

目录

一、	序言	6
二、	概述和工具介绍	7
1)	Hypervisor 概述	7
a)	虚拟化的历史	7
b)	硬件虚拟化技术	7
c)	虚拟机的启动过程	8
d)	Hypervisor 的使用架构	10
2)	HVM 特定平台介绍	10
	AMD-V	10
	Intel-VT _x	14
	Intel-VT _d (如果时间充裕则写)	14
三、	HVM 技术细节	16
四、	体验 NewBluePill	17
1)	编译 NewBluePill	17
2)	演示 NewBluePill	19
3)	调试 NewBluePill	21
五、	NewBluePill 程序逻辑	25
1)	Nbp 的初始化过程	25
1.	总体概述	25
2.	具体描述	25
2)	DbgClient 的初始化过程	26
3)	Nbp 的卸载过程	26
4)	DbgClient 的卸载过程	26
5)	Bpknock 的作用	26
六、	NewBluePill 硬件相关层	30
	技术背景	30
七、	NewBluePill 内存系统	31
1)	相关文件:	31
2)	技术背景:	31
3)	总体功能介绍:	34
4)	实现过程:	34
	MmInitManager()方法	34
	MmSavePage ()方法	35
	MmSavePage ()方法	37
	MmSavePage ()方法	37
八、	NewBluePill VMExit 事件管理系统	38
1)	注册机制	38
2)	触发机制	38
九、	NewBluePill 调试系统	39
十、	NewBluePill 恶意代码部分	40
十一、	动手写自己的第一个 HVM 程序	41

1)	实验目的.....	41
2)	实验概述.....	41
3)	实验过程.....	41
十二、	移植 NBP 到 32 位系统.....	42
十三、	开发自己的序列号验证器.....	42
十四、	相关文档.....	43
十五、	其它有关 HVM 技术的项目.....	43
十六、	参考文档.....	44