
ISC
2015
中国互联网安全大会
360互联网安全中心
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
云安全论坛

云虚拟化系统的漏洞挖掘技术

演讲人：唐青昊

职务：**360 Marvel Team** 负责人

未知攻 焉知防

团队介绍

国内**首支**虚拟化安全研究团队（**Marvel Team**），研究内容为云安全领域的虚拟化平台**攻防技术**，致力于**保持领先**的脆弱性安全风险发现和防护能力，针对主流虚拟化平台提供如下工具和解决方案。

–漏洞挖掘系统

–逃逸攻击工具

支持docker，xen，kvm

–宿主机加固解决方案

拒止虚拟机逃逸

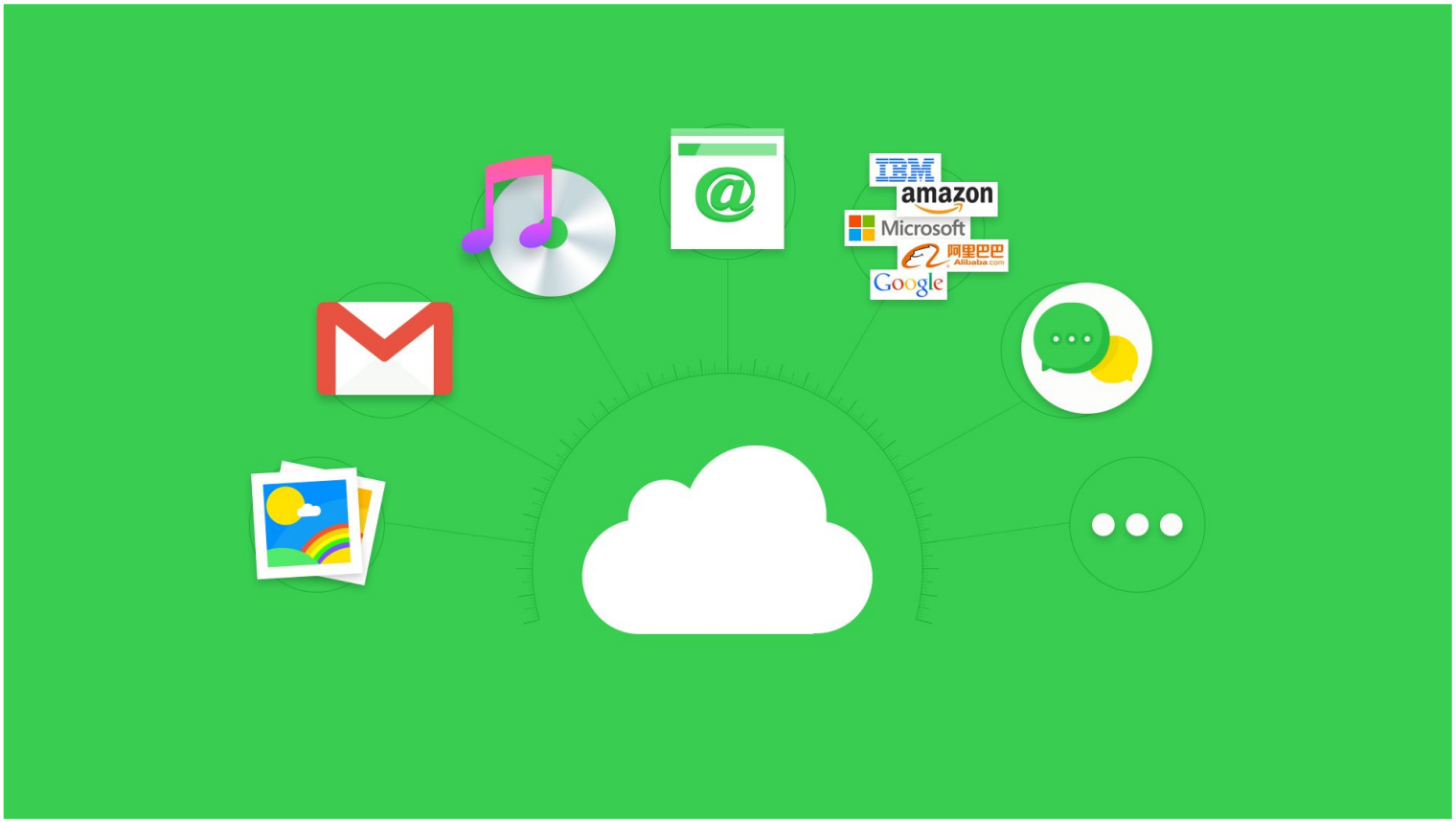
无代理查杀虚拟机

议程

- 脆弱性简介
- 网卡设备漏洞挖掘
- 测试框架

脆弱性简介

云计算



虚拟化系统

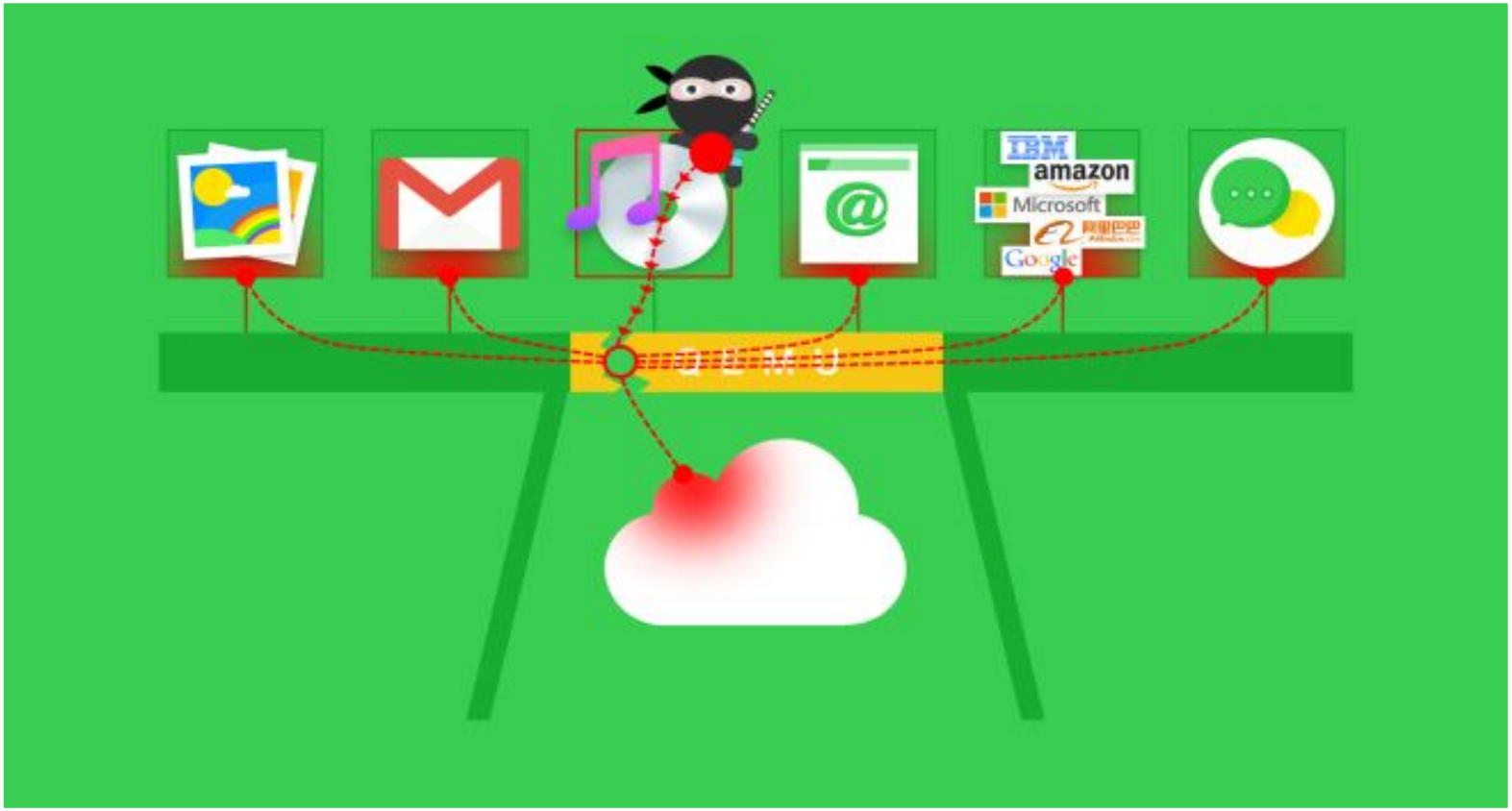
国内主流

- **xen**
- **kvm**
- **vmware**系列

功能

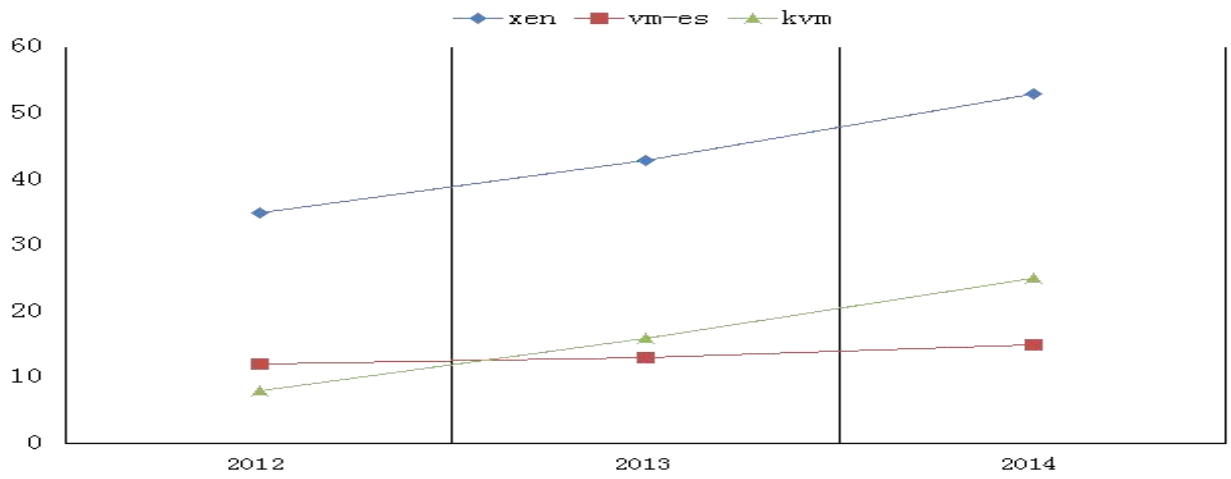
- 量化分配
- 灵活调度

虚拟机逃逸



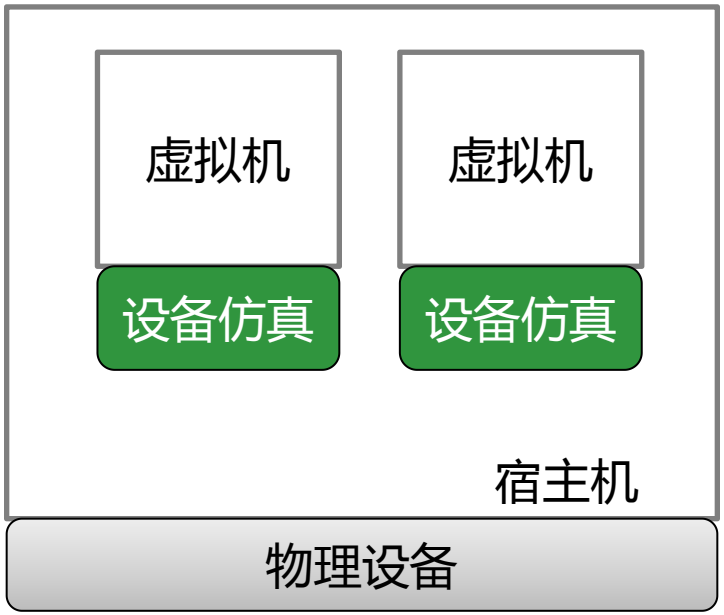
脆弱性发展趋势

	xen	vm-es	kvm	Total
