HTTP Fingerprinting and Advanced Assessment Techniques

Saumil Shah
Director, Net-Square

Author: “Web Hacking - Attacks and Defense”
BlackHat Asia 2003, Dec 18, Singapore
The Web Hacker’s playground
Looking through the key-hole

• All we can see is HTTP.
• Front-end web server - it all begins here.
• First line of defence.
  • Worms
  • Script kiddies
  • Focussed attacks
The Evolution of Web Defense

- Tight web server configuration.
- Web server plug-in filters.
- Secure coding.
- Security by obscurity.
Security by obscurity

- Who is running IIS? … Not me!
- Web server target acquisition:
  - largely by banner grabbing

```
$ nc 192.168.7.247 80
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Content-Location: http://192.168.7.247/Default.htm
Date: Fri, 01 Jan 1999 20:09:05 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Fri, 01 Jan 1999 20:09:05 GMT
ETag: W/"e0d362a4c335be1:ae0"
Content-Length: 133
```
Security by obscurity

- Patch web server binaries to change server banner.
  - e.g. “Microsoft-IIS/5.0” rewritten to be “Apache/1.3.26”
- If source is available, recompile with different server banner.
  - e.g. “Apache/1.3.26” rewritten to be “WebSTAR”
- Works well in defeating certain automated attacks / script kiddies.
Security by obscurity

- Web server configuration rules / plug-ins to disguise the server header.
- Re-order HTTP header fields, change cookie names, filter certain responses, etc.

```
$ nc 192.168.7.247 80
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Date: Fri, 01 Jan 1999 20:06:24 GMT
Server: Apache/1.3.19 (Unix) (Red-Hat/Linux) mod_ssl/2.8.1 OpenSSL/0.9.6 DAV/1.0.2 PHP/4.0.4pl1 mod_perl/1.24_01
Content-Location: http://192.168.7.247/Default.htm
Last-Modified: Fri, 01 Jan 1999 20:06:24 GMT
ETag: W"e0d362a4c335be1:ae0"
Accept-Ranges: bytes
Content-Length: 133
Content-Type: text/html

with ServerMask 2.0
```
HTTP Fingerprinting

- Objective: To accurately determine the underlying web server platform.
- Also attempt to uncover any plug-ins, app servers, etc.
- Based on implementation assumptions / peculiarities of the HTTP protocol spec.
HTTP Fingerprinting

- Fingerprinting logic
  - Decision-tree based methods
  - Statistical methods
  - Neural Network based methods

- Fingerprinting engine
  - Set of test cases, carefully chosen
  - Response-tree
  - Weight vectors
HTTP Fingerprinting Techniques

- Deviation from HTTP RFCs
- Behaviour not specified by the HTTP RFCs
- Default behaviour
- Header field order
- Implementation peculiarities
- Error analysis
- Cookie strings
- … similar to OS fingerprinting
HTTP Fingerprinting - Accuracy

- Choice of test cases
- Decision-trees are hard to scale
- Choice of result weights
- Scoring system
- Training input set (for neural networks)
httprint - advanced web fingerprinting

- Identifies web servers, despite obfuscation.
  - Does not rely on banner strings.
  - No string comparison, whatsoever.
  - Overcomes the customisable features of HTTP.
- Paper:
httprint – Features

- Available in GUI and command-line
  - Windows, Linux, FreeBSD and Mac OS X
  - Download from: http://net-square.com/httprint/
- Can easily add server signatures.
- Can import from nmap XML output - selects known web server ports automatically.
- All NEW! Confidence rating technique.
Banner Reported: Apache-AdvancedExtranetServer/2.0.44 (Mandrake Linux/11mdk) mod_perl/1.99_08 Perl/v5.8.0 mod_ssl/2.0.44 OpenSSL/0.9.7a PHP/4.3.1

