การบริหารด้านการรักษาความปลอดภัยของ Web Server

Presented by

Somphol Boonjing,
CISSP, CISA, RHCE, CCNA,
MCSA/MCSE 2000/2003
somphol@wisdomwork.org

Wisdom Work, Co., Ltd.
http://www.wisdomwork.org

Word of wisdom

- INFOSEC main pillars -> C.I.A.
  - Confidentiality of ...
  - Integrity of ...
  - Availability of ...
- Each system is unique in term of security protection
  - Depending on how much you want to protect
  - There often are a price to pay in one way or another, sometimes, in form of money, sometimes in form of other trade off.
  - However, best practice does exist for whatever you want to do, but be want, nothing is perfect, after all, we live in an imperfect world

Web Server Risk Management Framework

- Asset Identification
  - Also, assess cost of your asset
- Threat Identification
- Vulnerability identification
- Risk analysis through threat and vulnerability mapping
- Quantify or quality those risks
- Finding cost effective countermeasure for those risks

Asset Identification
(What exactly are you protecting)

- Integrity of web pages
- Integrity of database content
- Confidentiality of various credentials
- Confidentiality of database content
- Integrity of ... privileges
- Integrity of OS parameters and settings
- Availability of information on hard disk
- Availability of information on databases
- Availability of integral parts
  - Domain name
  - Bandwidth / Internet connection / ...

Assess cost of your asset

- Cost of replacement
- Cost of loss of ... confidentiality
- Cost of loss of ... integrity
- Cost of loss of ... availability
- This number is actually determined what to protect and what cost
  - At the end of the day, security should be cost effective. Security shall not stand by itself, the goal is to help business achieve it mission.

Threat Identification

- Hackers
- Unauthorized access from insiders/personals
- Misuse/abuse by users
- Natural disruption
- Fire/Power shortage/etc.
- Bot
- Machine automated attacker (mostly for DoS)
  - e.g. E-mail application for google

Vulnerability Identification

- Unhardened OS (Linux/Windows)
- Ineffective access control
- ineffective firewall (gateway/host centric)
- ineffective/improper file & directory permissions
- ineffective OS options (e.g. kernel options/windows server security options)
- Unencrypted credential

Vulnerability Identification (cont)

- Unpatched software (OS/servers/applications)
  - OS (Linux/Windows)
  - Servers
    - Apache & its components (PHP, jpgraph, etc.)
    - IIS and its components
    - SSH
    - FTP
    - POP3/IMAP
    - Streaming servers
    - Squid proxy

Vulnerability Identification (cont)

- Applications
  - phpMyAdmin
  - Squirrelmail
  - Mambo
  - postNuke
  - phpBB

Risk analysis through threat and vulnerability mapping

- Denial of service
- Domain hijacking
- Hardware failure
- Intrusion through application vulnerabilities
- Intrusion through server (and its associated components) vulnerabilities
- Intrusion through improper assignment of object (file/directory/etc) privileges

Risk analysis through threat and vulnerability mapping

- Intrusion through improper handling of credentials
  - Storage
  - Transmission
- Web defacement

My favorite shortcut

- Those steps are formal, yet effective
- Following them will help you identify your protection **more thoroughly**
  - Don't forget, after all, your system is unique and require unique protection
- However, I do have some quick shortcut to offer
  - Be warn, however, that it may not represent every possible control you may want to put in place to protect you system.

My Favorite Recommendations

- Get reliable hardware
- Always update your software and its components
  - Automated update is highly recommended
    - You selection of Linux distribution also play some role here
    - Redhat Enterprise / Fedora / Debian
    - Self-compilation of software does have it drawback
  - Software do have bug
  - By software, I mean every piece of software involved

My Favorite Recommendations

- Finding ways to setup gateway/host-centric firewall, esp. the latter.
  - Access control is of extremely helpful
    - SSH does not mean for the whole world to access
    - Spoofed IP is surely a sign of bad intention
- Tighten up file and directory access control
  - Linux Posix ACL is a way to go
  - SELinux is showing a good promise

My Favorite Recommendations

- Tighten up OS security related options
  - Linux through kernel options
  - Windows through security options
- Transfer of unencrypted or too-easy-to-decrypt or decryptable credential over network
  - Sniffer is everywhere!
- Beware of credential attack through automated attack such as dictionary attack
  - Bad selection of password is the weakest link that is hard to weed out

Tools: Windows

- Windows
  - Software RAID
    - RAID1 is less troublesome
  - Windows update
  - Windows firewall (access control for incoming traffic)
  - Windows MMC's security configuraiton and analysis
  - IPSec for selected traffic encryption (e.g. FTP)

Tools: Linux

- Linux
  - Software RAID
    - RAID1 is less troublesome
  - iptables
  - Distro's automated update e.g. apt-get, up2date
  - Kernel options e.g. tcp_syncookies
  - Posix ACL
  - Apache's access control
  - MySQL's access control

Other helping tools

- Vulnerability assessment
  - X-Scan v.3.1
    - A few configuration suggestion for opening port (which should be quit a few) is worth while
    - Please understand that this kind of software does generate false positive/negative result (i.e. Interpret the output at your own discretion)

Web application design guide

- Mind the handling of credential (storage and transfer)
  - Pause after a few invalid attempt
- Guard every box of your input
  - Range check
  - Format check
  - Etc.
- Encryption/hash can be your friend
- Session management MUST be good (not as easy to implement)

Q&A

- Feel free to ask questions