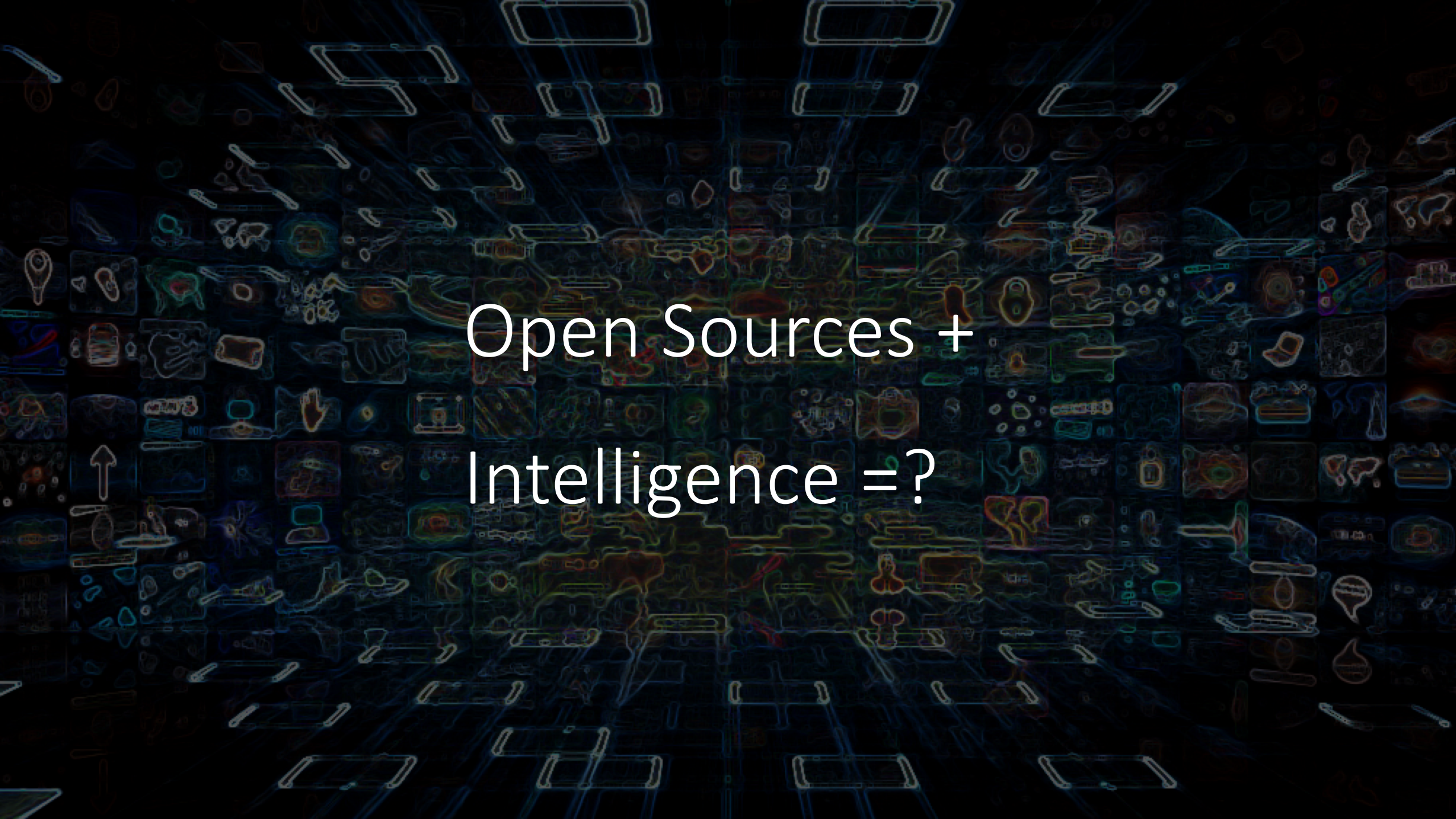
Open Source Intelligence in Cybersecurity

Anastacia Webster

Overview

- Open Sources + Intelligence = ?
- Open Source Intelligence in Cybersecurity?
- Finding Tools to Use
- Non Technical Tools/ Skills
- Technical Tools/ Skills
- Demonstration Tools
- Demonstration


Open Sources +
Intelligence =?

