

CSE508

Network Security



2024-04-04

## Reconnaissance

Michalis Polychronakis

*Stony Brook University*

# Information Gathering

First step of an attacker: gather as much information as possible about a particular target

Human, system, organization, ...

Dependencies and third-party interactions are also important

Example: the Target 2013 breach was achieved through the compromise of a third-party HVAC vendor who had access to the internal network

Peripheral or “forgotten” systems are often less secure than publicized web servers, application servers, email endpoints, ...

*Every piece of information counts!*

**Passive reconnaissance:** no direct interaction with the target system

Information gathering from public sources

Passive network eavesdropping

Dumpster diving (e.g., printed documents, data from discarded hard disks)

Information leakage (e.g., data breaches → dumps)

**Active reconnaissance:** attackers' activities can be directly observed

Network scanning

Service enumeration

OS and service fingerprinting/probing

Social engineering

# OSINT (Open-source Intelligence Gathering)

Intelligence collected from *publicly* available sources

As opposed to covert or clandestine sources

Wide variety of types of information and sources

*Search engines:* public documents, forgotten web pages, exposed login interfaces, dashboards, historical data, ...

*Public data:* courthouse documents, tax forms, budgets, ...

*Media:* articles, interviews, blog posts, ...

*Social media:* LinkedIn/Facebook/Twitter/etc., mailing lists, ...

*Professional/academic sources:* reports, presentations, ...

*Metadata:* documents, EXIF, executables, email headers, ...

...

# Overall OSINT Process

## Source identification

Identify potential sources of information

## Data harvesting

Collect and harvest information from the selected as well as newly discovered sources

## Data processing and integration

Process the harvested information for actionable intelligence

## Data analysis

Analyze the processed information using OSINT analysis tools

## Results delivery

Report findings to customer/red team

# Search Engines

*Google, Bing, Yandex, Baidu, ...*

Refined searches for certain kinds of information (“Google-Fu”)

Useful operators: `intext`, `intitle`, `inurl`, `filetype`, `site`, ...

*Netcraft*: uptime and web server info

*Internet Archive’s Wayback Machine*: old site versions

*Reddit/Google/Yahoo groups*: sysadm questions, gossip, ...

*LinkedIn*: persons within an organization, interests, ...

*Qualys’ SSL report*: SSL configuration of public web servers

Many more: phone directories, “people” search, government/state databases, open data APIs, dark web search, ...

## Background

Site title	HOME   Department of Computer Science	Date first seen	June 2005
Site rank	185389	Primary language	English
Description	Not Present		

## Network

Site	<a href="http://www.cs.stonybrook.edu">http://www.cs.stonybrook.edu</a>	Domain	stonybrook.edu
Netblock Owner	Pantheon	Nameserver	nocnoc.stonybrook.edu
Hosting company	Pantheon	Domain registrar	Unknown
Hosting country	US	Nameserver organisation	Unknown
IPv4 address	23.185.0.4 ( <a href="#">VirusTotal</a> )	Organisation	Unknown
IPv4 autonomous systems	AS54113	DNS admin	dns_tech@stonybrook.edu
IPv6 address	2620:12a:8001:0:0:0:0:4	Top Level Domain	Educational entities (.edu)
IPv6 autonomous systems	AS54113	DNS Security Extensions	Unknown
Reverse DNS	Unknown		

## IP delegation

### IPv4 address (23.185.0.4)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority

[LEARN MORE](#)[REPORT FRAUD ↗](#)

## Hosting History

Netblock owner	IP address	OS	Web server	Last seen
	23.185.0.4	Linux	nginx	15-Jan-2024
<a href="#">Pantheon 717 California St Fl 3 San Francisco CA US 94108</a>	23.185.0.2	Linux	nginx	17-Oct-2023
<a href="#">Pantheon 717 California St Fl 3 San Francisco CA US 94108</a>	23.185.0.2	unknown	nginx	12-Apr-2021
<a href="#">Pantheon 717 California St Fl 3 San Francisco CA US 94108</a>	23.185.0.2	Linux	nginx	9-Jul-2020
▶ Amazon.com, Inc. Amazo...	107.22.178.157	Linux	nginx	4-Sep-2018
▶ State University of Ne...	130.245.27.2	-	Apache/2.2.22 Ubuntu	15-Apr-2017
▶ State University of Ne...	130.245.27.2	Linux	Apache/2.2.22 Ubuntu	3-Mar-2017
▶ State University of Ne...	130.245.27.2	Linux	Apache	5-Aug-2014
▶ State University of Ne...	130.245.27.2	Linux	Apache/2.2.3 Red Hat	25-Apr-2010
▶ State University of Ne...	130.245.27.2	Solaris	Netscape-Enterprise/3.5.1	4-Apr-2005

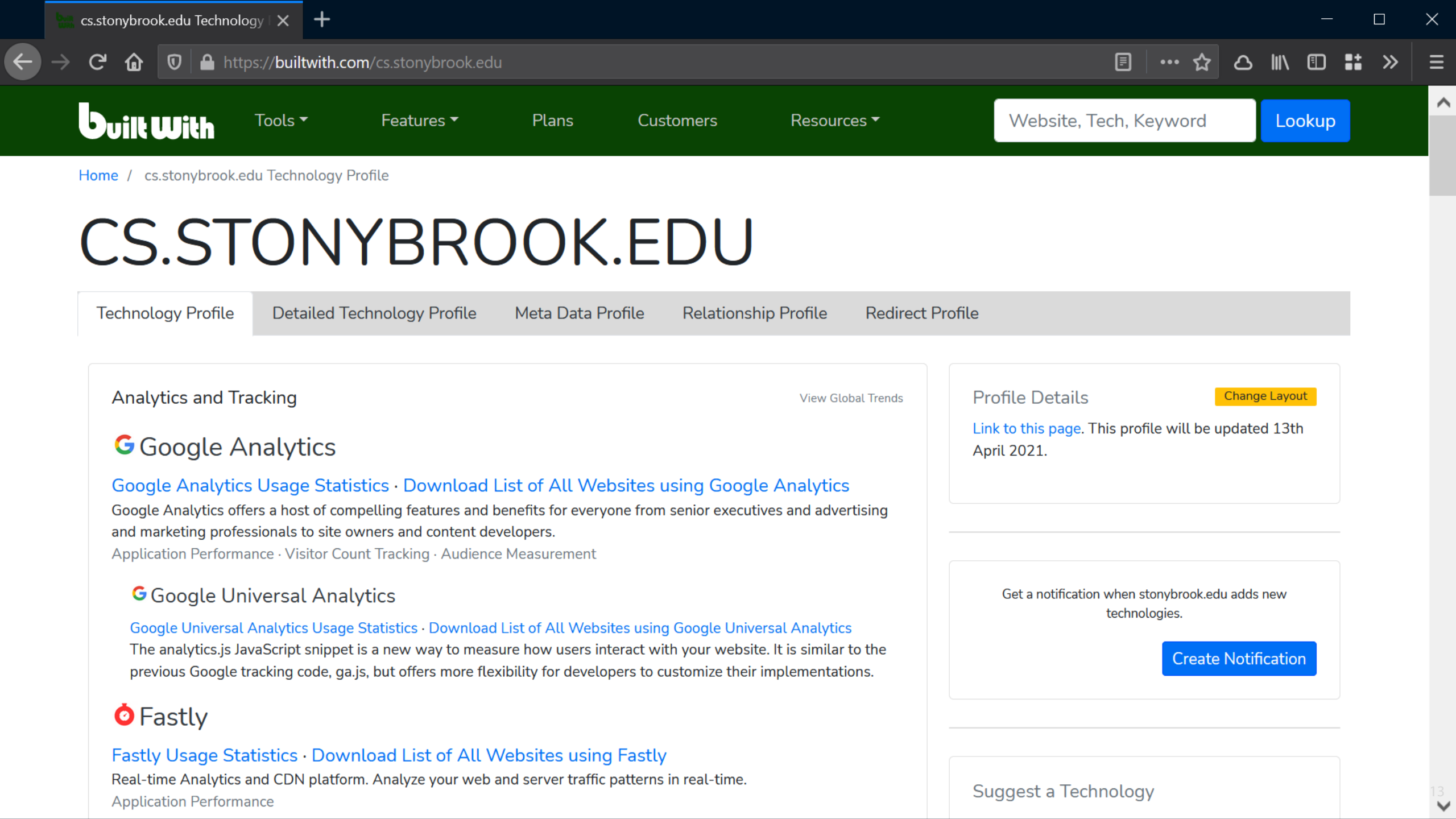
## Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of [rules](#). Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see [open-spf.org](#).

