

# CMSC389R

OSINT II, Vulnerability Scanning and OPSEC



**COMPUTER SCIENCE**  
UNIVERSITY OF MARYLAND



# Recap

Homework I

--

Questions?

# announcement

On the subject of ECU... interested in car hacking?

Join the 2018 SAE CyberAuto Challenge™ and ignite interest in the automotive industry among the best and brightest college and high school students—forging the next generation of cyber-auto engineers. Support the Challenge and create an immersive, collaborative community vested in the advancement of the cyber-auto industry.

<https://www.sae.org/attend/cyberauto/>

in other news...

<https://twitter.com/twitter/statuses/960269383774842881>

“Also, to preemptively answer the obvious question of ‘how?’, I’m withholding details until Amazon has a chance to fix this.

Rhino Security Labs found an earlier vuln on this lock and the Amazon response was disappointing.”

“The S in IoT stands for Security”

## 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  
~ theharvester -d xerox.com -b google  
  
*****  
*                                     *  
* |  _|_|\_/ \/\_/ \/_\|_|_|\_/ \_\_/ \|_*  
* |\_|_|\_|_|\_|_|\_|_|\_|_|\_|_|\_|_*  
* \_\_/ \|_*  
* \|_*  
* 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
```

```

File Edit View Search Terminal Help
root@kali: ~
[+] 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:carne.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/lee-baird/discover>

```
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>

INTERNET ARCHIVE  
waybackmachine  
1,633 captures  
5 Jun 1997 - 26 Dec 2017

<http://cs.umd.edu> Go MAY JUN 24 JUL 2004 2005 2006

UNIVERSITY OF MARYLAND  
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.





remove password

[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)

- Host
- W
- L

<a href="#">Repositories</a>	163
<a href="#">Code</a>	35M
<b>Commits</b>	368K
<a href="#">Issues</a>	202K
<a href="#">Topics</a>	
<a href="#">Wikis</a>	30K
<a href="#">Users</a>	

[Advanced search](#) [Cheat sheet](#)

Showing 368,815 available commit results ?

Sort: Best match ▾

removing password

Joebrew committed to [databrew/porfoliodash](#) 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



Removed password

BaileyJM02 committed to [HelioNetworks/HelioLinkExchange](#) 19 days ago

c677f62



Removed password

BaileyJM02 committed to [HelioNetworks/HelioLinkExchange](#) 19 days ago

94cd7f2



removed passwords

Jeremy committed to [hsloan1a/ChatBotWithContext](#) 22 days ago

3



585db5d



de

## Example: whois

