Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

John the Ripper

Vamos começar a usar o John the Ripper em 2 etapas para quebrar uma senha. Primeiro ele usará o arquivo **passwd** e **shadow** para criar um arquivo de saída. Em seguida, você realmente usa ataque de dicionário contra esse arquivo para decifrá-lo. Ou seja, John the Ripper usará os dois arquivos a seguir:

/etc/passwd

/etc/shadow

No Linux, o hash da senha é armazenado no arquivo */etc/shadow*. Para o bem deste exercício, vou criar um novo usuário john nomes e atribuir uma senha simples "123456 para ele.

```
root@kali:~# useradd -m john -G sudo -s /bin/bash

root@kali:~# passwd john

Enter new UNIX password: <password>

Retype new UNIX password: <password>

passwd: password updated successfully
```

Agora que nós criamos a nossa vítima, vamos começar com comandos unshadow. O comando unshadow combinará os as tentativas de */etc/passwd* e */etc/shadow* para criar um arquivo com detalhes de nome de usuário e senha. Quando você simplesmente digitar unshadow, ele mostra o uso de qualquer maneira.

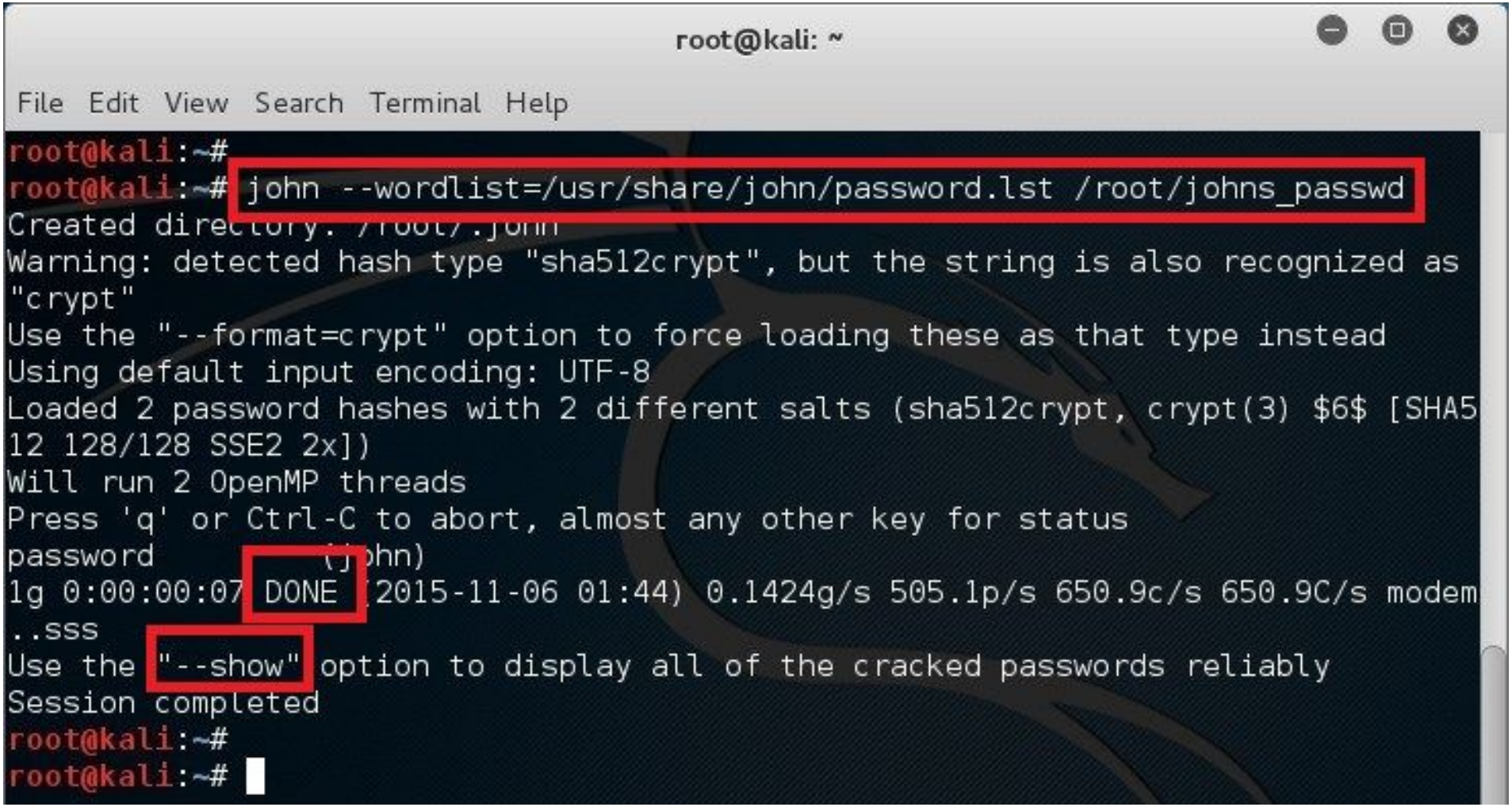
```
# unshadow
Usage: unshadow PASSWORD-FILE SHADOW-FILE
# unshadow /etc/passwd /etc/shadow > /root/johns_passwd
```

Neste ponto, só precisamos de um arquivo de dicionário para continuar com o cracking. O John vem com o seu próprio arquivo de senha pequeno e ele pode ser localizado em /usr/share/john/password.lst. Mostrei o tamanho desse arquivo usando o seguinte comando.

```
# ls -ltrah /usr/share/john/password.lst
```

Você pode usar suas próprias listas de senha também ou fazer o download na Internet (há muitos arquivos de dicionário em tamanho de terabyte!).

John the Ripper



John the Ripper

```
# john --wordlist=/usr/share/john/password.lst /root/johns_passwd
```

Parece que funcionou. Portanto, agora podemos usar a opção john --*show* para listar senhas hackeadas. Observe que é uma senha simples que existia no dicionário, portanto funcionou. Se não fosse uma senha simples, então você precisaria de um dicionário muito maior e muito mais tempo para quebrá-lo.

```
# john --show /root/johns_passwd
```