

0x00前言

前几天参加HITB-XCTF的readfile。除了常规的：cat,tac,less,more,head,tail,nl tailf命令之外，收集了几个花式读文件内容的命令，可能只有CTF环境中才用得到吧！，记录分享一下。

Linux花式读取文件内容

ps:目标是获取flag.txt的内容

- **static-sh**读取文件：static-sh ./flag.txt等同于/???/?????-?? ./flag.txt

```
static-sh ./flag.txt
#■■■■■
./flag.txt: line 1: flag{this_is_a_test}: not found
# ■■■■
/???/?????-?? ./flag.txt
#■■■■■
./flag.txt: line 1: flag{this_is_a_test}: not found
```

- **paste**读取文件paste ./flag.txt /etc/passwd

```
paste ./flag.txt /etc/passwd
#■■■■■
flag{this_is_a_test}    root:x:0:0:root:/root:/bin/bash
                        daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
                        bin:x:2:2:bin:/bin:/usr/sbin/nologin
                        sys:x:3:3:sys:/dev:/usr/sbin/nologin
                        sync:x:4:65534:sync:/bin:/bin/sync
//■■■
```

- **diff**读取文件diff ./flag.txt /etc/passwd

```
diff ./flag.txt /etc/passwd
#■■■■■
1c1,45
< flag{this_is_a_test}
\ No newline at end of file
---
> root:x:0:0:root:/root:/bin/bash
> daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
> bin:x:2:2:bin:/bin:/usr/sbin/nologin
> sys:x:3:3:sys:/dev:/usr/sbin/nologin
> sync:x:4:65534:sync:/bin:/bin/sync
```

- **od**读取文件od -a ./flag.txt

```
od -a ./flag.txt
#■■■■■
0000000  f  l  a  g  {  t  h  i  s  _  i  s  _  a  _  t
0000020  e  s  t  }
0000024
```

- **bzmore**读取文件bzmore ./flag.txt

```
bzmore ./flag.txt
#■■■■■
-----> ./flag.txt <-----
flag{this_is_a_test}
```

- **bzless**读取文bzless ./flag.txt

```
echo `bzless ./flag.txt`
#■■■■■
-----> ./flag.txt <----- flag{this_is_a_test}
```

点击收藏 | 1 关注 | 2

[上一篇 : Blockchain can be...](#)
[下一篇 : VulnHub|渗透测试入门 \(三\)](#)

1. 0 条回复
- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#)
[关于社区](#)
[友情链接](#)
[社区小黑板](#)