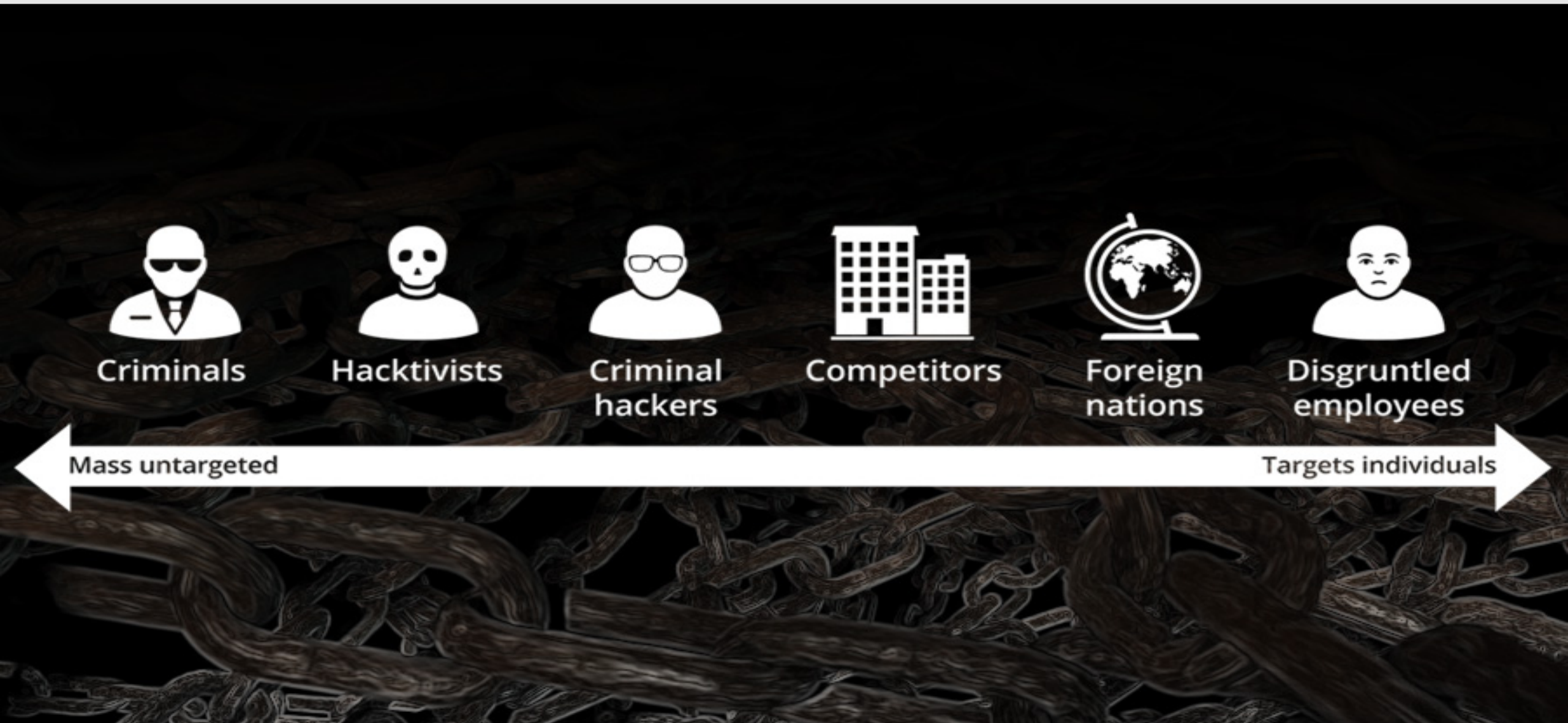
Open Source Intelligence in Cybersecurity

