

## 常见的需要用的网站(工具)

[hyperv symbol](#)

[guest调试机子支持 一代和二代](#)

[vmx.h的下载\(用于静态分析\)](#)

[hyperv hypercall的识别](#)

[hyperv hypercall的文档网站\(TLFS\)](#)

[bindiff调试小技巧\(目的是为了装载strcpy等公用函数的符号\)](#)

```
; enum HYPERV_STRUCTS, mappedto_396
Self          = 0
CpuIndex      = 8
CurrentThread  = 38h
LogicalCpuIndex = 8080h
CurrentVP     = 82E0h
IDT           = 8340h
GDT           = 8348h
CurrentPartition = 83A8h
CurrentVMCS   = 18480h
```

## 常见的需要用的网站(学习)

[first step to hyper-v\(理论\)](#)

[Virtualization Based Security part2\(理论\)](#)

[Virtualization Based Security part1\(理论\)](#)

[VBS\\_Internals.pdf\(理论\)](#)

[Battle of SKM and IUM\(理论\)](#)

[Ring 0 to Ring -1 Attacks\(理论\)](#)

[A Dive in to Hyper-V Architecture and Vulnerabilities\(理论 tensec演讲的ppt有翻译\)](#)

[Hardening Hyper-V through offensive security research\(调试目标\)](#)

[Hyper-V vmswitch.sys VmsMpCommonPvtHandleMulticastOids Guest to Host Kernel-Pool Overflow\(调试\)](#)

[Windows 10 Device Guard and Credential Guard Demystified\(理论\)](#)

[Hyperv debugging 环境设置\(调试\)](#)

[Hyper-v Internal\(调试\)](#)

## 一些厉害的师傅(hyper-v相关)的twitter

[peter老师](#)

[AmarSaar老师](#)

Alex老师