**DirtyCow提权漏洞复现（CVE-2016-5195）复现**

(By Jean)

目录

[1. 环境部署 2](#_Toc13141)

[2. 漏洞复现 2](#_Toc1264)

[3. 参考 3](#_Toc31447)

# 环境部署

|  |  |  |
| --- | --- | --- |
| **主机** | **操作系统** | **IP** |
| 靶机 | Metasploitable2-Linux | 192.168.180.131 |
|  |  |  |

靶机下载地址：

<https://sourceforge.net/projects/metasploitable/>

# 漏洞复现

该漏洞影响范围：

影响范围： Linux kernel >= 2.6.22（2007年发行，到今年10月18日才修复）

即低于以下内核版本均存在该漏洞：

Centos7 /RHEL7 3.10.0-327.36.3.el7

Cetnos6/RHEL6 2.6.32-642.6.2.el6

Ubuntu 16.10 4.8.0-26.28

Ubuntu 16.04 4.4.0-45.66

Ubuntu 14.04 3.13.0-100.147

Debian 8 3.16.36-1+deb8u2

Debian 7 3.2.82-1

靶机新建test用户：

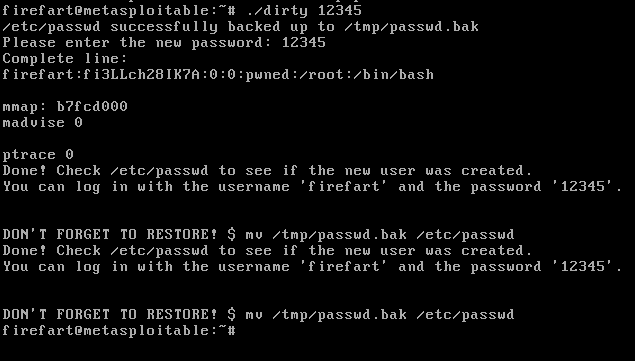
useradd test

切换到test用户，su test

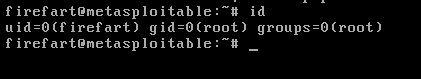
下载漏洞利用程序后，上传到靶机，然后进行编译：

gcc -pthread dirty.c -o dirty -lcrypt

然后执行./dirty 12345



成功获取到一个root权限的用户（此时firefart就是root用户）



# 参考

<https://juejin.cn/post/6844903453420945416>