Roy Wattanasin
Offensive & Defensive OpenSource Intelligence (OSINT)

ISSA NE 2018 Meeting
11/07/2018
Disclaimer

• You do not hold the presenter liable and accept full responsibility for your actions

• The presentation does not endorse or approve and assumes no responsibility for the content, accuracy or completeness of the information presented

• This presentation does not represent the opinions of any of the organizations that I am currently working for or have worked for

• You will use any tools mentioned in an ethical, professional and legal manner
whoami

- Healthcare information security professional
- Former adjunct faculty at Brandeis University
- Conference(s) organizer, creator, etc. – Former lead of @BSidesBoston, co-organizer of @basconf & @owaspboston co-host
- IoT, healthcare medical device security, application security & DFIR
- Former ISSA CISO member
  - CISO Mentor Series
  - Pre-Professionals Meetup
- @wro
Agenda

- OSINT
  - Offensive
  - Defensive

- Questions
90% of breaches come from phishing, social engineering.
OSINT

• “Produced from publically available information that is collected, exploited and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.” - Wikipedia

• The art of gathering information that is publically available using various tools.
How Can It Be Used?

• Information on your target is valuable and relevant.

• “Knowledge is power only if man knows what facts not to bother with.” Robert Staughton Lynd

• “Make sure that the information is accurate and as accurate as possible.” Chris Hadnagy

• Document, storage and catalog information
  • List questions
  • Determine if information is useful or not
How Can It Be Used?

- Dumpster Diving
  - The law states that, “A person has no reasonable expectation of privacy for contents of garbage and has relinquished any property interest of garbage . . .” – *(This is dependent on where you are and is a case-by-case basis.)*
  - What information can be obtained?
    - Vishing – voice phishing
      - Caller ID spoofing
OSINT Frameworks

- OSINT-Framework
  - OSINT-Framework
  - https://github.com/lockfale/osint-framework

- Other Videos and Training
  - https://inteltechniques.com/
Search Engines vs Google vs Baidu vs Others

- Duck Duck Go  https://duckduckgo.com
- Startpage  https://startpage.com
- ReverseIP  https://yougetsignal.com

- Google  https://google.com
- Baidu  https://baidu.com
- Bing  https://bing.com
- Yandex  https://yandex.com

Books

- Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 5th edition – Michael Bazzell

- More books Amazon wishlist
Additional Search Engines

- FaceSearch  http://www.facesaerch.com
- MashedWorld  http://data.mashedworld.com/dualmaps/map.htm
- SocialMention  http://www.socialmention.com
- PIPL  https://pipl.com
- Geosearchtool  http://geosearchtool.com
  (Geolocated Youtube videos by time, keyword, radius etc.)
- urlscan.io  http://urlscan.io - websites
- Tininfo  https://tinfoleak.com/ - Twitter
Additional Search Engines

- Zoominfo.com - https://www.zoominfo.com/
- Payscale.com - https://www.payscale.com/
- Domain IP history, subdomains
  - DNS records - https://www.dnsstuff.com/
  - Archive.org - https://archive.org/
- Linkedin - https://www.linkedin.com/
Additional Search Engines

- DNS records
  - Mxtoolbox - https://mxtoolbox.com/
  - Nslookup
  - Dig (Linux, Windows etc.) – domain information groper

- Email addresses
  - Email Hunter, theHarvester - https://hunter.io/
    https://tools.kali.org/information-gathering/theharvester

- Browser extensions
  - Chrome extensions
    - Skrapp - https://www.skrapp.io/
    - Rapportive – plugin connector with info from Linkedin, social media etc.
Additional Search Engines

• Subdomains
  • Wolframalpha.com - https://www.wolframalpha.com
  • Searchdns.netcraft.com - https://searchdns.netcraft.com/
  • Sublist3r - https://github.com/aboul3la/Sublist3r/blob/master/sublist3r.py
  • Basic checks – vulnerabilities in subdomains
  • Censys IP Search – http://censys.io

• Website Profiling
  • Wappalyzer - https://www.wappalyzer.com/
  • Buildwith - https://builtwith.com/
  • Job boards
  • Forums

• Source Code Aggregators
  • Github searches, searchcode.com - https://searchcode.com/
  • Gist search - https://gist.github.com/search
  • Nerdydata.com - https://nerdydata.com/
Additional Search Engines