Banner Deduced: Apache/2.0.x

<table>
<thead>
<tr>
<th>Web Server Version</th>
<th>Instances</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache/2.0.x</td>
<td>126</td>
<td>81.29</td>
</tr>
<tr>
<td>Apache/1.3.[4-24]</td>
<td>118</td>
<td>64.83</td>
</tr>
<tr>
<td>Apache/1.3.27</td>
<td>117</td>
<td>62.94</td>
</tr>
<tr>
<td>Apache/1.3.26</td>
<td>116</td>
<td>61.09</td>
</tr>
<tr>
<td>Apache/1.3.[1-3]</td>
<td>113</td>
<td>55.74</td>
</tr>
<tr>
<td>Apache/1.2.6</td>
<td>113</td>
<td>55.74</td>
</tr>
<tr>
<td>Agranat-EmWeb</td>
<td>72</td>
<td>10.29</td>
</tr>
<tr>
<td>Stronghold/4.0-Apache/1.3.x</td>
<td>66</td>
<td>7.13</td>
</tr>
<tr>
<td>Netscape-Enterprise/4.1</td>
<td>59</td>
<td>4.28</td>
</tr>
<tr>
<td>Com21 Cable Modem:</td>
<td>56</td>
<td>3.31</td>
</tr>
<tr>
<td>Oracle Servlet Engine:</td>
<td>55</td>
<td>3.02</td>
</tr>
<tr>
<td>Microsoft-IIS/6.0:</td>
<td>55</td>
<td>3.02</td>
</tr>
<tr>
<td>Microsoft-IIS/5.1:</td>
<td>55</td>
<td>3.02</td>
</tr>
<tr>
<td>Microsoft-IIS/5.0 ASP.NET:</td>
<td>55</td>
<td>3.02</td>
</tr>
</tbody>
</table>

No obfuscation.
Verification of testing.
**Banner Reported:** WebSTAR  
**Banner Deduced:** Apache/2.0.x

<table>
<thead>
<tr>
<th>Banner</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache/2.0.x:</td>
<td>80</td>
<td>51.61</td>
</tr>
<tr>
<td>Com21 Cable Modem:</td>
<td>79</td>
<td>49.15</td>
</tr>
<tr>
<td>Apache/1.3.26:</td>
<td>78</td>
<td>46.76</td>
</tr>
<tr>
<td>Apache/1.3.27:</td>
<td>78</td>
<td>46.76</td>
</tr>
<tr>
<td>Apache/1.3.[4-24]:</td>
<td>77</td>
<td>44.44</td>
</tr>
<tr>
<td>Apache/1.3.[1-3]:</td>
<td>72</td>
<td>33.94</td>
</tr>
<tr>
<td>SMC Wireless Router 7004VWBR:</td>
<td>72</td>
<td>33.94</td>
</tr>
<tr>
<td>dwhttpd (Sun Answerbook):</td>
<td>72</td>
<td>33.94</td>
</tr>
<tr>
<td>EMWHTTPD/1.0:</td>
<td>68</td>
<td>26.76</td>
</tr>
<tr>
<td>Microsoft-IIS/5.1:</td>
<td>68</td>
<td>26.76</td>
</tr>
<tr>
<td>Microsoft-IIS/5.0 ASP.NET:</td>
<td>68</td>
<td>26.76</td>
</tr>
<tr>
<td>Netscape-Enterprise/4.1:</td>
<td>64</td>
<td>20.60</td>
</tr>
<tr>
<td>AOLserver/3.5.6:</td>
<td>62</td>
<td>17.87</td>
</tr>
<tr>
<td>Apache/1.2.6:</td>
<td>62</td>
<td>17.87</td>
</tr>
<tr>
<td>TightVNC:</td>
<td>59</td>
<td>14.20</td>
</tr>
<tr>
<td>Microsoft-IIS/5.0:</td>
<td>58</td>
<td>13.09</td>
</tr>
</tbody>
</table>

Recompiled Apache banner patching. Easy to tell
Banner Reported: Apache/1.3.23 (Unix)
Banner Deduced: Microsoft-IIS/5.0

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Count</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft-IIS/5.0</td>
<td>124</td>
<td>80.00</td>
</tr>
<tr>
<td>Microsoft-IIS/5.1</td>
<td>119</td>
<td>69.34</td>
</tr>
<tr>
<td>Microsoft-IIS/5.0 ASP.NET</td>
<td>119</td>
<td>69.34</td>
</tr>
<tr>
<td>Microsoft-IIS/4.0</td>
<td>92</td>
<td>27.43</td>
</tr>
<tr>
<td>Microsoft-IIS/6.0</td>
<td>82</td>
<td>17.67</td>
</tr>
<tr>
<td>Apache/1.3.26</td>
<td>79</td>
<td>15.26</td>
</tr>
<tr>
<td>Apache/1.3.27</td>
<td>78</td>
<td>14.50</td>
</tr>
<tr>
<td>Apache/1.3.[1-3]</td>
<td>77</td>
<td>13.77</td>
</tr>
<tr>
<td>Apache/1.2.6</td>
<td>77</td>
<td>13.77</td>
</tr>
<tr>
<td>Apache/1.3.[4-24]</td>
<td>77</td>
<td>13.77</td>
</tr>
<tr>
<td>Netscape-Enterprise/4.1</td>
<td>70</td>
<td>9.27</td>
</tr>
<tr>
<td>Apache/2.0.x</td>
<td>69</td>
<td>8.72</td>
</tr>
<tr>
<td>Agranat-EmWeb</td>
<td>67</td>
<td>7.67</td>
</tr>
<tr>
<td>Oracle Servlet Engine</td>
<td>63</td>
<td>5.81</td>
</tr>
<tr>
<td>Microsoft-IIS/URLScan</td>
<td>56</td>
<td>3.24</td>
</tr>
<tr>
<td>Com21 Cable Modem</td>
<td>55</td>
<td>2.94</td>
</tr>
</tbody>
</table>

