CMSC389R

OSINT and OPSEC

COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

recap

Successful setup?

OSINT Handbook

Ethics Writeup

Questions?

announcements

Majority of submission received via ELMS

Make sure to push your HW to your github, too

We are pulling the repos at 11:59 PM deadline day

Any questions from last week?

kali

Demo

(tools, usage, wordlists, etc)

passive intelligence gathering

- OSINT: Open-Source Intelligence
  - Collection
  - Exploitation
  - Dissemination

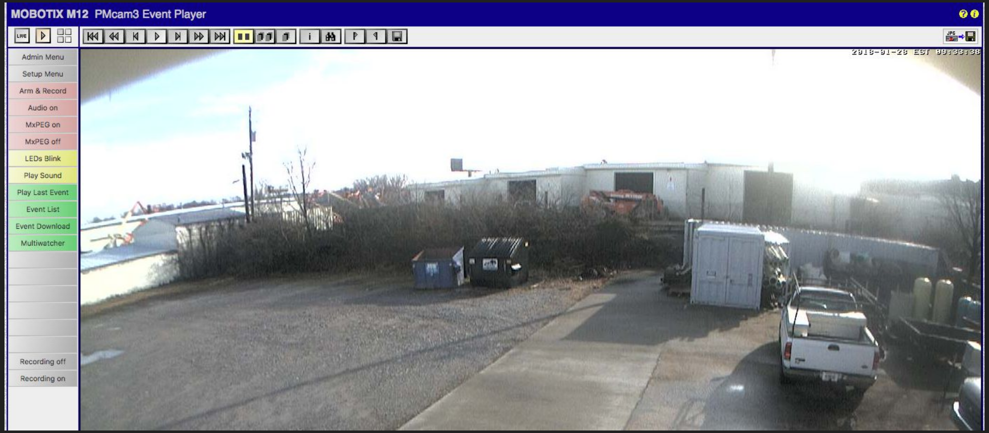
of publicly available information for a particular intelligence requirement.

OSINT

- Tailored searches (ie. dorks, etc.)
- Web services (ie. Bazzell’s OSINT techniques, centralops, Shodan/Censys, Google, WayBack, Facebook, etc.)
- CLI (ie. whois, nmap, theharvester, etc.)

Example: IP cameras

- Google hacking!
  - www.exploit-db.com/google-hacking
- inurl:control/multiview
- "This file was generated by Nessus"

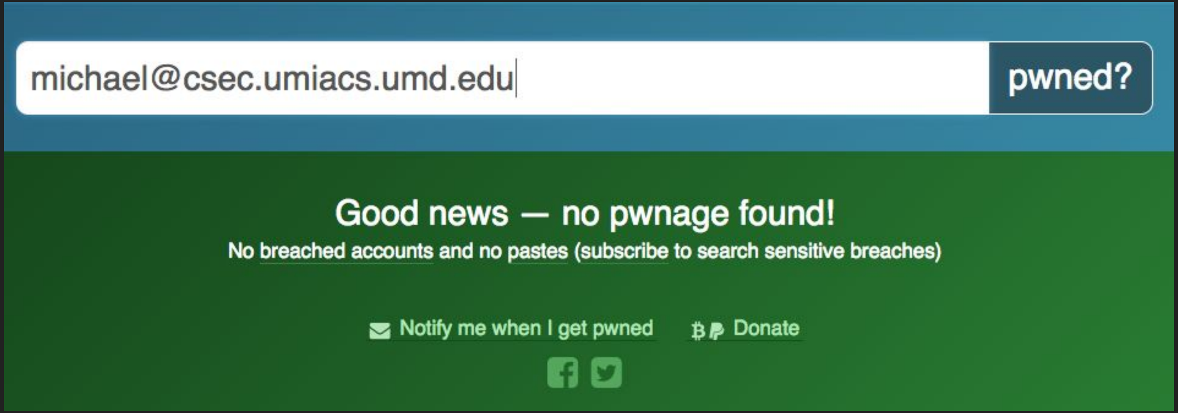


Example: pastebin.com

- Most popular paste site on the web
    - https://pastebin.com
- … or search across multiple paste sites:
    - https://inteltechniques.com/osint/menu.pastebins.html
- https://twitter.com/PastebinLeaks (old)

Example: haveibeenpwned.com

- “Check if you have an account that has been compromised in a data breach”
    - https://haveibeenpwned.com



michael@csec.umiacs.umd.edu

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

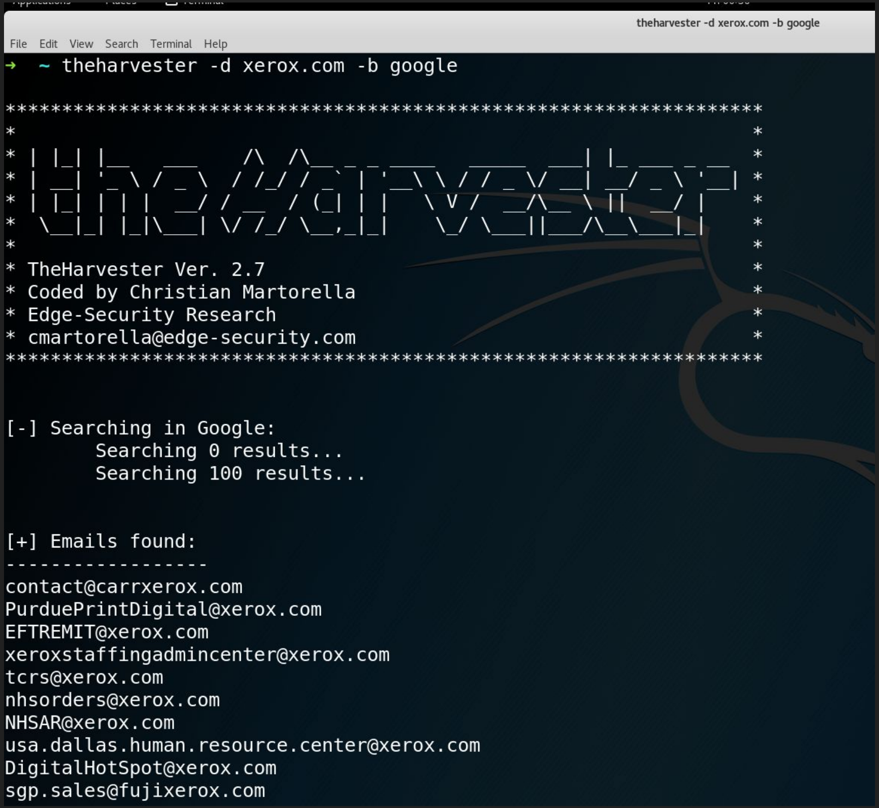
Example: nmap

- Port scanner
    - Displays services/OS/etc… of an IP address(es)
    - https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
- Very noisy
    - The network admin will see you nmap’ing them

