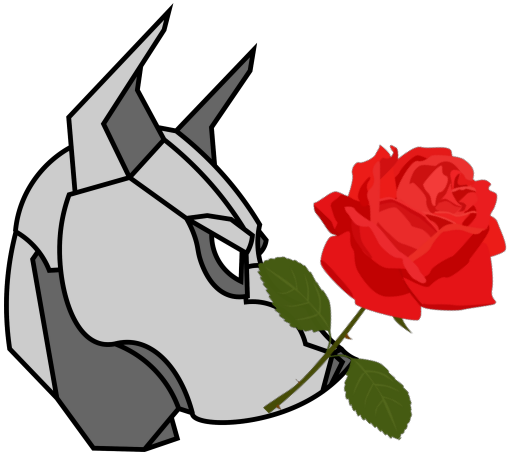
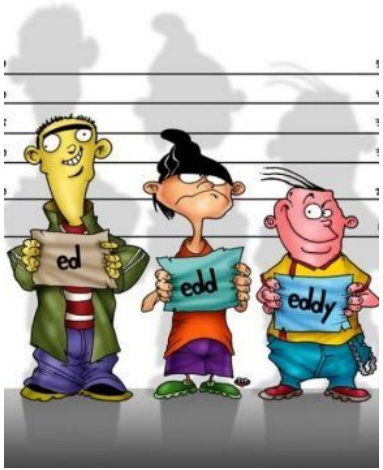
Cyber Defense Organization

Spring 2020 - Google Dorking



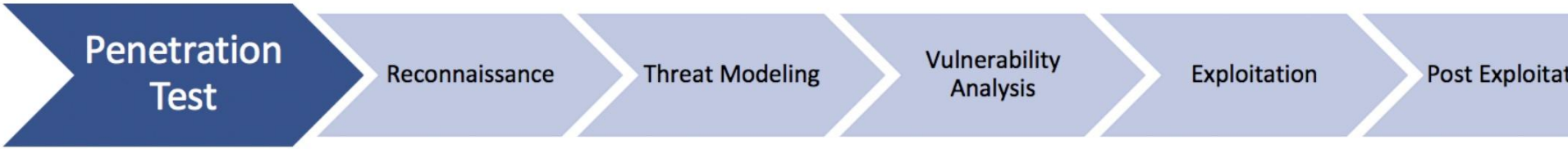
Disclaimer

- Please do not use this to log into websites/ databases/ etc or download files you find that you don't have permission to. That is illegal and CDO is not responsible for what happens to you.
- You could be prosecuted under CFAA



OSINT - Open Source Intelligence

- Definition: Using basic internet searching to find information on the target. This information must be Publicly Available to be considered OSINT
- Used by: Pen-Testers, Red Team, malicious hackers
- Why is it used: Because it's easy, and a good way to find information about your target

