# GoldenEye-v1靶机练习实践报告

*下载地址:*

*<https://drive.google.com/open?id=1M7mMdSMHHpiFKW3JLqq8boNrI95Nv4tq>*

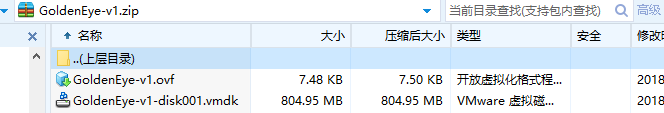
*<https://download.vulnhub.com/goldeneye/GoldenEye-v1.ova>*

*<https://download.vulnhub.com/goldeneye/GoldenEye-v1.ova.torrent>     ([Magnet](magnet:?xt=urn:btih:74335FA5992A98DD607AEFEB05F335CB2A62E9E2&dn=GoldenEye-v1.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))*

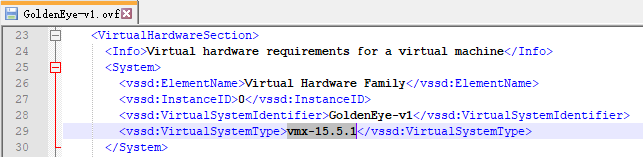
## 安装靶机

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。



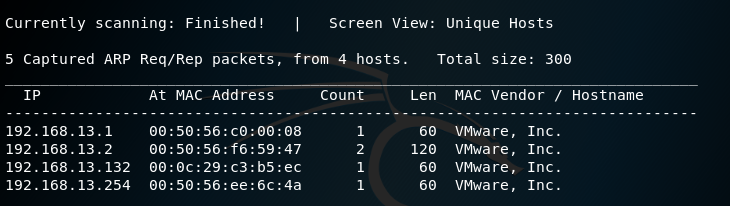
用记事本打开.ovf文件并修改“<vssd:VirtualSystemType>”为自己的VMWare版本，此处我用的是是vmx-15.5.1。