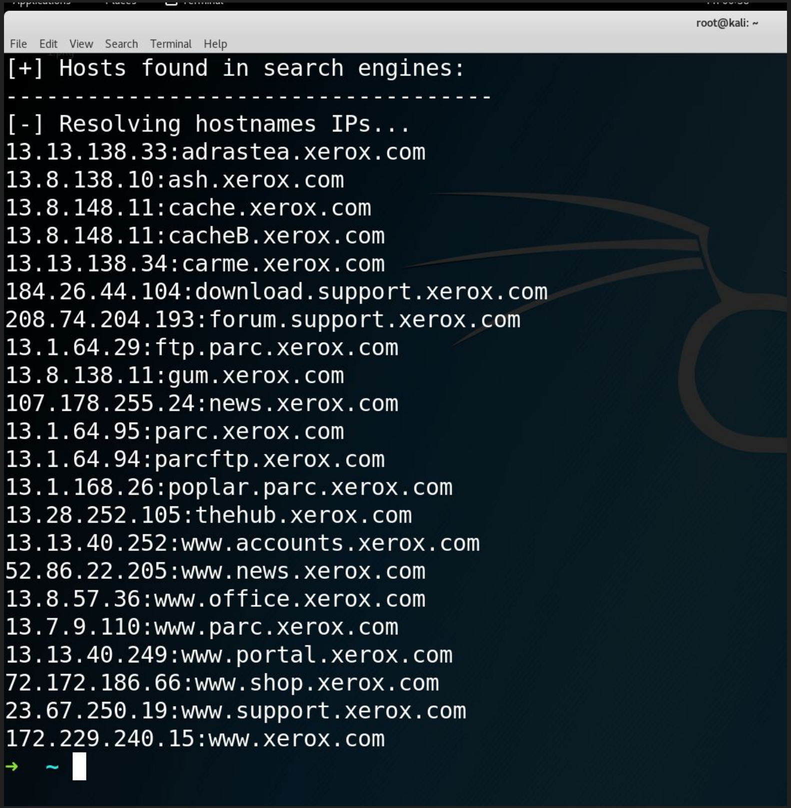
Example: shodan & censys

- Search the Internet for devices
  - https://www.shodan.io
  - https://censys.io
- What if…
  - http://www.defaultpassword.com

Example: theharvester


theharvester -d xerox.com -b google
File Edit View Search Terminal Help

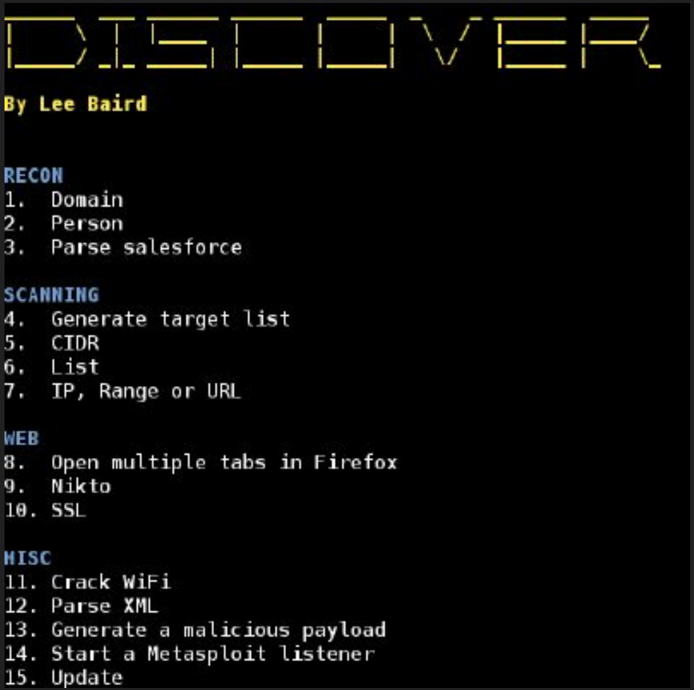
```
➜  ~ theharvester -d xerox.com -b google

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.7                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...


[+] Emails found:
------------------
contact@carrxerox.com
PurduePrintDigital@xerox.com
EFTREMIT@xerox.com
xeroxstaffingadmincenter@xerox.com
tcrs@xerox.com
nhsorders@xerox.com
NHSAR@xerox.com
usa.dallas.human.resource.center@xerox.com
DigitalHotSpot@xerox.com
sgp.sales@fujixerox.com
```



```
[+] Hosts found in search engines:
------------------------------------
[-] Resolving hostnames IPs...
13.13.138.33:adrastea.xerox.com
13.8.138.10:ash.xerox.com
13.8.148.11:cache.xerox.com
13.8.148.11:cacheB.xerox.com
13.13.138.34:carme.xerox.com
184.26.44.104:download.support.xerox.com
208.74.204.193:forum.support.xerox.com
13.1.64.29:ftp.parc.xerox.com
13.8.138.11:gum.xerox.com
107.178.255.24:news.xerox.com
13.1.64.95:parc.xerox.com
13.1.64.94:parcftp.xerox.com
13.1.168.26:poplar.parc.xerox.com
13.28.252.105:thehub.xerox.com
13.13.40.252:www.accounts.xerox.com
52.86.22.205:www.news.xerox.com
13.8.57.36:www.office.xerox.com
13.7.9.110:www.parc.xerox.com
13.13.40.249:www.portal.xerox.com
72.172.186.66:www.shop.xerox.com
23.67.250.19:www.support.xerox.com
172.229.240.15:www.xerox.com
➜  ~ 
```

Example: discover

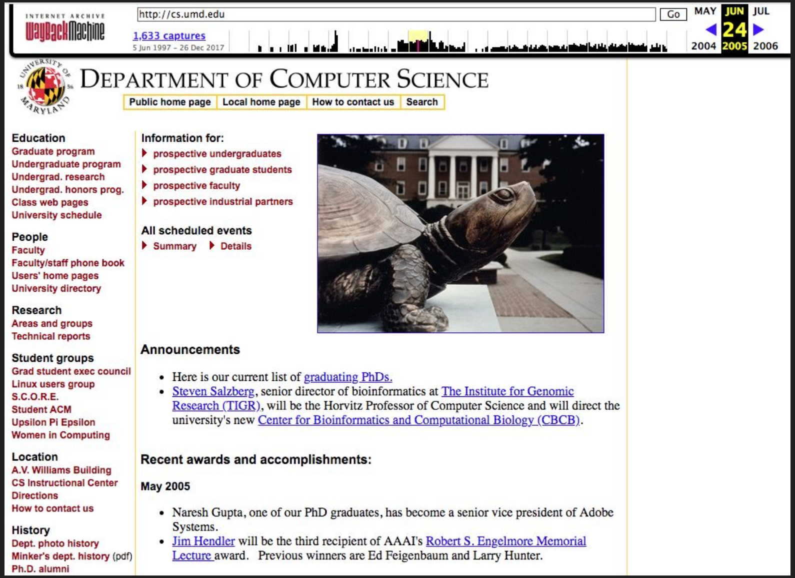
- Automated OSINT scripts
  - Follow installation instructions
  - https://github.com/leebaird/discover



```
By Lee Baird

RECON
1.  Domain
2.  Person
3.  Parse salesforce

SCANNING
4.  Generate target list
5.  CIDR
6.  List
7.  IP, Range or URL

WEB
8.  Open multiple tabs in Firefox
9.  Nikto
10. SSL

MISC
11. Crack WiFi
12. Parse XML
13. Generate a malicious payload
14. Start a Metasploit listener
15. Update
```

Example: wayback machine

- View the historical changes of a website
  - ○ https://archive.org/web



DEPARTMENT OF COMPUTER SCIENCE

Public home page | Local home page | How to contact us | Search

Education
Graduate program
Undergraduate program
Undergrad. research
Undergrad. honors prog.
Class web pages
University schedule

People
Faculty
Faculty/staff phone book
Users' home pages
University directory

Research
Areas and groups
Technical reports

Student groups
Grad student exec council
Linux users group
S.C.O.R.E.
Student ACM
Upsilon Pi Epsilon
Women in Computing

Location
A.V. Williams Building
CS Instructional Center
Directions
How to contact us

History
Dept. photo history
Minker's dept. history (pdf)
Ph.D. alumni

Information for:
- prospective undergraduates
- prospective graduate students
- prospective faculty
- prospective industrial partners

All scheduled events
Summary · Details

Announcements

- Here is our current list of graduating PhDs.
- Steven Salzberg, senior director of bioinformatics at The Institute for Genomic Research (TIGR), will be the Horvitz Professor of Computer Science and will direct the university's new Center for Bioinformatics and Computational Biology (CBCB).

