

How Big is Your Foot?

Open Source Intelligence Gathering



Timothy Fawcett, CISSP
Robert Martinez



Guernsey, founded in 1928 in Oklahoma City provides a wide range of engineering, architecture, and consulting services. Guernsey has provided consulting services to electric cooperatives since the rural electrification program was started in the 30's. Just within the last 20 years, Guernsey has enjoyed a broad range of consulting assignments with over 200 electric cooperatives. Security-related services encompassing both physical and cyber security have long been a component of our electric cooperative consulting engagements.



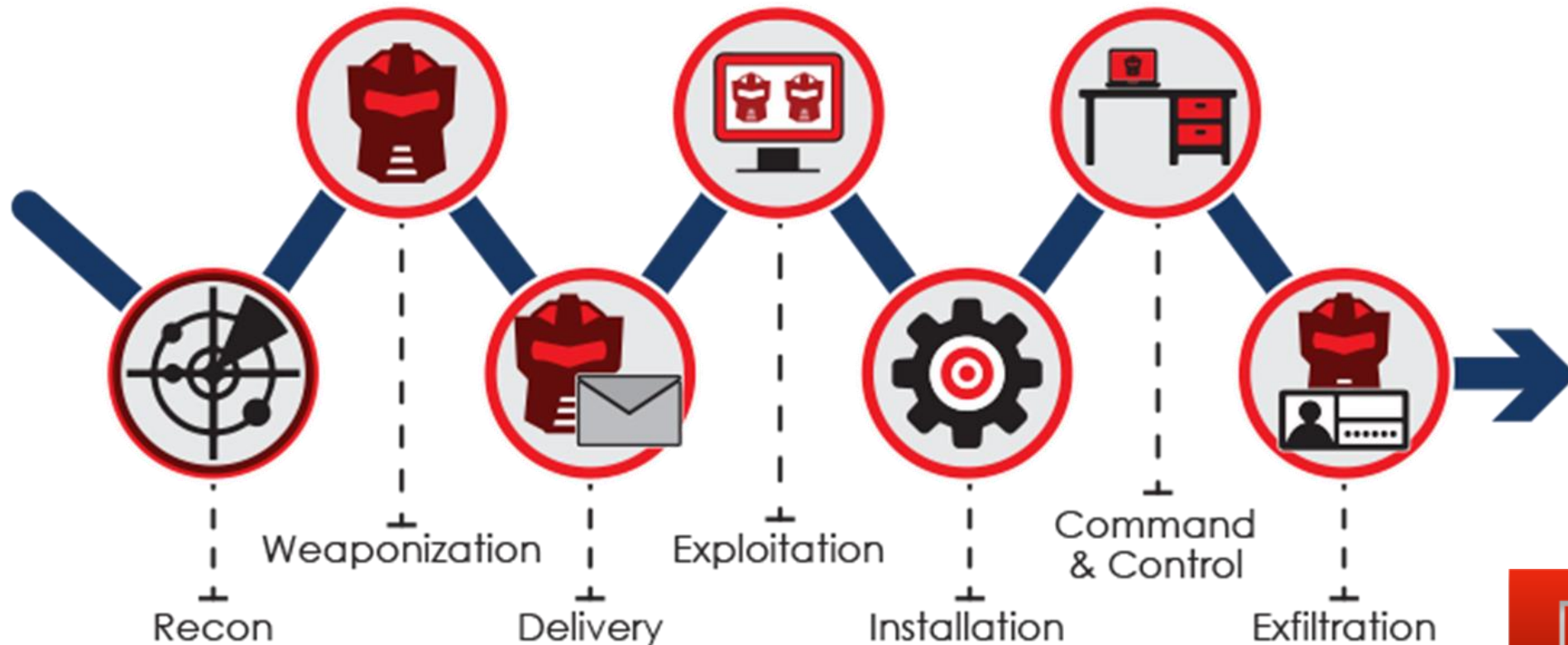
Tim Fawcett is a Senior Consultant and Director of Cyber Security Consulting with Guernsey. Tim has nearly 18 years of information assurance experience performing IT audits, risk assessments, and cyber threat and vulnerability analyses. Over his career Tim has consulted for scores of companies from start-ups to Fortune 500 companies. In six years at Guernsey Tim has provided cyber security consulting dozen of companies including over 20 electric cooperatives and municipalities in ten states. Tim is a Certified Information Systems Security Professional, a Certified Information Systems Auditor, a Payment Card Industry Professional, and a Certified AlienVault Security Engineer.



Robert Martinez is a Security Analyst with Guernsey. He has over 16 years of IT experience in areas of System Administration and Information Security. Many of the projects he completed for his clients include developing security policy, designing custom software to strengthen security and seamlessly integrate it into the environment. Robert has had the opportunity to work for companies in the Engineering, Medical, Law, and Media industries. At Guernsey, Robert uses a variety of enterprise related solutions as well as the same technology that hackers would use to penetrate networks and exploit vulnerabilities.

First Things First!

The Cyber Kill Chain® framework is part of the Intelligence Driven Defense model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective, the first step in this chain is reconnaissance.



guernsey

Reconnaissance

- Intelligence Gathering
- Target Selection
- Open Source Intelligence (OSINT)
- Covert Gathering
- Footprinting



guernsey

Intelligence Gathering

- Intelligence collection involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence
- An intelligence gathering network is a system through which information about a particular entity is collected for the benefit of another through the use of more than one, inter-related source. Such information may be gathered by a military intelligence, government intelligence, or commercial intelligence network.

Target Selection

- Identification and Naming of Target
- Consider any Rules of Engagement limitations
- Check your Ethics
- Size of the company and revenue
- Consider end goal
- Politics

Open Source Intelligence (OSINT)

- Open-source Intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources.
- OSINT under one name or another has been around for hundreds of years. With the advent of instant communications and rapid information transfer, a great deal of actionable and predictive intelligence can now be obtained from public, unclassified sources.
- In most cases it is legal to obtain information in this way. This means that despite the high potential for harm this critical information may be obtained at little or no risk to the third party.

