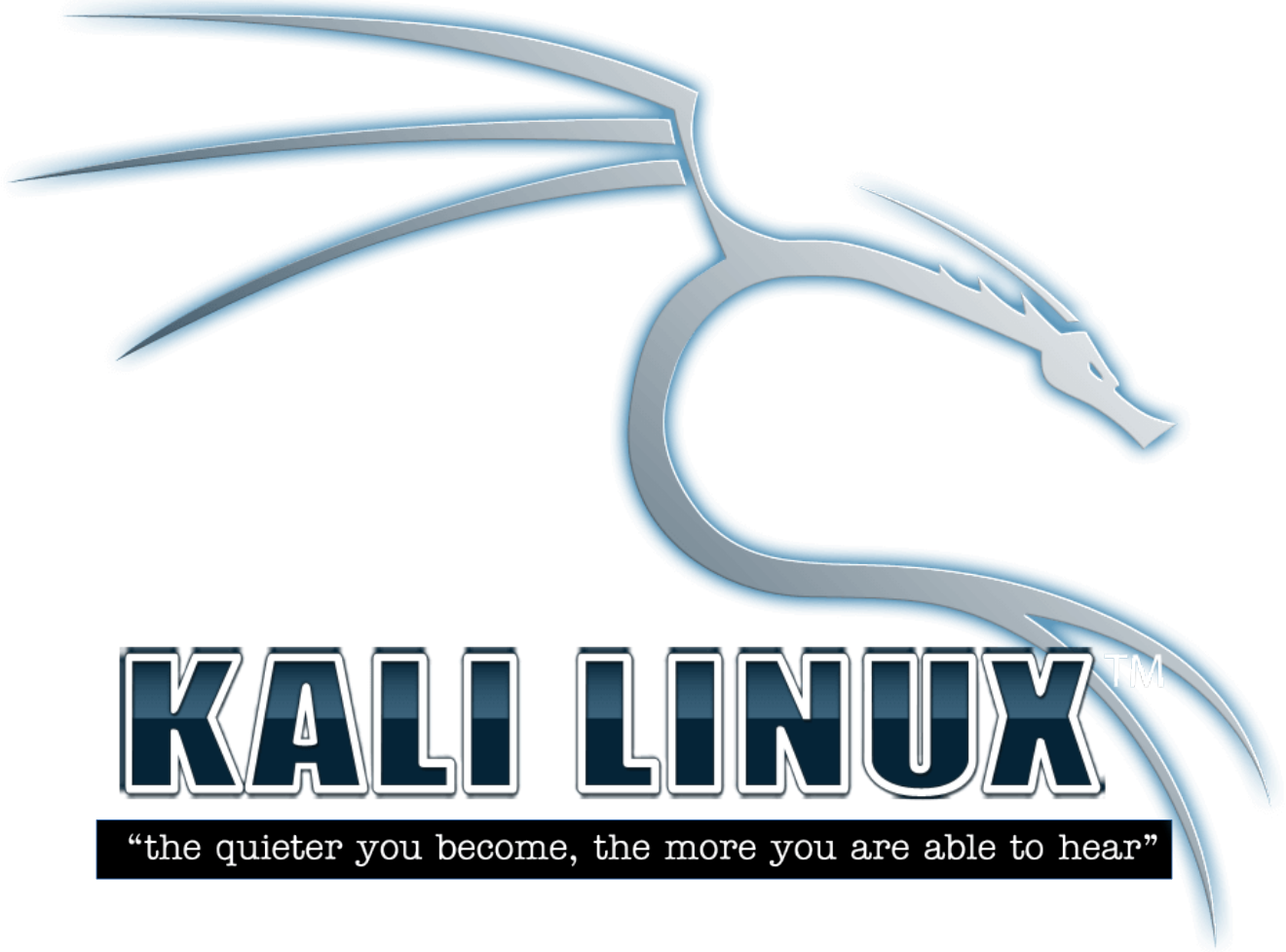
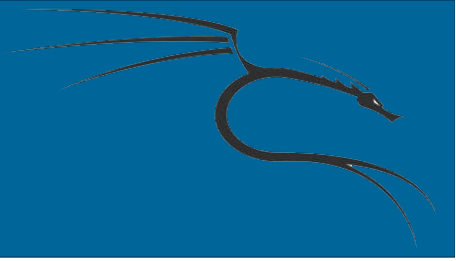
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:
http://vmzsolutions.com.br

Rainbow tables

Uma Rainbow Tables é uma tabela de pesquisa que oferece uma memória de troca de tempo usado para recuperar o texto simples de um *hash* de senha gerado por uma função hash, muitas vezes uma função de hash criptográfico.