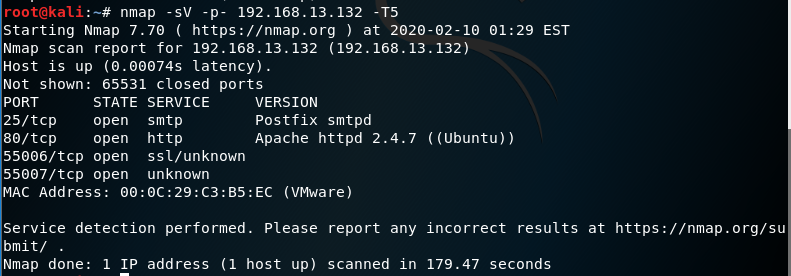


打开靶机后，用nmap工具竟然扫不到ip,排查下来该靶机默认网络连接方式是“主机模式”，修改为“NAT模式”即可。

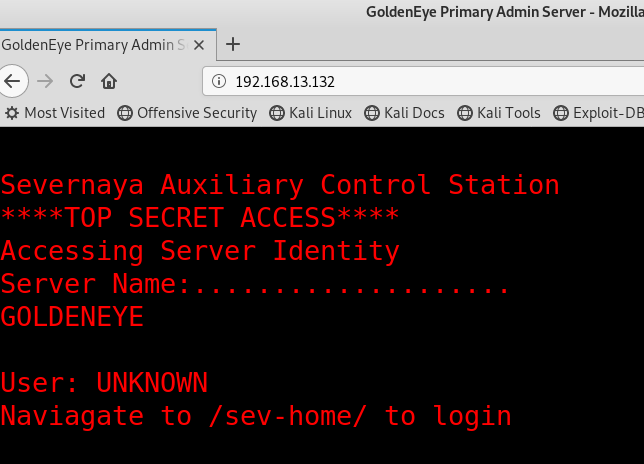
## 夺旗步骤

第一步：IP扫描，端口扫描

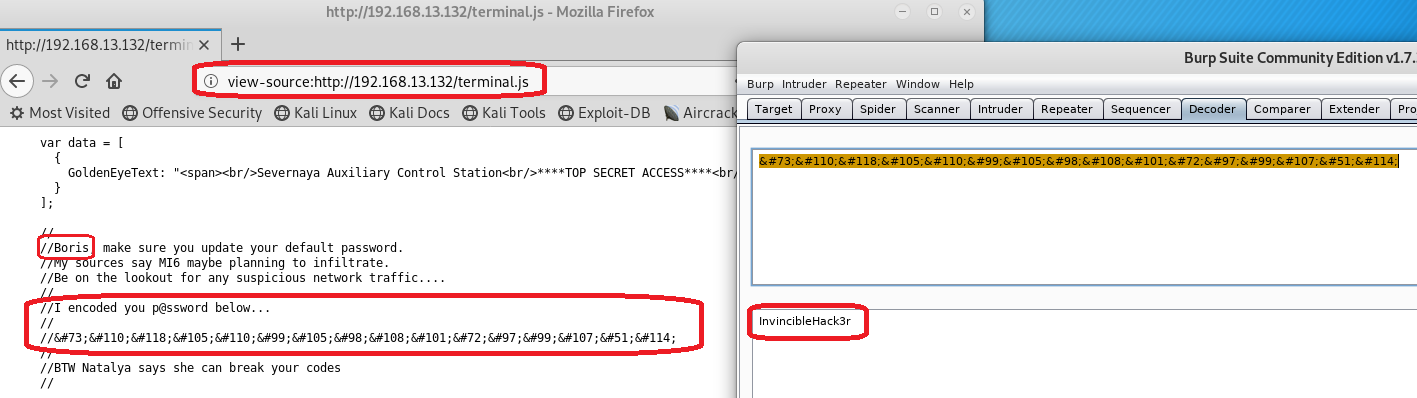




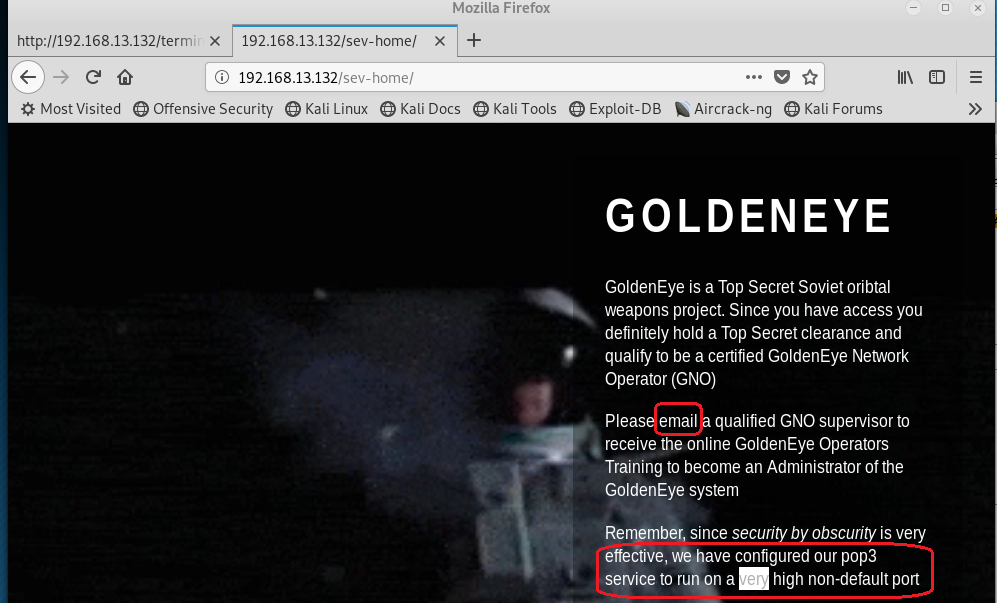
我们看到该靶机的80端口打开，因此在浏览器中访问，提示导航到/sev-home/，导航过去，提示输入用户口令。



