



# HTTP Fingerprinting and Advanced Assessment Techniques

**Saumil Shah**

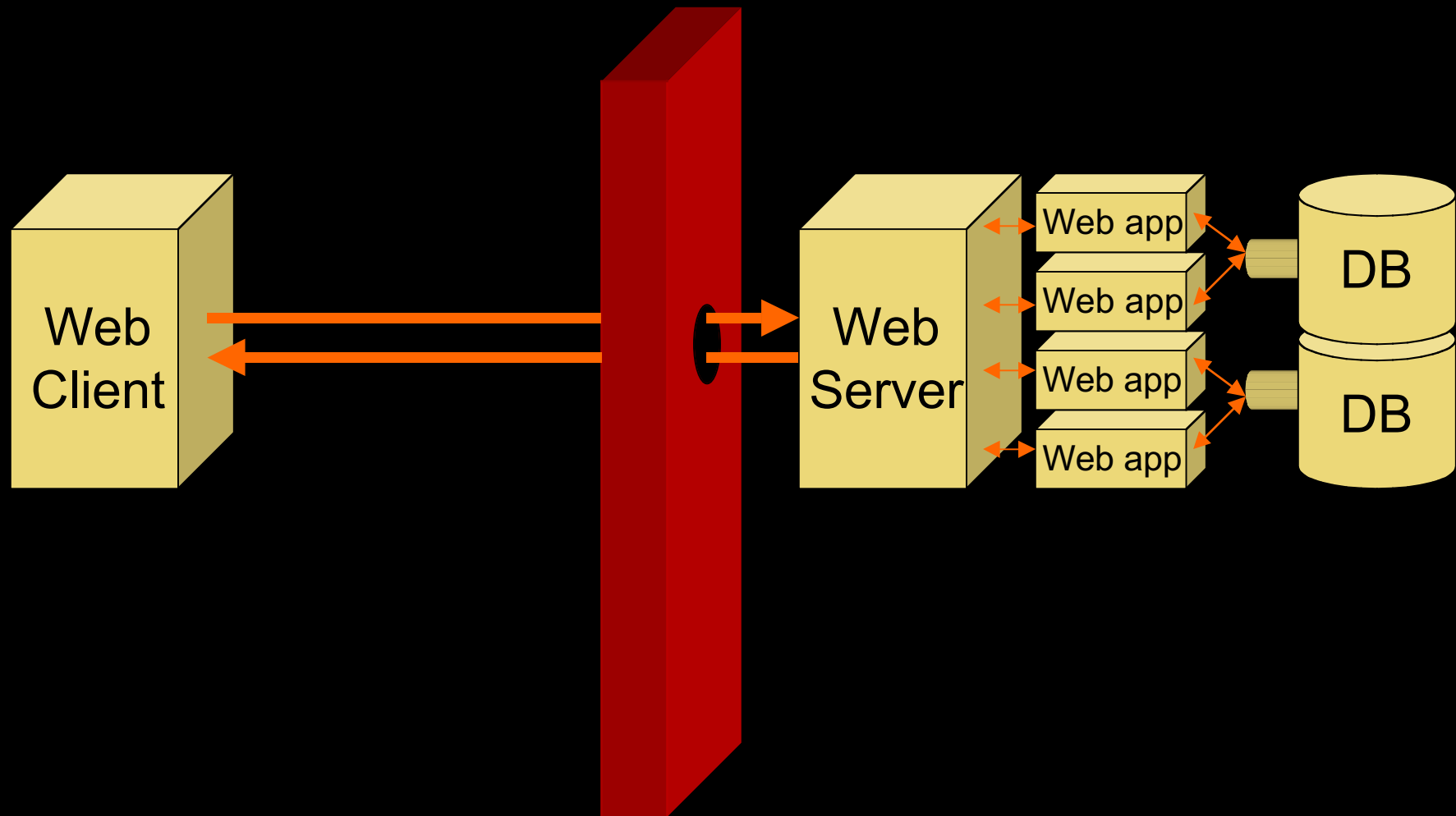
**Director, Net-Square**

**Author: "Web Hacking - Attacks and Defense"**

**BlackHat Asia 2003, Dec 18, Singapore**



# The Web Hacker's playground



# 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.



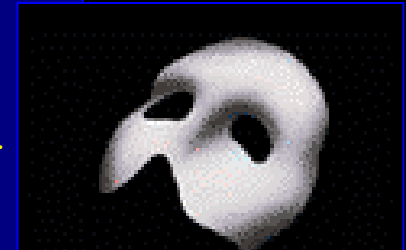
# Security by obscurity

- 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/4.0.4p11 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)



# httpprint - 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:
  - [http://net-square.com/httpprint/httpprint\\_paper.html](http://net-square.com/httpprint/httpprint_paper.html)

# 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.
- New confidence rating technique.



# httprint - Confidence Ratings

- 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.



