



University of Maryland University College

Teaching Intrusion Detection and Intrusion Prevention on the Virtual Platform: Hands-On Laboratory Exercises

Dr. Jim Q. Chen, Barry Williams, and
Alkalifa A. Samake

March 2009

Acknowledgements

- Special thanks to other people in the lab group for their support of this project: John Smet, Lamin Kamara, Nicole Regobert, Sharon A. Archer, Marcelle S. Owens, Grant Kolani, and Khalid Bendidi

Objectives

- Discuss the challenges in running a network security lab
- Explain virtual platform
- Discuss a solution using virtual platform
- Demonstrate the lab exercises of intrusion detection and intrusion prevention running on a VMware server
- Discuss the benefits and the limitations
- Discuss lessons learned and future research

Challenges in Running a Lab

- Support for an increasing number of students
- Maintenance of existing equipment
- Setting up and configuring new equipment
- Efficiency
- Physical space
- Cost

Traditional Solution

- Purchase more pieces of equipment
- Hire more support personnel
- Purchase services from outside vendors
- Allocate additional physical space

Consequences

- More complicated environment
- Reduced quality of service
- Hard to manage
- More cost

Virtual Platform Solution

- From peer-reviewed publications:
- **Definition**: Seetharaman and Murthy (2006):
Software virtualization is "a powerful mechanism for running multiple operating systems - and hence, multiple applications on different software platforms - on the same physical hardware".
- **Benefits**: Magnusson (2005): "Virtualization can ease software development in an increasingly interconnected world".

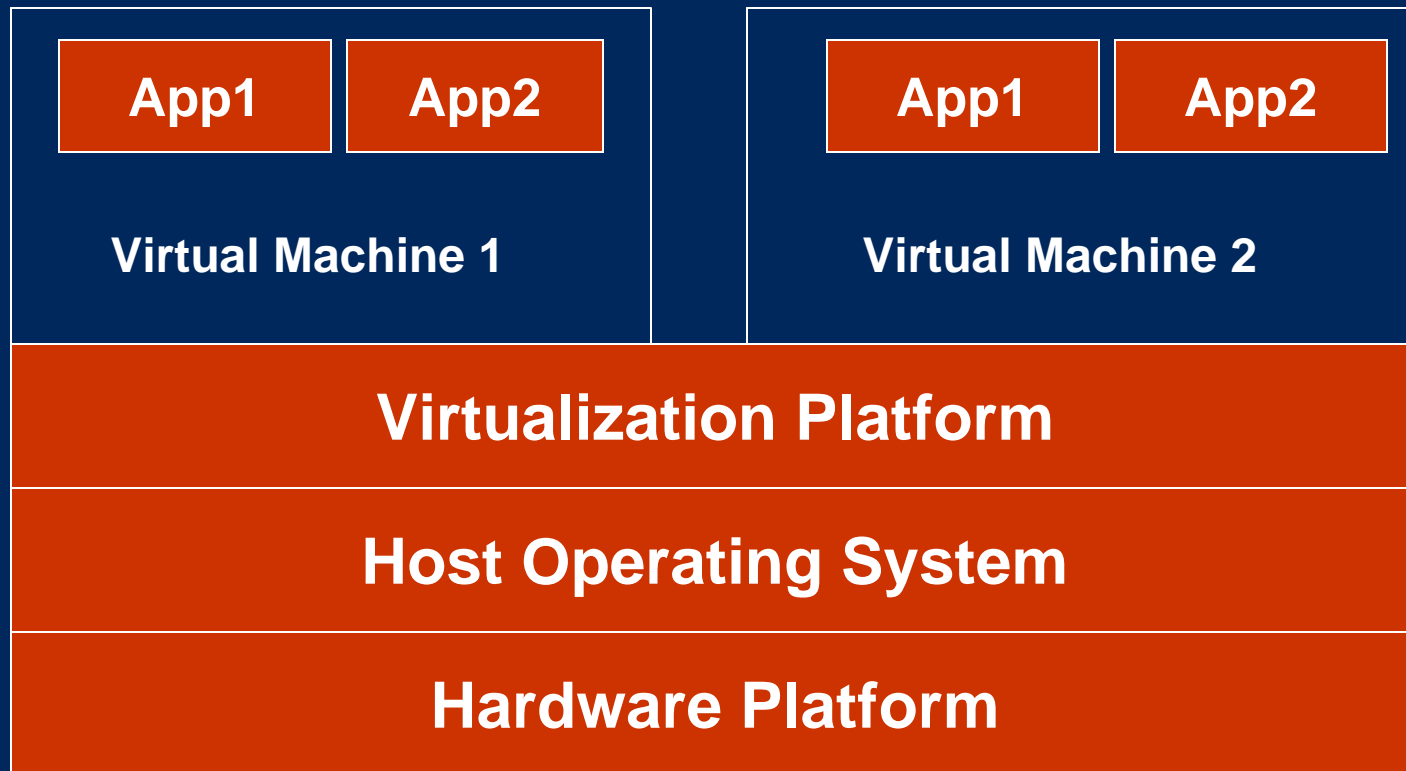
Virtual Platform Solution

- **Function**: Uhlig and others (2005): "Full virtualization of all system resources - including processors, memory, and I/O devices - makes it possible to run multiple operating systems on a single physical platform".
- **Educational Implication**: Armitage, Gaspar, and Rideout (2007): "Open source virtualization solutions could solve classroom management headaches".

