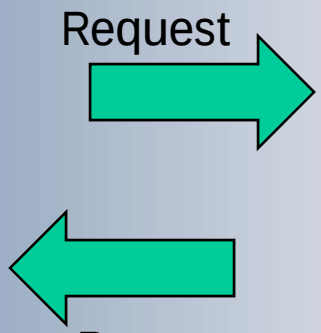
HTTP Headers



SHODAN

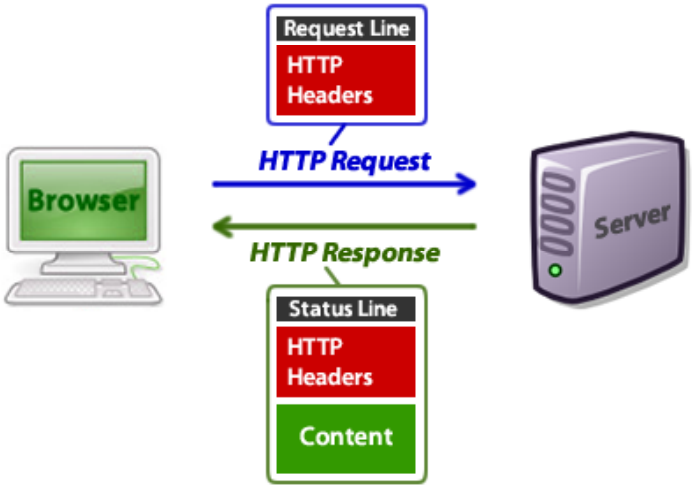
HTTP Headers

- A Client-Server communication protocol
  - Request-response architecture
    - Client makes request
    - Server issues response
- Version 0.9 – 1991
  - Stateless – single method GET
- Version 1.0 - 1996
  - Stateless
- Version 1.1 – 1997
  - Ability to keep connections open
  - Reduced latency (less TCP/IP overhead)
  - Pipelining: allows for multiple requests at once

HTTP Headers

General Structure

- Start_Line<CRLF> (no whitespace)
- Message Header<CRLF>
- <CRLF>
- Message Body<CRLF>



HTTP Headers

- Start_Line (request or response)
  - Request
    - Method<SP>Request-URI<SP>HTTP-Version<CRLF>
  - Response
    - HTTP-Version<SP>Status-code<SP>Response-Phrase<CRLF>
- Message Header
  - Field_name:<SP>Field_value, Field_value<CRLF>
- Message Body
  - Binary data

HTTP Request Methods

- GET – Retrieve the URL
- POST – Send data to the server
- HEAD – Retrieve header (plus response code)
- OPTIONS – Request available options
- PUT – Store document at specified URL
- DELETE – Delete specified URL
- TRACE – invoke a remote loop-back message
- CONNECT – w/proxy, switch to a SSL tunnel

HTTP Header Fields

- Accept – acceptable content types

  Accept: text/plain
- Charset – character sets

  Accept-Charset: utf-8
- Language

  Accept-Language: en-US
- Cache-Control – caching mechanism

  Cache-Control: no-cache
- Cookie
- **Referer**

  Referer: http://pacific.edu/wiki
- **User-Agent**

HTTP Header Examples

- Date: Fri, 31 Dec 2011 23:59:59 GMT
- Content-Type: text/html
- Content-Length: 1354
- From: someone@pacific.edu
- Last-Modified: Fri, 31 Dec 2011 23:59:59 GMT
- Server: Apache/2.3
- User-Agent: Mozilla/5.0Gold

User Agent String

- The User-Agent HTTP header indicates the browser and operating system
- Allows for browser specific content (features)
- Logging – web analytics
- Use for redirection
- User-agent sniffing

Examples:

Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

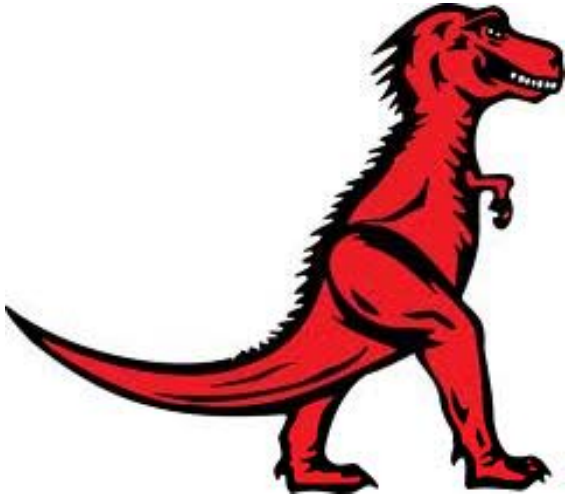
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)

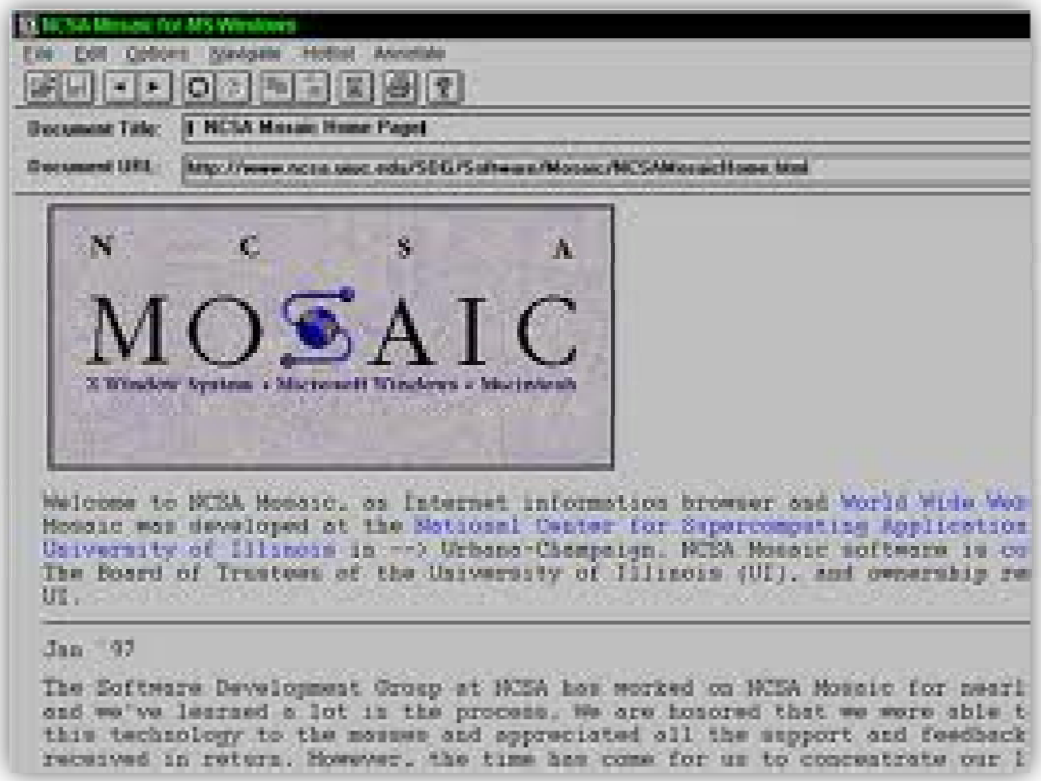
Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)

Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Hi_There; Trident/5.0)

Browser Types

- Mozilla?
- For historical reasons, IE identifies self as “Mozilla”
- Was codename for Netscape Navigator
- Portmanteau of "Mosaic killer"
- IE spoofed Mozilla to receive content for Netscape

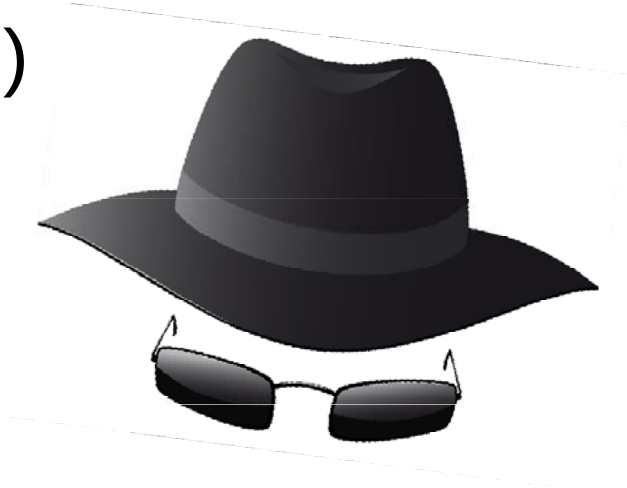




HTTP Header Fields

Referrer (also referer SP) optional

- Part of HTTP request sent by browser to server
- URL of previous page from which link was followed
- Used in web analytics
- Used by paysites to secure content
  - Referrer spoofing
- Used in black-hat SEO
  - (Search Engine Optimization)



HTTP Response Code

- Code number is computer readable
- Status code is a three-digit integer
- Phrase is human readable – may vary

  - 1xy indicates an informational message only
  - 2xy indicates success of some kind
  - 3xy redirects the client to another URL
  - 4xy indicates an error on the client's part
  - 5xy indicates an error on the server's part

HTTP Response Code

- 200 OK
- 206 Partial content
- 301 Moved Permanently
- 302 Moved Temporarily
- 400 Bad Request

  request sent by client was syntactically incorrect
- 401 Authorization Required
- 403 Forbidden

  server understood request but refused to fulfill it
- 404 Not Found

  the requested resource is not available
- 500 Internal Server Error

  error in HTTP server prevented fulfilling request

Remember This

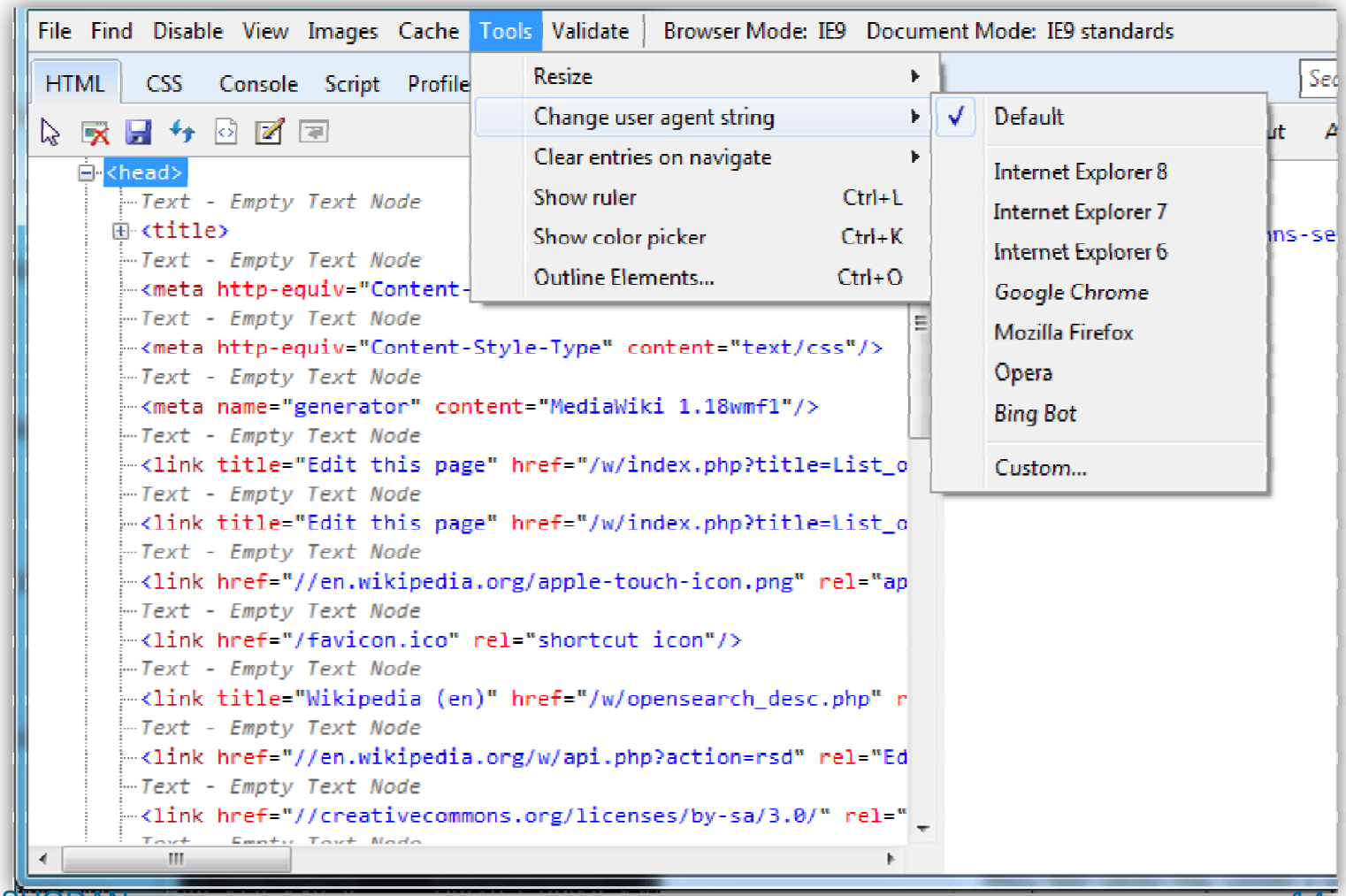
From the header fields the server can determine:

- **The page you came from**
- Your operating system
- The OS version
- **Your web browser**
- Browser version
- It already knows your IP address

Unless you lie…

Changing User Agent String

- Various Firefox Plugins
- IE – Developer Tools - a significant set of tools



HTTP Headers

An example....

