Oracle HTTP server security

OGH DBA Dag

14 September 2010

Frits Hoogland
Who am I?

- Frits Hoogland
  - Working with Oracle products since 1996
- Interests
  - Databases
  - Application servers
  - Operating systems
  - Web techniques, TCP/IP, network security
  - Technical security, performance
- Blog: http://fritshoogland.wordpress.com
- Email: fhoogland@vxcompany.com
- Oracle ACE Director
- OakTable member
Agenda

- Oracle database versus apache
- What is security
- Firewall
- Architecture
- Webserver
- Hardening
- How to harden?

- Example: incorrect config
- HTTPS
- Scans
- Scanning yourself
- Information spilling
- Instances
- mod_security
- Recap
Show of hands

- How many of you are Oracle DBA’s?
- How many of you run public accessible webservers?
- How many of you did take precautions like modifying httpd.conf and/or hired a company to try to hack?
Oracle database vs. apache

- Difference
  - Usage
  - Accessibility
  - Placing in the network
  - Security patches / CPU
What is security?

Information security (wikipedia):

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.
Firewall!
Firewall

host.example.com

httpd (tcp/80)
Firewall

- A firewall manages network traffic
  - Denies or permits network access based on rules
  - This means either full access to daemon/service/process or no access
Firewall

- Examples of firewalls:
  - PIX (Cisco)
  - Netscreen (Juniper)
  - Firewall Software Blade (Check Point)

- But also
  - iptables (linux)
Architecture

- Host example.com
  - Firewall
  - Webserver
    - httpd (tcp/80)
    - ssh (tcp/22)
    - portmap (tcp/111)
    - rpc.statd (tcp/676)
    - sendmail (tcp/25)
    - cups (tcp/631)
  - Appserver
    - ajp13 (tcp/8007)
    - ssh (tcp/22)
    - portmap (tcp/111)
    - rpc.statd (tcp/676)
    - sendmail (tcp/25)
    - cups (tcp/631)
- Host dmz.local
  - Firewall
  - Webserver
    - httpd (tcp/80)
    - ssh (tcp/22)
    - portmap (tcp/111)
    - rpc.statd (tcp/676)
    - sendmail (tcp/25)
    - cups (tcp/631)
  - Appserver
    - ajp13 (tcp/8007)
    - ssh (tcp/22)
    - portmap (tcp/111)
    - rpc.statd (tcp/676)
    - sendmail (tcp/25)
    - cups (tcp/631)
- Appserver
  - Firewall
  - Appserver
    - tnslsnr (tcp/1521)
    - ssh (tcp/22)
    - portmap (tcp/111)
    - rpc.statd (tcp/676)
    - sendmail (tcp/25)
    - cups (tcp/631)
- Host db.local
  - Firewall
  - Appserver
    - tnslsnr (tcp/1521)
    - ssh (tcp/22)
    - portmap (tcp/111)
    - rpc.statd (tcp/676)
    - sendmail (tcp/25)
    - cups (tcp/631)
Webserver

- Clients communicate with the webserver directly.

- Traffic from and to the webserver is unfiltered.
  - In most cases
    - Juniper SSG, Cisco ASA
    - Netasq, Astaro, Sonicwall, Fortinet
    - Snort inline
Webserver

- Apache http daemon
  - Functionality
  - Configuration

- Default configuration after install
FastCGI echo

Request number 48, Process ID: 69810

No data from standard input.

