CIS 700/002 : Special Topics : Maltego

Sangdon Park
CIS 700/002: Security of EMBS/CPS/IoT
Department of Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania

March 17, 2017
Brief Introduction

• Software used for reconnaissance
  – Visualize publicly available information
Terminology

• Entity
  – It is represented as a node on a graph and can be anything such as a domain, person, phone number, etc.
  – 20 entities + custom entities

• Transform
  – It is a piece of code that takes one entity to another

• Machine
  – It chains multiple transforms together to automate common/tedious tasks.
Caution!

• Data crawling may be illegal depending on the terms of use of websites

3. Safety

We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to keep Facebook safe, which includes the following commitments by you:
1. You will not post unauthorized commercial communications (such as spam) on Facebook.
2. You will not collect users’ content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.
3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
4. You will not upload viruses or other malicious code.
5. You will not solicit login information or access an account belonging to someone else.
6. You will not bully, intimidate, or harass any user.
7. You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
8. You will not develop or operate a third-party application containing alcohol-related, dating or other mature content (including advertisements) without appropriate age-based restrictions.
9. You will not use Facebook for any purpose intended to harm others or to promote harm to others.
10. You will not do anything that interferes with or hinders the normal operation of Facebook or any other websites.
11. You will not facilitate or encourage any activity that is intended to disrupt or damage Facebook.

PETE WARDEN’S BLOG

Run a machine
Build My Entity Graph from Scratch
Maltego OpenSSL Heartbleed Transform

https://disk0nn3ct.svbtle.com/maltego-openssl-heartbleed-transform
Maltego OpenSSL Heartbleed Transform

Heartbleed test

If there are problems, head to the FAQ

Results are now cached globally for up to 6 hours.

Enter a URL or a hostname to test the server for CVE-2014-0160.

koreabridge.net

Go!

koreabridge.net IS VULNERABLE.
Reference

- cis.upenn.edu/~sangdonp/demomaltego.html
Practice Problems

• Check the heartbleed vulnerability of all webservers under *.cis.upenn.edu domain
• What is the most used server technologies of *.paterva.com sites?