Recon	Weaponize	Deliver	Exploit	Install	C2	Actions
Gather data and intelligence on target organization	Craft malicious payload, use exploits for vulnerabilities	Payload sent to target (phishing)	Compromise system	Install malware, obtain credentials and establish backdoors.	Navigate internal network and setup command and control	Ultimate goals achieved

PHASE 1: RECON

- Research the target
- Collect/Analyze information about online actives/public presence
  - Social Media
  - Harvest Email Addresses
  - Government Records
  - Public News
  - Scan internet facing systems and applications
- Build Profile

RECON ACTORS

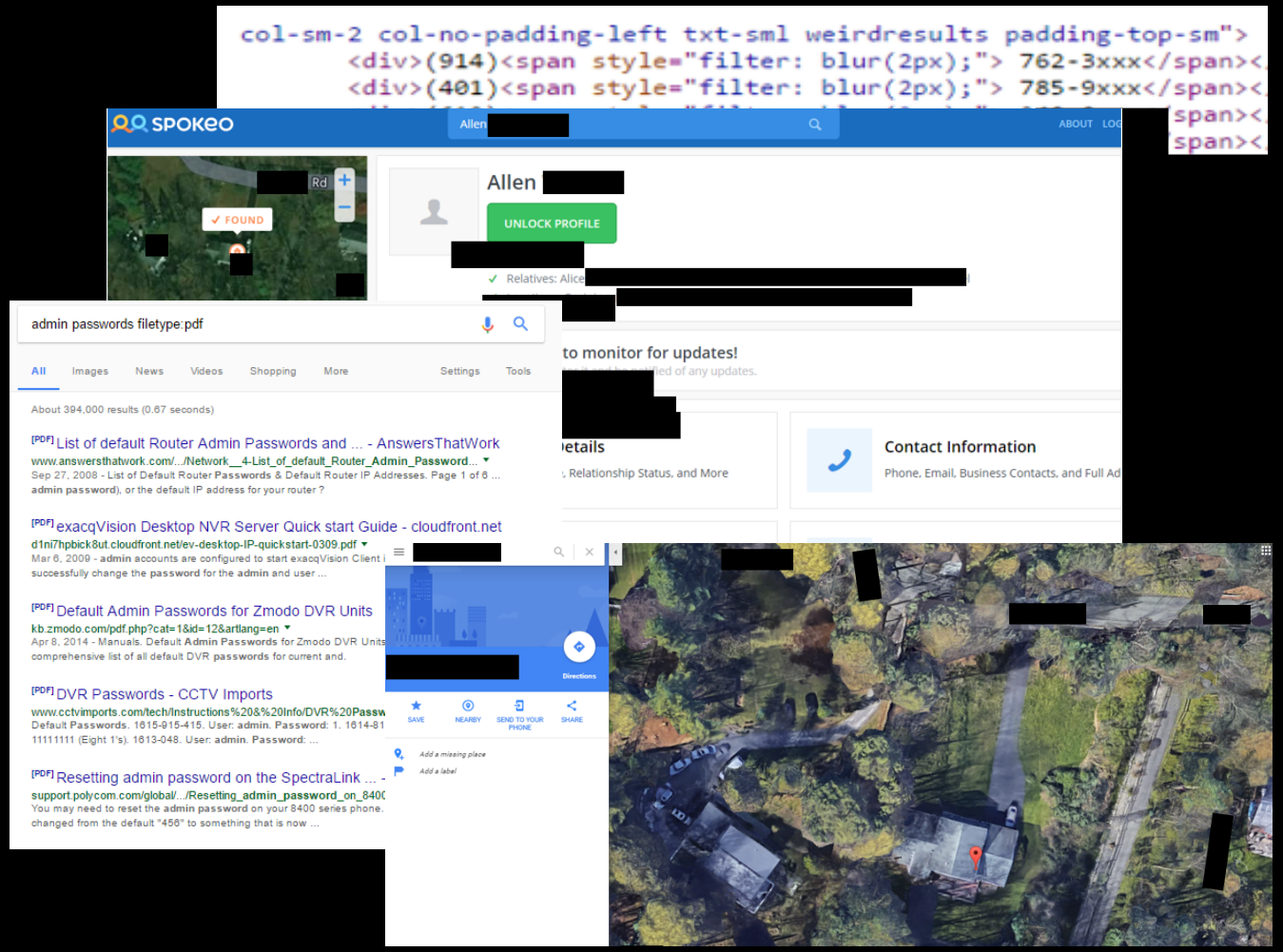


Finding Tools to Use

- Tons of FREE Tools out there for you to use…
  - https://osintframework.com/
  - https://inteltechniques.com/menu.html
  - https://www.i-intelligence.eu/osint-tools-and-resources-handbook-2018/
  - http://reconvillage.org
  - Search GitHub…

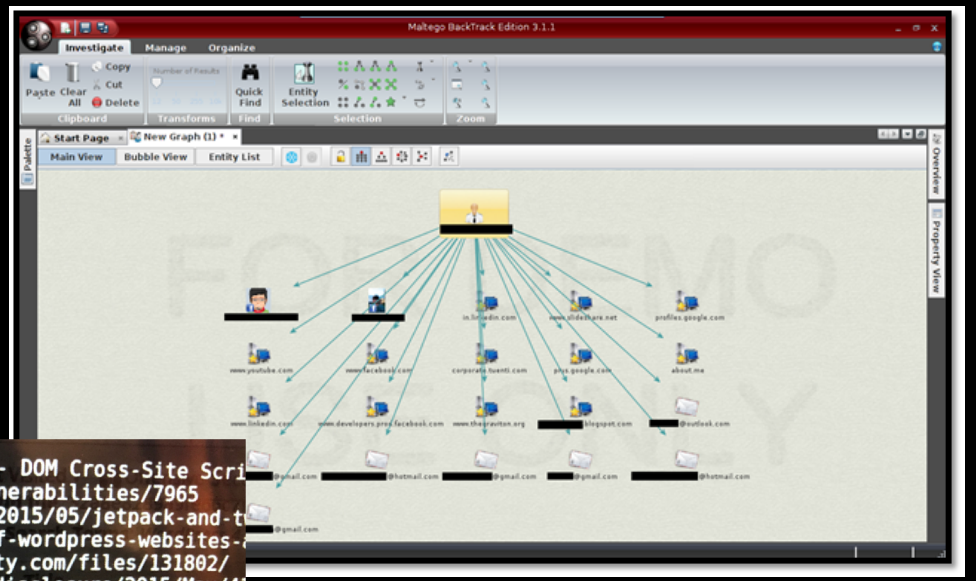
Non Technical Tools/ Skills

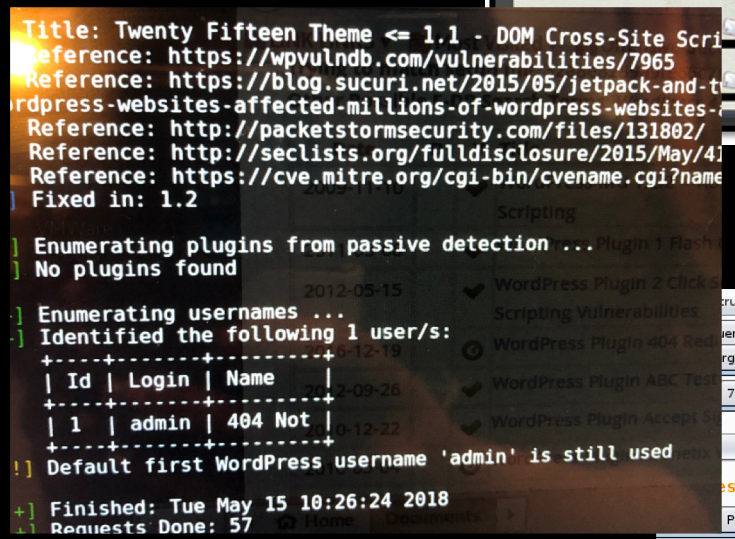
- Google Booleans
- View Source/ Inspect
- People Search Engines
- Social Media
- Browser Extensions
- Mapping/ Surveillance TV
- Reverse Phone Look Ups
- CMS Look Ups