Request environment:

```
FCGI_ROLE=RESPONDER
TZ=America/Chicago
DOCUMENT_ROOT=/webapps/local/htdocs
FORMS60_WEB_CONFIG_FILE=/webapps/local/htdocs/forms60/formsweb.cfg
HTTP_ACCEPT=application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png, */*
HTTP_ACCEPT_ENCODING=gzip, deflate
HTTP_ACCEPT_LANGUAGE=en-us
HTTP_CONNECTION=keep-alive
HTTP_HOST=localhost:9999
HTTP_REFERER=http://www.google.nl/search?hl=nl&source=hp&q=inurl%3Afcgi-bin%2Fecho&meta=&aq=f&aqf=aql=&oq=&gs_rfai=
HTTP_USER_AGENT=Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-us) AppleWebKit/531.22.7 (KHTML, like Gecko) Version/4.0 ORACLE=home/oracle
ORACLE_HOME=/webapps/local/oracle
PATH=.:usr/bin:/etc/usr/sbin:/usr/ucb:/usr/dt/bin:/usr/bin/X11:/sbin
PERL5LIB=/webapps/local/oracle/Perl/perl/lib/5.0503:/webapps/local/oracle/Perl/perl/lib/site_perl/5.005
REMOTE_ADDR=
REMOTE_PORT=43201
SCRIPT_FILENAME=/webapps/local/oracle/Perl/cgi-bin/echo
SCRIPT_URI=http://localhost/cgi-bin/echo
SERVER_ADDR=
SERVER_ADMIN=
SERVER_NAME=
SERVER_PORT=80
SERVER_SIGNATURE=
Oracle HTTP Server Powered by Apache/1.3.19 Server at localhost Port 80

SERVER_SOFTWARE=Oracle HTTP Server Powered by Apache/1.3.19 (Unix) PHP/4.4.3 mod_ssl/2.8.1 OpenSSL/0.9.5a mod_fastcgi/2.2.10
UNIQUE_ID=S96af6EHCM0AAG-gVF8
GATEWAY_INTERFACE=CGI/1.1
```
Hardening

- Any public accessible service should be configured to only do what it is intended to do.

- This means:
  - All excess services and functionality disabled
  - Services and functionality which are needed limited as much as possible
How to harden?

- Webserver scanner: Nikto2
  - Demo: usage of nikto
+ Uncommon header 'tcn' found, with contents: choice
+ ETag header found on server, inode: 3425418, size: 20042, mtime: 0x43e7685d;493cf3fe
+ Number of sections in the version string differ from those in the database, the server reports: oracle-application-server-1
0g/10.1.2.0.2oracle-http-serveroracleas-web-cache-10g/10.1.2.0.2(g;max-age=0+0;age=0;ecd=173870093575,0) while the database has: 10.1.3.1.0. This may cause false positives.
+ Oracle-Application-Server-10g/10.1.2.0.2oracle-HTTP-ServerOracleAS-Web-Cache-10g/10.1.2.0.2(G;max-age=0+0;age=0;ecd=173870093575,0) appears to be outdated (current is at least 10.1.3.1.0)
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE, POST, PUT, DELETE, CONNECT, PATCH, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ HTTP method ('Allow' Header): 'CONNECT' may allow server to proxy client requests.
+ HTTP method ('Allow' Header): 'PROPFIND' may indicate DAV/WebDAV is installed. This may be used to get directory listings if indexing is allow but a default page exists.
+ HTTP method ('Allow' Header): 'PROPPATCH' indicates WebDAV is installed.
+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web server.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in httpd.conf or restrict access to allowed hosts.
+ OSVDB-3233: /index.html.de: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
+ OSVDB-3233: /index.html.en: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
+ OSVDB-3233: /index.html.es: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
+ OSVDB-3233: /index.html.fr: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
+ OSVDB-3233: /icon.png: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
+ OSVDB-3233: /icons/README: Apache default file found.
How to harden?

- **Webserver scanner:** Nikto2
  - Demo: usage of nikto

- **Global vulnerability scanner:** Nessus
  - Demo: usage of nessus 4.2
<table>
<thead>
<tr>
<th>Host</th>
<th>Progress</th>
<th>Total</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Open Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.12</td>
<td>98%</td>
<td>175</td>
<td>16</td>
<td>25</td>
<td>109</td>
<td>25</td>
</tr>
</tbody>
</table>
How to harden?

- Webserver scanner: Nikto2
  - Demo: usage of nikto

- Global vulnerability scanner: Nessus
  - Demo: usage of nessus 4.2

- Scan, resolve findings, scan, resolve, etc.
How to harden?