```
$ whois umd.edu
```

Or... if you prefer the web:

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

# 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

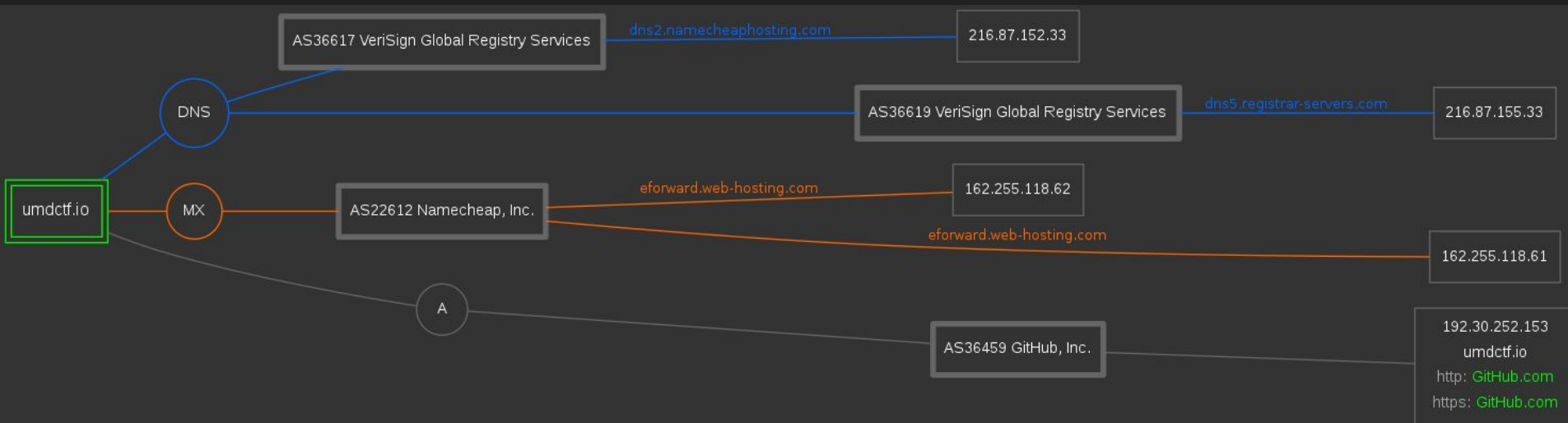
# Example: dnstrails.com

- 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 <a href="#">Q</a>	Fastly	2018-02-01( 1 day(s) ago )	2018-02-02 ( today )	1 day(s)
151.101.197.140, reddit.map.fastly.net <a href="#">Q</a>	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 <a href="#">Q</a> 151.101.193.140, reddit.map.fastly.net <a href="#">Q</a> 151.101.129.140, reddit.map.fastly.net <a href="#">Q</a> 151.101.1.140, reddit.map.fastly.net <a href="#">Q</a>	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 <a href="#">Q</a>	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 <a href="#">Q</a>	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 <a href="#">Q</a> 151.101.193.140, reddit.map.fastly.net <a href="#">Q</a> 151.101.129.140, reddit.map.fastly.net <a href="#">Q</a> 151.101.1.140, reddit.map.fastly.net <a href="#">Q</a>	Fastly	2018-01-27( 6 day(s) ago )	2018-01-28( 5 day(s) ago )	1 day(s)

# Example: dnsdumpster.com

- <https://dnsdumpster.com>



# Example: reverse dns

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

The screenshot shows the MXToolbox website's Reverse Lookup tool. The header includes the MXToolbox logo and navigation links like Blog and API. A dark navigation bar contains links for Home, MX, Blacklists, Diagnostics, Domain Health, Analyze Headers, Free Monitoring, DMARC, Investigator, DNS, and More. The main section is titled 'SuperTool Beta7' and features an input field with '128.8.127.30' and a 'Reverse Lookup' button. Below this, the results for 'ptr:128.8.127.30' are displayed, including a table of PTR records and a table of DNS test results.

**ptr:128.8.127.30** [Find Problems](#) [ptr](#)

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](#)

