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

1. Recon: Gather data and intelligence on target organization
2. Weaponize: Craft malicious payload, use exploits for phishing
3. Deliver: Payload sent to target (phishing)
4. Exploit: Compromise system
5. Install: Install malware, obtain credentials and establish backdoors
6. C2: Navigate internal network and setup command and control
7. Actions: 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

- Criminals
- Hacktivists
- Criminal hackers
- Competitors
- Foreign nations
- Disgruntled employees

From mass untargeted to targets individuals
Finding Tools to Use

• Tons of FREE Tools out there for you to use...
  • https://osintframework.com/
  • https://inteltechniques.com/menu.html
  • http://reconville.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
- Dirbuser
- 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.