# httpprint - example 1

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**

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

No obfuscation.

Verification of testing.



# httpprint - example 2

Banner Reported: **WebSTAR**  
Banner Deduced: **Apache/2.0.x**

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

Recompiled Apache  
banner patching.  
Easy to tell



# httpprint - example 3

Banner Reported: **Apache/1.3.23 (Unix)**

Banner Deduced: **Microsoft-IIS/5.0**

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

Servermask:  
80% confidence that  
the underlying server  
is Microsoft-IIS/5.0



# httpprint – Win32 GUI interface

httpprint version 0.200

Input File  
:\Documents and Settings\Administrator\Desktop\win32\input.txt Load  txt  nmap

Signature File  
C:\Documents and Settings\Administrator\Desktop\win32\signatu

Host	Port	Banner Reported	Banner Deduced	Conf.%
www.cnn.com	80	Netscape-Enterprise/6.1 AOL	Netscape-Enterprise/4.1	69.03
www.ibuyspy.net	80	Microsoft-IIS/6.0	Microsoft-IIS/6.0	58.71
www.hp.fi	80	Microsoft-IIS/4.0	Microsoft-IIS/4.0	60.65
www.zope.org	80	Zope/(unreleased version, python 2.2.3, ...	Zope/2.6.0 Apache Proxied ZServer/1.1...	62.58
www.apache.org	80	Apache/2.0.48-dev (Unix)	Apache/2.0.x	72.90

Netscape-Enterprise/6.1 AOL  
811C9DC5FCCC535A811C9DC5811C9DC5811C9DC594DF1BD04276E4BB811C9DC5  
811C9DC5811C9DC52A200B4C4D0ACB9C11DDC7D7811C9DC51F3B8C162655F350  
FCCC535B811C9DC5FCCC535B811C9DC5E2CE69272576B769E2CE6926811C9DC5  
811C9DC5FCCC535A811C9DC56ED3C2956ED3C2956ED3C2956ED3C2956ED3C295  
6ED3C2956ED3C295811C9DC5E2CE6927E2CE6920

Netscape-Enterprise/4.1: 107 69.03  
Netscape-Enterprise/6.0: 87 32.36  
Microsoft-IIS/5.1: 83 27.04  
Microsoft-IIS/5.0 ASP.NET: 83 27.04

