Teaching Network Security Using VITAL

Efstratios L. Gavas[1] and Keith O'Brien[2]

[1]Polytechnic Institute of NYU

[2]Cisco Systems

CISSE 2012

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Network Security at NYU-Poly

- Graduate Level *Network Security*
- Mixed class
  - Full-time and Part-time student
  - Novice and Professionals
  - Both traditional classroom and all virtual instruction

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

What is VITAL?

- Virtual InformaTion Assurance Laboratory (VITAL)
  - also goes by *Virtual Lab* or *VLAB*
- Designed around classroom
  - started when other virtualization options where limited
  - not around server room like VMWare or MS Hyper-V
  - not around research like DETER or GENI
- NSF funded
  - Xen-based
  - open source from front to back

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Student Background

- Highly Varied
- Limited time spent on basics
  - not *just* because we are mean

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

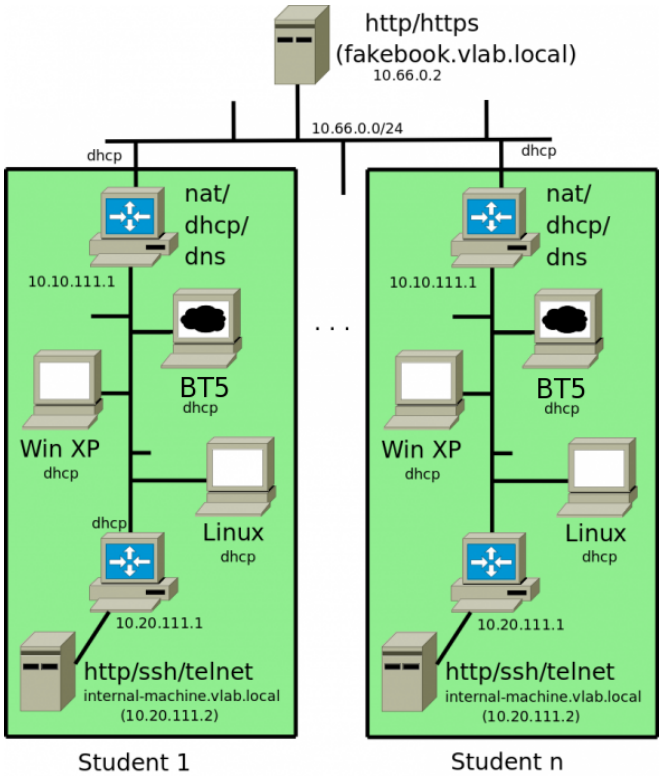
Teaching Offensive Attacks

- Hands-on experience is critical
- Need a safe place to play

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Labs

- Standard Student Network



Labs

- 8 Labs (10 hours each)
- first 4 labs focus on *Network Attack Methodology*
  1. Recon / Information Gather
  2. Scanning / Enumeration
  3. Vulnerability Identification
  4. Exploitation
  5. Post Exploitation / Keeping Access
  6. Covering Tracks

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Lab – Recon, Scanning, and Identification

- Use Backtrack 5 (nmap, Nessus, etc)
- Start to *Think like an Attacker*

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Lab – Exploitation

- Achieve remote shell
- Most will use pre-built *Metasploit* modules

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Lab – Rootkits, and Hiding

- Attack Windows XP
- Use *HackerDefender* as example rootkit

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Labs

- Last 4 labs discuss defensive technologies
- Firewalling
- IPsec / SSL
  - still focus on hands-on experience
  - use *SSLStrip* to MITM

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Why Opensource?

- Flexibility – we needed it
  - Utilize existing tools (Munin, iftop, tcpdump, etc...)
  - Ease of development

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Goals of VITAL

Overarching goals of the VITAL project are:

- Facilitate the adoption by different institutions
- Easy for faculty from different institutions to add hands-on components to their courses
- Enrich student experience in cyber security
- Attract more students to cyber security

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Goals of VITAL

Platform needed the following properties:

- Easy to install, maintain with minimal hardware
- Open source allowing users to extend its functionality
- Bundled with a set of prepackaged assignments
- Allows a community of users to contribute assignments