HTTP Headers

- An HTTP Request to amazon.com

HTTP Request Header
Connect to 72.21.214.128 on port 80 ... ok

GET / HTTP/1.1[CRLF]
Host: www.amazon.com[CRLF]
Connection: close[CRLF]
User-Agent: Mozilla/4.0 (compatible; MSIE 11; Windows 9;net/)[CRLF]
Accept-Encoding: gzip[CRLF]
Accept-Charset: ISO-8859-1,UTF-8;q=0.7,*;q=0.7[CRLF]
Cache-Control: no-cache[CRLF]
Accept-Language: de,en;q=0.7,en-us;q=0.3[CRLF]
Referer: http://remulak.net/[CRLF]
[CRLF]

HTTP Headers

HTTP Response Header

Name	Value	Delim
Status: HTTP/1.1 200 OK		
Date:	Mon, 06 Feb 2012 06:34:33 GMT	
Server:	Server	
Set-Cookie:	skin=noskin; path=/; domain=.amazon.com; expires=Mon, 06-Feb-2012 06:34:33 GMT	
pragma:	no-cache	
x-amz-id-1:	10NNZA3RJCTGW00VXYCR	
p3p:	policyref="http://www.amazon.com/w3c/p3p.xml",CP="CAO DSP LAW CUR ADM IVAo IVDo CONo OTPo OUR DELi PUBi OTRi BUS PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA HEA PRE LOC GOV OTC "	
cache-control:	no-cache	
expires:	-1	
x-amz-id-2:	mTvMEWPifmS4Bw+9uMXh6mB/P1ZCYncKzOTxEPdkAy/QmjgDAW4X8xghKuY0tU2e	
Vary:	Accept-Encoding,User-Agent	
Content-Encoding:	gzip	
Content-Type:	text/html; charset=ISO-8859-1	
Set-cookie:	session-id-time=2082787201l; path=/; domain=.amazon.com; expires=Tue, 01-Jan-2036 08:00:01 GMT	
Set-cookie:	session-id=180-5522149-0840427; path=/; domain=.amazon.com; expires=Tue, 01-Jan-2036 08:00:01 GMT	
Transfer-Encoding:	chunked	

Followed by the HTML, Scripts, Java, CSS, etc.

Summary

- Hidden HTTP data including headers, cookies, authentication, etc. are sent from browser to the server
- HTTP Header data can also be sent from server to the browser, e.g. error codes, redirection codes, etc.

- Resources:
  - http://www.useragentstring.com/
  - http://www.web-sniffer.net

HTTP using telnet

```
root@hatter:/# telnet www.treacle.com 80
Trying 63.206.191.202...
Connected to www.treacle.com.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 09 Feb 2012 03:53:43 GMT
Server: Apache/2.2.17 (Unix) DAV/2
Accept-Ranges: bytes
Content-Length: 5477
Connection: close
Content-Type: text/html

Connection closed by foreign host.
```

HTTP Response

- HTTP headers are a **banner** message
- Other applications/services have similar banner messages
- A typical Telnet banner

```
root@hatter:/# telnet
www.treacle.com
Trying 63.206.191.202...
Connected to www.treacle.com.
Escape character is '^]'.
Connection closed by foreign host.
```

Banners

- Google indexes web page content
- What if something indexed the response banners?
  - HTTP 80
  - FTP 21
  - Telnet 23
  - SSH
  - SNMP
- With filters for IP netbock, country, OS, & port

- *Searching the database doesn't touch devices*

  Penetration testing in the cloud

  Shodan *- by John Matherly*

SHODAN

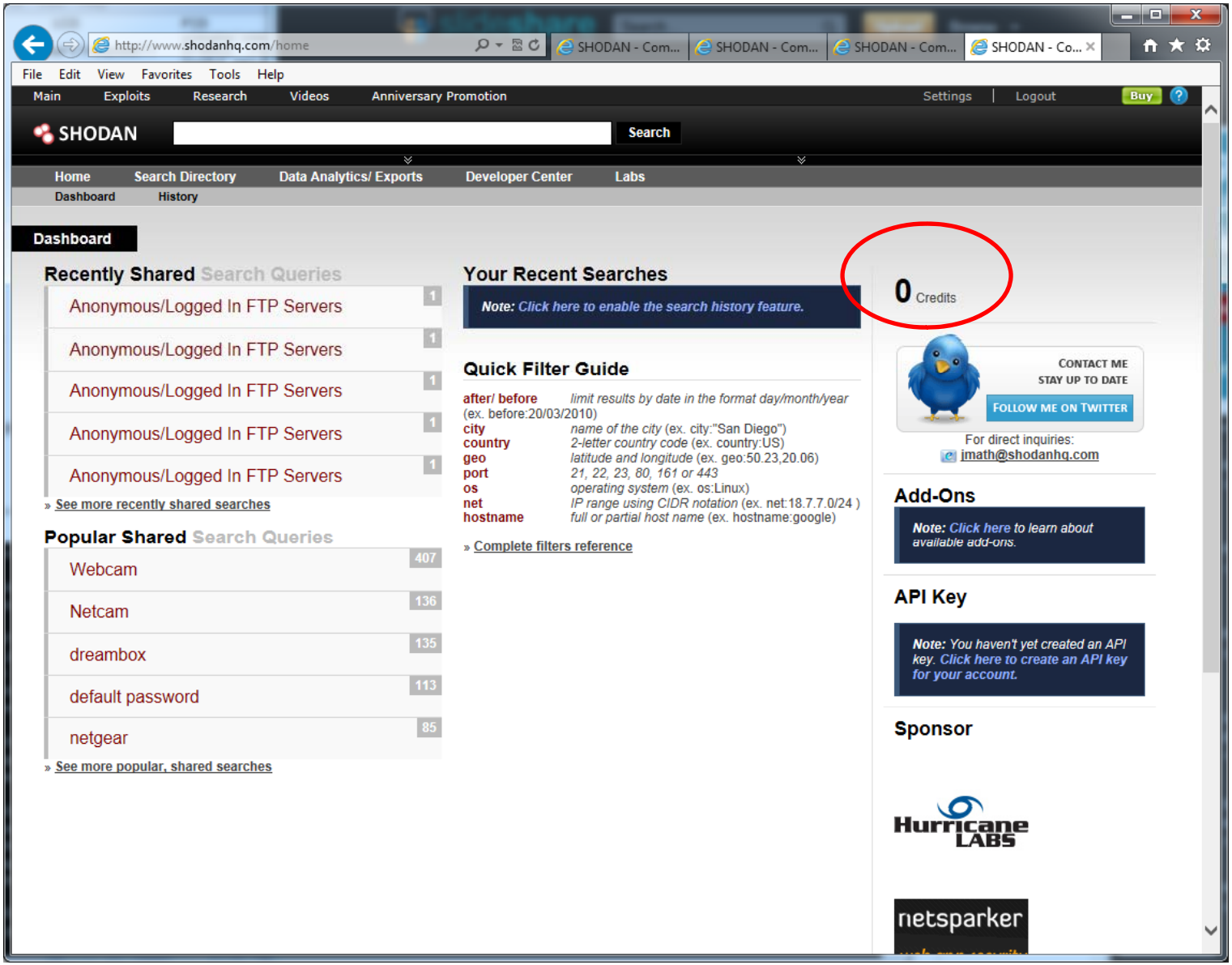
The **S**entient **H**yper-**O**ptimized **D**ata **A**ccess **N**etwork (Shodan) - a specialized network search engine for scanable Internet facing devices. Where Google looks at content, Shodan interrogates ports and grabs the resulting banners (e.g. the network device responses), indexing them for searches.