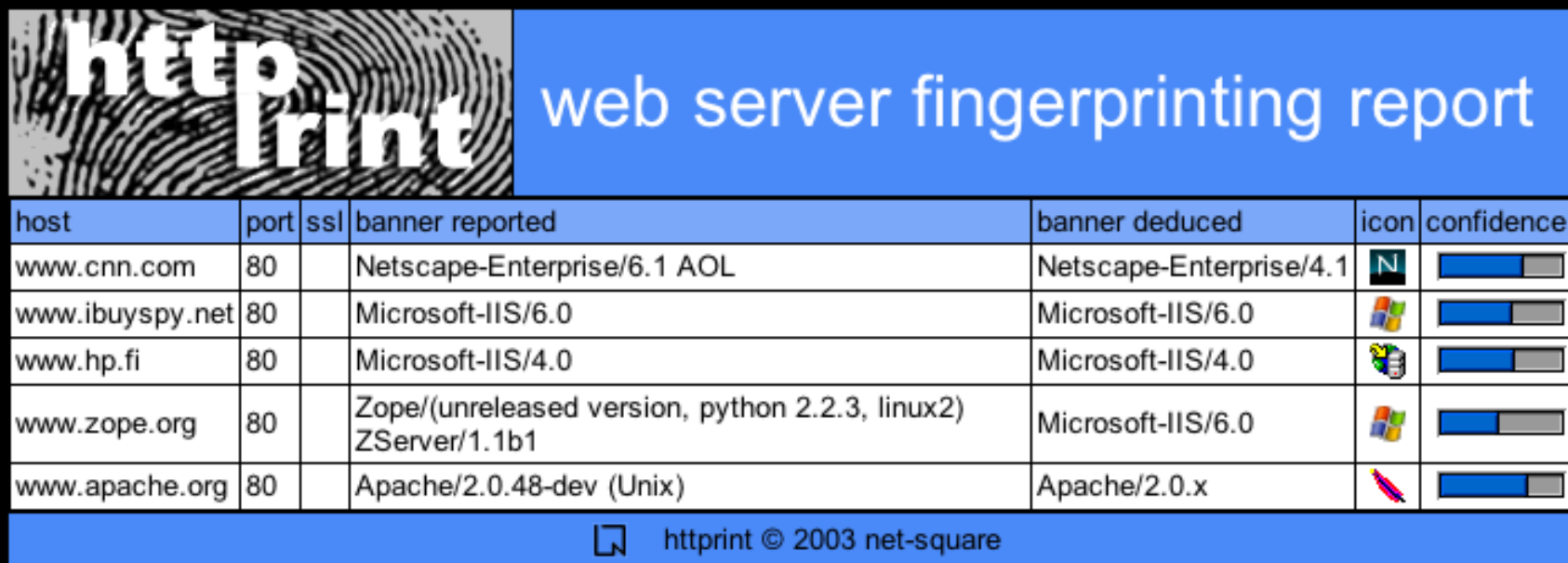
Report File  
C:\Documents and Settings\Administrator\Desktop\win32\httpprint  html  xml  
 csv Run Stop Clear All Options











HitPrint has been completed.



# httpprint – Reports

- Slick HTML reports!



host	port	ssl	banner reported	banner deduced	icon	confidence
www.cnn.com	80		Netscape-Enterprise/6.1 AOL	Netscape-Enterprise/4.1		
www.ibuyspy.net	80		Microsoft-IIS/6.0	Microsoft-IIS/6.0		
www.hp.fi	80		Microsoft-IIS/4.0	Microsoft-IIS/4.0		
www.zope.org	80		Zope/(unreleased version, python 2.2.3, linux2) ZServer/1.1b1	Microsoft-IIS/6.0		
www.apache.org	80		Apache/2.0.48-dev (Unix)	Apache/2.0.x		









httpprint © 2003 net-square


- Now in CSV format as well. Import at will!
- XML reports in enterprise version.



# httprint - Applications

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


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

 httprint © 2003 net-square













# httprint - Real Disguised Servers

- Report below shows five real servers:



web server fingerprinting report

host	port	ssl	banner reported	banner deduced	icon	confidence
www.walmart.com	80		Microsoft-IIS/5.0	Apache/2.0.x		
www.foundstone.com	80		WebSTAR	Apache/2.0.x		
www.port80software.com	80		Yes we are using ServerMask	Microsoft-IIS/5.1, Microsoft-IIS/5.0 ASP.NET, Microsoft-IIS/4.0		
www.ubizen.com	80		web server	Apache/2.0.x		
www.datek.com	80		Ameritrade Web Server	Netscape-Enterprise/4.1		

 httprint © 2003 net-square

- In accordance with Netcraft results.



# 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.



# 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

# Normal error page

## 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>
<HR>
<ADDRESS>Apache/1.3.26 Server at 192.168.7.70 Port 8222</ADDRESS>
</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](mailto: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



```
$ nc 192.168.7.70 8222
GET /junk HTTP/1.0
```

**HTTP/1.1 200 OK**

Date: Tue, 04 Feb 2003 01:41:06 GMT

Server: Apache-AdvancedExtranetServer/1.3.19 (Linux-Mandrake/3mdk) mod\_ssl/2.8.2