Warning: It appears that this host does not have an SPF record. There may be an SPF record on stonybrook.edu: Check the [site report](#).

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any [mail-enabled subdomains](#). It is recommended to add an SPF record to any subdomain with an MX record.





Tools ▾

Features ▾

Plans

Customers

Resources ▾

Website, Tech, Keyword

Lookup

Home / cs.stonybrook.edu Technology Profile

# CS.STONYBROOK.EDU

Technology Profile

Detailed Technology Profile

Meta Data Profile

Relationship Profile

Redirect Profile

## Analytics and Tracking

[View Global Trends](#)

### Google Analytics

[Google Analytics Usage Statistics](#) · [Download List of All Websites using Google Analytics](#)

Google Analytics offers a host of compelling features and benefits for everyone from senior executives and advertising and marketing professionals to site owners and content developers.

[Application Performance](#) · [Visitor Count Tracking](#) · [Audience Measurement](#)

### Google Universal Analytics

[Google Universal Analytics Usage Statistics](#) · [Download List of All Websites using Google Universal Analytics](#)

The analytics.js JavaScript snippet is a new way to measure how users interact with your website. It is similar to the previous Google tracking code, ga.js, but offers more flexibility for developers to customize their implementations.

### Fastly

[Fastly Usage Statistics](#) · [Download List of All Websites using Fastly](#)

Real-time Analytics and CDN platform. Analyze your web and server traffic patterns in real-time.

[Application Performance](#)

## Profile Details

[Change Layout](#)

[Link to this page](#). This profile will be updated 13th April 2021.

Get a notification when stonybrook.edu adds new technologies.

[Create Notification](#)

[Suggest a Technology](#)

# SpiderFoot <http://www.spiderfoot.net/>

 SpiderFoot [New Scan](#) [Scans](#) [Settings](#) [About](#)

## Zeus IP: 92. [REDACTED] 226

[Status](#) [Browse](#) [Graph](#) [Scan Settings](#) [Log](#) [Refresh](#) [Download](#)  [Search](#)

Type	Unique Data Elements	Total Data Elements	Last Data Element
<a href="#">Affiliate - Internet Name</a>	24	24	2015-04-13 01:00:57
<a href="#">Affiliate - IP Address</a>	22	22	2015-04-13 01:00:57
<a href="#">BGP AS Membership</a>	1	1	2015-04-13 01:01:00
<a href="#">BGP AS Peer</a>	103	103	2015-04-13 01:02:32
<a href="#">DNS TXT Record</a>	1	1	2015-04-13 01:00:14
<a href="#">Domain Name</a>	1	1	2015-04-13 01:00:08
<a href="#">Domain Whois</a>	1	1	2015-04-13 01:00:14
<a href="#">Email Gateway (DNS 'MX' Records)</a>	1	1	2015-04-13 01:00:14
<a href="#">HTTP Headers</a>	2	2	2015-04-13 01:00:35
<a href="#">HTTP Status Code</a>	1	2	2015-04-13 01:00:35
<a href="#">Internet Name</a>	3	3	2015-04-13 01:00:34
<a href="#">IP Address</a>	1	2	2015-04-13 01:00:07
<a href="#">Linked URL - External</a>	69	72	2015-04-13 01:00:51
<a href="#">Linked URL - Internal</a>	2	2	2015-04-13 01:00:35
<a href="#">Name Server (DNS 'NS' Records)</a>	2	2	2015-04-13 01:00:14



# 23.185.0.2

Reverse Unknown

### Geoloc \*

Country US  
 City Unknown  
 Organization [Fastly](#)  
 ASN AS54113  
 Subnet 23.185.0.0/24

### Inetnum

Country US  
 Netname Undisclosed  
 Subnet Undisclosed  
 Information Undisclosed

### Pastries

- <https://pastebin.com/zP9Mu7Dp> (2019-02-13)
- <https://pastebin.com/4DzCDmgz> (2019-02-12)
- <https://pastebin.com/qREigUhN> (2019-02-12)
- <https://pastebin.com/PnEN3mnQ> (2019-02-11)
- <https://pastebin.com/JW4E8B7q> (2019-02-10)
- <https://pastebin.com/4McCpDyX> (2019-02-10)
- <https://pastebin.com/bSZc3gay> (2019-02-09)
- <https://pastebin.com/aEJ3stwz> (2019-02-07)
- <https://pastebin.com/7m1SJAnW> (2019-02-07)
- <https://pastebin.com/W7J5VqgA> (2019-02-06)

### Resolver

- Forward - [jobstobedone.org](http://jobstobedone.org) (2019-02-13)
- Forward - [comunilife.org](http://comunilife.org) (2019-02-13)
- Forward - [factor-tech.com](http://factor-tech.com) (2019-02-13)
- Forward - [payasvcs.com](http://payasvcs.com) (2019-02-13)
- Forward - [freedomrc.org](http://freedomrc.org) (2019-02-13)
- Forward - [littlebodies.com.cn](http://littlebodies.com.cn) (2019-02-12)
- Forward - [novonordiskportal.ca](http://novonordiskportal.ca) (2019-02-12)
- Forward - [gileadportal.ca](http://gileadportal.ca) (2019-02-12)
- Forward - [www.thegoco.com](http://www.thegoco.com) (2019-02-12)
- Forward - [webtalkies.in](http://webtalkies.in) (2019-02-12)



# Google Dorking

<code>intext</code>	look for keywords only in main text
<code>allintext</code>	look for all the keywords only in main text
<code>inurl</code>	look for keywords only in URL
<code>allinurl</code>	look for all the keywords only in URL
<code>intitle</code>	look for keywords only in title
<code>allintitle</code>	look for all the keywords only in title
<code>inanchor</code>	look for keywords in anchor links
<code>site</code>	search only within the given site
<code>ext/filetype</code>	look only for the given type of file
<code>link</code>	look for external links to pages
<code>numrange</code>	look for specific numbers
<code>daterange</code>	look for a particular date range

inurl:"sap-system-login" - x

← → ↻ <https://www.google.com/search?q=inurl:"sap-system-login"> ☆ ☰

Google inurl:"sap-system-login" 🔊 🔍 Sign in

All Images News Videos Shopping More Search tools ⚙️

About 478 results (0.17 seconds)

**Logon - SAP Web Application Server - Consumers Energy**  
[https://www.consumersenergy.com/.../hrrcf\\_a\\_startpa...](https://www.consumersenergy.com/.../hrrcf_a_startpa...) Consumers Energy

**Configure Automatic SAP System Login with sapshcut - ITsiti**  
[itsiti.com/configure-automatic-sap-system-login-with-sapshcut](https://itsiti.com/configure-automatic-sap-system-login-with-sapshcut)  
Please make sure that you already insert all your SAP system configuration in your SAPGUI shortcut (normally in desktop). To test the SAP system with no ...

