FUNDAMENTOS BÁSICOS Y HACKING ÉTICO

PRÁCTICA

El objetivo de esta práctica es crear un script (.sh) con bash utilizando diferentes herramientas de footprinting y fingerprinting, además de otras opciones propuestas a continuación.

Máquinas a utilizar:

- Kali Linux (principal)
- Máquina vulnerable: ordenador del puesto del profesor

0. Título del menú:

Se puede utilizar las herramientas figlet o toilet para crear este tipo de títulos.

- Para instalarlas (actualiza los repositorios antes): `sudo apt install toilet figlet`
- Para ver las fuentes: `/usr/share/figlet`
- Para ver las opciones que ofrecen las herramientas, usa `man figlet` o `man toilet`. La herramienta toilet ofrece más opciones.

Ejemplos:

Llamada simple:

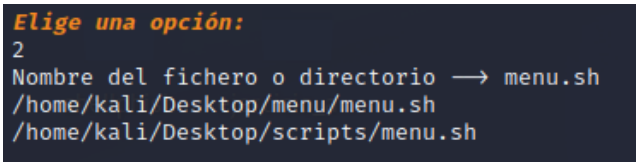
```
figlet -c Menu  --> justificado

figlet -f tipo_fuente -c Menu

toilet -f future Menu

toilet --metal -f script Hola
```

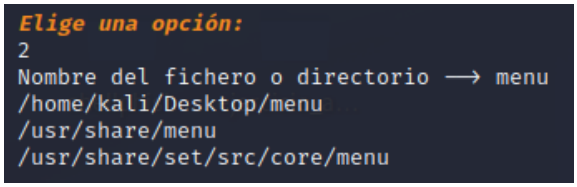
1. Saludar

Implementa esta opción de manera que crees un saludo original.

2. Buscador de ficheros o directorios

Indicando el nombre (parcial o completo) del fichero o directorio, que muestre la(s) ruta(s) donde se encuentran. Sólo debe indicar la ruta, evitando otra información ("*Permission denied*", por ejemplo).





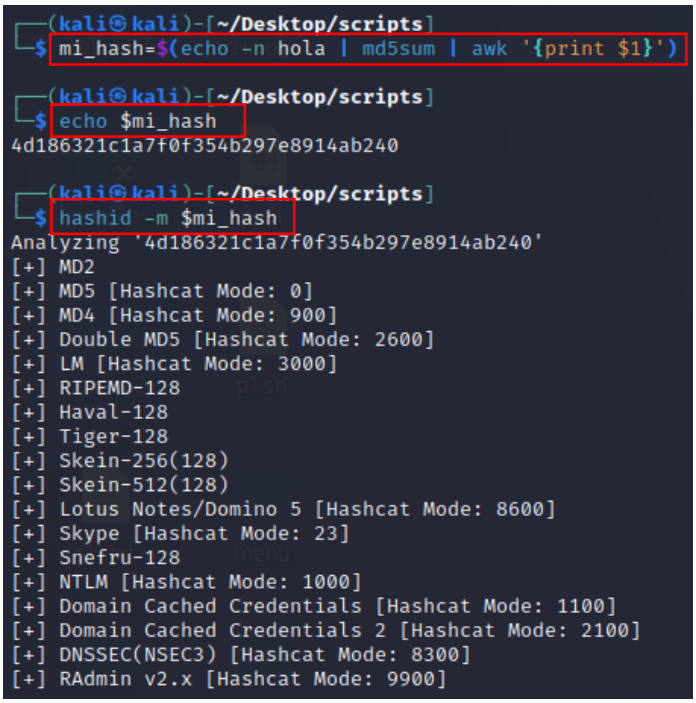
EXTRA-1: añade más opciones en este buscador. Para ello puedes usar otras opciones y/o comandos: find, wheris, locate, which…

3. Ataque de diccionario

Para esta opción se propone utilizar la herramienta **John the Ripper**.

a) Debe pedir por pantalla un **hash**
b) **Identificar el algoritm**o con el que está cifrada la contraseña → mostrar resultado de ejecución de **hashid** para que después el usuario elija el algoritmo (*format*):

