# 八、Bash脚本编程



## Linux黑客基础-55-Shell脚本编程（1）shell脚本速成班

作为一名黑客必须要具备脚本编写的能力,至少熟悉一门编程语言

bash shell script（shell脚本的编写能力）

Your First Script: “Hello, Hackers-Arise!”你的第一个脚本

#!/bin/bash //脚本的第一行

告诉你的操作系统您要使用哪个解释器

# This is my first bash script. Wish me luck. //注释语句

添加注释的好处：

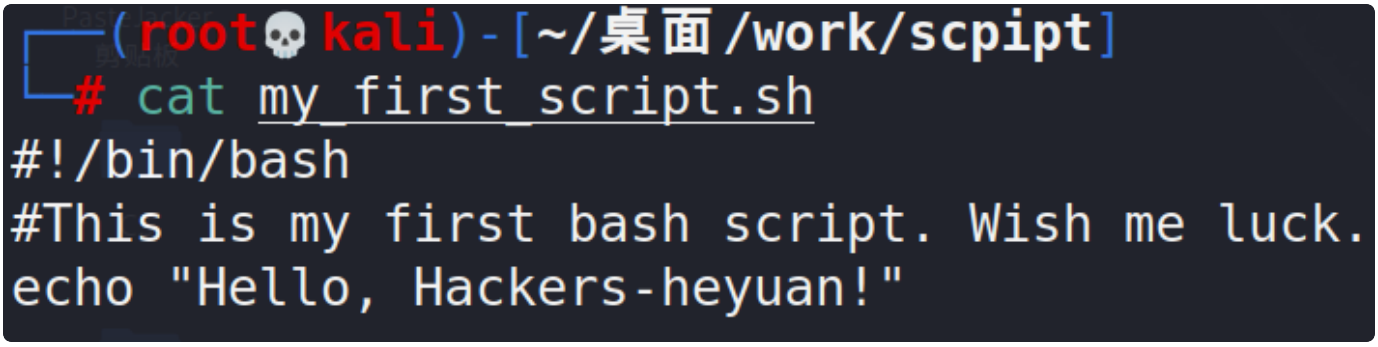
对脚本的说明（脚本是为了做什么以及编写的思路、说明等）

echo "Hello, Hackers-heyuan!"

第一个脚本案例

第一个脚本 Plain Text

```
┌──(root💀kali)-[~/桌面/work/scpipt]
└─# cat my_first_script.sh
#!/bin/bash
#This is my first bash script. Wish me luck.
echo "Hello, Hackers-heyuan!"
```




给脚本添加可执行权限

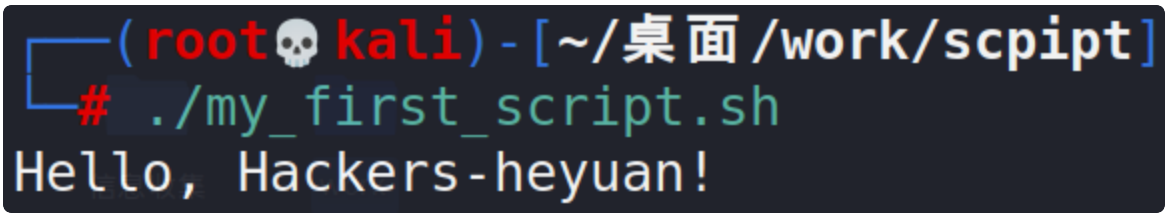
chmod 777 my_first_script.sh

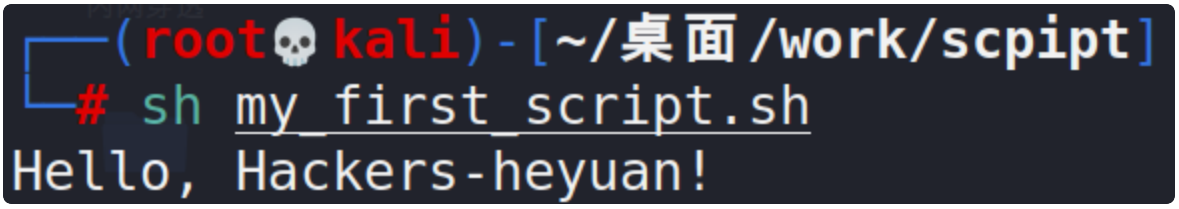
执行脚本

1、文件名前的./告诉系统我们希望在HelloHackersArise 所在的当前目录文件中执行此脚本。

2、它还告诉系统，如果在另一个名为 hellohackersrise 的目录中有另一个文件，请忽略它，只在当前目录中运行 hellohackersrise。在您的系统上似乎不太可能有另一个具有此名称的文件。