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

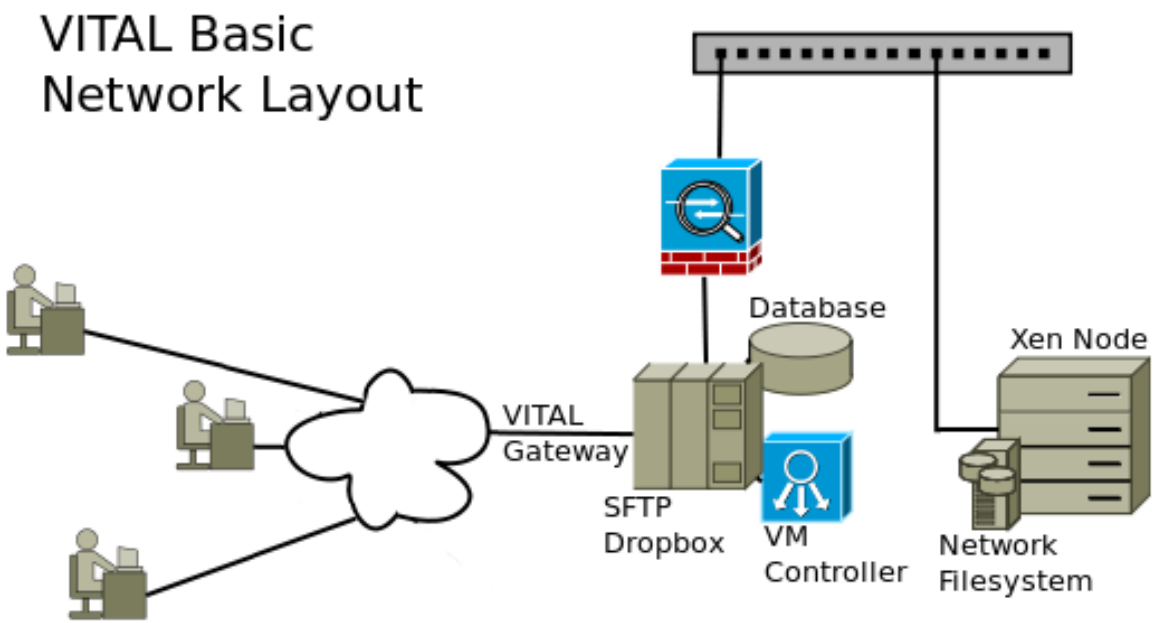
VITAL Architecture

Three main components:

- Controller – Handles the processing of all management operations for the VMs (eg. start, stop, restore).
- Gateway – Provides users web access to VM consoles, using VNC, while isolating access from the internet.
- Xen Nodes – Cluster of servers used to provide virtualization service.

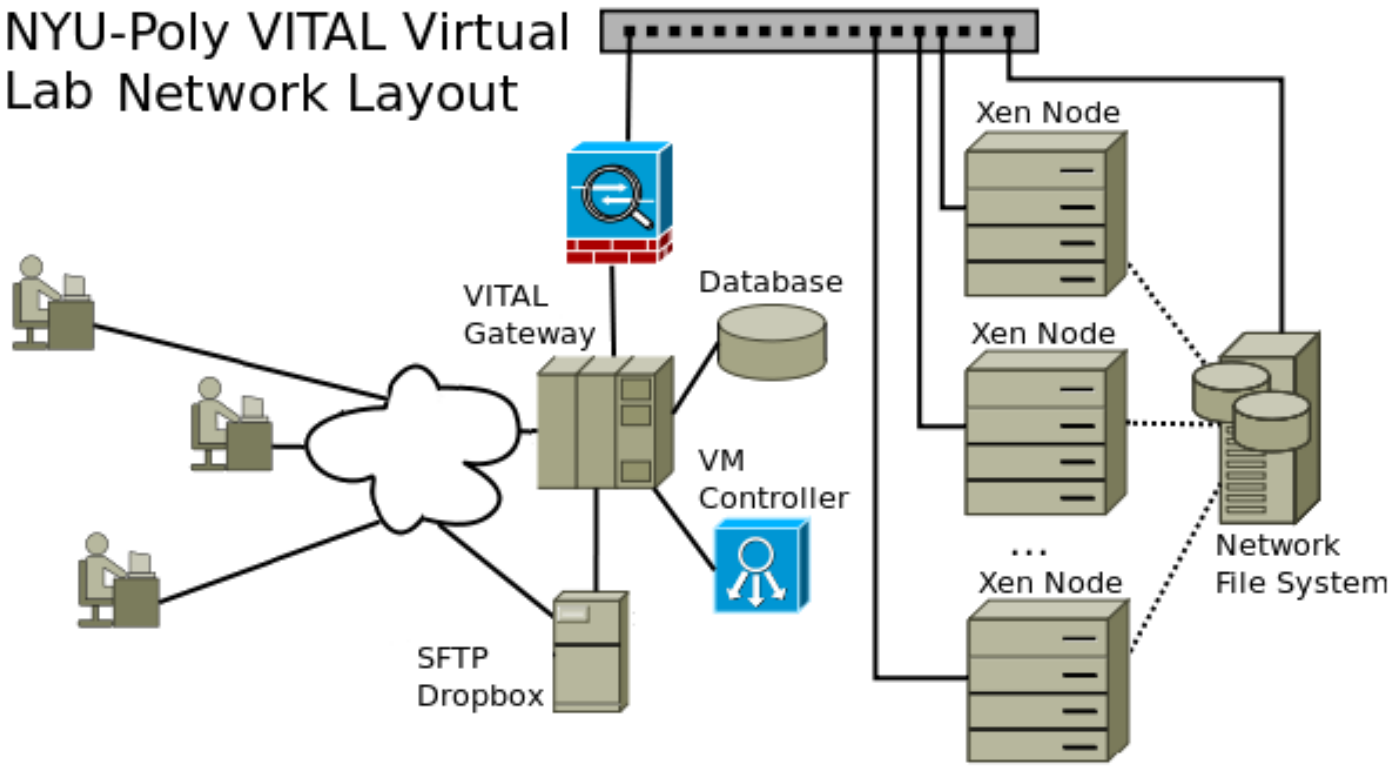
NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Basic Layout



NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

NYU-Poly Layout



NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Future Work

- Expand online resources
- Move from Xen 3.x to 4.x
- HTML 5 VNC interface

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Summary

- Hands-on exercises are critical
- A safe environment is needed
- Download and contribute
  - Lessons, documentation, and downloads
  - `https://vital.poly.edu/release/`

Contact me: egavas {at} isis.poly.edu

NYU:poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY