# W34KN3SS靶机练习实践报告

*下载地址:*

* <https://www.dropbox.com/s/jyzimyvqyghlm14/W34KN3SS.ova?dl=0>
* <https://download.vulnhub.com/w34kn3ss/W34KN3SS.ova>
* <https://download.vulnhub.com/w34kn3ss/W34KN3SS.ova.torrent>     ([Magnet](magnet:?xt=urn:btih:683104ACD4EDD0BD572F17505DE4E8C5C3E43EC1&dn=W34KN3SS.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))

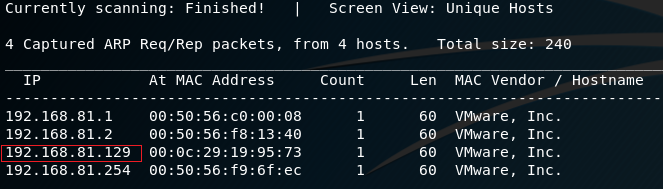
## 安装靶机

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。

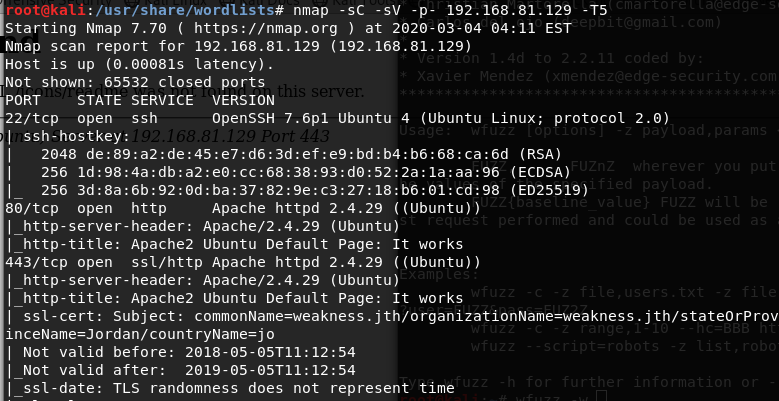
解压ova文件，得到.ovf文件和.vmdk文件，直接用VMWare打开.ovf文件即可。

## 夺旗步骤

首先，IP扫描，端口扫描。

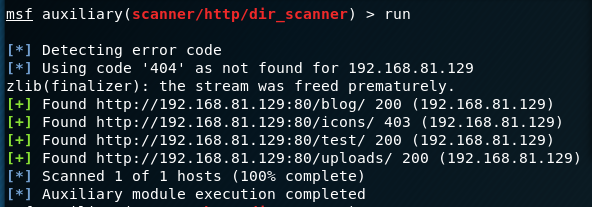


目标靶机的IP地址是192.168.81.129，nmap对该IP进行端口扫描。



该靶机开放三个端口，22、80、443。首先用简单字典爆破ssh，未成功。

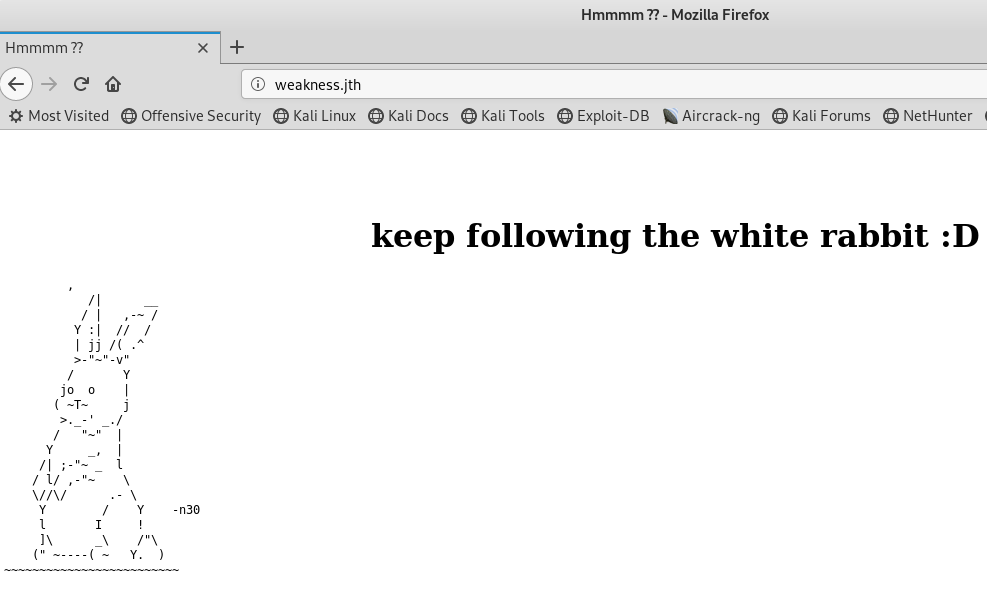
访问80端口和443端口，只有apache配置页面，其余什么都没有。对靶机上的apache服务进行目录扫描。两个端口扫出来的目录差不多，看到http://192.168.81.129:80/uploads/，猜测存在文件上传的地方，但查看源码，查看页面没有任何发现。



