

INTRO TO ETHICAL HACKING
MIS 5211.001
Week 3
Site:
<https://community.mis.temple.edu/mis5211sec702fall2020/>

1

Tonight's Plan

- Reconnaissance

MIS 5211.001 2

2

Reconnaissance

- Attacker gathers publicly available data
 - People
 - Corporate culture
 - Technologies in use
 - Terminology
- This is an important step as it will help focus later activities

MIS 5211.001 3

3

Inventory

- ❑ Maintain an inventory of what you find
 - Keep a log bog
 - Create a spreadsheet
 - Whatever works for you
- ❑ Record key information
 - IP Addresses
 - Target names
 - Search queries used
 - OSs in use
 - Known vulnerabilities
 - Any passwords found

MIS 5211.001 4

4

More on Inventory

- ❑ Leave room to annotate future information that may be discovered as you go
- ❑ Examples:
 - Open ports from port scanning
 - Search from compromised hosts
 - Etc...

MIS 5211.001 5

5

Competitive Intelligence

- ❑ Think like a business competitor
 - Lines of business
 - Major products or services
 - Who's in charge
 - Officers
 - VPs
 - Press Releases
 - Where are their physical locations
 - Who are the major competitors in there market place
- ❑ The same kind of information you would gather for a job interview.

MIS 5211.001 6

6

Search Engines

- ❑ Don't just use Google
 - Bing
 - Yahoo
 - Ask
 - DuckDuckGo
- ❑ All search engines filter data, but they don't all filter the same way

MIS 5211.001 7

7

Google w/ "-"

- ❑ Combine techniques from Google Hacking
- ❑ Site:temple.edu -www.temple.edu

bing site:temple.edu -www.temple.edu

1178 RESULTS

Home | William Sell - African American Abolitionist
<http://www.temple.edu/~sell>
 William Sell, an African American Abolitionist is a collection of digitized textual resources, breaking the life and times of Sell and his family, primarily his

Listserve - Temple University
<http://listserve.temple.edu/>
 Listserve is a collection of electronic discussion groups which are online forums where people discuss a particular topic by receiving and posting.

Ron Levy Group - Temple University - Center for...
<http://list.temple.edu/~ronlevy>
 Welcome to the Ron Levy Group website! The Levy Group moved to Temple University on January 1, 2014. We are very excited about the move! We use a combination of ...

Temple University - Alumni
<http://alumni.temple.edu/>
 Office of Alumni Relations Temple University 100 Sullivan Hall 1330 Park Walk Philadelphia, PA 19122

bing site:temple.edu -www.temple.edu -alumni.temple.edu -listserve

1636 RESULTS

Ron Levy Group - Temple University - Center for...
<http://list.temple.edu/~ronlevy>
 Welcome to the Ron Levy Group website! The Levy Group moved to Temple University on January 1, 2014. We are very excited about the move! We use a combination of ...

Fort Washington Campus - Temple University
<http://www.temple.edu/~fwcampus>
 Credit courses for adult learners at the Graduate and Professional Education Center. Includes programs, analysis, and forms of graduation.

Parking Information | Admissions - Temple University
admissions.temple.edu/visit/parking-information
 Office of Undergraduate Admissions, 1801 North Broad St., Council Hall 103 Philadelphia, PA 19122 610.526.0206, Directories & Accommodations Parking Information

Fall Open House | Admissions - Temple University
admissions.temple.edu/visit/open-house
 Office of Undergraduate Admissions, 1801 North Broad St., Council Hall 103 Philadelphia, PA 19122 610.526.0206, Directories & Accommodations Parking Information

MIS 5211.001 8

8

Older Versions of Websites

- ❑ WayBack Machine
 - <http://archive.org/web/web.php>

INTERNET ARCHIVE

<http://temple.edu>
 Saved **1,821 Times** between **January 8, 1997** and **September 9, 2014**.


PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.

MIS 5211.001 9

9

Open Job Posting

- ❑ Job requirements can often provide insight into technologies in use, and where staffing shortages may result in weaknesses
- ❑ Check multiple sites
 - Monster.com
 - Dice.com
 - Organizations site
 - ❑ http://www.temple.edu/hr/departments/employment/jobs_within.htm
 - Local job sites
 - ❑ <http://regionalhelpwanted.com/philadelphia-jobs/?sn=83>



MIS 5211.001 10

10

People

- ❑ LinkedIn
- ❑ Facebook



MIS 5211.001 11

11

Don't Forget About Maps

- ❑ Google Maps
- ❑ MapQuest
- ❑ Google Earth



MIS 5211.001 12

12

Dig (Domain Information Groper)

- ❑ The Dig command is used to gather additional DNS information
- ❑ May also be used to make zone transfers.
- ❑ Zone transfers may include details around other assets within an organization.
- ❑ **CAUTION, don't go further than basic dig command on the next page as you may start triggering alerts in more security focused organizations.**

