|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
| 渗透测试课程设计报告 | | | | | | |
| Vulnhub渗透测试实战靶场GOLDENEYE | | | | | | |
|  | | | | | | |
|  | | 班级： | | 2019信息安全1 |  | |
|  | | 学号： | | 2019065124 |  | |
|  | | 姓名： | | 殷祥凯 |  | |
|  | | | | | | |
|  | 教师评语： | | | | |  |
|  | 实验难度：\_\_\_\_\_\_  完整程度：\_\_\_\_\_\_  格式规范：\_\_\_\_\_\_  资料完备：\_\_\_\_\_\_  其它说明：\_\_\_\_\_\_ | | | | |  |
|  |  | | 教师签名： | | |  |
| 2022年6月 | | | | | | |

设计报告简表

注：本表为设计报告的简要总结，篇幅限制为一页。

|  |  |
| --- | --- |
| 课程设计题目 | 渗透GOLDENEYE靶机 |
| 个人信息 | 班级：\_2019信息安全1  学号：\_\_2019065124\_\_\_\_  姓名：\_\_\_\_\_殷祥凯\_\_\_\_\_ |
| 课程设计方案 | 搭建GOLDENEYE靶机环境学习相应的知识完成渗透测试，并且对其进行一定的安全加固。该靶机很多信息要通过邮件来获得，有助于提高渗透测试侦察和信息分析的能力。 |
| 采用的工具、方法 | 客户机：kali虚拟机  靶机：GOLDENEYE靶机（Ubuntu）  Vmware  Nmap  Burpsite  NetCat  通过建立监听会话获得反弹shell，然后提权获得root权限 |
| 完成情况 | 成功完成了靶场的安装和对于靶机的渗透测试，并完成了相应的加固。 |
| 参考资料 | [1]李华峰著.Kali Linux2 网络渗透测试实践指南:第2版.人民邮电出版社.2021  [2]渗透测试集成靶场vulhub的搭建.(2022). https://codeantenna.com/a/CXArAOgS1f |

/

1 设计目标

学习CVE-2013-3630漏洞相关知识，掌握nmap端口扫描工具和metasploit，并综合利用渗透测试课程所学知识完成对靶机的渗透测试，获取flag 。

2实验环境与部署

**2.1 实验环境**

靶机：GOLDENEYE靶机

客户机：kali操作系统

**2.2 客户机搭建**

步骤1：从kali官网下载相应的虚拟机文件，kali官网提供了虚拟机压缩包，下载想用文件即可，如图2.1所示。

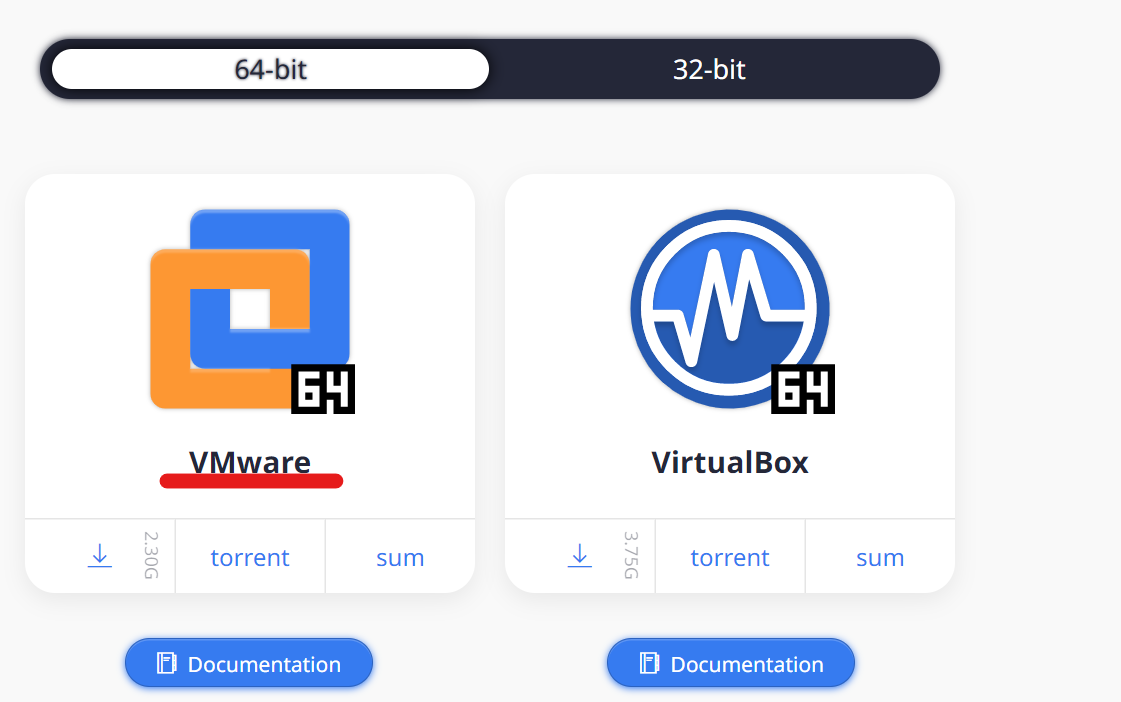


图2.1 下载kali虚拟机

步骤2：配置网络连接方式，为了避免对于外网产生影响，这里使用特定的虚拟网络如图2.2所示。

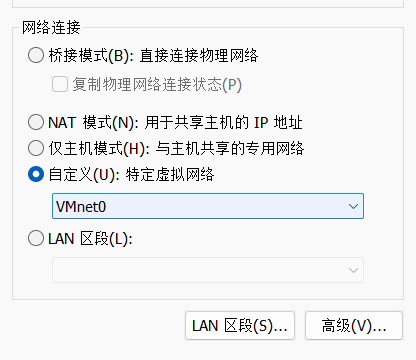


图2.2 设置靶机的网络

**2.3 靶机搭建**

步骤1：从相应网站下载靶机，如图2.3所示。



图2.3 下载靶机

步骤2：使用Vmware导入靶机，如图2.4所示，并将其和客户机设置为同一种网络连接模式。

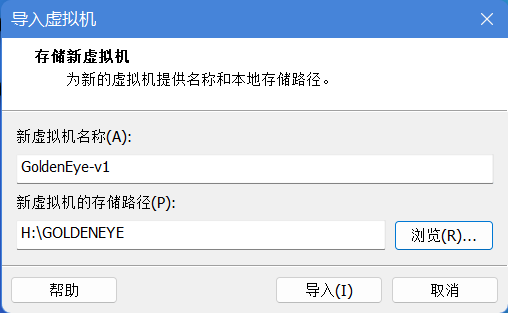


图2.4 导入靶机

步骤3:启动靶机。

3实验内容与实验要求

通过端口扫描、漏洞分析、漏洞利用获得flag。

4实验过程与分析

步骤1：查看客户机所在的网段，如图4.1所示。

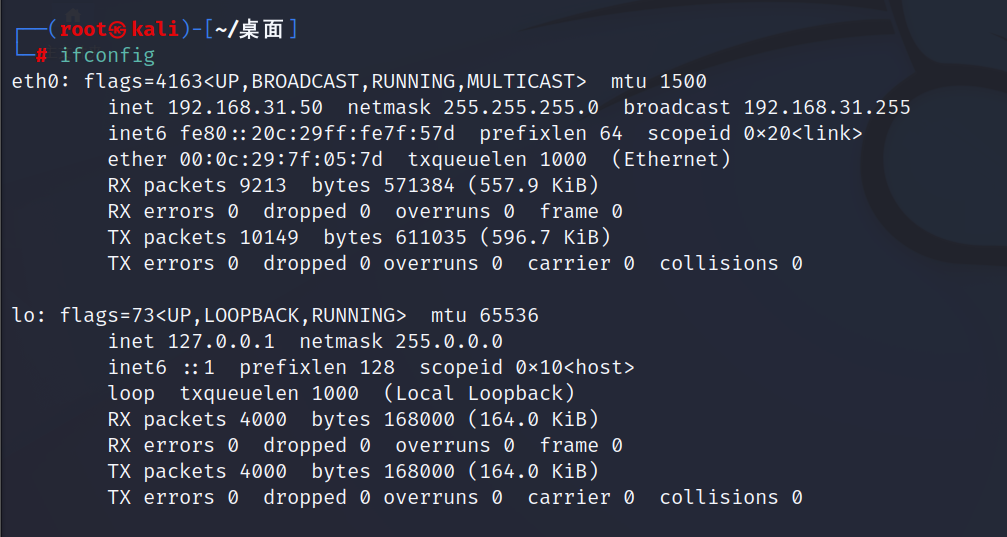


图4.1 查看客户机所在网段

步骤2：利用nmap对客户机所在网段进行扫描。结果如图4.2所示，网段内一共有四台主机，“192.168.31.50”主机为客户机，1号主机应当是宿舍路由器的ip，“192.168.31.136”机应当与虚拟网网络有关，于是基本可以认定靶机IP为“192.168.31.225”。

