Summary of External Assessments Conducted on Distributed Systems

S.A.L.T. Presentation, August 2nd , 2012

Curtis McNay - Director, IT security

The Reason for the Project

- During a Board of Visitors meeting an inquiry was made concerning the security of distributed servers at the University. Subsequently, the IT Security Office (ITSO) produced a document that summarized risk presented by these distributed servers
- ITSO was then task with contracted with third party security assessors to perform assessments on a limited sampling of system listed in the original risk statement. These included systems supported by academic departments and a functional offices.
- The purpose of this document is to provide a summary of findings for these assessments

Findings

A number of servers were found with high risk vulnerabilities. These include out of date versions of critical applications, unpatched software and misconfigurations. The risk to the university includes:

- Threat to reputation
- Threat of a compromised system being used to steal credentials
- Staging for attacks on other internal and/or external systems
- Loss of departmental work and/or resources.
- Exposure of highly sensitive data

High Risk Vulnerability Findings

Out of Date Software

- Web: Apache Outdated Version
- Web: Apache HTTP Server Byte Range DoS
- MySQL < 4.0.21 mysql_real_connect() Function Remote Overflow
- PHP < 5.3.9 Multiple Vulnerabilities
- Unsupported Operating System
- Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow
- Adobe Flash Media Server < 3.5.7 / 4.0.3 Denial of Service
- Obsolete Web Server
- Oracle GlassFish Server < 3.1.1.1 Web Container Component Unspecified Vulnerability
- Web Service, Apache Tomcat

High Risk Vulnerability Findings

Unpatched Software

- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code
- Execution
- MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution
- MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution
- Multiple missing Oracle Patches
- Samba 'AndX' Request Heap-Based Buffer Overflow

High Risk Vulnerability Findings

Misconfiguration

- Anonymous FTP providing root access to system partition with writable directories
- SQL Injection possible on publicly accessible website exposing production database and all tables
- Microsoft Windows SMB Shares –Unprivileged Access to File Share
- SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability
- Web form collecting highly sensitive data using unencrypted channel, HTTP protocol. Highly sensitive data in back end database unencrypted.
- Unencrypted Login Request

Medium Risk Vulnerability Findings

Outdated Software

- Multiple Adobe Cold Fusion Vulnerabilities
- Dell OpenManage 'HelpViewer' Redirect
- Apache HTTP Server httpOnly Cookie Information Disclosure – Outdated Software

Medium Risk Vulnerability Findings

Unpatched Software

- SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability –Misconfiguration & Unpatched software
- Adobe Dreamweaver dwsync.xml Remote Information Disclosure
- Web: Cross site scripting in web applications- Misconfiguration & Coding Error
- Windows: Windows Null Session Enumeration
- mDNS DetectionServer
- Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Medium Risk Vulnerability Findings

Misconfigurations

- Web: Cross site scripting in web applications- Misconfiguration & Coding Error
- mDNS DetectionServer
- Apache WebDAV Module PROPFIND Arbitrary Directory Listing
- Web services, Cross Site Scripting In Web Applications- Misconfiguration, Coding error.
- SNMP Enabled with Default Community Strings
- SSL/TLS Information Disclosure Vulnerability – Misconfiguration/Unpatched Software
- SSL V2 Weak Key and outdated version
- PHP expose_php Information Disclosure
- Terminal Services Encryption Level is Medium or Low
- Terminal Services Doesn't Use Network Level Authentication
- Multiple Adobe Products XML External Entity (XXE) Injection - Misconfiguration, coding error