2012	35	12	8	**50**
2013	43	13	16	**72**
2014	53	15	25	**103**



差异

普通服务器



虚拟化服务器

指令仿真缺陷

- CVE-2012-0217 XEN SYSRET 指令漏洞
- CVE-2014-3610 KVM 指令解码漏洞

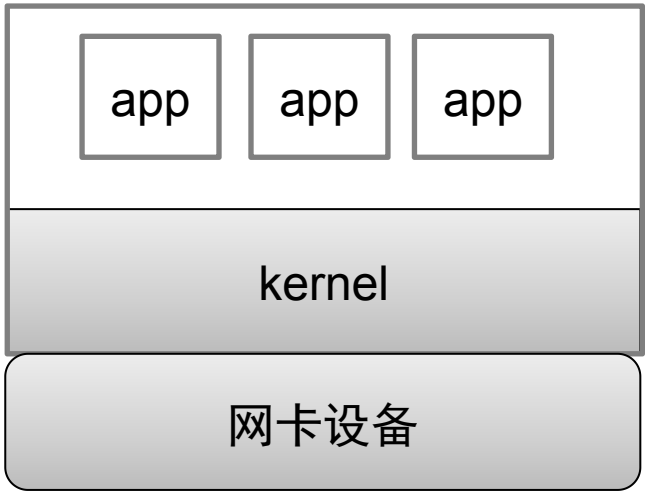
外设处理缺陷

- 毒液漏洞
- [360 0day] qemu e1000 设备漏洞
- [360 0day] vmware e1000网卡设备漏洞
- More 0days

网卡设备漏洞挖掘

仿真器原理

- 用户空间
