OFFSEC TOOLS

darodrig · dpuente- · juanrodr · acostal-

Cybersec · 42 Madrid

Pequeño compendio de ejercicios relacionados con las redes y la ciberseguridad que te podrían ser útiles en algún momento de la vida. O puede que no.

Contents

Antes de empezar

Requisitos

- Docker
- Init_docker.sh
- Suficiente espacio en disco
- Qué hacer si Docker no arranca en los Mac

Instrucciones

- Si un ejercicio contiene archivos, estos se encontrarán en la propia carpeta del ejercicio.
- Se sugieren ciertas herramientas, pero puedes utilizar cualquier otra.
- Si un ejercicio te resulta muy fácil, puedes ayudar a un compañero.
- Sentido común, Google, RTFM.

Ex00 - Creando el entorno:

Iniciamos docker con init_docker.sh.

Nos situamos en la ruta donde está `docker-compose.yml` Lanzamos los servicios sobre los que trabajaremos:

```
docker-compose up -d
```

Creamos el Dockerfile con las herramientas necesarias:

```
cat << EOF >> Dockerfile
FROM kalilinux/kali-rolling
RUN apt-get update --allow-insecure-repositories && \
    apt-get install -y --allow-unauthenticated \
        john \
        hashcat \
        file \
        wordlists \
        wfuzz \
        nmap \
        dirsearch \
        tcpdump \
        zip
EOF
```

Construimos la imagen y la ejecutamos, enlazando la carpeta actual como un volumen:

```
docker build -t offsec .
docker run \
    -it \
    --mount type=bind,source="$(pwd)",target=/root/offsec \
    offsec
```

Ejercicios

Ex01

¿Están actualizados los servicios? ¿Cuál es la versión más reciente de cada uno de ellos? Averígualo usando `nmap` apuntando a tu IP local.

`Guarda los resultados en un archivo ex01/out.txt.`

Ex02

Utiliza `tcpdump` para generar un archivo .pcap con el tráfico resultante de acceder desde el navegador al wordpress que has lanzado en el primer ejercicio.

`Guarda el resultado en un archivo ex02/out.pcap.`

Ex03

¿Es posible interpretar el tráfico del archivo pcap? Extrae en formato legible el contenido del pcap.

`Guarda los resultados en ex03/out.txt.`

Ex04

Utiliza `dirsearch` para encontrar las urls disponibles en el puerto 8080.

`!! apunta a tu IP local`

`!! puede que haya diccionarios listas de palabras en internet`

`Guarda los resultados en ex04/out.txt.`

Ex05

Intenta identificar qué algoritmo podría dar como resultado estos hashes. Puedes usar hashid, o mejor aún, **Houndsniff**.

```
a1d0c6e83f027327d8461063f4ac58a6
```

```
73475cb40a568e8da8a045ced110137e159f890ac4da883b6b17dc651b3a8049
```

¿Y qué diantres es esto?

```
YTFkMGM2ZTgzZjAyNzMyN2Q4NDYxMDYzZjRhYzU4YTY=
```

```
Guarda los resultados en ex05/out.txt.
```

Ex06

Los archivos data y data2 no tienen extensión. ¿Podrías recuperarla? Encuentra una herramienta para ello.

```
Guarda los resultados en ex06/out.txt.
```

Ex07

- Lee sobre los archivos /etc/passwd y /etc/shadow.
- Crea un archivo que contenga 5 usuarios con sus respectivas contraseñas generadas con el algoritmo MD5. Las contraseñas serán lo suficientemente débiles como para poder hallarlas en un tiempo razonable.

  user:passwd:uid:gid:gecos:home:shell ...
- Averigua el uso de John the Ripper para romper las contraseñas por fuerza bruta.

  ```
  man john
  ```
- Detalla los pasos seguidos en ex07/out.txt

Ex08

Con el comando `zip`, crea un archivo comprimido con contraseña.

```
man zip
```

Ahora busca la forma de hallar la contraseña del zip por fuerza bruta. Utiliza una contraseña breve y predecible por diccionario para tardar menos.

```
man hashcat
```

```
Guarda los resultados en ex06/out.txt.
```

Puedes detener todos los contenedores con

```
docker stop $(docker ps -q)
```

Puedes eliminar todos los contenedores con

```
docker rm $(docker ps -aq)
```

Bonus

Ex09

ctf.hacku.org/register ;)