



Ohio Information Security Conference '08

Hands-On Incident Response Testing Years 1 & 2

Keith Fricke – Cleveland Clinic

Matt Curtin - Interhack



Cleveland Clinic

INTERHACK

■ Introductions

■ Part 1 - Fricke

- IR Testing Philosophy & Methodology
- IR Test – Year 1
- IR Test – Year 2

■ Part 2 - Curtin

- IR Post Mortem Purpose & Intent
- IR Post Mortem Years 1 & 2

■ Keith Fricke - CISSP

- 22+ years IT experience
- Past 9 years InfoSec focused
- Data Security Administrator for Cleveland Clinic's 9 Community Hospitals
- Adjunct Professor, MIS Dept., Ursuline College

■ Matt Curtin - CISSP

- Founder & CEO of Interhack
- Specialties in Computer Forensics and Information Assurance
- Expert Legal Testimonies
- Author
- OSU Adjunct Faculty, Computer Science & Engineering Dept.

Why a Hands-On Test?

- It's Like DR Testing
- The best laid plans.....
- Skill Assessment





- Define Objectives
- Type of Incident
- Critical Questions
 - How much prep time & test time?
 - What roles needed for prep & test?
 - Skills needed vs. skills possessed?
 - Equipment needed?





- Test Location & Travel
- Feeding the Natives
- Identifying Assumptions/Limitations
- Interactive Role Playing

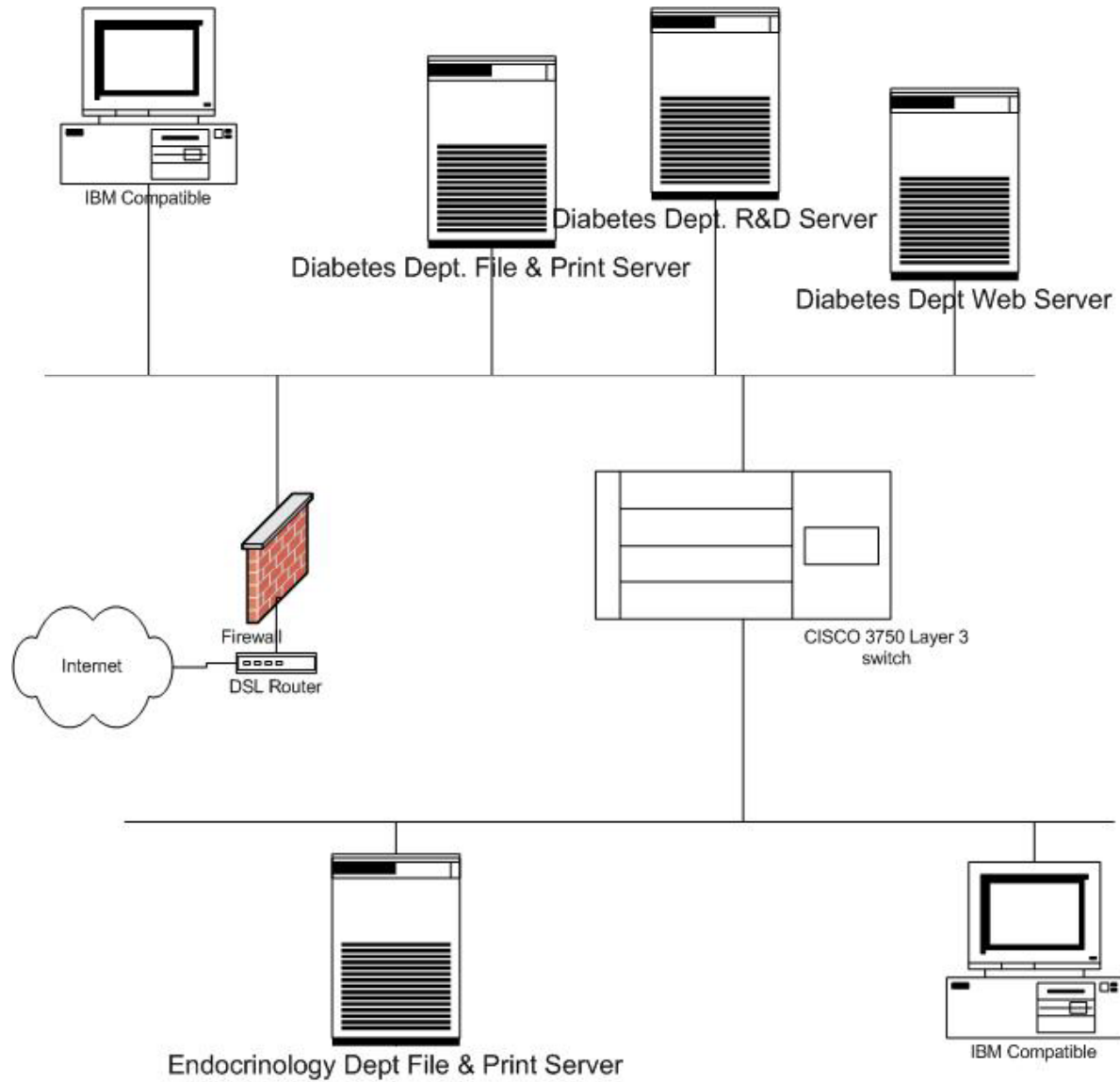
Objectives

- Test our Playbooks
- Skill Assessment
- Recognition of Policy Violations
- Feedback:
 - Value of test
 - Improvements in planning
 - Improvements in execution

