Week 10
OSINT

Slides By: Thomas Quig

Announcements

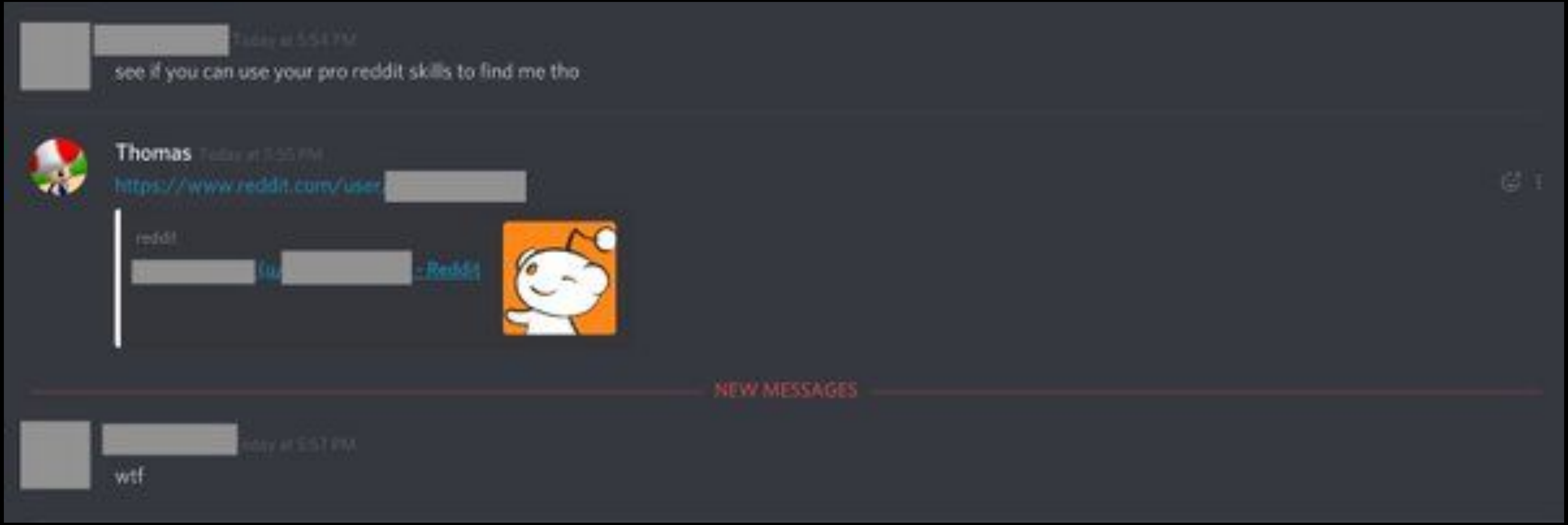
Shib auth, we are in need of maintainer/s

Merch form now: sigpwny.com/merch

Spray paint social @ some point

Infra transfer → hoard flags today!

sigpwny{thomas_has_a_wattpad}



[redacted] [redacted] Today at 5:54 PM

see if you can use your pro reddit skills to find me tho

Thomas Today at 5:55 PM

https://www.reddit.com/user[redacted]

reddit

[redacted] (u/[redacted] - Reddit

[redacted] [redacted] oday at 5:57 PM

wtf

OSINT

Open **S**ource **INT**elligence

What is OSINT

- Open Source
  - The stuff you are gathering is accessible to the general public (most of the time)
  - If it is not immediately accessible, it will be with some amount of enumeration.

- Intelligence
  - Information that can be used / is valuable for some operation.
  - Big range of value
    - Birthdays and usernames >> post content etc.

- Pseudonyms
  - Recon, Cyberreconnisance, HUMINT etc.
  - Generally considered “easy” in security (not true)

A Warning

OSINT, especially HUMINT (Human Intelligence) is functionally **stalking.**

DON'T BE A CREEP

Make sure you have permission before OSINTing someone/thing

You could find something you don’t like / weren’t supposed to

Types of Intelligence

System Intelligence, Network Intelligence, Organizational Intelligence, Human Intelligence

Types of Intelligence

- Systems Intelligence

- Network Intelligence

- Organizational Intelligence

- Human Intelligence ← **Primary focus of today's talk**

Systems Intelligence

what is it made of?

Systems Intelligence - Summary

Get information about a system you are attacking.

Trick the system into giving you that information voluntarily

Methods

- Port scanning
- Information probes
- IRL Intelligence

Network Intelligence

where is it and who is it talking to?

Network Intelligence - Summary

Like system intelligence, but focused more on communications.

Given a network of systems, who talks to who and why.

What is the dataflow to, from, and within a network

Realistically a lot of what you do here is going to be on Windows stuff, **so this section will be more geared towards that.**

Organizational Intel

what are they doing!?!?

Organizational Intel - Summary

Gathering information on organizations

- What is their opsec like?
- Who works for them?

Policy decisions

- are the company’s lawyers assholes?

Human Intelligence

who is this person?

