管中窥豹-

小谈云平台虚拟化安全

caiyuguang@360.cn
Qihoo360 cloud securtiy team

关于我

蔡玉光
奇虎360云安全架构师/负责人

接触信息安全10余年，6年的安全从业经验。
曾就职于东方微点，反病毒、主动防御研发。
渗透测试、二进制安全领域专家。

目录

IDCC

- 管中窥豹
- 什么是虚拟化
- 渗透虚拟化
- 虚拟化安全之道

目录

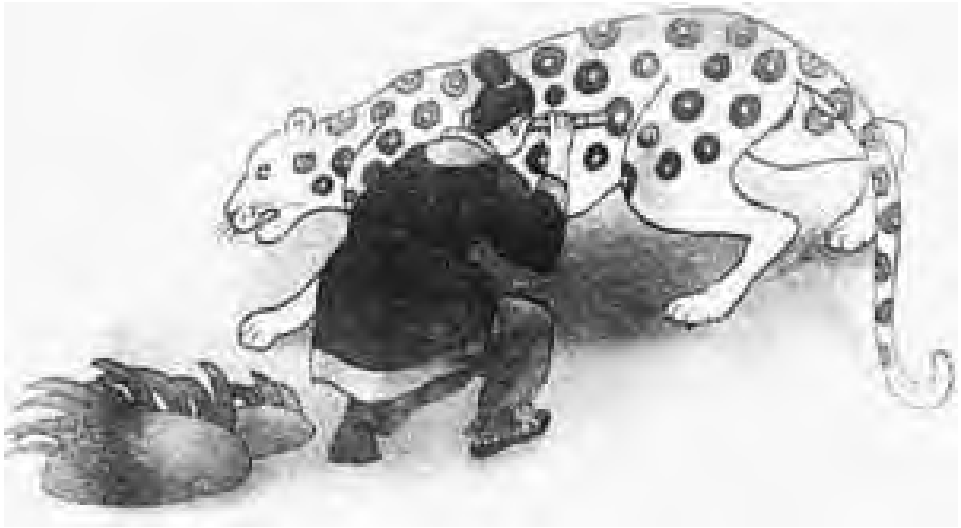
IDCC

- 管中窥豹
- 什么是虚拟化
- 渗透虚拟化
- 虚拟化安全之道

管中窥豹

IDCC

- 渗透测试思维



- to be or not to be?