TEST 1

- Test Time & Location
- Prep Time
- Roles
- The Scenario
- Highlights

Network Diagram



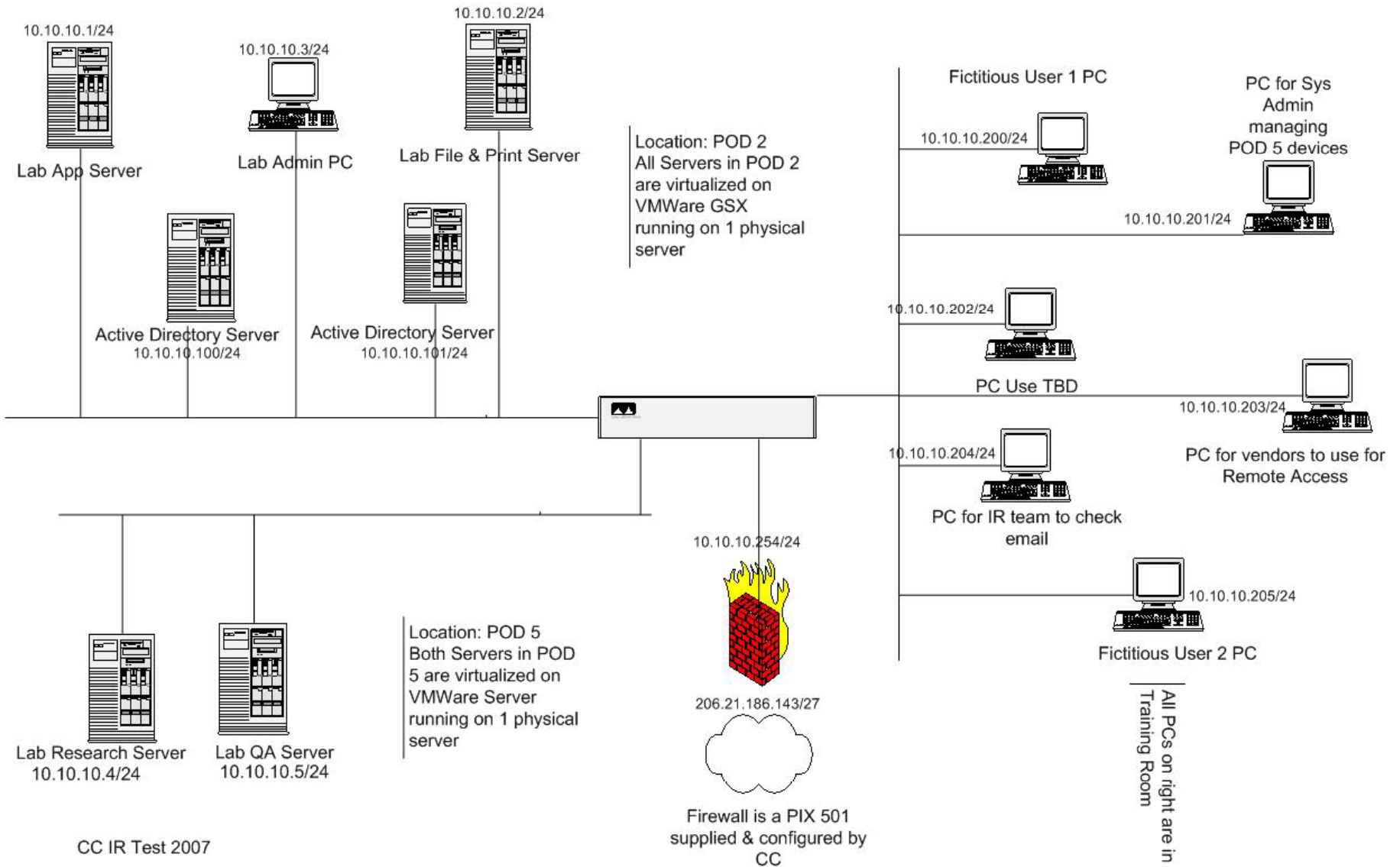
TEST 2



O-ISC '08
Ohio Information Security Conference

- Differences in
 - Test Time & Location
 - Prep Time
 - Roles & New Logistics
- The Scenario
- Kickoff Reversal
- Highlights

Network Diagram



The Post Mortem Discussions



O-ISC '08
Ohio Information Security Conference

- Assessment vs. Demonstration
- Around the Table – What does evidence suggest?
- Effects of using playbooks
- Doing analysis & jumping to conclusions
- Year 2 vs. Year 1
 - Conversations had disconnects as relayed from person to person
- Remember the question you're trying to answer
- Technical people drill deep vs. Mgmt view

- Legal, HR, Privacy, Physical Security, Internal Audit, Info Sec, Network Engineering
- Discussed Department Roles in IR
- Discussed types of threats that exist
- The best feedback from test was negative

Recognizing mud vs. blood

- Tools have specific purposes
 - Have right tool for the right problem
 - Use them with the right understanding
 - Tools gives output we need

Internal Audit's comment on tool use

Wrap Up

- First Responder Training
- A Peek at 2008
- Q&A



Questions & Answers

Contact Information



Keith Fricke
Cleveland Clinic
216-738-5121
kfricke@cchseast.org

Matt Curtin
Interhack
614-545-4225
cmcurtin@interhack.com