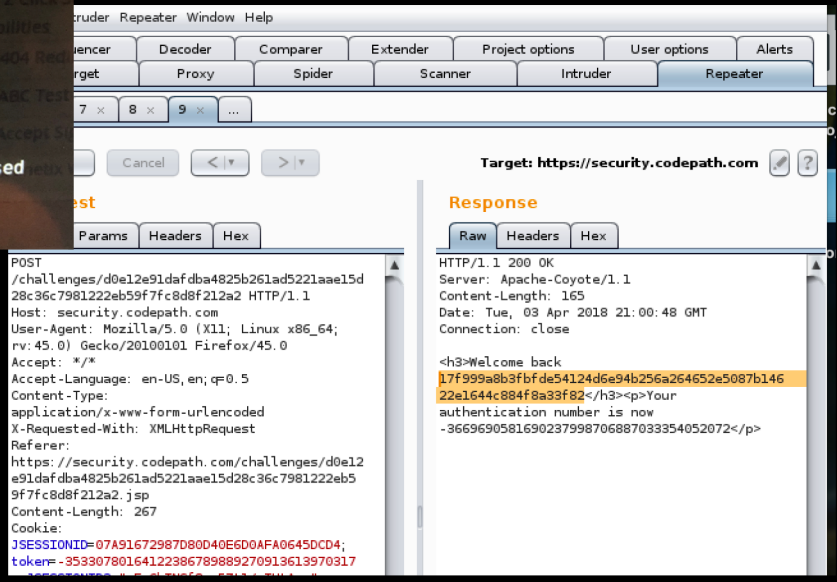


Technical Tools/ Skills

- Maltego
- Burp
- WPScan
- Wireshark
- Dirbuster
- Creepy
- Buscador
- Email/Username/Password Generators