Covert Gathering

Covert means not getting caught. In the reconnaissance phase this is gathering open source information about a target, or searching for a target anonymously.



guernsey

Foot-printing

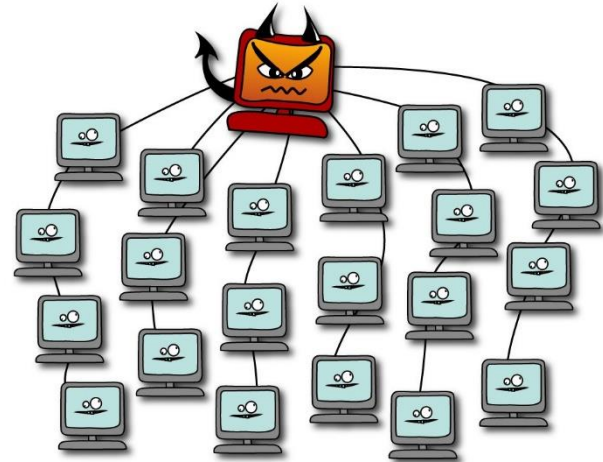
The process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment. This information can be open source or from direct inspection.



guernsey

Sources of OSINT?

Botnets



Nation State



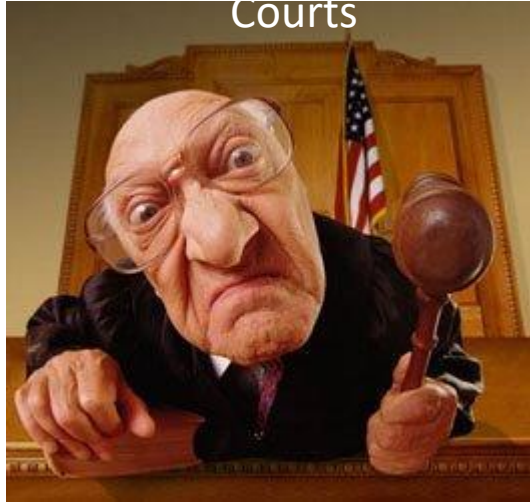
Companies



“researchers”



Courts



guernsey

Sources of OSINT

Government at all levels

- . FOIA
- . Building Permits
- . Patent offices
- . Court Records

Business Records

- . SEC Filings
- . Legal Activities
- . Press Releases
- . Job Postings

Paid services and Public records

- . Credit Reports
- . People searched
- . Real Estate Records
- . Military Records
- . Associations Directories



guernsey

Corporate - Logical

- Business Partners
- Business Clients
- Competitors
- Product line
- Marketing accounts
- Meetings
- Significant company dates
- Job openings
- Charity affiliations
- Court records
- Political donations
- Professional licenses or registries



monster®



guernsey

Corporate - Infrastructure Assets



- Network blocks owned
- Email addresses
- Eternal infrastructure profile
- Technologies used
- Purchase agreements
- Remote access
- Application usage
- Defense technologies
- Human capability



guernsey

Corporate - Financial

- Reporting
- Market analysis
- Trade capital
- Value history



Individual - History

- Court Records
- Political Donations
- Professional licenses or registries



guernsey

Individual - Social Network Profile

- Metadata Leakage
- Tone
- Frequency
- Location awareness
- Social Media Presence



Who Uses Threat Intel?



Criminals and hacktivists



Organized Crime



Why is OSINT Used by Bad Actors

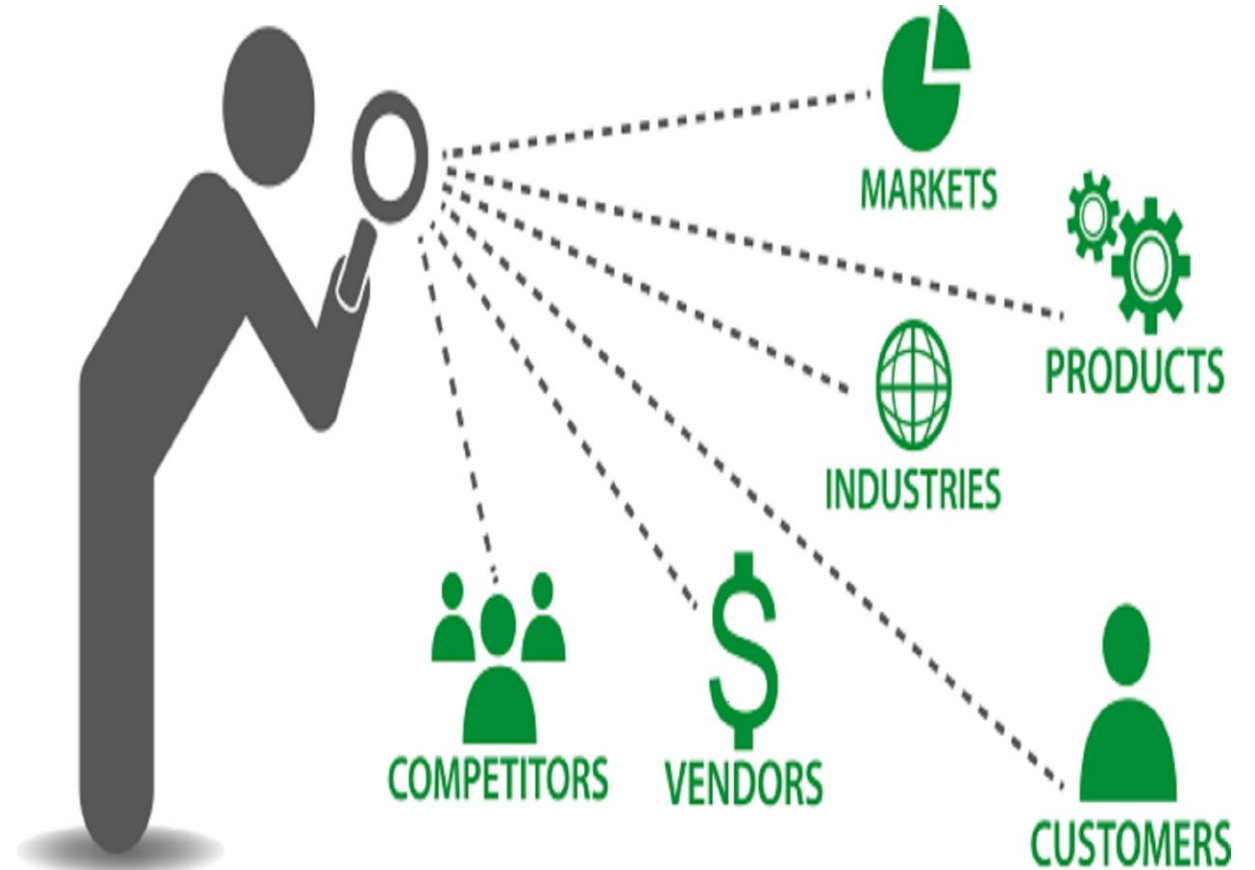
- Passive
- Easy to Automate
- Legal
- Low to no cost
- Low risk



