

Securing the Apache Web Server

Jaqui Lynch

Mainline Information Systems
Email – jaqui.lynch@mainline.com

Session I12



Agenda

- Anatomy of a Web Transaction
- General
- Firewall and Network
- Web Server Parameters (1-8)
- Security
- Directory Access
- Tools
- UNIX versus NT
- CGI Scripts, SSL, Credit Cards
- Links
- Questions



Anatomy of a Web Transaction

What's in a URL?

- `http://www.share.org:80/sanfran/index.html`
- `Http://` gopher, ftp, http, https - protocol
- `www.share.org:80/`
- Request template
 - `sanfran/index.html`
- Methods
 - Get and post
- URL means Universal Record Locator

Anatomy of a Web Transaction

- User enters URL (server waiting for reqs)
- Client does dns lookup to find out server ip
- Client connects TCP/IP to server
- Client sends http request
- Server analyses the request, reads file from local storage, sends mime header (i.e. `text/html`) and then the text
- Server may do a dns lookup
- Server makes a log entry of the get
- Client formats according to mime header
- Each gif, animation, etc is a separate get
- Each get is a separate request

General

- Make sure you are at the latest version
 - (currently 1.3.26 and 2.0.40)
- Make sure all operating system patches are installed
- Make sure the system has been secured correctly
- All admins to have their own accounts and use sudo
- Take regular backups and test them for restores
- Policies for public_html
- Determine policies for cgi scripts
 - I.e. all scripts in a central place and they get put there after someone who knows what they are doing looks at them

Firewall & Network

- Do not accept ICMP redirects or pings on broadcast addresses
- IP source routed packets should be declined
- Do not allow packets into your network from outside that supposedly come from your network
- Do not allow packets out of your network from inside that supposedly come from outside
- Shut down all unnecessary ports on the webserver
 - Allow www, https, email out, dns and ssh/sftp
- Use secure protocols such as ssh and sftp rather than telnet and ftp

Web Server Parameters 1

- ServerAdmin real email address
- User & Group Never root
- Indexing no
 - Knowledge is power – don't allow directory listings
- ServerType
 - Standalone or inetd standalone
- MinSpareServers 5
- Max SpareServers 10
 - HARD_SERVER_LIMIT in http.h is 256



Web Server Parameters 2

- StartServers 5
- MaxClients 150
 - max concurrent threads/children
 - Helps ward off connect DOS attacks
- MaxRequestsPerChild 30
- Timeout 300
 - Wait on get, post, put, acks
 - ServerSignature off
 - Why advertise the software and version number?



Web Server Parameters 3

- Log Types
 - Referrer
 - Agent
 - Access/transfer
 - Error
 - Combined
 - Scriptlog
- Logs can now go to separate logs, or to syslog
- Put logs in their own filesystem and on their own disks in a busy system
- Only keep logs you actually will use

Web Server Parameters 4

- LogLevel
- Emerg - Emergencies - system is unusable
- Alert - Action must be taken immediately
- Crit - Critical Conditions
- Error - Error Conditions
- Warn - Warning Conditions
- Notice - Normal but significant conditions
- Info - Informational
- Debug - Debug level messages
 - Use debug when testing, info or warn the rest of the time

Web Server Parameters 5

- Keepalive (http 1.1)
 - On/off on
 - Provides for persistent connections and up to 50% latency speedup for html with many images
 - MaxKeepAliveRequests 100
 - Puts a limit on so that this connection cannot hog server resources
 - KeepAliveTimeout 15
 - Time to wait between requests before closing a persistent session
- ListenBacklog
 - Max length of queue of pending connections – may need to increase if under a TCP SYN flood attack

Web Server Parameters 6

- HostnameLookups
 - Off
 - On
 - Double
- If setting this on on a busy server consider putting a local DNS server on the system
- Can turn hostname lookups off inside of server_status and other directives as follows:
- HostnameLookups off
- `<Files ~ "\.(html|cgi)$">`
- `HostnameLookups on`
- `</Files>`
- Leave off and use logresolve to postprocess the logs

Web Server Parameters 7

- `http://www.share.org` vs `http://www.share.org/`
- `FollowSymLinks` and `SymLinksIfOwnerMatch`
 - If not on it causes multiple `lsstat` commands if use short and long URLs
 - `http://www.abc.com`
 - `http://www.abc.com/htdocs/`
 - `http://www.abc.com/htdocs/index.html`
 - `lsstat` results are not cached
 - Use `FollowSymLinks` only, and only if needed (websphere uses it)
- `AllowOverride`
 - Set to `none` or Apache will try to open the default password file (usually `.htaccess`) every time you try to access this directory

Security

- No security
- Basic
 - Password & data clear text
- Digest
 - MD5 – only data clear text
- SSL
- Server Side Includes
 - Restrict these to trusted users especially the `exec` form
- User maintained directories (`public_html`)
- `Robots.txt` and spiders/web crawlers
- Time Synchronization
 - Use NTP or similar

Directory access

- Who needs to be able to upload and change pages
- Set directory permissions and cgi permissions
- Make sure you are logging and logs are cycled and saved
- Write cron scripts to parse logs and to check permissions regularly

Tools to review

- Sudo
- Cgiwrap
- Ssh and sftp
- Hardware and software firewalls
- Web log analysers
- COPS
- Saint, ISS & Nessus
- Tripwire

Things to worry about

- Buggy versions of Apache
- Bugs in CGI scripts
- Access to unauthorized documents/data due to misconfigurations or bugs
- Denial of service attacks
- Trust relationships with other servers and databases
- Use SSL to avoid network eavesdropping
- Addons such as frontpage extensions or cold fusion



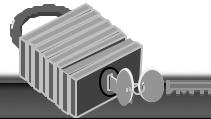
UNIX/Linux versus NT 1/2

- Hacker insurance is cheaper (5-15%) for Linux over Windows
- IIS web servers are down twice as often as Apache
- UNIX tends to be free of Viruses
 - 60,000 for Windows
 - 40 for Linux
- July 2001 Gartner recommended people move from IIS to Apache on Linux for security reasons
- Patches come out within hours not weeks



UNIX/Linux versus NT 2/2

- Easier to secure than Windows
 - 3 times as many Windows web sites get hacked (see attrition.org)
- Not susceptible to viruses and some worms such as:
 - I love you
 - Code Red
 - Nimda
 - Businesses spent over \$1.2 billion on fixing Code Red problems alone
- Securityfocus February 2002
 - IIS attacked 17 million times
 - Apache only 12,000 times



CGI Scripts

- Major source of security holes
- Do not keep any of the default ones – replace them with your own
- CGI wrappers
 - Perform security checks on scripts, change ownership or permissions, limit scope
 - Cgiwrap
 - Sbox
 - suEXEC (comes with Apache Webserver)



Adding SSL

- Download openssl, mod_ssl and install with Apache following instructions
- Code ssl directives
- Do not mix secure and insecure directories on pages
- Get a certificate from Verisign, Thawte or whoever and install it – you can use a selfsigned one temporarily

Credit Cards

- Use ssl or noone will use your site
- Never save credit card numbers unless you encrypt them
- Leave them encrypted even in your database
- Investigate credit card proxy systems such as CyberCash, SET and OpenMarket

Useful Links

- <http://www.linuxsecurity.com>
- <http://www.apache.org>
- <http://www.apacheweek.com/features/security-13> (list of known security problems in 1.3)
- <http://www.apacheweek.com/security/>
- <http://www.cert.org/>
- <Http://www.ntsecurity.com/>

Questions???