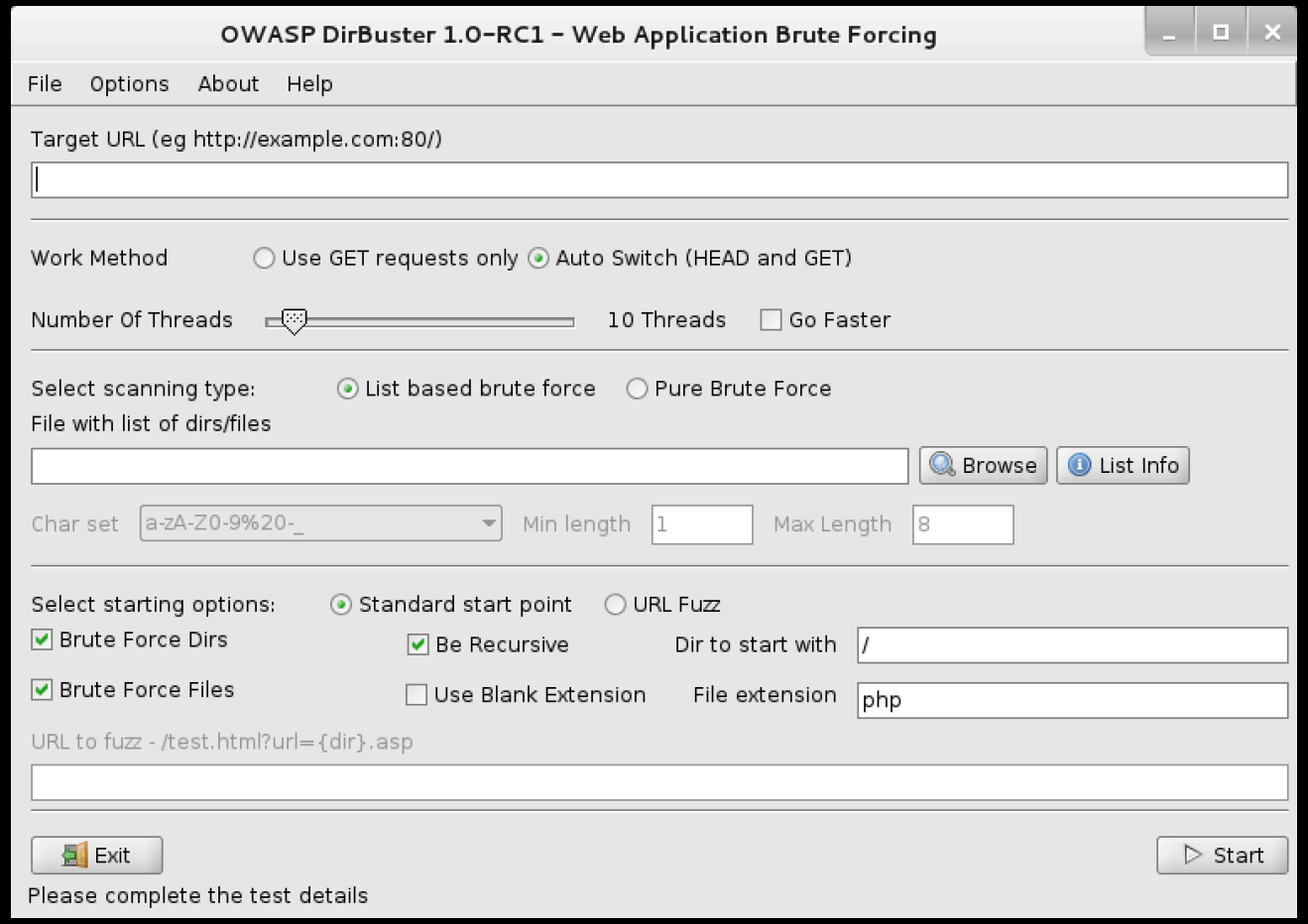




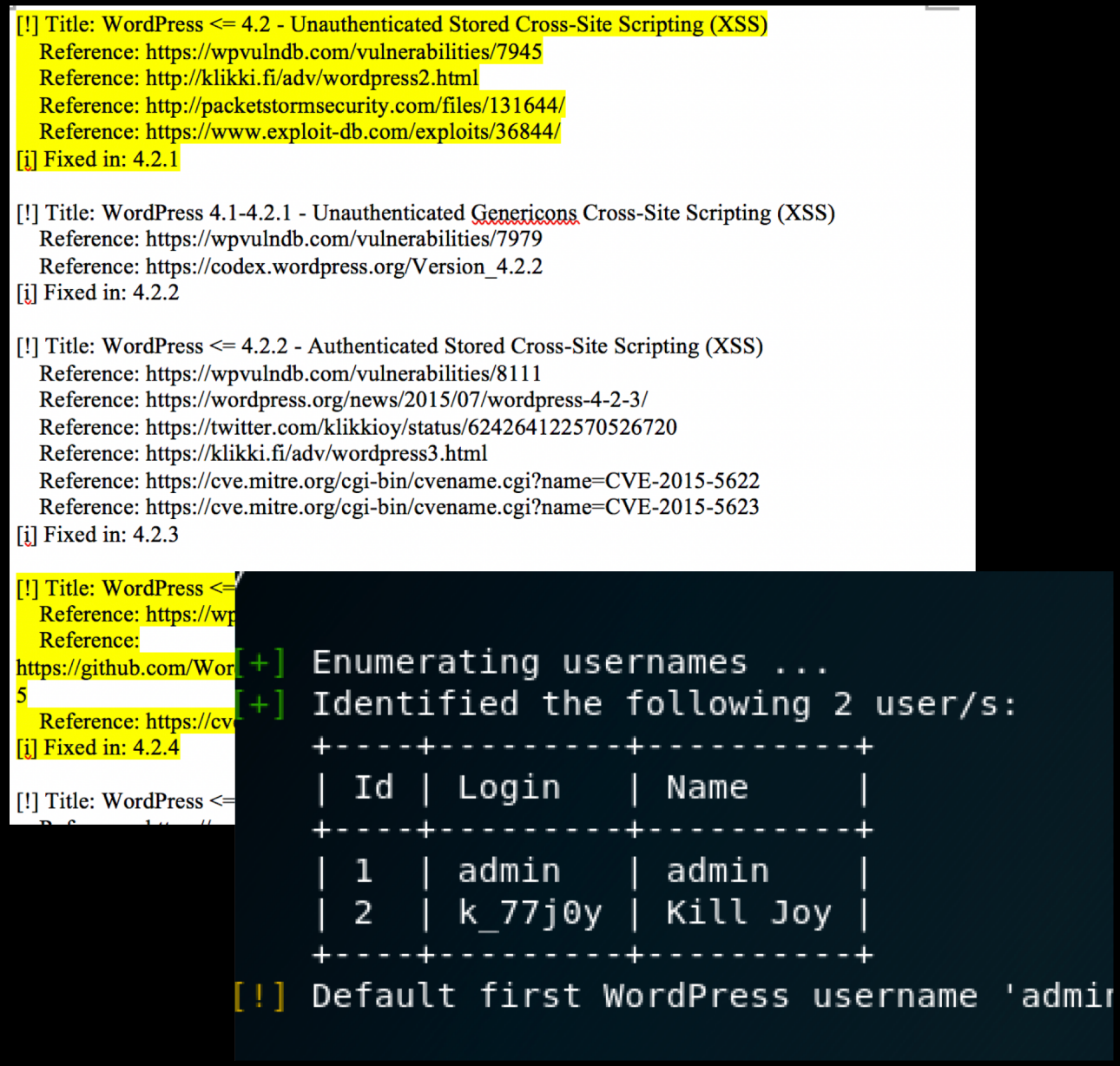


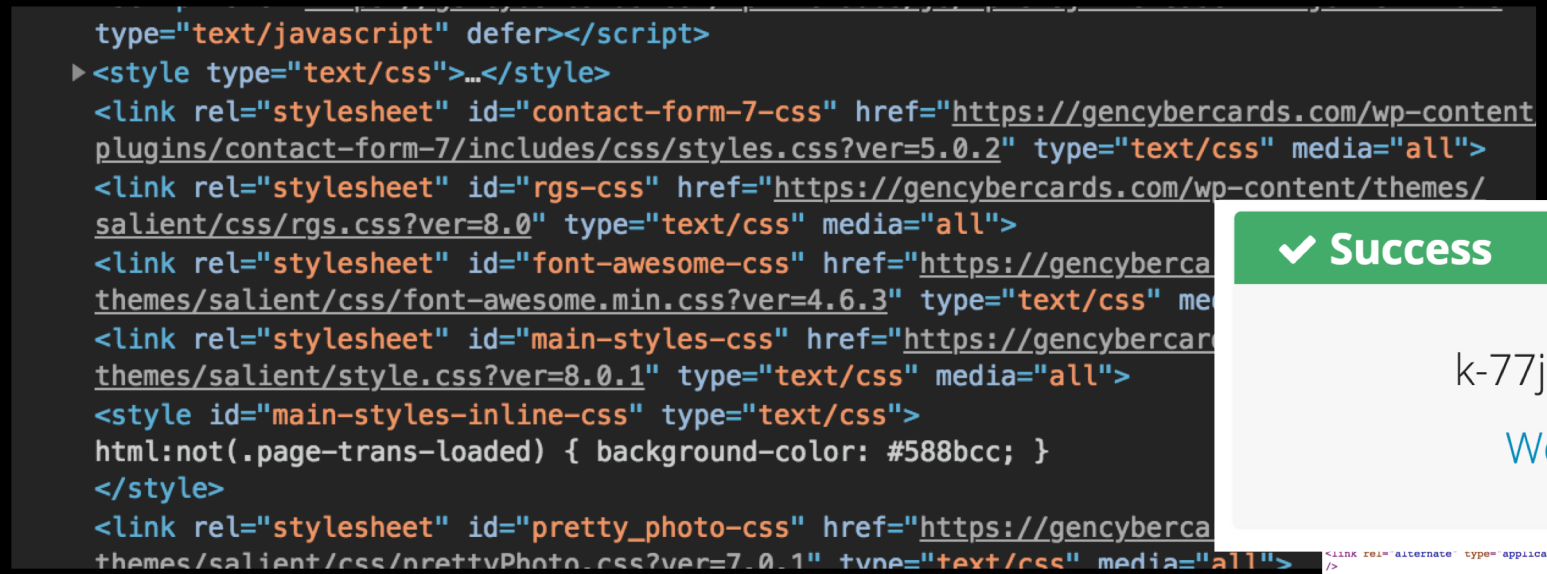
