Web Application Security

Rajendra Kachhwaha
rajendra1983@gmail.com

October 6, 2015

Outline

Web Server Architecture:

1. Web Server: Internet Information Services
2. Internet Information Services: Versions
3. Features of IIS
4. Attacks on a Web Server

Web Server: Internet Information Services

1. Internet Information Services (IIS, formerly Internet Information Server) is an extensible web server created by Microsoft for use with Windows NT family.
2. IIS supports HTTP, HTTPS, FTP, FTPS, SMTP and NNTP.
3. It has been an integral part of the Windows NT family since Windows NT 4.0, though it may be absent from some editions (e.g. Windows XP Home edition), and is not active by default.
4. The first Microsoft web server was a research project at the European Microsoft Windows NT Academic Centre (EMWAC), part of the University of Edinburgh in Scotland, and was distributed as freeware.
5. However, since the EMWAC server was unable to handle the volume of traffic going to Microsoft.com, Microsoft was forced to develop its own web server, IIS.

Web Server: Internet Information Services:Versions

1. IIS 1.0 was initially released as a free add-on for Windows NT 3.51.
2. IIS 2.0 was included with Windows NT 4.0.
3. IIS 3.0, which was included with Service Pack 2 of Windows NT 4.0, introduced the Active Server Pages dynamic scripting environment.
4. IIS 4.0 was released as part of the "Option Pack" for Windows NT 4.0. It introduced the new MMC-based administration application.
5. IIS 5.0 shipped with Windows 2000 and introduced additional authentication methods, support for the WebDAV protocol, and enhancements to ASP.
6. IIS 5.1 was shipped with Windows XP Professional, and was nearly identical to IIS 5.0 on Windows 2000.

Web Server: Internet Information Services:Versions

7. IIS 6.0, included with Windows Server 2003 and Windows XP Professional x64 Edition, added support for IPv6 and included a new worker process model that increased security as well as reliability.
8. IIS 7.0 was a complete redesign and rewrite of IIS, and was shipped with Windows Vista and Windows Server 2008. IIS 7.0 included a new modular design, a hierarchical configuration system allowing for simpler site deploys, a new Windows Forms-based management application and increased support for the .NET Framework.
9. IIS 7.5 was included in Windows 7 and Windows Server 2008 R2. It has improved WebDAV, FTP modules & command line administration in PowerShell. It also introduced TLS 1.1 and TLS 1.2 support and process isolation for application pools.

Web Server: Internet Information Services:Versions

10. IIS 8.0 is only available in Windows Server 2012 and Windows 8. IIS 8.0 includes SNI (binding SSL to hostnames rather than IP addresses), Application Initialization, centralized SSL certificate support, and multicore scaling on NUMA hardware, among other new features.
11. IIS 8.5 is included in Windows Server 2012 R2 and Windows 8.1. This version includes Idle worker-Process page-out, Dynamic Site Activation, Enhanced Logging, ETW logging, and Automatic Certificate Rebind.
12. IIS 10 is included in Windows Server 2016 and Windows 10. This version includes support for HTTP/2.

Features of IIS:

IIS 6.0 and higher support the following:

1. Authentication

IIS 7.0 has a modular architecture. Modules, also called extensions. These modules are individual features that the server uses to process requests and include the following:

2. Security modules: Used to perform many tasks related to security in the request-processing pipeline, such as specifying authentication schemes, performing URL authorization, and filtering requests.
3. Content modules: Used to perform tasks related to content in the request-processing pipeline, such as processing requests for static files, returning a default page when a client does not specify a resource in a request, and listing the contents of a directory.

Features of IIS:

4. Compression modules: Used to perform tasks related to compression in the request-processing pipeline, such as compressing responses, applying Gzip compression transfer coding to responses, and performing pre-compression of static content.
5. Caching modules: Used to perform tasks related to caching in the request-processing pipeline, such as storing processed information in memory on the server and using cached content in subsequent requests for the same resource.
6. Logging and Diagnostics modules: Used to perform tasks related to logging and diagnostics in the request-processing pipeline, such as passing information and processing status to HTTP. sys for logging, reporting events, and tracking requests currently executing in worker processes.

Features of IIS:

IIS 7.5 includes the following additional or enhanced security features:

7. Client certificate mapping
8. IP security
9. Request filtering
10. URL authorization

IIS 8.0 offers new features targeted at performance and easier administration. The new features are:

11. Application Initialization: a feature that allows an administrator to configure certain applications to start automatically with server startup. This reduces the wait time experienced by users who access the site for the first time after a server reboot.

Features of IIS:

12. Splash page during application initialization: the administrator can configure a splash page to be displayed to the site visitor during an application initialization.
13. ASP.net 4.5 support: In IIS 8.0, ASP.net 4.5 is included by default.
14. Centralized SSL certificate support: a feature that makes managing certificates easier by allowing the administrator to store and access the certificates on a file share.

