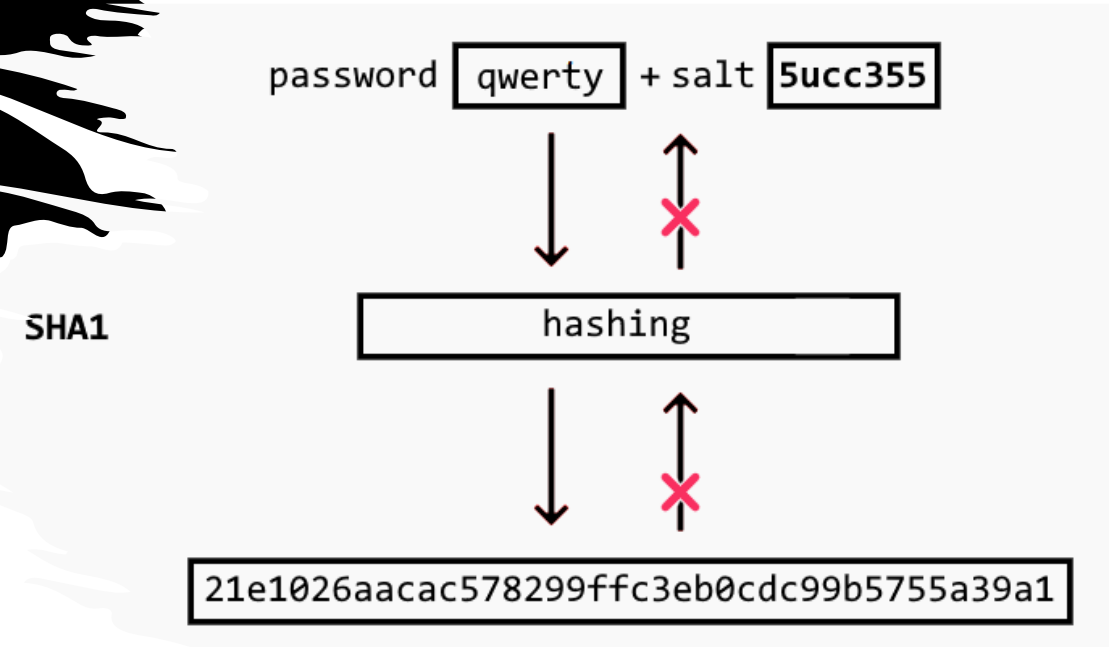
- Nível de fragilidade da função hash usada;
- Enumeração de usuários com mesmo hash de senha;
- Muitos hashes iguais indicam senhas simples ou senha padrão;
- Escalação de privilégios, caso existam perfis com diferentes privilégios com mesmo hash;
- Compreensão da lógica para composição de senhas na organização;
- Nível de segurança e esforço para comprometimento do ambiente.



SALT

(...) consiste na geração de random bits que são adicionados à palavra-chave, o que garante maior segurança uma vez que as passwords são armazenadas e registradas baseadas na encriptação da palavra-chave + algoritmo Salt.

GONÇALVES A., 2012



RNG: RANDOM NUMBER GENERATORS

(...) cryptographically-secure pseudorandom number generators (CSPRNGs) are algorithms which, provided an input which is itself unpredictable, produce a much larger stream of output which is also unpredictable. This stream can be extended indefinitely, producing as much output as required at any time in the future.

Cloudflare., 2017

RESULTADO

PASSWORD + SALT = HASH ÚNICO:

- Senha (Password) + Salt (123)
  - 42f749ade7f9e195bf475f37a44cafcb

- Senha (Password) + Salt (456)
  - b24ecc40cef177b0334c4cfa91f94d28

- Senha (Password) + Salt (789)
  - 00ab1b7b67089046530864l7f8fbcd12

ARMAZENAMENTO SEGURO DE SENHAS

ANDERSON SILVA LIMA
WWW.LINKEDIN.COM/IN/LS-ANDERSON