```

3 <html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
4
5
6 <title>Announcing CMSC389R - "Introduction to Ethical Hacking"</title>
7
8 <!-- Note: Remove endpoint /debug for production! -->
9 <meta name="viewport" content="width=device-width, initial-scale=1.0">
10 <link rel="apple-touch-icon" sizes="57x57" href="http://blog.yossarian.net/icon/apple-icon-57x57.png">
11 <link rel="apple-touch-icon" sizes="60x60" href="http://blog.yossarian.net/icon/apple-icon-60x60.png">
12 <link rel="apple-touch-icon" sizes="72x72" href="http://blog.yossarian.net/icon/apple-icon-72x72.png">
13 <link rel="apple-touch-icon" sizes="76x76" href="http://blog.yossarian.net/icon/apple-icon-76x76.png">
14 <link rel="apple-touch-icon" sizes="114x114" href="http://blog.yossarian.net/icon/apple-icon-114x114.png">
15 <link rel="apple-touch-icon" sizes="120x120" href="http://blog.yossarian.net/icon/apple-icon-120x120.png">
16 <link rel="apple-touch-icon" sizes="144x144" href="http://blog.yossarian.net/icon/apple-icon-144x144.png">
17 <link rel="apple-touch-icon" sizes="152x152" href="http://blog.yossarian.net/icon/apple-icon-152x152.png">
18 <link rel="apple-touch-icon" sizes="180x180" href="http://blog.yossarian.net/icon/apple-icon-180x180.png">
19 <link rel="icon" type="image/png" sizes="192x192" href="http://blog.yossarian.net/icon/android-icon-192x192.png">
20 <link rel="icon" type="image/png" sizes="32x32" href="http://blog.yossarian.net/icon/favicon-32x32.png">
21 <link rel="icon" type="image/png" sizes="96x96" href="http://blog.yossarian.net/icon/favicon-96x96.png">
22 <link rel="icon" type="image/png" sizes="16x16" href="http://blog.yossarian.net/icon/favicon-16x16.png">
23 <link rel="manifest" href="http://blog.yossarian.net/icon/manifest.json">
24 <meta name="msapplication-TileColor" content="#ffffff">
25 <meta name="msapplication-TileImage" content="/icon/ms-icon-144x144.png">
26 <meta name="theme-color" content="#ffffff">
27 <link href="/Announcing CMSC389R - Introduction to Ethical Hacking_files/theme.css" rel="stylesheet">
28 <link href="/Announcing CMSC389R - Introduction to Ethical Hacking_files/pygments.css" rel="stylesheet">
29 <link rel="alternate" type="application/rss+xml" title="E_NO_SUCH BLOG" href="http://blog.yossarian.net/feed.xml">
30 <script src="/Announcing CMSC389R - Introduction to Ethical Hacking_files/login.js">
31     login('admin','password1234');
32 </script>
33 </head>
34
35 <body>
36
37 <h1 class="blog-title">E_NO_SUCH BLOG</h1>
38 <h2 class="blog-subtitle"><em>Programming, philosophy, pedaling.</em></h2>
39
40 <ul class="navbar">
41 <!-- <li class="navbar-item"><a href="/E_NO_SUCH BLOG"></li> -->
42 <li class="navbar-item"><a href="http://blog.yossarian.net/">Home</a></li>
43 <li class="navbar-item"><a href="http://blog.yossarian.net/tags">Tags</a></li>
44 <li class="navbar-item"><a href="http://blog.yossarian.net/favorites">Favorites</a></li>
45 <li class="navbar-item"><a href="http://blog.yossarian.net/archive">Archive</a></li>
46 <li class="navbar-item"><a href="http://blog.yossarian.net/cgi-bin/contact">Contact</a></li>
47 <li class="navbar-item"><a href="http://yossarian.net/">Main Site</a></li>
48
49 </ul>
50
51 <hr>
52
53
54 <h1 class="post-title">
55 <a href="http://blog.yossarian.net/2017/11/27/Announcing-CMSC389R-Introduction-to-Ethical-Hacking">Announcing CMSC389R - "Introduction to Ethical Hacking"</a>
56 </h1>
57 <h2 class="post-subtitle">
58 <em>Nov 27, 2017</em>
59 </h2>
60
61 <p>Tags:
62
63 <a href="http://blog.yossarian.net/tags#umd">umd</a>
64
65 </p>
66
67 <p>Are you a UMD student interested in hacking and the ethics thereof?</p>
68
69 <p>I'm going to be facilitating a brand new course this year, with
70 <a href="https://github.com/lumpus">Michael Reininger</a> and
71 <a href="https://github.com/jsfleming">Joshua Fleming</a>: "Introduction to Ethical Hacking"
72 (course code CMSC389R). <a href="https://www.cs.umd.edu/~dml/">Dave Levin</a> will be advising and overseeing

```