Servermask: 80% confidence that the underlying server is Microsoft-IIS/5.0
httpprint – Win32 GUI interface
httprint - nmap imports

- Can import from nmap’s XML outputs.
- nmapporlist.txt
  - identifies candidate HTTP ports
  - SSL flag
  - customisable
httpprint – Reports

- Slick HTML reports!

<table>
<thead>
<tr>
<th>host</th>
<th>port</th>
<th>ssl</th>
<th>banner reported</th>
<th>banner deduced</th>
<th>icon</th>
<th>confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.cnn.com">www.cnn.com</a></td>
<td>80</td>
<td></td>
<td>Netscape-Enterprise/6.1 AOL</td>
<td>Netscape-Enterprise/4.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.ibuyspy.net">www.ibuyspy.net</a></td>
<td>80</td>
<td></td>
<td>Microsoft-IIS/6.0</td>
<td>Microsoft-IIS/6.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.hp.fi">www.hp.fi</a></td>
<td>80</td>
<td></td>
<td>Microsoft-IIS/4.0</td>
<td>Microsoft-IIS/4.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.zope.org">www.zope.org</a></td>
<td>80</td>
<td></td>
<td>Zope/(unreleased version, python 2.2.3, linux2)</td>
<td>Microsoft-IIS/6.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ZServer/1.1b1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.apache.org">www.apache.org</a></td>
<td>80</td>
<td></td>
<td>Apache/2.0.48-dev (Unix)</td>
<td>Apache/2.0.x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Now in CSV format as well. Import at will!
- XML reports in enterprise version.
Improved Fuzzy Logic method for picking the best match.

Allows us to identify false positives.

Indicates if a server signature is not present within the set of known signatures.
httprint - Managing Signatures

• Signature database - ASCII text file.
• If a signature does not exist, cut-and-paste the httprint output from the unknown server.

Microsoft-IIS/4.0
CD2698FD6ED3C295811C9DC5811C9DC5050C5D2594DF1BD04276E4BB811C9DC5
0D7645B5811C9DC509DB9B3E9D69031D6014C217811C9DC5811C9DC580FF2CD2
FCC535BE2CE6923E2CE6923811C9DC5E2CE69272576B769E2CE69262CEAB43E
6ED3C295E2CE692009DB9B3E811C9DC5811C9DC56ED3C2956ED3C295E2CE6923
6ED3C2956ED3C295811C9DC5E2CE69276ED3C295
icon: iis4_5.gif

# 30/07/03
Microsoft-IIS/5.0
CD2698FD6ED3C295E4B1653082C10D64050C5D2594DF1BD04276E4BB811C9DC5
0D7645B5811C9DC52A200B4C9D69031D6014C217811C9DC5811C9DC52655F350
FCC535BE2CE6923E2CE69232FCDA61AE2CE69272576B769E2CE69262CD2698FD
6ED3C295E2CE692009DB9B3E811C9DC5811C9DC56ED3C2956ED3C295E2CE6923
6ED3C2956ED3C295811C9DC5E2CE69276ED3C295
icon: iis4_5.gif
httprint - Applications

- Proper target selection for assessment.
- Detect 802.11 APs from the wired network.
- Web enabled devices (printers, storage, etc)