  - **send**
- 内核空间
  - syscall
  - tcp_*
  - ip_*
  - dev_*
  - e1000_*
- 仿真设备
  - 网卡
  - hub
  - slirp

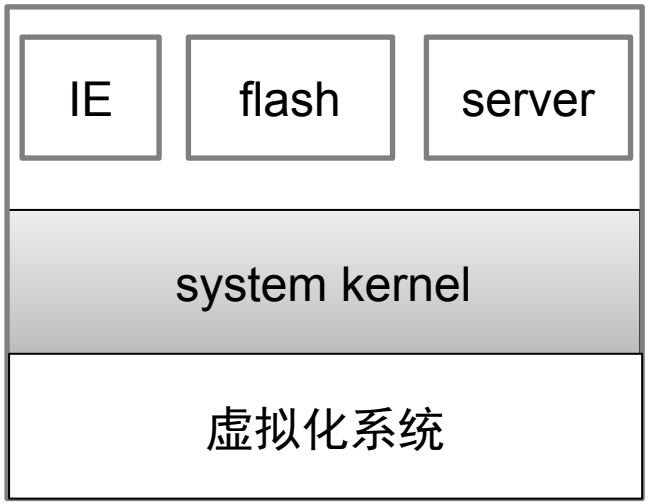


网卡设备原理

- 初始化
  - 分配端口，映射地址
  - 设备状态及资源设置
- 数据传输
  - 设备TDT寄存器检测到write指令
  - 处理描述符表
  - 处理3种描述符：context，data，legacy
  - 发送数据
  - 设置状态位，等待处理下一次操作
- 处理细节
  - 环形内存
  - TSO：tcp分段分流技术