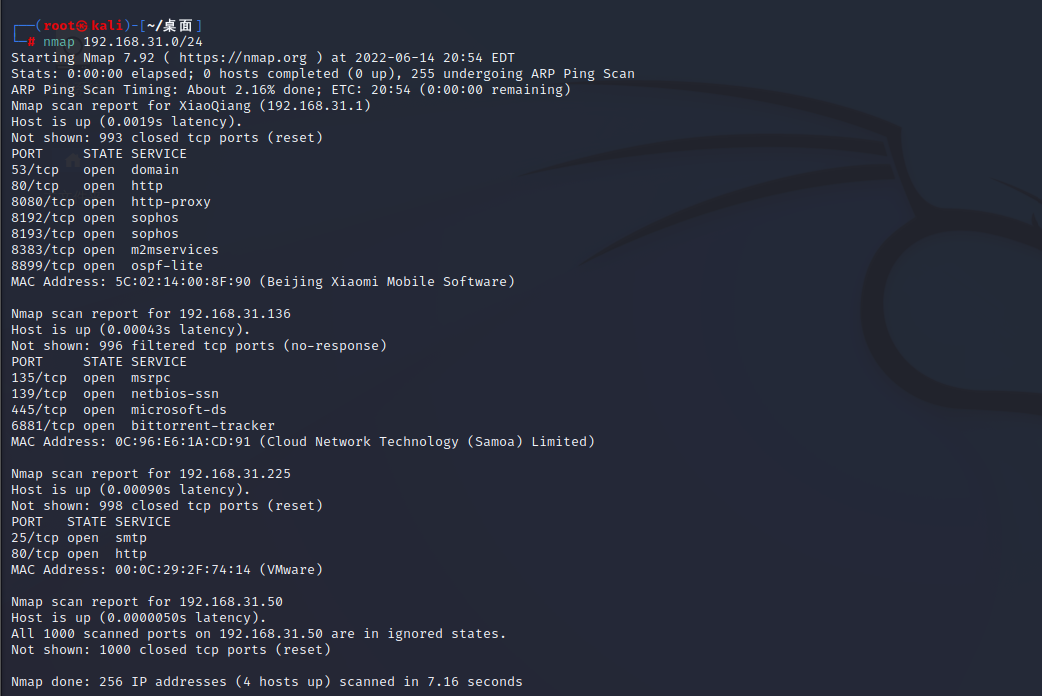


图4.2 对客户机所在网段进行扫描

步骤3：对目标靶机进行更加详细的扫描。结果如图4.3所示，开放了smtp和http服务，且还有两个pop3端口。

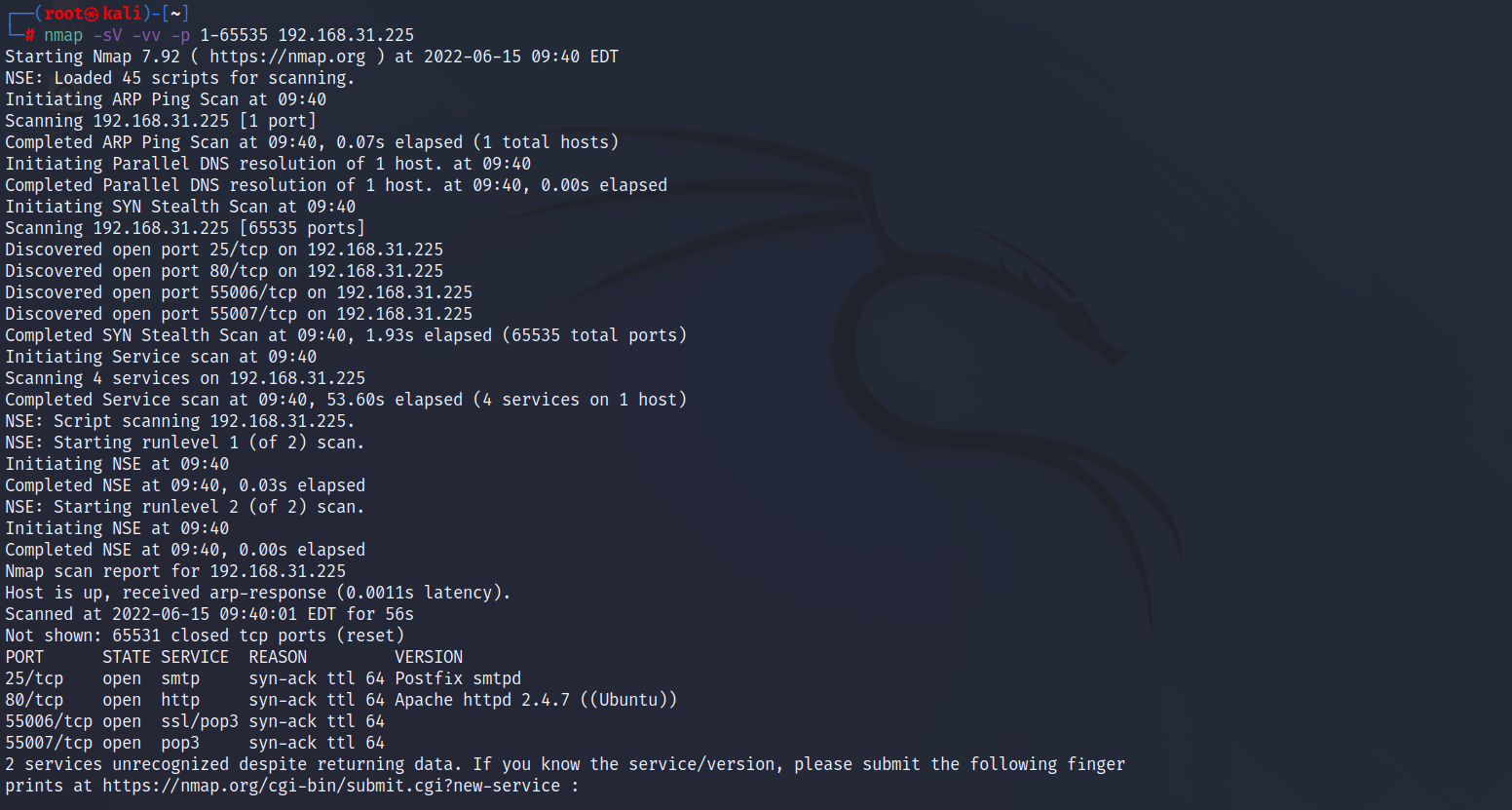


图4.3 对靶机进行仔细扫描

步骤4：既然开放了http服务自然应当尝试登录查看有无有用的消息，在浏览器输入网址，结果如图4.4所示。根据提示进入/sev-home/页面，如图4.5所示。发现需要进行登录所以我们要寻找有关账户和密码的信息。

