Hashcat

Hash

Input

Algoritmo

Hash

Principais algoritmos de hash

MD5 (I28 bits, 32 caracteres) → Rápido, mas fraco contra ataques.

SHA-I (I60 bits, 40 caracteres) → Melhor que MD5, mas ainda vulnerável.

SHA-256 (256 bits, 64 caracteres) → Mais seguro, usado em criptografia moderna.

NTLM → Usado por sistemas Windows para armazenar senhas.

Objetivo

Sumário

Introdução

- Uma ferramenta de recuperação de senhas que utiliza força bruta, dicionário e técnicas avançadas para quebrar hashes.
- Hashcat foi criado por Dominik Homberger a mais de 10 anos e é amplamente utilizado em auditorias de segurança para testar a resistência de senhas.

Casos de uso

- Auditoria de segurança: Verificar a força de senhas em um sistema.
- Recuperar senhas esquecidas ou perdidas.
- Identificar vulnerabilidades de autenticação.

Não serve só para hackinagens

Vantagens

- Suporta uma vasta gama de algoritmos de hash (MD5, SHA, bcrypt, etc.).
- Múltiplos modos de ataque como força bruta, dicionário, máscara, e híbrido.
- Otimizado para ser usado tanto em CPUs quanto em GPUs.

Desvantagens

- Precisa de HW.

Demonstração

Perguntas