Recent awards and accomplishments:

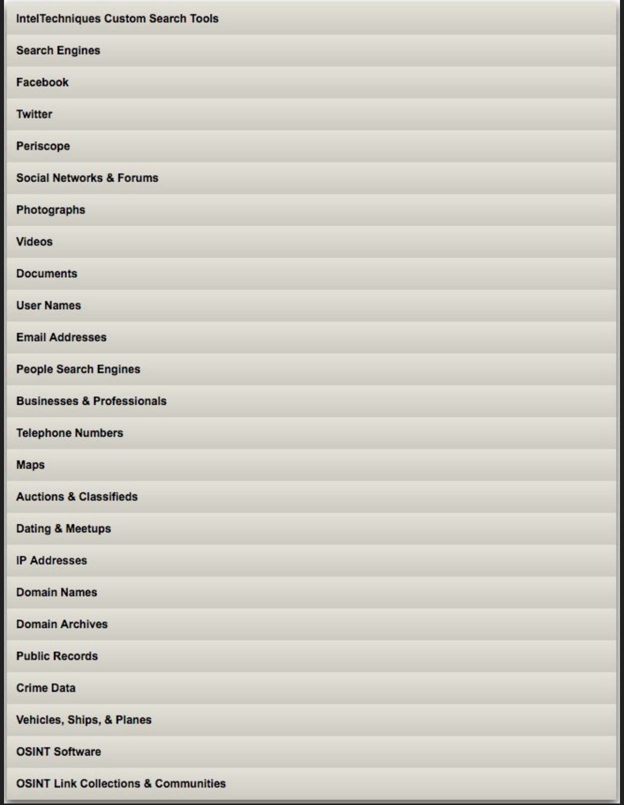
May 2005

- Naresh Gupta, one of our PhD graduates, has become a senior vice president of Adobe Systems.
- Jim Hendler will be the third recipient of AAAI's Robert S. Engelmore Memorial Lecture award. Previous winners are Ed Feigenbaum and Larry Hunter.

Example: IntelTechniques

https://inteltechniques.com/

https://inteltechniques.com/buscador/ (VM)



IntelTechniques Custom Search Tools

Search Engines

Facebook

Twitter

Periscope

Social Networks & Forums

Photographs

Videos

Documents

User Names

Email Addresses

People Search Engines

Businesses & Professionals

Telephone Numbers

Maps

Auctions & Classifieds

Dating & Meetups

IP Addresses

Domain Names

Domain Archives

Public Records

Crime Data

Vehicles, Ships, & Planes

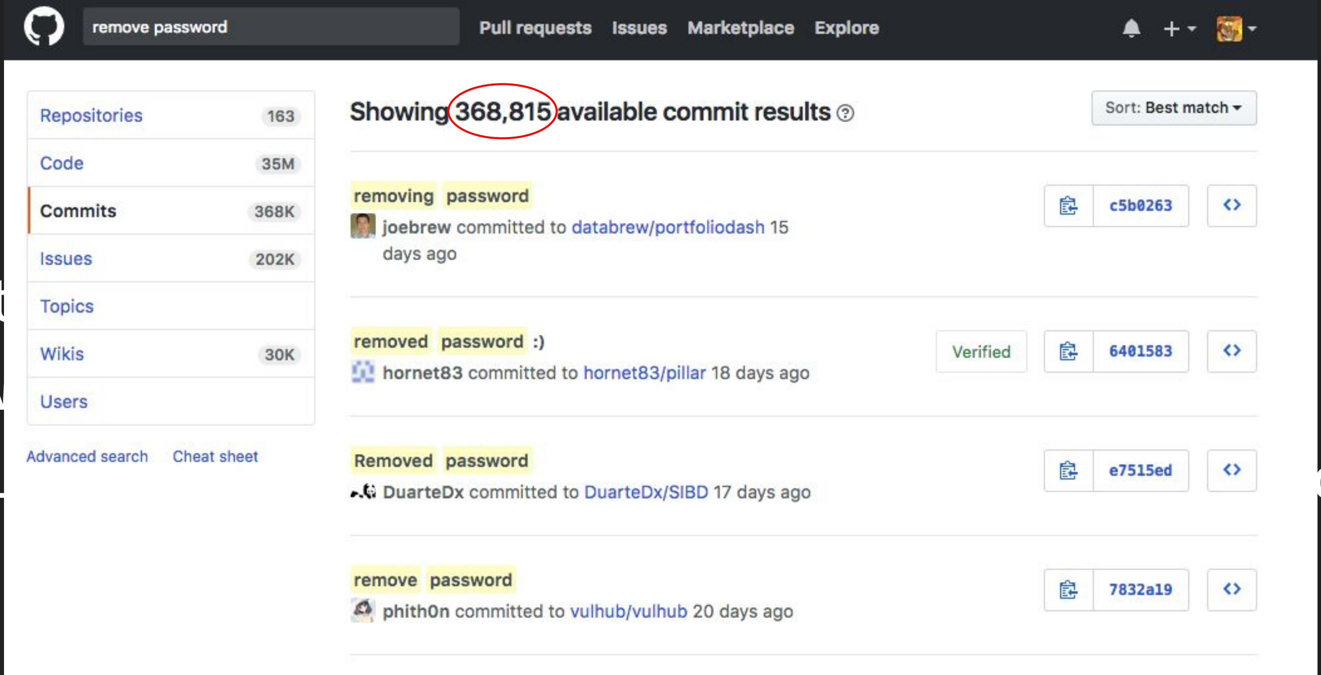
OSINT Software

OSINT Link Collections & Communities

Example: Github

- Hosted version control
  - Where open-source code lives
  - Look for git commits and changes to code

- Host
  - W
  - L de



remove password

Pull requests Issues Marketplace Explore

Repositories	163
Code	35M
Commits	368K
Issues	202K
Topics	
Wikis	30K
Users	

Advanced search Cheat sheet

Showing 368,815 available commit results

Sort: Best match

removing password
joebrew committed to databrew/portfoliodash 15 days ago
c5b0263

removed password :)
hornet83 committed to hornet83/pillar 18 days ago
Verified 6401583