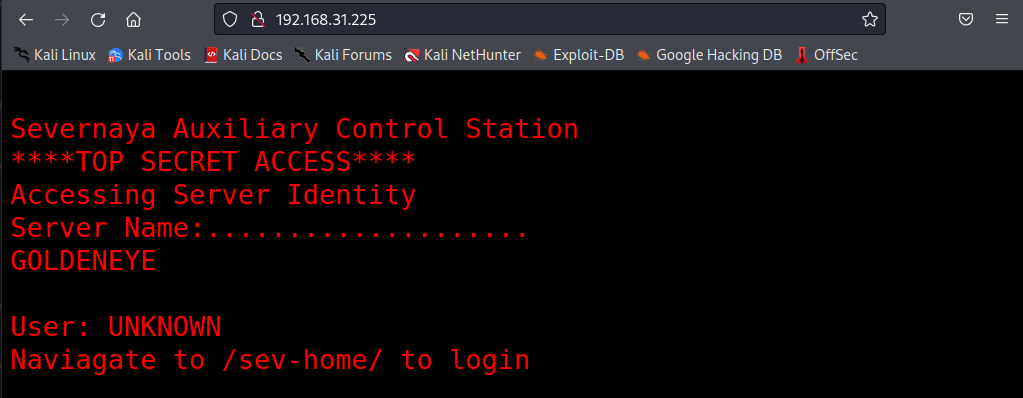


图4.4 登录目标网站

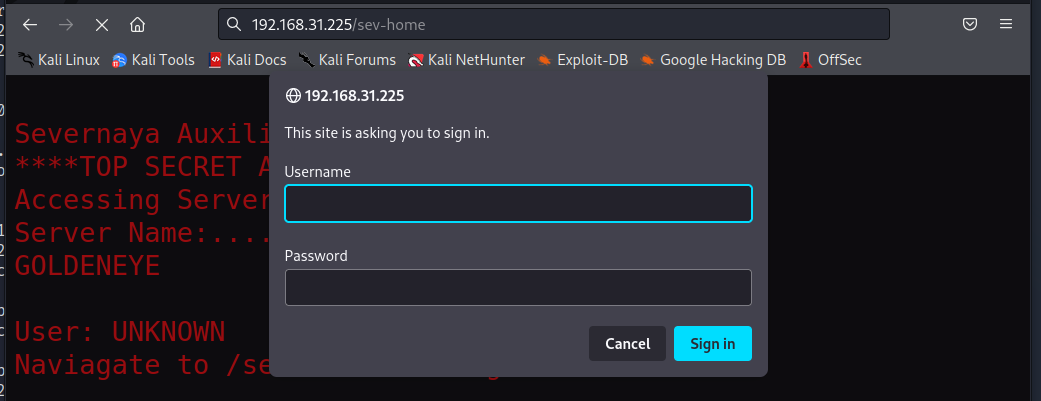


图4.5 sev-home页面

步骤5：由于暂时没有其他思路所以查看一下网站的源码看能否找到突破点，源码如图4.6所示。其中最引人注目的就是“terminal.js”。查看“terminal.js”如图4.7所示，找到了疑似账号和密码的信息。其中疑似账户名的是“Boris”和“Natelya”。而密码采用了编码手段。

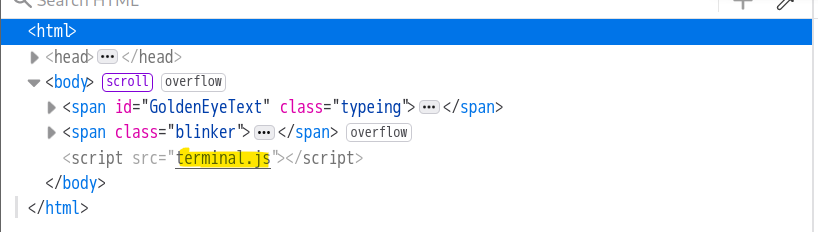


图4.6 网站源码

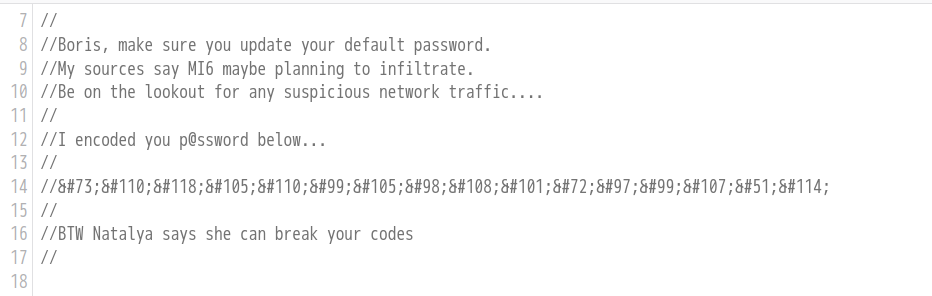


图4.7 terminal.js内容

步骤6：使用BurpSuit对密码进行破解，但是kali中的BurpSuit无法正常启动，查找资料发现是JDK版本的问题，查看系统现有的JDK版本并选择合适的版本，如图4.8所示。然后使用BurpSuit中的decoder模块进行解码，如图4.9所示结果为“InvincibleHack3r”



图4.8 更改Java版本

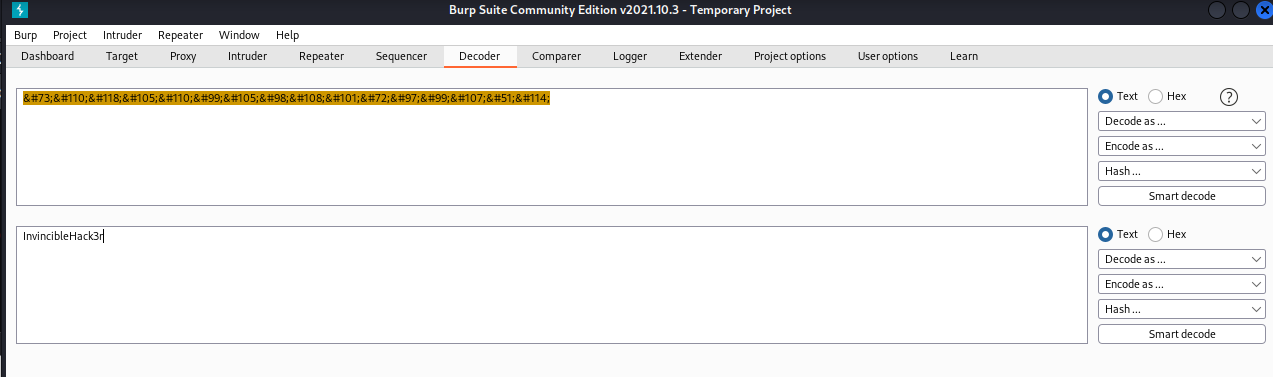


图4.9 使用BurpSui解码

步骤7：尝试登录，登陆成功，登陆后的界面如图4.10所示。根据网站的提示知道下一步可能和pop3邮箱有关，且端口是一个端口号较大的端口。在扫描阶段靶机存在55006和55007两个端口和pop3有关，但是55006还有ssl服务所以猜测是55007端口。

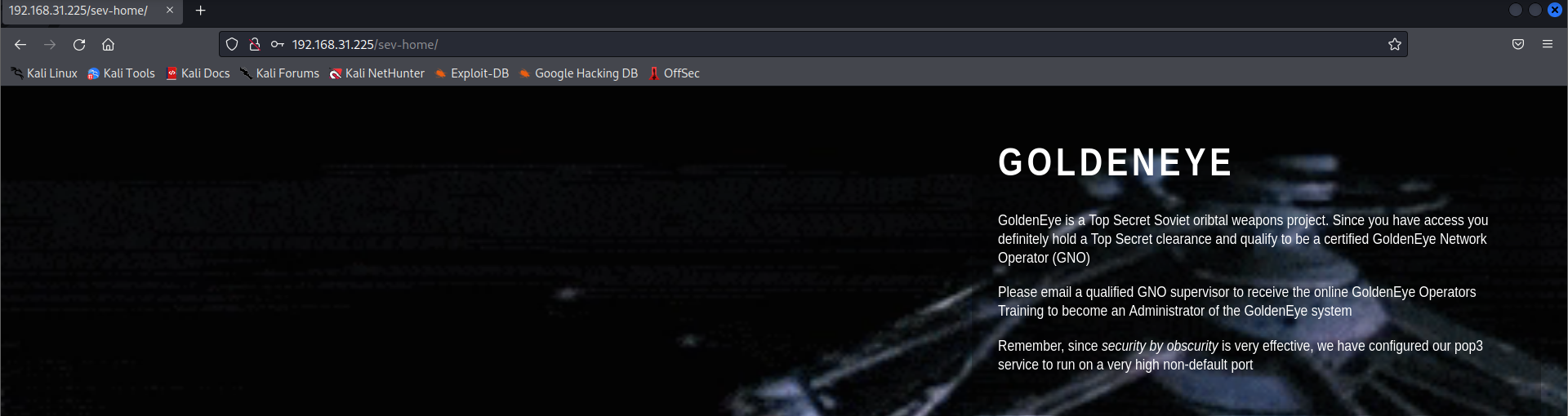


图4.10 登陆成功

步骤8：远程连接pop3服务器，从中下载index.html文件，如图4.11所示。查看文件内容如图4.12所示。应当是需要账号和密码才能登录pop3邮箱。

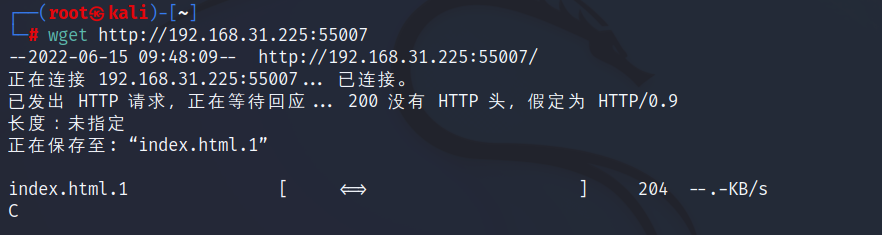


图4.11 远程连接pop3服务器

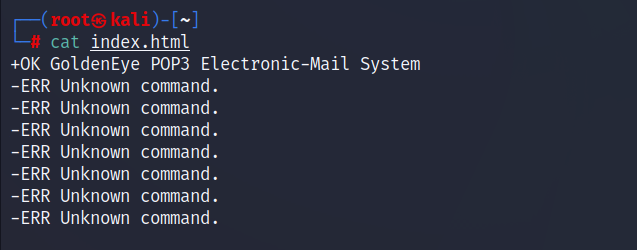


图4.12 查看index.html

步骤9：terminal.js 中提醒用户要修改默认密码，所以可能用户密码并不复杂可以尝试使用暴力破解。首先构造用户名字典如图4.13所示，然后使用系统自带的密码字典进行暴力破解，如图4.14所示。分别获得了natalya和boris的密码。

