FA2022 Week 05

OSINT I

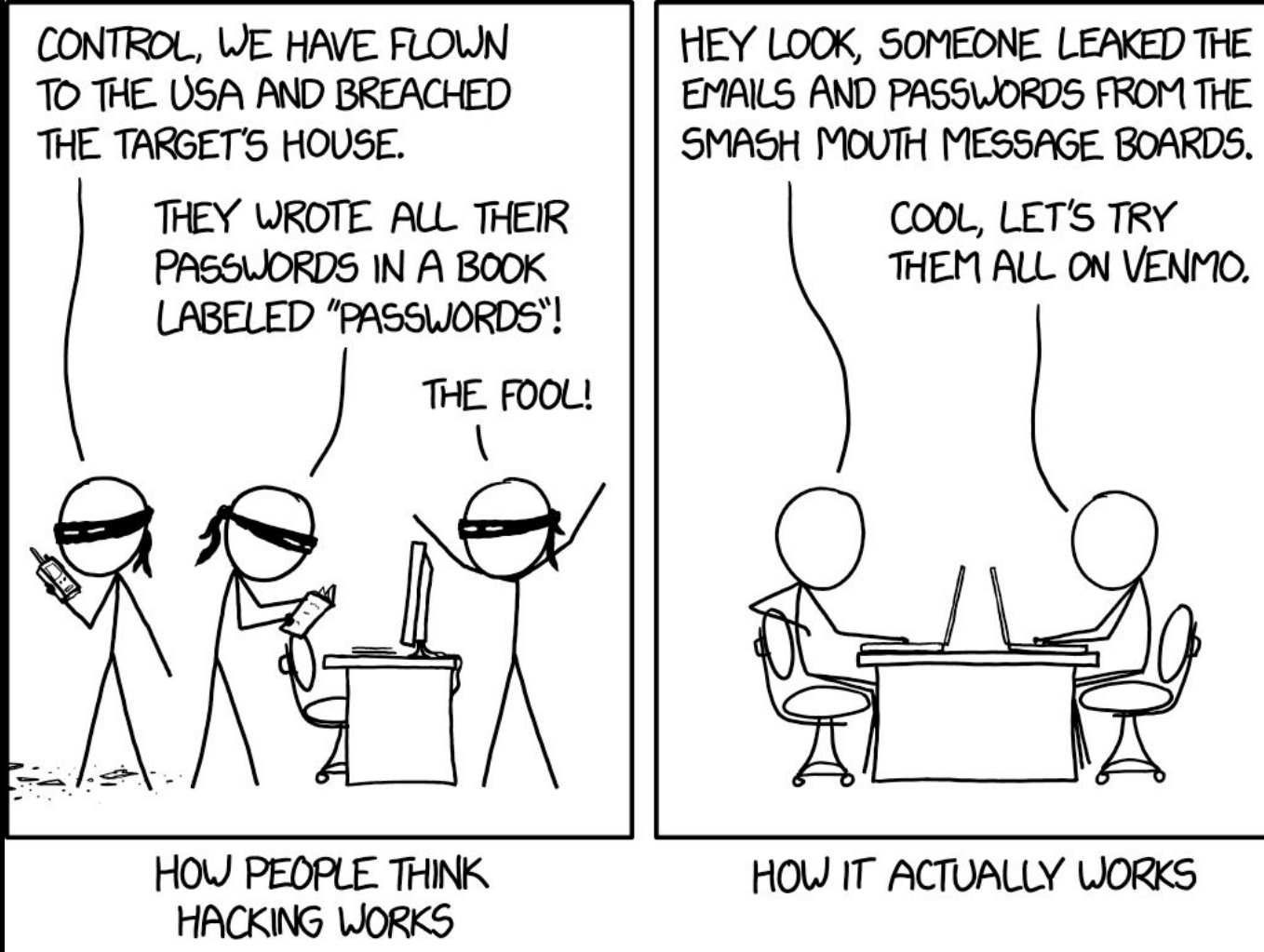Thomas Quig, Julius White, Danny Poje

Announcements

- Fall CTF went great
    - Approx. 300 Attendees!