Human Intelligence

- This is easiest thing to learn
- Creating a map of a person
    - Everything from social media to IRL address

- Tons of different methods, too many to put on a summary page

Essentially stalking but purposeful and less creepy

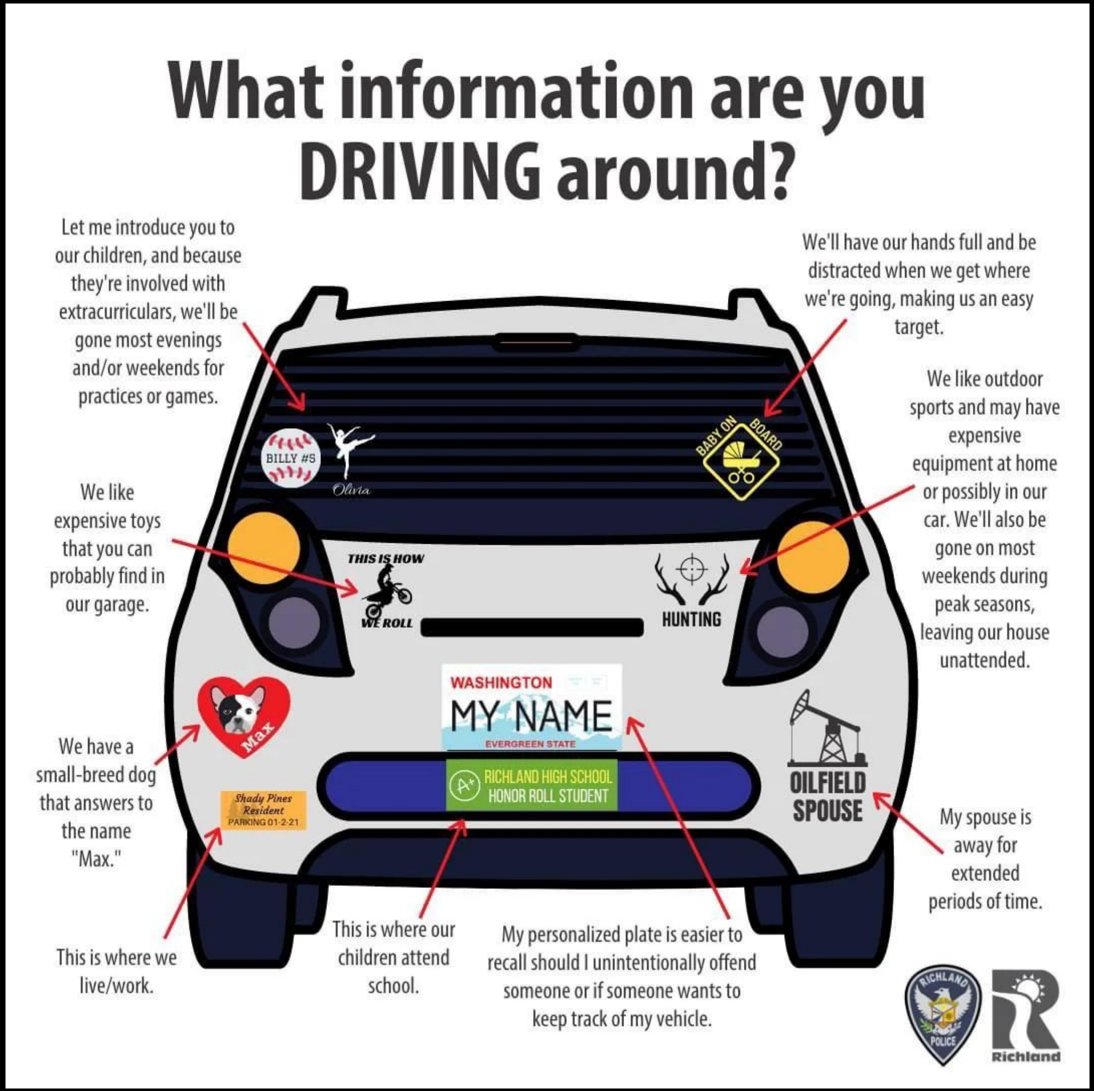
Human Information Gathering Methods

- **Easy Mode**
  - Social Media
  - Shared Username, use Sherlock

- **Medium Mode**
  - In depth searching utilizing Google Dorking etc
  - Look around networked profiles (friends, followers etc)
  - Paid Services
    - Bullshit like 95% of the time
    - If multiple paid services point to same thing it might be valid

- **Hard Mode**
  - Voting Records
    - Can enumerate given birth month and address
  - **make new friend**
    - Social Engineering
    - be **GODDAMN** careful about your motives

Information Leakage



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 expensive toys that you can probably find in our garage.

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 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.

General OSINT Methods

mostly applies to everything

OSINT Tips - Identities

Split Identities

- Most people have **two** identities online
  - Professional
  - Casual
- Your job when doing OSINT is to link them

Sherlock

- Can be used to find specific usernames on tons of platforms.
- Definitely try it on your usernames!