guernsey

Why is OSINT Used by Companies

- Market Research
- Customer Information
- Sales Leads
- SWOT



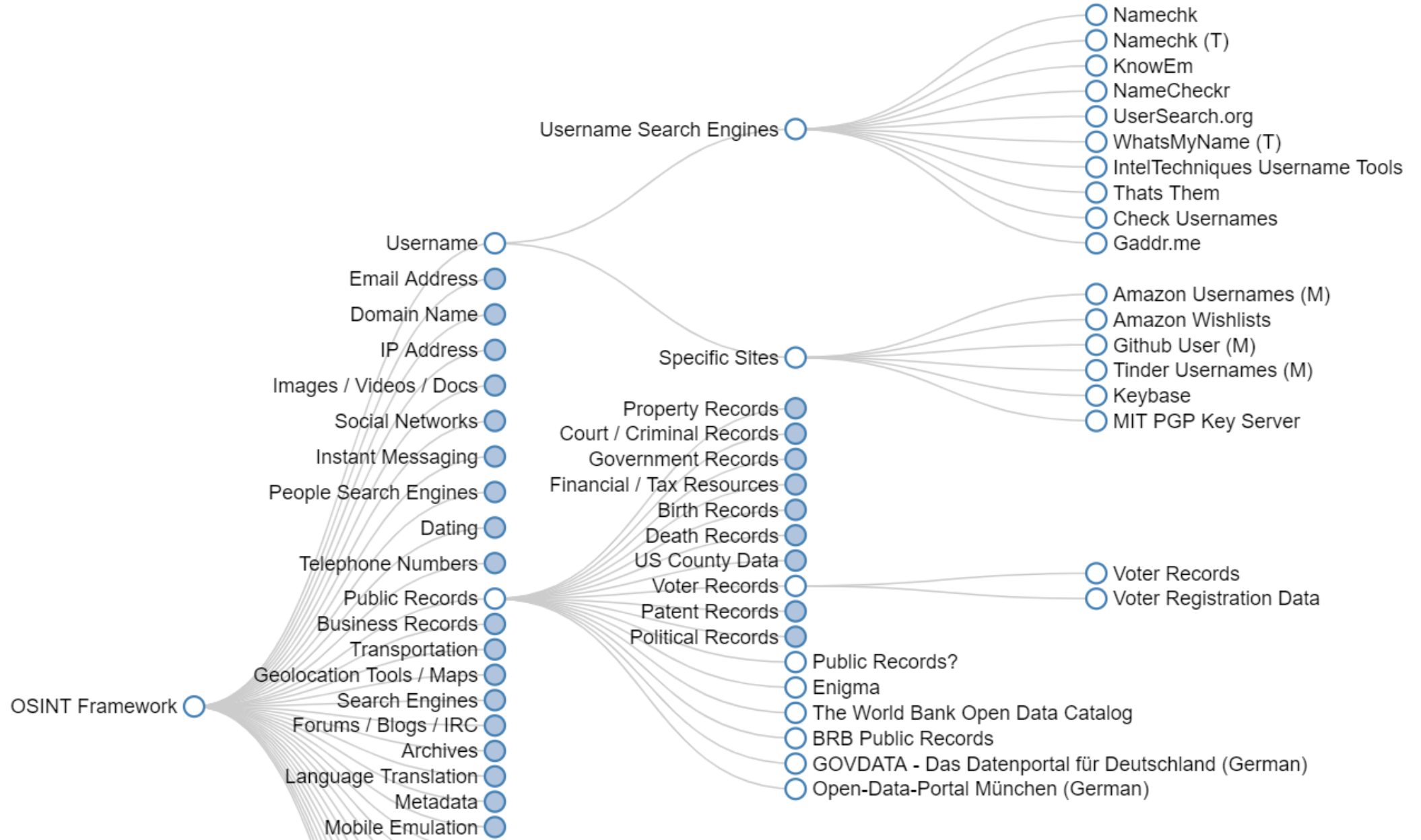
guernsey

Ways of Gathering and Compiling OSINT

Passive: Unlike using tools that can leave a signature such as nmap/openvas, the majority of OSINT scripts scrape 3rd party databases and search engines which often cannot be tracked and return great results.