- Social Event this weekend (Saturday)
    - Vote on what it will be by Friday @ 7PM

- Back to 1404???
    - We don't know when… earliest Oct 7.

OSINT

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

What is OSINT

- Open Source
  - The stuff you are gathering is accessible to the general public
  - If it is not immediately accessible, it will be

- 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 Ethics)

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 / aren't supposed to

Explicit OSINT Code of Ethics

1. You will **not INTERACT** with any user without first confirming with absolute certainty that they are a part of the challenge. In the case of these challenges, there is **no need to create any content**

2. You will **not perform any port scans on backend services** or attempt to do any investigation by logging in to any of the aforementioned accounts. This is **not web hacking**

3. You will **not perform invasive investigative OSINT on other people without their explicit consent**. This includes friends, family, coworkers, and strangers.

While exceptions exist to this code, those exceptions don't apply here!

Why is this important?

CYBERSECURITY

Google and Facebook got tricked out of $123 million by a scam that costs small businesses billions every year — here's how to avoid it

PUBLISHED THU, MAR 28 2019·1:13 PM EDT

Kate Fazzini
@KATEFAZZINI

SHARE f in ✉

KEY POINTS
- Google and Facebook paid out $23 million and $100 million respectively to a cybercriminal from Lithuania, who pleaded guilty to wire fraud in New York this week.

- The companies were scammed out of the payments by a technique known as business email compromise or invoice fraud.

- Unlike most companies and individuals who are victimized by this type of crime, the tech giants were able to recover the funds. Most aren't so lucky, and many companies take a massive hit or are forced out of business by this type of crime.

TV

Mad Money   WATCH LIVE ▶

UP NEXT | Shepard Smith 07:00 pm ET   Listen

ADVERTISEMENT

CNBC BRAND STUDIO

CNBC Brand Studio with Salesforce

Enlightened was founded to help people lead healthier lives without compromising on tasty treats. This is how better data is helping to rapidly grow their business and launch a new

CNN BUSINESS

Types of Intelligence

- Systems Intelligence

- Network Intelligence

- Organizational Intelligence

- Human Intelligence

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

Port Scanning - Common Ports

Port	Service	Port	Service	Port	Service	Port	Service
20-21	FTP (File Transfer)	137-139	NetBIOS (Sessions)	530	RPC (Remote Procedure Calls)	3479	PlayStation Network
22	SSH (Secure Shell)	156	SQL (Databases)	666	DOOM ONLINE	4070	Amazon Echo Dot → Spotify
23	Telnet (Text comms)	194	IRC (Chatting)	666	Aircrack-ng C2 Server	4444	Metasploit listener
25	SMTP (Mail Transfer)	311	macOS Server (Admin)	740-754	Kerberos related stuff	5000	AirPlay (Among Others)
53	DNS (Domains)	389	LDAP (Windows) (Active Directory Access)	1776	EMIS (1st Responders)	5900	VNC (Virtual Network Computing)
67-68	Bootstrap / DHCP	443	HTTPS (Websites)	3074	Xbox for Windows	5985	Powershell (Remote Management)
80	HTTP (Websites)	444	AD (Windows) (Active Directory)	3306	MySQL (Databases)	8080	Alternate HTTP (Also 8000 / 8008)
88	Kerberos (Authentication)	445	SMB (Windows)	3389	RDP (Microsoft Remote)	25565	Minecraft Server

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Port Scanning - Implications

- Adversarial
  - Ports being open can often provide information about a system.
  - If 80, 443, and 8080 are open it probably has a website.
  - But if 53, 445, 3389, etc… it is likely a Domain Controller (DC)

- Ethical / Legal
  - Port scanning can harm system availability
  - Starts to enter a legally / ethically grey area
  - **DO NOT PORTSCAN THE GODDAMN US GOVERNMENT**

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

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

Organizational Intel

What are they doing!?!?

Organizational Intel - OpSec

- How is an organization's OpSec?
  - What is the email format (firstname.lastname)

  - Preferred _____ (airline, hotel etc.)

  - What are their IT/security protocols?