没有头绪如何处理就去看源码，果然在terminal.js里面看到了提示，HTML编码的“&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114;”密码解码后是“InvincibleHack3r”，注释中还提到”Boris用默认密码”，这一串密码也不像是默认密码，可能是提示其他地方。



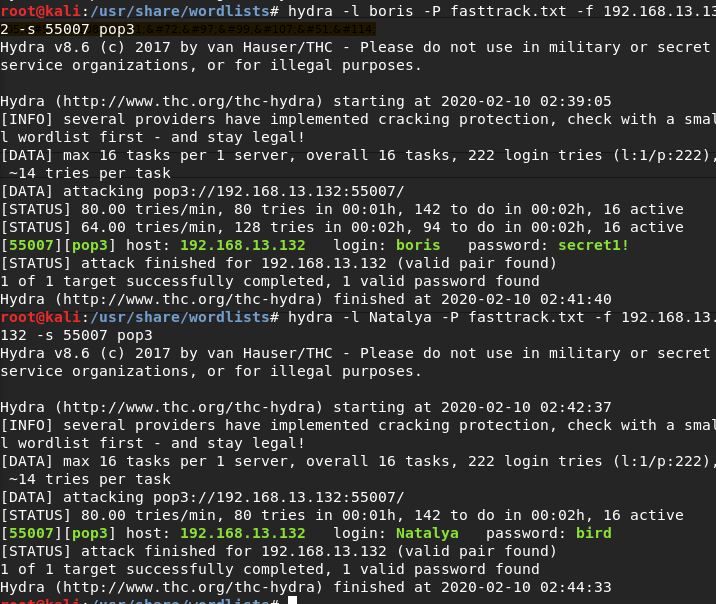
使用口令“Boris:InvincibleHack3r”登陆，竟然错误，这里还有一个小坑需要注意，用户名是“boris”。登陆后又有提示，pop3服务部署在大端口上，结合nmap扫描结果，猜测是端口55006，55007。



查看网页源码，又看到一个藏在注释里的提示，pop3的用户名由两个“Boris”和“Natalya”。

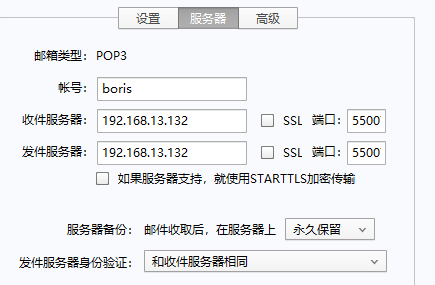


前面注释中提示boris用的是默认密码，用字典库跑一下试试。爆破出pop3服务的两组用户口令，“boris:secret1!”、“Natalya:bird”。

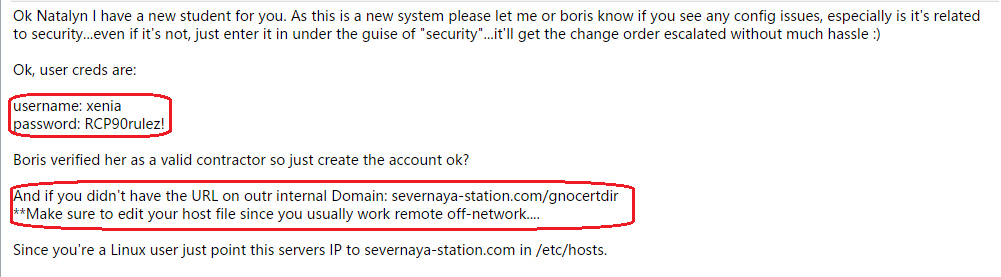


用Foxmail登陆boris和Natalya的邮件账户,下图中端口显示不全，其实是55007和55006.