Automated: Open source OSINT tools, scripts, and web applications; almost completely automate every aspect of OSINT and typically available for free. (this covers my next point low to no cost)

Tools for OSINT



OSINT Software

OSINT gathering can take up valuable time and resources if automation and the proper tools are not being leveraged in your environment. Thankfully the tools needed to perform OSINT gathering are lowcost to free and in most cases can completely automate the process after the initial configuration.



guernsey

Top 20 OSINT Tools According to securitytrails.com

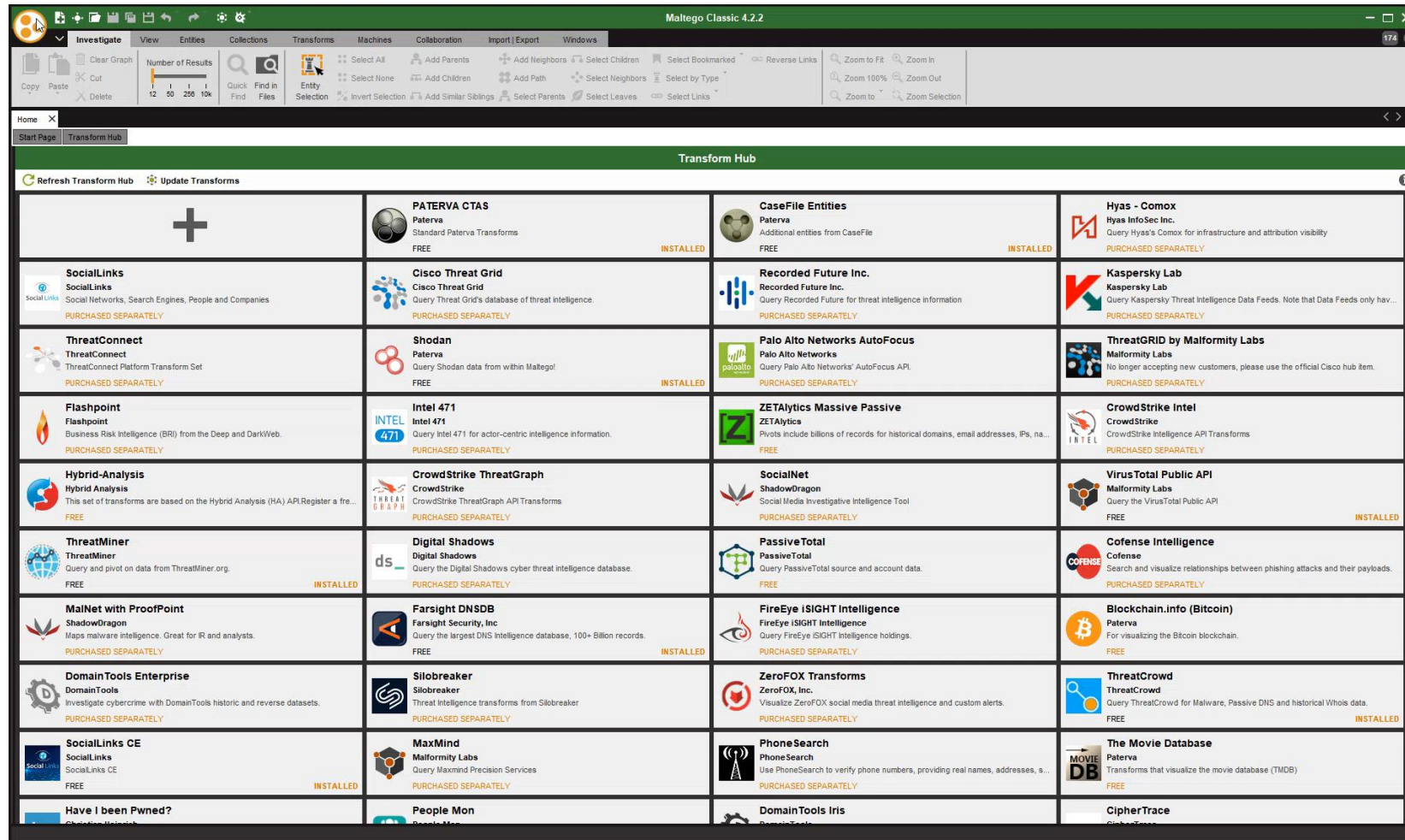
- | | | |
|--------------------|------------------|-----------------|
| 1. OSINT Framework | 10. theHarvester | 18. Fierce |
| 2. CheckUserNames | 11. Shodan | 19. Unicornscan |
| 3. HavelbeenPwned | 12. Jigsaw | 20. Foca |
| 4. BeenVerified | 13. SpiderFoot | |
| 5. Censys | 14. Creepy | |
| 6. BuiltWith | 15. Nmap | |
| 7. Google Dorks | 16. WebShag | |
| 8. Maltego | 17. OpenVAS | |
| 9. Recon-Ng | | |

OSINT Tools: Maltego

Maltego is proprietary software used for open-source intelligence and forensics, developed by Paterva. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.

Maltegos reports are great out of the box and can connect to a variety of 3rd party sources both free and paid. It allows your organization to fine tune your OSINT solution to fit your needs.

OSINT Tools: Maltego



OSINT Tools: SpiderFoot

SpiderFoot is a free OSINT automation tool. Its goal is to automate the process of gathering intelligence about a given target, which may be an IP address, domain name, hostname, network subnet, ASN or person's name. SpiderFoot is considered to be

**“The Most Complete OSINT Collection And Reconnaissance Tool”
– KitPloit.com**

OSINT Tools: SpiderFoot

The benefits of SpiderFoot are:

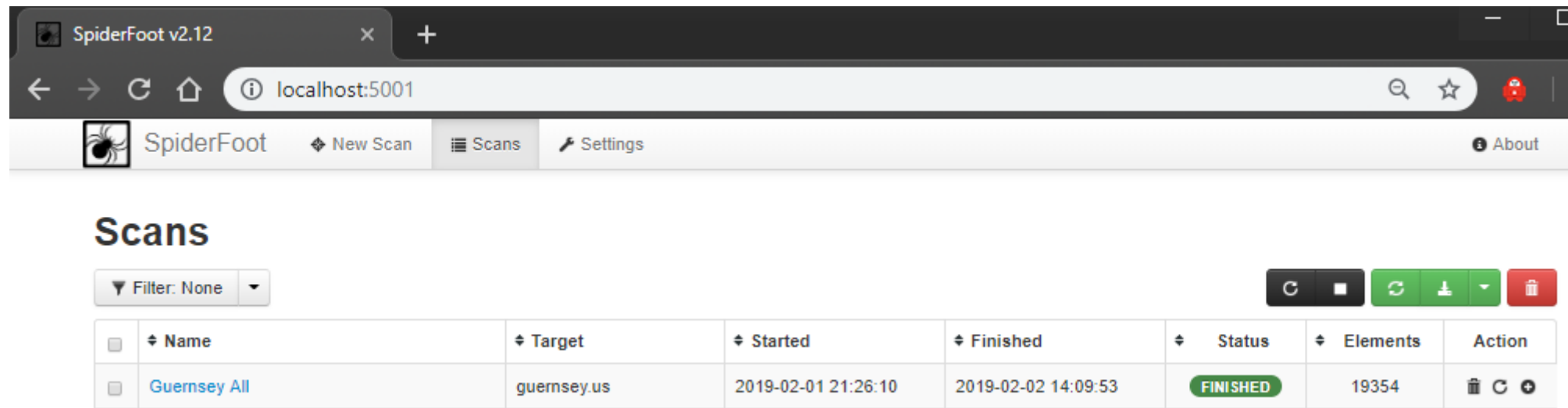
- Easy to configure and deploy
- Over 100 data sources
- Web based interface or CLI for further automation
- Free






guernsey

OSINT Tools: SpiderFoot


- Web based user interface



The screenshot displays the SpiderFoot v2.12 web interface in a browser window. The address bar shows 'localhost:5001'. The interface includes a navigation bar with 'New Scan', 'Scans', and 'Settings' tabs. Below the navigation bar, the 'Scans' section is active, showing a table of scan results. A filter dropdown is set to 'Filter: None'. The table contains one entry: 'Guernsey All', which has a target of 'guernsey.us', started on '2019-02-01 21:26:10', finished on '2019-02-02 14:09:53', and a status of 'FINISHED'. The table also shows '19354' elements and an 'Action' column with icons for deleting, refreshing, and adding.

Name	Target	Started	Finished	Status	Elements	Action
Guernsey All	guernsey.us	2019-02-01 21:26:10	2019-02-02 14:09:53	FINISHED	19354	  

OSINT Tools: SpiderFoot

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

New Scan

Scan Name

Seed Target

[By Use Case](#) [By Required Data](#) [By Module](#)

☒ All **Get anything and everything about the target.**

All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

☐ Footprint **Understand what information this target exposes to the Internet.**

Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

☐ Investigate **Best for when you suspect the target to be malicious but need more information.**

Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

☐ Passive **When you don't want the target to even suspect they are being investigated.**

As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

[Run Scan](#)

Note: Scan will be started immediately.

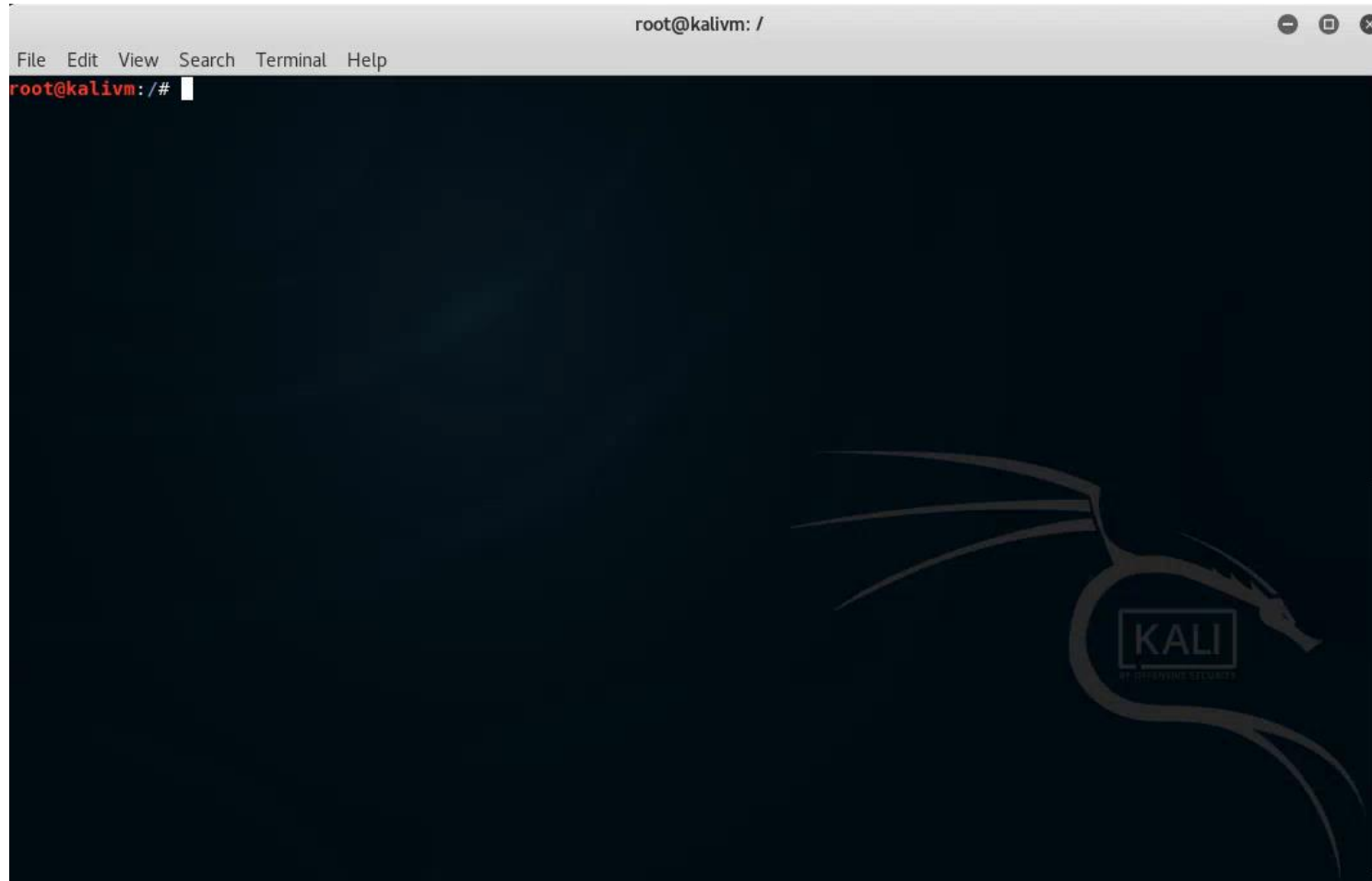
OSINT Tools: Haveibeenpwned.com

Domain search allows you to find all email addresses on a particular domain that have been caught up in any of the data breaches currently in the system. You can also receive notifications if they appear in future breaches by providing a notification email. You will receive a summary email regarding impacted accounts if anything on your organization's domain(s) shows up again in the future.