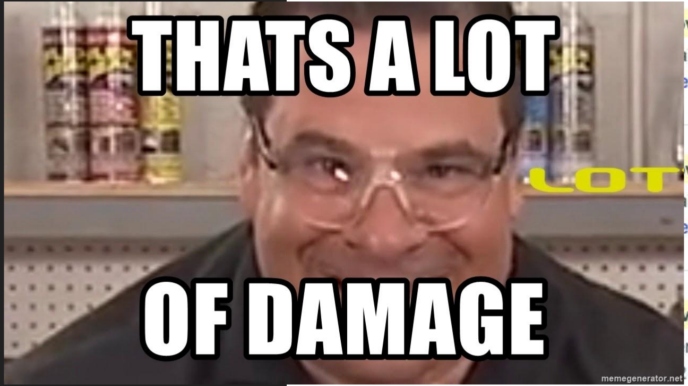
Removed password
DuarteDx committed to DuarteDx/SIBD 17 days ago
e7515ed

remove password
phith0n committed to vulhub/vulhub 20 days ago
7832a19

ved password
ileyJM02 committed to
elioNetworks/HelioLinkExchange 19 days ago
c677f62

ved password
ileyJM02 committed to
elioNetworks/HelioLinkExchange 19 days ago
94cd7f2

ved passwords
remy committed to hsloan1a/ChatBotWithContext
days ago
3 585db5d



Example: whois

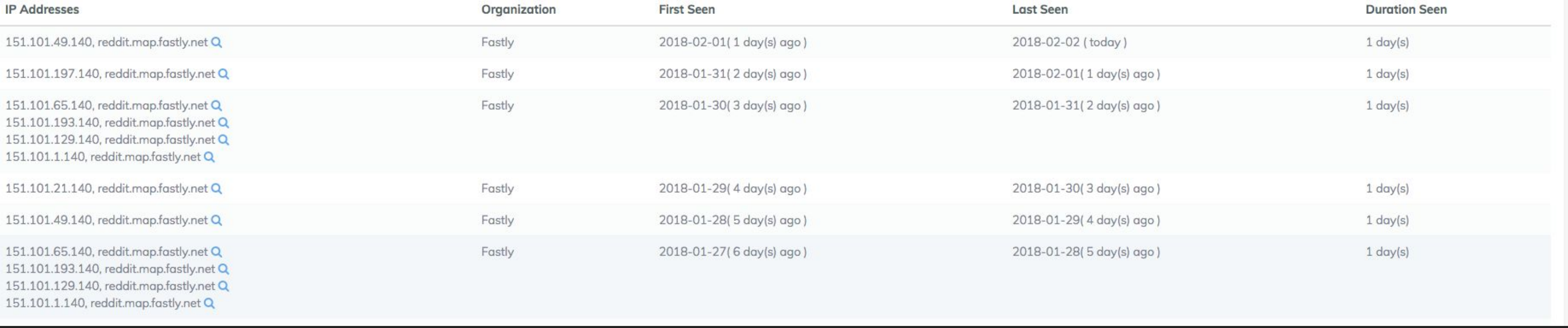
```
$ whois umd.edu
```

Or… if you prefer the web:

https://centralops.net/co/DomainDossier.aspx

Example: dnstrails.com

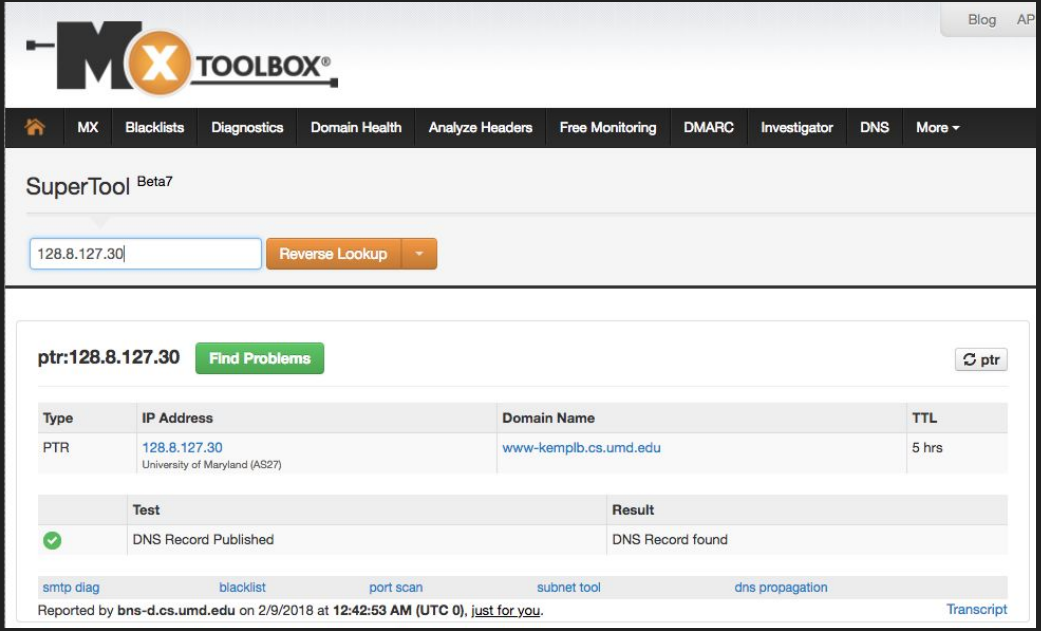
- Repository of historical DNS records
  - https://dnstrails.com/



IP Addresses	Organization	First Seen	Last Seen	Duration Seen
151.101.49.140, reddit.map.fastly.net 🔍	Fastly	2018-02-01(1 day(s) ago)	2018-02-02 (today)	1 day(s)
151.101.197.140, reddit.map.fastly.net 🔍	Fastly	2018-01-31(2 day(s) ago)	2018-02-01(1 day(s) ago)	1 day(s)
151.101.65.140, reddit.map.fastly.net 🔍 151.101.193.140, reddit.map.fastly.net 🔍 151.101.129.140, reddit.map.fastly.net 🔍 151.101.1.140, reddit.map.fastly.net 🔍	Fastly	2018-01-30(3 day(s) ago)	2018-01-31(2 day(s) ago)	1 day(s)
151.101.21.140, reddit.map.fastly.net 🔍	Fastly	2018-01-29(4 day(s) ago)	2018-01-30(3 day(s) ago)	1 day(s)
151.101.49.140, reddit.map.fastly.net 🔍	Fastly	2018-01-28(5 day(s) ago)	2018-01-29(4 day(s) ago)	1 day(s)
151.101.65.140, reddit.map.fastly.net 🔍 151.101.193.140, reddit.map.fastly.net 🔍 151.101.129.140, reddit.map.fastly.net 🔍 151.101.1.140, reddit.map.fastly.net 🔍	Fastly	2018-01-27(6 day(s) ago)	2018-01-28(5 day(s) ago)	1 day(s)

Example: reverse dns

- https://mxtoolbox.com/ReverseLookup.aspx



ptr:128.8.127.30

Type	IP Address	Domain Name	TTL
PTR	128.8.127.30 University of Maryland (AS27)	www-kemplb.cs.umd.edu	5 hrs

