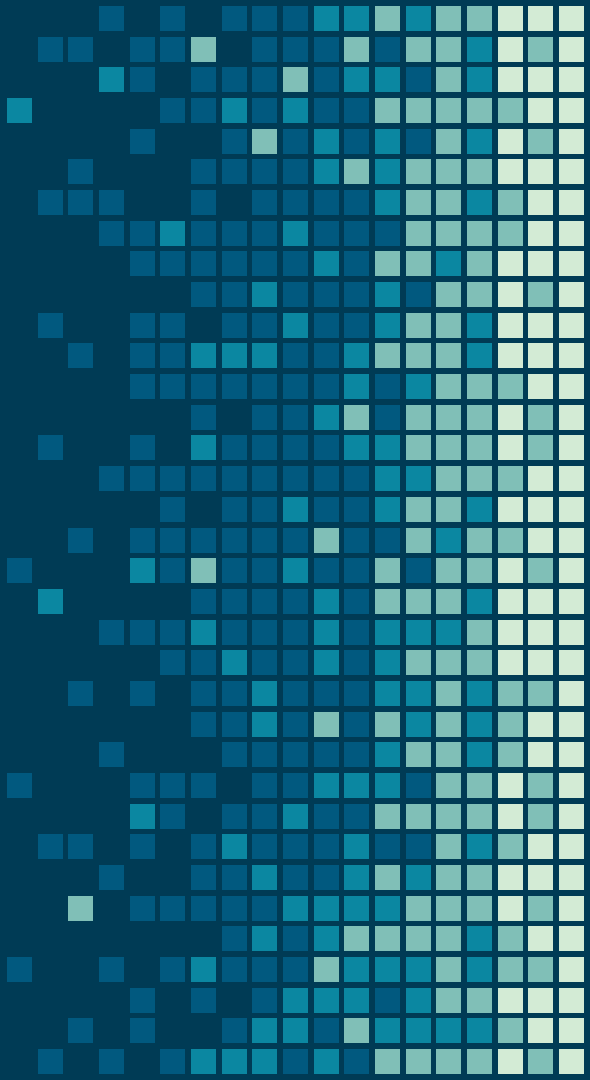
OSINT

Thomas Quig

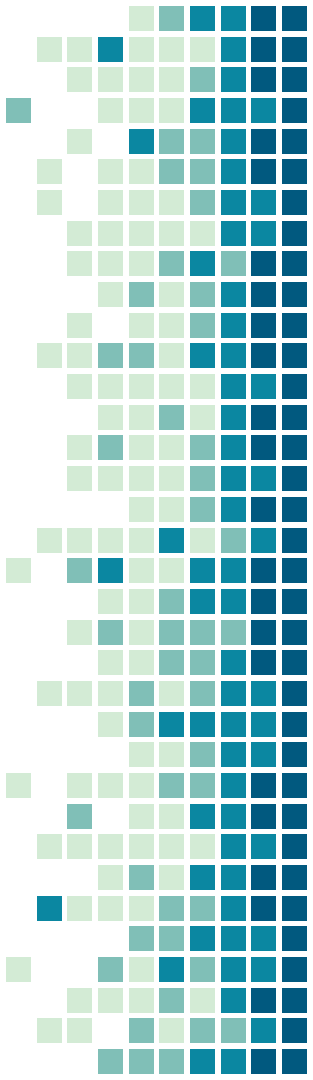


What Is OSINT

- Gathering information before an attack/pentest
- 4 Types of Information
  - Network Information
  - Host Information
  - Security Policies
  - Human Information
- OSINT as an acronym
  - Open Source Intelligence
  - Professional Term for Recon

Things not to do

- Don't break the law
- Don't doxx people
  - If someone is doxxing you, REPORT don’t RESPOND.
  - Responding could result in more bad happening to you.
- Remember DDDS
  - **Don’t**
  - **Do**
  - **Dumb**
  - **Stuff**



Network Information

- What is the public IP address of the person/company you need information on?
  - Lots of ways to get this
    - Various direct message applications
    - Get them to go to a website of yours
      - Easy but also risky.
  - What ports/local IPs are open on the IP you now have
    - nmap
    - netkitten
- What does the network look like
  - Banner grabbing from Open ports
    - $ nk verizon.net 80
    - GET / HTTP/1.1
- Domain names owned by the person/company
- **Minimize interaction** with the target network which may raise flags in computer logs.
  - Going to a target website once is probably 1/1000000 accesses in a day, but going 1000 times will raise a red flag in server logs.

Host information

- OS family
  - What version of the os is the host running information on
    - What vulns are known in that version.
      - Effective Power
- Usernames
- Who has elevated permissions?
- Default passwords
  - SigPwny got hacked :(
- Architecture type