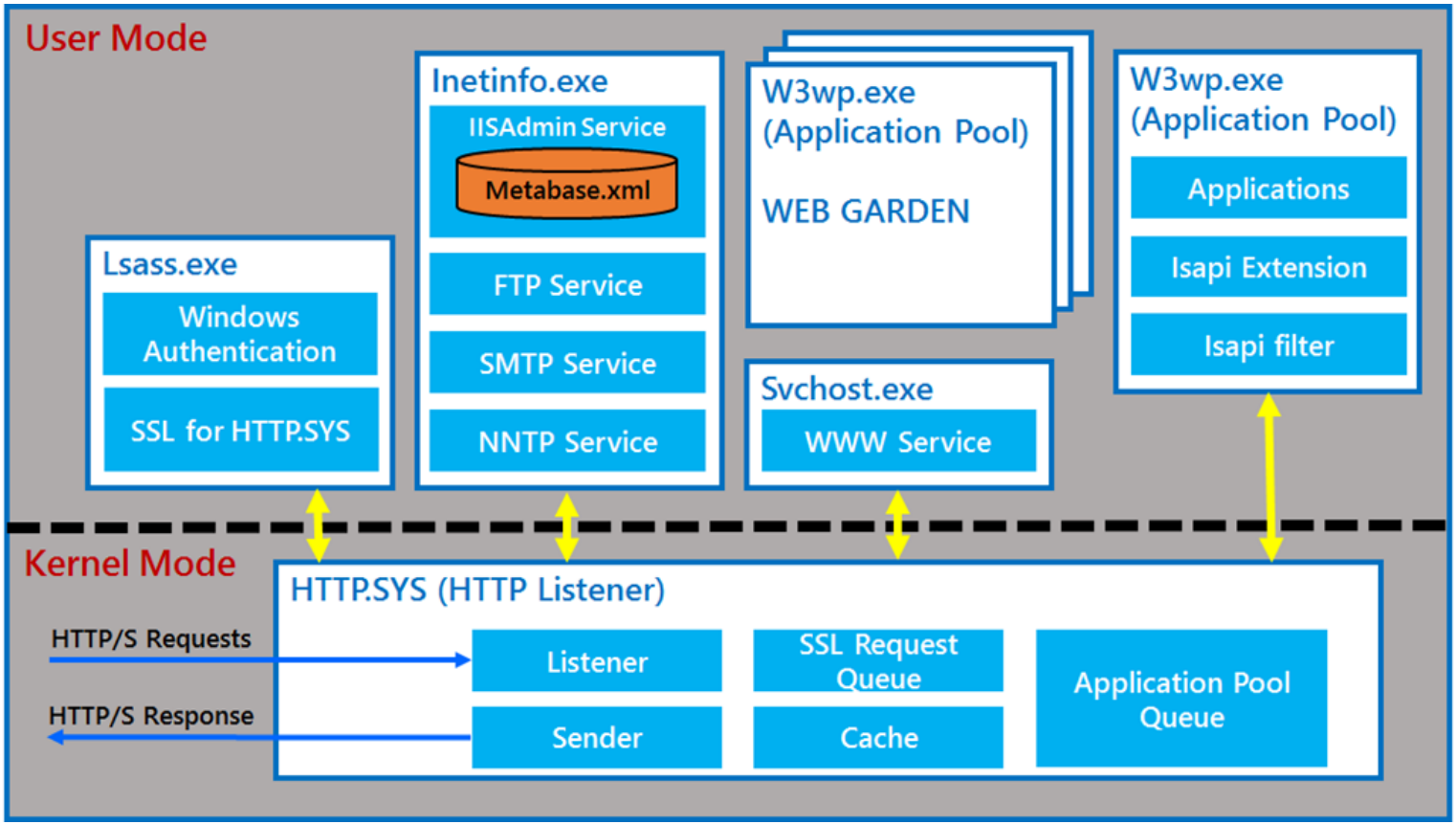
IIS 8.0 offers new features targeted at performance and easier administration. The new features are:

15. Multicore scaling on NUMA hardware: IIS 8.0 provides several configuration options that optimize performance on systems that run NUMA, such as running several worker processes under one application pool.