<table>
<thead>
<tr>
<th>host</th>
<th>port</th>
<th>ssl</th>
<th>banner reported</th>
<th>banner deduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.50.50.117</td>
<td>80</td>
<td></td>
<td>Microsoft-IIS/5.0</td>
<td>Microsoft-IIS/4.0</td>
</tr>
<tr>
<td>10.50.50.100</td>
<td>8080</td>
<td></td>
<td>Netscape-Enterprise/6.0</td>
<td>Netscape-Enterprise/6.0</td>
</tr>
<tr>
<td>10.50.50.36</td>
<td>80</td>
<td></td>
<td>Microsoft-IIS/5.0</td>
<td>Microsoft-IIS/4.0, Microsoft-IIS/5.0, Microsoft-IIS/5.0 ASP.NET</td>
</tr>
<tr>
<td>10.50.50.40</td>
<td>80</td>
<td></td>
<td>-</td>
<td>Hewlett Packard xjet</td>
</tr>
<tr>
<td>10.50.50.155</td>
<td>8080</td>
<td></td>
<td>Microsoft-IIS/5.0</td>
<td>Microsoft-IIS/5.0 ASP.NET</td>
</tr>
<tr>
<td>10.50.50.27</td>
<td>80</td>
<td></td>
<td>Snap Appliances, Inc./3.0.566</td>
<td>Snap Appliances, Inc./3.x</td>
</tr>
<tr>
<td>10.50.50.108</td>
<td>80</td>
<td></td>
<td>Apache/1.3.26 (Unix)</td>
<td>Apache/1.3.26</td>
</tr>
<tr>
<td>10.50.50.101</td>
<td>80</td>
<td></td>
<td>-</td>
<td>SMC Wireless Router</td>
</tr>
</tbody>
</table>

httprint © 2003 net-square
### htpprint - Real Disguised Servers

- Report below shows five real servers:

<table>
<thead>
<tr>
<th>host</th>
<th>port</th>
<th>ssl</th>
<th>banner reported</th>
<th>banner deduced</th>
<th>icon</th>
<th>confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.walmart.com">www.walmart.com</a></td>
<td>80</td>
<td></td>
<td>Microsoft-IIS/5.0</td>
<td>Apache/2.0.x</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.foundstone.com">www.foundstone.com</a></td>
<td>80</td>
<td></td>
<td>WebSTAR</td>
<td>Apache/2.0.x</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.port80software.com">www.port80software.com</a></td>
<td>80</td>
<td></td>
<td>Yes we are using ServerMask</td>
<td>Microsoft-IIS/5.1, Microsoft-IIS/5.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.ubizen.com">www.ubizen.com</a></td>
<td>80</td>
<td></td>
<td>web server</td>
<td>Apache/2.0.x</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.datek.com">www.datek.com</a></td>
<td>80</td>
<td></td>
<td>Ameritrade Web Server</td>
<td>Netscape-Enterprise/4.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- In accordance with Netcraft results.

htprint © 2003 net-square
httpprint - Pitfalls

- Can compare against only KNOWN signatures.
- Global redirects:
  - 301/302 for everything
- Global authentication restriction:
  - 401 auth required
- Timeouts / flaky servers.
- Confidence ratings help identify false positives.
Other attempts in HTTP fingerprinting

- hmap | amap | vmap | nmap

<table>
<thead>
<tr>
<th>hmap</th>
<th>amap</th>
<th>vmap</th>
<th>nmap</th>
<th>httprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>YES</td>
</tr>
</tbody>
</table>

- obfuscated banners
- num. of requests

- 180+ (http)
- 1* (http)
- 7
- 1* (http)
- 21
HTTP Response Codes

- Customised error pages.
- A non existent page should return an HTTP 404 code.
- Many servers return:
  - 301/302 - redirect to some starting page
  - 200 OK - to fool crawlers
  - …and other customised codes.
- Cannot rely on server’s response codes.
Page Signatures

- Objective: To accurately identify proper HTTP response codes.
- Minimize false positives.
- Greatly helps in automated testing.
- Can be extended beyond error detection
  - e.g. group similar pages together
Page Signatures

- Each HTTP response has a page signature.
- Content independent.
- Ability to overlook random content.
- Constant length.
- Computation time: $O(n)$
- Comparison time: $O(k)$

200:A302E6F1DC10112A5AF8624E5EA11B367F93DD04
Not Found

The requested URL /junk was not found on this server.

Apache/1.3.26 Server at 192.168.7.70 Port 8222

$ nc 192.168.7.70 8222
GET /junk HTTP/1.0

HTTP/1.1 404 Not Found
Date: Tue, 04 Feb 2003 06:22:00 GMT
Server: Apache/1.3.26 (Unix) mod_perl/1.26 mod_ssl/2.8.9 OpenSSL/0.9.6e
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
<head>
<title>404 Not Found</title>
</head>
<body>
<h1>Not Found</h1>
The requested URL /junk was not found on this server.<p>

</body>
</html>
Customised error page

Sorry!