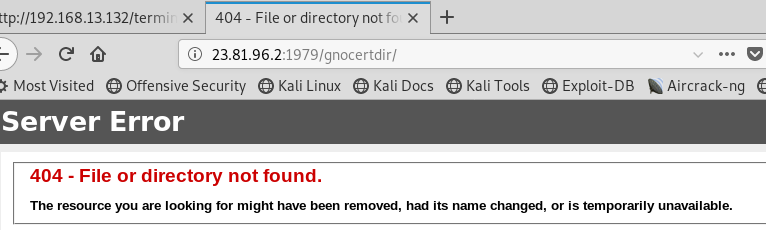




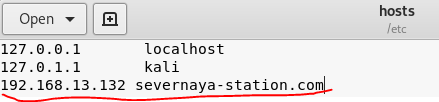
查看邮件内容：



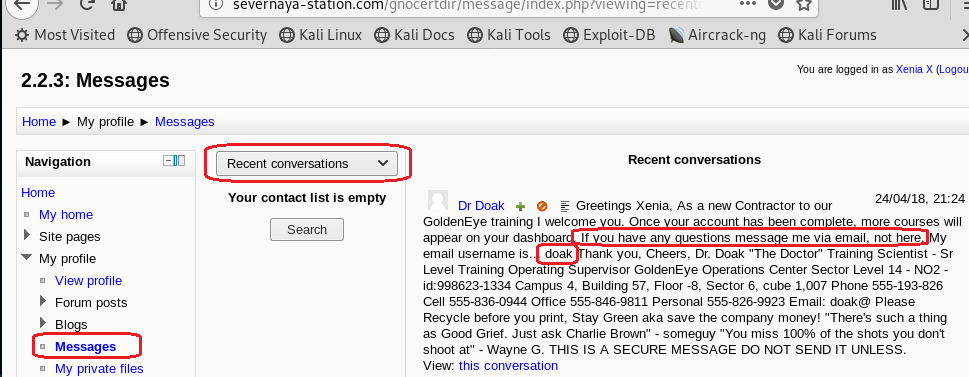
直接访问”http://severnaya-station.com/gnocertdir”报错。



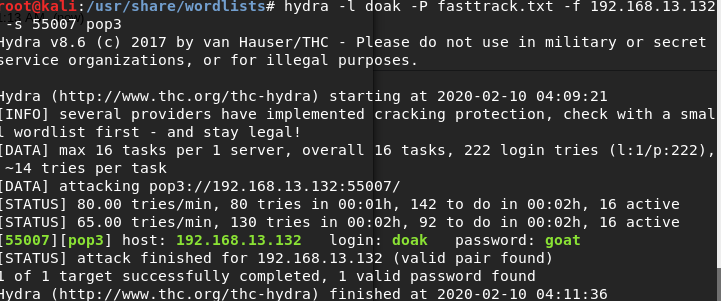
仔细看提示，发现还需要修改hosts文件。



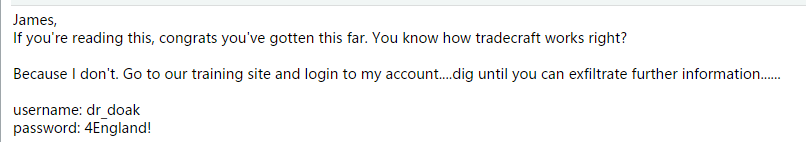
然后用口令”xenia:RCP90rulez!”登陆。发现名为doak的人让Xenia发邮件给他，还不是”@contrax.mil”这个邮件服务器，难道是POP3?



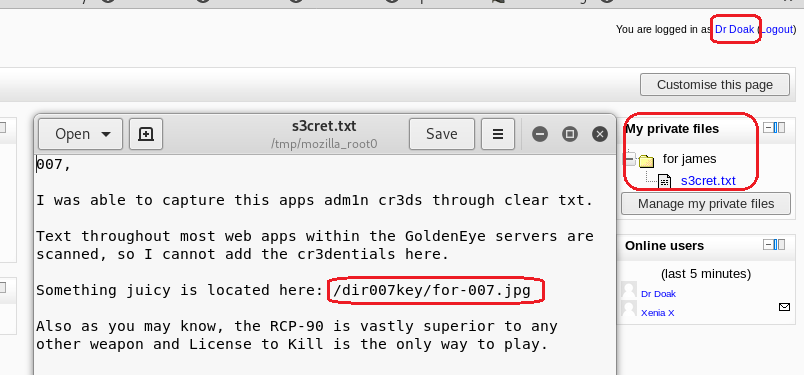
再次尝试爆破，又获取一对用户口令”doak:goat”。



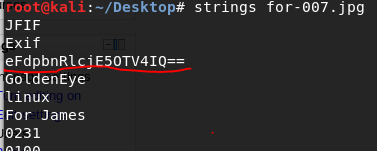
查看邮件，获取另一个人在“http://severnaya-station.com/gnocertdir/”网站的登陆口令。