**Logon - SAP Web Application Server**  
<https://suppliers.danfoss.com/?sap-system-login-oninputprocessing...>

**LOGIN تسجيل الدخول - SAP Web Application Server**  
[https://jobs.aramco.com/.../hrrcf\\_a\\_reg\\_applwizard\\_ext?sap-system-logi...](https://jobs.aramco.com/.../hrrcf_a_reg_applwizard_ext?sap-system-logi...)

**Logon - SAP Web Application Server**  
<extranet.fater.it:8003/.../bbpstart/?sap-system-login...> - Translate this page

**Logon - Infosys Careers Web Application**  
[https://careers.infosys.com/.../zhrrcf\\_a\\_startpage\\_row\\_lateral?sap-system...](https://careers.infosys.com/.../zhrrcf_a_startpage_row_lateral?sap-system...)

**Logon - SAP Web Application Server - Oak Ridge National ...**  
[https://recruiting.ornl.gov/.../zornl\\_a\\_startpage\\_ext\\_cand?sap-system-log...](https://recruiting.ornl.gov/.../zornl_a_startpage_ext_cand?sap-system-log...)

**Anmeldung - SAP Web Application Server**  
[https://online-hr.zf.com/.../hrrcf\\_a\\_...](https://online-hr.zf.com/.../hrrcf_a_...) - Translate this page ZF Friedrichshafen

**Logon - Mol**  
<https://recruiting.mol.hu/.../sap/system/login.htm?> - Translate this page

intitle:"RouterOS" intitle:"configuration page" intext:"You have connected to

Google

intitle:"RouterOS" intitle:"configuration page" intext:"You have connected to

All Videos Images Shopping News More Search tools

About 363 results (0.21 seconds)

**RouterOS router configuration page**  
ns.dacogr.com/ ▼  
You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator. User:

**RouterOS router configuration page**  
oakamyan.muk.ac.ir/ ▼  
You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

**RouterOS router configuration page**  
dakorwest.com/ ▼  
You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

**RouterOS router configuration page**  
191.36.165.228/ ▼  
You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator. Select action ...

**RouterOS router configuration page**  
95.142.143.47/ ▼  
You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator. Select action:.

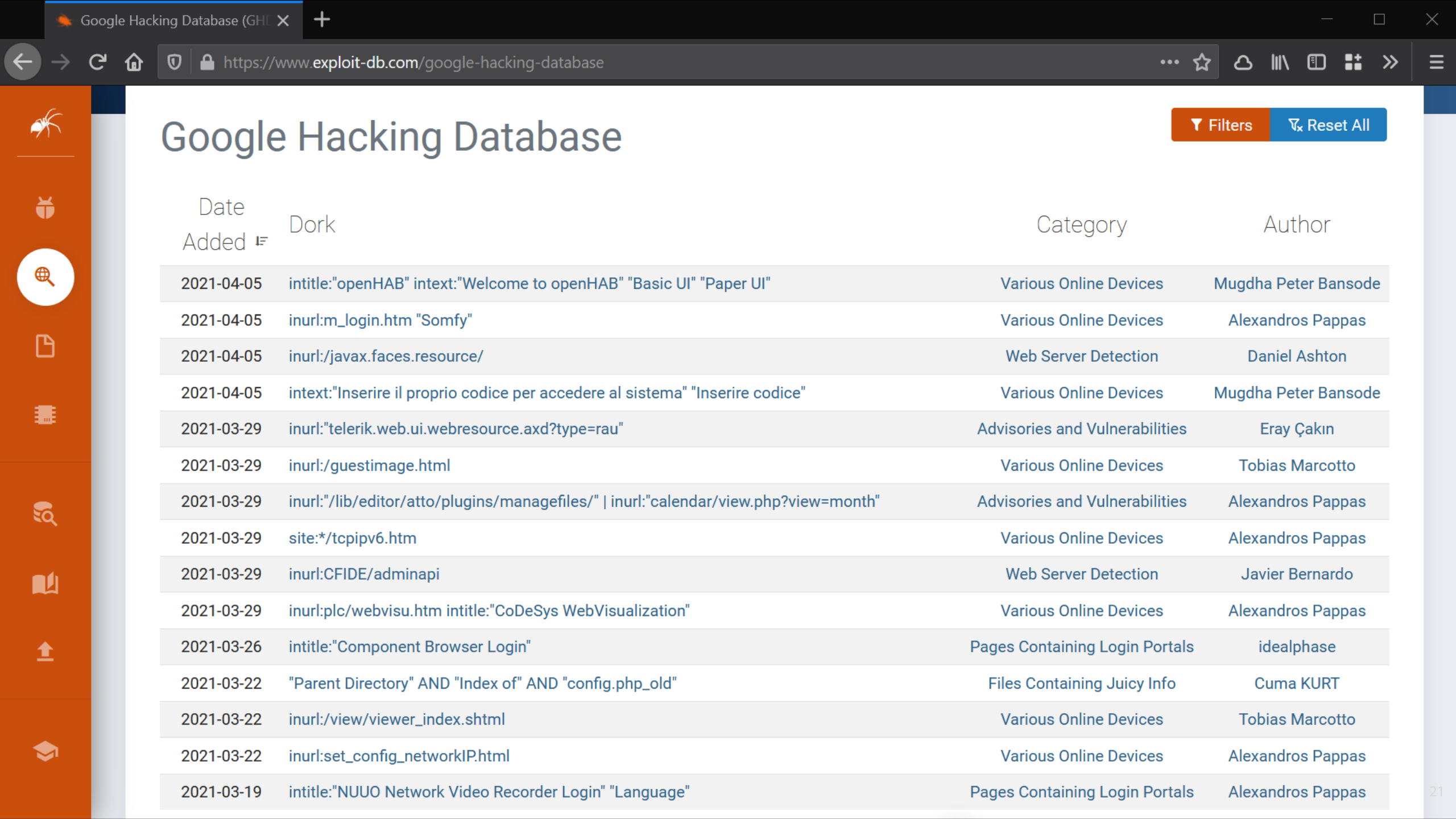
**RouterOS router configuration page - Catalog Software**  
www.catalogsoftware.org/get/dl/467194/ ▼  
You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

Browser window showing a Google search for "Password=" inurl:web.config -intext:web.config ext:config. The search results display several entries related to web.config files, including snippets of configuration code and file paths.