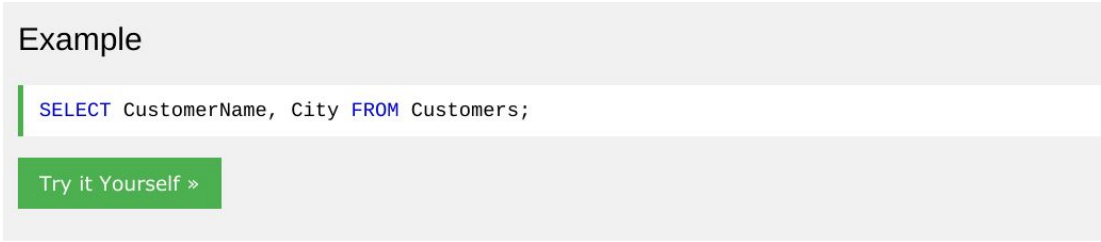


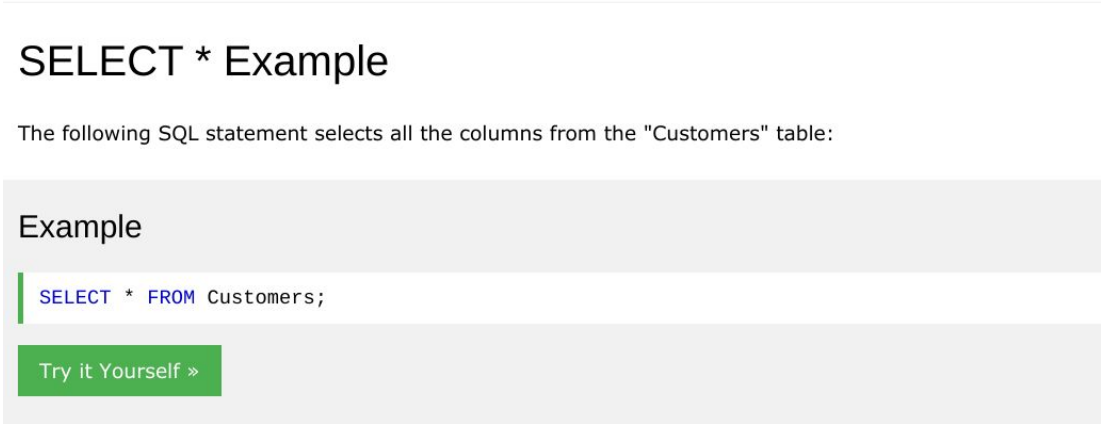
What is Google Dorking?!?

- If you work at Google are you a dork?
- A form of OSINT
- Obviously we are using Google for this but how/ why?

What does googling actually mean?

- You are querying a database
- But google is “smart” so it doesn’t need the extra junk