目录

IDCC

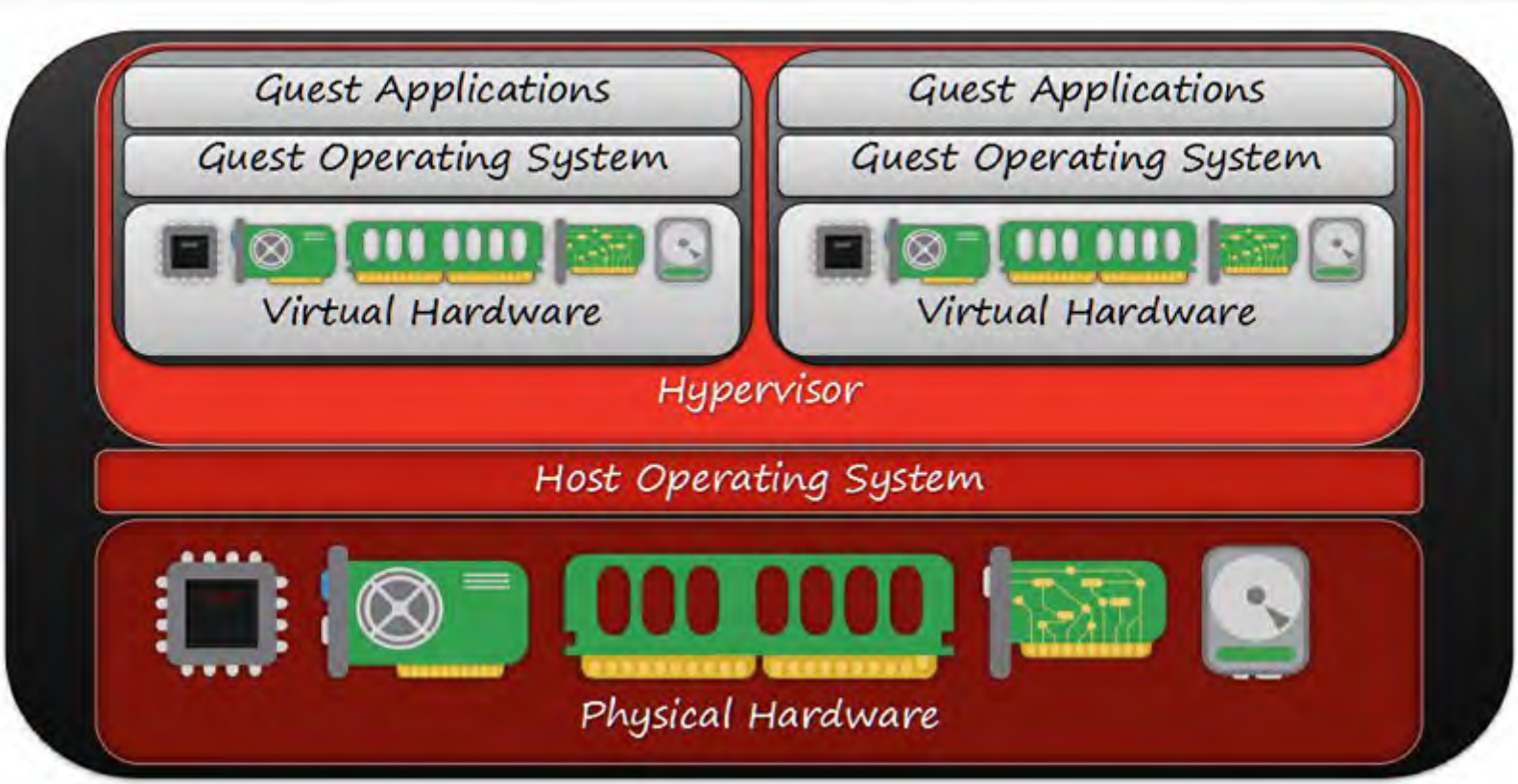
- 管中窥豹
- 什么是虚拟化
- 渗透虚拟化
- 虚拟化安全之道

什么是虚拟化

IDCC

- 软件用来创建模拟型的硬件平台
  - 可以模拟网卡、显卡、硬盘等
  - 可以复制创建
  - 可以由hypervisor来管理
- 软件和硬件的可解耦
  - 构建一个虚拟层
  - 提供个类型的硬件支持

什么是虚拟化


Guest Applications
Guest Operating System
Virtual Hardware
Guest Applications
Guest Operating System
Virtual Hardware
Hypervisor
Host Operating System
Physical Hardware

目录

IDCC

- 管中窥豹
- 什么是虚拟化
- 渗透虚拟化
- 虚拟化安全之道

渗透虚拟化 CVE-2015-3456

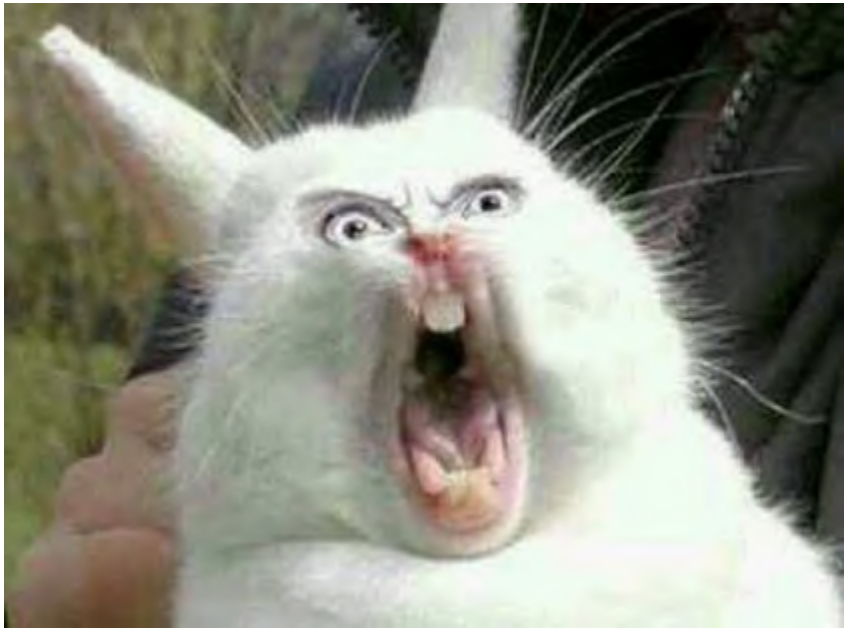
IDCC

HELLO WORLD! I'M VENOM.

渗透虚拟化 CVE-2015-3456

IDCC

NO! ……



渗透虚拟化 CVE-2015-3456

IDCC

漏洞预警：“毒液（VENOM）”漏洞影响全球数百万虚拟机安全（附POC）

JackFree +10 共51079人围观，发现11个不明物体 编辑 举报

数据中心存在Venom漏洞 黑客可渗透到每一台设备

2015年05月15日04:40 来源：赛迪网 手机看新闻

VENOM：比 Heartbleed 还危险的虚拟机漏洞

作者： SANJI FENG 2015 年 5 月 14 日, 下午 4:00

F 福布斯中文网

【Venom漏洞可能打开云端的潘多拉魔盒】这是一个被安全
液）的漏洞，存在于虚拟软盘驱动器的代码当中，这些代码
被很多云服务提供商所使用，但不要惊慌，它不会造成太大

渗透虚拟化 CVE-2015-3456

IDCC

Stop it! Batman

渗透虚拟化 CVE-2015-3456

IDCC

Sorry! I am busy...

渗透虚拟化 CVE-2015-3456

IDCC

你知道遗憾是什么感觉吗

渗透虚拟化 CVE-2015-3456

IDCC

- CrowdStrike的Jason Geffner发现开源仿真器QEMU中一个和虚拟软盘控制器相关的安全漏洞，代号VENOM，CVE编号为CVE-2015-3456

- 在QEMU实现的虚拟软盘控制器代码中在对Fdctrl数据结构的访问中存在fifo数组下标(pos/index)访问校验不严，导致可以构造特定I/O端口访问操作来实现数组的越界访问

- 很拗口...

Thank you!