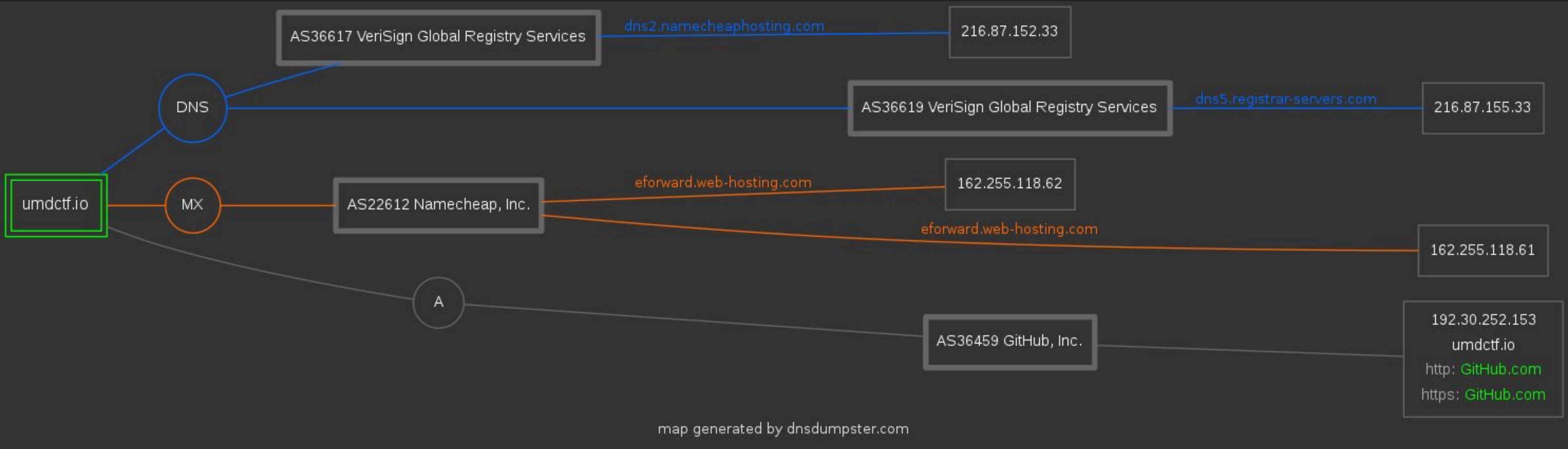
	Test	Result
✓	DNS Record Published	DNS Record found

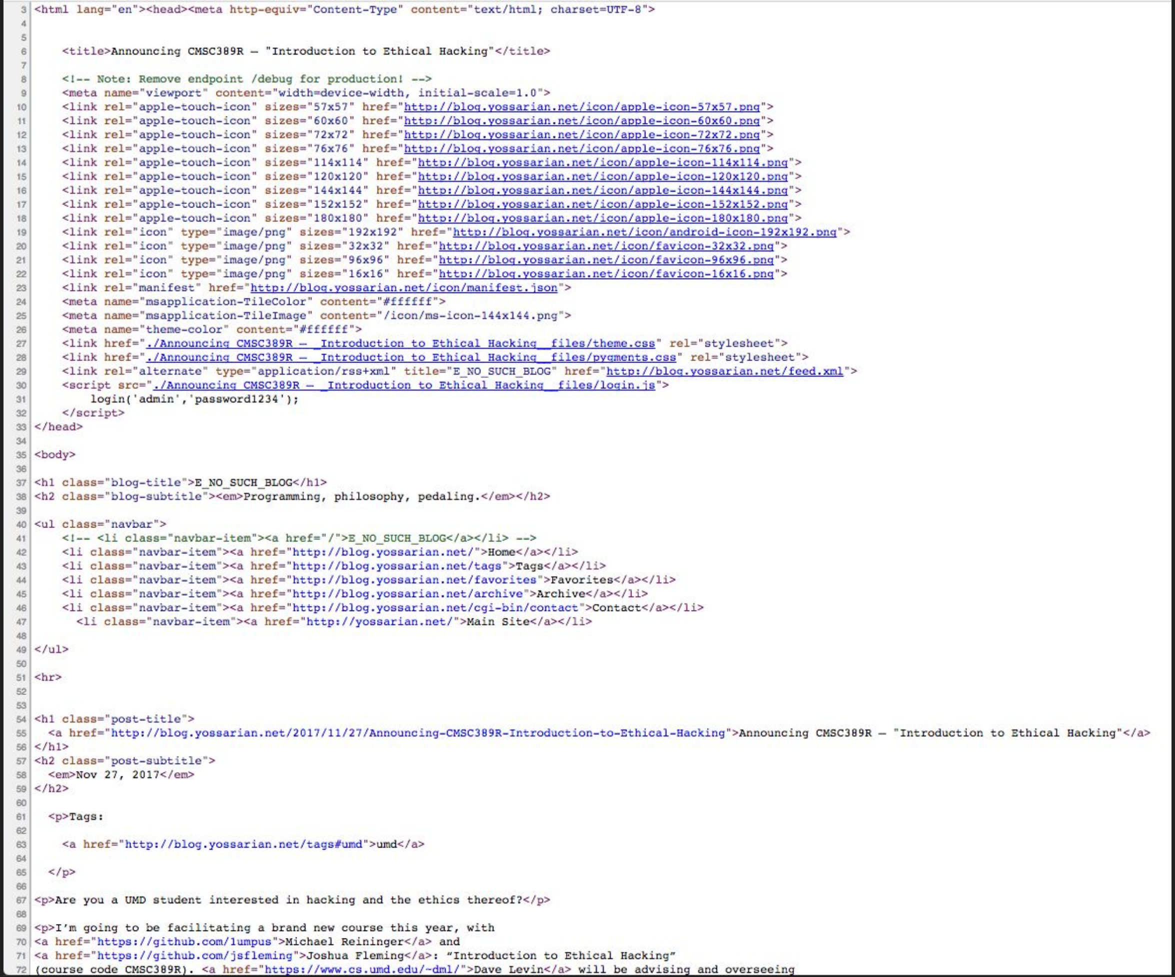
smtp diag blacklist port scan subnet tool dns propagation

Reported by **bns-d.cs.umd.edu** on 2/9/2018 at **12:42:53 AM (UTC 0)**, just for you. Transcript