OSINT Tools: theHarvester

- theHarvester is a tool for gathering subdomain names, e-mail addresses, virtual hosts, open ports/ banners, and employee names from different public sources (search engines, pgp key servers).
- theHarvester is a really simple tool, but very effective for the early stages of a penetration test or just to know the visibility of your company in the Internet.
- theHarvester is now shipping with kali Linux by default which means bad actors and pen testers will be using this utility.

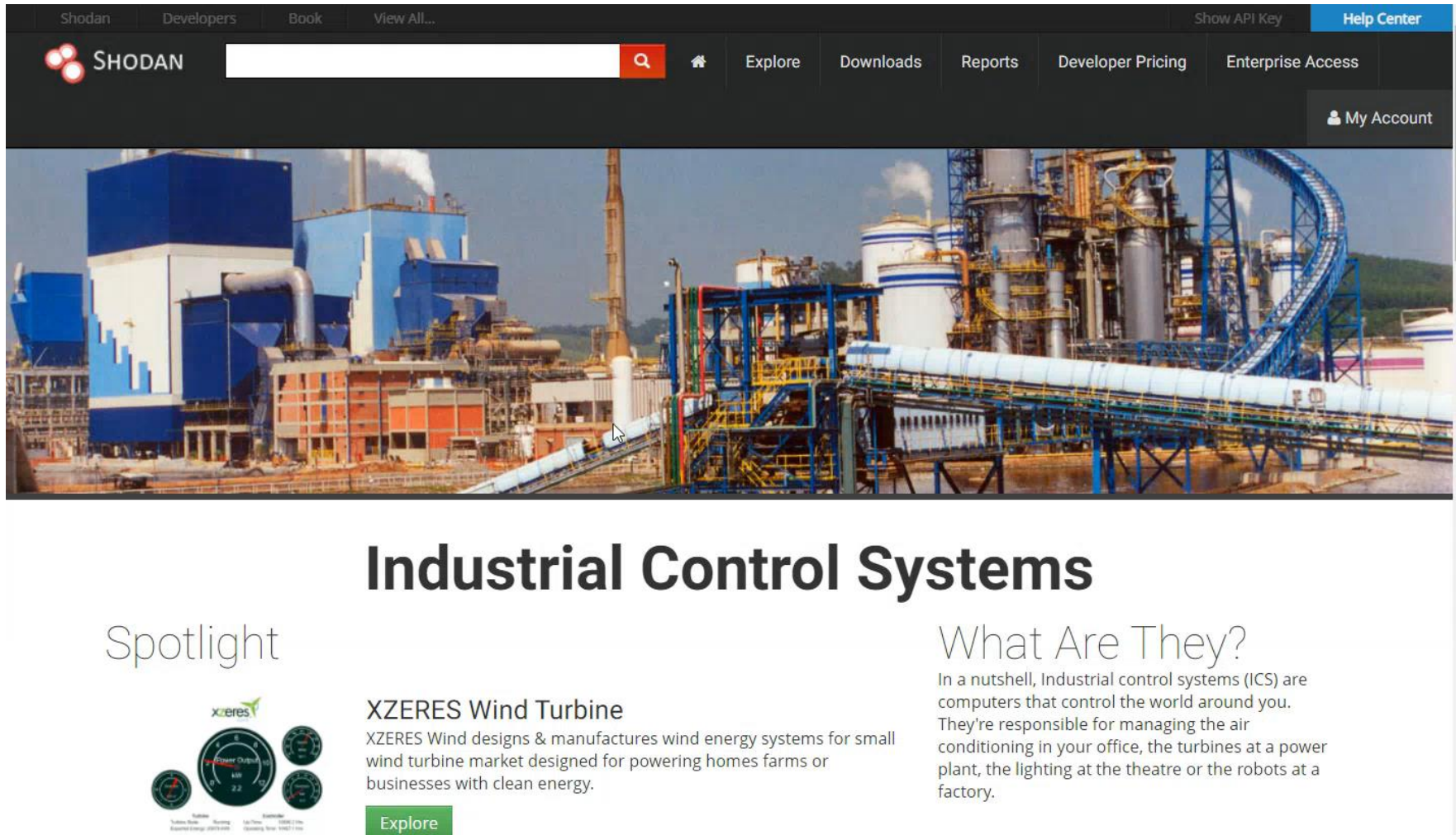
OSINT Tools: TheHarvester



OSINT Tools: Websites

- [Osintframework.com](https://osintframework.com) - OSINT website directory.
- [Shodan.io](https://shodan.io) - Search engine that lets the user find specific types of computers connected to the internet using a variety of filters.
- [Haveibeenpwned.com](https://haveibeenpwned.com) - Check if you have an account that has been compromised in a data breach.
- [DNSdumpster.com](https://dnsdumpster.com) - domain research tool that can discover hosts related to a domain.
- [VPNhunter.com](https://vpnhunter.com) - VPN Hunter discovers and classifies the VPNs and remote access services of any organization.