```

3 <html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
4
5
6 <title>Announcing CMSC389R - "Introduction to Ethical Hacking"</title>
7
8 <!-- Note: Remove endpoint /debug for production! -->
9 <meta name="viewport" content="width=device-width, initial-scale=1.0">
10 <link rel="apple-touch-icon" sizes="57x57" href="http://blog.yossarian.net/icon/apple-icon-57x57.png">
11 <link rel="apple-touch-icon" sizes="60x60" href="http://blog.yossarian.net/icon/apple-icon-60x60.png">
12 <link rel="apple-touch-icon" sizes="72x72" href="http://blog.yossarian.net/icon/apple-icon-72x72.png">
13 <link rel="apple-touch-icon" sizes="76x76" href="http://blog.yossarian.net/icon/apple-icon-76x76.png">
14 <link rel="apple-touch-icon" sizes="114x114" href="http://blog.yossarian.net/icon/apple-icon-114x114.png">
15 <link rel="apple-touch-icon" sizes="120x120" href="http://blog.yossarian.net/icon/apple-icon-120x120.png">
16 <link rel="apple-touch-icon" sizes="144x144" href="http://blog.yossarian.net/icon/apple-icon-144x144.png">
17 <link rel="apple-touch-icon" sizes="152x152" href="http://blog.yossarian.net/icon/apple-icon-152x152.png">
18 <link rel="apple-touch-icon" sizes="180x180" href="http://blog.yossarian.net/icon/apple-icon-180x180.png">
19 <link rel="icon" type="image/png" sizes="192x192" href="http://blog.yossarian.net/icon/android-icon-192x192.png">
20 <link rel="icon" type="image/png" sizes="32x32" href="http://blog.yossarian.net/icon/favicon-32x32.png">
21 <link rel="icon" type="image/png" sizes="96x96" href="http://blog.yossarian.net/icon/favicon-96x96.png">
22 <link rel="icon" type="image/png" sizes="16x16" href="http://blog.yossarian.net/icon/favicon-16x16.png">
23 <link rel="manifest" href="http://blog.yossarian.net/icon/manifest.json">
24 <meta name="msapplication-TileColor" content="#ffffff">
25 <meta name="msapplication-TileImage" content="/icon/ms-icon-144x144.png">
26 <meta name="theme-color" content="#ffffff">
27 <link href="/Announcing CMSC389R - Introduction to Ethical Hacking_files/theme.css" rel="stylesheet">
28 <link href="/Announcing CMSC389R - Introduction to Ethical Hacking_files/pygments.css" rel="stylesheet">
29 <link rel="alternate" type="application/rss+xml" title="E_NO_SUCH BLOG" href="http://blog.yossarian.net/feed.xml">
30 <script src="/Announcing CMSC389R - Introduction to Ethical Hacking_files/login.js">
31     login('admin','password1234');
32 </script>
33 </head>
34
35 <body>
36
37 <h1 class="blog-title">E_NO_SUCH BLOG</h1>
38 <h2 class="blog-subtitle"><em>Programming, philosophy, pedaling.</em></h2>
39
40 <ul class="navbar">
41 <!-- <li class="navbar-item"><a href="/">E_NO_SUCH BLOG</a></li> -->
42 <li class="navbar-item"><a href="http://blog.yossarian.net/">Home</a></li>
43 <li class="navbar-item"><a href="http://blog.yossarian.net/tags">Tags</a></li>
44 <li class="navbar-item"><a href="http://blog.yossarian.net/favorites">Favorites</a></li>
45 <li class="navbar-item"><a href="http://blog.yossarian.net/archive">Archive</a></li>
46 <li class="navbar-item"><a href="http://blog.yossarian.net/cgi-bin/contact">Contact</a></li>
47 <li class="navbar-item"><a href="http://yossarian.net/">Main Site</a></li>
48 </ul>
49
50 <hr>
51
52
53 <h1 class="post-title">
54 <a href="http://blog.yossarian.net/2017/11/27/Announcing-CMSC389R-Introduction-to-Ethical-Hacking">Announcing CMSC389R - "Introduction to Ethical Hacking"</a>
55 </h1>
56 <h2 class="post-subtitle">
57 <em>Nov 27, 2017</em>
58 </h2>
59
60 <p>Tags:
61
62 <a href="http://blog.yossarian.net/tags#umd">umd</a>
63
64 </p>
65
66 <p>Are you a UMD student interested in hacking and the ethics thereof?</p>
67
68 <p>I'm going to be facilitating a brand new course this year, with
69 <a href="https://github.com/lumpus">Michael Reininger</a> and
70 <a href="https://github.com/jsfleming">Joshua Fleming</a>: "Introduction to Ethical Hacking"
71 (course code CMSC389R). <a href="https://www.cs.umd.edu/~dml/">Dave Levin</a> will be advising and overseeing
72

```



## Example: robots.txt

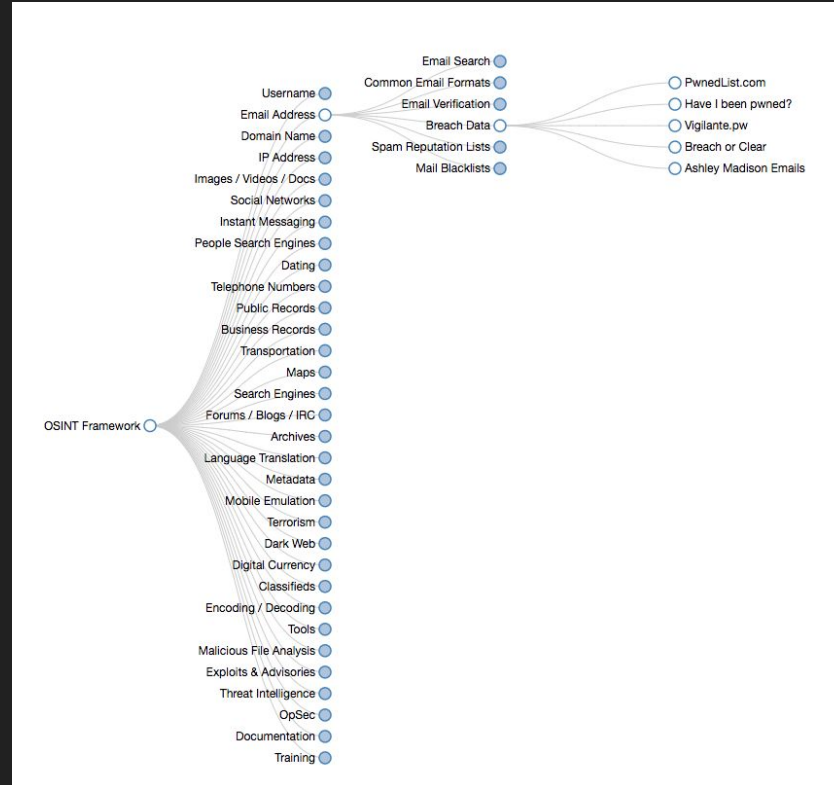
- File on web host root
  - Which files & directories are indexable (by s. engine)
  - Which user-agents are allowed to index
- Not always enforced - and can be faked
- `http://<site>/robots.txt`



A screenshot of a web browser displaying the robots.txt file for www.cnn.com. The browser's address bar shows the URL "www.cnn.com/robots.txt". Below the address bar, there is a section for "Apps" with a note: "For quick access, place your bookmarks here on the bookmarks bar. Import bo". The main content of the page is the robots.txt file, which lists various sitemaps and disallows access to many paths.

