OSINT Workshop (Hands on!)
SANS Security Awareness Summit 2019
The Internet has changed over the years

World Wide Web

The World Wide Web (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists, Policy, November’s W3 news, Frequently Asked Questions.

What’s out there?

Pointers to the world’s online information, subjects, W3 servers, etc.

Help

on the browser you are using

Software Products

A list of W3 project components and their current state. (e.g. Line Mode, X11 Viola, NeXTStep, Servers, Tools, Mail robot, Library)

Technical

Details of protocols, formats, program internals etc.

Bibliography

Paper documentation on W3 and references.

People

A list of some people involved in the project.

History

A summary of the history of the project.

How can I help?

If you would like to support the web.

Getting code

Getting the code by anonymous FTP, etc.

http://info.cern.ch/hypertext/WWW/TheProject.html

https://www.google.com/maps/search/Restaurants/@32.759902,-117.2864638,11.83z
People share so much data

**Where they are**


**Who they are with**

People share so much data

Their likes


Their hobbies

https://www.pexels.com/photo/action-active-activity-adult-415188/
The US government shares data

https://www.fec.gov/data/receipts/individual-contributions/?two_year_transaction_period=2020&min_amount=2000

<table>
<thead>
<tr>
<th>Contributor name</th>
<th>Recipient</th>
<th>State</th>
<th>Employer</th>
<th>Receipt date</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green, C J</td>
<td>FRIENDS TO ELECT DR. GREG MURPHY TO CONGRESS</td>
<td>TN</td>
<td>HOMEMAKER</td>
<td>07/10/2019</td>
<td>$2,800.00</td>
</tr>
<tr>
<td>Green, C J</td>
<td>FRIENDS TO ELECT DR. GREG MURPHY TO CONGRESS</td>
<td>TN</td>
<td></td>
<td>07/10/2019</td>
<td>$2,800.00</td>
</tr>
<tr>
<td>Renu EPAK D</td>
<td>PRAMILA FOR CONGRESS</td>
<td>NJ</td>
<td></td>
<td>06/30/2019</td>
<td>$2,800.00</td>
</tr>
</tbody>
</table>
Our religious and community groups share

https://issuu.com/servantchurch/docs/newsletter_070319_all_web?fr=xKA9_7U1NQ
Groups conduct campaigns to influence us at scale

https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=US&impression_search_field=has_impressions_lifetime&q=gun%20control
Computers create and alter pics, videos, and audio

Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news

By Janus Vincent | Apr 17, 2018, 1:14pm EDT


https://thispersondoesnotexist.com/
People used to have to "dumpster dive" to get info
Now our sensitive data is mostly online
And available for "others" to retrieve

https://www.pexels.com/photo/two-alien-inside-car-wallpaper-365625/
Who am I?

• **SANS Author** of SEC487 (OSINT class)

• **OSINT Consultant** (Spotlight Infosec LLC)

• **OSINTCurio.us** Founder

• **Cyber security** for 15+ years

• **Psychology** degree

• Social media @**WebBreacher**
What would you call...

• Searching for a coffee shop on Bing Maps?
• Looking for a new job on monster.com?
• Researching a business you want to invest in?
• Finding that long lost friend?
• Examining an old photo to see where it was taken?
We call it

OSINT - Open Source Intelligence

Searching and examining available/open data and applying it to answer questions
Who uses OSINT?

• **Law enforcement**
  • Awareness
  • Catching suspects

• **Intelligence community**
  • Awareness
  • Recruitment
  • Analysis of assets

• **Parents**

• **Businesses**
  • Recruiting/sourcing
  • Understanding risk
  • Business intelligence

• **Criminals**
  • Preparation for action
  • Bragging about exploits

• **People dating**
  • Who is this other person?
Why should you care about OSINT?

• People are **sharing** things about us online
• People are **collecting** those things and potentially using them
• Understanding **risk** to yourself, your family, and your organization

How do professionals "OSINT"?

• Gather OS data
• Refine it into OS information
• Add "what does this mean?" and make it OSINT

The OSINT Cycle

• Professionals have distinct stages they move through in OSINT work

• Starting with gathering requirements from stakeholders and moving clockwise around the cycle
Let's do some OSINT!

• This is a hands-on workshop
• I will show an OSINT skill and how we use it
• Then you will get time to try it on your computer

Potential networking issues

• Please tether your laptop or use a VPN
• This way our network traffic comes from different IPs
Module 1: Bookmarks and Links
Beginning with URLs

• We will begin with websites that have excellent OSINT resources

• These sites list URLs to tools or other sites you can use for OSINT

• https://osintframework.com
• http://osintframework.de
• https://intelx.io/tools
• https://yoga.osint.ninja
OSINT Framework - osintframework.com
Welcome to the OSINT Open Source Intelligence Framework landing page. This free resource is dedicated to search and used for training purposes. It seeks no financial gain. All information herein can be found in open sources and is for educational purposes only. Please comply with any terms of service should those apply. I would encourage you to make an own framework that reflects your workflow and assignments. Start.me hosts and provides this free bookmarking service and because its free it runs marketing analytics on its site. MindMup provides the online Mindmapping functionality and does not track users. Use responsibly. You are welcome to reach out or follow me on twitter: @digintelsosint

