WEB AND DATABASE SECURITY BEST PRACTICES

Presented By:

Bryan Miller
CCIE, CISSP

SYRINX
TECHNOLOGIES
MOBILE.AGILE.FOCUSED

Agenda

- Introduction
- Threats
- Attack Vectors
- General Best Practices
- Web Server Security
- Database Security
- Free Tools
- Questions

Introduction

- Biography
  - 25+ Years in Information Technology
  - Positions at VCU, Circuit City, DiVX, Cabletron, Dataline, SyCom Technologies, Packet360
  - CCIE, CISSP, M.S. in Computer Science
  - President, Syrinx Technologies LLC

Threats

- Web and database servers continue to grow in complexity.
- Applications are generally written with security as an afterthought.
- New vulnerabilities are discovered every day in operating systems, application servers and in the applications themselves.
- Exploits have become very easy to obtain and use.

Attack Vectors

- Common web server vulnerabilities
  - SQL Injection
  - Cross Site Scripting (XSS)
  - Cookie tampering
  - Directory traversals
  - Privilege escalation
  - Session hijacking
  - Web defacements

Attack Vectors (cont.)

- Common database server vulnerabilities
  - Incorrect permissions
  - Account management
  - Data theft (Confidentiality)
  - Data manipulation (Integrity)
  - Denial of service (Availability)

General Best Practices

- Start with the operating system

  - Develop a hardening procedure with checklists
    - When building the server, always apply the latest patches and update as needed.
    - Remove all unnecessary services, protocols, accounts, applications, etc.
    - Where possible, install some form of host-based intrusion detection/prevention (IDS/IPS) software.

General Best Practices (cont.)

- Start with the operating system

  - Develop a hardening procedure with checklists
    - Ensure that all system account passwords are not easily guessed, cannot be found in dictionaries and comply with all applicable password policies.
    - Always hardcode TCP/IP configuration information.
    - Ensure that proper file permissions are configured correctly on all critical directories/files.

General Best Practices (cont.)

- Start with the operating system
  - Develop a hardening procedure with checklists
    - Configure logging on critical system events, such as failed logon attempts.
    - Ensure that appropriate anti-virus software is installed and configured properly.
    - Whenever possible, install and configure the server in a lab environment without direct access to the corporate network or the Internet.

General Best Practices (cont.)

- Moving on to the Application

  - After installing the web or database server application, ensure that any hotfixes, security patches or other necessary updates are installed.
  - Ensure that any application-layer account passwords are not left blank, at their defaults or set to anything that can be easily guessed using brute-force tools.
  - Ensure proper application-layer permissions are set at every layer of the application.

General Best Practices (cont.)

- Moving On to the Application
  - Modify the host-based IDS/IPS if necessary to accommodate the new application.
  - If any remote access or control components are installed, ensure that they use some form of robust encryption (not Telnet!).
  - Put procedures in place to ensure that any application patches are installed along with operating system patches.

General Best Practices (cont.)

- Moving On to the Application
  - Enable logging of critical security events.
  - Test the application from a security perspective before loading any test or live data.
  - Encrypt data whenever possible – “at rest” and “in motion”

General Best Practices (cont.)

- Don’t forget about the network

  - Control access to the servers using ACL’s where appropriate
  - Only open the minimum ports and protocols necessary
  - Use both ingress and egress filters where appropriate

Web Server Security

- Some general best practices
  - Install the web application data (the web site) on a different drive than the operating system. This eliminates a class of attacks called “directory traversals”.
  - Make sure to change all default application-layer passwords.

Web Server Security (cont.)

- Some general best practices
  - Remove all demo programs and any unnecessary components of the web server application.
  - Run as many security testing programs as possible before releasing the server for daily use.

Web Server Security (cont.)

- IIS specific best practices

  - Where possible, use the latest version of the web server software.
  - Unmap any application mappings not being used.
  - Where possible, limit the HTTP verbs that specific pages will accept.
    - For static pages, limit all access to HTTP GET only.

Web Server Security (cont.)

- IIS specific best practices
  - Remove Internet printing (IPP).
  - Remove all sample/help directories.
  - Rename O/S Administrator account.

Web Server Security (cont.)

- Apache specific best practices
  - Whenever possible, compile the application from known source code. Always check the MD5 or PGP checksums.
  - Chroot the server so directory traversal attacks are eliminated.
  - Run the web server process as a non-root user.

Web Server Security (cont.)

- Apache specific best practices
  - Change the “Server:” token in the HTTP response header to disguise the web server type.
  - Lock the password for this user and disable shell access.
  - Disable any unnecessary modules.

Web Server Security (cont.)

- Apache specific best practices
  - Remove all unnecessary directories and set proper file permissions.
  - Create appropriate startup, reload and shutdown scripts.

Database Security

- MS SQL Best Practices
  - Ensure the SA account has a non-blank password. This also applies to MSDE-based applications
  - Never configure the SA password to be the same as any other account, especially the O/S Administrator password.
  - Remove all unnecessary stored procedures, especially “xp..cmdshell”.

Database Security (cont.)

- MySQL Best Practices
  - Always set a password for the “root” account.
  - Apply application patches as appropriate.
  - Always run the database server process as a non-root user whenever possible.
  - Delete the “test” database and the default “user” account.

Database Security (cont.)

- MySQL Best Practices
  - If remote access is not needed, disable TCP/IP support.
  - Chroot the database process if possible.

Database Security (cont.)

- Oracle Best Practices
  - Always change the account passwords for the default Oracle accounts, especially the following:
    - sys
    - system
    - dbsnmp
    - outln
    - ctxsys
    - ordsys
    - mtssys
    - mdsys
    - wksys

Database Security (cont.)

- Oracle Best Practices
  - Set the proper permissions for low-privilege accounts such as dbsnmp
  - Remove the “scott/tiger” account.
  - Disable all unnecessary accounts.

Database Security (cont.)

- Oracle Best Practices
  - Configure a password in the Listener service.
  - Configure appropriate logging on security-related events.
  - Apply application patches as appropriate.

Database Security (cont.)

- PHP Best Practices
  - Run only the latest versions of PHP.
  - Make sure you validate all user input.
  - Use session info instead of cookies.
  - Avoid using variables in Include statements.
  - Turn off the display of error messages. You can still log them to a file.

Database Security (cont.)

- PHP Best Practices
  - Be very careful with global variables.
  - Make sure “magic_quotes_gpc ” support is disabled.
  - Set “safe mode on” – test before production.
  - Set file extension for all include files to “.PHP”.

Free Tools

- Operating System
  - Microsoft Baseline Security Analyzer
  - Microsoft Windows Server Update Services
  - Nessus
  - Nmap
  - Foundstone SuperScan 4
  - Metasploit

Free Tools (cont.)

- Web Servers
  - URLScan 3.1 (IIS 5.1-7)
  - IISLockdown 2.1 (IIS < 6.0)
  - Nikto (Perl)
  - N-Stalker (free and commercial)

Free Tools (cont.)

- Web Servers
  - Nessus
  - Wget
  - THCSSLCheck
  - Proxies: Achilles, Paros, WebScarab

Free Tools (cont.)

- Database Servers
  - MS SQL
    - Cain/Abel
    - SQLDict
    - SQLForce
    - SQLPing3

Free Tools (cont.)

- Database Servers
  - Oracle
    - Cain/Abel
    - TNSCMD (Perl)
    - WinSID
    - CheckPWD

Free Tools (cont.)

- Database Servers
  - MySQL
    - Cain/Abel

Questions

Thank You Very Much for Your Time and Attention!

SYRINX
TECHNOLOGIES
MOBILE.AGILE.FOCUSED