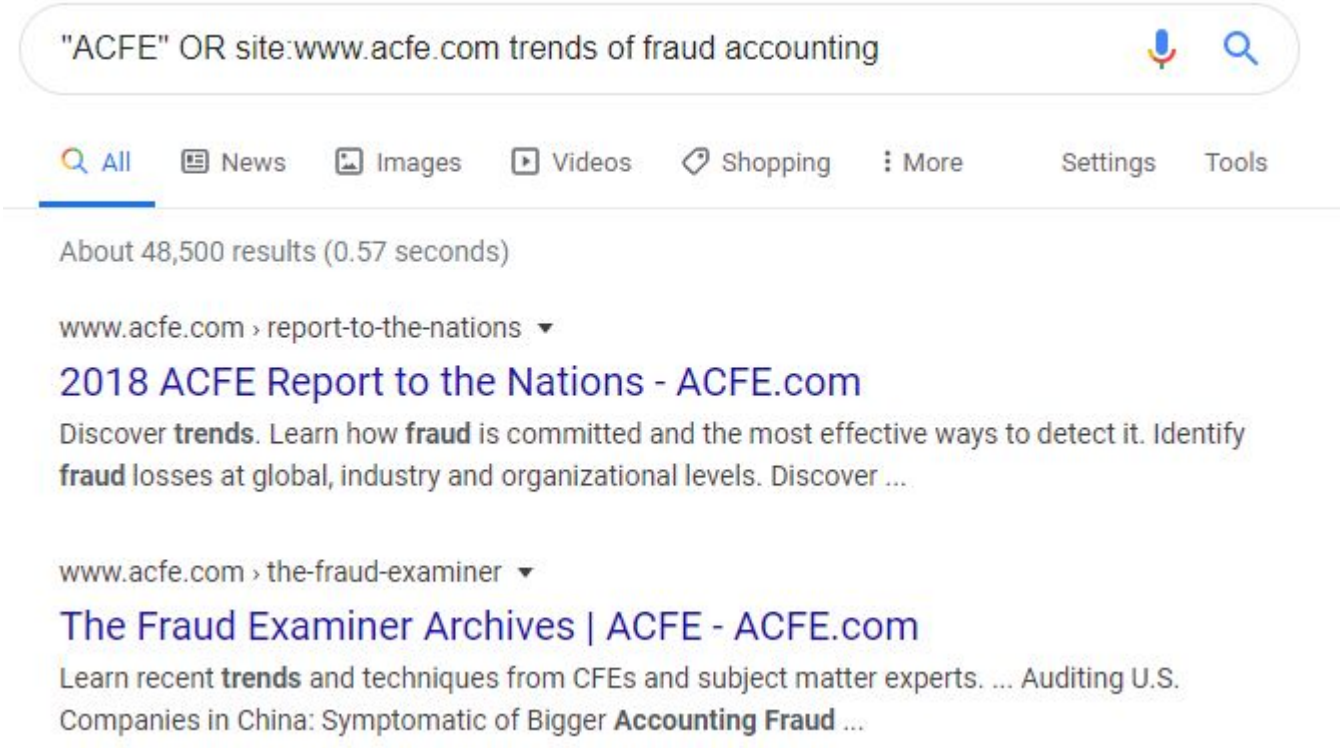


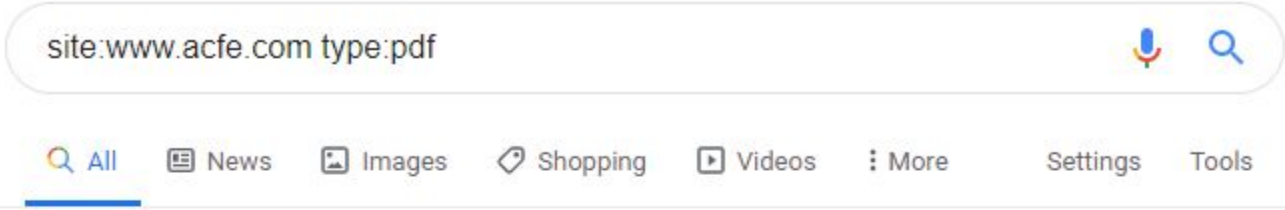
^ Mega simplification... but it worky for our case

How does this work?

- You might have heard of ways to make your google search better
- Examples...
  - Adding quotes around the word you're searching
    - puppy dog sweaters vs "puppy dog sweaters"
  - Using the hyphen to exclude words
    - Mustang -car -cars
- Google dorking uses more advanced operators to find things

How most people use this





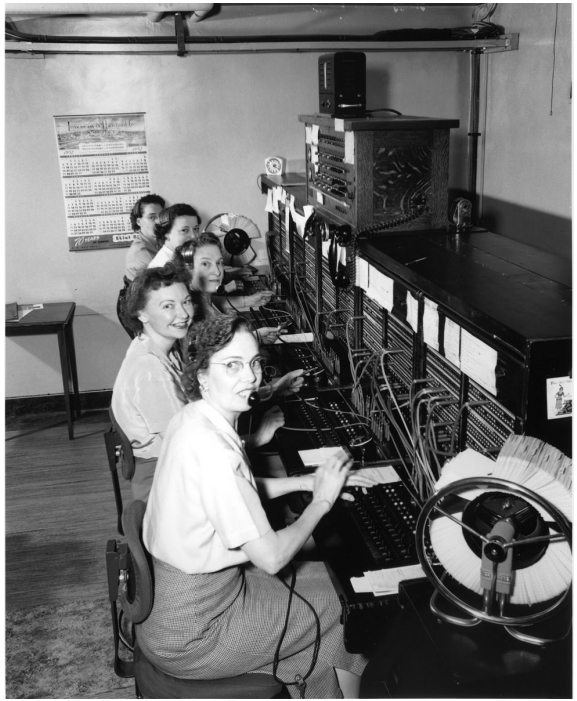
type:pdf lets you find official stuff

What are WE looking for??

- Misconfigured devices that are pointing out to the internet
- Examples of these things
  - FTP servers
  - Webcams
- Files that made their way out to the internet (probably on accident)
  - Log files
  - Excel sheets
  - Config Files
  - Frankly any file of importance
- Fun stuff