OpenSSL/0.9.6 PHP/4.0.4p11

Connection: close

Content-Type: text/html; charset=ISO-8859-1

```
<html><body><H1>Sorry!</H1><p>Random number: 318405.070147527<p>The link you requested
<b>http://192.168.7.2/junk</b> was not found
<p>Please contact the site administrator at <a href="mailto:root@dev.null">
root@dev.null</a> 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

200:A24518F019393885AD2B6A363342B876B6D27B8C http://192.168.7.2/junk

200:A24518F019393885AD2B6A363342B876B6D27B8C http://192.168.7.2/foundsquat

200:A24518F019393885AD2B6A363342B876B6D27B8C http://192.168.7.2/nope.html

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



# Application Fingerprinting

- apprint - prototype application server fingerprinting tool.
- 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.

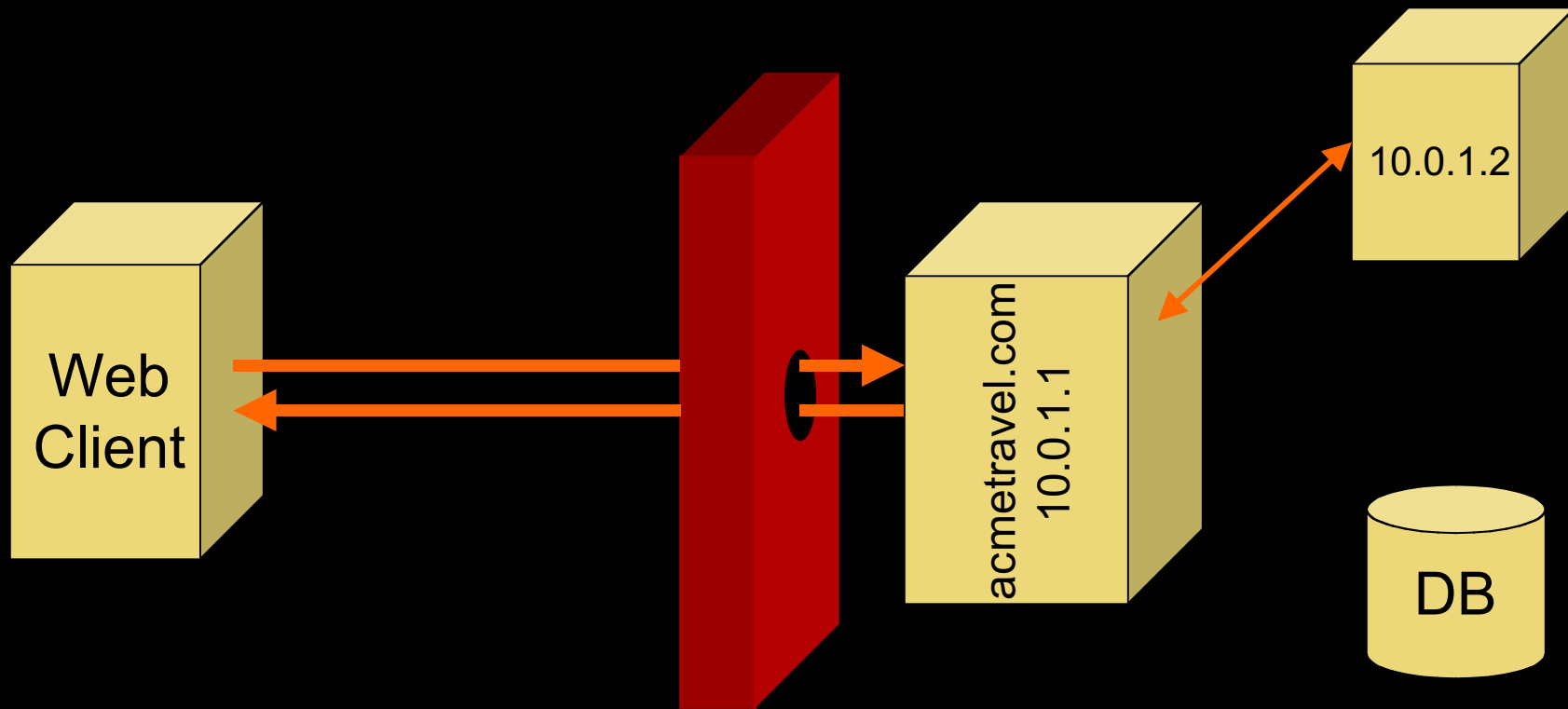


# Reverse Proxy Servers

- 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



GET http://10.0.1.2/ HTTP/1.0



# Port Scanning through Proxies

- Issue multiple GET requests to the proxy:
  - GET http://10.0.0.3:21/ HTTP/1.0
  - GET http://10.0.0.3:25/ HTTP/1.0
  - GET http://10.0.0.3:135/ HTTP/1.0
  - GET http://10.0.0.3:139/ HTTP/1.0
- Use Page signatures to identify accurately if a port is open on an internal host.



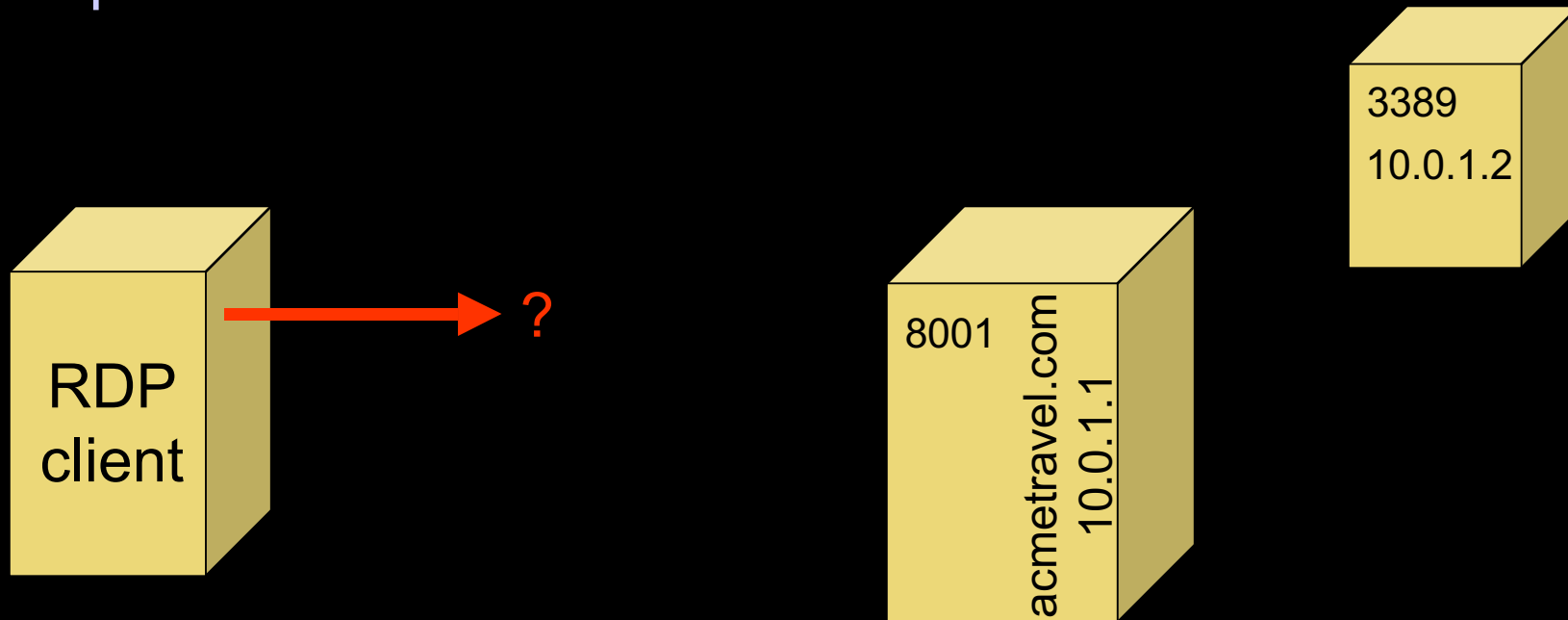
# Better CONNECTivity

- 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.



# CONNECTivity through proxies

The problem: to connect to an internal Term Server



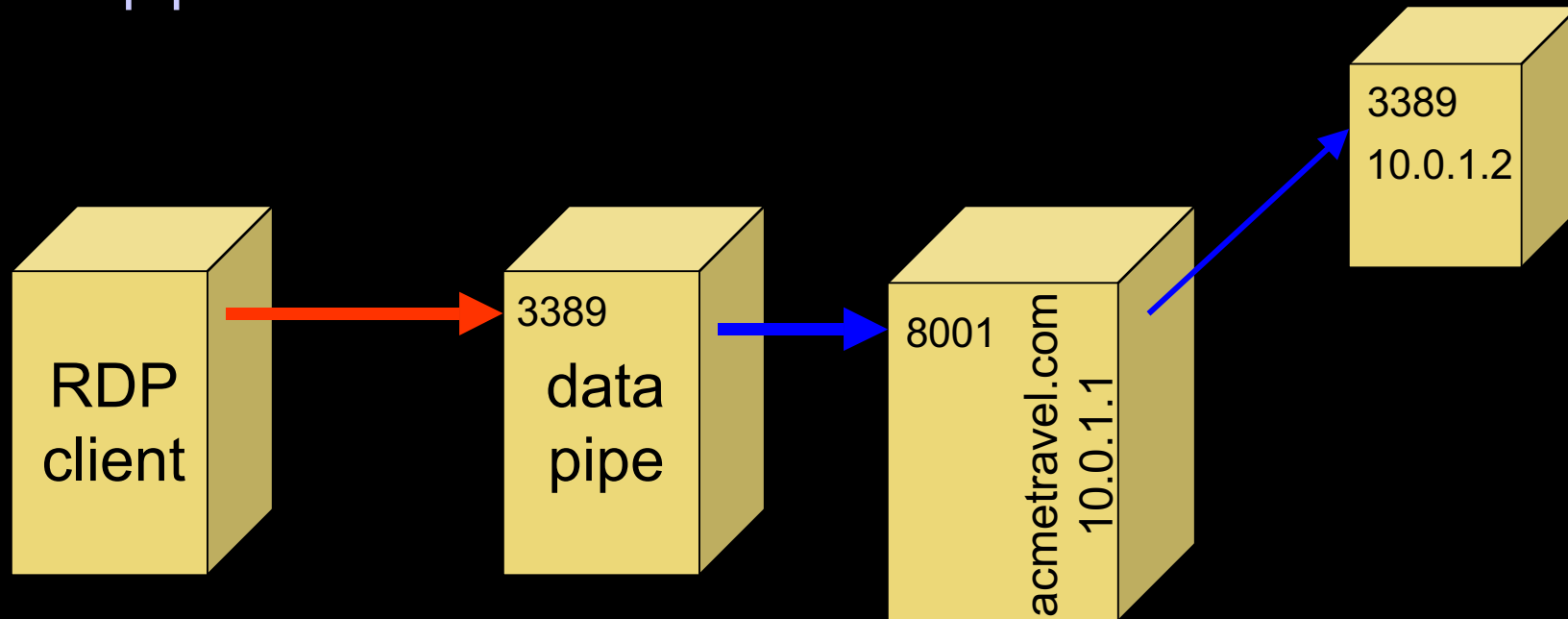
We know `www.acmetravel.com:8001` allows reverse proxying.





# CONNECTivity through proxies

