Overview

- Security problems
- Management issues
- Securing the operating system
- Securing web server software
- Protecting information and data in a careful and systematic manner.
- Deploying network protection mechanisms
- Maintaining the secure configuration
  - This lecture is based on NIST Special Publication 800-44 Version 2

Threats Summary

- The server may be compromised by exploiting software bugs in the web server, operating system, or active content
  - Use the compromised server to
    - To attack external entities directly (e.g., from the compromised host against an external server)
    - To attack external entities or indirectly (e.g., placing malicious content on the compromised Web server)
    - To access information on the Web server may be read or modified.
      - To gain unauthorized access to resources elsewhere in the organization.
      - To support command injection attacks or cross-site scripting.
  - Information transmitted between the Web server and the browser may be intercepted.
- Access to information and services may be denied via Denial of Service attacks (DoS or DDoS)
How to Secure Against Threats

- Be aware there are threats
- Assure that the individuals responsible are qualified and vetted
- Conduct formal risk assessment and best practices analysis and be sure they cover:
  - Written policies and procedures
  - Configuration and change control
  - Contingency and continuity planning
  - Testing, certification, and accreditation

The Threats

- The threats to web servers are made more prominent because
  - The servers are by definition exposed globally
  - Attacks are more automated and rapidly propagated
  - The array of software from network infrastructure through OS to the webserver itself to active content is more complicated and open than is desirable
  - The staff responsible for web server maintenance and content is often not adequately trained

General Principles for Security

- Simplicity: the simpler the system, the easier it is to insure correct operation
- Mediation: Access to system information and services should be wrapped by software that insures access controls
- Separation of Privilege: keep roles, rights, access as granular as possible and in the process insure least privilege.
- Defense in Depth: layer security mechanisms, particular for critical areas.
- Work Factor: as a general rule, the work required to break a system should exceed the value of the information or access obtained
- Logging: all actions should be logged with an eye to being able to identify a system failure and its causes.
Planning and Management

• Assuming qualified individuals who have been vetted and who are trained in security principles. There are at least three roles:
  • A CIO level establishes policy and cost-benefit analysis
  • A Security Manager insures practices are applied that are consistent with policy
  • A Web/System Administrator implements practices and provides evidence of conformance
• Develop a deployment plan
  • Purpose of the server
  • Network services to be provided
  • Roles and responsibilities of users who will access the web server
  • Physical and network location of the server and protections provided

Full-Blown Documentation

• When a server provides critical functions, one would expect formal specification of:
  • Organizational System Security Policies
  • Configuration/Change Control and Management
  • Risk Assessment and Management
  • Secure Programming Practices
  • Security Awareness and Training
  • Contingency, Continuity of Operations, and Disaster Recovery

Programming Practices

• The web application developer provides the basis on which security is built:
  • Authentication, authorization, and access control mechanisms are used as required.
  • Includes input validation on headers, query strings, cookies, form fields, and hidden fields.
  • Processes errors in a secure manner.
  • Insures sensitive information is transmitted processed and/or stored securely.
  • Maintains application-specific logs related to critical operations.
  • Hardens the application against application-level DoS attacks.
Regards to Operating System

• Patch and upgrade the operating system
• Remove or disable unnecessary services and applications
• Configure operating system user authentication
• Configure resource controls
• Install and configure additional security controls
• Perform security testing of the operating system.

Web Server Platforms

• Depending on the nature of the web server, a number of different platforms might be considered:
  • General OS provide minimal security and require significant setup
  • Trusted Operating Systems have been specifically configured and tested to provide maximum security
  • Web server appliances are general operating systems bundled with webserver software. They are secured within the limits of the OS and optimized for use as a web server
  • Security appliances (security gateways, content filters, authentication gateways, etc.) can also be added around the physical server to enhance security

Securing the Operating System

• Given an appropriately hardened and robust OS environment to start with, the steps to harden the OS include:
  • Patch and upgrade the OS offline or in a protected virtual lan
    • Document the steps taken
    • Note known unmitigated vulnerabilities
  • Remove or disable unneeded services
    • File and print sharing
    • Language compilers and libraries
    • Email services
    • Etc., etc., etc. -- see OS specific plans
Configure User Authentication

- Remove or disable all default accounts and groups, especially guest accounts and accounts with known passwords
- Disable any non-interactive shell accounts
- Create needed user groups and user accounts – providing only the needed access. Make access and rights group dependent
- Make sure the password policy is set appropriately – length, composition, aging, reuse, authority
- Install any advanced security mechanisms deemed appropriate – certificates, smart cards, etc.

Install Additional Security Management Options

- Anti-malware software, such as antivirus software, anti-spyware software, and rootkit detectors.
- Host-based intrusion detection and prevention software, including DoS attacks.
- Host-based firewalls, to protect the server from unauthorized access.
- Patch management software to ensure that vulnerabilities are addressed promptly.