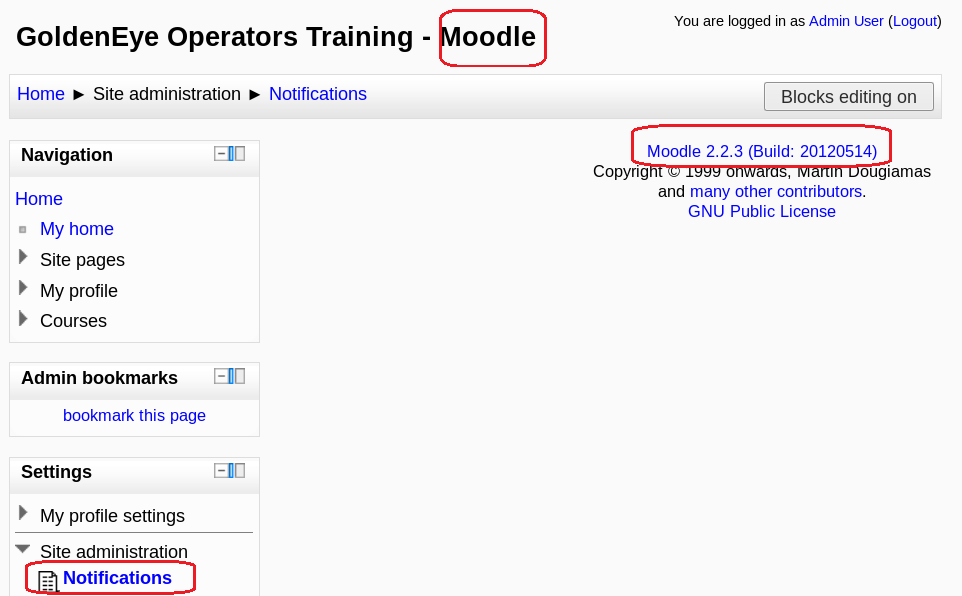
登陆后找到s3cret.txt文件,定位到关键路径”/dir007key/for-007.jpg”。



