



Spring Conference 2006

IT Security – A Pragmatic Approach

Josh Peck
Sr. Systems Engineer
KanREN, Inc.
peck@kanren.net
<http://www.kanren.net/~peck>

IT Security

- Popular topic
- Hard to track down
- Can be costly
- CONFUSING!

Goals

- Increase understanding of IT security
- Take ownership of security processes
- Make a real difference

IT Security: What is it?

- Long Term Process
- Should Include
 - Policy / Procedure
 - Education
 - Technology

IT Security: What isn't it?

- Security Cannot be Bought
 - Not a firewall
 - Not a NIDS / NIPS
 - Not a Honeypot / Honey net
 - Not a VPN
 - Not Strong Passwords
 - Not Encryption
 - Not a Simple Budget Line Item

IT Security is not Simple

- IT Security is not a collection of parts
- “But we spent our entire security budget, aren’t we safe?”

Areas of Focus

- Best Practices
- Risk Management
- Policy / Procedure
- Education

Best Practices

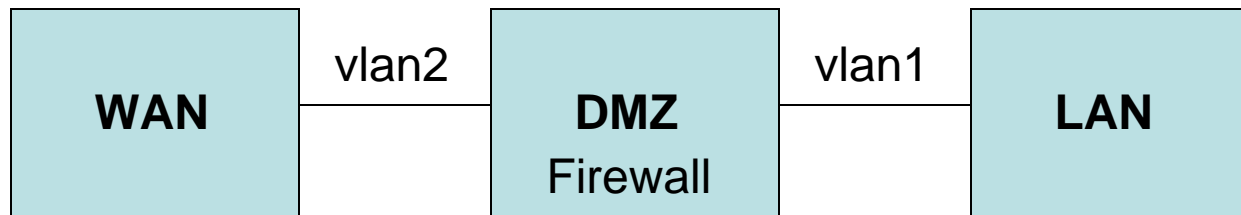
- Perimeter Security
- Encryption / VPN
- People Hacking
- Scoped Access

Perimeter Security

- Commonly Inside = Good, Outside = Bad
- Should be Integrated with Security Strategy
 - SMTP is Commonly Blocked
 - Gnutella / Instant Messaging
 - What else is denied?

Perimeter Security – DMZ

- Small Network Between WAN and LAN
- Enforce at Layer 2 with VLANs if possible



Perimeter Security – NIDS / NIPS

- Monitors Data Packets for Anomalies
 - Often Commercial
 - Can be Costly (\$\$\$)
- Josh's Great Analogy
 - Firewall = Locked Doors
 - Network Intrusion Detection = Burglar Alarm
 - Network Intrusion Prevention = ADT

Encryption / VPN

- Remote Access is Scary
- VPN
- Use Secure (encrypted) Protocols
 - Free, Just Needs Configured
 - Telnet to SSH
 - POP3 to POP3/S
 - IMAP to IMAP/S
 - SMTP to SMTP-AUTH + STARTTLS
 - HTTP to HTTPS