- Upgrades can alter behavior
- Upgrades can introduce new findings
- Configuration changes can add/remove behavior

- Scans are no guarantee for having a correct configuration
Example: incorrect config

- We got a host: oel5-http / 10.0.1.12
- This host has a webserver at 7777/tcp
  - Default port of an ohs version 11.1 on linux

- Open ports:

```bash
vx1t090101:~ fritshoogland$ nmap 10.0.1.12 -PN
Starting Nmap 4.85BETA8 ( http://nmap.org ) at 2010-05-04 14:49 CEST
Interesting ports on 10.0.1.12:
Not shown: 999 filtered ports
PORT     STATE SERVICE
7777/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 25.92 seconds
```
Example: incorrect config

- The host and webserver was hardened.

- Some administrator tried to configure something in apache, and added to httpd.conf:

  ProxyRequests On
  ProxyVia On
  AllowCONNECT 25 22 80 443

  - Probably to use some proxy functionality
  - Application keeps functioning correctly
    - Let’s see what this introduces...
Friday, June 22, 12

[oracle@oel5-http ~]$ mail
"/var/spool/mail/oracle": 1 message 1 unread
>U 1 hacker@yoursite.com Tue May 4 16:33 12/419
&
Message 1:
From: hacker@yoursite.com Tue May 4 16:33:37 2010
Date: Tue, 4 May 2010 16:32:52 +0200
From: hacker@yoursite.com

I mailed using your sendmail!!

&
Example: incorrect config

host.example.com

Firewall

host.dmz.local

Webserver

httpd (tcp/7777)

ssh (tcp/22)

portmap (tcp/111)

rpc.statd (tcp/676)

sendmail (tcp/25)

cups (tcp/631)
HTTPS

Q: Does HTTPS make your site more secure?
HTTPS

- Same host: oel5-http / 10.0.1.12
- This host has a webserver at 4443/tcp
  - Default SSL port of an ohs version 11.1 on linux

- Open ports:

```
vxlt090101:~ fritshoogland$ nmap -PN 10.0.1.12

Starting Nmap 4.85BETA8 ( http://nmap.org ) at 2010-05-05 14:45 CEST
Interesting ports on 10.0.1.12:
Not shown: 999 filtered ports
PORT     STATE SERVICE
4443/tcp open  pharos
Nmap done: 1 IP address (1 host up) scanned in 19.00 seconds
```
HTTPS

- HTTPS encrypts communication
  - It doesn’t make your site more secure

- It’s not possible to access sendmail, though
  - A proxy relays communication
  - This means a ‘connect’ will try to do an SSL handshake with sendmail
Most scans are done in an automated way

- MOSTLY simple scans, searching for known vuln.
  (from apache access_log:)
  - CONNECT <host> :<port>
  - GET ../..../etc/passwd
  - GET /scripts/..%.c0%af../winnt/system32/cmd.exe?+/c+dir+c:\
  - GET /scripts/root.exe?/c+dir+c:\

- Some are targeted attacks
  - Often careful investigations
  - Often hardly visible
    - Low pace
    - Different ip addresses
Scanning yourself

- To harden for the ‘outside’,
- you need to scan from the ‘outside’!

This is doable with ‘tor’
- Tor is implemented as a proxy
  - It hops a few tor hosts
  - Then comes out somewhere randomly
  - After 10 minutes, it re-does this, and comes out somewhere else
  - It’s not very fast...
- Any tool which is able to use a proxy can use it
  - Nessus does not use a proxy
Information spilling

- A webserver ‘spills’ information about itself
  - This is controlled with the ‘ServerTokens’ directive
  - Ranges from ‘Full’ (most information):

```
vxt090101:~ fritshoogland$ printf "HEAD / HTTP/1.0\n\n" | nc 10.0.1.12 7777
HTTP/1.1 200 OK
Date: Thu, 06 May 2010 07:59:57 GMT
Server: Oracle-Application-Server-11g/11.1.1.2.0
Oracle-HTTP-Server (Unix) mod_ssl/11.0.0.0.0 OtherSSL/0.0.0 mod_plsql/11.1.1.0.0 mod_onsint/2.0
Last-Modified: Sun, 25 Apr 2010 12:22:40 GMT
ETag: "25d84f-2b16-4850eb7692400"
Accept-Ranges: bytes
Content-Length: 11030
Connection: close
Content-Type: text/html
Content-Language: en
```
Information spilling