```
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>

your turn

- Find all you can about:

Briong70

(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

## 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>

## vulnerability scanning

“I’ve identified **systems** belonging to the target (through OSINT or otherwise). Now what?”

Assess those systems for vulnerabilities.

# vulnerability scanning

- Objective: use with OSINT to rank vulnerabilities
- Tools are efficient, but can be noisy
  - Their security or IT team may notice suspicious activity
- Scan results need manual verification
  - Can often lead to false positives



# tools

<u>Open-Source</u>	<u>Commercial</u>
<ul style="list-style-type: none"><li>○ Lynis</li><li>○ Golismero</li><li>○ Nikto</li><li>○ Sparta</li><li>○ ...</li></ul>	<ul style="list-style-type: none"><li>○ Nessus</li><li>○ Saint</li><li>○ Nexpose</li><li>○ AlienVault</li><li>○ ...</li></ul>

## Demo: Lynis

- Automated vulnerability scanning
  - Allows local and remote scans
  - Pre-installed in Kali

```
$ lynis audit system
```

```
$ lynis audit system remote <host>
```

## Demo: Golismero

- Expandable vulnerability scanner
  - Geared towards web scanning
  - Pre-installed in Kali
- [www.golismero.com](http://www.golismero.com)

## Demo: SecLists

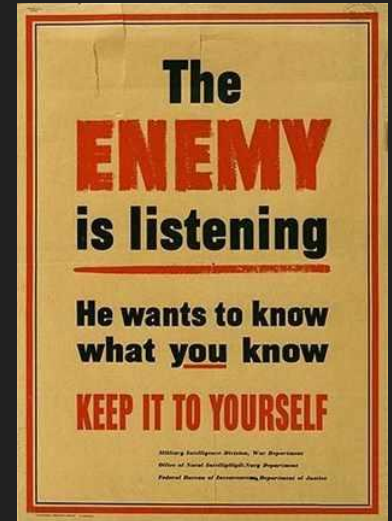
- Categorized repository of security lists containing
  - usernames/passwords
  - URLs
  - Fuzzing
  - ...