Went online late 2009.

Shodan is a search engine for cloud penetration testing. Instead of finding an exploit that works on a target system, with Shodan you can take any exploit, and find a system vulnerable to it. You are not actively running scans, but rather asking the Shodan cloud “what do you know about this already”.

www.shodanhq.com

After Registering

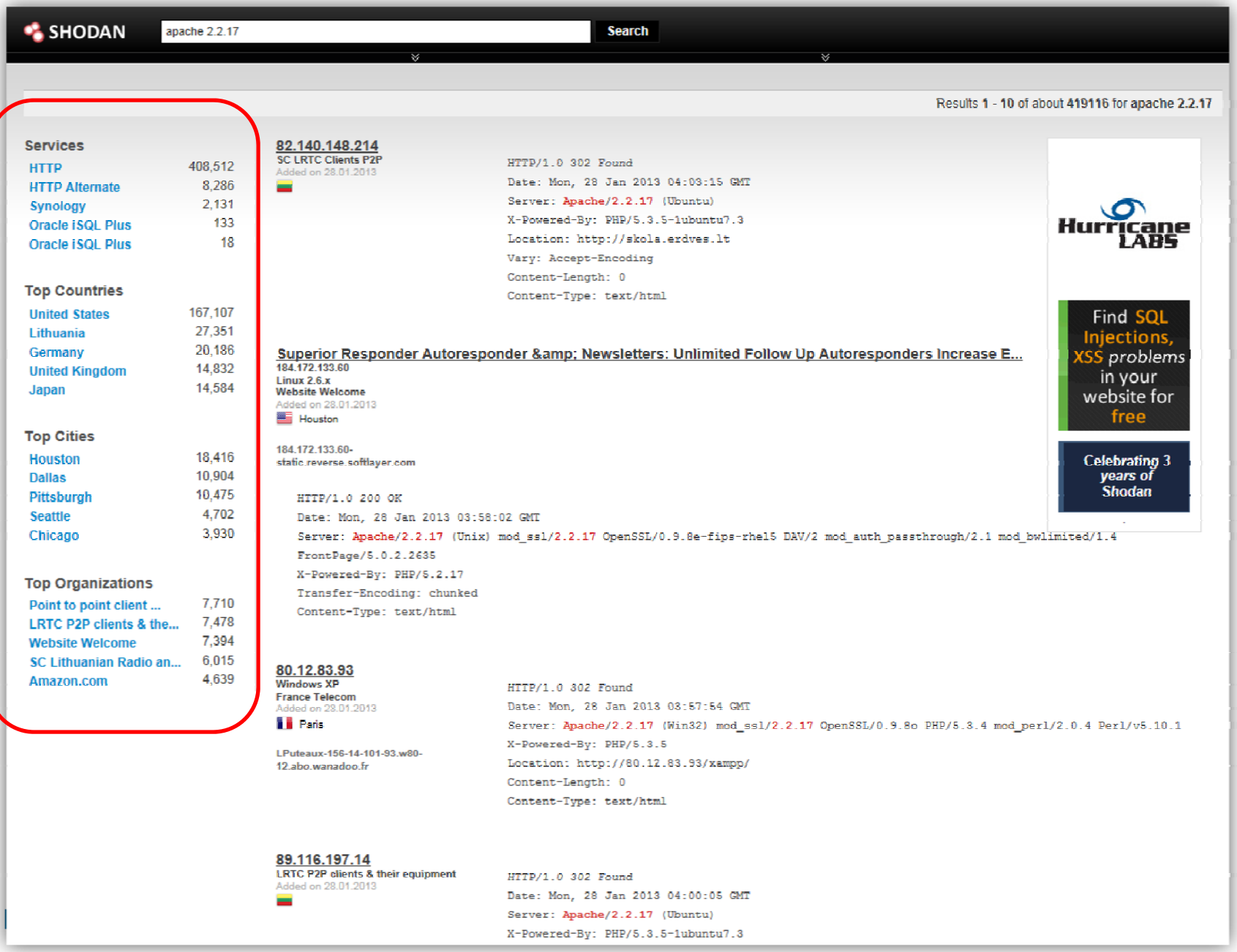


Commercial Shodan Training

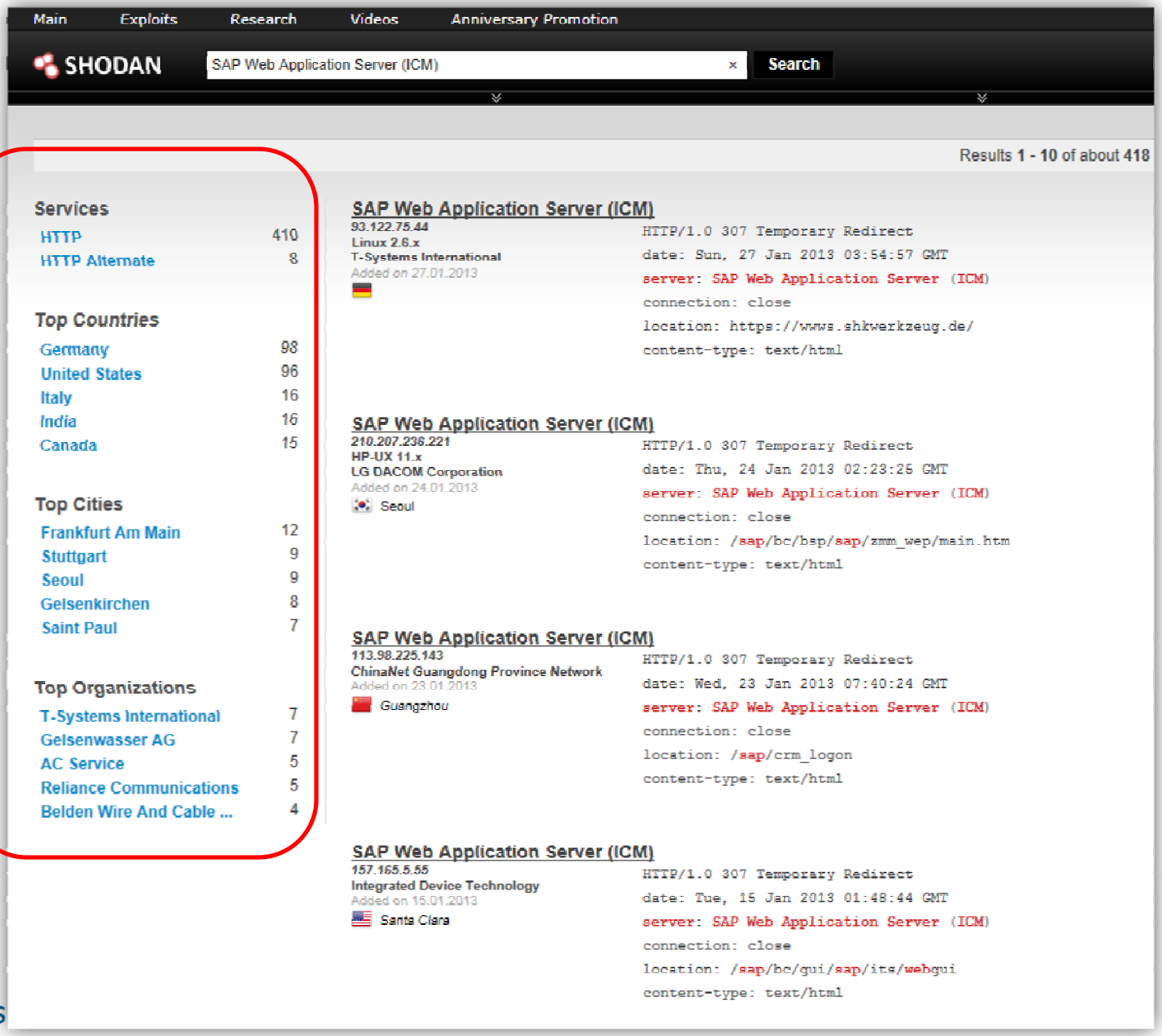
Shodan Certified Penetration Tester $495

