Technology Knowledge Base 2019-03

by bugnofree

Publish → 2019-03-01 Update → 2019-04-10

Technology Knowledge Base 主页 https://github.com/ikey4u/tkb, 欢迎 star 或通过二维码入群.

本期所提到的有附加资源下载地址为 https://github.com/ikey4u/tkb/tr..., 资源前缀为日期形式 `2019-03-xx` .

- 2019-03-01 http://pages.cs.wisc.edu/~remzi/...

  Operating Systems: Three Easy Pieces

  一本优秀的开源操作系统书籍.

  PDF 见 datum 目录.

- 2019-03-02 http://man7.org/conf/lca2013/IPC...

  An introduction to Linux IPC

  man7 手册维护者, The linux programming interface 的作者讲解 Linux 进程间通信方式.

  下面的分享来自 @SmoKER

  ```
  根据公有云的威胁检测实践,做了个安全数据分析方向的tutorial,欢迎有兴趣入坑的同学勾搭
  ppt http://t.cn/EfssvNn
  freebuf http://t.cn/EfZrMQj
  鬼麦子师傅的域名监控:https://github.com/guimaizi/get_domain
  ```

PDF 见 datum 目录.

- 2019-03-03 https://techblog.mediaservice.ne...

  IoT Hacking 之 UART 协议

- 2019-03-04 https://github.com/ikey4u/tkb/bl...

  网络是怎样连接的.

  当你在浏览器中输入了网址到显示出网页内容, 这中间到底发生了什么?

  日本人写的一本书, 通俗易懂. 非扫描版本.

  - 来自 @z3r0yu https://github.com/bitsadmin/wes...

    Just released Windows Exploit Suggester - Next Generation! Based on the output of Windows' systeminfo.exe utility, this tool provides you with the list of vulnerabilities the OS is vulnerable to, including any exploits for these vulnerabilities. Get it at: https://t.co/juCqs7yyyW https://t.co/TmNO0QW07E

- 2019-03-05 https://mislove.org/teaching/cs4...

  美国东北大学的计算机网络基础课程, 这是其讲解 NAT 网络的课件 2019-03-05.Network Address Translation (NAT).pdf.

  可以在闲暇时间看一下, 有助于内网反向穿透原理的理解.

- 2019-03-06 https://www.rsaconference.com/wr...

  RSA Conference 2019

  4G to 5G Evolution: In-Depth Security Perspective

- 2019-03-07 https://github.com/emcrisostomo/...

  fswatch是一个跨平台(linux, mac, windows, freebsd)的文件更改监视,获取通知警报在指定的文件或目录的内容被改变或修改.

它在不同的操作系统上执行四种类型的监视器,例如:

- 基于Apple OS X的文件系统事件API的监视器构建.
- 基于kqueue的显示器,目前在FreeBSD的4.1通知接口还支持许多* BSD系统,OS X的包容性.
- 基于Solaris内核的文件事件通知API的监视器及其附加功能.
- 基于inotify的监视器,一个显示文件系统对应用程序修改的内核子系统.
- 基于ReadDirectoryChangesW的监视器,它是记录更改为目录的Windows API.
- 定期检查文件系统状态,在内存中保存文件修改时间,以及手动确定文件系统更改(可在任何地方使用stat)的监视器.

fswatch的特点

- 支持几种特定于OS的API
- 允许递归目录监视
- 使用包含和排除正则表达式执行路径过滤
- 支持自定义记录格式
- 此外,它支持周期性空闲事件

- 2019-03-08 https://github.com/Genymobile/sc...

  Display and control your Android device

  在电脑上显示和控制 Android 设备

- 2019-03-09 http://jeffe.cs.illinois.edu/tea...

  昨天在网上看到的, 一份在 HackerNews 上获得点赞上千的算法讲义, 来自20年教学经验的UIUC计算机教授

- 2019-03-10 https://github.com/wcventure/Fuz...

  近期关于Fuzzing的Paper集合,还挺详细的

  来自 @z3r0yu

- 2019-03-11

    - z3r0yu http://zeroyu.xyz/2019/03/11/NAV...

      以后准备每周更一篇论文笔记,大概会涉及Web安全,Fuzz和sandbox这三个方面.

      今天分享第一篇论文笔记--NAVEX: Precise and Scalable Exploit Generation for Dynamic Web Applications,此论文发表在27th USENIX Security Symposium,此研究受到DARPA 支持.它是一种结合静态分析和动态分析来对WebApp自动化审计并构造攻击Exp的方案.

      方案思路很棒,如果研究自动化代码审计的小伙伴可以看下这篇.

    - Network Forensics, Wireshark Basics, Part 1 https://www.hackers-arise.com/si...

- 2019-03-12 https://blog.ret2.io/2017/11/16/...

  Dangers of the Decompiler A Sampling of Anti-Decompilation Techniques

  这里有一个中文版本: https://xz.aliyun.com/t/1602

  另外对于 Positive SP 的解决, 这里提供了一种实践的方法

  Fixing "positive SP value has been found" error in IDA Pro https://arrowd.name/posts/2016-1...

- 2019-03-13 https://codeforces.com/blog/entr...