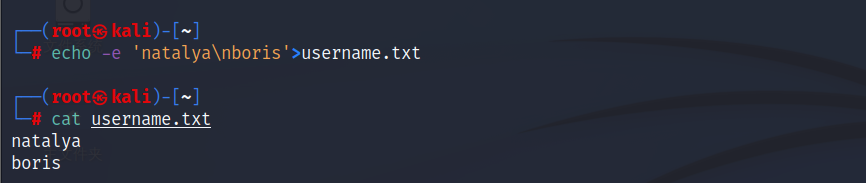


图4.13 构造用户名字典

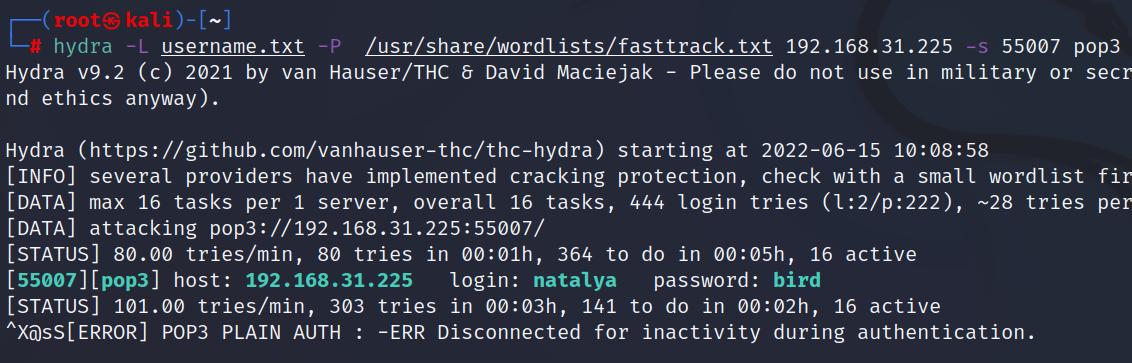


图4.14 暴力破解密码

步骤10：用使用用户boris登录pop3邮箱，如图4.15所示。并查看下邮箱中的邮件如图4.16-4.18所示。第一封邮件的内容是邮箱由管理员负责，第三封邮件的内容是在服务器的root目录下存在一个很重要的文件。

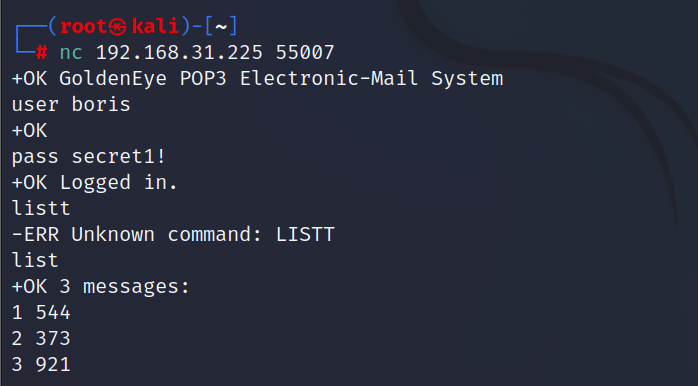


图4.15 登录boris邮箱

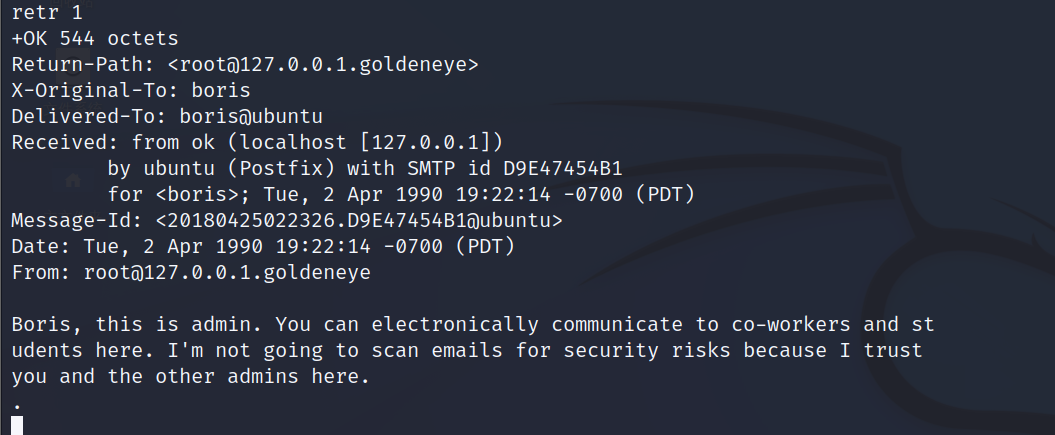


图4.16 boris邮箱的第一封邮件

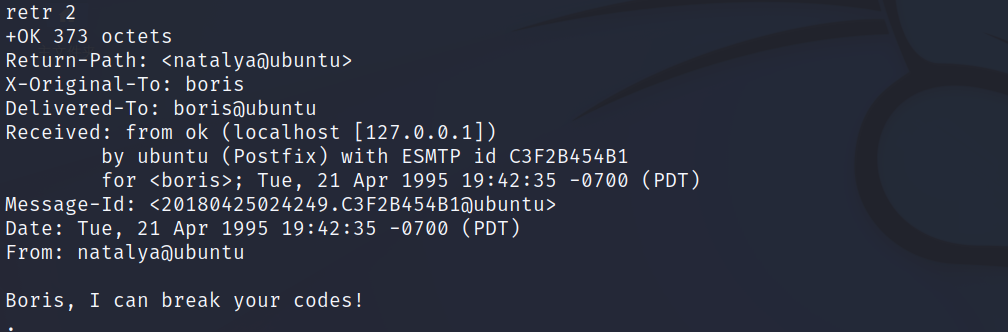


图4.17 boris邮箱的第二封邮件

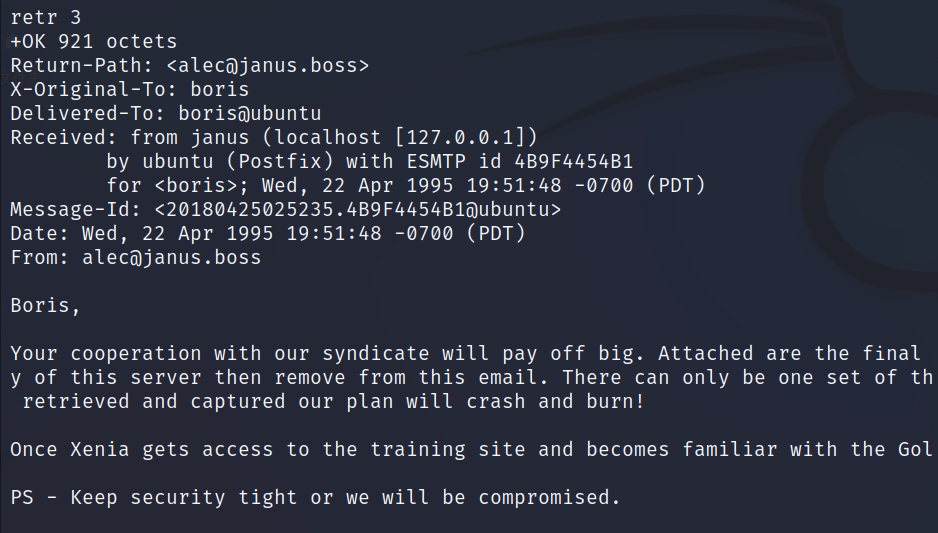


图4.18 boris邮箱的第三封邮件

步骤11：用使用用户natalya登录pop3邮箱，如图4.19所示。并查看下邮箱中的邮件如图4.20-4.21所示。从第二封邮件中获得一组用户密码，并且得到一个域名。