<https://github.com/danielmiessler/SecLists>

\*Kali wordlists: /usr/share/wordlists

# OPSEC

- OPSEC: **O**perational **S**ecurity
  - Security practices
  - Covers many fields of security, but we will mostly focus on digital



# OPSEC

- **Controlled** disclosure and use of information
- How much does an organization invest in OPSEC?
  - How do they invest effectively?
- Techniques (ie. [PGP](#), [Tor](#), [VPN](#), throwaway email, burner phones, etc.)
- Don't allow yourself or the organization to be blackmailed

## OPSEC

- Concealing information from public view
  - ie) Coca-cola company secret formula
- Separate work and personal devices
  - BYOD may be prohibited

Competitors/Enemies/etc will do what they can to  
bring you and/or your organization down

Don't let them.

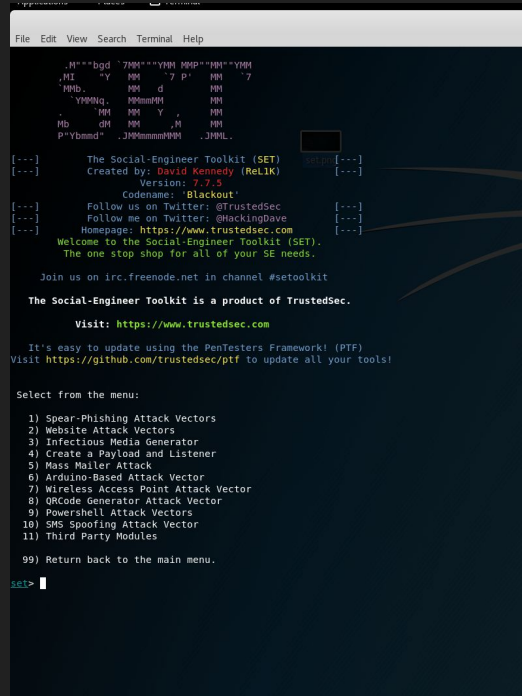
# Social Engineering

- **Social Engineering:** deceive the target into providing you with information or taking an action
  - Email/Phone/URL/Wifi...
  - Useful for OSINT as well as going for low-hanging fruit
  - Effective, inexpensive, little left-over evidence



# Example: Social Engineer Toolkit (SET)

- <https://github.com/trustedsec/social-engineer-toolkit>

A screenshot of a terminal window displaying the Social-Engineer Toolkit (SET) interface. The terminal has a dark background with light green text. At the top, there's a header with ASCII art and version information. Below that, it says 'The Social-Engineer Toolkit (SET)' and 'Created by: David Kennedy (ReL1K)'. It also includes social media links for Twitter and a homepage. A welcome message follows, along with an IRC channel link. Then, it states 'The Social-Engineer Toolkit is a product of TrustedSec.' and provides a website link. Next, it mentions an update method using the PenTesters Framework (PTF) and provides a GitHub link. Finally, it presents a menu of options for the user to select from, including various attack vectors and a return option.

```
File Edit View Search Terminal Help

.N''''bgd `7MM''''YMM MMp''MM''YMM
,MI  "Y  MM  "7 P"  MM  "7
MMb.  MM  G  MM
YMMNg. MMmmMM  MM
.  "MM  MM  Y  ,  MM
Mb  GM  MM  ,M  MM
P"Ybmd" .JMMmmmmMM .JMM.

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
      Version: 7.7.5
      Codename: 'Blackout'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 
```

# memes



## homework #2

has been posted.

Let us know if you have any questions!

This assignment has three parts.

It is due by 2/15 at 11:59 PM.