```
./datapipe 3389 10.0.1.2 3389 acmetravel.com 8001
```

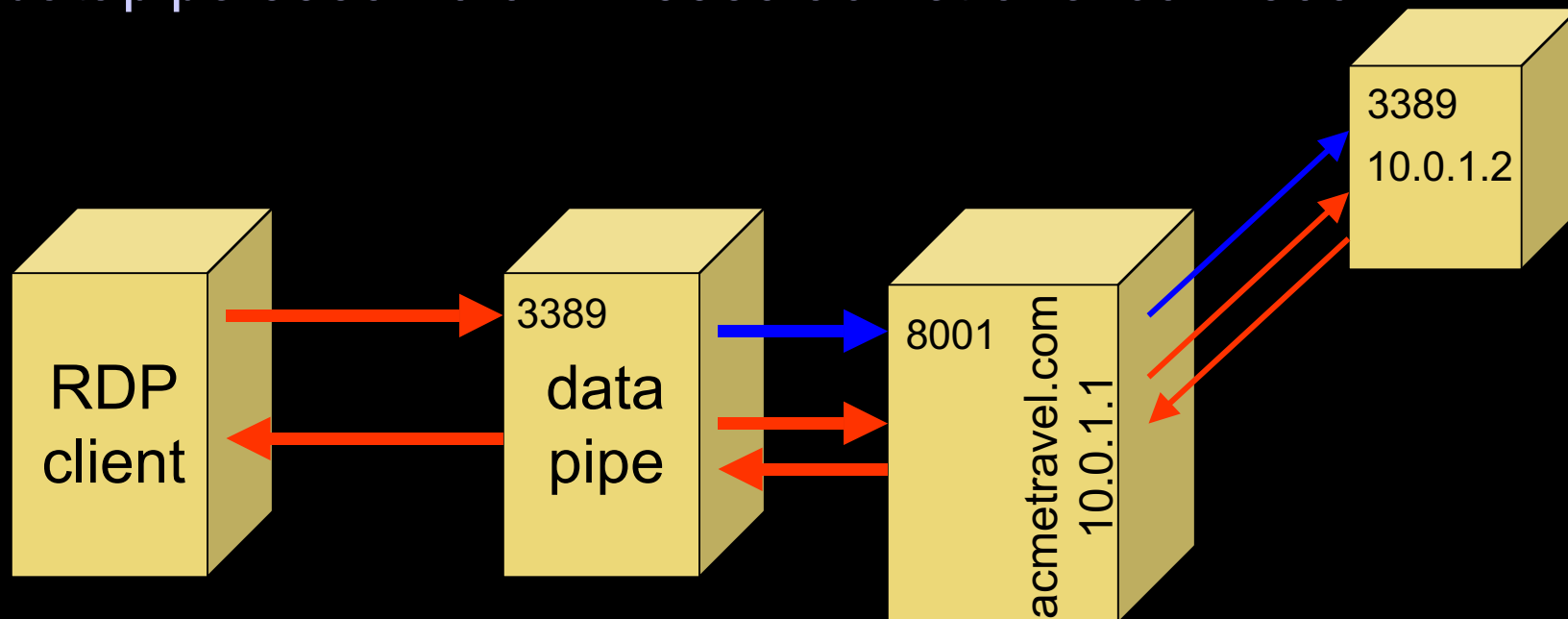