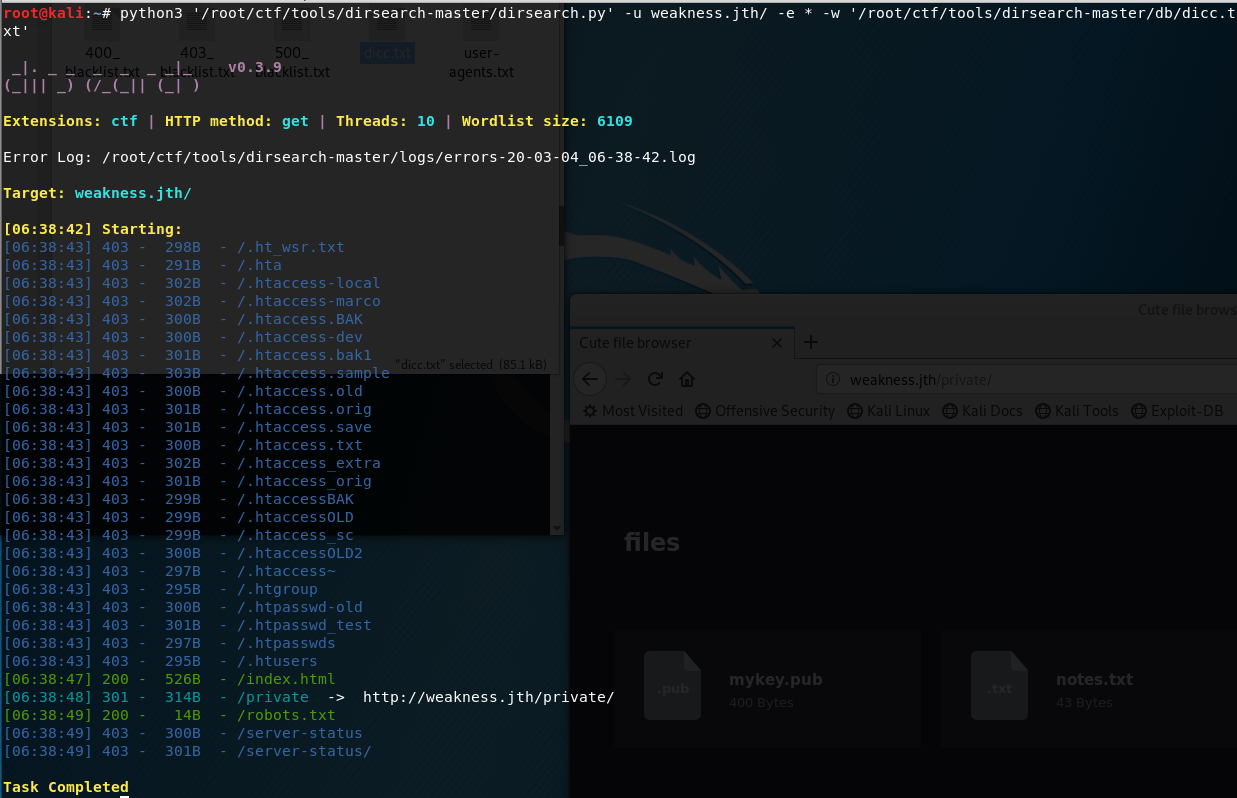
陷入僵局，求助大牛，才知道443端口下的ssl-cert信息非常关键，它表示数字证书相关信息。

|  |  |
| --- | --- |
| **字段名** | **字段值** |
| 公用名称  (Common Name) | 简称：CN 字段，对于 SSL 证书，一般为网站域名；而对于代码签名证书则为申请单位名称；而对于客户端证书则为证书申请者的姓名； |
| 单位名称  (Organization Name) | 简称：O 字段，对于 SSL 证书，一般为网站域名；而对于代码签名证书则为申请单位名称；而对于客户端单位证书则为证书申请者所在单位名称； |

