BUUCTF [ACTF2020 新生赛]Exec 1

原创

Manba_77 于 2022-03-14 10:16:23 发布 1607 收藏

分类专栏： CTF 之 BUUCTF 文章标签： linux

本文链接：https://blog.csdn.net/MateSnake/article/details/123471468

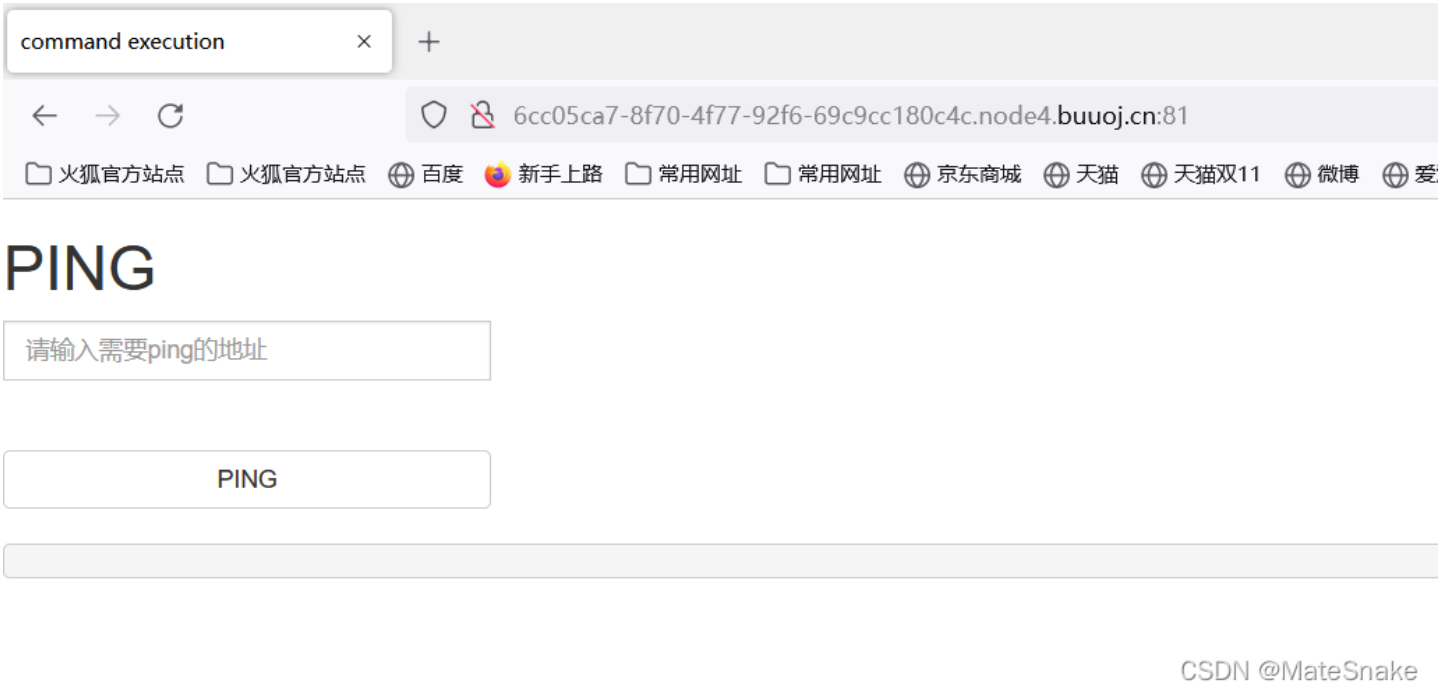
CTF 之 BUUCTF 专栏收录该内容

2 篇文章 0 订阅

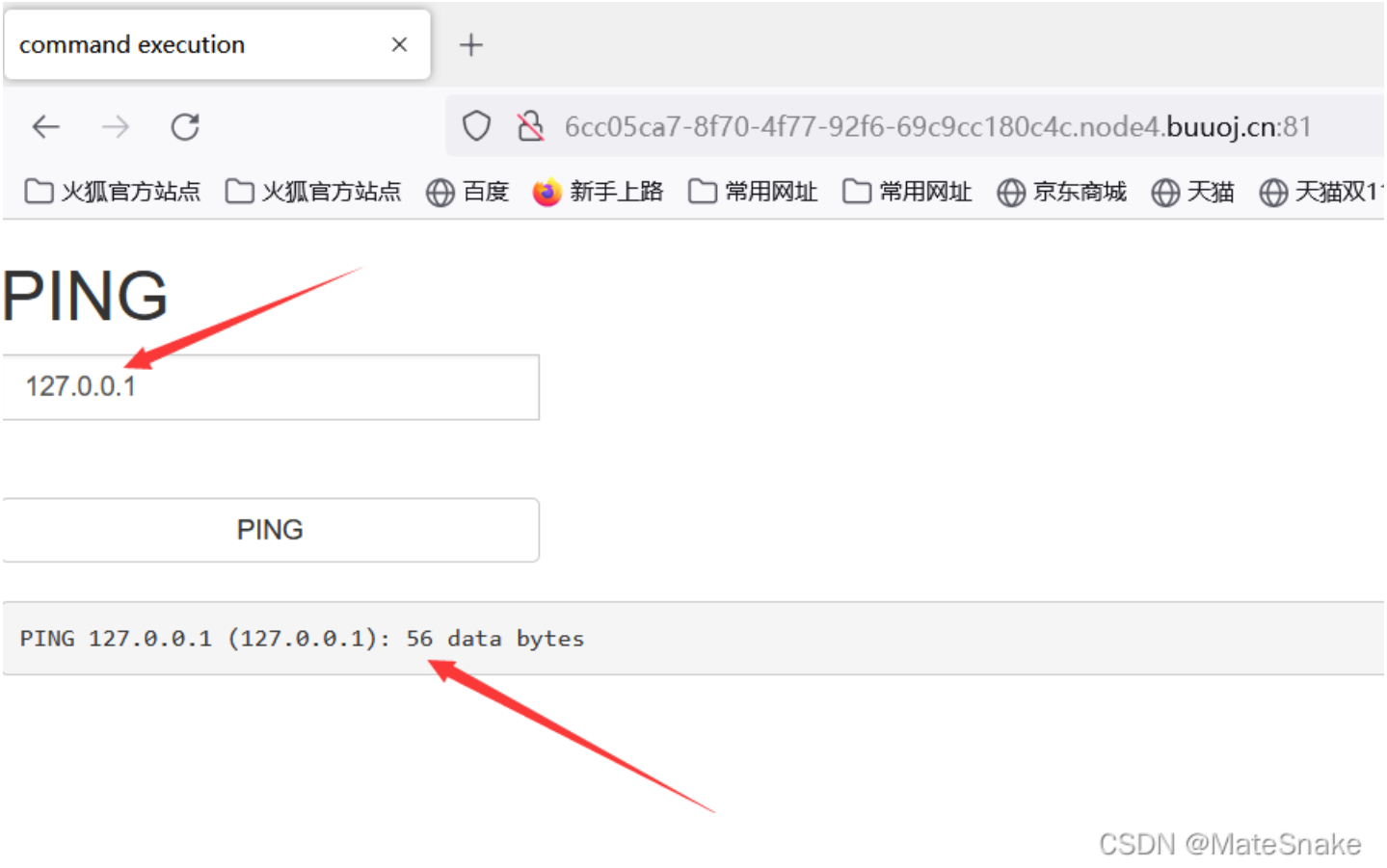
订阅专栏

开启题目


题目
解题快手榜
[ACTF2020 新生赛]Exec
1
感谢 Y1ng 师傅供题。
靶机信息
剩余时间: 10391s
http://6cc05ca7-8f70-4f77-92f6-69c9cc180c4c.node4.buuoj.cn:81
销毁靶机
靶机续期
已解锁
Flag
提交
CSDN @MateSnake


command execution
6cc05ca7-8f70-4f77-92f6-69c9cc180c4c.node4.buuoj.cn:81
火狐官方站点
火狐官方站点
百度
新手上路
常用网址
常用网址
京东商城
天猫
天猫双11
微博
PING
请输入需要ping的地址
PING
CSDN @MateSnake

先ping一下它自己



这里注意：

TTL表示您使用ping命令发送的数据包在网络中的持续时间。
TTL=56表示你的机器发送数据包到对方IP并确认，要花费56毫秒。
一般情况下，TTL=56表示对方是Windows 98或者是Linux操作系统

