# Linux环境下常见漏洞利用技术

君莫笑呵呵哒 / 2017-03-21 03:41:00 / 浏览数 8938 安全技术 资源分享 顶(0) 踩(0)

---

记得以前在drops写过一篇文章叫 linux常见漏洞利用技术实践 ,现在还可以找得到(https://woo.49.gs/static/drops/binary-6521.html),
不过当时开始学pwn不久,很多理解有偏差.
现在时间过去了一年多,还经常有朋友发私信问我其中的实例程序还在不在,很遗憾我自己也没有了哈:)
前不久要给别人做个这方面的培训,于是写了这个ppt,其中有我自己一些粗浅的理解,在此分享给大家,

在ppt中,基本每一种技术我都附了一个实例及对应的exp.都打包在一起了.
其中引用了一些前辈的内容,感谢他们的分享.
ppt中有我的联系方式,欢迎大家和我交流

1 常见工具的使用
1 IDA
2 gdb
3 peda
4 rp++,ROPGadget
5 pwntools
6 libcdb.com,libc-database
7 系统自带小工具
2 程序的分析步骤
3 常见漏洞类型
1 栈溢出
2 格式化字符串漏洞
3 整数漏洞
4 堆漏洞
1 堆溢出
2 double free
3 UAF
4 其他
4 常见防御技术及绕过方法
1 Canary
2 NX
3 ASLR
4 RELRO
5 PIE
5 一些其他值得注意的地方

examples.zip (3.6 MB) 下载附件
Linux环境下常见漏洞利用技术.pptx.zip (3.6 MB) 下载附件
点击收藏 | 1 关注 | 1
上一篇：利用 PHP7 的 OPcache... 下一篇：利用思维导图快速读懂框架和理清思路之禅道

1. 39 条回复


cakycookie 2017-08-08 15:01:46

好好学习

0 回复Ta


0day 2017-08-11 09:27:15

0 回复Ta

---


seize 2017-08-12 10:28:21

xiexie

0 回复Ta

---


y0ung 2017-09-01 02:58:03

学习学习

0 回复Ta

---


baselinesafe 2017-09-01 03:24:55

怎么下载呢！朋友啊！

0 回复Ta

---


酸奶、 2017-09-01 07:54:39

6666666666666666

0 回复Ta

---


鲸鱼 2017-09-01 07:58:23

好好学习！！！

0 回复Ta

---


溜马仔 2017-09-01 08:54:22

非常感谢。

0 回复Ta

---


test123 2017-09-01 09:33:39

好好学习了。谢谢

0 回复Ta

---


如风 2017-09-03 01:55:46

windows或许对于很多人而言都有熟悉，现在有了Linux。给力

0 回复Ta

---


ih0cker 2017-09-04 02:23:35

谢谢分享

0 回复Ta

---


hellocat 2017-09-04 09:06:28

学习学习

0 回复Ta

---


goodcat666 2017-09-04 15:45:56

666666666666666

0 回复Ta

---


goodcat666 2017-09-04 15:48:30

怎么下载呢！朋友啊！

0 回复Ta

---


涨姿势 2017-09-27 09:17:20

谢谢~

0 回复Ta

---


小马安全 2017-09-28 00:43:22

谢谢分享

0 回复Ta

---

岁月别催 2017-09-28 03:13:21

多谢楼主

0 回复Ta

---

岁月别催 2017-09-28 03:14:41

链接失效了 楼主还能在分享一份吗

0 回复Ta

---

c0de 2017-09-29 02:57:55

强大，正好需要

0 回复Ta

---


hades 2017-09-29 03:23:57

没有私效吧

0 回复Ta

---


tankesun 2017-09-29 05:58:51

TKS

0 回复Ta

---


haha182 2017-09-29 14:12:22

谢谢分享

0 回复Ta

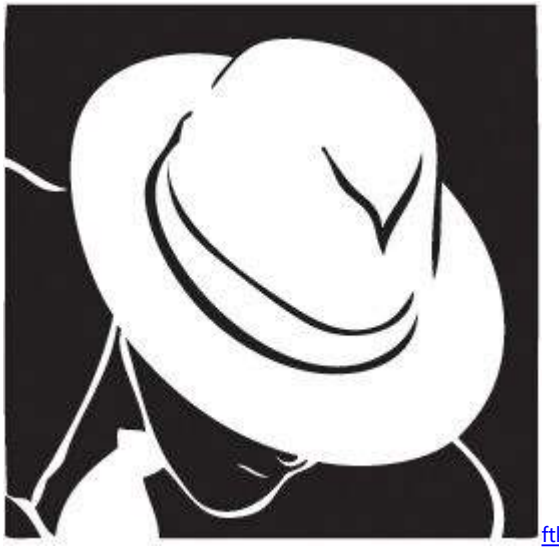
---


jinglingshu 2017-09-30 03:24:48

谢谢分享

0 回复Ta

---


ftkahzmodan 2017-09-30 03:44:56

膜

0 回复Ta

---


萌萌哒的小白 2017-10-13 14:37:54

感谢分享

0 回复Ta

---


浪子彦 2017-10-13 15:56:49

在哪下载啊。

0 回复Ta

---


pass 2017-10-18 19:01:05

赶紧get

0 回复Ta

---


pass 2017-10-18 19:01:27

411111

0 回复Ta

---


小马安全 2017-10-19 00:35:33

谢谢分享

0 回复Ta

---


ghostman 2017-10-19 01:10:34

学习学习

0 回复Ta

---


huraway 2017-10-19 15:16:59

Linux环境下常见漏洞利用技术好棒

0 回复Ta

---


huraway 2017-10-19 15:19:13

好好学习了

0 回复Ta

---


le0nis 2017-10-20 07:46:18

大牛都转战这里了啊 膜拜

0 回复Ta

---


wilsonlee1 2017-10-20 08:53:28

嗯 ~所以要前排围观ing

0 回复Ta

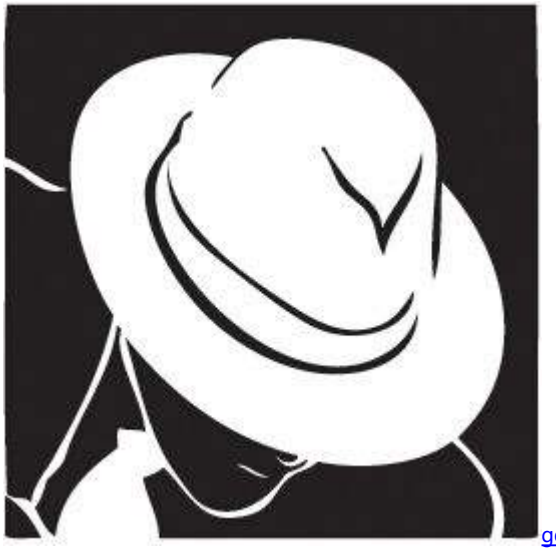
---


tren 2017-10-21 14:28:43

谢谢~

0 回复Ta

---


gdyhw 2017-10-26 06:07:21

6666

0 回复Ta

---


三叶草 2017-10-26 07:25:18

感谢

0 回复Ta

---


鹰城广场 2017-10-28 08:49:24

在哪下载的

0 回复Ta

---


niexinming 2017-12-15 17:03:35

学习了

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