Search query: "Password=" inurl:web.config -intext:web.config ext:config

About 728 results (0.20 seconds)

- web.config**  
ftp.mvaonline.com/partners.mvacolumbia.com/wwwroot/web.config  
... connectionString="Data Source=ns1.nightshade.arvixe.com;Initial Catalog=dnn\_mva;User ID=cballesteros;Password=[REDACTED]" providerName="System."
- Copy of web.config - EarSinus.com**  
earsinus.com/new/Copy%20of%20web.config  
... the provider is specified passwordAttemptThreshold="int" The number of failed password attempts, or failed password answer attempts that are allowed before ...
- Web.config**  
ftp://60.250.85.148/StreamStore/WG/WebService/Web.config  
C:\wra10\FCT FcPumps.xml WaterLevel.xml Data Source=127.0.0.1;Initial Catalog=River;User ID=sa;Password=[REDACTED]
- web.config - Axis HR**  
www.axishrpro.co.uk/wwwroot/web.config  
SQLExpress;Database=hrpro;User ID=hrpro;Password=[REDACTED] /> </connectionStrings>  
<appSettings> <add key="SQLServerConn" value="Server=.
- D:\IMG\_Catalogazione\ server=192.168.0.157 ...**  
ftp://37.186.241.19/InformFTP/pub/RussoM/.../marubi.../Web.Config  
D:\IMG\_Catalogazione\ server=192.168.0.157;Trusted\_Connection=false;User ID=sa;Password=[REDACTED] Initial Catalog=marubi\_web\_cp; server=192.168.0.157 ...
- web.config - PASA**  
www.pasaweb.com/forum/web.config  
... during which failed password attempts and failed password answer attempts are tracked enablePasswordRetrieval="[true|false]" Should the provider support ...



# Google Hacking Database

Filters Reset All

Date Added	Dork	Category	Author
2021-04-05	intitle:"openHAB" intext:"Welcome to openHAB" "Basic UI" "Paper UI"	Various Online Devices	Mugdha Peter Bansode
2021-04-05	inurl:m_login.htm "Somfy"	Various Online Devices	Alexandros Pappas
2021-04-05	inurl:/javax.faces.resource/	Web Server Detection	Daniel Ashton
2021-04-05	intext:"Inserire il proprio codice per accedere al sistema" "Inserire codice"	Various Online Devices	Mugdha Peter Bansode
2021-03-29	inurl:"telerik.web.ui.webresource.axd?type=rau"	Advisories and Vulnerabilities	Eray Çakın
2021-03-29	inurl:/guestimage.html	Various Online Devices	Tobias Marcotto
2021-03-29	inurl:"/lib/editor/atto/plugins/managefiles/"   inurl:"calendar/view.php?view=month"	Advisories and Vulnerabilities	Alexandros Pappas
2021-03-29	site:*/tcpip6.htm	Various Online Devices	Alexandros Pappas
2021-03-29	inurl:CFIDE/adminapi	Web Server Detection	Javier Bernardo
2021-03-29	inurl:plc/webvisu.htm intitle:"CoDeSys WebVisualization"	Various Online Devices	Alexandros Pappas
2021-03-26	intitle:"Component Browser Login"	Pages Containing Login Portals	idealphase
2021-03-22	"Parent Directory" AND "Index of" AND "config.php_old"	Files Containing Juicy Info	Cuma KURT
2021-03-22	inurl:/view/viewer_index.shtml	Various Online Devices	Tobias Marcotto
2021-03-22	inurl:set_config_networkIP.html	Various Online Devices	Alexandros Pappas
2021-03-19	intitle:"NUUO Network Video Recorder Login" "Language"	Pages Containing Login Portals	Alexandros Pappas



## Non-technical Information

Any kind of information about persons, operations, behaviors, is very useful for targeted attacks

*Spear phishing:* messages that appear to come from trusted sources

*Watering hole attacks:* target the members of a group by infecting websites they are known to regularly visit

Social networks, corporate websites, partners/third-parties, mailing lists, impersonation, social engineering, ...

LinkedIn, Twitter, Facebook, Instagram, Glassdoor, GitHub, Stackoverflow, ...

Public actions may also reveal actionable information

Example: the target's system administrator asks on ServerFault how to secure Nginx

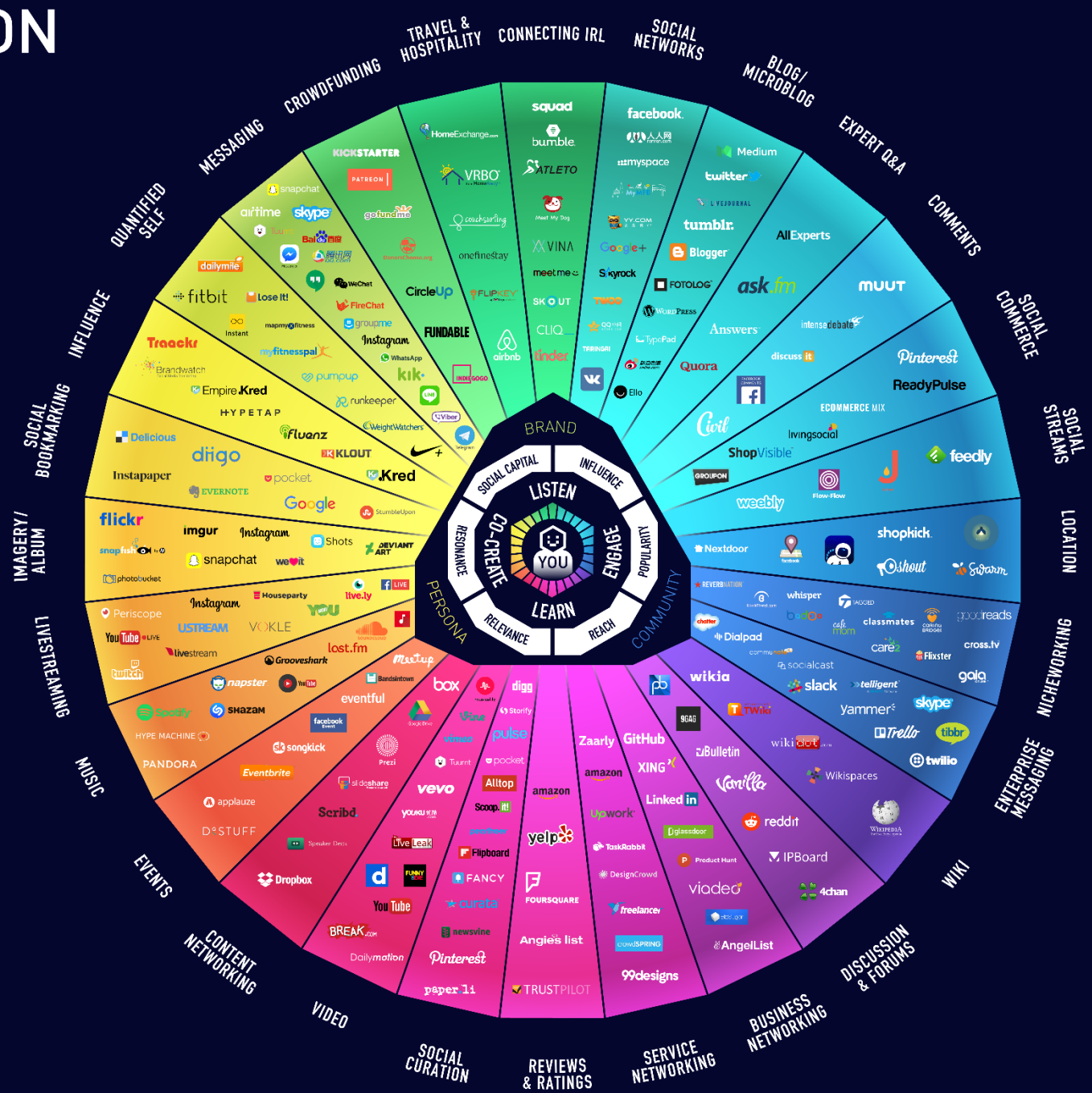
# CONVERSATION PRISM 5.0

Brought to you by  
Brian Solis & JESS3

## Social Media Gave Everyone a Voice

The Conversation Prism debuted in 2008 as social media was exploding online. Social media would change everything about how we communicate, learn and share. It forever democratized information and reset the balance for influence.

