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. Dicho script se usará para enumerar vulnerabilidades y buscar posibles brechas de seguridad en una máquina vulnerable. Esa máquina, será configurada por otro alumno de clase y los profesores asignaran a cada alumno una al azar.

Máquinas virtuales a utilizar:

- Kali Linux (principal)
- Metasploitable: para poder realizar alguna prueba (*OPCIONAL*)
- Máquina “adhoc” que os facilitará el compañero.

Configuración de red:

- Red NAT

Creación de la máquina Vulnerable:

La máquina deberá estar basada en un servidor Linux (independientemente de que distro sea) y tendrá un mínimo de 5 vulnerabilidades y un máximo de 8 (bien sean servicios obsoletos o software que ya traigan esas vulnerabilidades).

La máquina, al arrancarla, no podrá mostrar la IP que tiene, aunque la obtendrá por DHCP.

El usuario root deberá estar habilitado con una contraseña oculta en algún fichero. Ese fichero deberá tener la palabra clave *password*. En este fichero la contraseña debe estar cifrada con el algoritmo que se elija (que no sea imposible pero que tampoco sea el más común).

Para la obtención de la contraseña de root, primero se deberá encontrar el usuario y password de la máquina, que deberán ser "típicos". Esto es así, para que se pueda obtener acceso mediante el script que creareis y algún diccionario básico.

El usuario root deberá tener un flag.txt donde se podrá dejar el mensaje que se desee…siempre que no ofenda a más de 3 colectivos.

****Ejemplo de vulnerabilidad: un puerto 22 habilitado para ssh con user admin y Password admin*

Archivos de logs

La máquina vulnerable debe guardar dos archivos de logs: uno de Nginx y otro de Apache. Ambos tienen que tener 120 líneas como mínimo y recoger actividades sospechosas. Estos archivos servirán para completar el punto 2 del script.

Aplicación web vulnerable

La máquina vulnerable debe tener instalada una aplicación web vulnerable (o varias). Esta aplicación puede ser una de las que se listan a continuación u otra similar:

- Juice Shop
- WebGoat
- Multillidae
- DVWA

Script:

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. Análisis de logs

En la máquina vulnerable debe de haber algún log (Apache, Nginx) que haya registrado actividades de diferentes direcciones IP.
El script debe estar preparado para analizar el **archivo de logs de Nginx** para buscar actividades sospechosas y sacar un informe.

Ejemplo de resultados posibles :

- Direcciones IP que han intentado realizar solicitudes a horas poco habituales
- Direcciones IP que han realizado intentos de acceso repetido a recursos inexistentes
- Direcciones IP que realizan un número elevado de solicitudes en un periodo corto (muchas en pocos segundos, seguidas)
- Accesos a directorios restringidos o sensibles: direcciones IP que intentan acceder a directorios como /etc/passwd, /var/, o /proc/…
- …

EXTRA-1: añade la opción de realizar un informe de análisis de actividades sospechosas del **archivo de logs de Apache**.

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>
```

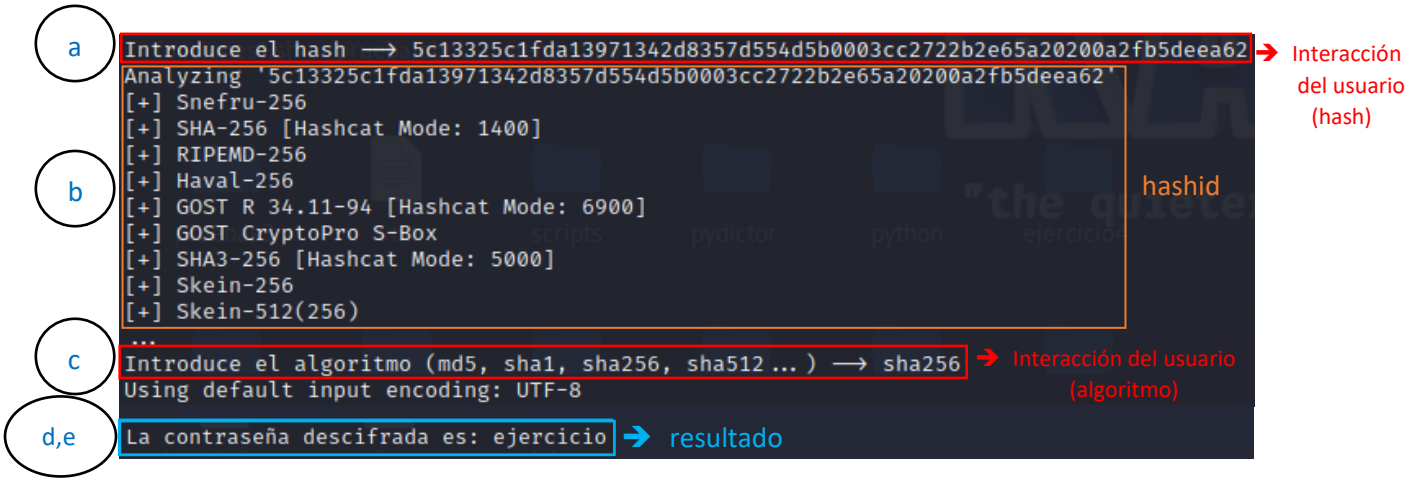
```
┌──(kali㉿kali)-[~/Desktop/scripts]
└─$ mi_hash=$(echo -n hola | md5sum | awk '{print $1}')

