

**INTRO TO ETHICAL HACKING**

MIS 5211.701  
Week 3  
Site:  
<https://community.mis.temple.edu/mis5211sec701fall2020/>

---

---

---

---

---

---

---

---

1

**Tonight's Plan**

- Reconnaissance

MIS 5211.701 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 5211.701 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 5211.701

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 5211.701

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 5211.701

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 5211.701

7

7

---

---

---

---

---

---

---

---

---

---

## Google w/ " - "

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

The image shows two Bing search results side-by-side. The left result shows search results for 'site:temple.edu -www.temple.edu' with a list of links including 'Home | William Still: An African-American Abolitionist', 'Listserv - Temple University', 'Ron Levy Group - Temple University - Center for...', and 'Temple University - Alumni'. The right result shows search results for 'site:temple.edu -www.temple.edu -alumni.temple.edu -listserv' with links for 'Ron Levy Group - Temple University - Center for...', 'Fort Washington Campus - Temple University', 'Parking Information | Admissions - Temple University', and 'Fall Open House | Admissions - Temple University'.

MIS 5211.701

8

8

---

---

---

---

---

---

---

---

---

---

## Older Versions of Websites

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

The image is a screenshot of the WayBack Machine interface. At the top, it says 'INTERNET ARCHIVE' and 'Wayback Machine'. Below that, there is a search bar with 'http://temple.edu' entered and a 'BROWSE HISTORY' button. A message states 'Saved 1,821 times between June 6, 1997 and September 9, 2014.' Below this is a bar chart showing the frequency of captures over time. At the bottom, there is a calendar grid for the months of January, February, March, and April, with specific dates highlighted in blue, indicating when the website was archived.

MIS 5211.701

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](http://www.temple.edu/hr/departments/employment/jobs_within.htm)
  - Local job sites
    - <http://regionalhelpwanted.com/philadelphia-jobs/?sn=83>



MIS 5211.701 10

10

---

---

---

---

---

---

---

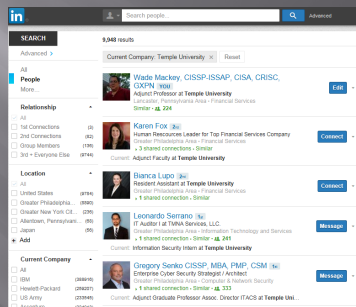
---

---

---

# People

- LinkedIn
- Facebook



MIS 5211.701 11

11

---

---

---

---

---

---

---

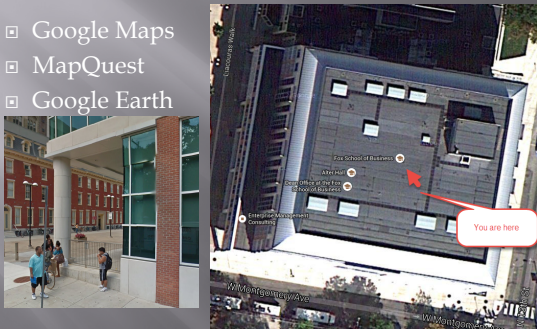
---

---

---

# Don't Forget About Maps

- Google Maps
- MapQuest
- Google Earth



MIS 5211.701 12

12

---

---

---

---

---

---

---

---

---

---

# Whois

- Whois
  - Database to lookup domain name, IP address and who registered the address
  - Web based or Command Line
    - whois google.com
  - <http://www.networksolutions.com/whois/index.jsp>

```

buster@buntu:~$ whois google.com
whois Server Version 2.0
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Server Name: GOOGLE.COM.AFTRICAMATS.ORG
Registrar: TUCOWS DOMAINS INC.
WHOIS Server: whois.TUCOWS.COM
Referral URL: http://donathelp.opensrs.net
      
```

WHOIS information for temple.edu:™

[Querying whois.education.net]  
 [Temp.edu.edu.edu.edu]

The Registry database contains WHOIS (EDU) domains. The data in the EDUCAUSE Whois database is provided to EDUCAUSE for information purposes in order to assist in the process of obtaining information about or related to who domain registrants names. The EDUCAUSE Whois database is authoritative for the EDU domain.

A Web interface for the EDU EDUCAUSE Whois Server is available at <http://whois.education.net>

In submitting a whois query, you agree that this information will not be used to drive, enable, or otherwise assist, in the registration of intellectual commercial advertising or publications via e-mail. The use of electronic procedures to harvest information from this service is generally prohibited, except as reasonably necessary to register or modify, add domain entries.

You may use "!" as a wildcard in your search. For further information regarding the use of the WHOIS server, please type: help

Domain Name: TEMPLE.EDU  
 Registrar: Temple University  
 180 N. Broad Street  
 Philadelphia, PA 19122  
 NETC@TEMPLE.EDU  
 Administrative Contact: Enterprise Systems Group  
 Temple University Computer Services  
 On Our Website: http://www.temple.edu  
 180 N. Broad Street  
 Philadelphia, PA 19122  
 NETC@TEMPLE.EDU  
 (215) 264-5335  
 whois@temple.edu  
 Technical Contact: Enterprise Systems Group  
 Temple University Computer Services  
 On Our Website: http://www.temple.edu  
 180 N. Broad Street  
 Philadelphia, PA 19122  
 NETC@TEMPLE.EDU  
 (215) 264-5335  
 whois@temple.edu

Name Server: NS1.TEMPLE.EDU 155.247.181.2, NS200.104.7000.100  
 NS2.TEMPLE.EDU 155.247.181.2, NS300.104.7000.100  
 Domain record last updated: 09-Jun-2014  
 Domain expires: 31-Jul-2015

