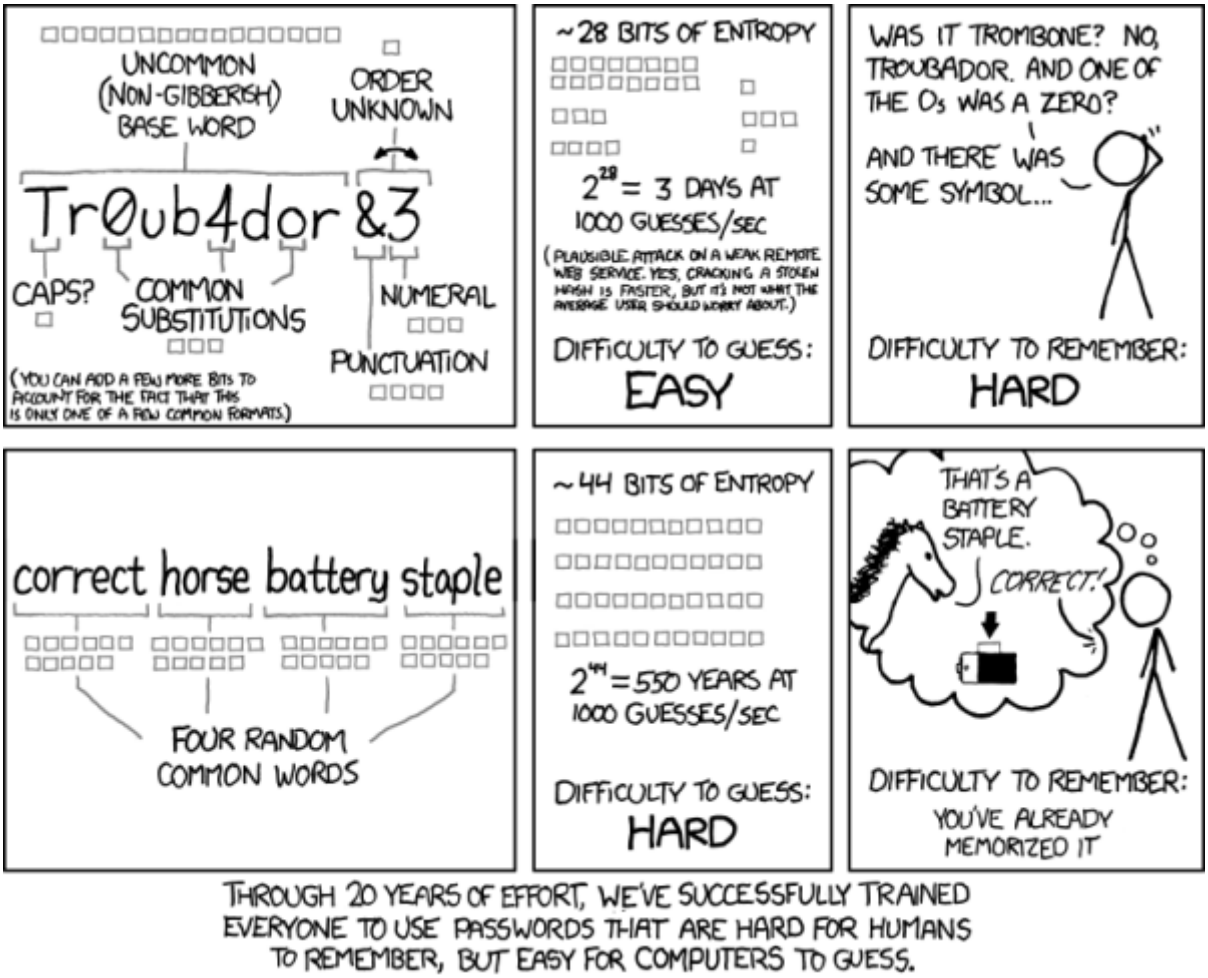
Quebra de senhas

Esta atividade prática visa compreender o uso de uma ferramenta de quebra de senha através de ataques do dicionário e 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, arquivos ZIP, PDF, etc.

"John" possui vários modos de operação, apresentados a seguir.

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
```

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

Existe a possibilidade de aplicar também regras de transformação de palavras:

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

Modo incremental

Este modo testa todas as variações possíveis de senha com até N caracteres, o que pode ser MUITO lento:

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

Pode-se restringir a busca exaustiva a um subconjunto de caracteres, usando um MODE:

```
john -incremental=MODE password-file
```

Os modos mais usuais são:

- ASCII - caracteres imprimíveis
- Alnum - alfanuméricos
- Digits - dígitos
- Alpha - letras
- Lower - letras minúsculas
- Upper - letras maiúsculas
- LowerNum, UpperNum - letras + dígitos
- LowerSpace, UpperSpace - letras + espaço

Outras opções

Quando John encontra uma senha, ele a mostra no terminal e a salva em um arquivo. As senhas já encontradas podem ser visualizadas com o comando `john -show`.

John pode ser interrompido (^C) e depois retomado com `john -restore`, continuando de onde havia parado.

Atividade

Antes de começar:

- Nos terminais do DINF, John está instalado no diretório `/home/soft/john`. Para incluí-lo em seu caminho de executáveis, use o comando a seguir no *shell*:

  ```
  export PATH=/home/soft/john/bin:${PATH}
  ```

- O diretório `/home/soft/john/wordlist` contém listas de palavras em várias línguas.

Em sala:

1. Analise os arquivos de senhas disponibilizados pelo professor (em password_files.zip).
2. Extraia e quebre o hash de cifragem destes dois arquivos PDF protegidos (dica: use este site para extrair o hash do arquivo PDF):

    - segredo-moleza.pdf
    - segredo-maisoumenos.pdf
    - segredo-pedreira.pdf
3. Identifique um site com tabelas *hash* pré-computadas e tente quebrar alguns dos hashes dos arquivos fornecidos pelo professor. Sugestões:
    - https://crackstation.net
    - http://www.md5this.com
    - https://www.hashkiller.co.uk
    - http://rainbowtables.it64.com

Em casa (opcional):

1. Extraia o arquivo de *hashes* de um sistema Windows, analise sua estrutura e tente quebrar suas senhas. Sugestão: use os programas `pwdump` ou `fgdump`.
2. Identifique ferramentas similares disponíveis na Internet e experimente uma delas com os mesmos arquivos (sugestões: Cain and Abel, HashCat, Ophcrack).