

Virtualization (In)Security Training

by

Invisible Things Lab

Training Agenda (Version 0.9)

Day 1 of 2

Part 0: Introduction

0900 — 0930

~ Lectures: 0900 — 0930

1. Administrivia
2. Virtualization & security brief intro
3. Training brief intro

Part 1: VM Escapes (DomU → Dom0)

0930 — 1230

~ Lectures: 0930 — 1115

1. Xen Architecture — brief introduction
2. A look at a few promising vulnerabilities in backend drivers
3. Focus on Xen PV Frame Buffer backed: exploitation discussion

~ Coffee Break: 1030 — 1045

4. Protection: Dom0 disaggregation and challenges

~ Labs: 1115 — 1230

1. Exploiting Xen PVFB bug (CVE-2008-1943)
2. Getting around SELinux in Dom0

~ Lunch Break: 1230 — 1400

Part 2: Getting into the hypervisor (Dom0 → Xen)

1400 — 1800

~ Lectures: 1400 — 1500

1. Classic DMA attacks against Xen
2. VT-d as a protection against DMA attacks

~ Labs: 1500 — 1600

1. "Xen Loadable Modules" framework (DMA attacks)

~ Coffee Break: 1600 — 1615

~ Lectures: 1615 — 1700

2. Getting around Xen VT-d protection using Remapping attacks
3. Digression about Memory controllers and SMM attacks

~ Labs: 1700 — 1800

2. VT-d against DMA attacks
3. Remapping attacks on Q35 (and testing the BIOS fix)

Part 3: Compromising the Hypervisor

1800 — 1900

~ Lectures: 1800 — 1900

1. Hypervisor Rootkits (not to be confused with BluePill!)

(to be continued...)

Day 2 of 2

Part 3: Compromising the Hypervisor (cont.)

0900 — 1230

~ *Labs: 0900 — 1000*

1. *Playing with Xen "DR Backdoor"*
2. *Playing with Xen "Foreign Backdoor"*

~ *Lectures: 1000 — 1115*

3. Bluepilling the Hypervisor

~ *Coffee Break: 1030 - 1045*

4. Nested Virtualization

~ *Labs: 1115 — 1230*

3. Playing with BluePillBoot
4. Playing with XenBluePill — Bluepilling Xen on the fly!

~ *Lunch Break: 1230 - 1400*

Part 4: Protecting the Hypervisor

1400 — 1700

~ *Lectures: 1400 — 1515*

1. Quick introduction to Trusted Computing (TPM, TXT, Trusted Boot)
2. Launch-time integrity — Trusted Boot via TXT
3. Bypassing TXT and SMM attacks
4. Runtime-protection: Dom0 disaggregation again

~ *Labs: 1515 — 1700*

1. Starting Xen with Intel Trusted Boot (tboot)
2. Tboot vs. BluePillBoot

~ *Coffee Break: 1600 - 1615*

3. Attacking SMM
4. Bypassing Intel TXT using an SMM attack
5. Patching the firmware to prevent SMM attack and TXT bypass
6. Playing with Dom0 disaggregation and VT-d support

Part 5: Getting into the Hypervisor Anyway (direct runtime attacks)

1700 — 1900

~ *Lectures: 1700 — 1800*

1. Xen hypervisor code security analysis
2. Exploiting overflows in the Xen hypervisor
3. Protecting hypervisors against direct attacks

~ *Labs: 1800 — 1900*

1. Looking at the Xen source code
2. Exploiting the FLASK heap overflow

Part 6: Philosophical Summary

1900 — 1930

~ *Lectures:*

1. Xen vs. other VMM systems — design comparison from security standpoint
2. VT and TXT as new means for building more secure systems
3. Practical lessons
4. The future of virtualization security?

Note:

1. Agenda is subject to change.
2. Times given in the agenda are subject to fluctuations.
3. Some lab exercises might be skipped due to time constraints or unexpected hardware problems.