```
CONNECT http://10.0.1.2:3389/ HTTP/1.0
```



# CONNECTivity through proxies

```
./datapipe 3389 10.0.1.2 3389 acmetravel.com 8001
```



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

RDP data passes through the established connection.



# Automated Web Security Assessment

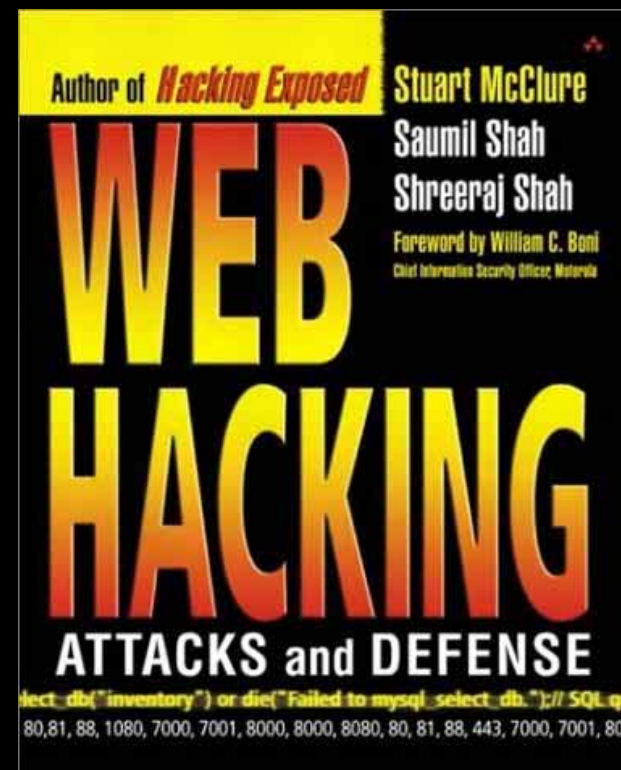
- The need for overcoming HTTP's customisable aspects:
  - Server banner strings
  - Response codes
- Improving accuracy
- Using core concepts to extend assessment techniques



# Closing Thoughts

- “You cant patch (or hide) carelessness”.
- Web Hacking: Attacks and Defense

Saumil Shah,  
Shreeraj Shah,  
Stuart McClure  
Addison Wesley – 2002.





**Thank you!**

saumil@net-square.com

<http://net-square.com/>