• Pasting Websites
  • Pastebin - https://pastebin.com/
  • Psbdmp.com - https://psbdmp.ws/

• Scan Engines
  • Qualys - https://www.qualys.com/forms/freescan/
  • Urlscan.io - https://urlscan.io/
  • Asfaweb.com - https://asafaweb.com/ (Analyzer for ASP websites)
  • Microsoft Office365 tenant searches

• Files
  • Exif data (Online ExifTool), FOCA (Elevenpaths)

• Social Media (Wechat and Whatsapp)
  • Reverse image searching, DataSploit, Geotracking, Username checks, keybase.io, PGP keys, Rapportive, Social Media Monitor
Additional Search Engines

- **IP**
  - Whois, ASN ID, MAC, Threat Intel. Feeds, Hurricane Labs

- **Website changes**
  - Changedetective.com, follow.net, Page monitor (chrome extension), public websites

- **Reverse image searching**
  - Tineye.com - [https://www.tineye.com/](https://www.tineye.com/)

- **People search engines** – [https://pipl.com](https://pipl.com), [https://www.zabasearch.com/](https://www.zabasearch.com/)

- **Phone number search engines**

- **Infosec Mindmaps**
Shodan

https://www.shodan.io

Explore Tag: iot
Browse saved searches with the tag: iot

Printers

Industrial Control Systems on the Internet
Returns all the industrial control systems that are publicly accessible on the Internet and running an actual industrial protocol.

Arm
IoT Arm devices (simple search)

TeaTime
Have I Been Pwned?

https://haveibeenpwned.com/
Google

https://www.exploit-db.com/google-hacking-database/

intitle:"Residential Gateway Configuration:" intext:"Cable Modem Information."

inurl:"sap-system-login"

intitle:"index of" .baseh_history

intitle:"Index of" "DCIM"

Inurl:yahoo_site_admin/credentials

index of /htdocs
<table>
<thead>
<tr>
<th>Date</th>
<th>Title</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-10-30</td>
<td>site:trello.com password</td>
<td>This will bring public Trello boards often containing user names and passwords. You can guess t...</td>
</tr>
<tr>
<td>2017-10-30</td>
<td>inurl:&quot;gradle.properties&quot; intext:&quot;p...</td>
<td>Google Dork: Files Containing Passwords Exploit Author: Huijun Chen ...</td>
</tr>
<tr>
<td>2017-10-17</td>
<td>intext:connectionString &amp; inturl:web &amp; ext:...</td>
<td><em>Category:</em> Files containing passwords <em>Summary:</em> A Google dork that gives SQL connection ...</td>
</tr>
<tr>
<td>2017-10-11</td>
<td>intitle:Index Of&quot; Intext:.ftpconfig</td>
<td>Description: FTP/SFTP credentials in .ftpconfig file from Atom text editor. Dork: intitle...</td>
</tr>
<tr>
<td>2017-08-03</td>
<td>inurl:vti_pvt/administrators.pwd</td>
<td>Here is a Google Dork to retrieve *sensitive information Login/password for MS FrontPage share...</td>
</tr>
<tr>
<td>2017-07-31</td>
<td>inurl:&quot;sitemapmanager.xml&quot; ext:xml -git</td>
<td>Finds FileZilla site manager files. containing FTP usernames and passwords Dxtroyer...</td>
</tr>
<tr>
<td>2017-06-22</td>
<td>Intext:DB_PASSWORD</td>
<td></td>
</tr>
<tr>
<td>2017-06-20</td>
<td>site:pastebin.com intext:<strong>@*.com:</strong></td>
<td>site:pastebin.com intext:<strong>@*.com:</strong> Finds pastebin.com dumped mail lists with passw...</td>
</tr>
<tr>
<td>2017-06-05</td>
<td>&quot;resources.db.params.password&quot; ext:ini -...</td>
<td>Finds lots of database usernames &amp; passwords! Dxtroyer...</td>
</tr>
<tr>
<td>2017-05-29</td>
<td>ext:reg &quot;[HKEY_CURRENT_USER\Software\ORL\Win...</td>
<td>Finds files with WinVNC passwords Dxtroyer...</td>
</tr>
<tr>
<td>2017-05-29</td>
<td>&quot;mysql_connect&quot; ext:inc</td>
<td>Finds scripts containing MySQL usernames and passwords Dxtroyer...</td>
</tr>
<tr>
<td>2017-05-29</td>
<td>&quot;iSpy Keylogger&quot; &quot;Passwords Log&amp;quo...</td>
<td>Description: iSpy keylogger logs Dork: &quot;iSpy Keylogger&quot; &quot;Passwords Log&quot; ext...</td>
</tr>
<tr>
<td>2017-05-17</td>
<td>&quot; End Stealer &quot; ext:txt</td>
<td>Finds logs from &quot;Black Stealer&quot;, an Internet password stealer Dxtroyer...</td>
</tr>
<tr>
<td>2017-05-12</td>
<td>&quot;FileZilla&quot; inurl:&quot;recentservers.xml...</td>
<td>Finds FileZilla recent server files with plain text usernames/passwords Dxtroyer...</td>
</tr>
</tbody>
</table>
Meta Data