OSINT Tips - Human Networks

People have friends

- and connect with them online
- abuse this to find information about a target

Check Friends/Family/Followers

- Is a target tagged in something? Are they mentioned? Did they respond to a friend?
- Friends & family may have information about a target
  - Birthdays and Facebook :(

OSINT Tips - Detection

Don't make noise

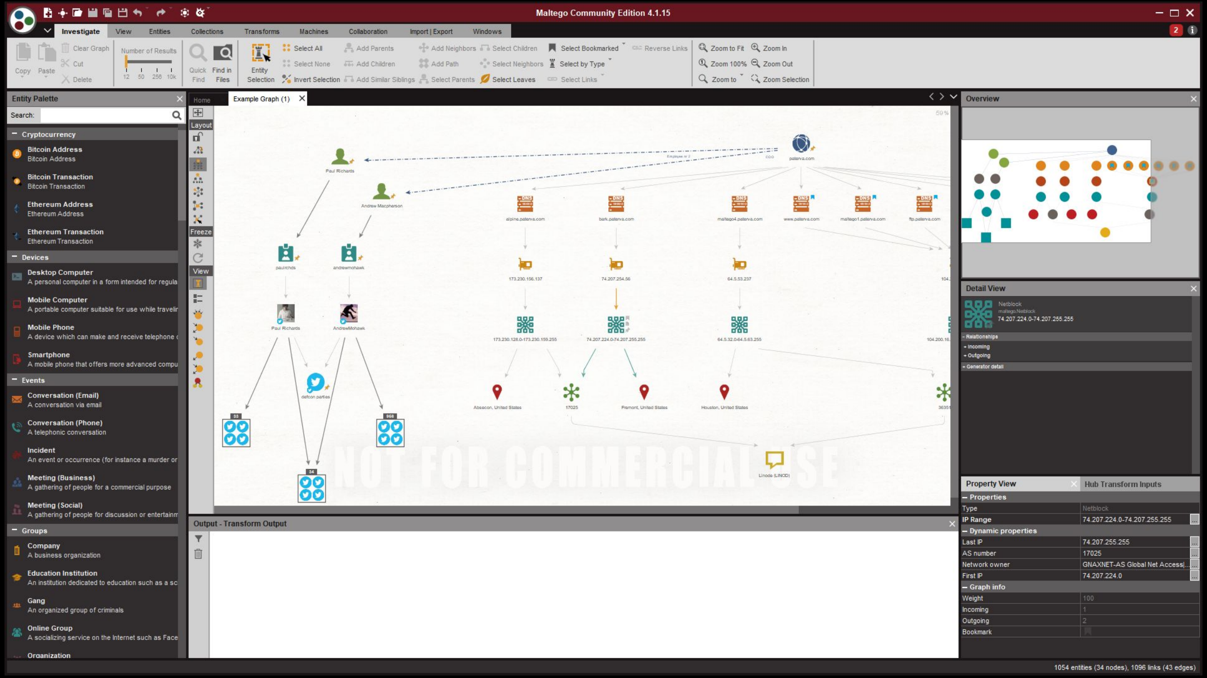
- Don’t do things that would get you noticed
  - LinkedIn Page Views (STAY ANONYMOUS, DON'T DO A LOT)
  - Learn from my mistakes, don't REPLY TO A COMMENT ASKING ABOUT SOME PIECE OF INFORMATION ABOUT SOMEONE.

- Viewing content is generally fine, creating content will often get you noticed. Stay low, stay out of the way, just make acct and look at what you need to.

OSINT Tools - Maltego

OSINT Mapping tool with extra features

Has “Transforms” that can connect.



Definitely give the Community Edition a Spin

Maltego at work

Other OSINT Resources

Michael Brazzel - Open Source Intelligence Techniques (The OSINT Bible)

Tracelabs - OSINT on real missing persons cases

Bellingcat OSINT - Cool OSINT Firm

https://ctf.cybersoc.wales/ : 24/7 Live OSINT CTF (many chals)

Challenge Start (31 challenges for this meeting!)

UIUCTF 2020 - HackerIsabelle (6 challenges)

UIUCTF 2021 - ChaplinCoding (8 challenges)

SP 2019 - TotallyAHuman3025 (11 challenges)

Fall CTF 2021 - SpaghettiEsports (3 challenges)

CCC 2021 - con_angry (3 challenges)

UPCOMING SUITE - **NOT FINISHED** (**20 challenges**)

Those are the usernames for the first challenge of each suite, go figure out which platforms they belong to!!!

Let us know if you are stuck / something seems down or broken

Next Meetings

Weekend Seminar: OSINT II

- More advanced OSINT Methods
- Other forms of OSINT (SysINT, OrgINT, NetINT)

Thursday: Networking

- Fundamentals of communication between hosts
- TCP / UDP / IP, Lower Level Communication (Overview of OSI Stack)
- Common Networking Vulnerabilities / Attacks