

EC521 - Cybersecurity Final Project: Open Source INTelligence (OSINT) Lab Generation

Maha Ashour, Jack Belmont, Pierre-François Wolfe

Boston University, College of Engineering



Goals

Lab generation project

- ▶ Open Source INTelligence (OSINT) for identifying vulnerabilities
- ▶ Introduce useful tools
- ▶ Provide an interesting and ethical learning scenario
- ▶ Build lab infrastructure: vulnerable webserver, synthetic datasets, challenges, etc.



OSINT Cycle

- ▶ Collect (gathering)
- ▶ Process (data validation)
- ▶ Exploit (determine value of information)
- ▶ Produce (consumable/usable data)

Maltego

- ▶ Data Mining Tool
- ▶ Direct Graphs for Link Analysis
- ▶ Relationship Analysis
- ▶ Transforms for streamlined searching

Other Tools

- ▶ **theHarvester**
 - ▶ Input: Web domain and data source (ex: bing, linkedin, shodan)
 - ▶ Output: Report with emails, subdomains, hosts, employee names, open ports, etc.
 - ▶ Method: Gathers public information about domain using custom python scripts for each data source
- ▶ **h8mail**
 - ▶ Input: [List of] email(s)
 - ▶ Output: Passwords - hashed or plain text
 - ▶ Method: Looks through “breach compilation” to find match
- ▶ **Metagoofil**
 - ▶ Input: Web domain
 - ▶ Output: Report with usernames, software/server versions, other info
 - ▶ Method: Uses Google search to gather document metadata from a given domain

