

Virtualization (In)Security Training

by

Invisible Things Lab

Topics Covered

The training uses Xen hypervisor to illustrate virtualization-related attacks and defenses. The following topics will be discussed over the 2-day hands-on class — each topic consists of lectures that are later followed by hands-on exercises ("labs") done by each participant alone or in a pair with another participant:

- ✓ VM Escapes (DomU → Dom0)
- ✓ Hypervisor hijacking (Dom0 → Xen)
- ✓ Compromising the hypervisor (hypervisor rootkits, not limited to BluePill!)
- ✓ Protecting the hypervisor
- ✓ Xen vs. other VMM systems
- ✓ VT and TXT as new means for building more secure systems

Consult the full agenda distributed together with this brochure for details.

Goals of the training

- ✓ Present an unbiased view on the security of bare-metal hypervisor systems (using Xen as an example), show exemplary attacks and study how various technology (e.g. Intel VT-d and TXT) and clever design of the VMM can help to improve security. Point out where the weaknesses are still present and what we can expect in the future.
- ✓ Provide a good baseline for comparing Xen-based products with other hypervisors on the market from security standpoint, thus allow for better decision making when buying virtualization products (participants will know what "hard questions" to ask vendors and what features to look for).
- ✓ Enable administrators of current virtualization systems to better plan the deployment in order to optimize security.
- ✓ Provide fun and excitement by enabling technically savvy attendees to perform real-world attacks on one of the most advanced and exciting technology (Xen 3.3, VT-d, TXT) on the planet.
- ✓ Provide food for thought for all people engaged in design or development of virtualization systems, as well as "normal" operating systems.

Target audience

Senior administrators of virtualization systems, security architects planning (secure) deployment of a virtualization solutions (especially Xen-based, but not limited to), virtualization systems and operating systems designers/developers, advanced security professionals interested in designing security solutions for virtualization-based systems, other curious individuals.

Required skills/knowledge

For everybody: Basic Linux console skills (will be using Linux-based OS for Dom0), basic knowledge of current OS and virtualization systems design,

Additionally for people willing to understand/complete most of the exercises: advanced Linux skills, advanced C system programming, basic knowledge of current systems hardware design, basic GDB skills, advanced experience with using Xen systems,

Additionally for people willing to understand/complete all the exercises: proficiency in using and understanding GDB, understanding of advanced exploitation methods, good understanding of contemporary computer systems hardware design, excellent understanding of Xen system design and implementation.

What to bring

Bring open and curious mind. Everything else will be provided.

About authors and trainers

This training has been prepared and will be presented by the Invisible Things Lab team, composed of: Rafal Wojtczuk, Alexander Tereshkin and Joanna Rutkowska. Invisible Things Lab is a boutique security research and consulting company, focusing on OS and virtualization systems security. ITL's members are experienced security researchers, well known for finding design and implementation weaknesses in a wide-range of operating systems, hypervisors and even system-level software, like BIOS, presenting new system compromise methods, as well as conducting a cutting-edge research into new defensive technology.

Our recent research on the topic within the last 12 months:

- ✓ Ring -3 Rootkits (to be presented at Black Hat USA 2009)
- ✓ Attacking Intel® BIOS (to be presented at Black Hat USA 2009)
- ✓ Attacking SMM Memory via Intel® CPU Cache Poisoning (March 2009)
- ✓ Attacking Intel® Trusted Execution Technology (Black Hat DC, February 2009)
- ✓ Adventures with a certain Xen vulnerability (October 2008)
- ✓ Subverting the Xen Hypervisor (Black Hat USA, August 2008)
- ✓ Detecting & Preventing the Xen Hypervisor Subversions (Black Hat USA, August 2008)
- ✓ Bluepillling the Xen Hypervisor (Black Hat USA, August 2008)

More details at: <http://invisiblethingslab.com/>

