# OSINT DOCUMENTATION

Robert A. Kalka Metropolitan Skyport – CPTC 2023

* Information gathering is the first step of any penetration test and involves fathering or collecting information about an individual, company, website, or system that you are targeting.
* The more information you have on your target, the more successful you will be during the latter stages of a penetration test.
* Information gathering is typically broken down into two parts:
  + Active info gathering – Interact directly with host, need authorization in a pen test.
  + Passive info gathering – Publicly accessible info.

Pertinent Information we are potentially looking for:

+ IP addresses

Shodan on 167.71.252.198: <https://www.shodan.io/host/167.71.252.198>

* Name Servers
  + 104.197.15.255 possible host address of mysql database; seen in set.sh
  + Openflights.org
  + 104.154.196.92
  + https://blog.openflights.org/$1;
  + [ns1.digitalocean.com](https://who.is/nameserver/ns1.digitalocean.com)
  + [173.245.58.51](https://who.is/whois-ip/ip-address/173.245.58.51)
  + [ns2.digitalocean.com](https://who.is/nameserver/ns2.digitalocean.com)
  + [173.245.59.41](https://who.is/whois-ip/ip-address/173.245.59.41)
  + [ns3.digitalocean.com](https://who.is/nameserver/ns3.digitalocean.com)
  + [198.41.222.173](https://who.is/whois-ip/ip-address/198.41.222.173)
  + <https://isreedyinthe.uk/>
    - Ras Pi server: http://rproxy46-hex-b.mythic-beasts.com/

+ Directories hidden from search engines  
+ Names

* Robert Kalka
  + Principle
  + Sculptor part time (so cool, very well rounded)
    - <https://www.robertkalka.com/>
    - Homie's woodworking site, personal info on here
      * Might be asked to check it out day of comp, gotta make sure to tell them it is out of scope
  + https://www.instagram.com/robertkalkacustomwoodworking/
* Andrea Wilson
  + IT Technician
  + Fired from previous position, just hired at RAKMS
  + Obtained IT Support Professional cert from [Coursera](https://www.linkedin.com/company/coursera/)!
  + Skills: iPad, Cat 5e, Printers, Excel, Calculator
  + Recently let go 🙁
    - #grindmode
  + Loves minions???
  + Spent almost 6 years on a career break (how did she explain that in an interview?) (“I signed an NDA”) (Damn you right)
  + Insta: a.wilson5443 (potential password... 5443)
    - Dog named erply meaning **enterprise software company** which provides **cloud-based** point of sale and inventory management technology
* Jessie Sharpes
  + IT Support Specialist
* Brandon Whittleton
  + Director of Public Relations
  + Rochester, New York
* Bella Sanchez
  + IT Support Specialist/Help Desk Technician
* Wendel Pruessen
  + Public Relations manager
* Remy Mercer
  + Community Outreach Coordinator
  + Wants to #savethepolarbears
* Samuel Reed
  + Github account
  + X: @tehreedy
* James Meyers
  + Systems administrator
  + Rochester, New York

+ Email addresses

[robertkalka@gmail.com](mailto:robertkalka@gmail.com) : Robert Kalka

+ Phone Numbers

(718) 486-8517 : Robert Kalka  
+ Physical Addresses

- Springfield, IL (airport location)  
+ Web technologies being used

* Digitalocean.com
* NAMECHEAP
* Shopify

+ Social media accounts

+ Public-facing Users

+ Public-facing Websites

* <https://liturgy.link/>
* <https://451c80.myshopify.com/password>
* <http://www.rakms.flights/>
  + Created with sedo domain parking?
* <https://kkms.us/>
* <https://rakms.net/>
  + nginx/1.18.0 (Ubuntu)

+ Proficient technologies

* Windows
* Printer support

+Potential Technologies

* Salesforce
* Google cloud
* MySQL
* Shopify

+ Public Repositories

+ Leaked Databases

* Both related to elite-levels.sql which generates table of elite users
* <https://github.com/jpatokal/openflights/commit/a957bf003c920115ac8a4205f3eb8a745a021982>
  + <https://github.com/jpatokal/openflights/commit/7a3ea0e1ea36a10c4b29ad3d8c2423cc9cdfa774>
* <https://github.com/jpatokal/openflights/commit/f1963a54daf90ab7a354dce3a9c7a7ca80f617ef>
  + Names a table and its columns
* <https://github.com/jpatokal/openflights/commit/3f9f5739aee47308f771645a494816d567f8e7ba>

+ Earlier Versions of Websites

* Does not exist in archive.org
* Reminder that we must NOT actively interact with any online utilities.
  + This is ALL passive reconnaissance.
  + We are trying to leave no trail on our OSINT research.

Serverside scripts/information

<https://github.com/jpatokal/openflights/blob/master/test/server/login.php>

+ The user password as `base64(md5(challenge + md5(password + lowercase(name))))`

+ **LAMP** (**L**inux, **A**pache, **M**ySQL, **P**HP/**P**erl/**P**ython)

+ Database information

* ../sql/db.pw -> database password(s) ? (from expire.sh)
* SELECT uid, name, email, editor, elite, units, locale
* FROM users
* Users table with attributes email, validity, elite (link to elite-level ?)
  + echo "SELECT email FROM users WHERE validity IS NOT null AND validity < NOW() AND elite != 'X' AND elite != '' AND email != '' ORDER BY validity DESC;" | $MYSQL
* Set.sh script
  + <https://github.com/jpatokal/openflights/blob/master/elite/set.sh>
* Expire.sh script
  + <https://github.com/jpatokal/openflights/blob/master/elite/expire.sh>

+CPTC Link info

* TSA
  + Develop network segmentation policies and controls to ensure that operational technology systems can continue to safely operate in the event that an information technology system has been compromised, and vice versa;
  + Create access control measures to secure and prevent unauthorized access to critical cyber systems;
  + Implement continuous monitoring and detection policies and procedures to defend against, detect, and respond to cybersecurity threats and anomalies that affect critical cyber system operations; and
  + Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers and firmware on critical cyber systems in a timely manner using a risk-based methodology.
* <https://www.securityweek.com/new-tsa-directive-aims-further-enhance-railway-cybersecurity/>
* <https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/>
* <https://www.reuters.com/world/us/united-airlines-issues-nationwide-ground-stop-due-computer-issue-abc-news-2023-09-05/>
* <https://www.reuters.com/technology/us-faa-some-aviation-computer-system-users-experiencing-slower-response-times-2023-01-25/>