13



# ARIN

- American Registry for Internet Numbers
  - Regional Internet Registry for US, Canada, and many Caribbean islands
  - ARIN is one of five regional registries
  - Provides services related to the technical coordination and management of Internet number resources
  - <https://www.arin.net>

14



# ARIN

## Results

Your IPv4 address is 97.454.173.150 SEARCH WHOIS help

all requests subject to terms of use [advanced search](#)

NUMBER RESOURCES | PARTICIPATE | POLICIES | FEES & INVOICES | KNOWLEDGE | ABOUT US | FEEDBACK

Organizations	Network Resources
<b>Temple University (TEMPLE)</b> Organization: Temple University Name: TEMPLE Street: Commonwealth Building, Room 870 Broad and Springdale, Philadelphia City: Philadelphia State/Province: PA Postal Code: 19122 Country: US Registrar Date: 1987-07-21 Last Updated: 2011-04-24 Comments: WHOIS Link: <a href="http://whois.arin.net/show/TEMPLE">http://whois.arin.net/show/TEMPLE</a> Web Site: <a href="http://www.temple.edu">http://www.temple.edu</a> See Also: Postal administrative system numbers See Also: Postal POC records	AMBLER (NET-192.41.174.0-1) 192.41.174.0 - 192.41.174.255 PENNLINK (NET-192.41.173.0-1) 192.41.173.0 - 192.41.173.255 FENNLINK (NET-192.41.175.0-1) 192.41.175.0 - 192.41.175.255 TEMPLE-RC (NET-192.41.176.0-1) 192.41.176.0 - 192.41.176.255 TYLER (NET-192.41.178.0-1) 192.41.178.0 - 192.41.178.255 TEMPLE-EDU (NET-155.247.0-1) 155.247.0.0 - 155.247.255.255 TEMPLE (NET-129.32.0-1) 129.32.0.0 - 129.32.255.255 TEMPLE-V6 (NET6-2020-104-7000-1) 2020.104.7000.0 - 2020.104.7000.ffff ffff ffff ffff

15





## 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-5211.701

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: MBZ: 0005 , udp: 4096
;; 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-5211.701

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-5211.701

21

21

---

---

---

---

---

---

---

---

## Windows Dig

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

MIS 5211.701

22

22

---

---

---

---

---

---

---

---

## DNS Query Websites

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

MIS 5211.701

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 5211.701

24

24

---

---

---

---

---

---

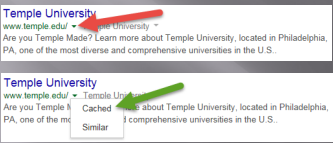
---

---



## 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 14:55:05 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

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

MIS 5211.701 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 5211.701 26

---

---

---

---

---

---

---

---

---

---

26

## Google Cache (Example)

- Without &strip=1



MIS 5211.701 27

---

---

---

---

---

---

---

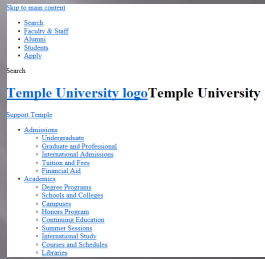
---

---

---

27

- With &strip=1



MIS 5211.701

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

- 1<sup>st</sup> 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
  - Work Independently
    - One to two page Executive Summary
    - Short (no more than three slides, no welcome slide) presentation
    - See "Exercise Analysis" tab for more details

MIS 5211.701

30

30

---

---

---

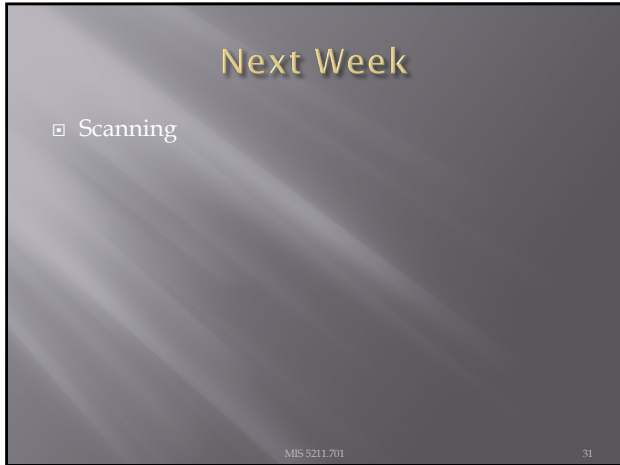
---

---

---

---

---



31

---

---

---

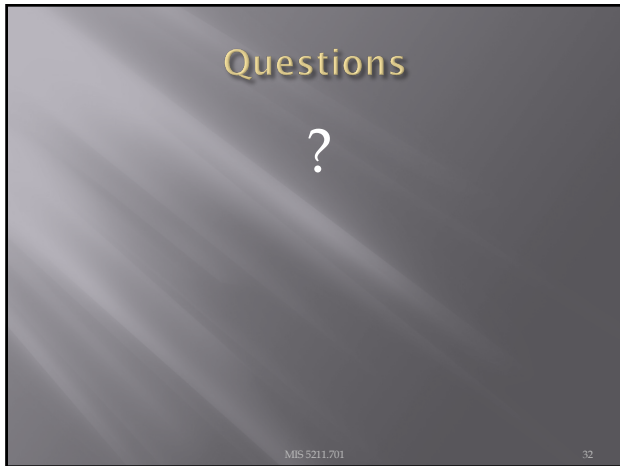
---

---

---

---

---



32

---

---

---

---

---

---

---

---