- Week long on-line course (Self-paced videos)
- Tools: **Shodan** and **BackTrack**
- Targets: Two Live CD's to exploit
- Penetration Test Methodology
- Use and selection of Hacker Tools
- System Exploitation Fundamentals
- Passwork Attacks (Remote & Local)
- Network Sweeping and Tracing
- OS and Version Detection
- Port Scanning Fundamentals
- Conduct Your Own Penetration Test
- Completion Assignment: Written Penetration Test Results

Search: apache 2.2.17



Shodan


Main
Exploits
Research
Videos
Anniversary Promotion
SHODAN
SAP Web Application Server (ICM)
Search
Results 1 - 10 of about 418
Services
HTTP 410
HTTP Alternate 8
Top Countries
Germany 98
United States 96
Italy 16
India 16
Canada 15
Top Cities
Frankfurt Am Main 12
Stuttgart 9
Seoul 9
Gelsenkirchen 8
Saint Paul 7
Top Organizations
T-Systems International 7
Gelsenwasser AG 7
AC Service 5
Reliance Communications 5
Belden Wire And Cable ... 4
SAP Web Application Server (ICM)
93.122.75.44
Linux 2.6.x
T-Systems International
Added on 27.01.2013
HTTP/1.0 307 Temporary Redirect
date: Sun, 27 Jan 2013 03:54:57 GMT
server: SAP Web Application Server (ICM)
connection: close
location: https://www.shkwerkzeug.de/
content-type: text/html
SAP Web Application Server (ICM)
210.207.236.221
HP-UX 11.x
LG DACOM Corporation
Added on 24.01.2013
Seoul
HTTP/1.0 307 Temporary Redirect
date: Thu, 24 Jan 2013 02:23:25 GMT
server: SAP Web Application Server (ICM)
connection: close
location: /sap/bc/bsp/sap/zmm_wep/main.htm
content-type: text/html
SAP Web Application Server (ICM)
113.98.225.143
ChinaNet Guangdong Province Network
Added on 23.01.2013
Guangzhou
HTTP/1.0 307 Temporary Redirect
date: Wed, 23 Jan 2013 07:40:24 GMT
server: SAP Web Application Server (ICM)
connection: close
location: /sap/crm_logon
content-type: text/html
SAP Web Application Server (ICM)
157.165.5.55
Integrated Device Technology
Added on 15.01.2013
Santa Clara
HTTP/1.0 307 Temporary Redirect
date: Tue, 15 Jan 2013 01:48:44 GMT
server: SAP Web Application Server (ICM)
connection: close
location: /sap/bc/gui/sap/its/webgui
content-type: text/html

Search: pacific.edu

138.9.110.139
Linux 2.6.x
University of the Pacific
Added on 15.01.2013
Stockton

pacshare.pacific.edu

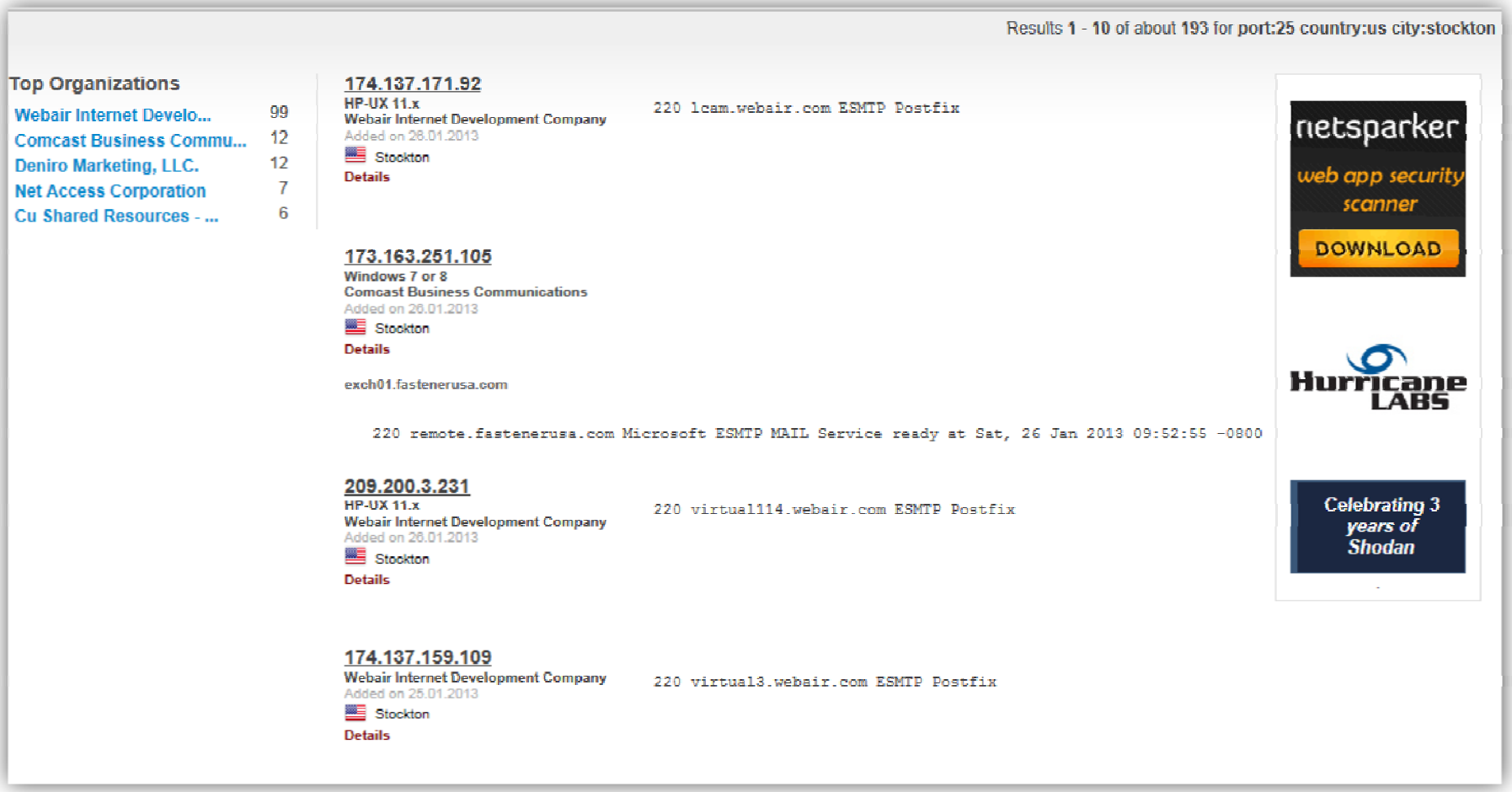
```
HTTP/1.0 302 Found
Date: Tue, 15 Jan 2013 04:56:02 GMT
Server: Apache
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Tue, 15 Jan 2013 04:56:02 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: sfcurl=deleted; expires=Mon, 16-Jan-2012 04:56:01 GMT; path=/; domain=.138.9.110.139;
location: https://pacshare.pacific.edu/courier/1000@/mail_user_login.html?
Content-Length: 0
Content-Type: text/html
```

