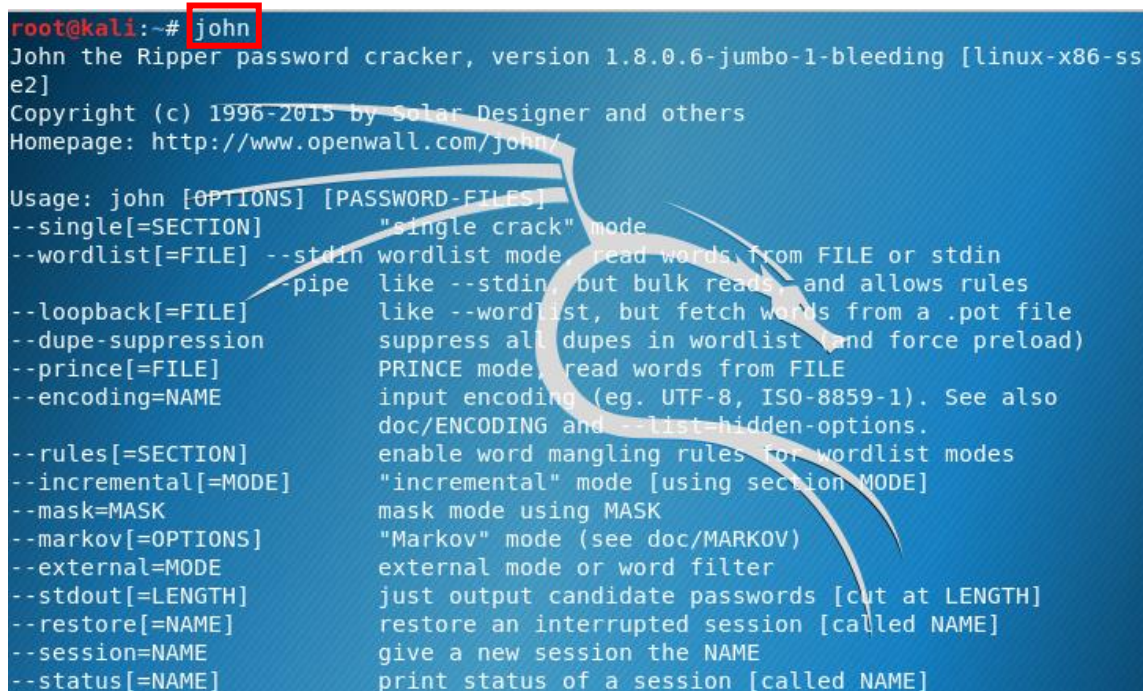


Força Bruta é o ataque que consiste em testar conjuntos de letras, palavras e caracteres, até descobrir uma senha ou uma **hash**. Existem várias maneiras de se realizar o **brute force**. Testando letra por letra, número por número. Você realiza um brute force incremental (baseado em testes) até concluir a verificação. Dependendo do tamanho da senha fica quase impossível quebrar com um computador doméstico com baixo desempenho. Nesse tipo podemos usar também uma **wordlist** (uma lista de palavras). Você também pode utilizar um banco de dados contendo vários **hashs** pré-definidos.

Descobrendo Hashs com o Johnny the Ripper

John the Ripper é um cracker de senha rápido, atualmente disponível para muitos tipos de sistemas Unix, Windows, DOS e OpenVMS. Seu objetivo principal é detectar senhas fracas.

1. Conhecendo o John. Acesse o terminal Kali e digite o comando abaixo:



```
root@kali:~# john
John the Ripper password cracker, version 1.8.0.6-jumbo-1-bleeding [linux-x86-ss
e2]
Copyright (c) 1996-2015 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION]      "single crack" mode
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
--pipe                  like --stdin, but bulk reads, and allows rules
--loopback[=FILE]       like --wordlist, but fetch words from a .pot file
--dupe-suppression      suppress all dupes in wordlist (and force preload)
--prince[=FILE]         PRINCE mode, read words from FILE
--encoding=NAME          input encoding (eg. UTF-8, ISO-8859-1). See also
                        doc/ENCODING and --list-hidden-options.
--rules[=SECTION]       enable word mangling rules for wordlist modes
--incremental[=MODE]    "incremental" mode [using section MODE]
--mask=MASK             mask mode using MASK
--markov[=OPTIONS]      "Markov" mode (see doc/MARKOV)
--external=MODE         external mode or word filter
--stdout[=LENGTH]      just output candidate passwords [cut at LENGTH]
--restore[=NAME]        restore an interrupted session [called NAME]
--session=NAME          give a new session the NAME
--status[=NAME]         print status of a session [called NAME]
```

Observe que ele te da todas as opções que você tem com a ferramenta.

2. Para realizar o ataque precisamos criar um arquivo de senhas. (Será utilizado para criptografar senhas;



```
root@kali:~# nano md5.php
```

3. Você precisará editar nesse arquivo um código PHP, para guardar a variável senha;

```
GNU nano 2.9.1

<?php
$senha = '12345';
echo md5($senha);
?>
```

O parâmetro \$Senha (é uma variável que guarda as senhas. Echo md5 escreverá a variável na tela. O MD5 é o algoritmo de criptografia. Nosso Objetivo será transformar essa senha “12345” em hash e solicitar que o John quebre.