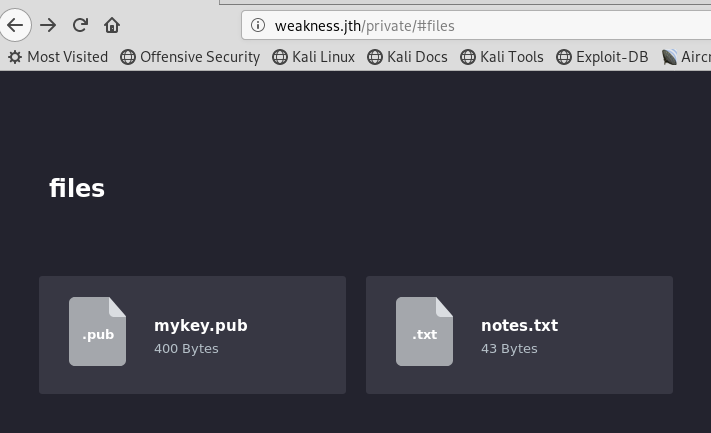
好像发现了一个域名weakness.jth，看名字就知道要访问它。



网站什么都没有，只有一只名为n30的兔子和一句话。继续进行目录扫描，发现三个可访问地址，逐个查看。

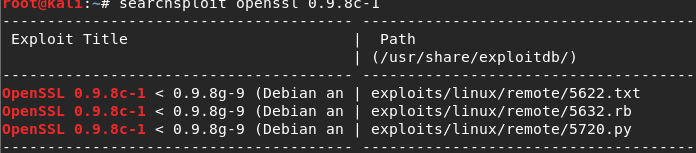


只有http://weakness.jth/private/有内容。



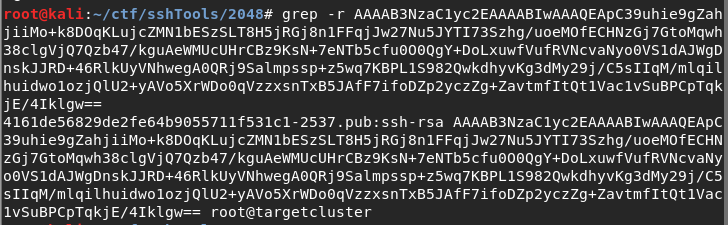
再次查看，告诉我们公钥信息，还有ssh的版本信息。难道是利用ssh的漏洞，通过公钥就能登陆靶机?马上使用kali自带的auxiliary/scanner/ssh/ssh\_log\_publickey进行利用，失败。

在漏洞中查查历史漏洞利用情况，发现5720.py可用，利用公钥文件可用爆破出私钥文件。

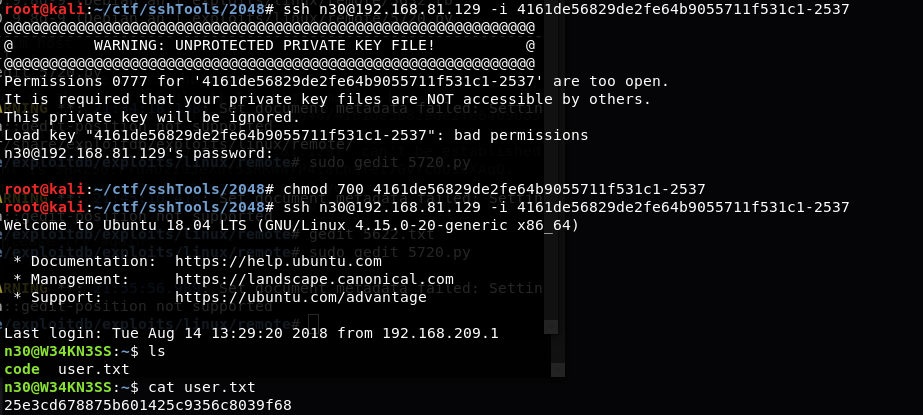


根据文件的提示下载

https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/5622.tar.bz2 ，解压缩后，原来文件夹内是用于爆破的公私钥对。既然我们有公钥，那么在文件夹内搜索mykey.pub的内容，发现目标私钥文件。