Discover other OSINT Frameworks
Username Lookup

Select from the checkbox list and enter a Username to search

- namevine
- peekyou
- usersearch
- knowem
- Twitter
- Facebook
- YouTube
- Tumblr
- Instagram
- SnapChat
- Profilr
- Gravatar
- Dehashed
- Tinder
- GitHub

Important: Make sure that popups are allowed. If you don’t see all new tabs opened after hitting search, go back to this tab and enable popups when your browser asks (Chrome: Right side in the URL bar).
Your OSINT Graphical Analyzer (YOGA)

Usage:

- Click and drag nodes (dots) around the page to view all content.
- Use the arrow keys to move around and Page Down/Up to zoom out and in.
- If an edge connecting 2 nodes has an O in the middle, mouse over it for descriptions of the actions.

Created by Micah
Exercise 1: Frameworks

• Open a web browser
• Visit the following sites
  • osintframework.com
  • osintframework.de
  • intel.io/tools
  • yoga.osint.ninja
• Explore the data available on each

5 Minutes
Module 2: Search Engines
Much of our work is done in search engines

• Use multiple search engines for different perspectives
  • DuckDuckGo.com
  • Bing.com
  • Yandex.com
  • Google.com

• Narrow results using search operators or directives

• Most search engines have "Advanced Search Forms"

• Operators sometimes work in multiple engines
<table>
<thead>
<tr>
<th>Operator</th>
<th>Function</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot; &quot; (Quotes)</td>
<td>Group terms together. Terms must appear in results as they do in the quotes.</td>
<td>&quot;SANS Security Awareness&quot;</td>
</tr>
<tr>
<td>- (Dash)</td>
<td>Negate term or directive. Do not show results with this content.</td>
<td>-WebBreacher</td>
</tr>
<tr>
<td>site:</td>
<td>The results must be indexed from the domain/URL specified.</td>
<td>site:sans.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td>site:www.sans.org/event</td>
</tr>
<tr>
<td>filetype:</td>
<td>The filetype or file extension of the results.</td>
<td>filetype:pdf</td>
</tr>
<tr>
<td>OR</td>
<td>One term or another</td>
<td>micah OR webbreacher</td>
</tr>
</tbody>
</table>
### Examples

<table>
<thead>
<tr>
<th>Operators</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;micah hoffman&quot; OR &quot;webbreacher&quot;</td>
<td>Results must have either the words micah hoffman in it or the word webbreacher</td>
</tr>
<tr>
<td>&quot;micah hoffman&quot; -site:sans.org</td>
<td>Results must have micah hoffman in them and NOT be from the sans.org domain</td>
</tr>
<tr>
<td>site:.gov filetype:xlsx</td>
<td>Results must be from a *.gov domain and be an Excel XLSX document</td>
</tr>
<tr>
<td>newsletter church OR temple OR mosque -sample -example -template -site:.com</td>
<td>Results must have the word newsletter in it and either church, temple, or mosque and none of the words sample, example, template and not be from a .com domain</td>
</tr>
</tbody>
</table>
Examples for people searching

• Results for people may have names in a variety of formats
• Ensure your search operators reflect these variations

"micah hoffman" OR
"hoffman, micah" OR
"micah_hoffman" OR
"micah-hoffman" OR
"hoffman micah"
Exercise 2: Search for Yourself

• Open a web browser
• Visit the following sites:
  • google.com
  • duckduckgo.com
  • bing.com
• Search for yourself
• Analyze results
Module 3: OSINTing User Names
User Names for OSINT

• We put **meaning** in our user names
  • Favorite topics
  • Dates
• They can be extracted from or used in **email addresses**
• We may use the same user name **across sites**

Example user names:
• BiggestRedSoxFan
• BiggestRedSoxFan1
• RobertLangdon1980
• fuzzybunny123
• DreadPirateRoberts
User name reuse is common

• People use the same user name on multiple websites
  • Facebook: fuzzybunny123
  • Instagram: fuzzybunny123
  • Twitter: fuzzybunny123

• Can we find all the web sites with the name and tie them to a single person?
User name checking sites

• There are web sites that allow you to check if a user name exists on a certain web site
  • The purpose is for you to find places where your name is NOT used
  • Then you can create your account and content on that site

• We use it in reverse and look for places where you CANNOT create an account

• Those are sites where the target name was found
Positive Results

https://namechk.com/
<table>
<thead>
<tr>
<th>Instagram.com/webbreacher/exists</th>
<th>Disqus.com/by/webbreacher/exists</th>
<th>Pinterest.com/webbreacher/Available</th>
<th>Codepen.io/webbreacher/unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jsfiddle.net/user/webbreacher...Available</td>
<td>Mobile.twitter.com/webbreacher...exists</td>
<td>Postebin.com/u/webbreacher unknown</td>
<td>Reddit.com/user/webbreacher unknown</td>
</tr>
<tr>
<td>Youtube.com/user/webbreacher...Available</td>
<td>Webbreacher.im/...com/Available</td>
<td>Ask.fm/webbreacher Available</td>
<td>Medium.com/@webbreacher Available</td>
</tr>
<tr>
<td>M.twitch.tv/webbreacher/pr...exists</td>
<td>Fiverr.com/webbreacher unknown</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Analysis is key