TsaiLab
138.9.110.146
Linux 2.6.x
University of the Pacific
Added on 21.09.2012
Stockton

```
HTTP/1.0 200 OK
Date: Fri, 21 Sep 2012 18:04:17 GMT
Server: Apache/2.2.11 (Ubuntu) PHP/5.2.6-3ubuntu4.5 with Suhosin-Patch
X-Powered-By: PHP/5.2.6-3ubuntu4.5
X-Pingback: http://tsailab.chem.pacific.edu/xmlrpc.php
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

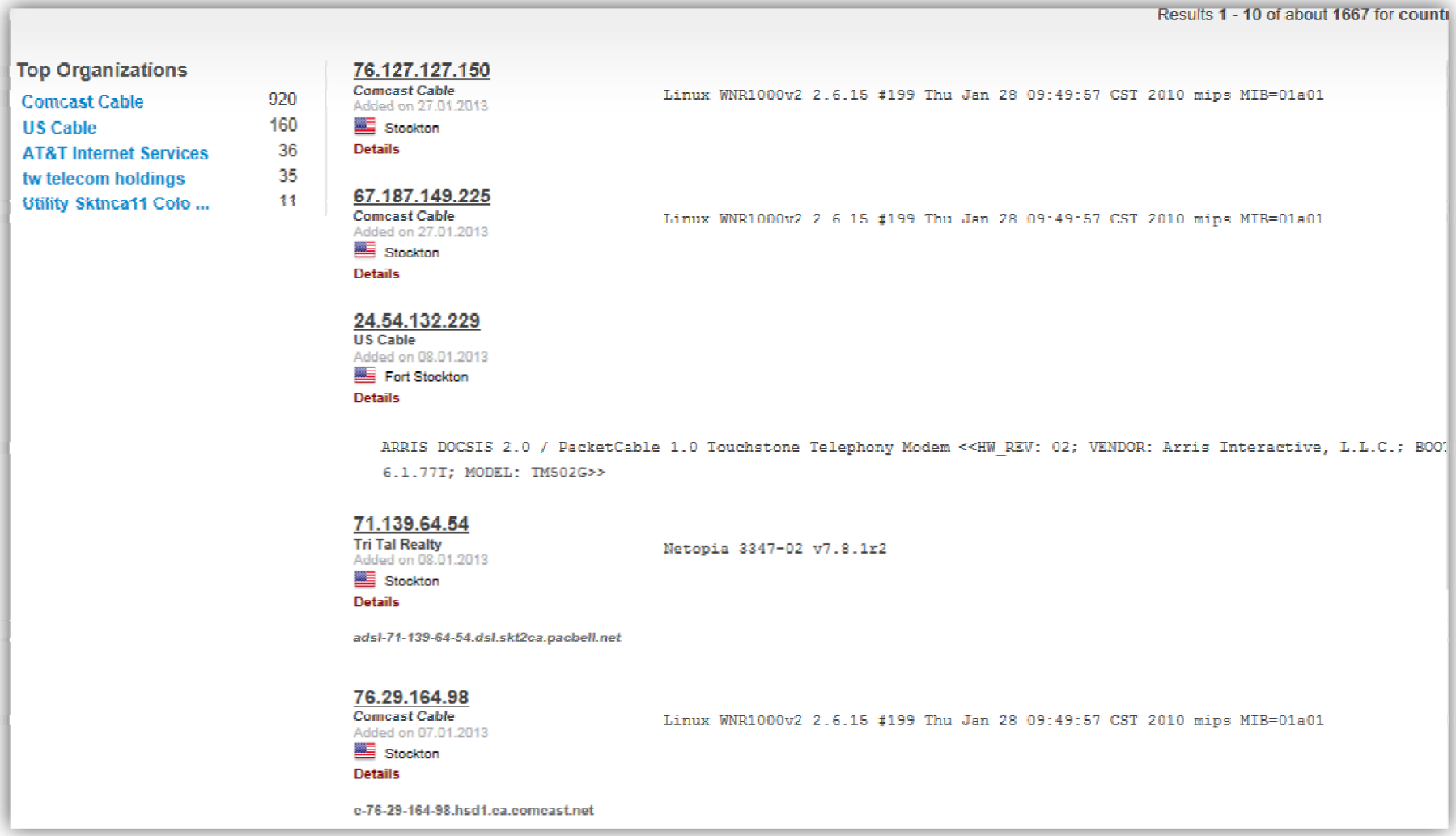
Shodan

- port:25 country:us city:stockton



City:Stockton Port:161

- SNMP – Simple Network Management Protocol



SNMP

- Typically have default password "public"
- Provides detailed system description
- Installed software
- Patches applied
- Interface counters

Shodan Queries

- http://www.shodanhq.com/?q=Ericsson+Television+Web+server

The links led to:

Status | Device Info | Alarms | Customization | Input | Service *plus* | Decode | Output | Download | SNMP | Presets

Status

Refresh

Name	ATSC Broadcast Receiver
IP Address #1	)47.242
IP Address #2	192.168.001.002
Current Status	**Major**
Current Time	2012-02-09 07:45:23
Uptime	0069 12:04:08 DAYS H:M:S
Input Status	LOCKED 188 19.396 Mbits/s
Video Status	RUNNING 1280x720 Progressive 59.940Hz 4:2:0 16:9 12.004 Mbits/s
Audio 1 Status	RUNNING AC-3
Audio 2 Status	STOPPED ---
Output Feed	2 (undefined)
Mode	ACTIVE

Time	Severity	Name	Source	Slot	Port	AlarmId	SubId	Info
2000-01-01 00:00:01	Major	Audio 2 Not Running	RX8000	1	0	1014	0	Audio 2 Not Running

Shodan Queries

- http://www.shodanhq.com/?q=intranet

217.69.39.35
Linux recent 2.4
Added on 07.02.2012
London
bulk01-af.mail.uk1.eechost.net