Random number: 1198361.67040379

The link you requested http://192.168.7.2/junk was not found

Please contact the site administrator at root@dev.null if you feel this is in error. Alternately, try searching with Google

In 1 minute, you will be refreshed back to the main page

<html><body><H1>Sorry!</H1><p>Random number: 318405.070147527</p>The link you requested http://192.168.7.2/junk was not found<p>Please contact the site administrator at root@dev.null if you feel this is in error. Alternately, try searching with Google</p>In 1 minute, you will be refreshed back to the main page<p><FORM method=GET action=http://www.google.com/search><IMG SRC=http://www.google.com/logos/Logo_40wht.gif border=0 ALT=Google align=absmiddle><INPUT TYPE=text name=q size=15 maxlength=255><INPUT type=submit name=btnG VALUE=Search></FORM></body></html>
Dealing with random content

- Page signatures are independent of content


- All of the above are 404 pages.
- Though their content may change, their signature doesn’t.
Application Fingerprinting

- apprint - prototype application server fingerprinting tool.
- COMING SOON!
- Identify the underlying Application Server plugged in to the front-end web server.
- e.g. Weblogic running on IIS, Tomcat running on Apache, etc.
- Based on Page Signatures.
Reverse Proxy Servers

- Web proxy servers may work both ways!
- Typically meant to allow users from within a network to access external web sites.
- May end up proxying HTTP requests from the outside world to the internal network.
- e.g. Compaq Insight Manager
- Usually happens when the front end web server proxies requests to back end app servers.
Reverse Proxying

Web Client

10.0.1.2

GET http://10.0.1.2/ HTTP/1.0

acmetravel.com

10.0.1.1

DB

10.0.1.2
Port Scanning through Proxies

- Issue multiple GET/CONNECTS requests to the proxy:
  - GET http://10.0.1.2:21/ HTTP/1.0
  - GET http://10.0.1.2:135/ HTTP/1.0
  - GET http://10.0.1.2:139/ HTTP/1.0
- Use Page signatures to identify accurately if a port is open on an internal host.
- Content-Location: headers!
  - divulge internal IP addressing scheme
Better CONNECTivity

- HTTP CONNECT can be used to open up a bi-directional TCP connection.
- Originally intended for SSL traffic.
- Often overlooked.
- Ability to tunnel arbitrary TCP data over an HTTP proxy connection.
- Once CONNECTed, the proxy simply passes the TCP data back and forth.
The problem: to connect to an internal Term Server

We know www.acmetravel.com:8001 allows reverse proxying.
We know that 10.0.1.2 port 3389 is open
CONNECTivity through proxies

./datapipe 3389 10.0.1.2 3389 acmetravel.com 8001

CONNECT http://10.0.1.2:3389/ HTTP/1.0
datapipe_http_proxy

- Modified original datapipe (1995 - Todd Vierling).
- Can establish TCP connections using CONNECT.
- Once established, TCP connections handed over to the calling client.
- Can handle multiple connections.
- http://net-square.com/datapipe_http/
CONNECTivity through proxies

./datapipe 3389 10.0.1.2 3389 acmetravel.com 8001

CONNECT http://10.0.1.2:3389/ HTTP/1.0
Connection is now established with remort port 3389
CONNECTivity through proxies

./datapipe 3389 10.0.1.2 3389 acmetravel.com 8001

CONNECT http://10.0.1.2:3389/ HTTP/1.0
Bi-directional RDP data passes through the established connection.
CONNECTivity through proxies

- Can be extended to any TCP protocol.
  - 3389 Terminal Server
  - 1433 MS SQL Server
  - 22 SSH
  - … whatever you want!
- As long as the proxy CONNECTs you through.
Automated Web Security Assessment

- The need for overcoming HTTP’s customisable aspects:
  - Server banner strings
  - Response codes
- Improving accuracy.
- Using core concepts to extend assessment techniques.
Closing Thoughts

- “You can’t patch (or hide) carelessness”.
- Web Hacking: Attacks and Defense
  Saumil Shah,
  Shreeraj Shah,
  Stuart McClure
Thank you!

saumil@net-square.com

http://net-square.com/

BlackHat Asia 2003, Dec 18, Singapore