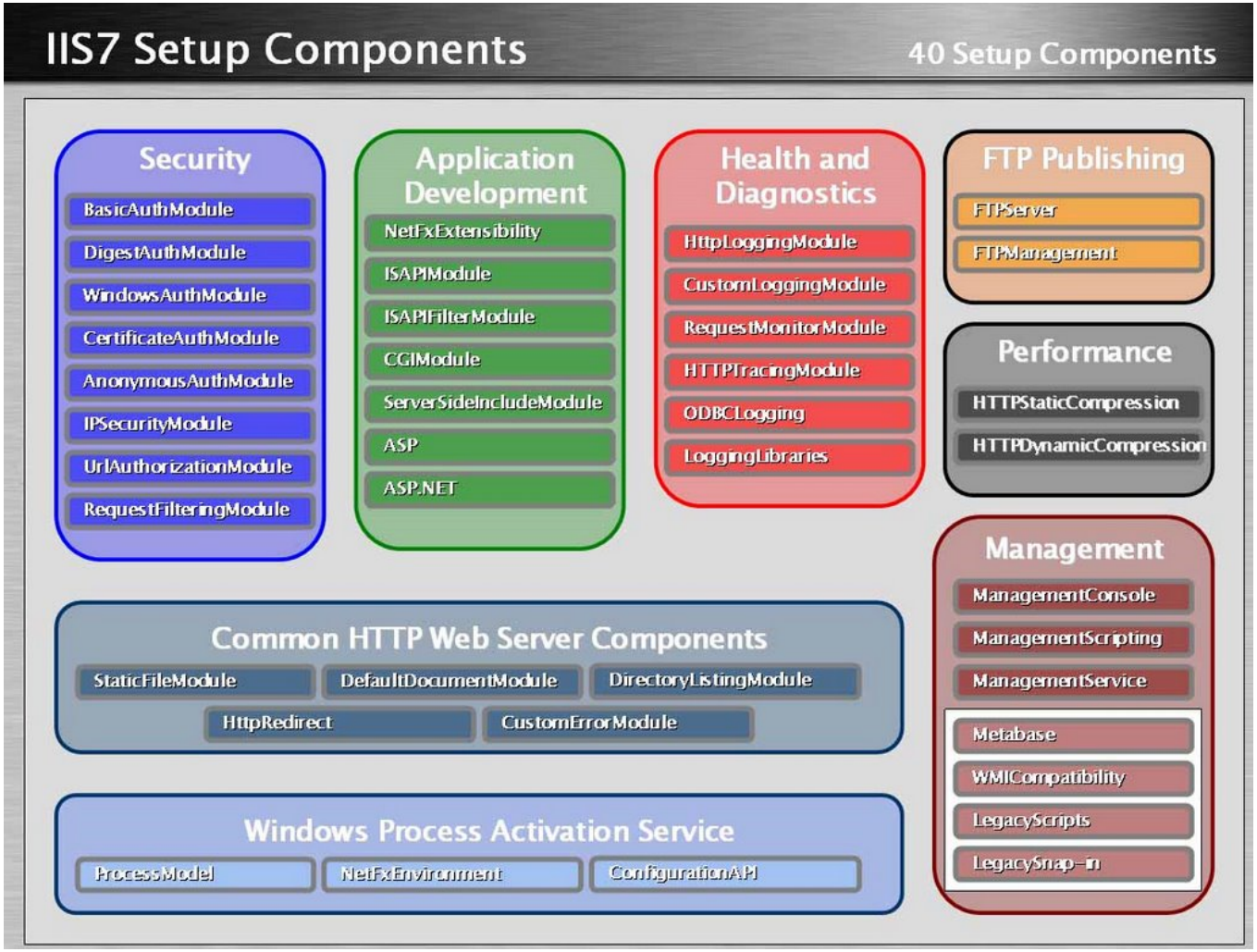
Features of IIS:

16. WebSocket Protocol Support.
17. Server Name Indication (SNI): SNI is an extension to Transport Layer Security, which allows binding of multiple websites with different hostnames to one IP address (similar to how Host Headers are used for non-SSL sites).
18. Dynamic IP Address Restrictions: a feature that enables an administrator to dynamically block IPs or IP ranges that hit the server with a large number of requests.
19. CPU Throttling: a set of controls that allow the server administrator to control CPU usage by each application pool in order to optimize performance in a multi-tenant environment.

Internet Information Services:



Internet Information Services:



Apache

1. Cost: Open source, free, no licensing fees
2. Advantages:
   - Is flexible because of ability to pick and choose various modules
   - Has enhanced security (notable, because vulnerabilities typically are attacked in Windows-based machines)
   - Has strong user-community support
   - Runs on UNIX, Windows, Linux, Mac OS
3. Disadvantage:
   - Is a process-based server, which means each simultaneous connection requires a thread that can incur significant overhead

IIS

1. Cost: Comes with Windows (could mean increased costs through licensing)
2. Advantages:
   - Is supported by Microsoft
   - Provides access to .NET framework & ASPX scripts
   - Integrates with other Microsoft services (Active Directory, MS SQL server, ASP, etc.)
3. Disadvantage:
   - Isn't able to customize as much as open-source web servers

Attacks on a Web Server

DoS/DDoS

- Jamming Networks
- Flooding Service Ports
- Misconfiguring Router
- Flooding Mail Server
- SYN Flooding attack
- Smurf Attack: A smurf attack is modification of the "ping attack" and instead of sending pings directly to the attacked system, they are sent to a broadcast address with the victim's return address. A range of IP addresses from the intermediate system will send pings to the victim, bombarding the victim machine with hundreds or thousands of pings.
- IP-Fragmentation Attack
- DNS Cache Poisoning