  C++ Tricks

  codeforces 社区给的各种 C++ 编码技巧, 比较有意思.

- 2019-03-14 https://liberty-shell.com/sec/20...

  DLL Hijacking & Ghidra

- 2019-03-15 https://m.habr.com/en/post/44331...

  Writing a wasm loader for Ghidra. Part 1: Problem statement and setting up environment

- 2019-03-16 http://linuxcommand.org/tlcl.php

  The Linux Command Line A Book By William Shotts

  中文版见这里 http://billie66.github.io/TLCL/b...

- 2019-03-17 https://blog.ret2.io/2018/06/19/...

  Timeless Debugging of Complex Software Root Cause Analysis of a Non-Deterministic JavaScriptCore Bug

  - https://github.com/c0ny1/chunked...

    Burp suite 分块传输辅助插件<--过waf

  - https://github.com/lcatro/How-to...

    一些阅读源码和Fuzzing 的经验.. <--应该算是编写fuzz的系列教程了,还在更新中

- 2019-03-18 https://www.cs.northwestern.edu/...

  C++ Iterators

- 2019-03-19 http://virtical.upv.es/pub/sc13....

  The Evolution of the ARM Architecture Towards Big Data and the Data-Centre

  pdf 保存于 github 的 datum 目录, 文件名称为

  2019-03-19.The.Evolution.of.the.ARM.Architecture.Towards.Big.Data.and.the.Data-Centre.pdf

- 2019-03-20
  - ARMv8-A A64 ISA Overview

    64bits ARM 汇编介绍, PDF 参见 datum/2019-03-20.RMv8_InstructionSetOverview.pdf

    - http://zeroyu.xyz/2019/03/20/Spo...

      今日分享一篇sandbox方面的笔记--Spotless Sandboxes: Evading Malware Analysis Systems using Wear-and-Tear Artifacts, 原文发表在2017 IEEE Symposium on Security and Privacy (SP).文章从攻防双方的博弈出发, 在攻击者角度将一些artifact的使用痕迹作为特征,使用决策树分类器进行训练来规避沙箱环境; 在防御者角度帮助沙箱系统进行改进,使其具有更逼近真实用户环境.

- 2019-03-21

  今天推荐两个在线文件传输工具

    - ffsend https://github.com/timvisee/ffse...

      Easily and securely share files from the command line. A fully featured Firefox Send client.

      这一个是火狐浏览器自带的功能, 有人用 rust 写了一个命令行工具.

    - transfer.sh https://transfer.sh/

      Easy and fast file sharing from the command-line.

      这是一个运行了 4 年+ 的在线网站, 十分良心.

      可以网页传输, 也可以命令行传输.

- 2019-03-22 http://flatassembler.net/index.p...

  FASM (flat assembler)

  开源的 x86, x86-64 汇编器.

- 2019-03-23 https://medium.freecodecamp.org/...

  Follow these steps to solve any Dynamic Programming interview problem

- 2019-03-24 https://nullprogram.com/blog/201...

  Endlessh: an SSH Tarpit

- 2019-03-25 http://speech.ee.ntu.edu.tw/~tlk...

  台湾大学李宏毅教授 2019 年机器学习视频.

  每一栏都标注了新增课程, 提供了课件和视频. 课程目录如下

  - 回归, 梯度下降
  - 分类, 逻辑回归, 错分类的原因
  - 深度学习, 反向传播, +异常检测
  - 卷积神经网络(CNN), Keras, +对抗样本攻击
  - 训练深度学习模型, +可解释 AI
  - 循环神经网络, +Order LSTM
  - Ensemble
  - 半监督学习,迁移学习, +终身学习(Life-long learning)
  - +元学习
  - seq2seq, +Transformer
  - +Few/Zero shot learning
  - 无监督学习, +BERT
  - 强化学习, +进一步讲解强化学习
  - +网络压缩
  - 生成对抗网络, +GLOW
  - +无监督域适应
  - 为什么使用深度学习, +深度学习理论

- 2019-03-26 https://web.stanford.edu/class/c...

  CS9: Problem-Solving for the CS Technical Interview

- 2019-03-27 https://github.com/NanXiao/strac...

  Strace little book

- 2019-03-28 https://research.checkpoint.com/...

  Karta – Matching Open Sources in Binaries

- 2019-03-29 https://github.com/getify/You-Do...

  You Dont Know JS

  - "Up & Going", https://github.com/getify/You-Do...
  - "Scope & Closures", https://github.com/getify/You-Do...
  - "this & Object Prototypes", https://github.com/getify/You-Do...
  - "Types & Grammar", https://github.com/getify/You-Do...
  - "Async & Performance", https://github.com/getify/You-Do...
  - "ES6 & Beyond", https://github.com/getify/You-Do...

- 2019-03-30 https://lolbas-project.github.io...

  Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts)

- 2019-03-31 http://www.muppetlabs.com/~bread...

  Bootstrapping Understanding An Introduction to Reverse Engineering

  题外话: 值得一提的是, 这个文章里面的代码样式十分新颖, 用一个表格设计了一个独特的代码展示样式