Virtual Platform Solution

- From non-peer-reviewed resource:
- **Definition:**
http://en.wikipedia.org/wiki/Virtual_platform: “In computer science, a virtual machine (VM) is a software implementation of a machine (computer) that executes programs like a real machine.”

Virtual Machine Concept



Seetharaman and Murthy (2006)

4 Categories of Virtualization

- http://en.wikipedia.org/wiki/Virtual_machines:
- Emulation or full system virtualization
- Para-virtualization
- Native virtualization
- OS-level virtualization

VMware

- Native virtualization
- Multiple instances of various operating systems on a single physical hardware platform

A Solution Using VMware

- Hardware: DELL server
- Software: VMware ESXi server and various operating systems
- What is built: a virtual closed network with multiple computers on a single VMware server

VMware ESXi Server

- Managed from workstation
- Supports multiple instances

Lab Exercises

- Ping
- ftp
- Vulnerability scanning
- Intrusion detection and prevention

Testing the Connectivity

- Ping different virtual machines from various virtual instances

Testing the Connectivity

- Ping various virtual machines from the Backtrack instance
- Demo

Testing the Connectivity

- Ping various virtual machines from the Fedora Linux instance
- Demo

Testing the Connectivity

- Ping various virtual machines from the Windows 2003 server instance
- Demo

Testing the Connectivity

- Ping various virtual machines from the Windows XP workstation instance
- Demo

Capturing FTP Traffic

- Use WireShark on the Windows XP workstation instance to capture FTP traffic
- The password is shown in the plain text
- Demo

Vulnerability Scanning

- Use SAINT to scan vulnerability within the virtual network
- Demo

Intrusion Detection and Prevention

- Use Snort to detect intrusion and prevent intrusion within the virtual network
- Demo

Benefits

- Easy to use
- Easy to manage
- Small physical footprint
- Efficient use of resources (space and time)
- Cost saving
- Able to support an increasing number of students
- Able to work with multiple operating systems in one environment
- Able to have better utilization of Backtrack tools

Limitations

- Huge requirement of memory
- No virtualization of switching and other relevant technology
- No virtualization of VoIP environment
- Free backup solution in VMWare ESXi server (snapshot) not completely satisfactory [3rd party solution: vOptimizer Pro, Vizioncore, Veeam]
- Difficulties associated with the saving of students' work product

Lesson Learned

- The VMware ESXi server managed from a workstation
- The number of virtual machines that can be run concurrently decided by the amount of memory available
- Available instructions not necessarily pertain to your specific environment (IDE [HDA] versus SCSI [SDA])
- Some external devices not recognized natively

Pedagogical Implication

- Minimum learning curve for students
- Real-life scenarios provided
- Creative thinking encouraged
- Learning enhanced with hands-on exercises

Future Research

- Add switching into virtual environment
- Test in the virtual environment the capability of intrusion detection and intrusion prevention systems in dealing with footprinting, scanning, enumeration, privilege escalation, gaining and maintaining access, expanding influence, and covering tracks
- Design lab exercises in network auditing in the virtual environment

Summary

- Virtual platform eases the management of hands-on lab.
- Virtual platform makes good and efficient use of resources while minimizing cost.
- Virtual platform reduces the complexity of using multiple machines concurrently.
- Virtual platform can be used to challenge students with real-life issues and enhance their learning.
- Virtual platform facilitates remote access.
- More research is needed because currently virtualization does not include all the networking technologies.

References

- Beale J, Baker A, Esler J, and others. (2007). *Snort IDS and IPS Toolkit*. Rockland, MA: Syngress Publishing, Inc.
- Chen J, Tsao V, Williams B, Olojo T. (2006). "Lesson Learned from Teaching Intrusion Detection and Intrusion Prevention with Snort", the 4th Annual SecureIT 2006 Information Technology and Network Security Conference, Anaheim, California. March 21 - 24, 2006
- Chen J, Goff D, Hoferek M, Sayani H. (2005) "Enhancing Information Assurance Education with Remote Access Laboratories", the 3rd Annual SecureIT 2005 Information Technology and Network Security Conference, San Diego, California. April 19 - 22, 2005
- Magnusson P. (2005). "The Virtual Test Lab", *Computer*, vol. 38, no. 5, pp. 95-97, May 2005

References

- Provos N, Holz T. (2008). *Virtual Honeypots: From Botnets Tracking to Intrusion Detection*. Upper Saddle River, NJ: Addison-Wesley, Pearson Education
- Seetharaman S, Murthy K. (2006). "Test Optimization Using Software Virtualization", *IEEE Software*, vol. 23, no. 5, pp. 66-69, Sep./Oct. 2006
- Snort, <http://www.snort.org>
- Tcpdump, <http://www.tcpdump.org>
- Uhlig R, Neiger G, Rodgers D, Santoni A, Martins F, Anderson A, Bennett S, Kagi A, Leung F, Smith L. (2005). "Intel Virtualization Technology", *Computer*, vol. 38, no. 5, pp. 48-56, May 2005
- WireShark, <http://www.wireshark.org>