Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

John the Ripper é uma ferramenta de software livre cracking de senha. O John the Ripper possui três modos de operação:

Dicionário (Wordlist): sendo o modo mais simples suportado pelo programa, este é o conhecido ataque de dicionário, que lê as palavras de um arquivo e verifica se são correspondentes entre si.

Quebra Simples (Single Crack): mais indicado para início de uma quebra e mais rápido que o wordlist, este modo usa técnicas de mangling e mais informações do usuário pelo nome completo e diretório /home em combinação, para achar a senha mais rapidamente.

Incremental: sendo o modo mais robusto no John the Ripper, ele tentará cada caractere possível até achar a senha correta, e por esse motivo é indicado o uso de parâmetros com o intuito de reduzir o tempo de quebra.

Externo (External): o modo mais complexo do programa que faz a quebra a partir de regras definidas em programação no arquivo de configuração do programa, que irá pré-processar as funções no arquivo no ato da quebra quando usar o programa na linha de comando e executá-las. Este modo é mais completo e necessita de tempo para aprender e acostumar-se.