Rainbow tables

Os RainbowCrack utiliza o algoritmo de troca de tempo de memória para decifrar as *hashes*. Difere dos métodos de brute force e de hash crackers. Seus principais aplicativos são:

- **rtgen**: Para criar a Rainbow Tables
- **rtsort**: Para organizar as Chains criadas e disponibiliza-las em ordem para uma rápida pesquisa
- **rcrack**: Para realizar a quebra da hash

Rainbow tables

Um *cracker hash* de força bruta gera todos os *plaintexts* possíveis e calcula as hashes correspondentes no alvo, então compare os hashes com o hash a ser quebrado. Uma vez que uma correspondência é achada, o *plaintext* (texto simples) é encontrado.

Rainbow tables

Se todos os plaintexts possíveis forem testados e nenhuma correspondência for encontrada, o texto não será decifrado.

Com este tipo de *cracking hash*, todos os resultados de computação intermediária são descartados. Ele usa conceito de Ataque de Tradeoff Time-Memory-Data.

Rainbow tables

Sintaxe: *rtgen hash_algorithm charset plaintext_len_min plaintext_len_max*

table_index chain_len chain_num part_index

Explicação:

hash_algorithm: O algoritmo dos hashes (lm, ntlm, md5, etc)

usado na rainbow table.

charset: A configuração dos caracteres (charset) do texto plano

na rainbow tables.

plaintext_len_min e plaintext_len_max: Esses dois parâmetros criam o tamanho possível de todo o texto plano na 'rainbow tables'. Caso o 'charset' é em números, o 'plaintext_len_min' é 1, e o 'plaintext_len_max' é 5, então a string seria "12345" e que será incluída na tabela, mas o valor "123456" **não**.

table_index, chain_len, chain_num e part_index: Esses quatro parâmetros são:

• O 'table_index' está relacionado ao 'reduce function' que é utilizado na 'rainbow table'.

• O 'chain_len' é o tamanho de cada 'rainbow chain' na 'rainbow table'. Uma 'rainbow chain' configurada como 16 bytes é a menor unidade em uma 'rainbow table'. Uma 'rainbow tables' contém inúmeras 'rainbow chains'.

- O 'chains_num' é o número de 'rainbow chains' em uma 'rainbow table'.
- O 'part_index' determina como o 'start point' em cada 'rainbow chain' é criado. Deve ser um número (ou começar com ele).

Viva o Linux

Rainbow tables

Para criarmos uma rainbow table com o uso do MD5, execute esses comandos em sua máquina: (**Processo altamente demorado, podendo levar de 2h á 7h de execução**).

```
# cd /usr/share/rainbowcrack/

#./rtgen md5 loweralpha-numeric 1 5 0 3800 33554432 0
```

Após esse processo devemos então organizar nossa lista e deixa-la indexada para agilizar o processo da quebra.

Para isso utilizamos a ferramenta rtsort:

```
# rtsort *.rt
```

Depois desse processo, basta realizar a tentativa da quebra com o commando rcrack:

```
# rcrack *.rt -h 5d41402abc4b2a76b9719d911017c592

# rcrack *.rt -l hash.txt
```

Rainbow tables

Esse rcrack é um trabalho de comparação de respostas, se você tiver uma lista de hashes poderá usar caso queria.

Rainbow tables

Agora que já vimos como rainbow tables trabalha, vamos pratricar e quebrar alguma hash do sistema Windows. Com a conta de um administratdor e sua senha *mullet* para tentar realizar a quebra do modo mais rápido possível.

Rainbow tables

- Primeiro temos que baixar a tabela de hashes do Windows XP free no site Ophcrack.
- Depois precisamos realizar a importação dessas hashes no Ophcrack
- Inserir a hash ou a SAM a ser quebrada
- Realizar o crack