Quebra de senhas

Esta atividade prática visa compreender o uso de uma ferramenta de quebra de senha através de força bruta.

Usando o John the Ripper

O software John the Ripper (JtR) é um quebrador de senhas (*password cracker*) bastante popular, usado para quebrar senhas de sistemas operacionais Windows e UNIX-like.

O JtR possui vários modos de operação:

- Modo *single*: testa variações das informações obtidas no próprio arquivo de senhas, como o nome completo do usuário e seu diretório de trabalho ($HOME). É o método mais simples e rápido para começar.

```
john -single password-file
```

- Modo *wordlist*: testa palavras em uma lista e variações delas. Pode ser lento se a lista de palavras for muito grande.

```
john -wordlist:wordfile password-file
```

ou aplicando também regras de transformação de palavras:

```
john -wordlist:wordfile -rules password-file
```

- Modo *incremental*: testa todas as variações possíveis de senha com até N caracteres; **este método pode ser MUITO lento**:

```
john -incremental password-file
```

Na maioria das distribuições Linux, listas de palavras usadas nos corretores ortográficos podem ser encontradas em `/usr/share/dict`.

Atividades

1. Analise dois arquivos de senhas dentre os disponibilizados pelo professor (em `trasgo:/usr/local/john/passwords`).
2. Extraia o arquivo de *hashes* de um sistema Windows, analise sua estrutura e tente quebrar suas senhas. Sugestão: use os programas `pwdump` ou `fgdump`.
3. Identifique ferramentas similares disponíveis na Internet e experimente uma delas com os mesmos arquivos (sugestões: Cain and Abel, HashCat, Ophcrack).
4. Identifique um site com tabelas *hash* pré-computadas e tente quebrar alguns dos hashes fornecidos (sugestão: http://wiki.insidepro.com/index.php/Hash_Databases) .