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

Google Hacking

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

-

- 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"

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

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

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

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"

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"

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

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

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

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…

Competitive Intelligence

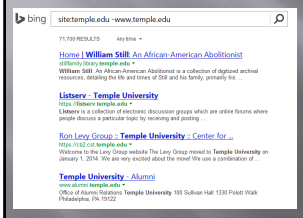
- Think like a business competitor
  - Lines of business
  - Major products or services
  - Who's in charge
    - Officers
    - VPs
  - Press Releases
  - Where are their physical locations
  - Who are the major competitors in there market place
- The same kind of information you would gather for a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

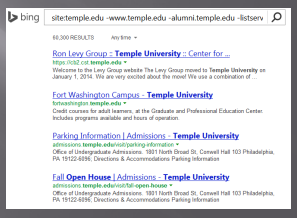
Search Engines

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

Google w/ "-"

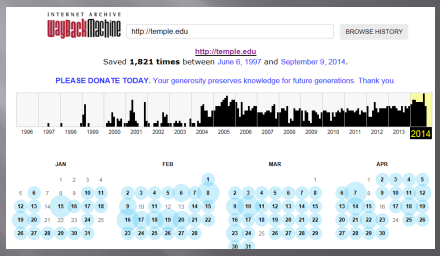
- Combine techniques from Google Hacking
- Site:temple.edu -www.temple.edu





Older Versions of Websites

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

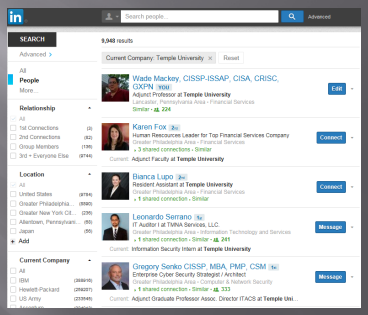


Open Job Posting

- 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

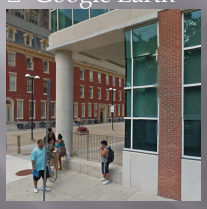
People

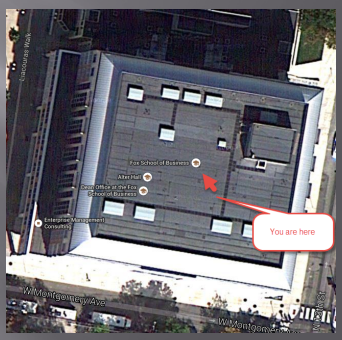
- LinkedIn
- Facebook



Don't Forget About Maps

- Google Maps
- MapQuest
- Google Earth





Whois

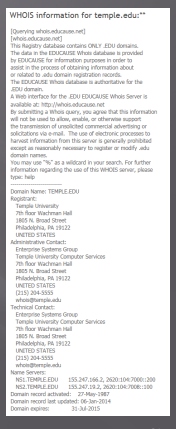
- Whois
  - Database to lookup domain name, IP address and who registered the address
  - Web based or Command Line
    - whois google.com
  - http://www.networksolutions.com/whois/index.jsp

```
tester@ubuntu:~$ 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.AFRICANBATS.ORG
   Registrar: TUCOWS DOMAINS INC.
   Whois Server: whois.tucows.com
   Referral URL: http://domainhelp.opensrs.net
```

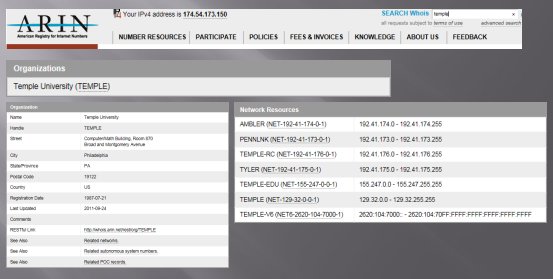


ARIN

- 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

ARIN

- Results



ARIN

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

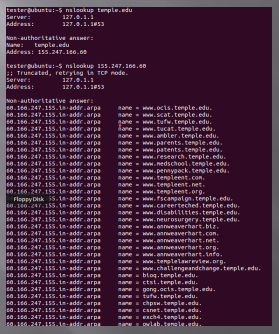
Point of Contact

Name	Ferrero , Adam
Handle	FERRE3-ARIN
Company	Temple University
Street	3rd floor Telecommunications 1101 W 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/cs
Phone	+1-267-[redacted] (Mobile) +1-215-[redacted] (Office)
Email	adam@temple.edu
RESTful Link	http://whois.arin.net/rest/poc/FERRE3-ARIN
See Also	Related organizations.

DNS

- Querying DNS Server
  - Examples
    - By domain name
      - Nslookup temple.edu OR nslookup ns1.temple.edu
    - Interactive
      - Nslookup
      - Followed by prompts
      - See next slide
      - Type exit to get out of interactive mode

DNS



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 then basic dig command on the next page as you may start triggering alerts in more security focused organizations.

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:~$
```


More on Dig

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

Windows Dig

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

DNS Query Websites

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

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

Google Cache

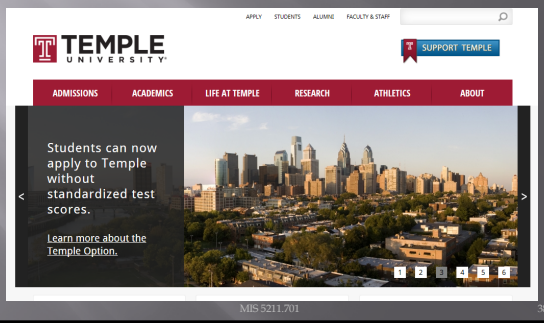
- The little green down arrow

Google Cache

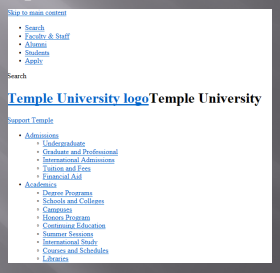
- &strip=1 – It's magic
- Right click the cache button and copy shortcut
- Paste short cut into notepad and append &strip=1 to the end
- Copy and paste into URL
- Now you get Google's cache without leaving a footprint in the target servers logs

Google Cache (Example)

- Without &strip=1



- With &strip=1



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"

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 then three slides, no welcome slide) presentation
    - See "Exercise Analysis" tab for more details

Next Week

- Scanning


Questions
?
MIS 5211.701
43