Exercício 1f - Ataque nos hashes vazados

Objetivo: Procurar por senhas fracas utilizando o John the Ripper e realizar *backup* das configurações do sistema de maneira segura.

Cenário inicial: Os endereços das interfaces físicas já estão configurados.

O John the Ripper é uma ferramenta de força bruta que quebra senhas baseado em hashes. Quando a senha de um usuário é fraca, mal elaborada ou estiver contida em uma WordList, ela será facilmente quebrada por essa ferramenta.

Entre no equipamento **KaliLinux**
login: ceptro
senha: ceptro
Abra o Terminal do KaliLinux **Terminal Emulator**

Parte 1 - Configurações necessárias para usar John the Ripper

1. O primeiro passo é criar usuário com uma senha fraca para ser quebrada depois. Crie dois usuários no **KaliLinux**, um usuário chamado **maria** com a senha **123456** e outro chamado **edu** com a senha **abc123**

```
#sudo adduser maria

Adding new group `maria' (1002) ...
Adding new user `maria' (1002) with group `maria' ...
Creating home directory `/home/maria' ...
Copying files from `/etc/skel' ...
New password: 123456
Retype new password: 123456
passwd: password updated successfully
Changing the user information for maria
Enter the new value, or press ENTER for the default
      Full Name []: [Enter]
      Room Number []: [Enter]
      Work Phone []: [Enter]
      Home Phone []: [Enter]
      Other []: [Enter]
Is the information correct? [Y/n] y
```

```
#sudo adduser edu

Adding new group `edu' (1003) ...
Adding new user `edu' (1003) with group `edu' ...
Creating home directory `/home/edu' ...
Copying files from `/etc/skel' ...
New password: abc123
Retype new password: abc123
passwd: password updated successfully
Changing the user information for edu
Enter the new value, or press ENTER for the default
      Full Name []: [Enter]
      Room Number []: [Enter]
      Work Phone []: [Enter]
      Home Phone []: [Enter]
      Other []: [Enter]
Is the information correct? [Y/n] y
```

2. Em sistemas linux, o arquivo /etc/shadow armazena as senhas de todos os usuários em formato de hash. Visualize o arquivo com o comando a seguir:

```
#sudo cat /etc/shadow
```

3. Já o arquivo /etc/passwd, armazena as informações básicas sobre os usuário no sistema (dados pessoais como nome completo e telefone). Visualize o arquivo com o comando a seguir:

```
#sudo cat /etc/passwd
```

4. Agora, precisamos fazer uma cópia do arquivo /etc/shadow e do /etc/passwd combinando-os em um único arquivo usando o comando unshadow:

```
#sudo unshadow /etc/passwd /etc/shadow > quebrahash.txt
```

5. Para quebrar as senhas fracas, vamos utilizar a WordList do próprio John the Ripper, que contém um pouco mais de 3500 de palavras pequenas para quebrar os hashes. Utilize o seguinte comando:

```
#sudo john --format=crypt --wordlist=/usr/share/john/password.lst
quebrahash.txt

Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt
6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
abc123       (edu)
123456       (maria)
2g 0:00:00:24 DONE (2023-09-04 17:46) 0.08220g/s 145.7p/s 153.6c/s 153.6C/s !@#$%..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

6. Para visualizar todos os hashes quebrados pelo John the Ripper, utilize o seguinte comando:

```
#sudo john --show quebrahash.txt

maria:123456:1001:1001:,,,:/home/maria:/bin/bash
edu:abc123:1002:1002:,,,:/home/edu:/bin/bash

2 password hashes cracked, 0 left
```

Parte 2 - Configuração no **MikrotikClientes**.

1. É uma boa recomendação manter sempre um *backup* atualizado das configurações atuais dos seus equipamentos.

2. Acesse o **MikrotikClientes** usando a credencial admin.

```
MikroTik Login: admin
Password: SenhaAdmin
```

3. Para fazer um *backup* das configurações do equipamento, você pode utilizar os comandos /export e /system backup.

4. O comando /export gera um arquivo de *backup* do tipo (.rsc) com as configurações do equipamento e o salva em texto plano. Ele não possui informações físicas do equipamento,

como, por exemplo, o endereço MAC das interfaces e também não possui as informações de usuários. Para gerar o arquivo (.rsc) de *backup* utilize o seguinte comando:

```
/export file=configuracao
```

5. O comando /system backup gera um arquivo de *backup* do tipo (.backup). Esse arquivo é um binário e contém todas as configurações do equipamento, incluindo as informações físicas. Para gerar o arquivo (.backup) de *backup* utilize o seguinte comando:

```
/system backup save name=configuracaoHash password=BackupSenha
```

6. Liste os dois arquivos no roteador.

```
/file print
```

7. Você deve guardar o *backup* numa máquina segura, pois as informações dos seus equipamentos estão nessa máquina e hashes de senhas podem ser quebrados, como acabamos de ver na experienciar anterior.

8. Acesse o **Cliente_Domestico**
   login: root
   senha: toor
9. Abra o terminal **Termit**
10. Agora, precisamos pegar o *backup* do equipamento de maneira segura. Para isso, podemos usar o SCP ou SFTP, ambos protocolos utilizam criptografia para proteger os dados durante o processo de transferência.

11. É importante lembrar que precisamos tomar cuidado com a permissão do seu usuário ao usar SFTP (podemos desativar o FTP, mas não podemos retirar a permissão do usuário de usar FTP). Utilize o SFTP para pegar as configurações.

```
#sftp -P 6022 edu@[4d0c:XX:0c00::1]:configuracao.rsc

Enter passphrase for key '/root/.ssh/id_rsa': SenhaClienteDomestico
```

12. Repita o mesmo comando para o segundo arquivo de *Backup*.

```
#sftp -P 6022 edu@[4d0c:XX:0c00::1]:configuracaoHash.backup

Enter passphrase for key '/root/.ssh/id_rsa': SenhaClienteDomestico
```

Você conseguiu pegar o arquivo? Qual o motivo para isso acontecer?

13. Tente mais uma vez, mas agora utilizando o usuário admin. Você conseguiu pegar o arquivo?