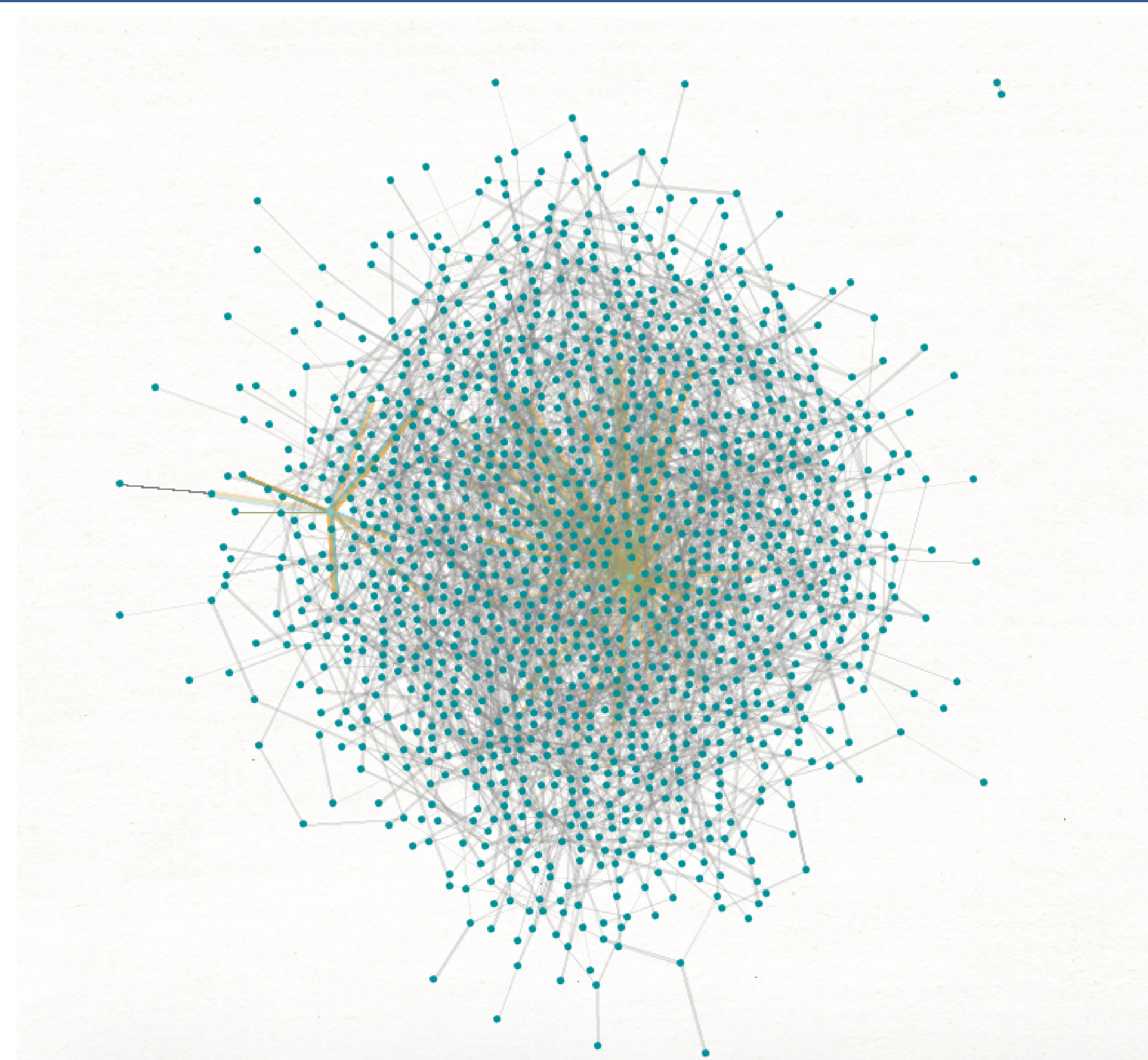
Maltego: Custom Transforms

```

16 @classmethod
17 def create_entities(cls, request, response):
18     domain = request.Value
19     harvester = 'theharvester'
20
21
22     try:
23         subprocess.call(['theharvester'], stdout=subprocess.DEVNULL, stderr=subprocess.DEVNULL)
24     except OSError as e:
25         harvester = 'theHarvester'
26
27     try:
28         sources = ['google', 'bing']
29         f = open('../log.txt', 'w')
30         for source in sources:
31             getResults = subprocess.Popen([harvester, '-d', domain,
32                                           '-b', source], stdout=f, stderr=f)
33             rc = getResults.wait()
34             if rc == 0:
35                 return_code = 0
36             f.close()
37
38         hits = 0
39         if return_code == 0:
40             f = open('../log.txt', 'r')
41             for line in f:
42                 matches = re.findall(r'[\w.-]+@[ \w.-]+', line)
43                 for match in matches:
44                     if match != "cmartorella@edge-security.com":
45                         hits += 1
46                         response.addEntity(Email, match)
47
48         if hits == 0:
49             response.addUIMessage('No emails found :(')
50
51 except IOError:
52     response.addUIMessage("An error occured during IO", messageType=UIM_PARTIAL)

```

Maltego: Network Analysis



Vulnerable Webserver

Features

- ▶ Login page with "Forgot my password" function

Login

Please fill in your credentials to login.

Username | kpeterson

Password

Login

[Forgot your password?](#)

- File download

Hi, kpeterson. Welcome to your personal portal.

[Sign Out of Your Account](#)

Download File [kpeterson/documents/contacts.txt](#)

Download File kpeterson/documents/notes/hiredNotes

Download File [kpeterson/documents/schedule](#)

Capture The Flag (CTF)

OSINT Notifications Users Scoreboard Challenges Admin Profile Settings Logout

Challenges

Corporate Hacking

Unhelpful Desk 5	Welcome Intern 5	More h8 5	Help Desk 5
Forget Me Not 5	MVP 10	Incoming 10	Which Musk 10
Contacts 10	Family comes first 10	Breach 20	More Vulnerabilities? 20
Custom Transform 20	Compromised 25		

Maltego Transform

Transform 1 5	Transform 2 5	Harvesting 5	Transform 0 10
Transform 3 10	More Harvesting 15		