• Running a tool gives you **data**
• Examining it to see if it is relevant and accurate turn that into **information**
• Once we gather all the username on sites, we have to **visit them**
• Are they you?
Exercise 3: Search for Your User Name

• Open a web browser
• Visit the following sites:
  • namechk.com
  • checkuser.org
• Search for your user names
• Analyze the results

15 Minutes
Faster, reliable results

• Using tools we can perform these searches across **180+ sites** in < 30 seconds

• We can search for **multiple** user names

• Free video "10 Minute Tip: Finding Usernames Fast!" on [https://osintcurio.us](https://osintcurio.us) [https://youtu.be/Bbrve9OppnM](https://youtu.be/Bbrve9OppnM)
Recon-NG Demo of the Profiler Module
Module 4: Using Breach Data
What is breach data?

• Data stolen from systems
• Usually includes usernames, passwords, and possibly emails
• Can include much more

https://intelx.io/?s=barack@whitehouse.gov
Breach Data for OSINT

1. Check for **valid email** addresses

2. Find **same username/email** used on multiple sites (Username Reuse)

3. Find **same password** across sites (Password Reuse)

https://dehashed.com/search?query=%22john@example.com%22
How do we access it?

• Free sites
  • havebeenpwned.com
  • spycloud.com
  • "Dark web"

• Download and normalize the data ourselves

• Pay for access
  • dehashed.com
  • weleakinfo.com
Is it ethical to use?

• Data stolen from systems
• Attackers use it all the time
• What is our ethical responsibility to the victims (website stolen from and its users)?
Exercise 4: Search for Yourself on Breach Data Site

• Open a web browser
• Visit the following sites:
  • haveibeenpwned.com
• Search for your user names
• Analyze the results

10 Minutes
Demo of Dehashed.com
Wrapping It Up
This is a portion of what we do

• Professional OSINT cases can take **weeks or months**

• We used only **free** sources

• What if you had **funding** and much more time?

• **bellingcat.com** does

OSINT Workshop Outcomes - Exercise 2

• You searched for yourself on multiple search engines
• Find anything "interesting"?
• Find anything you wish you hadn't?

• Action - Try to remove your data from the Internet

• Resources:
  • [https://inteltechniques.com/data/workbook.pdf](https://inteltechniques.com/data/workbook.pdf)
  • [https://the.osint.ninja/optoutdoc](https://the.osint.ninja/optoutdoc)
  • Search engines
OSINT Workshop Outcomes - Exercise 3

• You searched for your user names
• Find anything "interesting"?
• Find anything you wish you hadn't?

• Action - Segment your personal and work lives
• Use different user names for each type of account
  • Personal: fuzzybunny123
  • Work: micahhoffman
• Use different profile images/avatars on the different types of accounts
OSINT Workshop Outcomes - Exercise 4

• You searched for yourself on haveibeenpwned.com

• Did you find your email address was in a breach?

• Action 1 - Set up monitoring
  • Use the "Notify Me" link to receive alerts in the future

• Action 2 - Change breached account passwords
  • Any account found in the breach should have password changed
  • Reused breached email and password? Change those too

';--have i been pwned?
Check if you have an account that has been compromised in a data breach
https://haveibeenpwned.com/
Want more OSINT?

The OSINTCurious Project

https://osintcurio.us

- Blog posts
- 10 minute OSINT videos
- Bi-weekly webcast/podcast
- Free!!!
Want even MORE OSINT?

SANS SEC487: Open Source Intelligence Gathering and Analysis

- 6 days of OSINT
- Over 23 labs

https://sans.org/sec487

<table>
<thead>
<tr>
<th>Title</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis</td>
<td>SANS Network Security 2019&lt;br&gt;Las Vegas, NV&lt;br&gt;Micah Hoffman</td>
</tr>
<tr>
<td>SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis</td>
<td>SANS Paris September 2019&lt;br&gt;Paris, France&lt;br&gt;David Mashburn</td>
</tr>
<tr>
<td>SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis</td>
<td>SANS Dallas Fall 2019&lt;br&gt;Dallas, TX&lt;br&gt;Michael Murr</td>
</tr>
<tr>
<td>SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis</td>
<td>SANS Baltimore Fall 2019&lt;br&gt;Baltimore, MD&lt;br&gt;Micah Hoffman</td>
</tr>
</tbody>
</table>

Sep 9, 2019 - Sep 14, 2019
Sep 16, 2019 - Sep 21, 2019
Sep 23, 2019 - Sep 28, 2019
Oct 7, 2019 - Oct 12, 2019
Questions?

Micah Hoffman
@WebBreacher (Twitter)
imiah@spotlight-infosec.com

https://webbreacher.com