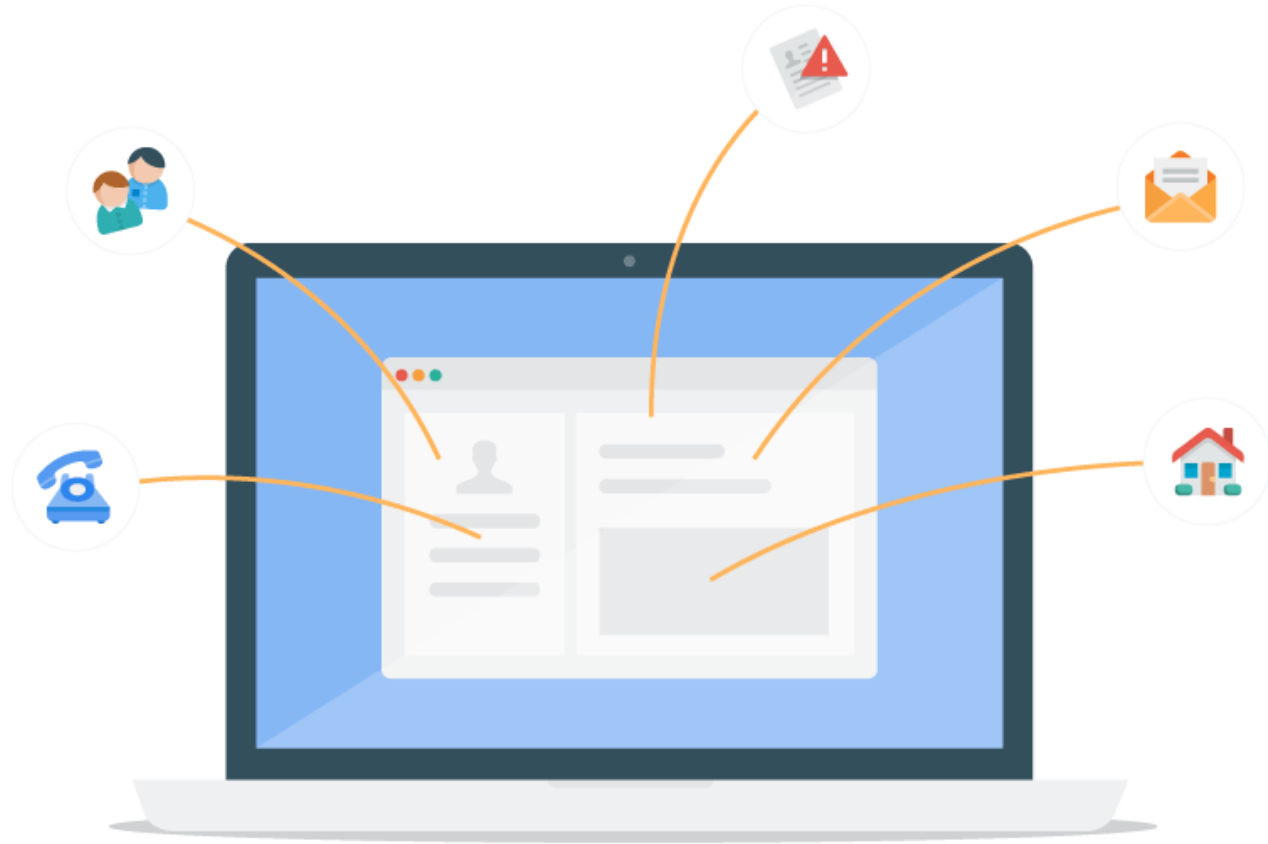
The Conversation Prism was designed as a visual map of the conversational networks that continue to reshape everything. Its purpose is to help you understand and appreciate the statusphere so that you can play a productive and defining role in the conversations shaping our future.



For more information check out  
[conversationprism.com](http://conversationprism.com)

# What is Spokeo?

Spokeo is a people search engine that organizes white pages listings, public records and social network information into simple profiles to help you safely find and learn about people.





Check the use of your brand or username on 160 Social Networks:

To check the availability of your username on over 500 social networks check out our new, updated site at: [KnowEm.com](https://knowem.com).

KnowEm also offers a Premium Service which will create profiles for you on up to 300 popular social media sites.

3.4k Shares



- |              |                        |                 |                  |
|--------------|------------------------|-----------------|------------------|
| You Tube     | Live Leak              | APSense         | Intense Debate   |
| Wikipedia    | Zimbio                 | Folkd           | Design Float     |
| Linked In    | Houzz                  | Watt Pad        | Stock Twits      |
| Twitter      | My Space               | Empire Avenue   | Fotki            |
| Ebay         | Game Spot              | Spark People    | Trend Hunter     |
| Tumblr       | Cracked                | N4G             | Ads Of The World |
| Pinterest    | Behance                | Veoh            | Eventful         |
| Blogger      | Sky Rock               | Ebaums World    | Tiny Chat        |
| Imgur        | Viadeo                 | Dzone Links     | Shock Wave       |
| Flickr       | We Heart It            | Mouth Shut      | Active Rain      |
| Word Press   | Fan Pop                | Yuku            | Destructoid      |
| Daily Motion | Dreams Time            | Fark            | Blog Catalog     |
| Reddit       | I Can Has Cheezburger? | Blog Talk Radio | Boonex           |
| CNET         | Meta Cafe              | Zedge           | Tech Dirt        |
| Vimeo        | Last FM                | Dat Piff        | Jigsy            |
| Slide Share  | Hi5                    | Wonder How To   | The Hype Machine |
| Deviant Art  | The Motley Fool        | Crunchy Roll    | Moby Picture     |
| Live Journal | Fixya                  | 8 Tracks        | Wall Inside      |
| Yelp         | Kongregate             | Red Bubble      | Programmable Web |
| Wikia        | My Fitness Pal         | BitLy           | All My Faves     |
| Armchair GM  | Ultimate Guitar        | Photo Dune      | Bigger Pockets   |
| Fiverr       | Dribbble               | Wanelo          | Kiva             |
| Etsy         | eToro                  | Active          | Blurb            |
| Ask FM       | Instructables          | Colour Lovers   | Fat Secret       |
| Source Forge | 500px                  | Listal          | Carbon Made      |
| Wiki How     | Gravatar               | Toluna          | Element14        |