┌──(kali㉿kali)-[~/Desktop/scripts]
└─$ echo $mi_hash
4d186321c1a7f0f354b297e8914ab240

┌──(kali㉿kali)-[~/Desktop/scripts]
└─$ hashid -m $mi_hash
Analyzing '4d186321c1a7f0f354b297e8914ab240'
[+] MD2
[+] MD5 [Hashcat Mode: 0]
[+] MD4 [Hashcat Mode: 900]
[+] Double MD5 [Hashcat Mode: 2600]
[+] LM [Hashcat Mode: 3000]
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5 [Hashcat Mode: 8600]
[+] Skype [Hashcat Mode: 23]
[+] Snefru-128
[+] NTLM [Hashcat Mode: 1000]
[+] Domain Cached Credentials [Hashcat Mode: 1100]
[+] Domain Cached Credentials 2 [Hashcat Mode: 2100]
[+] DNSSEC(NSEC3) [Hashcat Mode: 8300]
[+] RAdmin v2.x [Hashcat Mode: 9900]
```

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>
```

- **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, sha512 ... ) ⟶ a
Opción incorrecta. Vuelve a intentarlo
Introduce el algoritmo (md5, sha1, sha256, sha512 ... ) ⟶ sha123
Opción incorrecta. Vuelve a intentarlo
Introduce el algoritmo (md5, sha1, sha256, 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 **Hashcat**. Por lo tanto, se debe crear un menú que ofrezca utilizar John the Ripper o Hashcat:

```
ATAQUE DE DICCIONARIO
1. Crear hash
2. Ataque de diccionario con John the Ripper
3. Ataque de diccionario con Hashcat
4. Volver atrás
Elige una opción:
```

4. Fingerprinting

Realiza un proceso de **fingerprinting** con la herramienta **fping**.

- Debe elegirse la red.
- El escaneo podrá tener atributos adicionales.
- El resultado se muestra en pantalla.
- Debe encontrar a la máquina Target.

Realiza un proceso de **fingerprinting** con la herramienta **nmap**.

- Debe elegirse la IP objetivo, encontrada previamente con **fping**.
- El escaneo será simple, sin opciones adicionales
- 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
```

EXTRA-1: que guarde los servicios y los puertos abiertos de la víctima en un fichero cuyo nombre sea su IP:

172.20.131.110.txt
188.130.225.41.txt
…

EXTRA-2: que se puedan lanzar scripts.

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:

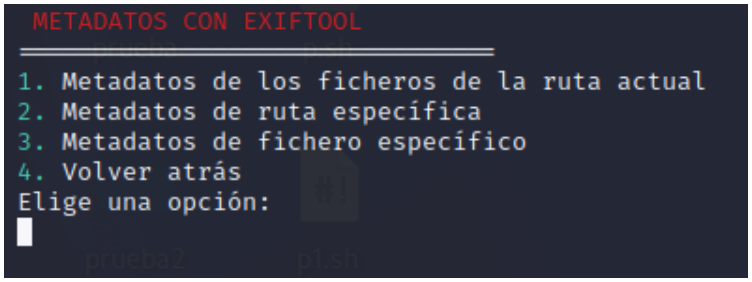
```
sudo apt install libimage-exiftool-perl
```

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



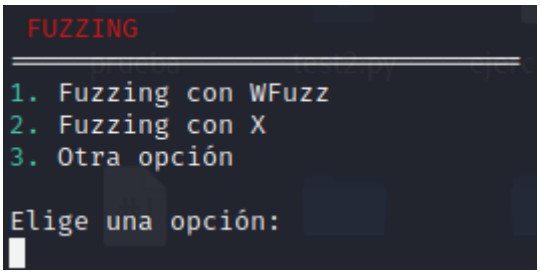
EXTRA-1: implementa la opción para editar los metadatos con exiftool. Para ello, añade las opciones que consideres en el menú anterior.

6. Fuzzing

Esta opción del script debe realizar un análisis de directorios utilizando **Wfuzz**. Se debe de automatizar la búsqueda de directorios ocultos en una URL de un servidor web que tenga instalado la máquina vulnerable objetivo.

Los resultados se deben mostrar por pantalla y guardarlos en un archivo txt.

EXTRA-1: Añade otra opción adicional en el menú del punto 6 para que se pueda utilizar otra herramienta con el mismo fin.



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)
- …