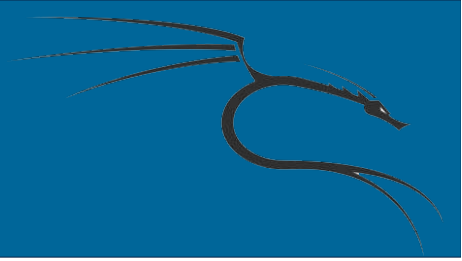
Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br



Hashes

Hash é uma sequência de bits criadas por um algoritmo de dispersão, normalmente representada em caracteres hexadecimais, que possibilita enxergar em números e em letras (0 a 9 e de A a F), simbolizando um nibble cada. Em tese: "hash é a transformação de uma enorme quantidade de informações em um pouca quantidade de informações".

Nibble - Sequência de quatro cifras binárias:

0010 0011 1001 0100 0111 0010 1000 0011 = 8 Nibbles

MD4: Foi criado no início da década de 90 por Ron Rivest. O MD4 sofreu vários ataques desde então, o que fez com que o algoritmo fosse considerado frágil.

MD5: O MD5 é um algoritmo de hash que contém 128 bits unidirecional criado pela RSA Data Security, Inc., e muito usado por softwares com protocolo P2P(Peer-to-Peer) checando a integridade e logins. Ele possui alguns métodos de ataque apresentados contra o MD5

SHA-1 (Secure Hash Algorithm): Criado pela NIST e NSA. Já foram exploradas falhas no SHA.

WHIRLPOOL: Desenvolvida por Paulo Barreto e por Vincent Rijmen. E está padronizada pelo ISO 10118-3.

O processo é unidirecional, ou seja fica impossível saber o conteúdo original a partir do hash. O valor do check-sum se altera se um único bit for modificado, colocado ou removido da mensagem.

Hashes

Os ataques aos banco de dados, o MD5 é o mais usado no quesito Hash

Encriptadores Online

http://www.md5encrypter.com/

http://md5encryption.com/

http://md5-encryption.com/

http://www.getrank.org/tools/md5-encrypter/

http://www.md5online.org/md5-encrypt.html

Decriptadores Online

http://www.md5decrypter.com/

http://www.md5decrypter.co.uk/

http://www.md5online.org/

http://www.md5decrypt.org/