OSINT Tools: Shodan.io



Shodan Developers Book View All... Show API Key Help Center

SHODAN

Explore Downloads Reports Developer Pricing Enterprise Access My Account

Industrial Control Systems

Spotlight

XZERES Wind Turbine

XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

Explore

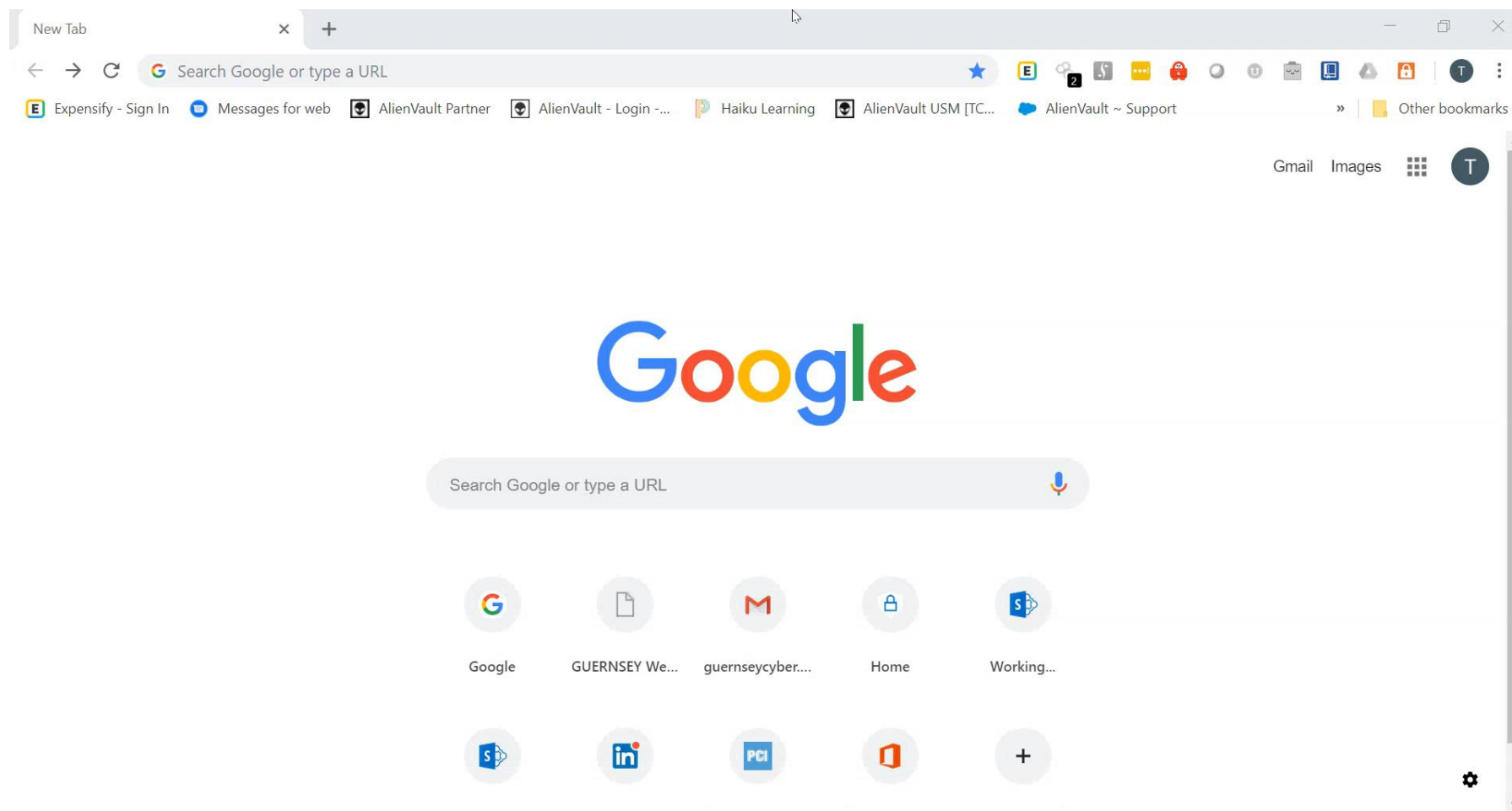
What Are They?

In a nutshell, Industrial control systems (ICS) are computers that control the world around you. They're responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.



