Xen and the Art of Safe Security Testing

By Luke St. Clair
Overview

- Motivation
- Goals
- Environment
- Uses
- Teaching
- Research
- Security Concerns
Motivation

- Security research requires testbeds
- It is difficult to separate resources
- Many different types of resources necessary
  - 2 options - many physical machines, or virtual machines
- Existing work
Goals

- Provide a large number of heterogeneous environments
- Separation from important resources
- Necessary access given
- Quick deployment of environments
- Flexibility
- Determine what needs to change
Environment

- Machines
- Memory
- Disk - 3R’s
- CPU
- Software
- Network
Uses (Examples)

- Class environment
- Security Testing
  - Multiple OSes
  - DDoS Attacks
  - HW attacks
Security Concerns

- What attacks are possible?
- Can you DoS this system?
- Networking leaks
- Device driver leaks
- Identifying the issues that arise from this type of environment
The Big Question:

Does this work, and does it get you anything?