– To ‘Prod’ (least information):

vxlt090101:~ fritshoogland$ printf "HEAD / HTTP/1.0

" | nc 10.0.1.12 7777
HTTP/1.1 200 OK
Date: Thu, 06 May 2010 08:06:04 GMT
Server: Oracle-Application-Server-11g
Last-Modified: Sun, 25 Apr 2010 12:22:40 GMT
ETag: "25d84f-2b16-4850eb7692400"
Accept-Ranges: bytes
Content-Length: 11030
Connection: close
Content-Type: text/html
Content-Language: en
Information spilling

– Lesser known is ‘custom’
- Which lets you specify the Server field (!):

In httpd.conf:

\textbf{ServerTokens} custom "Ping/Pong"

vxlt090101:~ fritshoogland$ printf "HEAD / HTTP/1.0\n\n" | nc 10.0.1.12 7777
HTTP/1.1 200 OK
Date: Thu, 06 May 2010 08:12:16 GMT
\textbf{Server: Ping/Pong}
Last-Modified: Sun, 25 Apr 2010 12:22:40 GMT
ETag: "25d84f-2b16-4850eb7692400"
Accept-Ranges: bytes
Content-Length: 11030
Connection: close
Content-Type: text/html
Content-Language: en
Information spilling

- No guarantee, just a precaution
  - Oracle 11.1.1.2.0 HTTP Server => Apache 2.2.13

- This is what the HMAP nessus plugin says:

  This web server was fingerprinted as : Apache/2.2.11 (Gentoo) mod_ssl/2.2.11 OpenSSL/0.9.8k

  which is not consistent with the displayed banner : Ping/Pong
By default, the webcache spills too:

```
vxl090101:~ fritshoogland$ printf "HEAD / HTTP/1.0\n\n" | nc 10.0.1.12 7785
HTTP/1.1 200 OK
Date: Thu, 06 May 2010 08:54:31 GMT
ETag: "25d84f-2b16-4850eb7692400"
Accept-Ranges: bytes
Content-Length: 11030
Content-Type: text/html
Content-Language: en
Connection: Close
Server: Oracle-Fusion-Middleware/11g (11.1.1.2) Ping/
Pong Oracle-Web-Cache-11g/11.1.1.2.0
(N;ecid=19496115347,0)
Last-Modified: Sun, 25 Apr 2010 12:22:40 GMT
```
Information spilling

- Web cache manager
  - Properties, Security settings
    - Servertokens: full/prod/none
  - When set to none:

```
vxl090101:~ fritshoogland$ printf "HEAD / HTTP/1.0\n\n" | nc 10.0.1.12 7785
HTTP/1.1 200 OK
Date: Thu, 06 May 2010 09:02:13 GMT
ETag: "25d84f-2b16-4850eb7692400"
Accept-Ranges: bytes
Content-Length: 11030
Content-Type: text/html
Content-Language: en
Connection: Close
Server: Ping/Pong (N;ecid=19496588444,0)
Last-Modified: Sun, 25 Apr 2010 12:22:40 GMT
```
Information spilling

- This is what HMAP nessus plugin says:

Nessus was not able to exactly identify this server. It might be:

Apache/2.2 (Mandriva Linux)
Oracle AS10g/9.0.4 Oracle HTTP Server OracleAS-Web-Cache-10g/9.0.4.0.0 (N)
Apache/2.0.50-54 (Unix)

The fingerprint differs from the known signatures on 4 point(s).
Ports < 1024

- On Linux/Unix requires root privileges
  - Webcache:
    - webcache_setuser.sh setroot oracle
    - set port 80 in admin site
  - Oracle HTTP Server:
    - chown root $ORACLE_HOME/ohs/bin/.apachectl
    - chmod 6750 $ORACLE_HOME/ohs/bin/.apachectl
    - change portnumber in httpd.conf