尝试使用管道符

第一种方法

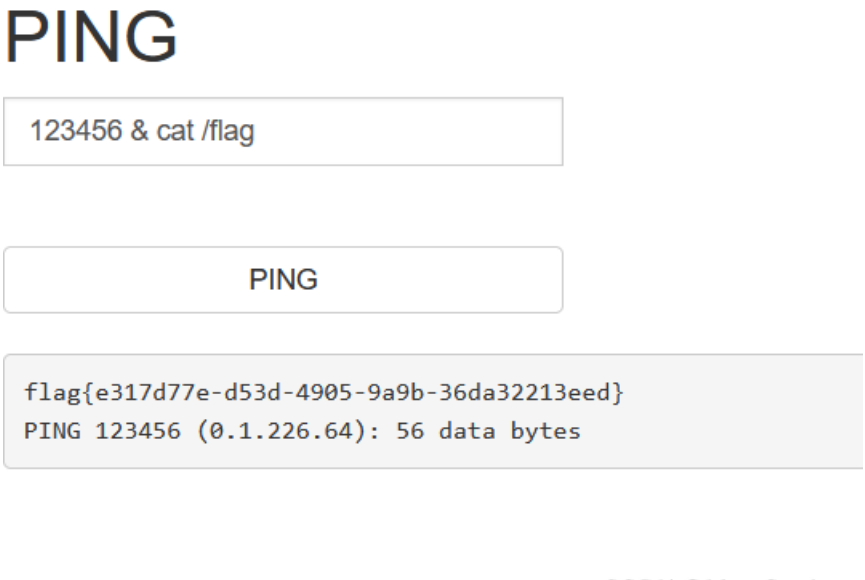
| 按位或
127.0.0.1 | cat /flag

第二种方法

|| 逻辑或 让||左边是执行错误的，这样它太会执行||右面的（这是计算机的惰性机制，只要前面执行正确了就不会再执行后面的了）
abc || cat /flag

第三种方法

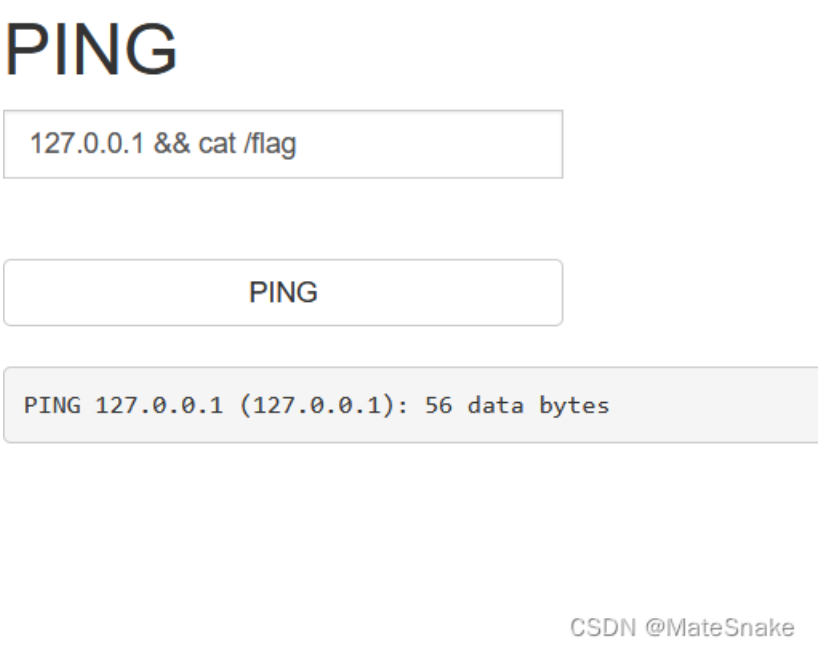
& 按位与 &前面和后面命令都要执行，无论前面真假
127.0.0.1 & cat /flag



第四种方法

&& 逻辑与 如果前面为假，后面的命令就不执行，如果前面为真则再执行后面命令，这样两条命令都会被执行

127.0.0.1 && cat /flag



但是没有出来结果，也不是很清楚什么原因

第五种方法

判断它可能是Linux系统，那么在Linux系统下；和&是一样的作用

127.0.0.1 ; cat /flag