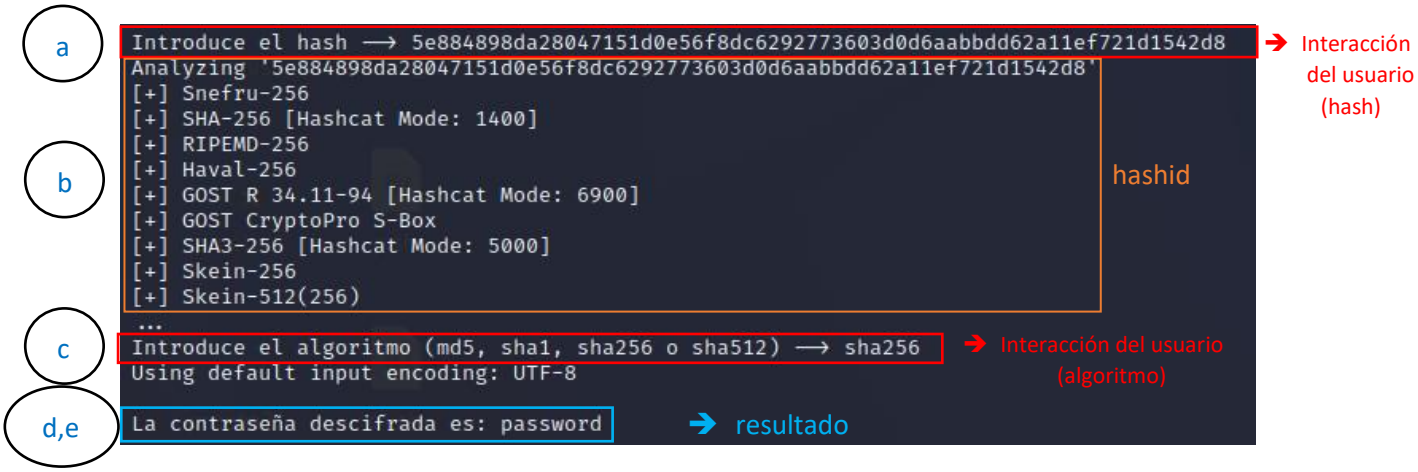
```
hashid -m <hash>
```



c) A continuación, pide por pantalla el algoritmo que utilice john para realizar el ataque. El hash debe guardarse en un archivo de texto.
d) Realiza el ataque con john, eligiendo por defecto un diccionario con la opción

```
--wordlist=/usr/share/john/password.lst
```

e) Mostrar contraseña y eliminar fichero que se ha utilizado para guardar el hash (necesario para utilizar la herramienta John the Ripper)



Notas:

- El procedimiento para realizar un ataque de diccionario con John the Ripper es el siguiente:

```
john --wordlist=<diccionario> --format=<algoritmo> <fichero_del_hash>
john --show <fichero_del_hash> --format=<algoritmo>
```

- Para simplificar y evitar tener que tratar con muchos algoritmos de cifrado, céntrate en el uso de los siguientes:

Algoritmo	Comando para obtener el hash	--format=<algoritmo>
MD5	md5sum	Raw-md5
SHA-1	sha1sum	Raw-sha1
SHA-256	sha256sum	Raw-sha256
SHA-512	sha512sum	Raw-sha512

En el ejemplo se indica “sha256”, pero en el script se usa `--format=Raw-sha256`

- Ejemplo para obtener un hash (para hacer pruebas):

```
echo -n hola | md5sum | awk '{print $1}'
```

- **Diccionarios**: puedes elegir el diccionario con el que realizar el ataque con la opción `--wordlist`, indicando la ruta absoluta o copiando el fichero correspondiente a misma ruta (u otra) donde se encuentra el script.

EXTRA-1: añade opción de comprobar que se ha escrito bien el algoritmo (punto c) que se elija al realizar el ataque con **john**:

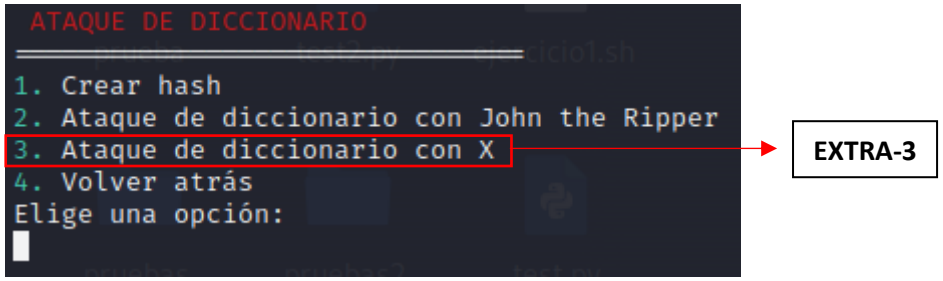
```
Introduce el algoritmo (md5, sha1, sha256 o sha512) ⟶ a
Opción incorrecta. Vuelve a intentarlo
Introduce el algoritmo (md5, sha1, sha256 o sha512) ⟶ sha123
Opción incorrecta. Vuelve a intentarlo
Introduce el algoritmo (md5, sha1, sha256 o sha512) ⟶ md5
```

EXTRA-2: añade la opción de que el usuario pueda elegir un diccionario con el que realizar el ataque (entre el punto c y el punto d):

- Archivo **password.lst** ubicado en /usr/share/john
- Archivo **rockyou.txt** (inicialmente comprimido, puedes descomprimirlo donde quieras)
- **Otro** que elijas o descargues

EXTRA-3: añade otra opción para este punto → Realiza lo mismo, pero con **otra herramienta, y propón un menú con diferentes opciones para el usuario**.

