WEB & DATABASE
SERVERS
The Heart & Brains of Your Web Site

"To rise from error to truth is rare and beautiful."

Victor Hugo (1802-1885)
French poet, novelist, playwright, essayist

Introduction

Heart & brains of any eCommerce Web site:
• Heart: the Web server: all data flows through the Web server!
• Brains: the database server: all data stored and recalled from the database!
• Our goal in this chapter is to learn about Web servers: Apache & IIS

What is a Web server?

• Every time a browser connects to a Web site, it connects to a Web server.
• Web server is a program that runs on a host computer that serves up Web pages
  • It sits around waiting for clients (browsers) to connect and request Web pages
  • Can serve up: HTML documents, plain text, images, sounds, video, etc...
  • May or may not be in a static form

What is a Web server?

• Sometimes called HTTP servers because uses HTTP to communicate server ↔ client
• Run on a variety of OS’s and on a variety of budgets
• Basically, 2 Web servers:
  • Apache: Apache Software Foundation (Open Source)
  • IIS: Microsoft
• Others? Probably...

Apache Overview...

• Powerful: performance and reliability is legendary
• Feature Rich: XML support, server-side includes, URL re-writing, virtual hosting, etc...
• Modular: features can be added or removed by configuration
• Extensible: Open source means you can write your own modules and share them

Apache Overview...

• Popular: Apache now powers approximately 60% of the Web today
  • Multiplatform
  • Help, Service, Maintenance
• Free: ‘nuff said!
• Maintained by Apache Software Foundation
• Many, many resources. Book has a listing of a few.

Apache Features

• Platform Support: Almost all flavors of Linux & UNIX, VMS, AS/400, Windows, NetWare, MacOS, OS/2, Be OS...
• Virtual Hosting
  • Allows multiple Web sites to be hosted by a single Web server
  • Supports both Name-based and IP-based hosting mechanisms

Apache Features
Server Side Includes
- Similar to CGI but on a small scale
- Security risk!

Dynamic Content with CGI
- One of the original dynamic content solutions
- Used mostly with Perl or shell scripts
- Not used as much anymore. Replaced by PHP, ASP, etc.

Apache Features
- Handlers
  - Handle Web requests based on a file name
  - Much of the Web handled this way today
  - .jsp requires Java engine so set up a handler that runs the JVM
  - .asp requires the Active Server Page engine...

IIS Overview...
- IIS = Internet Information Services
- Second in popularity to Apache
- Developed by Microsoft
- Part of MS overall strategy to dominate the World... oops, I mean the Internet 😊
- Actually, quite a remarkable piece of software
- Closely integrated into Windows OS's: able to take advantage of Windows features

IIS Overview...
- "Preferred" by corporate sites because of Microsoft "backing"
- IIS will run on Windows XP Pro (not Home)
  - Limitations
    - Only 10 concurrent connections (including non-Windows software)
    - No virtual hosting
  - Uses
    - A small intranet
    - Test bed
- Big corporate sites run IIS on Windows 2000/2003/2008 Server

IIS Overview...
- IIS has many components. Web server is just one of them (email, SMTP, FTP, etc.)
- IIS features:
  - Web server:
    - Static or dynamic Web page serving
    - Server-side includes
    - CGI
  - Documentation: thorough and online
  - FrontPage Extensions: allows development and sharing of Web site resources. FrontPage needed...

IIS Overview...
- IIS features: (cont.)
  - FTP Service: file transfers to/from remote computers
  - SMTP: receive and deliver email to/from other computers. No POP3 or IMAP for users.
  - IPP: print to network printers
  - Support for Remote Desktop Access
  - Support of InterDev Remote Development

IIS Security Issues...
Microsoft has been hurt by the security issues in IIS.
This does not mean there are no security issues in Apache!
The biggest threats to IIS:
- ISAPI: Internet Server API
- Virtual Directories
- Sample Files

IIS Security Issues...
ISAPI: (cont.)
- Buffer Overflow problems:
  - Most ISAPI calls are written in C/C++, which means they are just one notch above the metal and have direct access to memory and pointers
  - Buffer overruns in C/C++ are notorious and well documented
  - Nimba & Code Red took advantage of .ida ISAPI filters buffer overflow and was able to execute arbitrary code.
  - Solution (not perfect): Remove the filters you do not use!