```
HTTP/1.0 401 Authorization Required
Date: Tue, 07 Feb 2012 12:28:21 GMT
Server: Apache/2.2.6 (Unix)
WWW-Authenticate: Basic realm="Mail Intranet"
Content-Length: 476
Content-Type: text/html; charset=iso-8859-1
```

66.17.205.134
Added on 05.02.2012
Chicago

```
HTTP/1.0 302 Object moved
Server: Microsoft-IIS/5.0
Date: Sun, 05 Feb 2012 22:24:35 GMT
X-Powered-By: ASP.NET
Location: https://extranet1.dbr.com/intranet/login_db.asp
Content-Length: 168
Content-Type: text/html
Set-Cookie: ASPSESSIONIDAQSAQARR=DEHENCACAEJANHACKDBJONKC; path=/
Cache-control: private
```

192.54.176.189
Added on 05.02.2012
Nice

```
HTTP/1.0 302 Found
Date: Sun, 05 Feb 2012 21:45:51 GMT
Server: Apache/2.2.16 (Debian)
Location: https://www-intranet.oca.eu/
Vary: Accept-Encoding
Content-Length: 292
Content-Type: text/html; charset=iso-8859-1
```

Think about the headers, the dates, the cookie, what do they mean?

Shodan Queries

http://www.shodanhq.com/?q=Zhone%20SLMS

Zhone's SLMS (Single Line Multi-Service) access operating system...

DSL carrier/provider gear

Don't follow the links....

» Top countries matching your search

United States	68
Belarus	36
Argentina	23
Afghanistan	22
Iran, Islamic Republic of	19

206.54.106.122
Added on 06.02.2012
Riverton

```
HTTP/1.0 200 OK
Server: WindWeb/4.00
Connection: Keep-Alive
Keep-Alive:
Persist:
Last-Modified: Fri, 14 May 2010 12:00:00 GMT
Content-Type: text/html
WWW-Authenticate: Basic realm="Zhone SLMS Web Interface"
Transfer-Encoding: chunked
```

175.106.60.13
Added on 23.01.2012
Kabul

```
HTTP/1.0 200 OK
Server: WindWeb/4.00
Connection: Keep-Alive
Keep-Alive:
Persist:
Last-Modified: Fri, 1 January 1999 12:00:00 GMT
Content-Type: text/html
WWW-Authenticate: Basic realm="Zhone SLMS Web Interface"
Transfer-Encoding: chunked
```

80.94.226.97
Added on 23.01.2012
Minsk

```
HTTP/1.0 200 OK
Server: WindWeb/4.00
Connection: Keep-Alive
Keep-Alive:
Persist:
Last-Modified: Tue, 15 June 2010 12:00:00 GMT
Content-Type: text/html
WWW-Authenticate: Basic realm="Zhone SLMS Web Interface"
Transfer-Encoding: chunked
```

HTTP Headers - SHODAN

Force Multplier

- Force multiplication, in military usage, refers to an attribute or a combination of attributes which make a given force more effective than that same force would be without it.

- Shodan queries + Country filter = geopolitical ownage

MySQL exploit + Shodan query - port:3306 country:PK

Can add a 'city' filter as well!

A 'geo' filter = radius of a given latitude and longitude

Shodan for coders

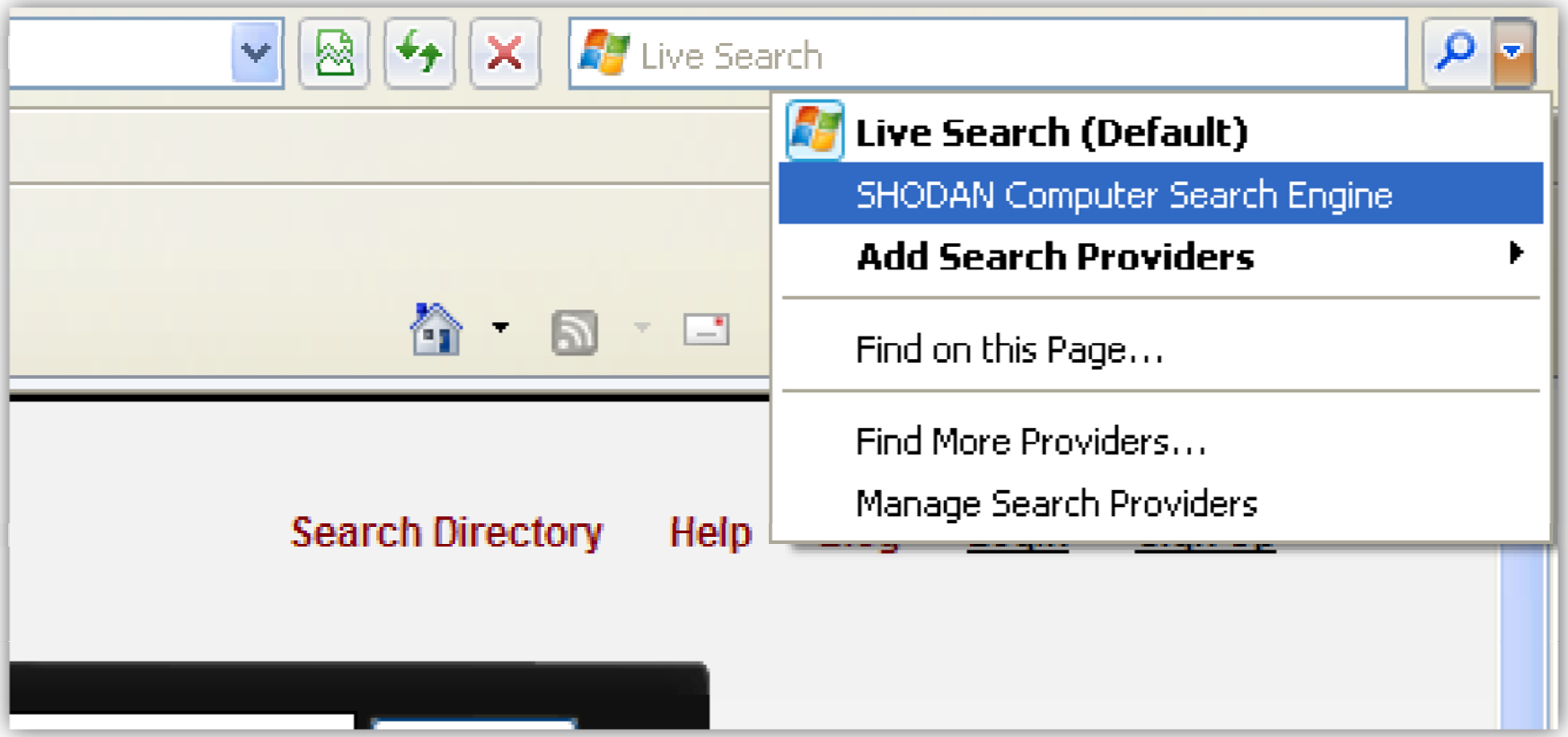
Additional information on Shodan libraries:

- http://docs.shodanhq.com/index.html
  - Python API documentation
  - Ruby API documentation
  - Pearl API documentation
- Includes information on using the:
  - Exploit DB
  - Metasploit modules
  - WiFi Positioning System – get a wireless router's physical address!

