University of Maryland University College

NEW LEARNING TECHNOLOGIES 2012 CONFERENCE

Leveraging Virtualization to Facilitate Online Delivery of Technical Courses

Stephen D. Gantz

CISSP-ISSAP, CEH, CGEIT, CRISC, CIPP/G, C|CISO

Assoc. Professor of Information Assurance

sgantz@faculty.umuc.edu

Agenda

- Introduction
- Context – The IA Program
- Challenges
- Virtualization Solution
- Deployment Considerations
- Demonstration
- Questions

Introduction

- UMUC is one of 11 colleges in the University of Maryland System
- Primarily focuses on adult students, with programs tailored to educational needs of working professionals
- Combined undergraduate and graduate enrollment is over 90,000
- Extensive online/distance education offerings including fully online degree programs
- Physical campuses/classrooms in Washington, DC metro area, Germany, and Japan

The Information Assurance Program

- IA is a specialization within the Masters in Information Technology, offering both 15-credit certificate and 36-credit degree programs
- Targeted at managers and technology professionals working with or managing secure information systems and the protection of information assets
- Core IA curriculum covers 6 courses plus a capstone; about half involve hands-on use of relevant technical tools and software
- Representative example: INFA 630 – Intrusion Detection and Prevention

INFA 630 – Intrusion Detection and Prevention

- INFA 630 provides technical instruction in IDS and IPS technologies, including security analysis techniques, signature development, rule writing, and security architecture
- Addresses both network-based and host-based technologies, but emphasizes network-based tools, including Wireshark and Snort
- Course requirements include installing and using tools, and completing a series of lab exercises demonstrating correct use of the tools

A Few Words About Snort

- Snort is a leading open-source NIDS
- Offers multi-platform support (including Windows), but developed and optimized largely as a Linux/Unix program
- Project development is led by Sourcefire, with 4-5 releases per year
- Can be installed with packages or from source
- Using Snort in operational environments requires several other tools and components

Challenges

- Installing and configuring tools like Snort is very technically detailed
- INFA 630 students have a wide range of technical skills, all of which need to be supported
- Users must work at the command line, as there is no graphical interface for the tool
- Experience shows a high rate of technical issues for students running Windows, especially Win 7
- In a typical semester, different students may be working on 5-6 different operating systems
- Textbooks on Snort quickly fall behind current releases

Problem Statement

- Historically, a large proportion of student (and faculty) time and effort is spent on setting up the required tools, not on using them to support course objectives
- Goal for INFA 630 is to provide a fool-proof set of instructions for installing and configuring Snort

OR

- For students unable or unwilling to do a manual install, to provide a pre-installed and configured version that simply needs to be adapted to local environments