guernsey

Default passwords are not a Secret



OSINT Tools: Google Dorks

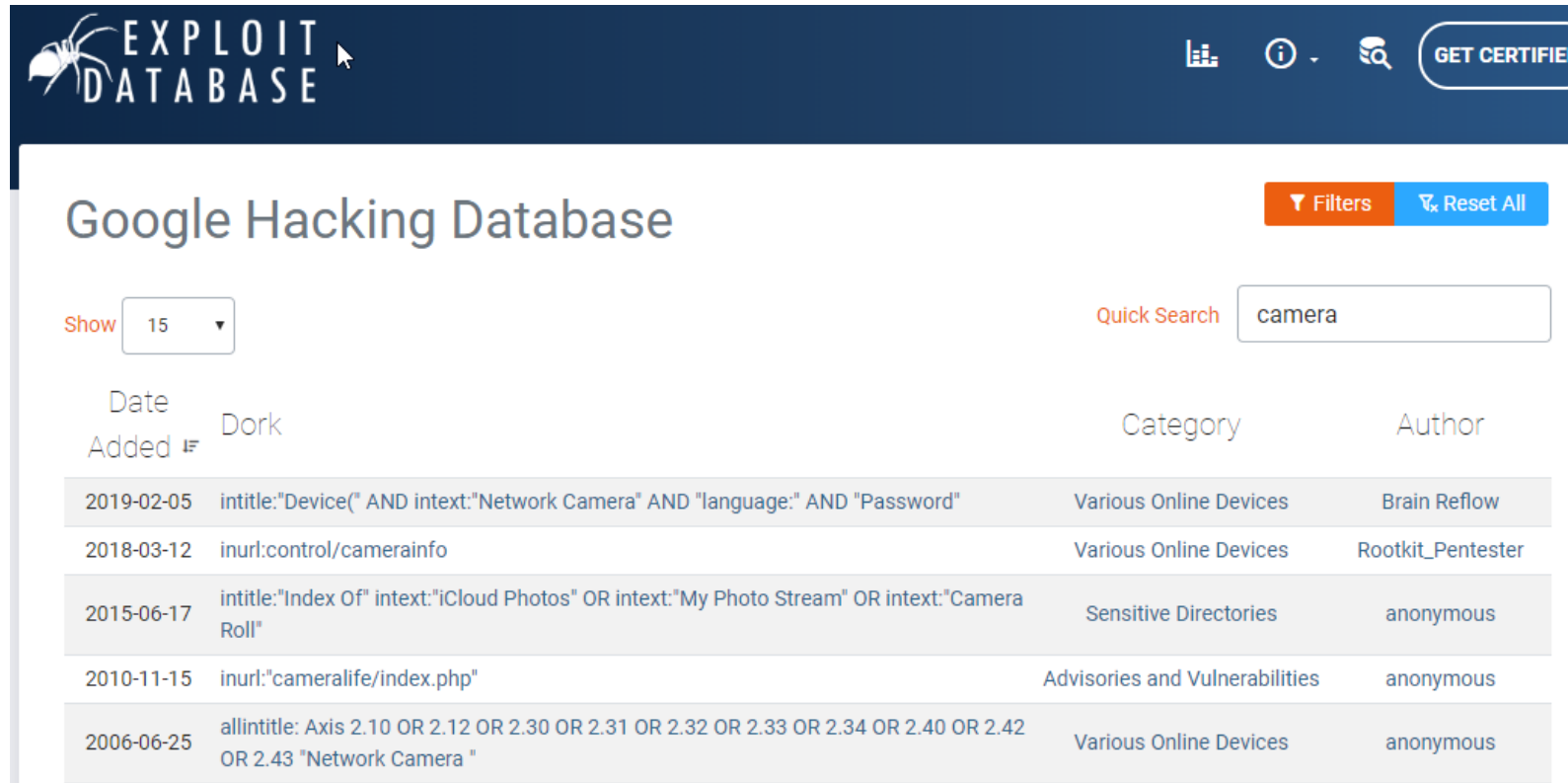
A Google dork is a search string that uses Google's custom search operators to filter down search results. When used creatively, these filters can return information that wasn't meant to be found. Exploiting Google dorks is known as Google dorking or Googlehacking.



guernsey

OSINT Tools: Google Dorks

exploit-db.com has an entire section of its database dedicated to user submitted Google Dorks



EXPLOIT DATABASE

GET CERTIFIED

Google Hacking Database

Filters Reset All

Show 15

Quick Search camera

Date Added	Dork	Category	Author
2019-02-05	intitle:"Device(" AND intext:"Network Camera" AND "language:" AND "Password"	Various Online Devices	Brain Reflow
2018-03-12	inurl:control/camerainfo	Various Online Devices	Rootkit_Pentester
2015-06-17	intitle:"Index Of" intext:"iCloud Photos" OR intext:"My Photo Stream" OR intext:"Camera Roll"	Sensitive Directories	anonymous
2010-11-15	inurl:"cameralife/index.php"	Advisories and Vulnerabilities	anonymous
2006-06-25	allintitle: Axis 2.10 OR 2.12 OR 2.30 OR 2.31 OR 2.32 OR 2.33 OR 2.34 OR 2.40 OR 2.42 OR 2.43 "Network Camera "	Various Online Devices	anonymous

OSINT Tools: Google Dorks

[About](#) [Store](#)

[Gmail](#) [Images](#)



[Sign in](#)



Google Search

I'm Feeling Lucky

[Advertising](#) [Business](#)

[Privacy](#) [Terms](#) [Settings](#)



guernsey

OSINT Tools: Internet Archives

- There are times when we will be unable to access web site information due to the fact that the content may no longer be available from the original source.
- Being able to access archived copies of this information allows access to past information.
- Perform Google searches using specially targeted search strings: `cache:<site.com>`
- Use the archived information from the Wayback Machine (<http://www.archive.org>).

OSINT Tools: Internet Archives

Internet Archive Wayback Machine

http://guernsey.us/about/our-team

Go

SEP OCT NOV

2015 22 2016 2017

1 capture

22 Oct 2016

About this capture

guernsey

CONTACT US

LEADERSHIP

Suhas Patwardhan, PE, Sr. VP
CEO/PRESIDENT
CHAIRMAN OF THE BOARD

Carl Stover, PE, Sr. VP
CHAIRMAN OF THE BOARD (EMERITUS)
SENIOR VICE PRESIDENT

Jared Stigge, JD, EVP
EXECUTIVE VICE PRESIDENT
SECRETARY OF THE BOARD

OSINT Tools: Internet Archives



guernsey

CONTACT US

Our Team

Sure, we've earned a reputation for quality over the past 90 years. No one sticks around as long as we have without that. But like they say, it's not what you know, it's who you know. Our clients may walk in the door because of our knowledge, but they keep coming back because of our people.

Whether they've been on the team for four months or 40 years, the people walking Guernsey's halls are serious about their work – and seriously interested in building a partnership with the clients they serve.

LEADERSHIP



Jared Stigge, JD
CEO/PRESIDENT



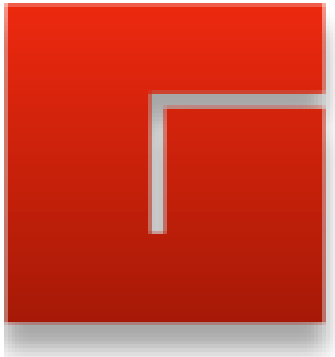
David Hedrick, COB
CHAIRMAN OF THE BOARD
DIRECTOR, ANALYTICAL SOLUTIONS



Jason Cobb, PE, Sr. VP
SENIOR VICE PRESIDENT
DIRECTOR, ARCHITECTURE &
ENGINEERING



guernsey



guernsey

5555 North Grand Boulevard
Oklahoma City, OK 73112-5507

T: 405.416.8182

M: 918.808.0558

timothy.fawcett@guernsey.us

robert.martinez@guernsey.us

guernsey.us