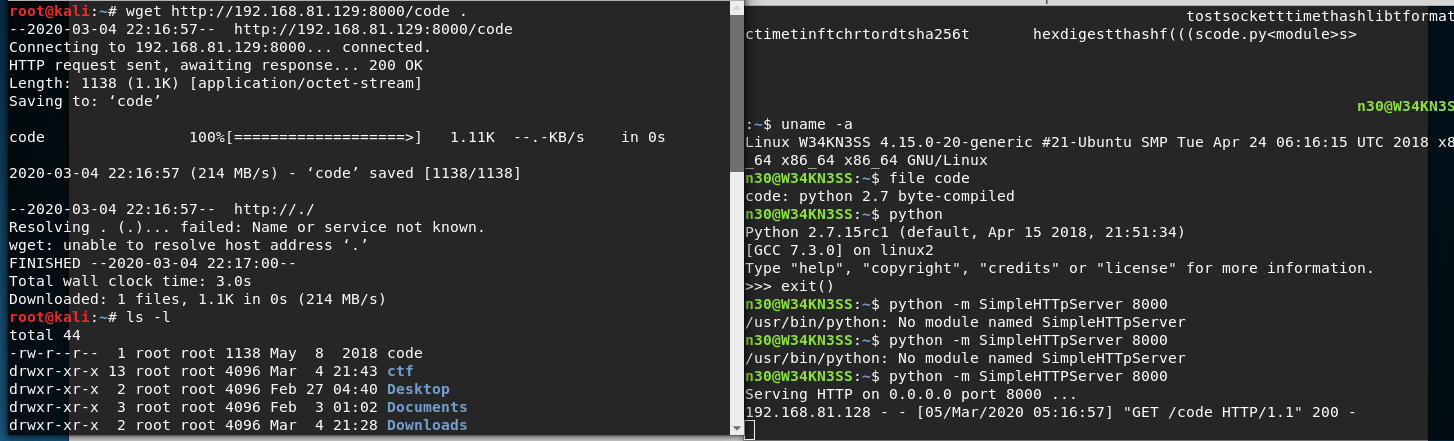


然后利用私钥登陆，当用户名设置未root时，一直提示失败，用户名应该是什么呢？灵光一现，兔子的名字时n30,试试，竟然成功了。期间需要根据提示修改私钥文件的权限属性为”0700”。

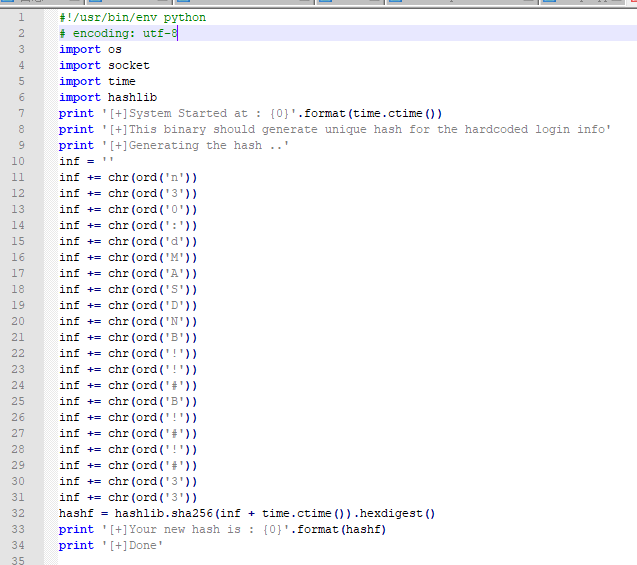


拿到一个flag，但是作者要求我们拿到root权限。查看目录下另一个文件code,用file查看code的文件类型。

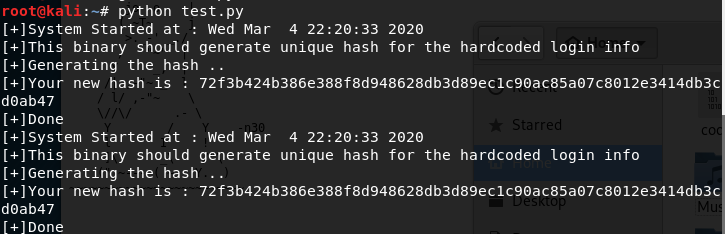
发现code时pyc文件，将该文件下载到本地后，反编译查看。



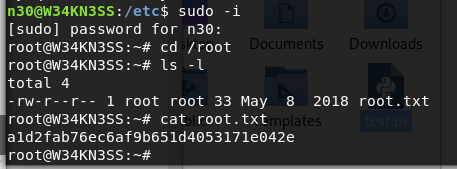
反编译后源码是:



执行得到一串hash。看到hash立刻就想到了linux登陆凭证。本人走了个岔路，对hash进行爆破...直接在代码中就能拿到”n30:dMASDNB!!#B!#!#33”,n30用户的口令是”dMASDNB!!#B!#!#33”。



登陆后在/root/root.txt取得flag即完成攻击练习。



## 总结

1. 首次遇到HTTPS的相关题型，主要关注SSL-CERT内的域名内容。
2. Kali自带的ssl\_login\_publickey不好用，工具要结合这searchsploit使用。