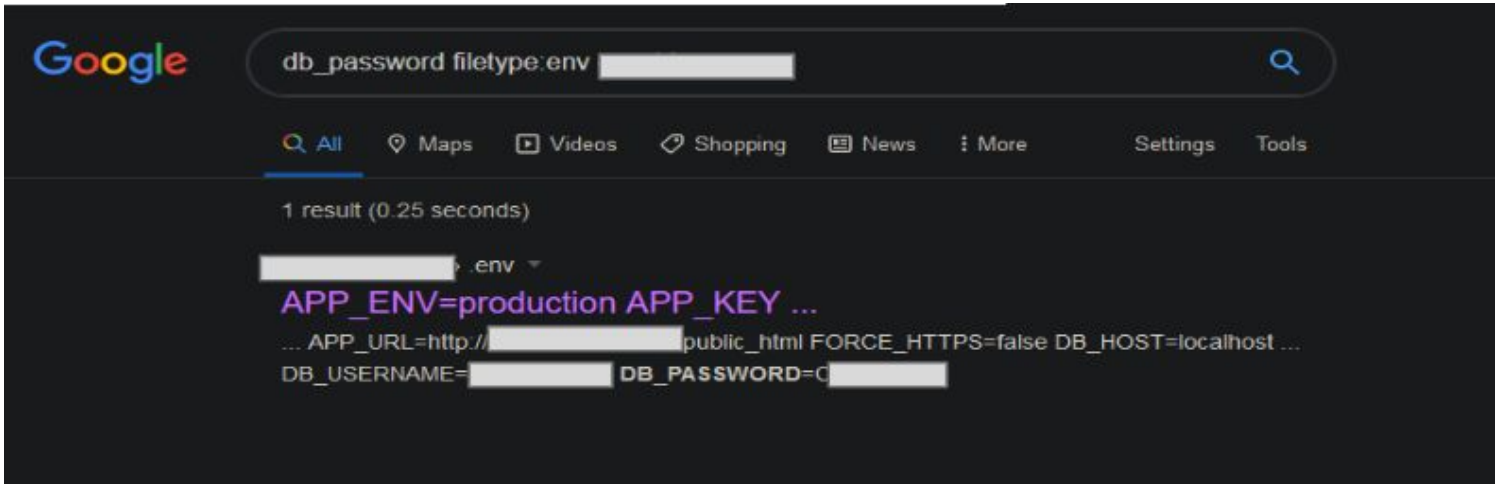
What are some of the operators?

- allintext:
  - Searches for specific text string
- allintitle:
  - Same as all in text but for the title
- site:
  - Looks for specific sites
- inurl:
  - Loos for things in the url
- filetype:
  - Looks for file types



A fun example

- db_password filetype:env WEBSITE.COM
- Why does this work?
  - It is looking for the variable db_password
  - A common variable in an environment file



Another example

- allintext: "WebcamXP 5"
- Searches for the WebcamXP 5

Date Added	Dork
2019-08-02	s3 site:amazonaws.com filetype:log
2019-07-31	s3 site:amazonaws.com intext:dhcp filetype:txt inurl:apollo
2019-07-31	site:amazonaws.com inurl:login.php
2019-06-04	s3 site:amazonaws.com filetype:sql
2019-05-31	s3 site:amazonaws.com filetype:xls login
2019-05-31	s3 site:amazonaws.com filetype:xls password

What might these be looking for?

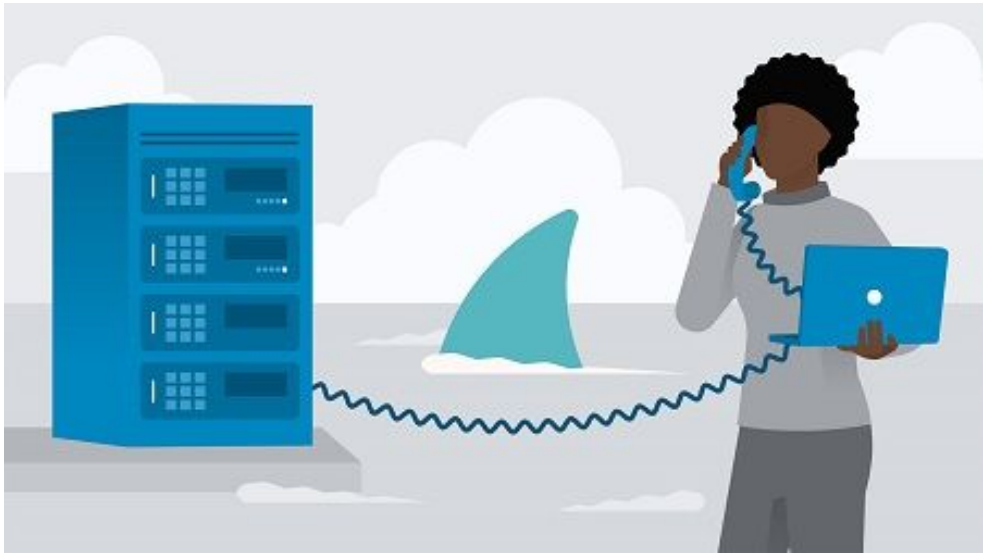
In Scope: Bug Bounties

https://www.bugcrowd.com/bug-bounty-list/

Hands on time

- Go to this link for a full list of operators and some example searches
- https://tinyurl.com/GoogleDorking

Next Time... Wireshark!



Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a new discord!