Regards the web server software

- Patch and upgrade the Web server application
- Remove or disable unnecessary services, applications, and sample content
- Configure Web server user authentication and access controls
- Configure Web server resource controls
- Test the security of the Web server application and Web content.
Regards web server operation

• Install only necessary services
• Isolate web content to a dedicated hard drive
• Define a single directory for active content
• Disable directory listings and use of links
• Remove all sample software and monitor directories for extraneous content
• Use authentication and certificates as necessary
• Install an Intrusion detection system

Initial Configuration of the Web Software

• Install the Web server software and apply any patches.
• Create a dedicated physical disk or logical partition for Web content.
• Remove or disable all services installed by the Web server application but not required (e.g., gopher, FTP, remote administration).
• Remove, disable all default login accounts created by the Web server installation, create new accounts as needed with unique names and passwords.
• Remove all manufacturers’ documentation, examples or test files from the server, including scripts and executable code.
• If appropriate security template or hardening scripts, exist for the server, apply them.
• Reconfigure HTTP service to not report Web server and OS type and version.

Access Controls

• Access controls set by the operating systems should be consistent with the access controls set by the web server.
• A hard boundary should be set around the content that the web server can access
• In particular, make sure access is limited to:
  • Logs
  • Security related files (password files and key files)
  • Server logs and audit files
  • Configurations files – system and application
Permissions for the Web Server

- The server should run as a user, not as root or administrator
- Web content should be readable, but not writable by this user
- Web content directories should not be writable to other services
- The webserver should be allowed to write, but not read logs files
- Restrict temp file writing to a given directory, and restrict access to temp files to the process that wrote them

Dealing with DOS

- Install web content on a different drive or partition
- Limit the amount of webspace allocated for uploads if uploads are allowed
- Don’t allow uploads to be read until they have been reviewed
- Insure that there is adequate space for logs to record information
- Configure the maximum number of network connections that are allowed and throttle excessive connections form a given IP

Regards Information Access

- Make sure there is no information accessible that shouldn’t be:
  - Classified or proprietary info
  - HIPPA restricted or FERPA restricted
  - Other legally restricted
  - Information about the hidden network or infrastructure
  - Information about vulnerabilities
Use of Robots.txt

- Websites cannot control access to their website by malicious agents except by the use of access controls.
- However, sometimes, especially when content is not rigorously controlled centrally, information can inadvertently be revealed.
- Robots.txt provides a mechanism by which compliant robots can be excluded. This helps when:
  - Robots should not index some pages
  - Robots are not helpful to the site and rob bandwidth

Sample Robot.txt

- To disallow all bots from specific directories:
  - User-agent: *
  - Disallow: /images/
  - Disallow: /banners/
  - Disallow: /Forms/
  - Disallow: /Dictionary/
- To disallow all bots from the entire Web site:
  - User-agent: *
  - Disallow: /
- To disallow a specific bot (in this case the Googlebot) from examining a specific Web page:
  - User-agent: GoogleBot
  - Disallow: tempindex.htm

Positive Controls on Content

- Identify information that should be published:
  - Identify the target audience (Why publish if no audience exists?)
  - Identify possible negative ramifications of publishing the information
  - Determine if access controls are needed
- Identify who is responsible for creating, publishing, and maintaining this particular information
- Periodically review published information to confirm continued compliance with organizational policy
Collection of Personal Information

- The Privacy Act requires organizations:
  - to minimize the information collected to that which is relevant and necessary to the business purpose
  - to collect information, to the greatest extent practicable, directly from the subject individual
  - to provide subject individuals:
    - Notice that information about them is being collected, including descriptions of what data is being collected, with whom it is being shared, and what is being done with that data
    - Opportunities to opt out of data collection unless the data collection is mandatory under law.
    - Opportunities to access and review the records

Protection against Phishing

- Phishing is a social engineering attack based on email.
- A given website cannot directly prevent phishing attacks, but can take steps to help mitigate against them by:
  - Informing users about phishing and your precautions to avoid it
    - When using email provide info that the user or organization can use to validate the communication but do not disclose confidential info
    - Personalize web content to assure users they are at the correct website
    - Use token that cannot be replayed in phishing
  - Monitor for the use of phishing attacks and inform users of same

Protection against Pharming

- Pharming attacks are based on technical compromises related to DNS resolution
- Organizations can mitigate pharming attacks by:
  - Insuring current versions of DNS are installed on their servers
  - Installing server side DNS protection
  - Monitoring DNS registrations
  - Using secure connections with authentication
  - Simplifying the server name structures
  - Using pre-shared secrets
Ongoing Efforts

- Analyze log files and IDS alerts on a regular basis
- Backing up critical information regularly
- Maintain an authoritative copy of the Web content
- Establishing and test procedures for recovering from compromise
- Applying patches in a timely manner
- Testing security periodically.