Demonstration Tools

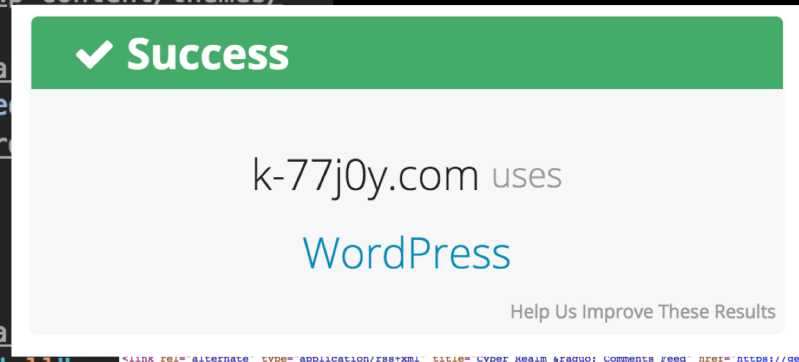
More Technical: DirBuster

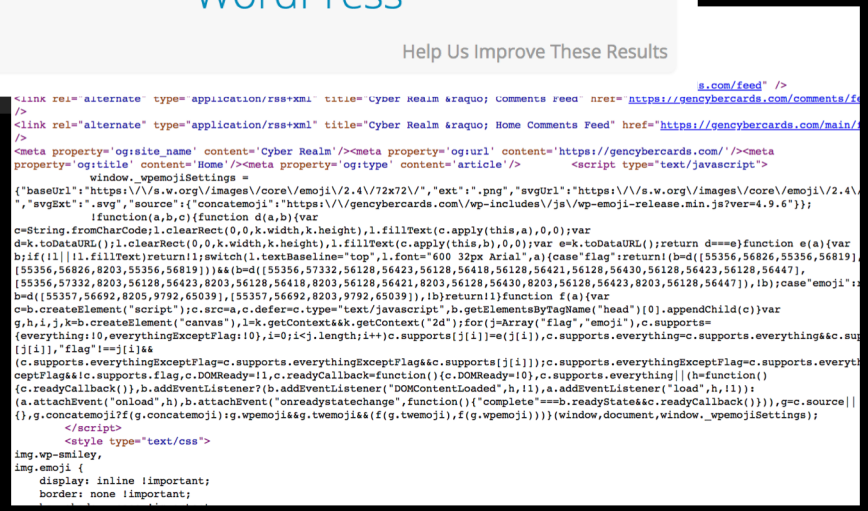


More Technical: WPScan









Non Technical: CMS/View Source/Inspect

Questions/Comments?

Email me at anastacia.webster@csusb.edu.