

INTRO TO ETHICAL HACKING

MIS 5211.701

Week 3

Site:

<http://community.mis.temple.edu/mis5211sec701fall2018/>

Tonight's Plan

- Network Components (Continued)
- Google Hacking
- Reconnaissance

MIS 5211.701

2

Google Hacking

- Search Bar Commands
 - -
 - Site:
 - Filetype:
 - Inurl:
 - Intitle:
 - Intext:
 - Allinurl:
 - Allintext:
 - Search Terms

MIS 5211.701

3

- Simple one that tells google to not include items that match what comes directly after "-"
- Example:
- Hacking -ethical - gives all results that include information about hacking as long as they do not include the term "ethical"

MIS 5211.701 4

Site:

- Site: restricts searches to a specific site
- Examples
 - Site:edu - Restricts searches to only sites ending in .edu
 - Site:temple.edu - Restricts searches to a specific top level site
 - Site:mis.temple.edu -Restricts searches to a sub-site

MIS 5211.701 5

Filetype:

- Restricts searches to a specific file type
- Examples
 - Filetype:pdf - Only responds with sites linked to Adobe documents with file extension of pdf
 - Filetype:xls - Only responds with sites linked to Microsoft spreadsheets documents with file extension of xls
 - Filetype:xlsx - Only responds with sites linked to Microsoft spreadsheets documents with file extension of xlsx - Excel's newer file format

MIS 5211.701 6

Inurl:

- Restricts searches to sites where specific word or phrase is in the url
- Examples
 - inurl:"/root/etc/passwd"
 - inurl:admin
 - inurl;j2ee/examples/jsp
 - inurl:backup

MIS 5211.701

7

Intitle:

- Restricts searches to sites where specific words are used in the title of a page
- Examples
 - intitle:index.of
 - intitle:"Test Page for Apache"
 - intitle:"Apache Status"
 - intitle:"PHP Explorer"

MIS 5211.701

8

Intext:

- Restricts results to documents containing term in the text
- Examples
 - intext:"root:x:0:0:root:/root:/bin/bash"
 - intext:"SteamUserPassphrase="
 - intext:"SteamAppUser=" -"username" -"user"
 - intext:"Usage Statistics for"

MIS 5211.701

9

Allinurl:

- Restricts results to those containing all the query terms you specify in the URL
- Examples
 - allinurl:/hide_my_wp=
 - allinurl:"/main/auth/profile.php"
 - allinurl:"owa/auth/logon.aspx"
 - allinurl:forcedownload.php?file=

Allintext:

- Restricts results to those containing all the query terms you specify in the text of the page
- Examples:
 - allintext: /iissamples/default/
 - allintext: "Please login to continue..."
 - allintext:"Browse our directory of our members top sites or create your own for free!"
 - allintext:"fs-admin.php"

Search Terms

- Key search terms
 - "index of /"
 - "Please re-enter your password it must match"

Google Hacking References

- GoogleGuide
 - http://www.googleguide.com/advanced_operators_reference.html
- Exploit Database
 - <http://www.exploit-db.com/>
- Wikipedia
 - http://en.wikipedia.org/wiki/Google_hacking
- Google Hacking Volume 3
 - https://www.amazon.com/Google-Hacking-Penetration-Testers-Third/dp/0128029641/ref=dp_ob_title_bk

MIS 5211.701

13

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

14

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

15

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

16

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

17

Search Engines

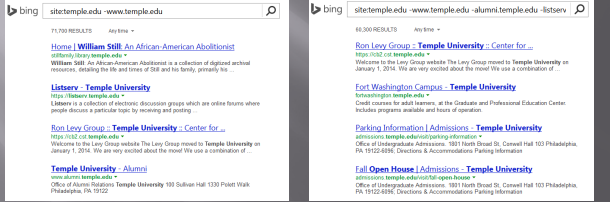
- Don't just use Google
 - Bing
 - Yahoo
 - Ask
 - DuckDuckGo
- All search engines filter data, but they don't all filter the same way

MIS 5211.701

18

Google w/ “-”

