

Virtualization (In)Security Training

by

Invisible Things Lab

Training Agenda (Version 1.1)

Day 1 of 2

Part 0: Introduction 0900 — 0930

~ Lectures: 0900 — 0930

- Administrivia
- Virtualization & security brief intro
- Training brief intro

Part 1: VM Escapes (DomU → Dom0) 0930 — 1230

~ Lectures: 0930 — 1030

- Xen Architecture — brief introduction
- Focus on Xen PV Frame Buffer backed: exploitation discussion

~ Coffee Break: 1030 — 1045

~ Labs: 1045 — 1230

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

~ Lunch Break: 1230 — 1400

Part 2: Getting into the hypervisor (Dom0 → Xen) 1400 — 1600

~ Lectures: 1400 — 1500

- Classic DMA attacks against Xen
- VT-d as a protection against DMA attacks
- Getting around Xen VT-d protection using Remapping attacks
- Digression about Memory controllers and SMM attacks

~ Labs: 1500 — 1600

- "Xen Loadable Modules" framework (DMA attacks)
- VT-d against DMA attacks

~ Coffee Break: 1600 — 1615

Part 3: Compromising the Hypervisor 1615 — 1900

~ Lectures: 1615 — 1645

- Hypervisor Rootkits (not to be confused with BluePill!)

~ Labs: 1645 — 1730

- *Playing with Xen "DR Backdoor"*
- *Playing with Xen "Foreign Backdoor"*

~ Lectures: 1730 — 1830

- Bluepilling the Hypervisor
- Nested Virtualization

~ Labs: 1830 — 1900

- Playing with BluePillBoot
- Playing with XenBluePill — Bluepilling Xen on the fly!

Day 2 of 2

Part 4: Protecting the Hypervisor

0900 — 1700

~ *Lectures: 0900 — 1230*

- An introduction to Trusted Computing (TPM, TXT, Trusted Boot)

~ *Coffee Break: 1030 - 1045*

- Launch-time integrity — Trusted Boot via TXT
- Trusted Computing examples

~ *Lunch Break: 1230 - 1400*

~ *Lectures: 1400 — 1445*

- Bypassing TXT and SMM attacks

~ *Labs: 1445 — 1515*

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

~ *Lectures: 1515 — 1600*

- Runtime-protection: Dom0 disaggregation again

~ *Coffee Break: 1600 - 1615*

~ *Labs: 1615 — 1700*

- Playing with Dom0 disaggregation and VT-d support

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

1700 — 1830

~ *Lectures: 1700— 1745*

- Exploiting overflows in the Xen hypervisor
- Protecting hypervisors against direct attacks

~ *Labs: 1745 — 1830*

- Looking at the Xen source code
- Exploiting the FLASK heap overflow

Part 6: Philosophical Summary

1830

~ *Discussion*

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.