虚拟化漏洞挖掘特点

- 目标更加底层



- 测试数据特殊

仿真设备测试方法

- 改变正常流程

  HOOK驱动函数

  修改内核文件

- 配合上下文环境

漏洞分析

- **Qemu e1000网卡设备**
- **Vmware e1000网卡设备**

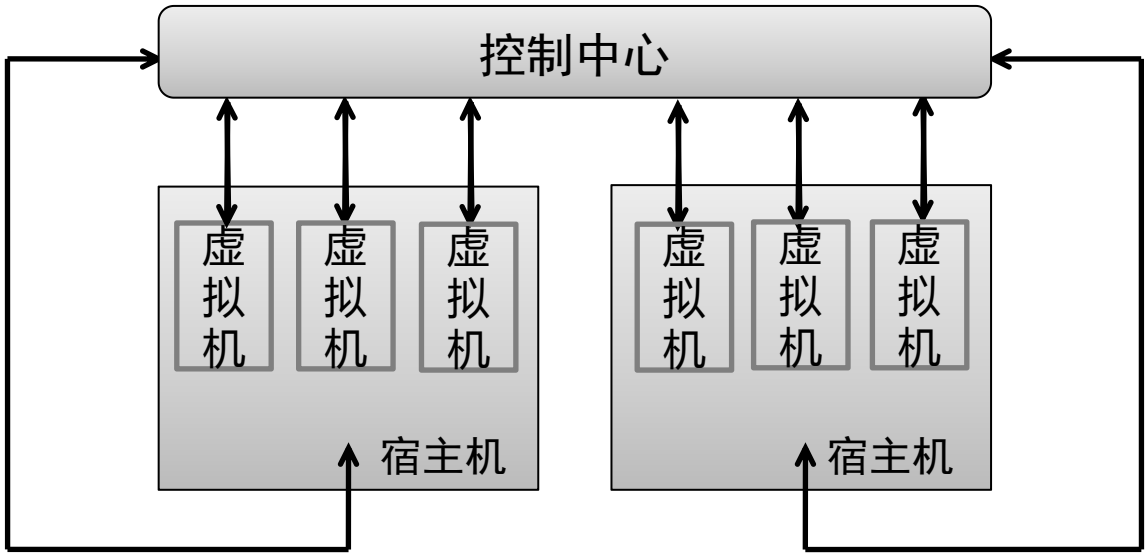
```
do {
    bytes = split_size;
    if (tp->size + bytes > msh)
        bytes = msh - tp->size;

    bytes = MIN(sizeof(tp->data) - tp->size, bytes);
    pci_dma_read(d, addr, tp->data + tp->size, bytes);
    sz = tp->size + bytes;
    if (sz >= tp->hdr_len && tp->size < tp->hdr_len) {
        memmove(tp->header, tp->data, tp->hdr_len);
    }
    tp->size = sz;
    addr += bytes;
    if (sz == msh) {
        xmit_seg(s);
        memmove(tp->data, tp->header, tp->hdr_len);
        tp->size = tp->hdr_len;
    }
} while (split_size -= bytes);
```