Enter Virtualization

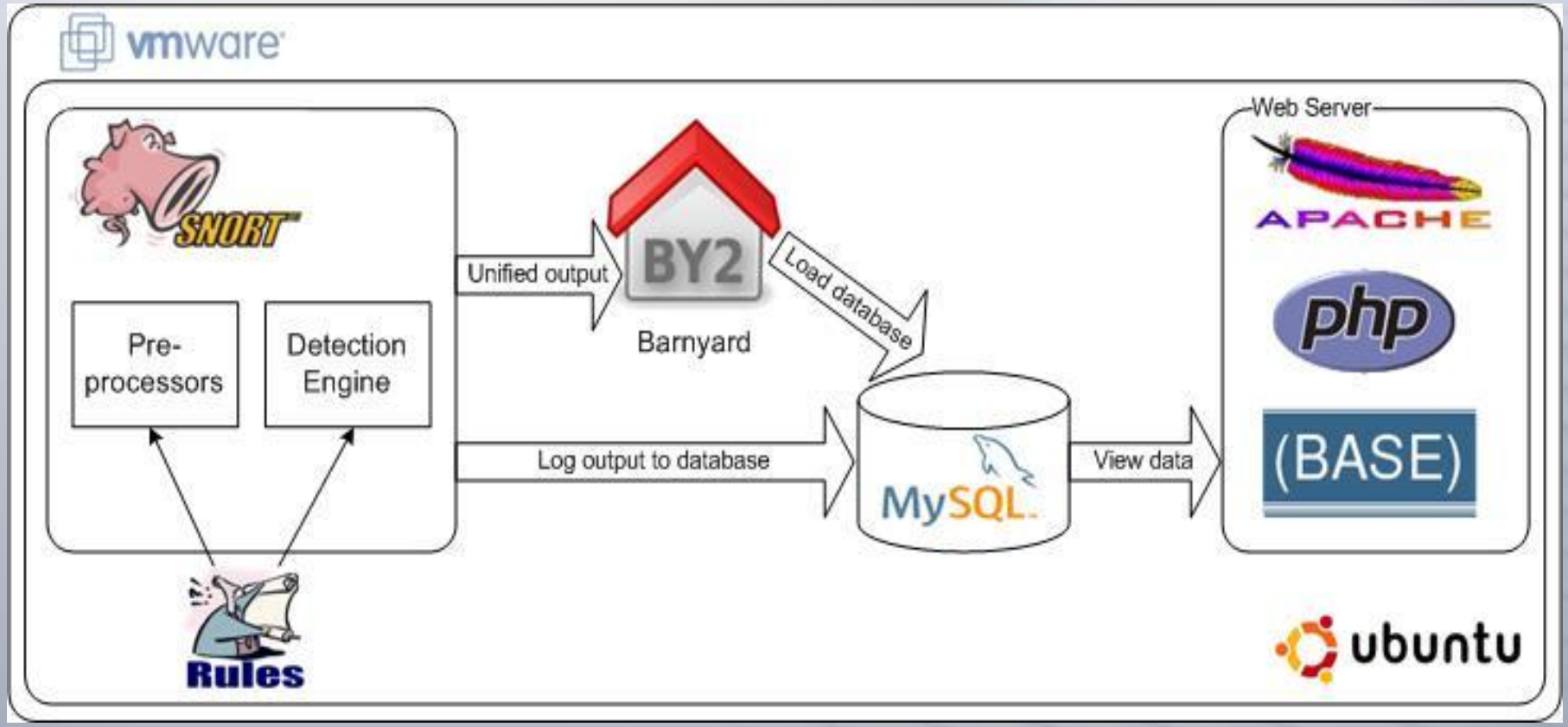
- Using virtual machine technology offers a viable solution to the problems students face working with specialized software in technical courses
- Virtualization allows students to work in a Linux environment without significant alteration to their regular (Windows or Mac) computers
- Virtualization also offers a common technical approach serving students at all levels of technical skill
- As a secondary but non-trivial consideration, student use of virtual machines is free

Solution Approach

- Virtual machine instances developed in VMWare
- Instances use Linux, preferred because:
  - Linux avoids distribution/license issues with Windows
  - Snort and related tools “in the wild” are most commonly run on Linux
- All software components and modules typically associated with a real-world implementation are included in the instance
- Step-by-step instructions of the process to create the VM and perform installation and configuration also provided to students and made available online

Solution Components

- The VM solution comprises all of the components shown here:



Deployment Considerations

- Virtual machine instances can be deployed and run locally (e.g., by each student) or hosted centrally and accessed remotely
- For standalone deployments, primary methods of distributing VM instances include:
  - Downloading VM software and INFA 630 instance from online file server
  - Put VM on DVD and package with course materials (students receive by mail)
- Hosted model involves a VM server running in the school's IT infrastructure, and instantiating one instance per student in each course

Current and Future Next Steps

- To date, only INFA 630 is using this approach
- Additional obvious candidates within the IA program include courses on network security and computer forensics
- Potentially much broader potential to use VM environments for technical courses in other programs
- Currently only providing standalone deployments; evaluating stand-up and ongoing support needs to move to a hosted VM server

Demonstration

- This brief demonstration shows:
  - VMWare software running on Windows 7
  - Ubuntu Linux 10.04 operating system VM instance
  - Small bit of configuration needed to adapt instance for local environment use
  - Example of typical student use of the VM

Useful Links and References

- VMWare – source for (free) VMWare Player and Server, and for (licensed) VMWare Workstation
  - http://www.vmware.com
- Technical Components
  - Ubuntu Linux: http://www.ubuntu.com/
  - Snort: http://www.snort.org/
  - Barnyard: http://www.securixlive.com/barnyard2/
- Installation Instructions
  - http://polaris.umuc.edu/~sgantz/Install.html

Questions?