- Date
- Time
- Document Creator
- Printer Used
- File Structure
- Passwords

Where can you find this information?
Maltego

- Opensource intelligence and forensics application
  - Offers data mining and information gathering that is easy to understand.
- System requirements
- Differences between commercial and community editions
<table>
<thead>
<tr>
<th>Feature</th>
<th>Maltego XL</th>
<th>Maltego Classic</th>
<th>Maltego CE</th>
<th>CaseFile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Cost</td>
<td>1800 USD</td>
<td>760 USD</td>
<td>Free</td>
<td>Free</td>
</tr>
<tr>
<td>Yearly Renewal Cost</td>
<td>760 USD</td>
<td>320 USD</td>
<td>Free</td>
<td>Free</td>
</tr>
<tr>
<td>Commercial Use</td>
<td>✔️</td>
<td>✔️</td>
<td>✗</td>
<td>✔️</td>
</tr>
<tr>
<td>Access to commercial Transform Hub</td>
<td>✔️</td>
<td>✔️</td>
<td>✗</td>
<td>N/A</td>
</tr>
<tr>
<td>Use with Internal Transform servers</td>
<td>✔️</td>
<td>✔️</td>
<td>✗</td>
<td>N/A</td>
</tr>
<tr>
<td>Standard OSINT Transforms</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Max number of results per transform</td>
<td>64,000</td>
<td>10,000</td>
<td>12</td>
<td>N/A</td>
</tr>
<tr>
<td>Max number of entities on a graph</td>
<td>1,000,000</td>
<td>10,000</td>
<td>10,000</td>
<td>N/A</td>
</tr>
<tr>
<td>Technical support</td>
<td>✔️</td>
<td>✔️</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Graph Export (CSV, XLS, XLSX, PDF and Image formats)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Graph Import (CSV, XLS, XLSX)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Shared Graph Sessions (Collaboration)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Machines (Transform Macros)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td><strong>Buy</strong></td>
<td><strong>Buy</strong></td>
<td><strong>Register</strong></td>
<td><strong>Read More</strong></td>
</tr>
</tbody>
</table>
Defensive

• Information aggregators
  • https://www.stopdatamining.me/opt-out-list/

• Public records
  • https://inteltechniques.com/menu.html

• Podcasts
  • https://inteltechniques.com/podcast.html

• Disposable email addresses

• Sudo application, Signal, ProtonMail, VPN, Credit Freeze, Privacy app

• Information Removal Workbook PDF
Additional Resources

- Twitter - #OSINT

- @aprilwright – 09/09/2017
  - https://github.com/jivoi/awesome-osint

- @peerlyst – 10/26/2017
  - http://ow.ly/4wGR30g8fh

- @peerlyst – 12/26/2017
Additional Resources

- Bank Information Security
  https://www.bankinfosecurity.com/interviews/most-breaches-trace-to-phishing-social-engineering-attacks-i-3516
Questions

• Any questions?

• Special thanks to Chris Hadnagy, April Wright, Rachel Tobac, Jayson Street and others for teaching and sharing OSINT tools and techniques!

• Slides will be publically posted in a few days

Thank you!

websecr at gmail dot com or @wro