4. Vamos executar o comando abaixo para exibir a hash MD5 que está contida no arquivo md5.php;

```
root@kali:~# php md5.php
827ccb0eea8a706c4c34a16891f84e7broot@kali:~#
```

5. Podemos copiar o hash gerado. Mas vamos fazer melhor, guardaremos dentro de um arquivo;

```
827ccb0eea8a706c4c34a16891f84e7broot@kali:~# php md5.php > senha.txt
```

6. Agora vamos dizer ao John para quebrar o hash criado (contido no arquivo senha.txt.). Vamos ajudar o John dizendo que nossa senha utiliza a criptografia MD5.

```
root@kali:~# john senha.txt --format=raw-md5
Using default input encoding: utf-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
12345(?)
1g 0:00:00 DONE 2/3 (2019-02-20 12:23) 14.28g/s 171.4p/s 171.4c/s 171.4C/s 12
3456..qwerty
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

A senha será exibida pelo John.

Observação o John tem dentro do banco de dados dele um Wordlist. Com várias combinações de senha, e a senha da nossa prática foi uma senha relativamente fraca.

Quebrando Hashs no Johnny the Ripper com Wordlist

1. Vamos primeiro modificar a senha no arquivo md5.php.

```
root@kali:~# nano md5.php
```

2. Insira uma nova senha: 123@Doc;

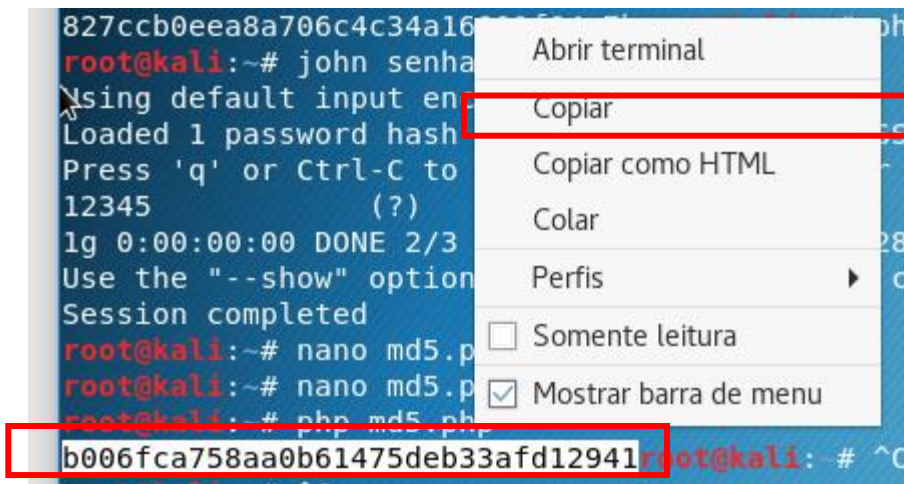
```
<?php
$senha = '123@Doc';
echo md5($senha);
?>
```

3. Vamos gerar o hash;

```
root@kali:~# php md5.php
b006fca758aa0b61475deb33afd12941root@kali:~#
```

4. Copiar e cola a hash no arquivo de senha;

```
827ccb0eea8a706c4c34a16
root@kali:~# john senha
Using default input enc
Loaded 1 password hash
Press 'q' or Ctrl-C to
12345             (?)
lg 0:00:00:00 DONE 2/3
Use the "--show" option
Session completed
root@kali:~# nano md5.p
root@kali:~# nano md5.p
root@kali:~# php md5.ph
b006fca758aa0b61475deb33afd12941root@kali:~# ^C
```



```
root@kali:~# nano senha.txt
```

5. Ao abrir o arquivo senha.txt cole o conteúdo.

```
GNU nano 2.9.1
827ccb0eea8a706c4c34a16891f84e7b
b006fca758aa0b61475deb33afd12941
```


6. Agora vamos criar uma Wordlist que vai ajudar o John a quebrar a senha. Como é um teste vamos colocar a própria senha no Wordlist. Uma dica você pode usar Wordlists prontas para realizar determinado ataque. **Posso colocar qualquer informação na Wordlist.**

```
root@kali:~# nano wordlist.txt
```

```
GNU nano 2.9.1
123@Doc
```

7. Insira o parâmetro de quebra de senha do Wordlist, ele vai quebrar os dois “hash” contidos no arquivo senhas.txt.

```
root@kali:~# john senha.txt --format=raw-md5 --wordlist=wordlist.txt
```

```
root@kali:~# john senha.txt --format=raw-md5 --wordlist=wordlist.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
123@Doc (?)
lg 0:00:00:00 DONE (2019-02-20 13:02) 5.000g/s 5.000p/s 5.000c/s 5.000C/s 123@Doc
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Desafio 01

Todo Linux guarda as senhas dos usuários no diretório **/etc/shadow** o super usuário Root usa hash 256 bit. Você só consegue pegar qualquer arquivo de senha se você estiver logado como root.

Usando o comando **unshadow /etc/passwd /etc/shadow > users.txt**

Você transfere todos os usuários e senha para o arquivo **users.txt**

Sua missão!

Descobrir a senha de Root!

Etapas Documentada! (Deverá conter print das etapas executadas) informando os itens abaixo:

- O que é a Função Hash;
- Pequeno descritivo sobre o JTR (Johnny The Ripper).
- Referencias.