```
# Search Shodan
        results = api.search('apache')
        # Show the results
        print 'Results found: %s' % results['total']
        for result in results['matches']:
                print 'IP: %s' % result['ip']
                print result['data']
                print ''
        except Exception, e:
        print 'Error: %s' % e
```

Shodan

- Search Shodan directly from your browser



Shodan

Filters:

- city: combine with country
- country: use country codes e.g. US IE MX
- geo: devices within radius of given lat & long
- hostname: value contained in hostname
- net: IP, subnet – use CIDR
- os: linux, cisco, "windows 2003"
- port: 21, 22, 23, and 80
- after: still online after date

Shodan

Additional filters can be purchased

- cert_version: SSL certificate version
- cert_bits: certificate public key length
- cipher_name: AES128-SHA, DES, MD5, etc.
- cipher_protocol: SSLv1, SSLv3, TLSv1

- SHODAN lets you export up to 1,000,000 search results in a structured XML format using the web interface

Shodan

Common query targets

- Internet routers
  - Web service enabled
- Internet servers
- Wireless access points
- Internet switches
  - Connected to Internet router
  - Harvest VLAN, SNMP information

Shodan

Once connected to device webserver, typical sub-pages:

- system.html
- security.html
- network.html
- wireless.html
- ddns.html
- accesslist.html
- audiovideo.html
- cameracontrol.html
- mailftp.html
- motion.html
- application.html
- syslog.html
- parafile.html
- maintain.html

Found Using Shodan

Flaw in Home Security Cameras Exposes Live Feeds to Hackers

By Kim Zetter | February 7, 2012 | 2:34 pm | Categories: Hacks and Cracks, Surveillance

WIRED

Follow @KimZetter

Like Send 63 likes. Sign Up to see what your friends like.

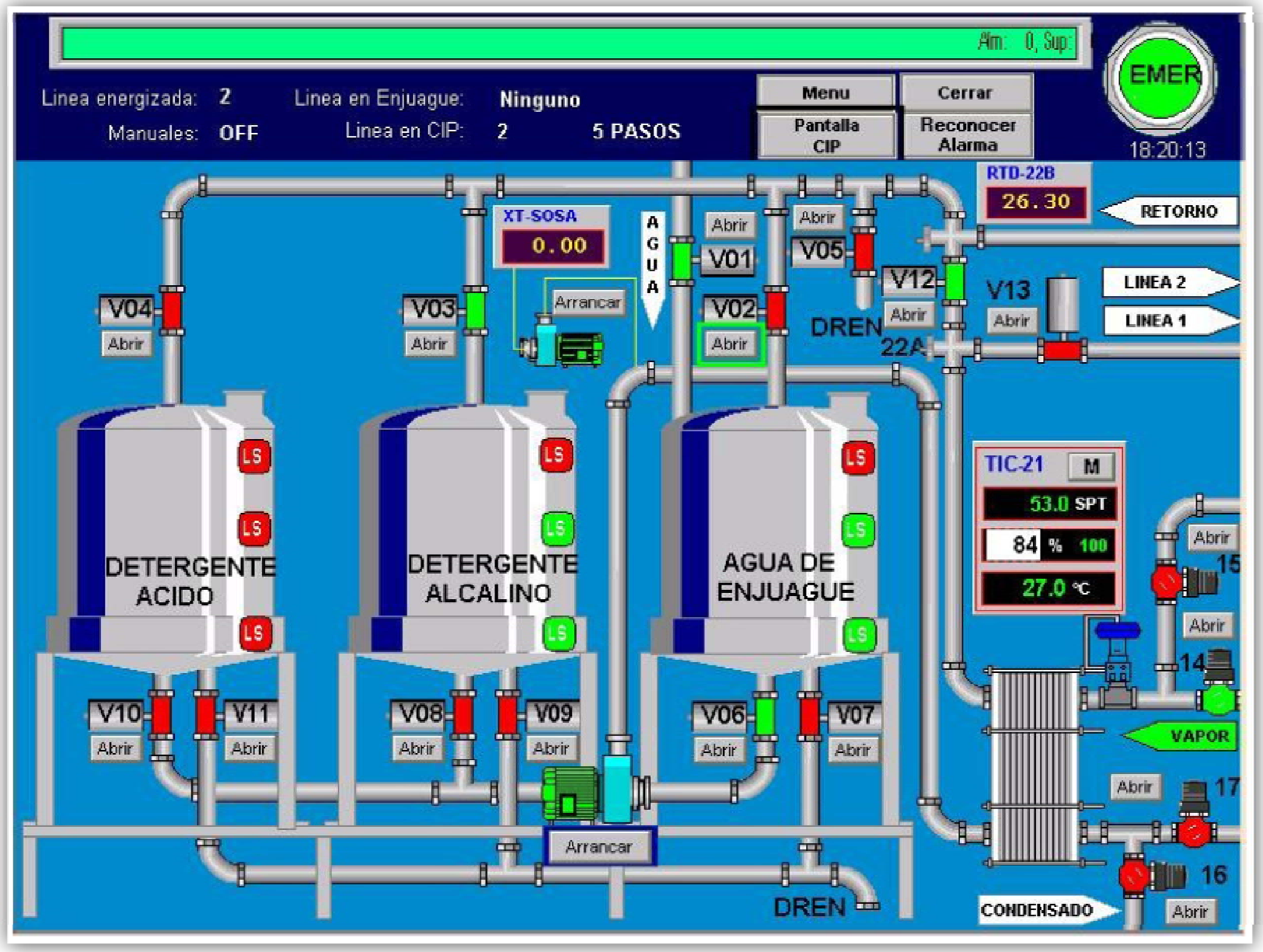
TRMB

Trimble GPS – GNSS – Global Navigation Satellite System receiver used for navigation, geology, surveying.
TRMB country:US = 547

Shodan

- In late 2010 hackers and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) were using Shodan to find insecure SCADA (System Control And Data Acquisition) installations that were Internet connected.
- Often with default vendor passwords.
  - Energy, water utilities
  - Traffic control systems
  - Red light cameras
  - HVAC and building automation
- Shamoon attack against Aramco Oil in Saudi Arabia destroyed data on 30,000 workstations (hit MBR)

SCADA Control Screen



Shodan Lab

- Read the 'schearer-shodan.pdf' GIYF
  - Or watch the video
  - Michael Schearer from DefCon18

- Then do the lab as homework
  - You'll need a network connection

- Additional links:
- http://eripp.com/ The Every Routable IP Project

Shodan