There's a way to crash someone's iPhone with a text message

Richard Hartley-Parkinson Wednesday 27 May 2015 2:27 pm

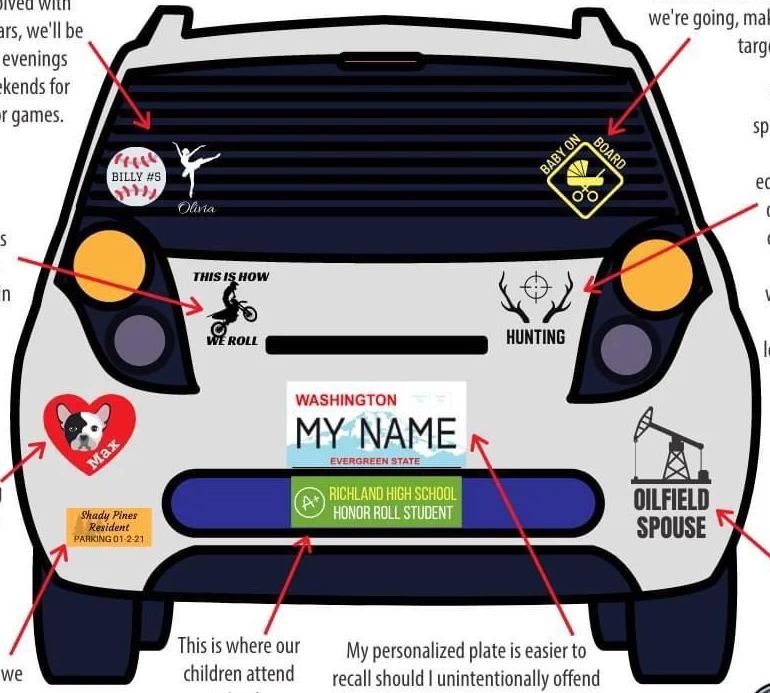
Security Policies

- Intrusion detection and countermeasures
- Historical legal action of persons/companies

Human information

- Home address, Home telephone number
- Frequent locations to hangout
  - Physical
    - Dorm, Union, ECEB, Grainger?
  - Online
    - Reddit, Twitter, Facebook, etc.
- Hobbies and interests
  - What subreddits are they active in etc.
- Activities
  - When do they go out, who do they go out with, how long are they gone.

What information are you DRIVING around?



Let me introduce you to our children, and because they're involved with extracurriculars, we'll be gone most evenings and/or weekends for practices or games.

We'll have our hands full and be distracted when we get where we're going, making us an easy target.

We like outdoor sports and may have expensive equipment at home or possibly in our car. We'll also be gone on most weekends during peak seasons, leaving our house unattended.

We like expensive toys that you can probably find in our garage.

We have a small-breed dog that answers to the name "Max."

My spouse is away for extended periods of time.

This is where we live/work.

This is where our children attend school.

My personalized plate is easier to recall should I unintentionally offend someone or if someone wants to keep track of my vehicle.

Richland Police

Richland

Learning about a Person

- Finding out the Host information, Network information, Security Policies, and Human Information about a person.
- Human Information is the easiest
- Continuous username
  - If a person uses the same username at a lot of places, it makes things easier.
  - Profile pictures
  - Reverse image searching is your good friend!
  - Plenty of websites do this.

Linking Handles to IRL Names

- If someone uses a handle, it's likely they use it on multiple platforms
- A handle from a semi anonymized platform is often linked to a social media platform.
- Even if the social is not anonymized, link to friends/followers of that social media.

Challenge Time

There is an existentialist, vexillology loving, totally not a robot, redditor who has been posting on r/uiuc and r/vexillology. Find him, don't tell people if you find him.

Ok here be an actual link

https://www.reddit.com/r/totallynotrobots/comments/b87iuo/this_man_who_is_undoubtedly_100_totally_not_a/

One of these people is definitely a Human.

How do you find removed posts?

Next slides have useful info about search engines/certain websites (Hints may or may not be included)

Interesting Facts and Search Techniques, Reddit

- Reddit is a semi-anonymous website
  - Some people deanonymize themselves.
    - Ex. President Obama, u/Giga_Gamby
  - Some people deanonymize themselves accidentally
    - u/Badongschlong, Yours truly.
  - Everyone gets sloppy.
- If you look long enough, you can usually link someone to a different account
- Search techniques
  - https://www.reddit.com/wiki/search
  - Author:
  - Selftext:
  - Boolean Operators
  - Comments NOT included in searching on reddit.
- Believe it or not you can actually have profiles

Twitter

- Always check Twitter bios, they often give out information you may need.
  - Twitter has a location and an advanced
  - Twitter has an advanced search bar, but it also has extra parameters.
  - https://lifehacker.com/search-twitter-more-efficiently-with-these-search-opera-1598165519
  - from:@ vs to:@ vs @
  - near: and within:
  - since: , until: , before:
  - :) , :(, ? operator, all boolean operators
  - “” vs just typing it in
- Check who they are following, check who is following them
- LOOK FOR MENTIONS OF OTHER ACCOUNTS
  - The more accounts, the more information you can gather.

Facebook

As Facebook banned my account 5 minutes after I made it, therefore I couldn’t set up any chals for Facebook.

If you get access to someones Facebook account, you can usually get any information you need.

Youtube

- Youtube doesn't allow you to search for comments, which makes makes finding information by comment searching difficult.
- Look for information that the channel left public. There is ALOT of it
  - Even if the discussion page is not visible, you can usually go there by adding /discussion at the end of the link.
- Youtube sends you the full banner image, not just the crop.
- About page
  - Often has EMAIL if the person was not paying attention on setup.
- Advanced search queries
  - Many are same as the other websites
  - https://tubularinsights.com/advanced-youtube-search-tips/

Github

- Github is good to look at if you are investigating a project.
- Old insecure versions of code.
- Look at commit messages, commit history.

Lastly

https://start.me/p/gy1BgY/osint

https://osintframework.com/

Hacker Isabelle! (UIUCTF, https://uiuc.tf)

Get Maltego CE (Real version if you have stonks)

Exercise common sense, don't do dumb stuff, don't break the law.

Get Creative, there is no one way to do OSINT. You get better with practice.