测试框架

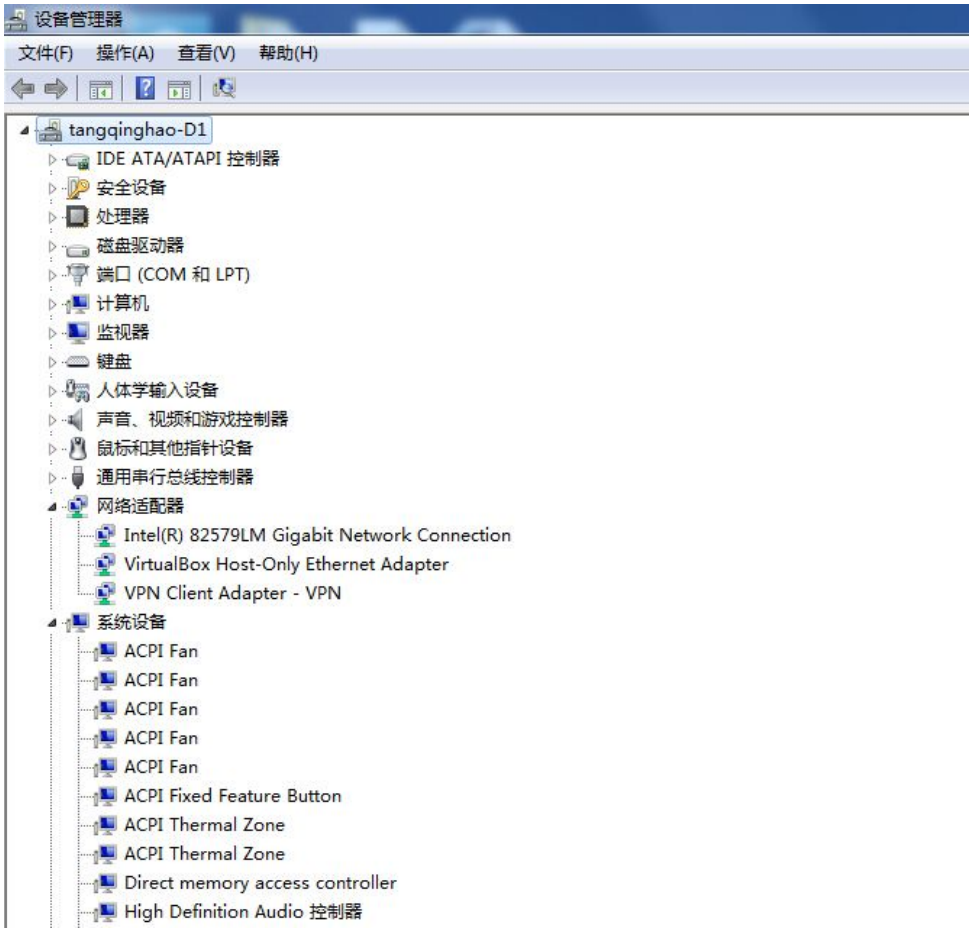
特点

- 利用平台共性
- 关注实现特性
  - 编码语言
  - 操作系统
  - 编码风格

架构



测试-收集设备信息


设备管理器
文件(F) 操作(A) 查看(V) 帮助(H)
tangqinghao-D1
IDE ATA/ATAPI 控制器
安全设备
处理器
磁盘驱动器
端口 (COM 和 LPT)
计算机
监视器
键盘
人体学输入设备
声音、视频和游戏控制器
鼠标和其他指针设备
通用串行总线控制器
网络适配器
Intel(R) 82579LM Gigabit Network Connection
VirtualBox Host-Only Ethernet Adapter
VPN Client Adapter - VPN
系统设备
ACPI Fan
ACPI Fan
ACPI Fan
ACPI Fan
ACPI Fan
ACPI Fixed Feature Button
ACPI Thermal Zone
ACPI Thermal Zone
Direct memory access controller
High Definition Audio 控制器