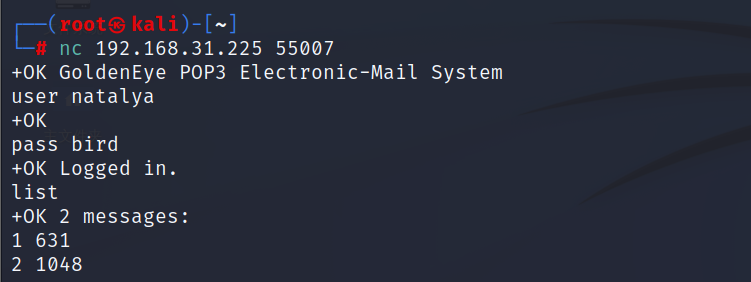


图4.19 登录natalya邮箱

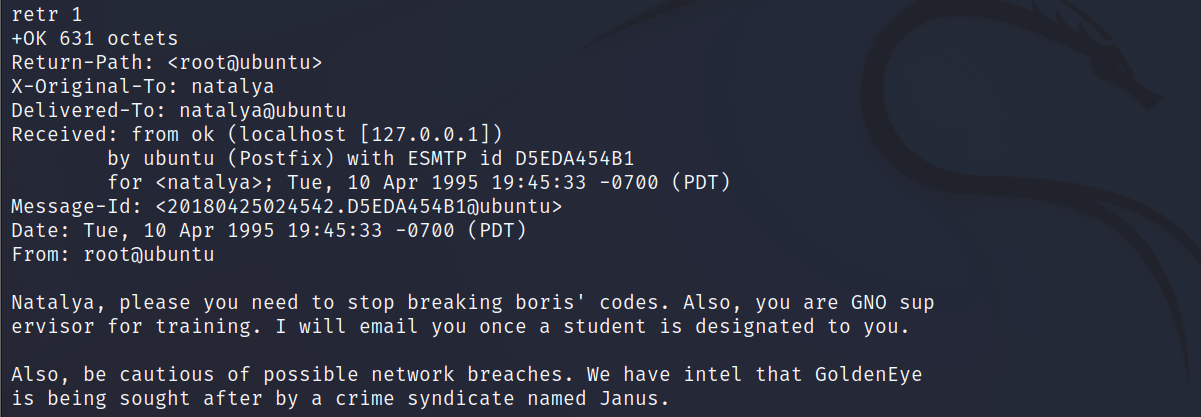


图4.20 natalya邮箱的第一封邮件



图4.21 natalya邮箱的第二封邮件

步骤12：将上一步获得的域添加到kali /etc/hosts本地域信息中如图4.22所示。然后使用浏览器访问域名，如图4.23所示。

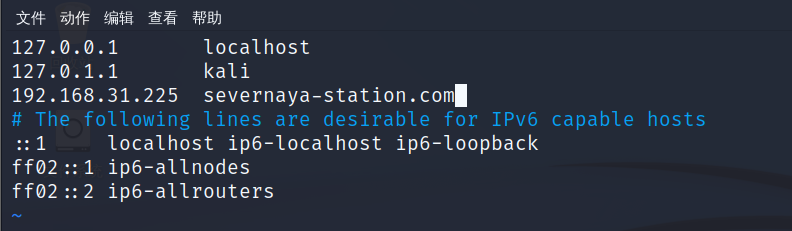


图4.22 添加域信息

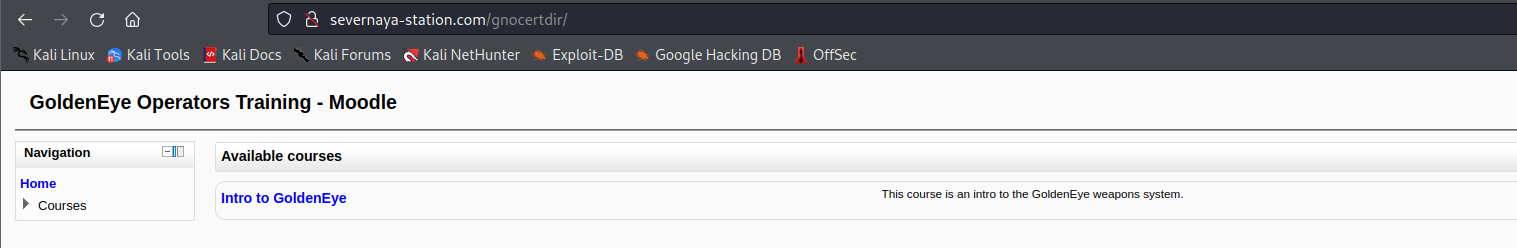


图4.23 访问域名

步骤13：使用从邮件中的获得账号密码登录，如图4.24所示。

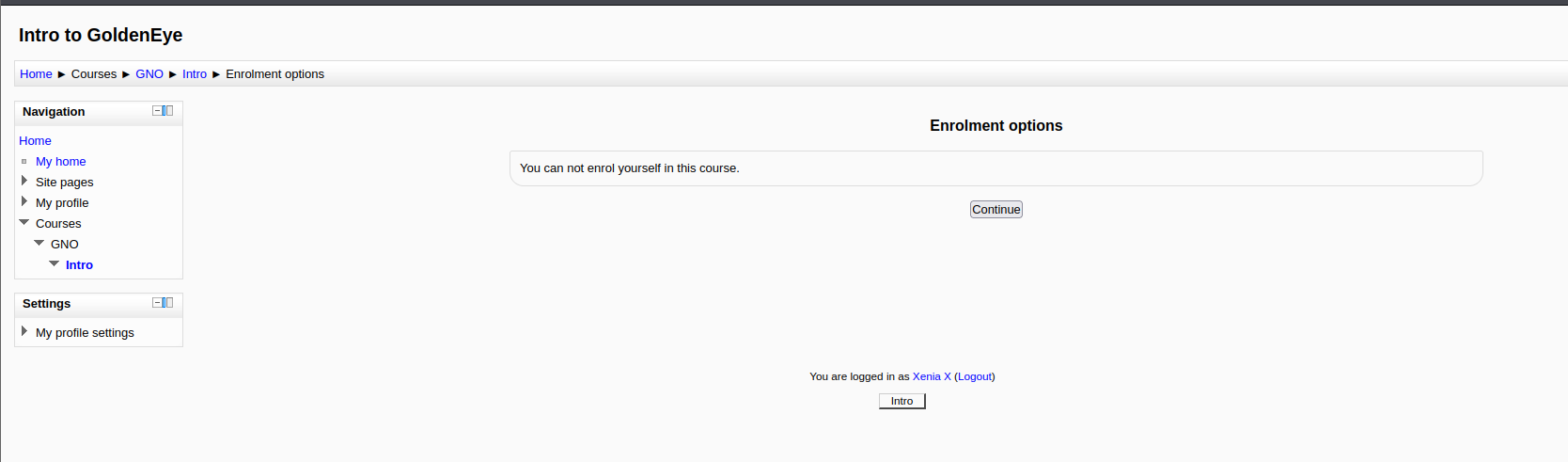


图4.24 登陆成功后界面

步骤14：查看网站内容，找到一封邮件，邮件内容如图4.25所示。获得了另一用户名，对该用户进行暴力破解，如图4.26所示。

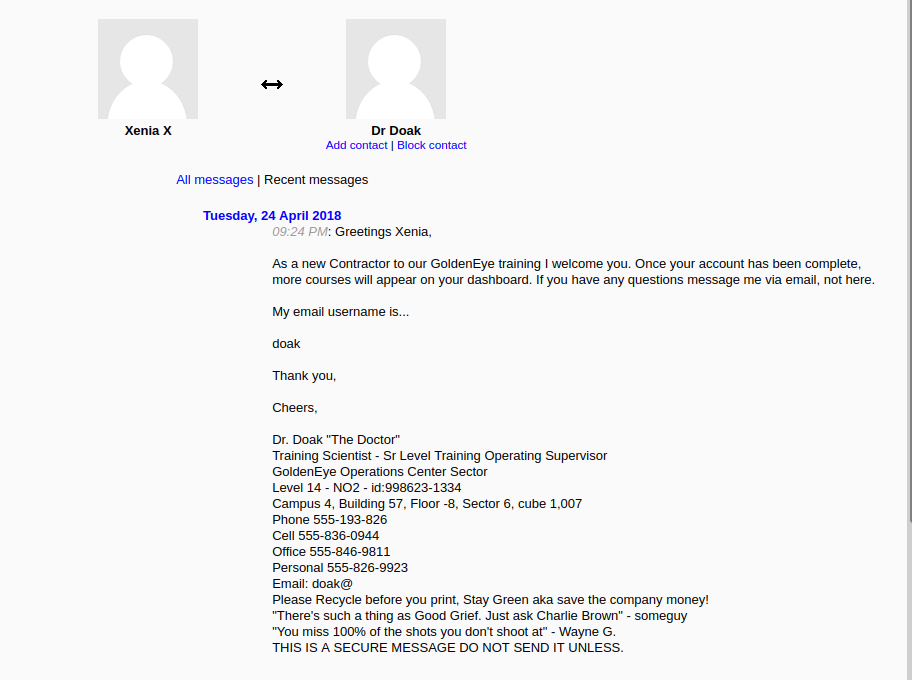


图4.25 邮件内容