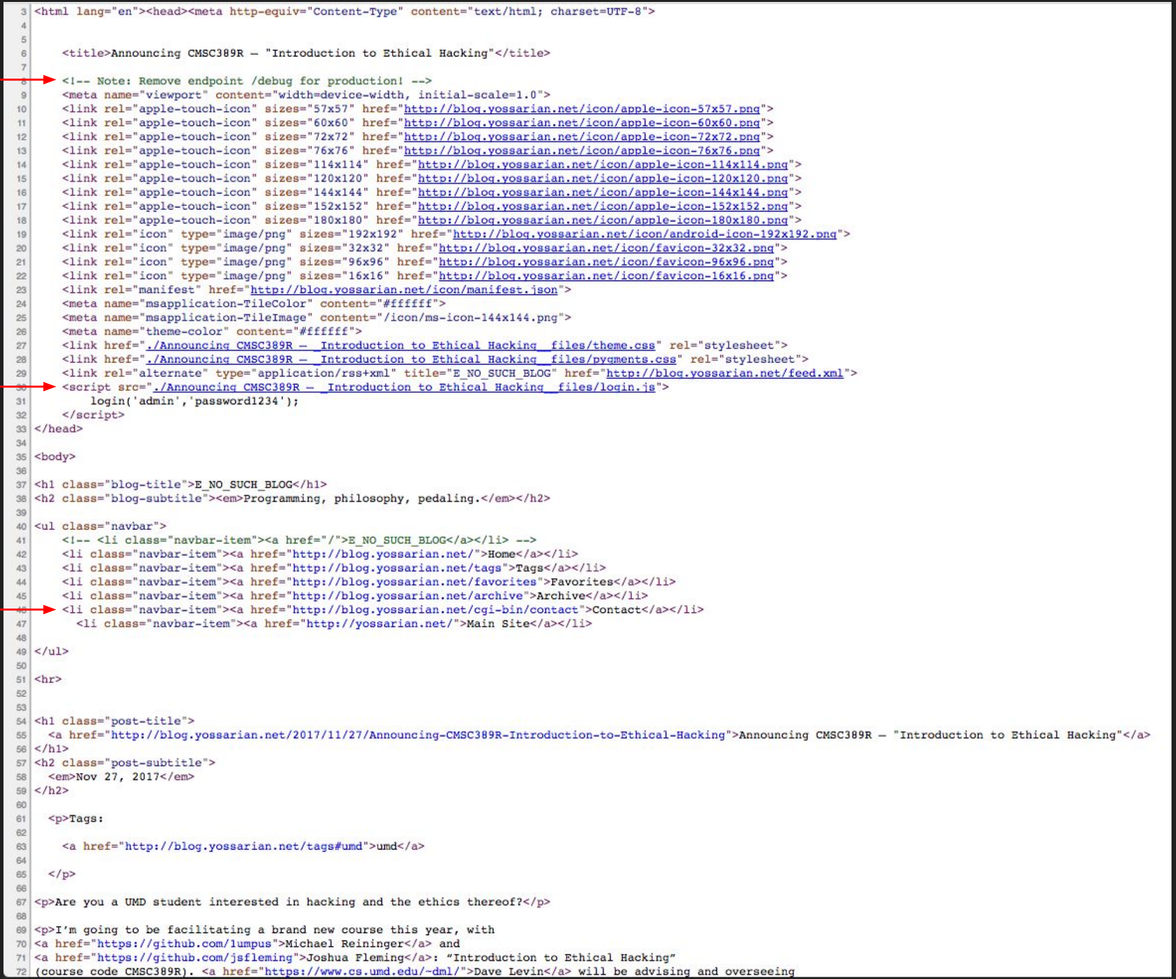
Example: dnsdumpster.com

- https://dnsdumpster.com





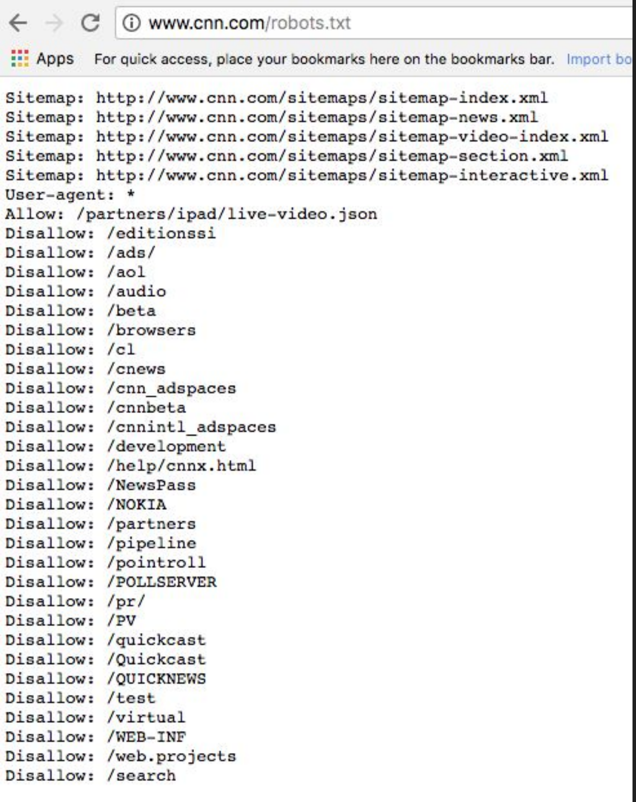
```html
<html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">


    <title>Announcing CMSC389R — "Introduction to Ethical Hacking"</title>

    <!-- Note: Remove endpoint /debug for production! -->
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="apple-touch-icon" sizes="57x57" href="http://blog.yossarian.net/icon/apple-icon-57x57.png">
    <link rel="apple-touch-icon" sizes="60x60" href="http://blog.yossarian.net/icon/apple-icon-60x60.png">
    <link rel="apple-touch-icon" sizes="72x72" href="http://blog.yossarian.net/icon/apple-icon-72x72.png">
    <link rel="apple-touch-icon" sizes="76x76" href="http://blog.yossarian.net/icon/apple-icon-76x76.png">
    <link rel="apple-touch-icon" sizes="114x114" href="http://blog.yossarian.net/icon/apple-icon-114x114.png">
    <link rel="apple-touch-icon" sizes="120x120" href="http://blog.yossarian.net/icon/apple-icon-120x120.png">
    <link rel="apple-touch-icon" sizes="144x144" href="http://blog.yossarian.net/icon/apple-icon-144x144.png">
    <link rel="apple-touch-icon" sizes="152x152" href="http://blog.yossarian.net/icon/apple-icon-152x152.png">
    <link rel="apple-touch-icon" sizes="180x180" href="http://blog.yossarian.net/icon/apple-icon-180x180.png">
    <link rel="icon" type="image/png" sizes="192x192" href="http://blog.yossarian.net/icon/android-icon-192x192.png">
    <link rel="icon" type="image/png" sizes="32x32" href="http://blog.yossarian.net/icon/favicon-32x32.png">
    <link rel="icon" type="image/png" sizes="96x96" href="http://blog.yossarian.net/icon/favicon-96x96.png">
    <link rel="icon" type="image/png" sizes="16x16" href="http://blog.yossarian.net/icon/favicon-16x16.png">
    <link rel="manifest" href="http://blog.yossarian.net/icon/manifest.json">
    <meta name="msapplication-TileColor" content="#ffffff">
    <meta name="msapplication-TileImage" content="/icon/ms-icon-144x144.png">
    <meta name="theme-color" content="#ffffff">
    <link href="./Announcing CMSC389R — _Introduction to Ethical Hacking__files/theme.css" rel="stylesheet">
    <link href="./Announcing CMSC389R — _Introduction to Ethical Hacking__files/pygments.css" rel="stylesheet">
    <link rel="alternate" type="application/rss+xml" title="E_NO_SUCH_BLOG" href="http://blog.yossarian.net/feed.xml">
    <script src="./Announcing CMSC389R — _Introduction to Ethical Hacking__files/login.js">
        login('admin','password1234');
    </script>
</head>

<body>

<h1 class="blog-title">E_NO_SUCH_BLOG</h1>
<h2 class="blog-subtitle"><em>Programming, philosophy, pedaling.</em></h2>

<ul class="navbar">
    <!-- <li class="navbar-item"><a href="/">E_NO_SUCH_BLOG</a></li> -->
    <li class="navbar-item"><a href="http://blog.yossarian.net/">Home</a></li>
    <li class="navbar-item"><a href="http://blog.yossarian.net/tags">Tags</a></li>
    <li class="navbar-item"><a href="http://blog.yossarian.net/favorites">Favorites</a></li>
    <li class="navbar-item"><a href="http://blog.yossarian.net/archive">Archive</a></li>
    <li class="navbar-item"><a href="http://blog.yossarian.net/cgi-bin/contact">Contact</a></li>
      <li class="navbar-item"><a href="http://yossarian.net/">Main Site</a></li>

</ul>

<hr>


<h1 class="post-title">
  <a href="http://blog.yossarian.net/2017/11/27/Announcing-CMSC389R-Introduction-to-Ethical-Hacking">Announcing CMSC389R — "Introduction to Ethical Hacking"</a>
</h1>
<h2 class="post-subtitle">
  <em>Nov 27, 2017</em>
</h2>

  <p>Tags:

    <a href="http://blog.yossarian.net/tags#umd">umd</a>

  </p>

<p>Are you a UMD student interested in hacking and the ethics thereof?</p>

<p>I’m going to be facilitating a brand new course this year, with
<a href="https://github.com/1umpus">Michael Reininger</a> and
<a href="https://github.com/jsfleming">Joshua Fleming</a>: “Introduction to Ethical Hacking”
(course code CMSC389R). <a href="https://www.cs.umd.edu/~dml/">Dave Levin</a> will be advising and overseeing
```



```html
<html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">