测试-组织测试数据

- 指令处理型

  特殊指令

  特殊状态

- 外设型

  状态顺序

  数据内容

测试-攻击仿真设备

- 用户空间
- 内核空间

反馈-测试结果

- 无影响
- 蓝屏
- 隐性结果
- 崩溃

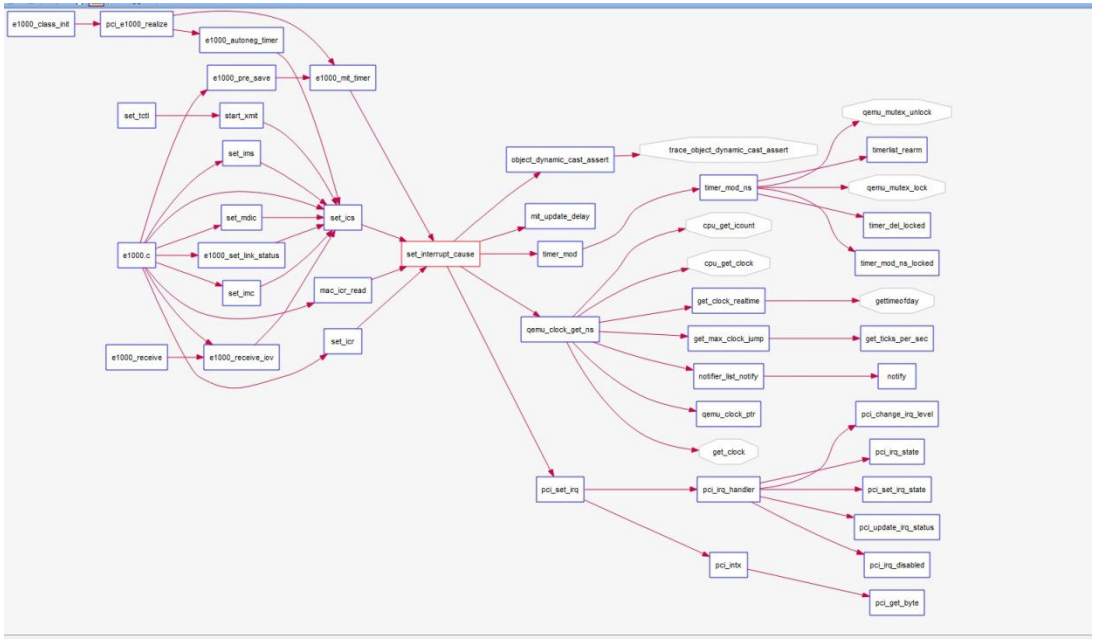
```
(gdb) c
Continuing.
[Thread 0x7fffa4ece700 (LWP 64212) exited]
[Thread 0x7fff97b7b700 (LWP 64211) exited]

Breakpoint 1, ne2000_receive (nc=0x7ffff9c2f7f0, buf=0x7fffffffd390 "RT",
    size_=126) at hw/net/ne2000.c:180
180     {
(gdb) disable
(gdb) c
Continuing.
[New Thread 0x7fff97b7b700 (LWP 64229)]

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff5c022dc in _int_malloc () from /lib64/libc.so.6
(gdb) bt
#0  0x00007ffff5c022dc in _int_malloc () from /lib64/libc.so.6
#1  0x00007ffff5c036b1 in malloc () from /lib64/libc.so.6
#2  0x00007ffff786c676 in malloc_and_trace (n_bytes=49280) at vl.c:2724
#3  0x00007ffff6923cd5 in g_malloc () from /lib64/libglib-2.0.so.0
#4  0x00007ffff6938e0a in g_slice_alloc () from /lib64/libglib-2.0.so.0
#5  0x00007ffff776a614 in virtio_blk_alloc_request (s=0x7ffff8894230)
    at /home/max/qemu-2.4.0/hw/block/virtio-blk.c:33
#6  0x00007ffff776ad06 in virtio_blk_get_request (s=0x7ffff8894230)
    at /home/max/qemu-2.4.0/hw/block/virtio-blk.c:192
#7  0x00007ffff776beed in virtio_blk_handle_output (vdev=0x7ffff8894230, vq=
    0x7ffff9924ff0) at /home/max/qemu-2.4.0/hw/block/virtio-blk.c:603
#8  0x00007ffff77aa921 in virtio_queue_notify_vq (vq=0x7ffff9924ff0)
    at /home/max/qemu-2.4.0/hw/virtio/virtio.c:921
#9  0x00007ffff77aca59 in virtio_queue_host_notifier_read (n=0x7ffff9925038)
    at /home/max/qemu-2.4.0/hw/virtio/virtio.c:1536
#10 0x00007ffff7a780f2 in qemu_iohandler_poll (pollfds=0x7ffff87c1240, ret=1)
    at iohandler.c:126
#11 0x00007ffff7a77d64 in main_loop_wait (nonblocking=0) at main-loop.c:503
#12 0x00007ffff7868e44 in main_loop () at vl.c:1902
#13 0x00007ffff7870f9e in main (argc=14, argv=0x7fffffffe238, envp=
    0x7fffffffe2b0) at vl.c:4653
(gdb)
```

