Technology Knowledge Base 2018-12

by bugnofree

Publish → 2019-01-05 Update → 2019-03-02

- 2018-12-18 https://github.com/corkami/pocs/...: MD5 和 SHA1 哈希碰撞 explotion
- 2018-12-19 https://googleprojectzero.blogsp...: 搜索程序的静态链接库中有漏洞的函数

```
文章比较长，看了大半个晚上才看完．这篇文章主要是结合了机器学习的方法进行相
似函数的提取对比.对实践而言，新的程序中往往用的是旧的开源库代码,如果发现了
一个已知开源库代码中漏洞，那么可以对流行的程序使用该文提到的方法进行测试，
如果被测试程序中发现了相应函数，那么就发现漏洞了．这一点比较有意思.对研究
而言，文末提出了进一步的研究方向，如果感兴趣可以关注一下.
```

- 2018-12-20 https://github.com/86hh/DreamLoa...: cross-platform PE loader

```
DreamLoader by hh86

some of its features:
- simple cross-platform PE loader, x86/x64 compatible code in a single execution path
- supports both Intel 386 and AMD64 Portable Executable files
- supports files with/without import table
- supports files with/without reloc table
- uses CRCs instead of API names to reduce code size

yes, this is HLDR32/HLDR64 from PE2SHC by hasherezade, but combined!
it's an idea I had when I proposed HLDR32 but it was discarded. :( now I have it. :)
it needs more testing, if a bug is found, let me know.
```

- 2018-12-21 https://github.com/Hack-with-Git...: A collection of various awesome lists for hackers, pentesters and security researchers
- 2018-12-22: https://github.com/tldr-pages/tl...: Linux用户的简化手册

```
A collection of simplified and community-driven man pages.
```

- 2018-12-23:https://github.com/mattgodbolt/c...

```
Run compilers interactively from your web browser and interact with the
assembly - 在浏览器中运行编译器,很方便测试各种编译器编译的代码.
PPT 介绍可以在这里找到: @[https://mattgodbolt.github.io/ce-lightning/]
```

- 2018-12-24 https://blog.techorganic.com/201...: 64-bit Linux stack smashing tutorial
- 2018-12-25 http://scz.617.cn:8/unix/2018121...: 未知网络服务分析之调试技巧
- 2018-12-26 https://github.com/joxeankoret/p...: pigaios : 一个用于将源代码直接和二进制文件进行比较的工具.

```
这个应该对二进制文件逆向很有帮助, 但我还没时间来试.
作者在 zeronights 会议上的 PPT(pigaios -
Diffing-C-source-codes-to-binarie.pdf) 我直接上传到群里,
如果大家有时间可以看看简要了解一下.
```

- 2018-12-27 https://lwn.net/Articles/631631/: How programs get run: ELF binaries
- 2018-12-28 https://justinmeiners.github.io/...: Write your Own Virtual Machine
- 2018-12-29 https://www.hackerspace.gr/wiki/...: Linux Kernel Namespaces
- 2018-12-30 https://github.com/j00ru/windows...: Windows System Call Tables
- 2018-12-31 https://hamberg.no/erlend/posts/...: A nice, little known C feature: Static array indices in parameter declarations

```
在C语言数组参数中使用静态数组的一个小trick,我第一次看到,大家可以看一下～
```