    <title>Announcing CMSC389R – "Introduction to Ethical Hacking"</title>

    <!-- Note: Remove endpoint /debug for production! -->
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="apple-touch-icon" sizes="57x57" href="http://blog.yossarian.net/icon/apple-icon-57x57.png">
    <link rel="apple-touch-icon" sizes="60x60" href="http://blog.yossarian.net/icon/apple-icon-60x60.png">
    <link rel="apple-touch-icon" sizes="72x72" href="http://blog.yossarian.net/icon/apple-icon-72x72.png">
    <link rel="apple-touch-icon" sizes="76x76" href="http://blog.yossarian.net/icon/apple-icon-76x76.png">
    <link rel="apple-touch-icon" sizes="114x114" href="http://blog.yossarian.net/icon/apple-icon-114x114.png">
    <link rel="apple-touch-icon" sizes="120x120" href="http://blog.yossarian.net/icon/apple-icon-120x120.png">
    <link rel="apple-touch-icon" sizes="144x144" href="http://blog.yossarian.net/icon/apple-icon-144x144.png">
    <link rel="apple-touch-icon" sizes="152x152" href="http://blog.yossarian.net/icon/apple-icon-152x152.png">
    <link rel="apple-touch-icon" sizes="180x180" href="http://blog.yossarian.net/icon/apple-icon-180x180.png">
    <link rel="icon" type="image/png" sizes="192x192" href="http://blog.yossarian.net/icon/android-icon-192x192.png">
    <link rel="icon" type="image/png" sizes="32x32" href="http://blog.yossarian.net/icon/favicon-32x32.png">
    <link rel="icon" type="image/png" sizes="96x96" href="http://blog.yossarian.net/icon/favicon-96x96.png">
    <link rel="icon" type="image/png" sizes="16x16" href="http://blog.yossarian.net/icon/favicon-16x16.png">
    <link rel="manifest" href="http://blog.yossarian.net/icon/manifest.json">
    <meta name="msapplication-TileColor" content="#ffffff">
    <meta name="msapplication-TileImage" content="/icon/ms-icon-144x144.png">
    <meta name="theme-color" content="#ffffff">
    <link href="./Announcing CMSC389R – _Introduction to Ethical Hacking__files/theme.css" rel="stylesheet">
    <link href="./Announcing CMSC389R – _Introduction to Ethical Hacking__files/pygments.css" rel="stylesheet">
    <link rel="alternate" type="application/rss+xml" title="E_NO_SUCH_BLOG" href="http://blog.yossarian.net/feed.xml">
    <script src="./Announcing CMSC389R – _Introduction to Ethical Hacking__files/login.js">
        login('admin','password1234');
    </script>
</head>

<body>

<h1 class="blog-title">E_NO_SUCH_BLOG</h1>
<h2 class="blog-subtitle"><em>Programming, philosophy, pedaling.</em></h2>

<ul class="navbar">
    <!-- <li class="navbar-item"><a href="/">E_NO_SUCH_BLOG</a></li> -->
    <li class="navbar-item"><a href="http://blog.yossarian.net/">Home</a></li>
    <li class="navbar-item"><a href="http://blog.yossarian.net/tags">Tags</a></li>
    <li class="navbar-item"><a href="http://blog.yossarian.net/favorites">Favorites</a></li>
    <li class="navbar-item"><a href="http://blog.yossarian.net/archive">Archive</a></li>
    <li class="navbar-item"><a href="http://blog.yossarian.net/cgi-bin/contact">Contact</a></li>
      <li class="navbar-item"><a href="http://yossarian.net/">Main Site</a></li>

</ul>

<hr>


<h1 class="post-title">
  <a href="http://blog.yossarian.net/2017/11/27/Announcing-CMSC389R-Introduction-to-Ethical-Hacking">Announcing CMSC389R – "Introduction to Ethical Hacking"</a>
</h1>
<h2 class="post-subtitle">
  <em>Nov 27, 2017</em>
</h2>

  <p>Tags:

    <a href="http://blog.yossarian.net/tags#umd">umd</a>

  </p>

<p>Are you a UMD student interested in hacking and the ethics thereof?</p>

<p>I’m going to be facilitating a brand new course this year, with
<a href="https://github.com/1umpus">Michael Reininger</a> and
<a href="https://github.com/jsfleming">Joshua Fleming</a>: “Introduction to Ethical Hacking”
(course code CMSC389R). <a href="https://www.cs.umd.edu/~dml/">Dave Levin</a> will be advising and overseeing
```

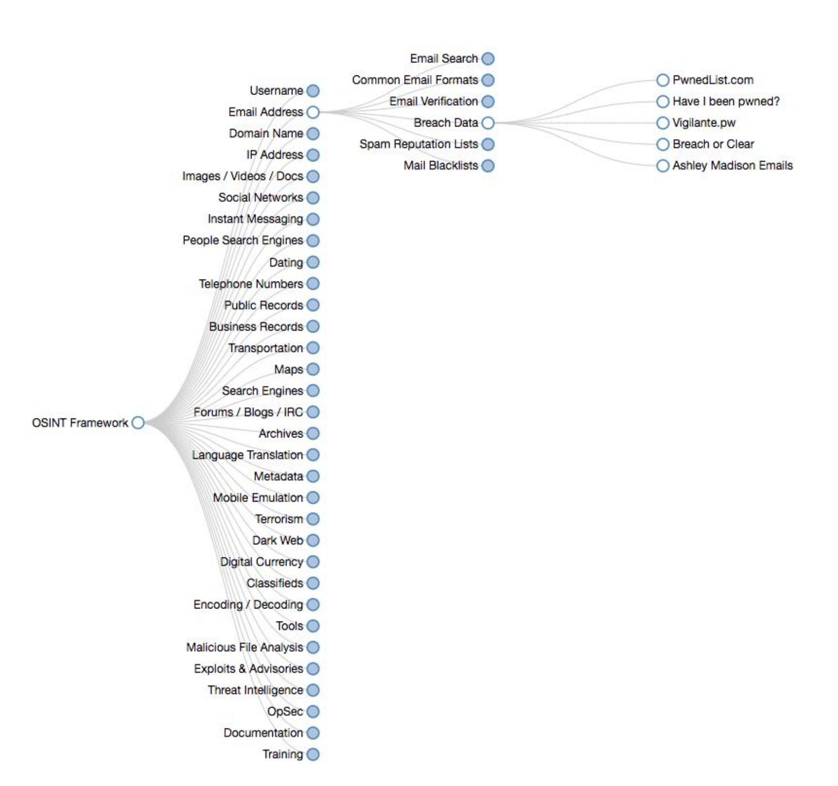
Example: robots.txt

- File on web host root
  - Which files & directories are indexable (by s. engine)
  - Which user-agents are allowed to index
- Not always enforced - and can be faked
- http://<site>/robots.txt