反馈-虚拟机自动管理

- 快照
- 重启
- 设备增删改查
- 调试启动
- 加载调试插件

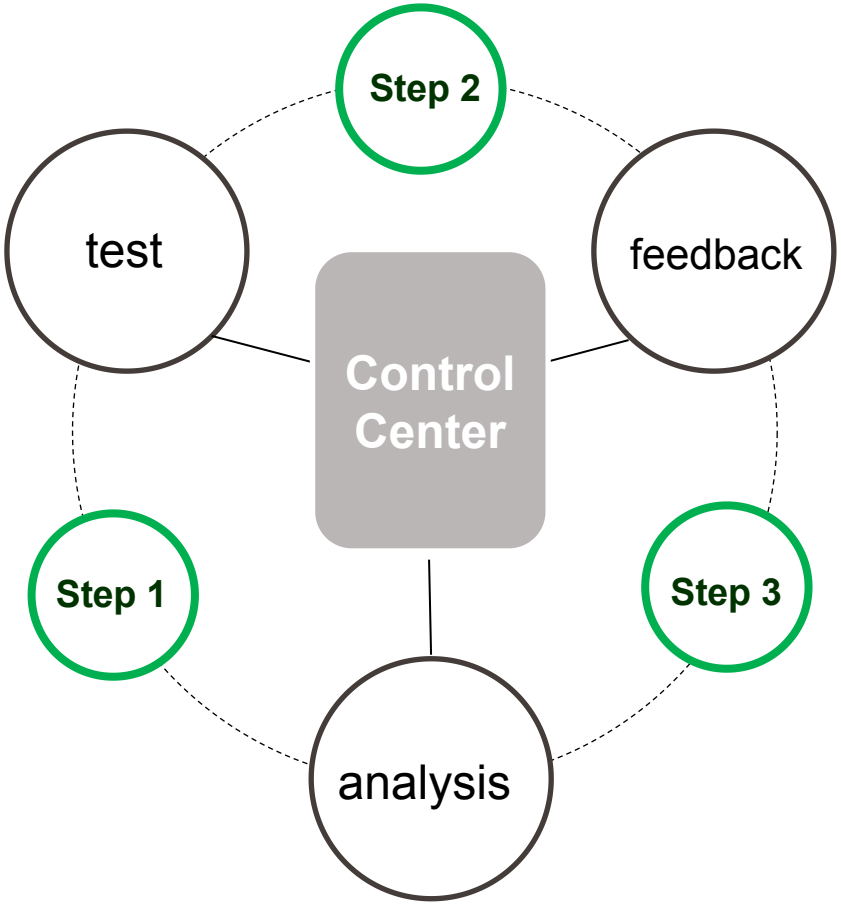
反馈-插装技术

- 动态插桩
- 静态插桩



控制中心-流程

- 下发测试
- 收集反馈
- 分析



控制中心-统计&优化

- 测试总次数
- 函数覆盖率
- 改良测试数据

测试结果

- **50**天
- **2**种平台
- **13**枚漏洞

总结

关注虚拟化安全，关注 **Marvel Team**

Q&A

Email：tangqinghao@360.cn
QQ：702108451