Technology Knowledge Base 2019-11

by bugnofree

Publish → 2019-11-01 Update → 2019-12-06

TKB 首页: https://github.com/ikey4u/tkb, 欢迎 star.

- 2019-11-01 https://reverse.put.as/2019/10/2...

  Crafting an EFI Emulator and Interactive Debugger

- 2019-11-02 https://gravitational.com/blog/s...

  SSH Handshake Explained

- 2019-11-03 https://rednaga.io/2016/09/21/re...

  Reversing GO binaries like a pro

- 2019-11-04 https://github.com/ownthink/Know...

  最大规模1.4亿中文知识图谱

- 2019-11-05 https://github.com/Linzaer/Ultra...

  1MB轻量级人脸检测模型

- 2019-11-06 https://github.com/SecWiki/sec-c...

  安全四维导图

- 2019-11-07 https://medium.com/@lerner98/rag...

  Rage Against the Maschine

- 2019-11-08 https://maxkersten.nl/binary-ana...

  Corona DDoS bot

- 2019-11-09 https://juejin.im/post/5dc4aa4be...

  为IDA加载调试符号

- 2019-11-10 https://github.com/emsec/hal

  HAL – The Hardware Analyzer

- 2019-11-11 https://webserver2.tecgraf.puc-r...

  Creating the smallest possible PE executable

- 2019-11-12 https://duanqz.github.io/2016-04...

  Android Local Manifests机制的使用实践

- 2019-11-13 https://www.xda-developers.com/a...

  Developers: It's super easy to bypass Android's hidden API restrictions

- 2019-11-14 https://d4mianwayne.github.io/po...

  Binary Exploitation - Format String + Buffer Overflow Vulnerability

- 2019-11-15 https://github.com/xrkk/awesome-...

  跟IDA Pro有关的资源收集.当前包括的工具个数450左右,并根据功能进行了粗糙的分类.部分工具添加了中文描述.

- 2019-11-16 https://blog.trailofbits.com/201...

  Destroying x86_64 instruction decoders with differential fuzzing

- 2019-11-17 https://nathandavison.com/blog/a...

Abusing HTTP hop-by-hop request headers

- 2019-11-18 https://medium.com/tenable-techb...

  RouterOS: Chain to Root

- 2019-11-19
  - HTTP parameter discovery suite https://github.com/s0md3v/Arjun
  - The meaning of refs and refspecs GIT 提交中的 refs 和 refspecs 含义 https://git.seveas.net/the-meani...
- 2019-11-20 https://securelist.com/hacking-m...

  Hacking microcontroller firmware through a USB

- 2019-11-21 https://www.peerlyst.com/posts/t...

  The Practical Guide to Radio Waves Hacking

- 2019-11-22 https://github.com/CoatiSoftware...

  Sourcetrail - free and open-source interactive source explorer

- 2019-11-23 https://rust-lang.github.io/api-...

  Rust API Guidelines

- 2019-11-24 https://www.youtube.com/playlist...

  Compilers and interpreters 课程

- 2019-11-25 https://repnz.github.io/posts/au...

  Autochk Rootkit Analysis

- 2019-11-26 https://github.com/pr0cf5/kernel...

  kernel exploit practice: SMEP + KPTI bypass

- 2019-11-27 https://n4r1b.netlify.com/en/pos...

  Understanding WdBoot (Windows Defender ELAM)

- 2019-11-28 https://blog.flanker017.me/text-...

  Text-To-Speech speaks pwned

  expolit code: https://github.com/flankerhqd/vendor-android-cves/tree/master/SMT-CVE-2019-16253

- 2019-11-29 https://dayzerosec.com/posts/ana...

  Analyzing Android's CVE-2019-2215 (/dev/binder UAF)

- 2019-11-30 https://checkra.in/

  iPhone 5s - iPhone X, iOS 12.3 and up jailbreak