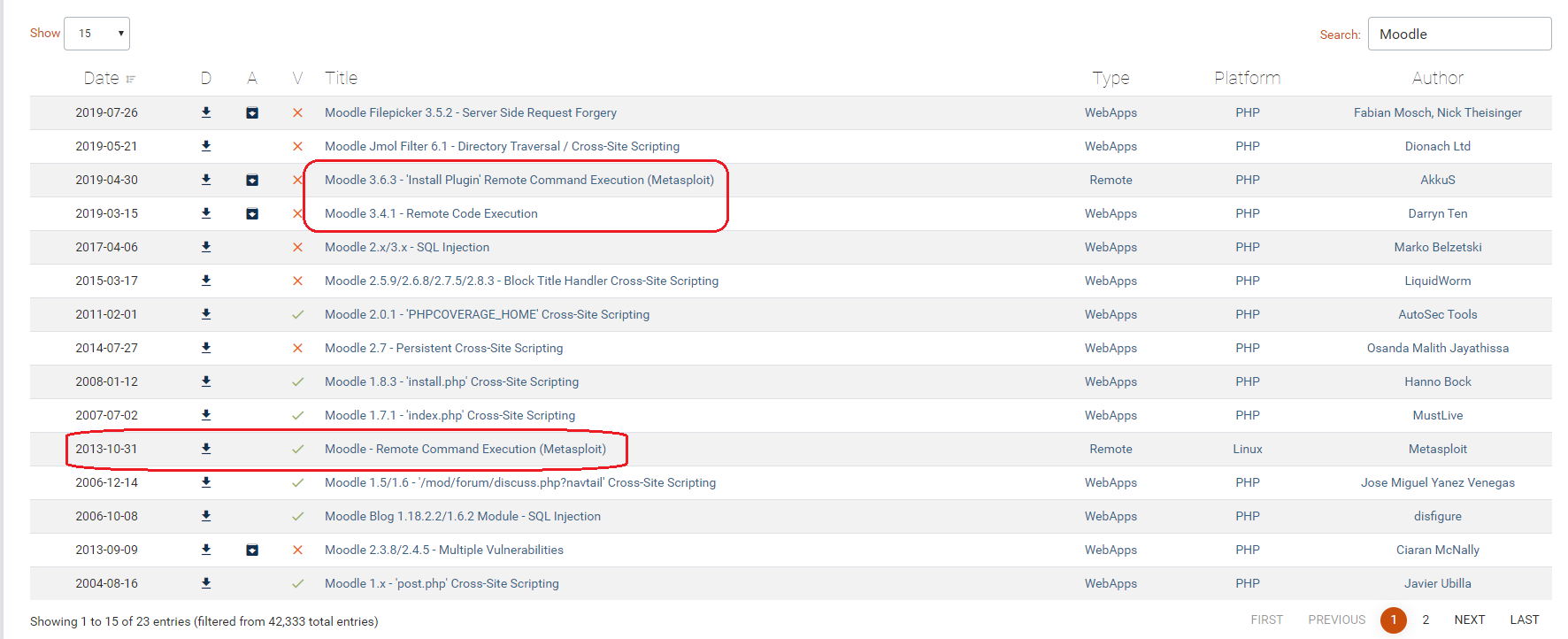
访问该图片未发现任何信息，将图片下载。Strings查看图片是否隐写字符串，发现一个很像base64的字符串，解码后得到密码”xWinter1995x!”。综合上面提示，得到该网页的一个用户口令”admin:xWinter1995x!”。



登陆后查看，未发现有更多的提示信息提供。但发现该网站是开源的在线学习教育平台，且版本为2.2.3，Build 20120514搜索一下这个框架开辟新思路。



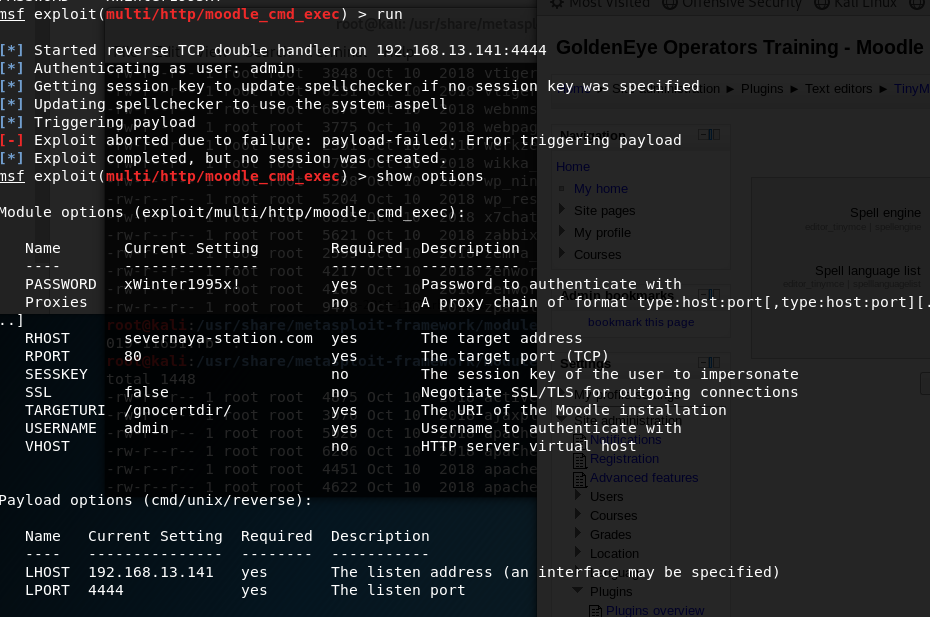
去<https://www.exploit-db.com/>搜索moodle,发现3个可利用的模块。其中Moodle3.4.1 Remote Code Execution是php编写，无法在Metasploit中直接利用，不考虑；Modle 3.6.3在metasploit中无法找到，自行将该文件添加到metasploit模块中。这里有个小技巧，Tile(MeTasploit)是Metasploit可直接利用的模块。