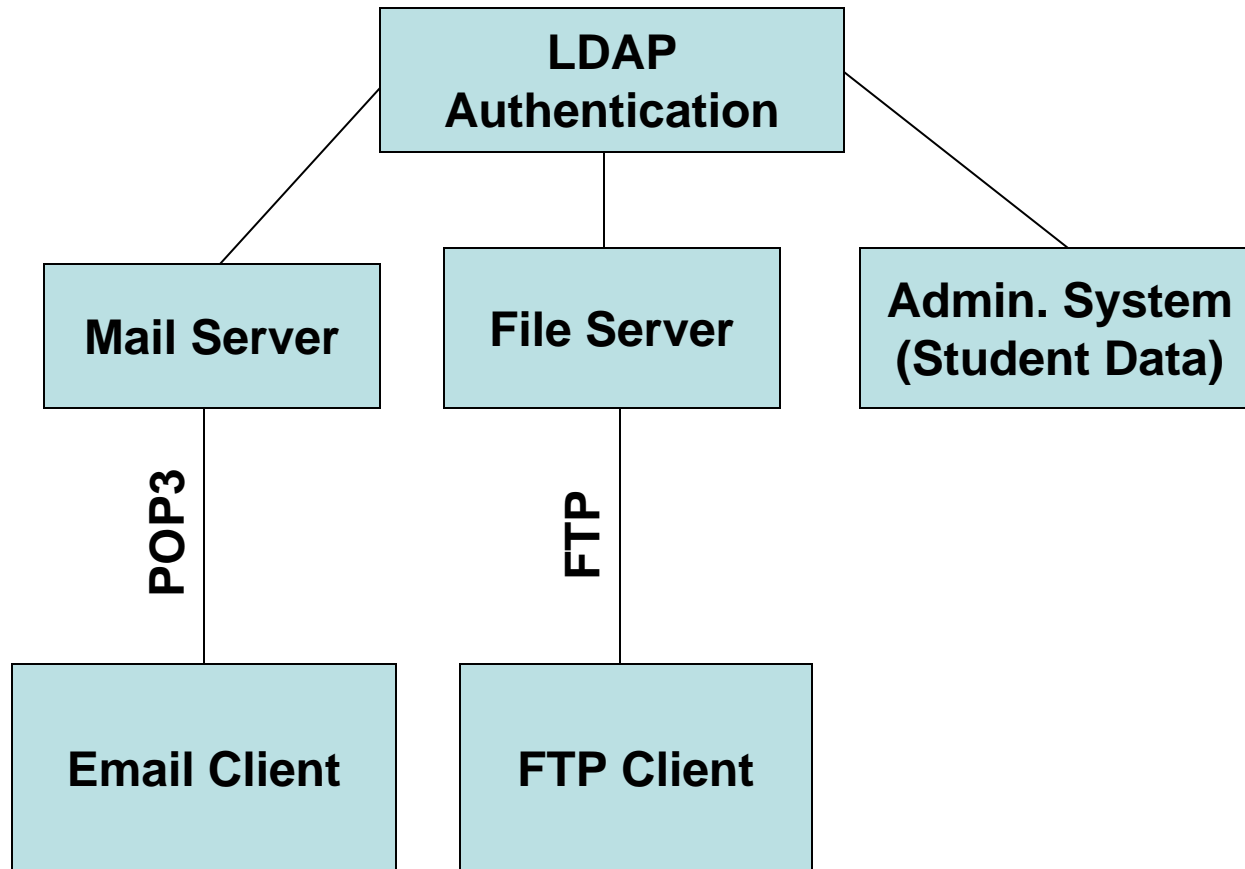
People Hacking

- You Are the Weakest Link!
- Phishing / Pharming
 - Social Engineering
- How to Mitigate Threat?
 - Education
 - Education
 - Education

Scoped Access

- Users will have Lax Security Habits
- How To Mitigate Threat?
 - Traditional Methods
 - Lock and Key with Scoped Access
 - Technical Methods
 - Scoped Accounts
 - Scoped Privileges

Scariest Architecture in the Entire World



Good Ideas

- Use VLANs
- Least Access
- Use Logging!
- Multiple Firewalls or Routed Network
- Enforce Policies with Technology

Risk Management

- Systematic Analytical Process
- Must be Pursued Frankly and Honestly
- All Threats are NEVER Fully Mitigated

Phase One: Risk Identification

- What are the Threats?
- Re-use Other Risk Assessment Processes
- IT Poses Unique Problems
 - Physical Threats
 - Logical Threats

Phase Two: Risk Analysis / Assessment

- Research and Understand Threats
- Begin Quantification

	Severity	Likelihood	Risk
Administrator Error	5	60%	1
Power Outage	10	30%	3
Equipment Theft	10	20%	2
Data Corruption	3	10%	0.3

Phase Three: Risk Mitigation

- How Will Risk be Mitigated?
- Which Risks will be Mitigated?
- Corrective Actions Suggested
 - Does Action Full Address Issue?
 - Not all Risks will be Mitigated

Phase Four: Implementation

- Implement Solutions
- Re-Use Existing Technical Procedures
- Normal Project Management

Phase Five: Maintenance / Monitoring

- Revisit Threats Periodically
- Technology is an Evolving Target

What Goes Wrong?

- Skipping to Mitigation Phase
- Failure to Understand Threats
- Ignore Real Threats, Address Easy Problems

Policies / Procedures / Guidelines

- Unpleasant and Unavoidable
- Policies
 - Formal, Reflect Legal Landscape
- Procedures and Guidelines
 - Less Formal, Reflect Technical Landscape

Policies

- Defines Acceptable Behavior
- Regulatory Compliance
- Users Aware of Protections and Responsibilities

Procedures

- Task Oriented, Sequential
- Good Procedures are Good Protection
- High Quality Processes Yield High Security

Guidelines

- Guidance in Specific Areas
- Commonly “Good Ideas”
- Examples
 - Password guidelines
 - Preferred Protocols

What Goes Wrong?

- User Rebellion!
 - Need User Buy-In
 - Need Implementer Buy-In
 - Need Management Buy-In

Education / Training: What to Do?

- Do Something!
- Integrate Security into Work-Flow
- Users Must Understand Threats
- Legal Ramifications of Doing Nothing are Great

How to Do It?

- Make it Relevant
- Get Help!
- Small Groups are Better
- Encourage Ownership

When to Do It?

- Early and Often
- New Employee Orientation
- Existing Employees May Need Caught Up

Questions?



Spring Conference 2006