  - Do org members have strong opsec
    - attacking a company = attacking people

  - Internal document leakage

Rachel Tobac, Opsec/SocEng badass

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

Human Information Gathering Methods

- **Profiles**
  - Links, pictures, **stuff that goes to other stuff**
  - Build a map of someone

- **Username Reuse**
  - Same across lots of places!
  - Helpful for these chals!

- Images
  - Reverse ____ searching!

- Deleted Content
  - Archivists save old websites!
  - Wayback machine!
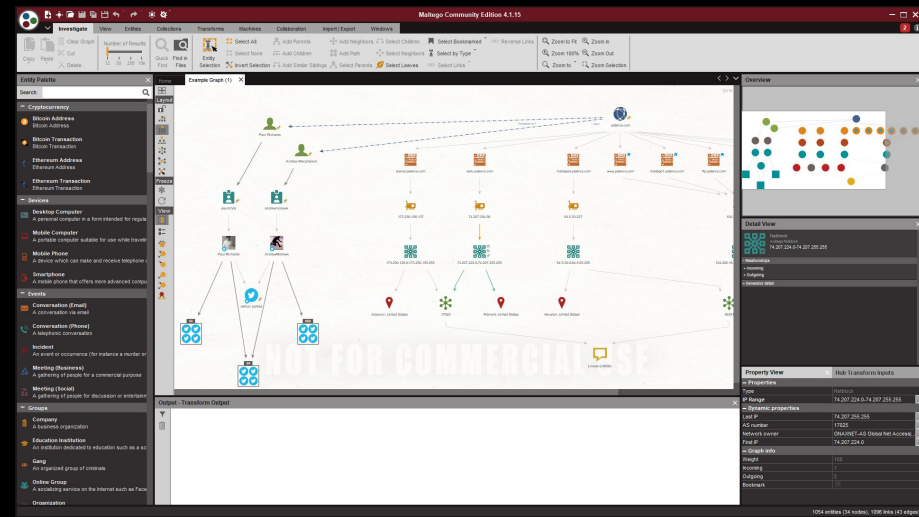
General OSINT Methods

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!

Twitter

- **TWEETS & replies are ALWAYS WHERE YOU SHOULD LOOK FIRST**

- Twitter bios have info, location, birthday, and a link to somewhere

- Advanced Searches: good

- Follower / Following lists can help find friends

YouTube

Channels

- Banner, Profile Picture
- About tab, playlists

Playlists

- Unlisted videos are **visible**

Videos

- Closed captions, different languages. 3 Englishes!
- Description, comments (not searchable)

GitHub

Profile page
- View featured repos
- Links, socials, location
- email

Repositories
- Commit history
- Pull Requests & Comments

Comments / User Content
- Can exist in many places

Unpin   Unwatch 1   Fork 0   Star 2

<> Code   ⊙ Issues   ⊔⊔ Pull requests   ⊙ Actions   ⊞ Projects   📖 Wiki   ⊘ Security   📈 Insights   ⚙ Settings

⊔° main ▾   ⊔° 2 branches   ⬙ 1 tag   Go to file   Add file ▾   Code ▾

About

🌎 Thomas-Quig Update README.md   06cc48f on Jan 31, 2021   ⟳ 421 commits

llss is a MTD (Moving Target Defense) that utilizes Hardware Address (MAC) randomization to provide a moving target. llss greatly increases the difficulty of sniffing, and ARP cache poisoning.

📁 captures	:)	2 years ago
📁 notes	Update bugs.md	2 years ago
📁 src	More test files	2 years ago
📁 tests	H	2 years ago
📄 README.md	Update README.md	2 years ago
📄 SECURITY.md	Create SECURITY.md	2 years ago
📄 TODO.md	Added TODO.md	2 years ago

🔗 llss.page

networking   security-tools   shuffling

hardware-address-shuffling

📖 Readme

☆ 2 stars

👁 1 watching

⊔° 0 forks

Releases 1

⬙ **Release 2.0.0** Latest
on Jun 25, 2021

Packages

No packages published
Publish your first package

≡ README.md   ✎

llss

LLSS, or 'Link Layer Stable Switcher' is a networking tool for linux-enabled devices designed for stability and security. llss is a MTD (Moving Target Defense) that utilizes Hardware Address (MAC) randomization to provide a moving target. This greatly increases the difficulty of sniffing, and ARP cache poisoning. At the moment, this project is **optimized to work in an ad-hoc, wireless environment**