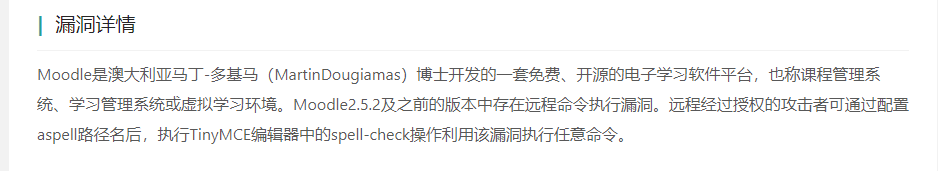
复制rb文件到指定目录后，重启msfconsole,并reload\_all重载所有模块，再次搜索即可查到该模块。



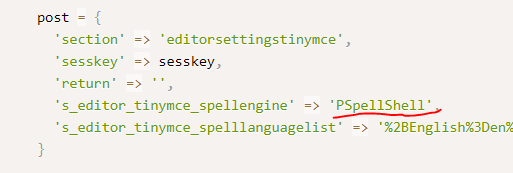
利用该模块失败，考虑Moodle-Remote Command Execution，直接利用还是失败。

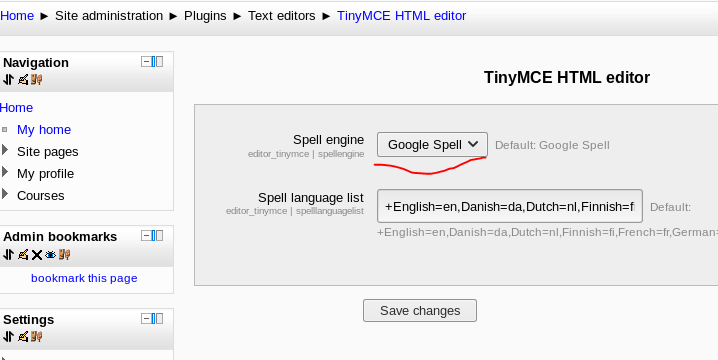


又卡住了，看漏洞介绍。

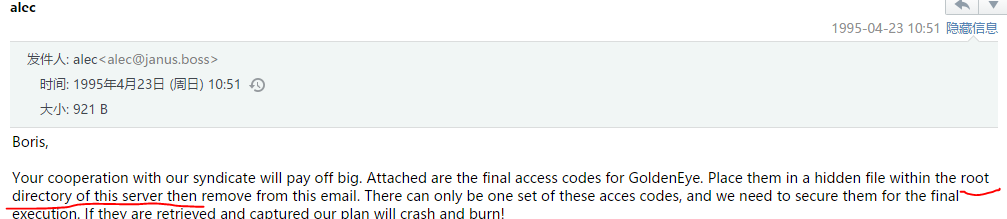


Exp中的设置PSpellShell和后台配置看到的spellengin好像有区别。

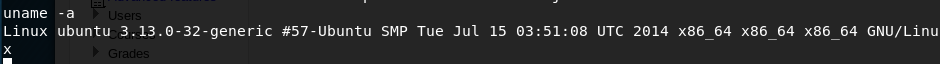




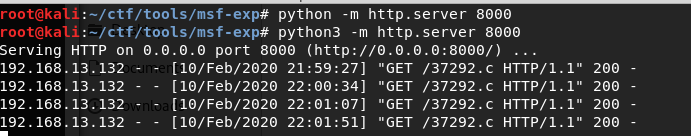
我先将exp中的PSpellShell修改为Google Spell，执行失败。又尝试将后台配置修改为PSpellShell,成功！