Have I Been Pwned: Check if you... x +


← → ↻ https://haveibeenpwned.com

Home Notify me Domain search Who's been pwned Passwords API About Donate ₿ ₩

# ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address **pwned?**

 Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

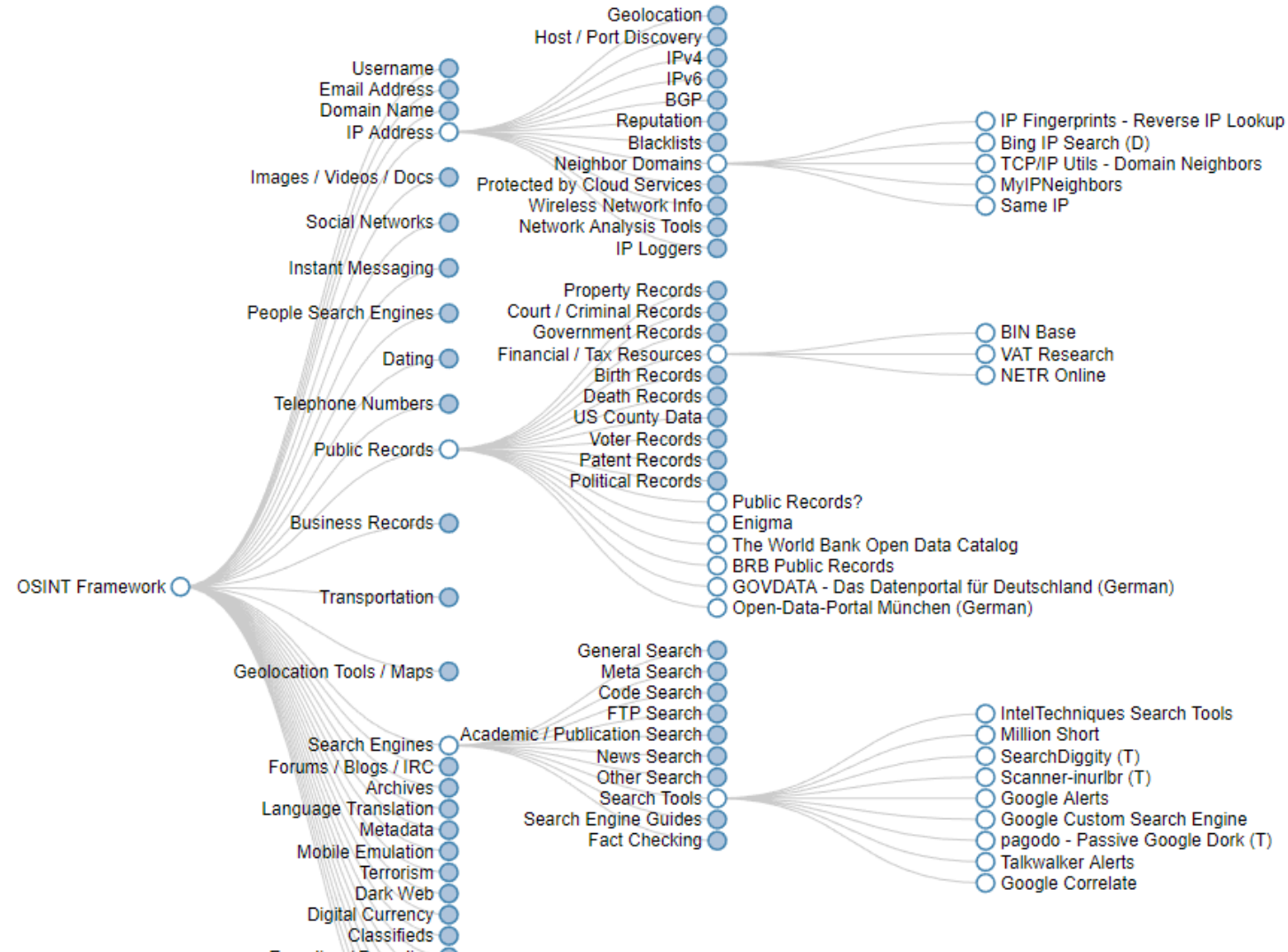
[Why 1Password?](#)

341	6,474,030,172	89,449	100,145,660
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches Recently added breaches

# OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally  
(D) - Google Dork, for more information: [Google Hacking](#)  
(R) - Requires registration  
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually





# Recon-ng <https://github.com/lanmaster53/recon-ng>

```

  /_/_/_/  /_/_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/
 /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/
/_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/
/_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/  /_/_/_/

Sponsored by...

      /\
     /\ \  /\
    /\  \/\  \/\
   /\  \/\  \/\  \/\
  // // BLACK HILLS \/\ \
 www.blackhillsinfosec.com

[recon-ng v4.7.3, Tim Tomes (@LaNMaSteR53)]

[79] Recon modules
[7]  Reporting modules
[2]  Import modules
[2]  Exploitation modules
[2]  Discovery modules

[recon-ng][default] > █
```



# Discover <https://github.com/leebaird/discover>

```
DISCOVER
```

```
By Lee Baird
```

```
RECON
```

1. Domain
2. Person
3. Parse salesforce

```
SCANNING
```

4. Generate target list
5. CIDR
6. List
7. IP, range, or URL

```
WEB
```

8. Open multiple tabs in Firefox
9. Nikto
10. SSL

```
MISC
```

11. Crack WiFi
12. Parse XML
13. Generate a malicious payload
14. Start a Metasploit listener
15. Update
16. Exit

```
Choice: _
```

# Maltego

The screenshot displays the Maltego Chlorine CE 3.6.0 interface. The main window shows a network graph with nodes of various colors (blue, yellow, red, pink, cyan, grey) connected by lines. The interface includes a menu bar (Investigate, Manage, View, Organize, Machines, Collaboration), a toolbar with icons for Copy, Paste, Cut, Delete, and various selection and zooming tools. On the left, there is a Palette with categories like Devices, Infrastructure, Locations, Penetration Testing, Personal, and Social Network. Below the Palette is a Run View section. On the right, there are Overview, Detail View, and Property View panels. A legend at the bottom right identifies node types: Website (blue), Person (grey), URL (yellow), Phrase (cyan), Phone Number (red), Location (green), Email Address (pink), and Domain (dark red).

Maltego Chlorine CE 3.6.0

Investigate Manage View Organize Machines Collaboration

Clipboard Transforms Find

Number of Results: 12 50 255 10k

Quick Find

Select All Add Similar Siblings Select Children Add Children Select by Type Zoom to Zoom In

Invert Selection Add Path Select Neighbors Add Neighbors Select Links Zoom to Fit Zoom Out

Select None Select Parents Add Parents Select Bookmarked Reverse Links Zoom 100% Zoom Selection

Zoom

Palette

Home ryan

Main View Bubble View Entity List

Overview

Detail View

Property View

<No Selection>

<No Properties>

Website Phrase Email Address  
Person Phone Number Domain  
URL Location

# WHOIS

Protocol for querying databases with registration information about assignees of internet resources

IP address blocks, domain names, and autonomous systems

Top registries: AFRINIC, APNIC, ARIN, IANA, ICANN, LACNIC, NRO, RIPE, InterNic

`whois` command-line utility

```
# whois stonybrook.edu
```

```
# whois 130.245.27.2
```

Registrars and third-party services provide web interfaces

Useful information

Registrar information, domain creation/expiration dates, primary DNS name servers

First Name, Last Name, Organization, physical address, phone number, and e-mail address

Assigned domain administrator, billing contact, technical contact

# DNS

## Valuable information about individual hosts

- IP addresses (A, AAAA) of certain domains

- Name (NS) and mail (MX) servers of a domain

- Name aliases (CNAME) and reverse mappings (PTR)

## Other useful records

- SRV: generic locator (protocol, host, port) for domain services (e.g., Kerberos, LDAP, SIP, XMPP)

- TXT: SPF, DKIM, DMARC (*email lecture*), and other custom information

- HINFO: CPU, OS, and other host-related information

## Various utilities: [nslookup](#), [dig](#), [host](#)

## Zone transfers (AXFR) provide all entries for a domain

- Used mostly for replication across secondary DNS servers

- Wealth of information, often very sensitive: subdomains, internal IPs/hosts, services used, ...