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

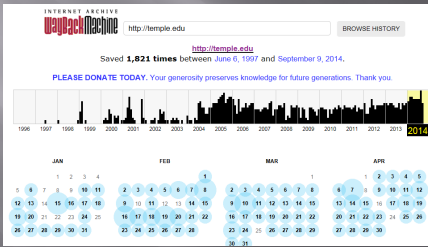


MIS 5211.701

19

Older Versions of Websites

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



MIS 5211.701

20

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>

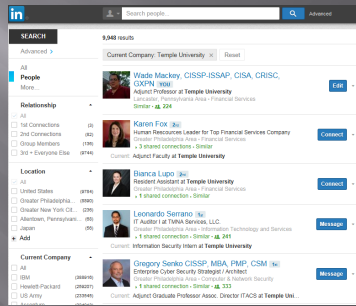


MIS 5211.701

21

People

- LinkedIn
- Facebook



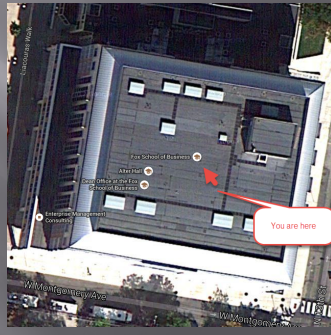
MIS 5211.701

22



Don't Forget About Maps

- Google Maps
- MapQuest
- Google Earth



MIS 5211.701

23



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>

```

tester@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.AFRICANMATS.ORG
Registrar: TUCOWS DOMAINS, INC.
Whois Server: whois.tucows.com
Referral URL: http://donahelp.opensrs.net
  
```

MIS 5211.701

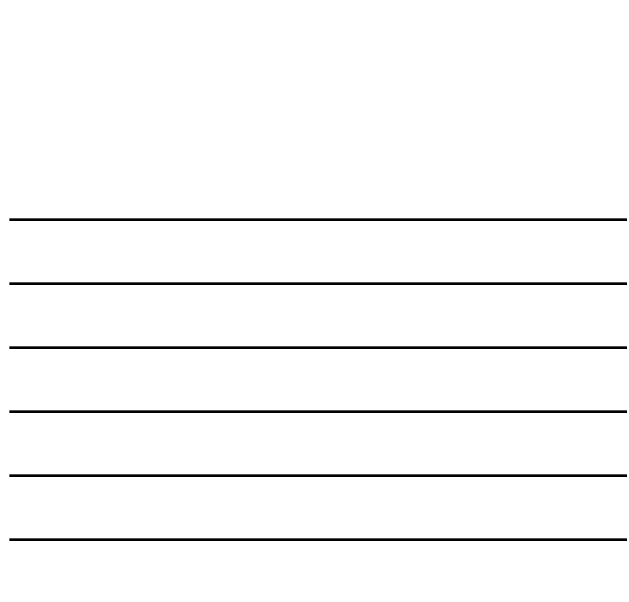
24

WHOIS information for temple.edu**

```

Observing whois.education.net
whois.whois.google.com
The Registry database contains ONLY .EDU domains.
The data in the EDUWHOIS Whois database is provided
to EDUWHOIS for information purposes in order to
assist in the process of obtaining information about
a domain to allow domain registrars to identify
the domain's registrant information for the
EDUWHOIS.
A whois member for the EDUWHOIS Whois Server is
available at: http://whois.education.net
By submitting a whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail. The use of electronic processes to
harvest information from this server is generally prohibited
except as necessarily necessary to register or modify an
EDUWHOIS member.
This whois page is an unauthenticated view. For further
information regarding the use of this WHOIS server, please
refer to: http://www.whois.edu

Domain Name: TEMPLE.EDU
Registrar:
Temple University
700 Four Westman Hall
380 S. Broad Street
Philadelphia, PA 19122
(610)222-3123
Administrative Contact:
Extension Systems Group
Temple University Computer Services
700 Four Westman Hall
380 S. Broad Street
Philadelphia, PA 19122
(610)222-3123
Technical Contact:
Extension Systems Group
Temple University Computer Services
700 Four Westman Hall
380 S. Broad Street
Philadelphia, PA 19122
(610)222-3123
Name Servers:
NS1.TEMPLE.EDU 155.247.194.2, 2000.104.7008.100
NS2.TEMPLE.EDU 155.247.194.2, 2000.104.7008.100
Domain Record Activated: 27-May-1987
Domain Record Expiration: 08-Jun-2004
Domain Expires: 31-Mar-2015
  
```



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

MIS 5211.701

25

ARIN

Results

Organizations

Temple University (TEMPLE)