www.cnn.com/robots.txt
Apps
For quick access, place your bookmarks here on the bookmarks bar.
Import bo

```
Sitemap: http://www.cnn.com/sitemaps/sitemap-index.xml
Sitemap: http://www.cnn.com/sitemaps/sitemap-news.xml
Sitemap: http://www.cnn.com/sitemaps/sitemap-video-index.xml
Sitemap: http://www.cnn.com/sitemaps/sitemap-section.xml
Sitemap: http://www.cnn.com/sitemaps/sitemap-interactive.xml
User-agent: *
Allow: /partners/ipad/live-video.json
Disallow: /editionssi
Disallow: /ads/
Disallow: /aol
Disallow: /audio
Disallow: /beta
Disallow: /browsers
Disallow: /cl
Disallow: /cnews
Disallow: /cnn_adspaces
Disallow: /cnnbeta
Disallow: /cnnintl_adspaces
Disallow: /development
Disallow: /help/cnnx.html
Disallow: /NewsPass
Disallow: /NOKIA
Disallow: /partners
Disallow: /pipeline
Disallow: /pointroll
Disallow: /POLLSERVER
Disallow: /pr/
Disallow: /PV
Disallow: /quickcast
Disallow: /Quickcast
Disallow: /QUICKNEWS
Disallow: /test
Disallow: /virtual
Disallow: /WEB-INF
Disallow: /web.projects
Disallow: /search
```

Example: OSINT Framework



http://osintframework.com

note

- We have not presented an *exhaustive* list of OSINT techniques and tools
- But the community is constantly growing
  - https://github.com/jivoi/awesome-osint

your turn

- Find all you can about:

kruegster1990

(and report back)

(hints)

You will know you are on the right track if…

1. you find link(s) to the UMD Cybersecurity Club or UMD
2. you find link(s) between username(s), email address(es) and IP address(es)
3. you find code/encryption keys/forum posts/etc

There may be easter eggs… Let us know if you find them :)

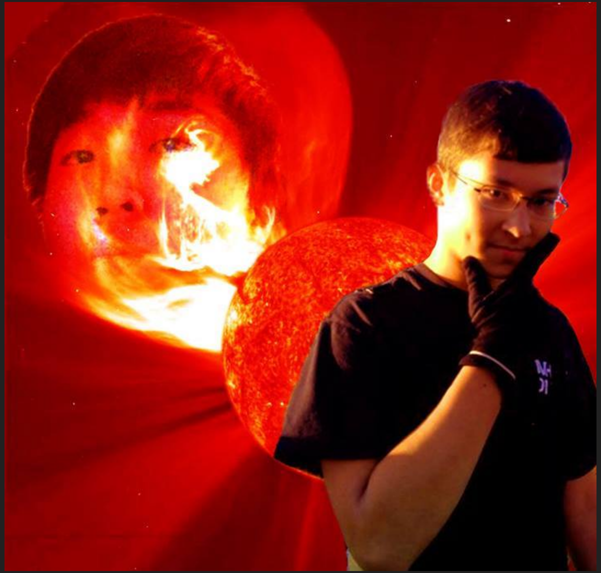
how to solve

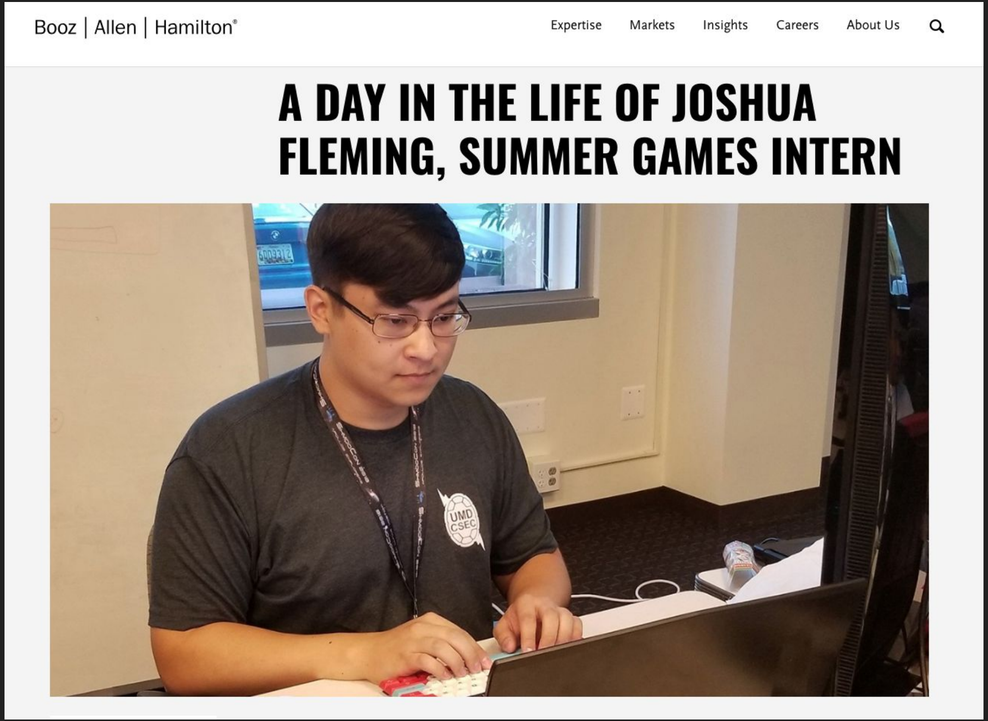
Acceptable solution: find an email and an IP address…

Come up to the front when you and your teammate(s) have found both pieces of information

a cautionary tale: josh

What can we find out about our own Josh Fleming?*





A DAY IN THE LIFE OF JOSHUA FLEMING, SUMMER GAMES INTERN

* with his permission

a cautionary tale: josh

- Josh goes by josofl, josofl12, ya_boi_quip_quip, jsfleming…
- He has 4 email address (with HIBP hits!)
  - Potentially leaked username and password!
- We also know:
  - His DNS and WHOIS domain history
  - His family, affiliates, organizations
- ...all from 30 minutes of OSINT!

a cautionary tale: josh

- With a little more effort, we could get:
  - His DOB, home address, cell number
- Conduct further attacks with gained knowledge
  - Password bruteforce
  - Social engineering
  - Attack surface discovery
  - …

homework #2

Will be posted tonight.

Let us know if you have any questions!

This assignment has two parts.

It is due by 9/13 at 11:59 PM.