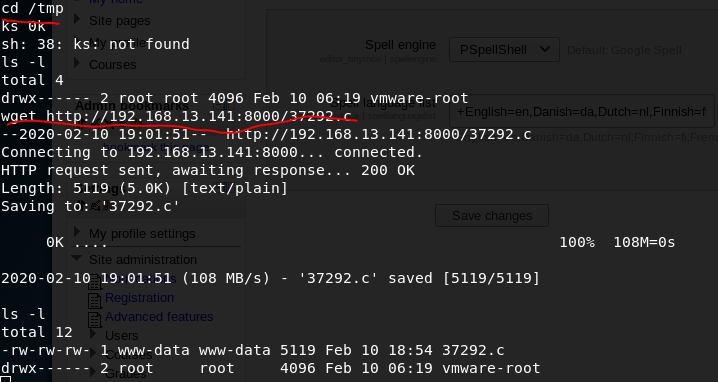


给Boris的邮件告诉我们，目标在root目录下的隐藏文件，可我们无法进入root目录。需要提权。查看靶机的操作系统版本

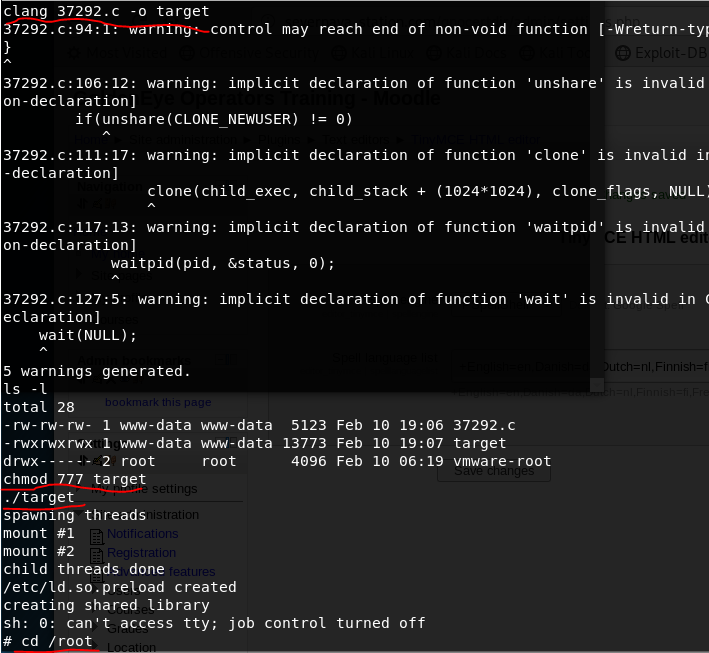


在exploit-db上下载exp,然后再kali机器上开一个http服务，然后再目标机上用wget下载，目标及下载后必须放在/tmp目录下，放在其他目录下提示“Permission deny”。

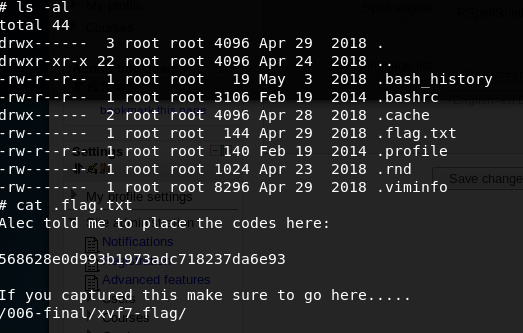




然后编译C文件，没有gcc就用clang替换，修改exp中的“gcc”为“clang”即可。



提权成功，注意目标再/root/下的隐藏目录。



Flag获取。

## 总结

1. 观察一定要仔细
2. 熟练使用工具
3. 看到网站后要考虑其用了什么框架，是否存在漏洞可被利用；查看网页源码，是否又隐藏信息。
4. 扩展知识面，对各种框架及其可能存在的漏洞进行总结整理。