Organization		Network Resources	
Name	Temple University	AMBLER (NET-192.41.174.0-1)	192.41.174.0 - 192.41.174.255
Handle	TEMPLE	FENNLINK (NET-192.41.173.0-1)	192.41.173.0 - 192.41.173.255
Street	Constitution Building, Room 670 Broad and Locust Streets, Philadelphia	TEMPLE-RC (NET-192.41.176.0-1)	192.41.176.0 - 192.41.176.255
City	Philadelphia	TYLOR (NET-192.41.175.0-1)	192.41.175.0 - 192.41.175.255
State/Province	PA	TEMPLE-DCU (NET-192.247.0-1)	192.247.0 - 192.247.255
Postal Code	19122	TEMPLE (NET-129.32.0-1)	129.32.0 - 129.32.255
Country	US	TEMPLE-V6 (NET6-2020-104-7000-1)	2020.104.7000 - 2020.104.7000.FFFF.FFFF.FFFF.FFFF
Registration Date	1997-04-21		
Last Updated	2011-04-25		
Comments	http://www.temple.edu/TEMPLE		
RESTM Link	http://ahnes.ann.netrestbox/TEMPLE		
See Also	Related organizations		
See Also	Related address system numbers		
See Also	Related IPSEC services		

MIS 5211.701

26

ARIN

Function	Point of Contact
Tech	FERRE3-ARIN (FERRE3-ARIN)
Abuse	FERRE3-ARIN (FERRE3-ARIN)
Admin	FERRE3-ARIN (FERRE3-ARIN)

Point of Contact

Name	Ferrero, Adam
Handle	FERRE3-ARIN
Company	Temple University
Street	3rd floor Telecommunications 1102 N. Montgomery Avenue
City	Philadelphia
State/Province	PA
Postal Code	19122
Country	US
Registration Date	2011-04-25
Last Updated	2014-07-02
Comments	http://www.temple.edu/ica +1-215-862-6600 (Office) +1-215-862-6600 (Office)
Email	adam@temple.edu
RESTM Link	http://ahnes.ann.netrestbox/FERRE3-ARIN
See Also	Related organizations

MIS 5211.701

27

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: 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 5211.701

31

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

32

Windows Dig

- Dig is available for windows 7
- Site:
 - <http://www.isc.org/downloads/bind/>

MIS 5211.701

33

DNS Query Websites

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

MIS 5211.701

34

More Tools

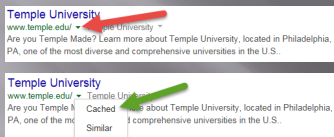
- Sensepost
 - <https://github.com/sensepost>
 - BiLE-Suite - The Bi-directional Link Extractor
 - A suite of perl scripts to find targets related to a given site

MIS 5211.701

35

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 5, 2014 14:55:06 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

Tip: To quickly find your search term on this page, press **Ctrl-F** or **⌘ F** (Mac) and use the find bar.

MIS 5211.701

36

Google Cache

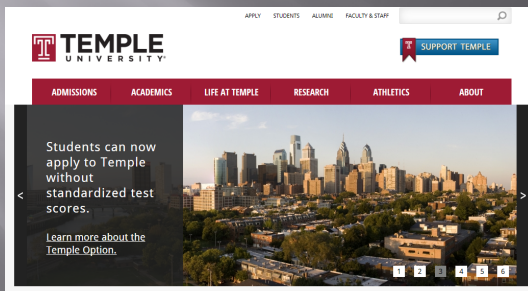
- &strip=1 - It's magic
- Right click the cache button and copy shortcut
- Paste short cut into notepad and append &strip=1 to the end
- Copy and paste into URL
- Now you get Google's cache without leaving a footprint in the target servers logs

MIS 5211.701

37

Google Cache (Example)

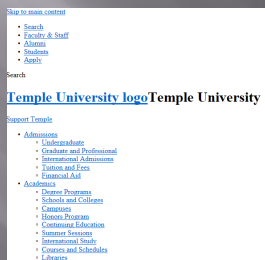
- Without &strip=1



MIS 5211.701

38

- With &strip=1



MIS 5211.701

39

Ruby

- Link to Language
 - <https://www.ruby-lang.org/en/>
- Link to Interactive Ruby Website
 - <https://ruby.github.io/TryRuby/>
- Work through exercise section labeled “Hey, Summary #1 Already” down to “Elemental”

MIS 5211.701 40

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

MIS 5211.701 41

Next Week

- Scanning

MIS 5211.701 42