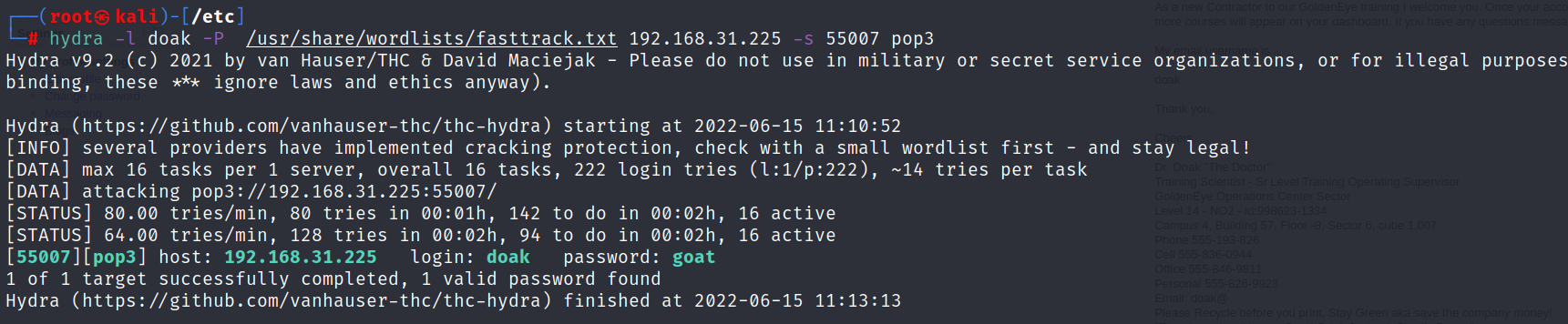


图4.26 暴力破解doak的密码

步骤15：查看doak用户的邮箱，查看邮箱中的邮件如图4.27所示。从邮件中获取了网站的另一用户密码，根据邮件语气推测改用户权限较高。

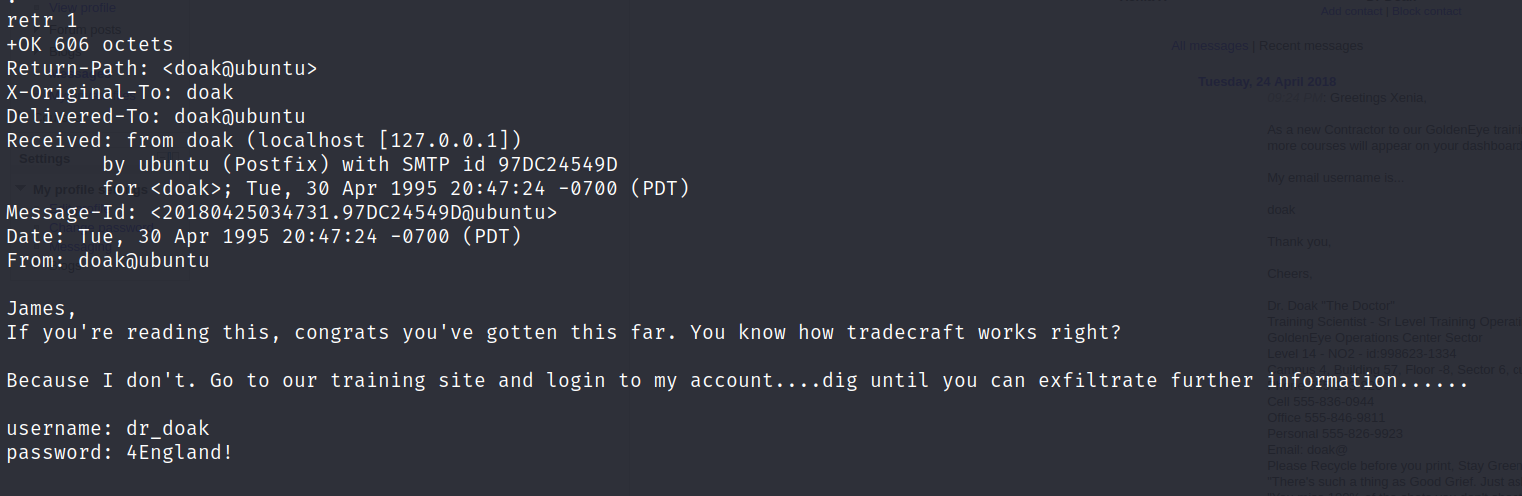


图4.27 doak邮件内容

步骤16：用新获得用户密码再次登录网站，找到一个私密文件，如4.28所示。将文件下载下来进行查看，文件内容如图4.29所示，主要是给出了一个图片的资源路径。根据所给路径获得图片，如图4.30所示。

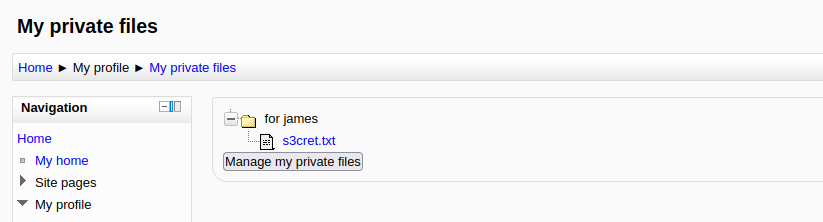


图4.28 doak的私密文件

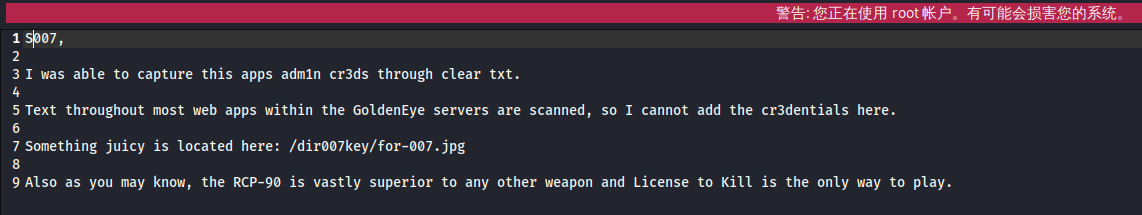


图4.29 私密文件内容

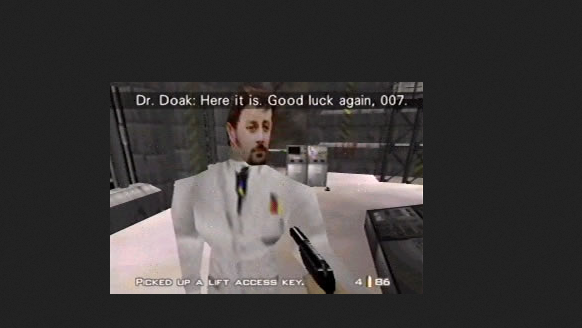


图4.30 查看图片

步骤17：由于没有其他线索，尝试将图片下载下来进行分析如图4.31所示，只有Image Description使用了编码，可能存在有用信息。对其进行解码，发现其格式很像系统默认的密码格式，推测是某用户的密码。根据提示推测应当是管理员的密码。