# DNS Brute Forcing

Zone transfers are usually restricted only among authorized servers

Although misconfigurations are common...

Alternative: *guess* valid DNS records

Dictionary attack using A/AAAA record requests

Query based on list of commonly used subdomains, hostnames, words, and so on (e.g., `www`, `mail`, `vpn`, `webaccess`, `msexchange`)

DNSSEC NSEC and NSEC3 zone walking

The NSEC record is used to give negative answers to queries, but has the side effect of allowing enumeration of all names

NSEC3 mitigates this, but still allows for dictionary attacks

# dnsenum <https://github.com/fwaeytens/dnsenum>

```
root@kali:~# dnsenum -f dns.txt cs.stonybrook.edu
dnsenum.pl VERSION:1.2.3

----- cs.stonybrook.edu -----

Host's addresses:
-----
cs.stonybrook.edu.          5      IN      A       130.245.9.212

Name Servers:
-----
mewho.stonybrook.edu.      5      IN      A       199.110.254.244
nocnoc.stonybrook.edu.     5      IN      A       129.49.7.3
whoisthere.stonybrook.edu. 5      IN      A       129.49.7.250

Mail (MX) Servers:
-----
aspmx2.googlemail.com.    5      IN      A       64.233.190.27
aspmx3.googlemail.com.    5      IN      A       209.85.203.27
aspmx.l.google.com.       5      IN      A       74.125.22.27
alt1.aspmx.l.google.com.  5      IN      A       64.233.190.27
alt2.aspmx.l.google.com.  5      IN      A       209.85.203.27

Trying Zone Transfers and getting Bind Versions:
-----
```

# Fierce <http://ha.ckers.org/fierce/>

```
root@kali:~# fierce -dns stonybrook.edu
DNS Servers for stonybrook.edu:
    mewho.stonybrook.edu
    whoisthere.stonybrook.edu
    nocnoc.stonybrook.edu

Trying zone transfer first...
    Testing mewho.stonybrook.edu
        Request timed out or transfer not allowed.
    Testing whoisthere.stonybrook.edu
        Request timed out or transfer not allowed.
    Testing nocnoc.stonybrook.edu
        Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
129.49.2.10    p250.cc.stonybrook.edu
129.49.2.6    pepprod.cc.stonybrook.edu
129.49.2.1    cisco-gw.cc.stonybrook.edu
129.49.2.2    dns4cc.cc.stonybrook.edu
129.49.2.3    peptest.cc.stonybrook.edu
129.49.2.7    psns.cc.stonybrook.edu
129.49.2.8    noldb.cc.stonybrook.edu
129.49.2.11   archive.cc.stonybrook.edu
129.49.2.12   nolpr.cc.stonybrook.edu
129.49.2.13   pepdev.cc.stonybrook.edu
129.49.2.14   twdbs.cc.stonybrook.edu
129.49.2.15   sandbox.cc.stonybrook.edu
```

# Network Scanning

Identify accessible hosts, running services, service and OS versions, ...

*Active probing:* target network can observe probe requests

As opposed to passive reconnaissance or querying of public sources

Stealthiness matters! Intrusion detection systems can easily detect noisy scans

Two main dimensions

**Horizontal scanning:** scan a subnet (or the whole internet) on a particular port

Example: find all hosts running a vulnerable service (internet worms)

**Vertical scanning:** scan all (or a subset of) ports on a given host

Optimization: scan common ports first

Scanning using `ping` and `netcat` can be used for quick assessments



# Nmap

De facto tool for network scanning

Support for many port scan types

- sS TCP SYN scan: just wait for the ACK
- sT TCP connect scan: full connection (useful for non-root)
- sU UDP scan: protocol-specific payload for known ports
- sA ACK scan: determine if a firewall is stateful
- sO IP protocol scan: determine IP protocols (TCP, ICMP, IGMP) used
- p Specify port range (default: 1000 most common ports)

Beyond simple port scanning: extensible framework with support for third-party scripts

```
auth, broadcast, brute, default, discovery, dos, exploit,  
external, fuzzer, intrusive, malware, safe, version, vuln
```



## Service Fingerprinting

After locating an open port, gather more information about its service

```
# nmap -sV 192.168.0.1 -p 22
```

Complete the connection and identify the software type and version

Version detection “interrogates” open ports to determine more about what is running

*Server-initiated dialog:* banner grabbing

Upon receiving a client connection, the server transmits a “banner” string that often includes version information (e.g., SSH)

*Client-initiated dialog:* speculatively send “probe” application requests

Nmap has about 6,500 dialogue patterns for more than 650 protocols such as SMTP, FTP, HTTP, etc.

# Banner grabbing: Apache

```
HTTP/1.1 200 OK
Date: Thu, 05 Sep 2019 17:42:39 GMT
Server: Apache/2.4.41 (Unix)
Last-Modified: Thu, 05 Sep 2019 17:40:42 GMT
ETag: "75-591d1d21b6167"
Accept-Ranges: bytes
Content-Length: 117
Connection: close
Content-Type: text/html
...
```

# Banner grabbing: Nginx

HTTP/1.1 200 OK

**Server: nginx/1.17.3**

Date: Thu, 05 Sep 2019 17:50:24 GMT

Content-Type: text/html

Content-Length: 117

Last-Modified: Thu, 05 Sep 2019 17:40:42 GMT

Connection: close

ETag: "5d71489a-75"

Accept-Ranges: bytes

...

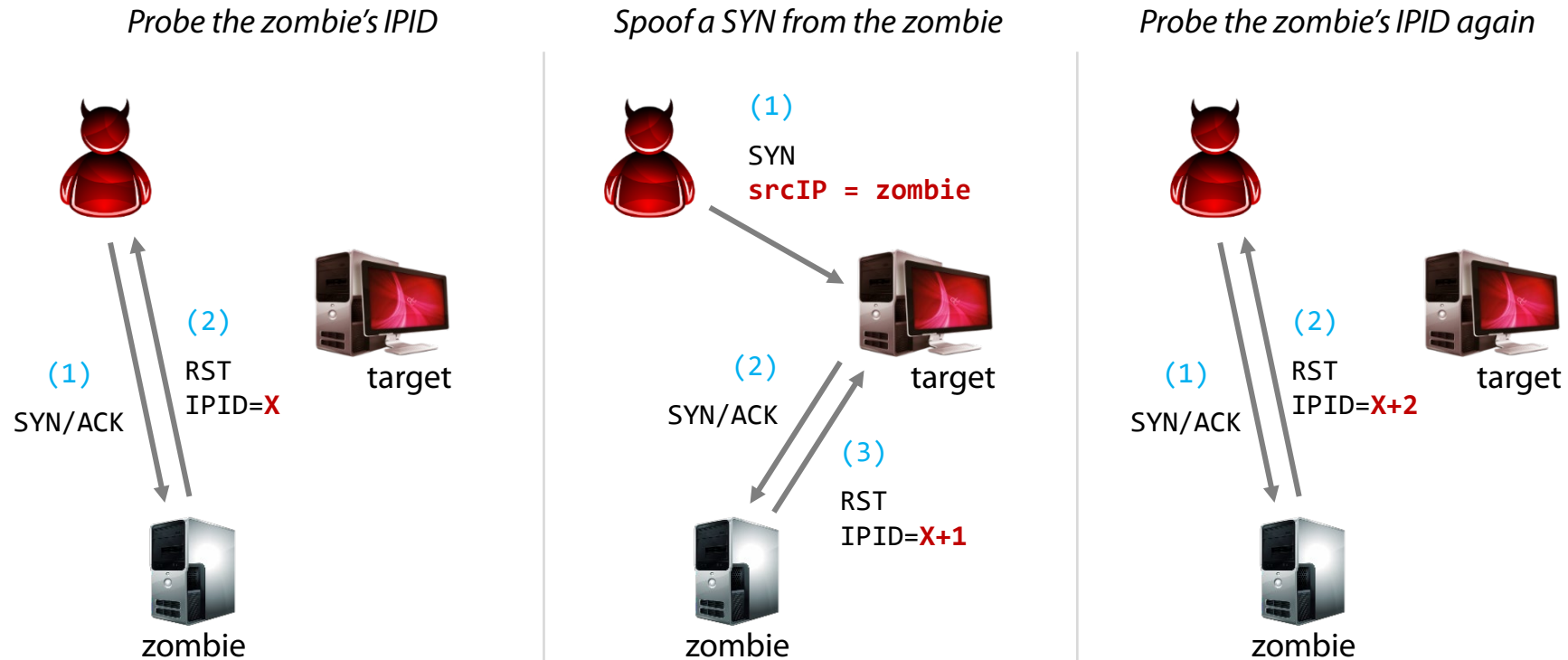
# Banner grabbing: Lighttpd

```
HTTP/1.0 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "4192788355"
Last-Modified: Thu, 05 Sep 2019 17:40:42 GMT
Content-Length: 117
Connection: close
Date: Thu, 05 Sep 2019 17:57:57 GMT
Server: lighttpd/1.4.54
...
```

