

**FTA Annual Conference**



**WEB Penetration Testing and Vulnerability Analysis**

**June 10, 2008**

**Timothy R. Blevins , KDOR Chief Information Officer**

1

## WEB Penetration Testing

- What is WEB Penetration Testing?
- When should Penetration Testing Happen?
- How does an Organization Prepare?
- What does a Pen test look like?
- What is the Cost and Size of the engagement?
- How to Select a Vendor
- What is expected as an outcome?
  - Vulnerability Results
  - Reports and Documentation
- Remediation
- Best Practices and Lessons Learned
- Questions

2

## What is WEB Penetration Testing?

### Testing of WEB Facing Applications

Thin Client, File Transfer, Appliance, Portal

Looking for vulnerabilities for exploitation

Checking for appropriate controls

Probing

Vulnerability Analysis

Penetration Testing

3

## When Should Penetration Testing Happen?

### **Want to be here**

The First Time

Periodically every 12 to 18 months

Significant WEB Presence Changes

Major Architectural Changes

Large Application Launch

### **Do not want to be here**

After Disclosure or Compromise

Requirement by an Audit

4

## How does an Organization Prepare?

- Inventory WEB presence
- Prioritize Risk of Applications
- Involve Key Personnel (Bus, IT, Sec, Serv Providers)
- Understand Bus App Peak Usage/Scheduling
- Educate IT and Sec Organization on Best Practices
- Engage Private Sector IT Security Firm
- Negotiate the work plan and the engagement
- Understand Deliverables Prior to Agreement/Examples

5

## What is the Cost and Size of the engagement?

### **Duration of Engagement**

- 3 to 4 Months
- 1 Month Scoping Statement of Work
- 1 Month Coordination
- 1-2 Months Conducting/Remediating/Documenting

### **Size of Engagement**

- 3 to 5 Agency Staff
- 3 to 5 Engagement Staff

### **Cost of Engagement**

- 20K to 100K
- Depends on # of URL's
- Depth of Vulnerability Assessment

6

## What does a Pen test look like?

### **Automated Phase**

- Robots and Automated Crawlers
- Open Source Products
- Proprietary Exploitation Software

### **Manual Phase**

- Heads Down on WEB application
- Inside your authenticated rule sets
- Inside your access controls

### **Documentation of Activities and Findings**

- Reports
- Findings

7

## How to Select a Vendor

- IT Security Industry
- Avoid Using Same Vendors as Security Product Providers
- Depth of Attack vs Cost
- Change Vendors Each Engagement
- Combine High Level Engagement Firm A
- Low Level Granular Engagement Firm B

8

## What is expected as an outcome?

### Vulnerability Results/Findings

Technical Name and Brief Explanation

Difficulty of the Exploit

Sophisticated, Moderate, Trivial

Business Impact

High, Medium, Low

Remediation Suggestion

Application Specific, clear, concise

9

## Vulnerability Results Sample

### Description: SQL Injection

Functions that processed database applications within the application did not validate user supplied query parameters.

Attackers could inject arbitrary SQL statements

### Difficulty of the Exploit: Moderate

Supplying unexpected parameter inputs by manipulating query construction results in changes to output generation

### Business Impact: High

Possible to extract arbitrary information from the database

### Remediation Suggestion:

Implement data validation routines to restrict query characters to known good values; use parameterized prepared statements

10

## What is expected as an outcome?

### Reports and Documentation

Initial Vulnerability Analysis at conclusion  
of scanning by server

Final list of Vulnerabilities by application at  
end of penetration testing

Weekly Project Status Reports

### Final Report

Executive Overview

Vulnerability Analysis

Remediation and Conclusions

11

## Remediation

### **Vulnerability Analysis Results**

Apply Recommendations and Fixes as appropriate,  
by level of difficulty, business impact, and ease of fix

### **Rescanning/testing for those vulnerabilities**

Vendor provided

### **Reporting**

Same format as previously described

12

## Lessons Learned

- Service Providers can believe an unplanned attack is underway**
- Intrusion Detection Systems can create alerts**
- Intrusion Prevention Systems can deny engagement or modify results**
- Many IT Security Professional Firms use Common Tools**
- Ask for copies of engagement reports prior to committing to engagements**
- Make sure the examples are similar to your environment or platform**
- In the engagement specifications, build in some additional time for quick remediation and re-scanning at no additional cost and already included in the engagement hours**

13

## Best Practices

- Regularly Schedule Engagements Yearly**
- Rotate Security Firms with Different product Sets and Engagement Tactics**
- Remediate during the engagement, not later**
- Insure you have rescanning after remediation available**
- Instill Lessons Learned into Development and ongoing Support standards and best practices**
- Institutionalize Knowledge into IT Development and Security Staffs**
- Create a Complete Test Environment for the Engagement**
- No Major Findings re-enforce best practices**

14

## **WEB Penetration Testing and Vulnerability Analysis**

ANY QUESTIONS?

**FTA Annual Conference 2008  
Timothy R. Blevins  
KDOR Chief Information Officer  
[TRB@kdor.state.ks.us](mailto:TRB@kdor.state.ks.us)**