3、在执行文件时使用./是一个很好的实践，因为这会将文件执行定位到当前目录，并且许多目录将具有重复的文件名，例如 start 和 setup。



PS1：shell脚本的扩展名通常以sh结尾

# Linux黑客基础-56-Shell脚本编程（2）添加带有变量和用户输入功能的脚本

写一个"带有变量和用户输入功能"的脚本 Plain Text

```
vi second_script.sh    创建 脚本
写入脚本
#!/bin/bash
#readname
echo -n "first name:"
read firstname
echo -n "last name:"
read lastname
echo -e "your first name is:${firstname}\n"
echo -e "your last name is:${lastname}\n"
chmod 777 second_script.sh    赋予权限
执行脚本
./second_script.sh
first name:heyuan
last name:lisijia
your first name is:heyuan
your last name is:lisijia
```

脚本优化

Plain Text

```
#!/bin/bash
#readname
#echo -n "first name:"
#read firstname
read -p "first name: " firstname
#echo -n "last name:"
#read lastname
read -p "last name: " lastname
echo -e "your first name is:${firstname}\n"
echo -e "your last name is:${lastname}\n"
```

# Linux黑客基础-57-Bash中常用快捷键（1）

1、Keyboard Shortcuts（bash中的常用快捷方式）

向上的光标键------调用最后一次执行的命令

ctrl+r　在历史命令中根据关键字查找指令进行调用，如果不匹配再按ctrl+r继续往下寻找

ctrl+z　把程序放在后台并停止运行

ctrl+c　终止当前命令的执行

ctrl+l　清屏

！！　重复上一条命令

command | less　允许你使用上下光标键滚动屏幕查看命令执行结果

!$（esc+.）重复上一个命令的最后有一个参数

ctrl+A　回到命令行的行首

ctrl+E　回到命令行的行尾

ctrl+U　删除光标前的所有内容，并且放到剪切板

ctrl+K　删除光标后的所有内容，并且放到剪切板

ctrl+Y　粘贴，配合ctrl+K和ctrl+U使用

ctrl+T　交换光标前后的字符

ctrl+W　删除光标前的一个单词或参数

ctrl+D　退出当前终端

ctrl+ <--　向左移动一个单词

ctrl+ >--　向右移动一个单词

# Linux黑客基础-59-Shell脚本编程（3）编写第一个黑客脚本

Your Very First Hacker Script: Scan for Open Ports

nmap-----网络扫描工具

Usage: nmap [Scan Type(s)] [Options] {target specification}

nmap［扫描类型] [扫描选项][扫描目标]

-sT：完全扫描（TCP的三次握手）

-p：指定扫描的端口

-oG：把扫描结果分类

MySQL：3306、FTP：21、远程桌面：3389

A Simple Scanner 一个简单的扫描器

nmap -sT 192.168.181.0/24 -p 3306 >/dev/null -oG MySQLscan

开发的nmap脚本

nmap Plain Text

```
#!/bin/bash
# This script is designed to find hosts with MySQL installed
nmap -sT 192.168.18.0/24 -p 3306 >/dev/null -oG MySQLscan
cat MySQLscan | grep open > MySQLscan2 |
cat MySQLscan2
```

# Linux黑客基础-60-Shell脚本编程（4）改进我们的扫描器

改进扫描器

使其不仅适用于您自己的网络。如果该脚本能够提示用户想要扫描的IP地址范围和要查找的端口

newnmap Plain Text

```
#!/bin/bash
# This script is designed to find hosts with MySQL installed
echo -n "please inout you scan network(eg:192.168.1.0-100)"
read ipnet
echo -n "please input you scan start ip(eg:1):"
read firstip
echo -n "please input you scan end ip(eg:100):"
read lastip
echo -n "please input you scan port(eg:80):"
read port
nmap -sT ${ipnet}${firstip}-${lastip} -p $port >/dev/null -oG script
cat script | grep open | awk '{print $2}' >newscript
cat newscript
```