Examples

Reddit

- Reddit is a semi-anonymous website

- Link people to **other platforms**

- Profile
  - Profile Pictures, Banner Photos
  - Comments, posts, links
  - Moderator
 - Awards

- Posts
  - Search by top

- **old.reddit.com**

LinkedIn

- LinkedIn is a very open website
  - Most people tend not to lie or be very hidden

- Profile
  - Profile & Banner Pictures
  - Posts, Comments, Socials
  - Experience, Education, Skills, and Activity
  - Email, Phone Number, and Address

- Comments / Content
  - Easily accessible to all

SoundCloud

- SoundCloud is a semi-anonymous website

- Often link to other socials; yet can be as anonymous as they want

- Creators / Publishers are more vulnerable

- Profile
  - Posted media, Profile Picture, Socials
  - Likes, Comments, and Reposts
  - Followers/Following
  - Playlists
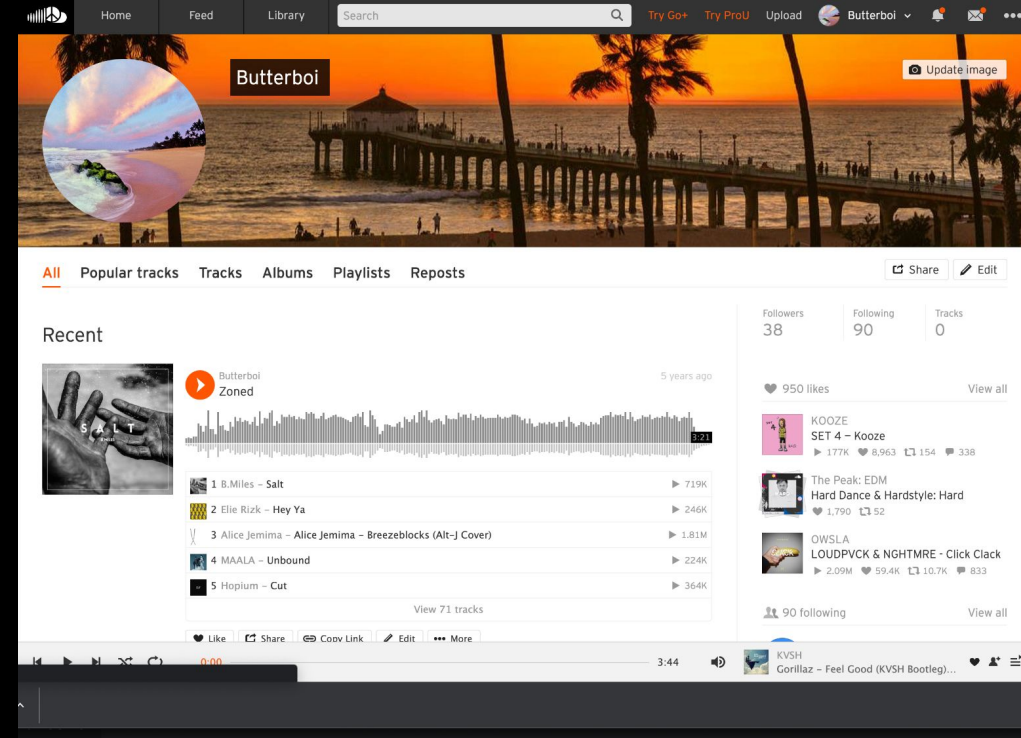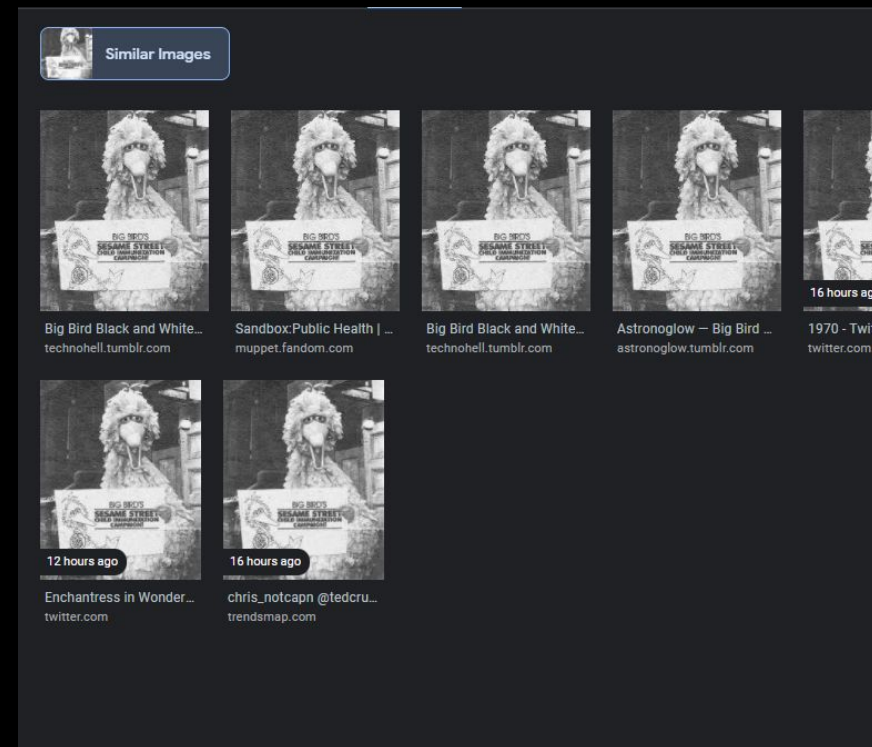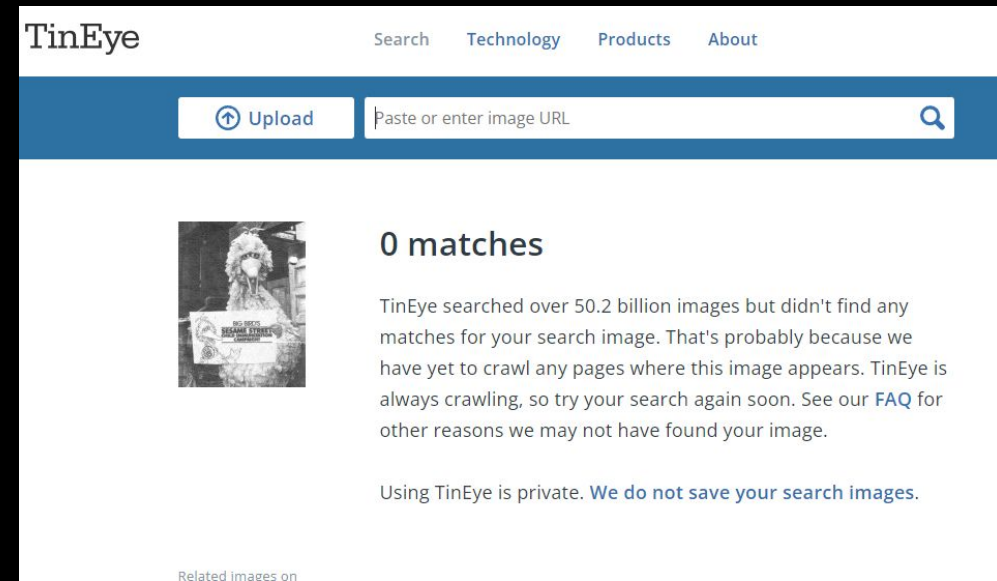
Challenge Collection

UIUCTF 2020 - HackerIsabelle (6 challenges)

UIUCTF 2021 - ChaplinCoding (8 challenges)

UIUCTF 2022 - Chucklephucke (6 challenges)

SP 2019 - TotallyAHuman3025 (11 challenges)

Fall CTF 2021 - SpaghettiEsports (3 challenges)

CCC 2021 - con_angry (3 challenges)

Fall CTF 2022 - Spoingusthecat (4 challenges)

FA 2022 - Check **ctf.sigpwny.com** (**8 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

2022-10-02 - **Assembly** (Seminar)

- Learn how assembly works!!!

2022-10-06 - **PWN/Binary Exploitation I** (Regular Meeting)

- Attack binaries!!! Buffer overflow!!