MIS 5211.001

19

19

Dig

- ❑ Example:

```

tester@ubuntu:~$ dig temple.edu
<<>> DIG 9.9.5-3-Ubuntu <<> temple.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44428
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: 0, MBZ: 0005 , udp: 4000
;; QUESTION SECTION:
;temple.edu.                IN      A
;; ANSWER SECTION:
temple.edu.                5      IN      A      155.247.166.60
;; Query time: 28 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Sep 09 19:52:17 PDT 2014
;; MSG SIZE rcvd: 55
tester@ubuntu:~$

```

MIS 5211.001

20

20

More on Dig

- ❑ <http://www.thegeekstuff.com/2012/02/dig-command-examples/>
- ❑ <http://www.cyberciti.biz/faq/linux-unix-dig-command-examples-usage-syntax/>

MIS 5211.001

21

21

Windows Dig

- ❑ Dig is available for windows 7
- ❑ Site:
 - <https://help.dyn.com/how-to-use-binds-dig-tool/>

MIS 5211.001 22

22

DNS Query Websites

- ❑ <http://dnsquery.org/> ★
- ❑ <http://network-tools.com/nslook/>

MIS 5211.001 23

23

More Tools


- ❑ Sensepost
 - <https://github.com/sensepost>
 - BiLE-Suite - The Bi-directional Link Extractor
 - A suite of perl scripts to find targets related to a given site

MIS 5211.001 24

24

Google Cache

- The little green down arrow



This is Google's cache of <http://www.temple.edu>. It is a snapshot of the page as it appeared on Sep 9, 2014 14:55:06 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

To quickly find your search term on this page, press Ctrl or ⌘ (Mac) and use the first bar.

MIS 5211.001 25

25

Google Cache

- &strip=1 - It's magic
- Right click the cache button and copy shortcut
- Paste short cut into notepad and append &strip=1 to the end
- Copy and paste into URL
- Now you get Google's cache without leaving a footprint in the target servers logs

MIS 5211.001 26

26

Google Cache (Example)

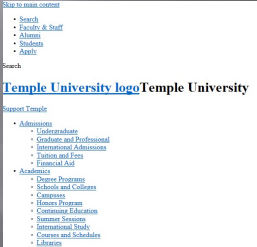
- Without &strip=1



MIS 5211.001 27

27

❑ With &strip=1



The screenshot shows a navigation menu for Temple University. The menu items are: Home, Faculty & Staff, Alumni, Students, and Search. Below the menu is a search bar with the text 'Temple University logo Temple University'. Underneath the search bar is a 'Support Temple' section with a list of links: Admissions (Undergraduate, Graduate and Professional, International Admissions, Tuition and Fees, Transfer Aid), Academic (Degree Programs, Schools and Colleges, Learning, Honors Program, Continuing Education, Summer Sessions, International Study, Courses and Schedules, Library).

MIS 5211.001 28

28

Ruby

❑ If interested in learning a bit about Ruby, try the below. This is **not** an assignment for the class. Just something you might find useful.

❑ Link to Language

- <https://www.ruby-lang.org/en/>

❑ Link to Interactive Ruby Website

- <https://ruby.github.io/TryRuby/>

29

29

Due for Next Week

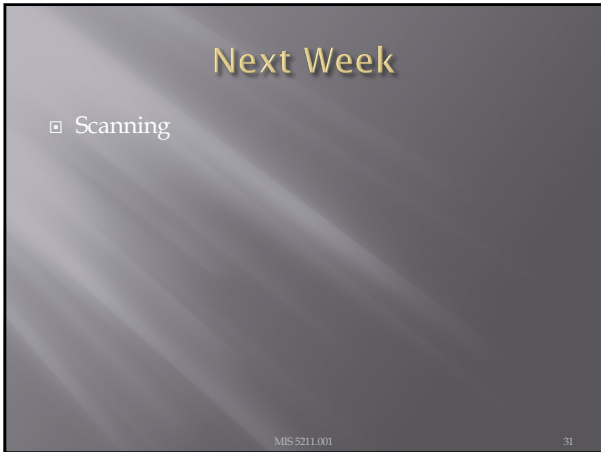
❑ 1st formal assignment

❑ From Syllabus

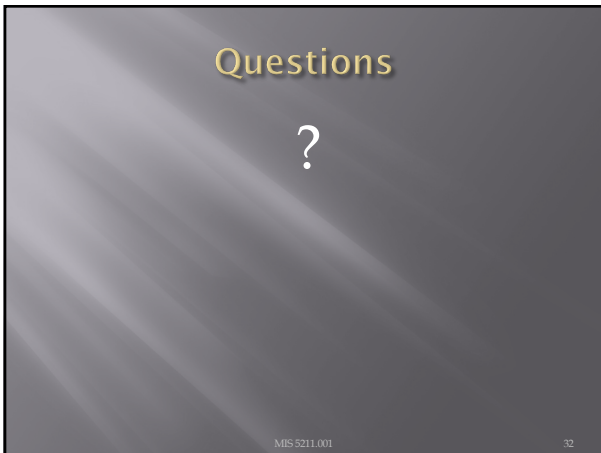
- (student presentations) Reconnaissance exercise using only publicly available information, develop a profile of a public company or organization of your choosing
- You may work in teams, or separately
 - One to two page Executive Summary
 - Short (no more than three slides, no welcome slide) presentation
 - See "Exercise Analysis" tab for more details

30

30



31



32