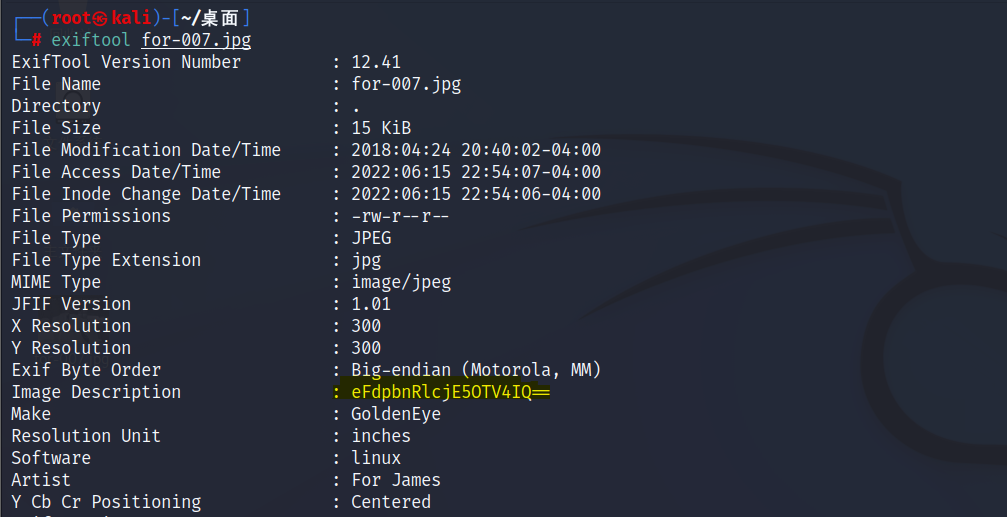


图4.31 对图片进行分析



图4.32 解码结果

步骤18：使用管理员账号密码尝试登录网站，登陆成功。发现管理员可以修改系统的路径，将其修改为一个python脚本，如4.33所示。并修改spell engine如图4.34所示。

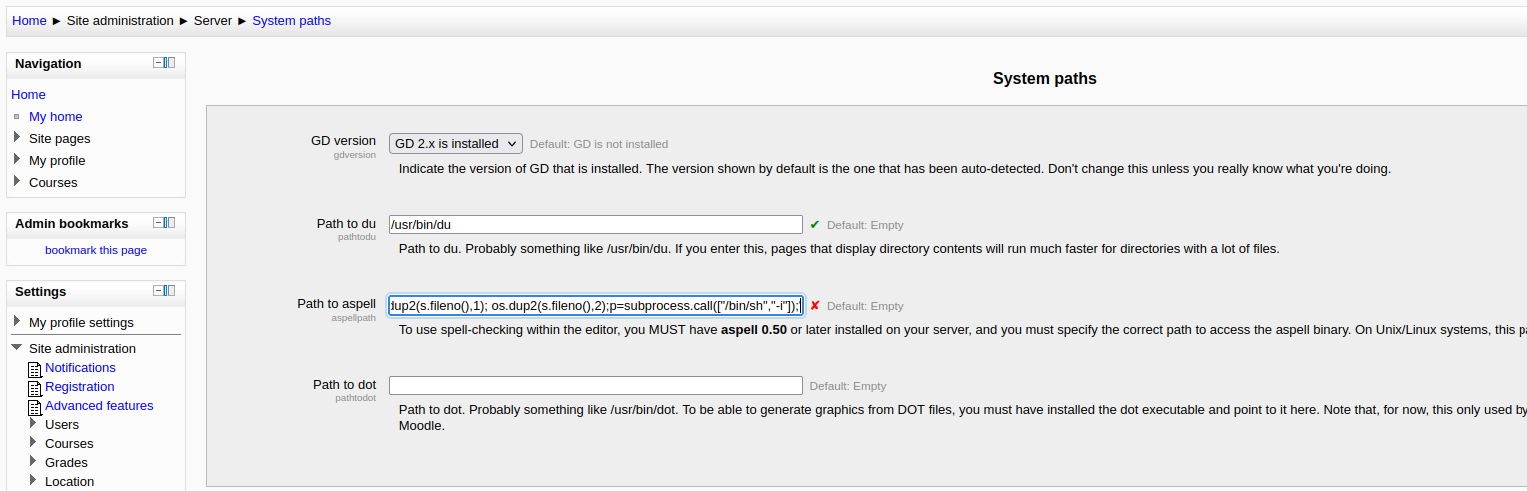


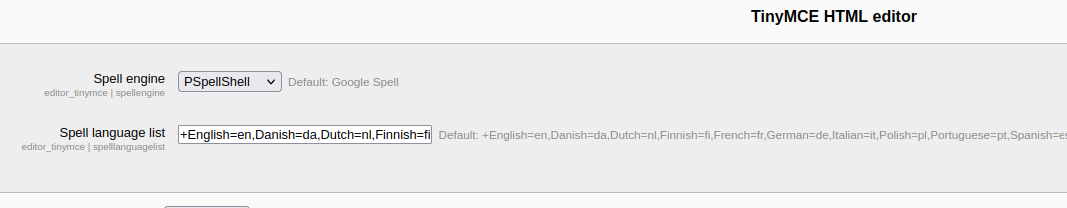
图4.33 将系统路径修改为python脚本

图4.34修改spell engine

步骤19：建立监听会话监听python脚本中写的端口，然后新建一个blog监听成功，如图4.35所示。

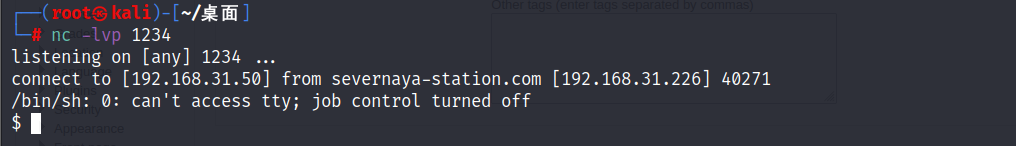


图4.35 监听成功

步骤20：通过python获取一个TTY，并查看靶机的一些信息，如图4.36所示。



图4.36 靶机基本信息

步骤21：根据靶机内核版本去查找相应的漏洞。查找结果如图4.37所示。

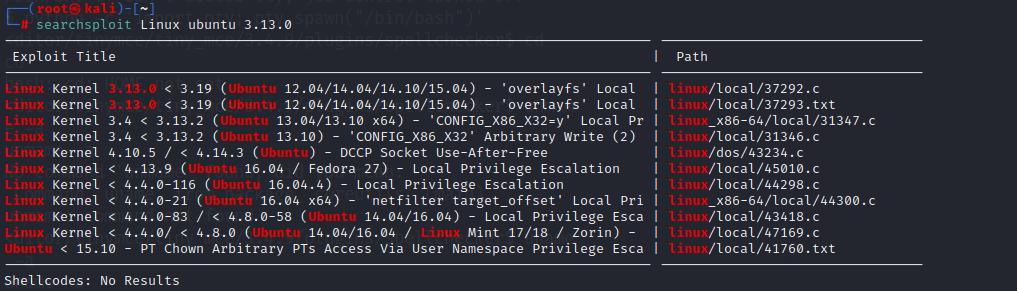


图4.37 靶机存在的漏洞

步骤22：需要搭建简易的服务器将本机上的文件传到靶机上来进行提权。建议服务器的搭建如图4.38所示。在靶机上下载相应的文件如图4.39所示。



图4.38 搭建简易服务器

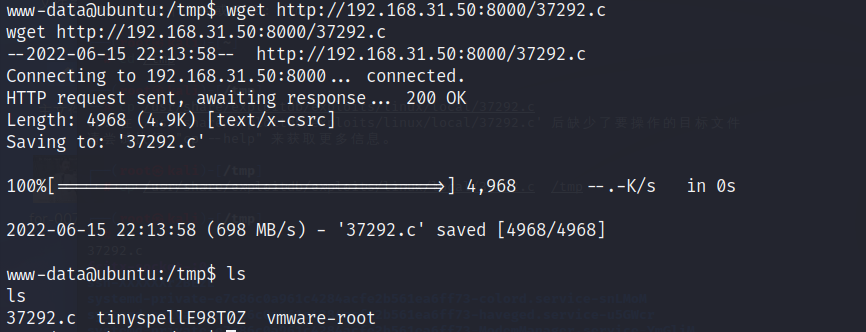


图4.38 从简易服务器下载文件

步骤23：编译37292.cw文件，失败，提示靶机没有安装gcc，但是安装gcc需要管理员权限。所以修改文件编译方式如图3.39所示，重新编译文件，并执行编译后的可执行文件如图3.40所示