Nota: también puedes añadir la opción de descifrar las contraseñas de otros archivos (zip, 7z, pdf…)



4. Fingerprinting

Realiza un proceso de **fingerprinting** con la herramienta **nmap** a la máquina vulnerable.

- Debe elegirse la IP objetivo
- Para realizar el escaneo, añade 4 parámetros del *cheat sheet* de nmap
- El resultado debe guardarse en un fichero, mostrando sólo la información relevante, quitando todo lo demás (puedes usar ***grep*** para ello, por ejemplo):

```
Puertos abiertos de la IP: 172.20.223.110
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
```

EXTRA-1: empleando OpenVas escaena la máquina objetivo y encuentra sus vulnerabilidades.

5. Footprinting

Realiza un proceso de footprinting con la herramienta **exiftool**. En clase se habrá explicado o se explicará para qué se utiliza: es una herramienta para obtener o editar los metadatos de directorios o ficheros.
Para realizar esta parte de la práctica es necesario instalar dicha herramienta:

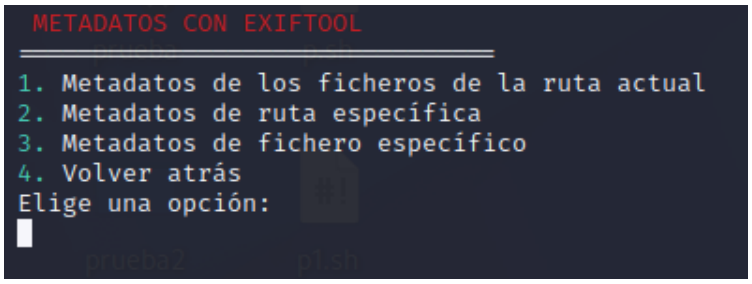
```
sudo apt install libimage-exiftool-perl
```

La sintaxis básica de exiftool es la siguiente:

```
exiftool <ruta>
exiftool <fichero>
exiftool <ruta/fichero>
```

Con esta herramienta, **el script debe ofrecer las siguientes opciones**:

- Metadatos de los ficheros de la ruta actual
- Metadatos de una ruta específica que indique el usuario
- Metadatos de un fichero específico indicado por el usuario



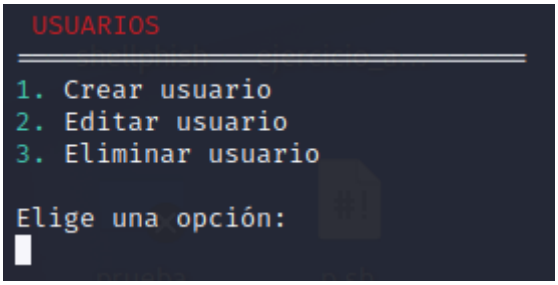
EXTRA-1: implementa la opción para editar los metadatos con exiftool. Para ello, añade las opciones que consideres en el menú anterior.

EXTRA-2: añade al menú **The Harvester** como otra herramienta de footprinting (sin un menú propio)

6. Gestión de usuarios

Desde esta opción el script nos tiene que ofrecer lo siguiente:

- Crear usuario: que pida nombre de usuario y contraseña
- Editar usuario: nombre, contraseña, shell…
- Eliminar usuario: indicando el nombre de usario



Utiliza los comandos que se han visto en clase: **useradd, usermod, userdel**

Los cambios deben verse reflejados en los archivos:

- **/etc/passwd**
- **/etc/shadow**
- **/etc/group**

Nota: Para mayor comodidad y para evitar problemas edita o elimina usuarios que hayas creado previamente.

EXTRA-1: añade la pregunta "**¿Aceptar? (s/n)**" en las opciones de editar o eliminar usuario. Si el usuario teclea s o S el script procederá con la edición o la eliminación, si no, no.

7. Ataque con metasploit

EXTRA-1: la herramienta metasploit se verá más adelante, pero es una opción extra para poder llegar a obtener la nota máxima.

Implementa esta opción de modo que automatice el uso de metasploit. Para ello se deben solicitar por pantalla varios datos, por ejemplo:

- IP de la víctima (rhosts)
- Exploit: palabra clave para buscar exploits (mysql, apache, samba…) (service)
- Puerto (rport)
- …