- chroot jail
  - No common practice with Oracle products
  - Would break OPMN
Instances

- New configuration setup
  - Used with ‘webtier’ and Weblogic server
  - Idea probably borrowed from Bea weblogic

- All variable files are put in directory structure
  - ‘Webtier’: OPMN, OHS, WebCache
  - Structure resides inside $ORACLE_HOME, in a directory beneath ‘instances’
mod_security

- Apache module
  - Function: OSI Layer 7 firewall
  - Used to be installed with 10g AS
    - But not configured.
  - Not delivered anymore
mod_security

- Some websites need filtering
  - Filtering inside SSL/HTTPS
  - Scanner&Robot detection
  - Protocol enforcement
  - Limit argument number, name length
  - Filtering of known attacks
  - Ability to log & block simple DoS attacks
  - Possibility to specify your specific application URL’s
mod_security

- It’s easy to add mod_security...
  - Add the EPEL repository
    
    ```
    ```
  
  - Install mod_security
    
    ```
    # yum install mod_security
    ```
  
  - Copy relevant files
    
    ```
    $ cp /etc/httpd/modules/mod_security2.so $ORACLE_HOME/ohs/modules/
    $ cp /etc/httpd/conf.d/mod_security.conf $ORACLE_INSTANCE/config/OHS/<name>/moduleconf/
    $ cp -r /etc/httpd/modsecurity.d $ORACLE_INSTANCE/config/OHS/<name>/
    ```
  
  - Modify the path’s in mod_security.conf to this instance.
mod_security

- Example:
  - “CONNECT localhost:25 HTTP/1.0” with telnet
  - Now results in “403 Forbidden”
  - Registration in modsecurity audit file:

--7d565676-A--
[20/May/2010:09:27:40 +0200] S-TkbH8AAAEEABQLqt4AAABF 10.0.1.2 55491 10.0.1.12 7777

--7d565676-B--
CONNECT localhost:25 HTTP/1.0

--7d565676-F--
HTTP/1.1 403 Forbidden
Content-Length: 210
Connection: close
Content-Type: text/html; charset=iso-8859-1
mod_security

- Some of the rules it triggered:

**Request missing a Host header**

**CONNECT is not an accepted method**

**And intercepted based on score!**
Recap

- Apache vs. Oracle database administration
- Apache configuration is specialised task
- Oracle HTTP Server 11.x security
- This presentation only touched the surface of securing (public) websites
- This presentation was about the webserver, which is very static of nature. An application server is very dynamic of nature...
Q & A

Thank you for attending!
Bibliography & Links

- Google hacking
  - [http://www.thenetworkadministrator.com/googlesearches.htm](http://www.thenetworkadministrator.com/googlesearches.htm)

- Corkscrew (getting ssh through a proxy)
  - [http://www.agroman.net/corkscrew/](http://www.agroman.net/corkscrew/)

- Center for Internet Security (security configuration benchmarks)
  - [http://www.cisecurity.org/](http://www.cisecurity.org/)

- Mod_security (apache http audit / filter)

- nmap (network mapper / scanner)
  - [http://nmap.org/](http://nmap.org/)
Bibliography & Links

- **hping (packet generator and analyzer)**
  - [http://www.hping.org/](http://www.hping.org/)

- **Wireshark (protocol analyzer)**
  - [http://www.wireshark.org/](http://www.wireshark.org/)

- **Nessus (vulnerability scanner)**
  - [http://www.nessus.org/nessus/](http://www.nessus.org/nessus/)

- **OpenVAS (open source vulnerability scanner)**

- **Metasploit (creating tools and using exploits)**

- **Nikto (web server scanner)**
  - [http://cirt.net/nikto2](http://cirt.net/nikto2)
Bibliography & Links

- **WebScarab (http(s) analyzer / manipulator)**

- **Burpsuite (web application attacker platform)**
  - [http://portswigger.net/suite/](http://portswigger.net/suite/)

- **OWASP (web application security project)**
  - [http://www.owasp.org/index.php/Main_Page](http://www.owasp.org/index.php/Main_Page)