Agentless Introspection for Commodity Servers

14 January 2015

John Shackleton

john.shackleton@adventiumlabs.com

This material is based upon work supported by the Air Force Research Lab, Rome, NY under Contract No. FA8750-10-D-0197. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Air Force Research Lab, Rome, NY.
The Host Protection Conundrum

- Co-residency creates vulnerability
- Slow response times
- Inflexible options to respond to specific attacks

Traditional defenses protect their host but rely on local operating system services
Quick Hypervisor Primer

Hypervisor

- Control Domain (domain 0)
- Hardware Emulation (QEMU)

User Virtual Machine

- Toolstack
- Device Drivers
- VM State Storage
- Full Hardware Emulation
Virtualization and Introspection

Host Operating System

System Calls

Hypervisor

Introspection Engine

Memory & Execution Data

Agentless Introspection Breaks the Circular Risk
The execution context of the host system must be understood before security analysis is conducted.
A Framework Approach

A more flexible architecture for monitoring multiple categories of attacks
XipWire Monitors Runtime OS Integrity

Windows Server 2008 R2 (kernel 7601)

- Kernel Image (ntoskrnl)
- Interrupt Handler (IDTR)
- Syscall registers

Monitored User VM

Static System Components & State
- Kernel Image
- Interrupt Handler
- Syscall Registers

Hypervisor

Introspection Engine

XipWire Codepack

Cryptographic Hash

Memory Scan

GUI
XipTop Reveals Rootkits

Monitored User VM

Process Data (hidden process)

Memory Scan

Introspection Engine

Raw Process Data

XipTop Codepack

GUI

Hypervisor

Process Data

© 2015 Adventium Labs.