IIS Security Issues...
Virtual Directories
- Virtual Directories are “pointers” to other directories
- Similar to Linux “directory links” (ln)
- Allows a link between a dir in the document root and a dir on the local hard drive.
- Sound like a Problem?
- Solution:
  - the default virtual directories must be removed
  - virtual directories should not be allowed into or out of the document root

IIS Security Issues...
Sample Programs
- Sample programs are provided by MS that show how IIS features work
- Sounds like a good idea, right?
- Well, yes... unless they contain errors or reveal security issues!
- Solution:
  - Assign access rights to the directories that hold the sample files
  - Don’t use the example files “right out of the box” i.e., unmodified

Database Servers
- The DB is at the heart of every Web application
- The DB contains all of the business data: a prime target for hackers!
- Primary e-commerce DB’s: MS SQL Server & Oracle
- Other SQL based DB’s: Access, MySQL, DB2, Sybase, Informix, ...

Structured Query Language (SQL)
- SQL is a standard database command set used by all database servers
- Commands allow you to:
  - Create databases & tables
  - Query data from tables
• Delete databases & tables
• Add/Delete DB users

22 SQL Poisoning
- SQL commands that contain incorrect characters or are mistyped producing an error or incorrect results
  - Basically, any invalid SQL command
- 2 types:
  - Data producing: Poisoned SQL commands that get passed directly to the DB server and give results other than the intended
  - Error producing: like data producing but the intent is not to obtain results but see the error and get config. info

23 Microsoft SQL Server
- One of the most widely used DB servers
- Since it is so popular, it is often the brunt of attacks
- Good example of a database that grew too fast for its own good
- Vulnerabilities warrant its own book!
- We’ll discuss a few of the general ones...

24 Microsoft SQL Server
- Stored Procedures (SP)
  - SP’s are SQL commands that are stored in the DB and execute natively improving performance
    ○ Sort of a "compiled" and saved SQL command
  - SQL Server installs with many SP’s written by MS – Convenient & vulnerable

25 Microsoft SQL Server
- Stored Procedures (SP) (cont)
  - Wow!  Look at these!  Imagine the possibilities...
    ○ sp_configure
    ○ sp_password
    ○ sp_who
    ○ xp_cmdshell
    ○ xp_grantlogin
    ○ xp_loginconfig
    ○ xp_logininfo

26 Microsoft SQL Server
- Stored Procedures (SP) (cont)
  - Countermeasures:
    ○ Delete all SP’s
    ○ Restrict access to SP’s
      - Deleting may not possible:
        - Applications may highly depend on SP’s
        - Not able to test extensively due to time deadline
      - It is possible to assign Access Control Lists (ACL) to SP’s

27 Microsoft SQL Server
- Default Databases
  - “Internal system” DB’s used by the server to maintain server functionality
  - master is the main data repository for all system info
    ○ Login/user account info
    ○ Configuration settings
○ System stored procedures
• Others: msdb, model & tempdb
• Each default DB is well known and well defined (documented) and contains a series of tables an attacker can go after

28 Microsoft SQL Server
○ Default System Tables
• Tables a hacker might be interested: Sysobjects, Syslogins, others...
• Bottom line: the tables contain info about the databases themselves and can give an attacker valuable info
○ Default System & Meta-data Functions
• Functions built-in to SQL Server
• Can provide valuable info to a hacker
• Cannot be “removed” so must filter input

29 Microsoft SQL Server
○ Passwords
• SQL Server has one of the worst mistakes in DB history: username: sa, password: blank
• BIG problem if not changed immediately after install

30 Oracle
○ “Unhackable?” “Unbreakable?” I don’t think so!
○ System Tables
• Like MS SQL Server, Oracle has system tables that maintain server functionality
• These must be guarded at all costs or a hacker can obtain your business data
• Oracle has security roles and privileges that should be routinely audited

31 Oracle
○ Passwords
• Default install passwords must be changed immediately after install
• Password policies (applies not just to Oracle)
  ○ Enforce a minimum length
  ○ Enforce character complexity
  ○ Enforce word complexity
  ○ Provide password lockout
  ○ Use password expiration
  ○ Avoid password reuse

32 Oracle
○ Privileges
• Oracle provides a rich privilege system
• DB admins can attach privileges to individual DB objects
• Misconfigured privileges on system objects allow for unauthorized view of data
○ Oracle Listener
• The listener has traditionally been the entry point for hackers
• “Listens” by default on port 1521 but can be changed

33 Oracle
○ Oracle Listener (cont)
• First step to hacking the listener is to request a listener status
• This could tell the attacker:
  ○ The OS host
  ○ Listener version
○ Start date and up time
○ Listener parameters and log files
○ Available services
  • The listener vulnerabilities are version dependent and include information leakage, file writing, buffer overflows and denial of service

Summary
⊗ Vulnerabilities exist in all Web and DB servers
⊗ Remember: security is a procedure not a goal
⊗ Installed default anything is bad and must be changed ASAP
⊗ Tight password policies must be enforced
⊗ Know your DB; know how to configure it