# Idle Scan

Hide scan attempts by blaming another “zombie” host

Zombie must be mostly idle (e.g., network printer) and have predictable IPID behavior



# ARP Scan

Extremely useful technique for host enumeration in a LAN

Find every active IPv4 device in the same subnet

Send a “*who has*” broadcast packet for each IP address of interest

Example: try all 254 host IP addresses for a /24 subnet

Retry a couple of times if no response is received

Linux command-line tool: `arp-scan`

```
# arp-scan 192.168.0.0/24
```

## Fast Internet-wide Scanning <http://zmap.io>

Scan the entire IPv4 address space for a given port in ~45 minutes using a single machine and a gigabit link

### Speed gains

Eliminate per-connection state by overloading packet header fields (src port, initial Seq No.)—similar concept to SYN cookies

Bypass TCP stack: raw socket for packet transmission, `libpcap` to receive responses

Send as many probes as NIC can support

Don't wait for timeouts! Just send a fixed number of probes (usually one is enough to achieve decent coverage)

### Support for additional tools/plugins

ZGrab, ZDNS, ZCrypto, ZLint, ZCertificate, ...





# Shodan: Let others do the scanning for you

The screenshot shows the Shodan search results page for the query "Server: SQ-WEBCAM". The browser address bar shows the URL: <https://www.shodan.io/search?query=Server%3A+SQ-WEBCAM>. The page features a navigation bar with the Shodan logo, a search input field containing the query, and links for "Explore", "Enterprise Access", and "Contact Us". A "Login or Register" button is also present. Below the navigation bar, there are tabs for "Exploits" and "Maps".

The main content area is divided into several sections:

- TOP COUNTRIES:** A world map showing the distribution of results by country. Below the map is a table:

Country	Count
Germany	51
Lithuania	43
Hungary	37
United States	33
Poland	26

- TOP SERVICES:** A table showing the most common services found:

Service	Count
HTTP	196
HTTP (8080)	46
HTTP (81)	25
HTTP (83)	12
HTTP (84)	6

- TOP ORGANIZATIONS:** A table showing the most common organizations:

Organization	Count
TEO LT	40
Deutsche Telekom AG	40
CD-Telematika a.s.	11
Orange Polska	8
Versatel Deutschland	5

- TOP PRODUCTS:** A table showing the most common products:

Product	Count
86FF11AB.dsl.pool.telekom.hu	1

The main search results are displayed in a list format. Each result includes the IP address, the organization name, the date added, the location, and the server response details. The first three results are:

- 88.47.208.93**  
c-88-47-208-93.hsd1.tn.comcast.net  
**Comcast Cable**  
Added on 2018-03-28 03:36:44 GMT  
United States, Antioch  
**Details**  
HTTP/1.1 200 OK  
Connection: close  
Cache-Control: no-cache  
**Server: SQ-WEBCAM**  
CONTENT-LENGTH: 2936
- 61.126.182.66**  
p7066-1pbfx02aobadoni.miyagi.ocn.ne.jp  
**NTT**  
Added on 2018-03-28 02:59:19 GMT  
Japan  
**Details**  
HTTP/1.1 200 OK  
Connection: close  
Cache-Control: no-cache  
**Server: SQ-WEBCAM**  
CONTENT-LENGTH: 537
- 84.236.88.241**  
84-236-88-241.pool.digikabel.hu  
**DIGI Tavkozlesi es Szolgáltato Kft.**  
Added on 2018-03-28 01:55:29 GMT  
Hungary, Eger  
**Details**  
HTTP/1.1 200 OK  
Connection: close  
Cache-Control: no-cache  
**Server: SQ-WEBCAM**  
CONTENT-LENGTH: 1002
- 134.255.17.171**  
86FF11AB.dsl.pool.telekom.hu  
**Magyar Telekom**  
**Details**  
HTTP/1.1 200 OK  
Connection: close



IPv4 Hosts 130.245.42.0/24

Register Sign In

Results Map Metadata Report Docs

Quick Filters

For all fields, see Data Definitions

Autonomous System:

15 SUNYSB - SUNY at Stony Brook

Protocol:

12 22/ssh
4 443/https
2 3389/rdp
2 80/http

Tag:

12 ssh
4 http
4 https
2 rdp
2 remote\_display

IPv4 Hosts

Page: 1/1 Results: 15 Time: 183ms Query Plan: expanded

130.245.42.61

SUNYSB - SUNY at Stony Brook (5719) Stony Brook, New York, United States

3389/rdp

RDP REMOTE\_DISPLAY

130.245.42.138

SUNYSB - SUNY at Stony Brook (5719) Stony Brook, New York, United States

Ubuntu 443/https

CloudFlare Origin Certificate, i2p-metrics.np-tokumei.net

130.245.42.84

SUNYSB - SUNY at Stony Brook (5719) Stony Brook, New York, United States

Ubuntu 16.04 22/ssh

130.245.42.7

SUNYSB - SUNY at Stony Brook (5719) Stony Brook, New York, United States

Ubuntu 22/ssh

130.245.42.1

SUNYSB - SUNY at Stony Brook (5719) Stony Brook, New York, United States

Debian 22/ssh, 443/https, 80/http

EdgeOS UBNT Router UI

130.245.42.22 (styx.cs.stonybrook.edu)

# Vulnerability Scanning

Scan each found service for known vulnerabilities

Next step after “target scanning”

Perform non-intrusive checks to identify vulnerabilities and configuration weaknesses

Many types vulnerability scanners

Remote vs. local

Authenticated vs. unauthenticated

Source code vs. binary

Popular vulnerability scanner: Nessus (proprietary) → OpenVAS

Large database of “vulnerability tests” for target systems