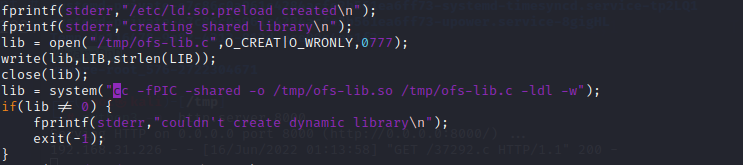


图4.39 修改文件编译方式

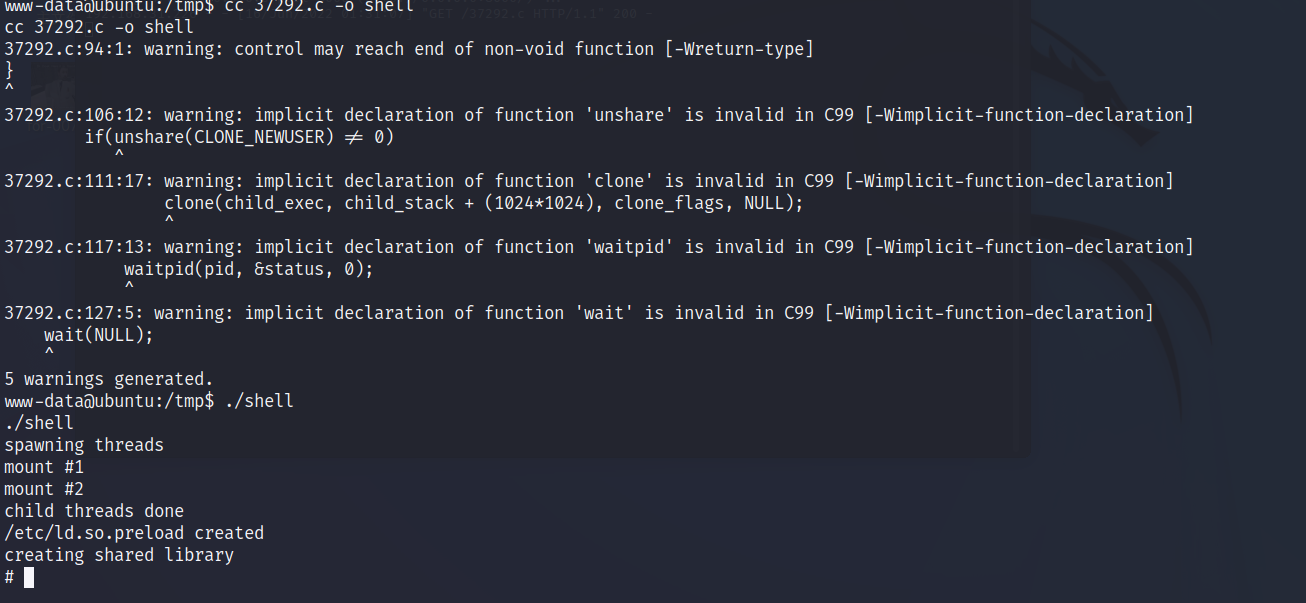


图4.40 编译并执行

步骤24：进入root目录下查看文件发现目录下有.flag.txt文件查看内容，内容如图4.41所示。并且还给了网站信息，查看获得如图4.42所示的页面。完成全部流程。

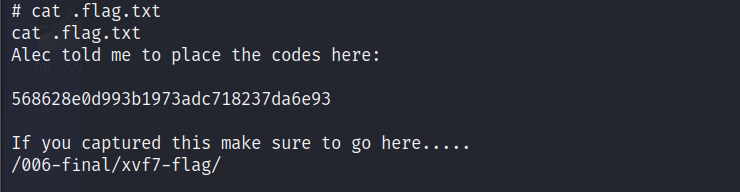


图4.41 查看flag



图4.41 查看页面信息

5思考题目

1. 对靶机的渗透中使用了反弹shell，反弹shell的原理是什么？

**答：**所谓的反弹shell，就是攻击机监听在某个TCP/UDP端口为服务端，目标机主动发起请求到攻击机监听的端口，并将其命令行的输入输出转到攻击机。首先我们要明白连接有两种一种就是我们平时连接服务器的那种主动的连接也叫正向连接。林一种连接是反向连接，就是攻击者指定服务端，受害者主机主动连接攻击者的服务端程序，即为反向连接。反弹shell的方法很多，本次案例中用到的就python是脚本方法，因为现在大多数Linux系统再带python。当靶机执行python脚本时就连接攻击机的特定端口，攻击机只要建立监听会话就可以进行模拟终端的输入和输出。

1. 本次渗透很多信息都是从邮件中获得的，但是真实渗透的渗透测试场景中邮件属于个人隐私，如何解决邮件泄露安全信息的风险？

**答**：通常渗透测试时，客户可能开放一部分邮件给测试人员，但是通常不会是所有的邮件，而且处于效率和时间的考虑，不可能查看所有邮件。所以最好的做法还是树立用户足够的安全意识，完善安全管理制度。然后对邮箱进行加固防止邮件内容泄露。

1. 根据渗透测试的攻击过程提出对靶机的加固。

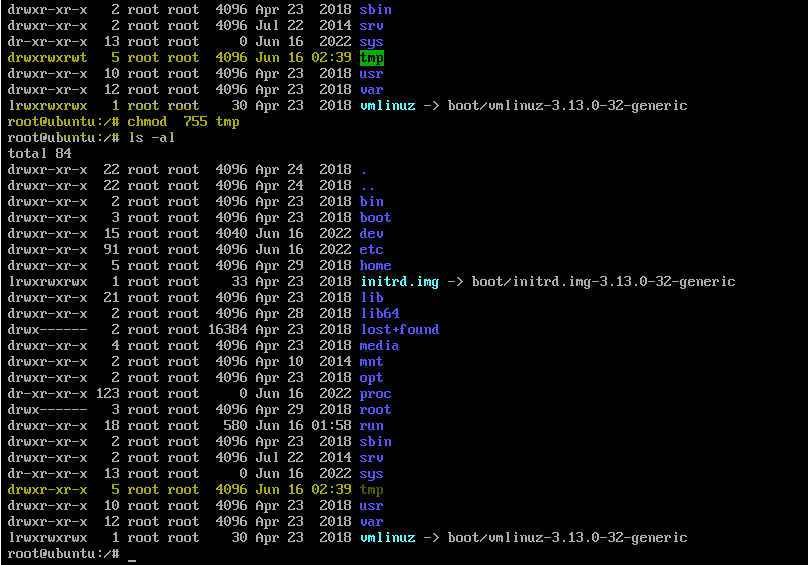
**答：**攻击者想要完成提权需要通过建议服务器下载相应的文件，由于下载需要在/tmp目录下完成，可以修改普通用户对该目录的权限取消写权限即可。如图5.1所示。

图5.1 修改目录权限

1. 了解本次渗透测攻击所用到的漏洞，进行简述。

**答：**Moodle 至 2.5.2 允许经过身份验证的远程管理员通过配置 aspell 路径名，然后在 TinyMCE 编辑器中触发拼写检查操作来执行任意程序

1. 在构建虚拟机渗透测试环境时网络模式选择哪一种模式较好？

**答：**Vwmare一共提供了四种网络模式，分别是桥接、NAT、主机、以及特定虚拟网络。NAT模式中虚拟机可以访问网络中的其他主机但是不可以被访问，换言之虚拟机之间不能互相访问，不适合用于渗透测试环境的搭建。桥接模式每个虚拟和主机一样单独分配IP地址，但是由于是在真实的网段中干扰太多不适合用于渗透测试。主机模式是在主机中模拟出一张网卡，虚拟机连接在网卡上，可以上网，虚拟机也可以互相访问。最后一种就是特定网络，只要虚拟机是同一网络下就可以互相访问，干扰风险最小，适合用于搭建测试环境。

6结论

本次课程设计搭建了一个渗透测试的环境，并且成功完成了对相应靶机的渗透测试。收获很多，首先就是在搭建环境中了解了各种网络模式，由于缺乏经验对于网络模式的选择不恰当导致开始时干扰太多，且容易造成对他人主机造成影响。其次也对于渗透测试信息的获取有了更多的理解，本次搭建的是黄金眼靶机，按照线索逐步找到最后的flag。不同于以前遇到的靶机，该靶机涉及大量的邮件，很多信息都是分析邮件获得的，给我的启示是我们不能只关注软件方面的漏洞也要注意人的安全意识培养。此外，该靶机涉及了很多不同的用户和不同的用户权限，但是由于用户对于信息读写的控制不严格，导致高权限用户把自己的信息透露给低权限用户，一旦获得一部分权限就可以借此获得更多权限。

最后在攻击的时候对于本学期学习的一些渗透计较做了回顾，深入了解了反弹shell的原理和用法，以及防范方法。并且通过攻击过程了解了靶机的弱点后对其进行的加固更加的具有针对性，加深了对于渗透测试意义的理解。

7参考文献

[1]渗透测试集成靶场vulhub的搭建.(2022). https://codeantenna.com/a/CXArAOgS1f

[2]李华峰著.Kali Linux2 网络渗透测试实践指南:第2版.人民邮电出版社.2021