Mason Competitive Cyber

Profiling & Dissecting a Web App: Recon to Scanning

Media Recording Notice

This meeting is more than likely recorded. Got a problem with that? Emit a sharp screech at the nearest exec now.

CC in a nutshell

- Established (yes we're sanctioned) in 2016, maxing out meetings our first year at about 6 people, then in Fall '17 30 or 40 across both rooms
- Established with a heavy CTF/cyber competition focus
  - Since expanded to accommodate PH gap
- Focus on hands-on work
- Chat on Slack a lot, makes almost everything available in pretty much every medium (slides, videos, VMs, etc)
- Socializes ***sometimes***
- Sponsored by Battelle, possible sponsorship by The Crypsis Group
  - Due to the people that work there

How can I stay posted/involved?

- **Speak up**
  - Speak at club
  - Communicate in the Slack, stay active
  - Offer advice and constructive criticism
- **Compete**
  - 9/10 times there's no barrier to entry and we'll say when there is
  - If you aren't qualified to be on a team, rest assured we'll privately tell you to get off of it
  - You learn a lot in a small period of time, get real practice
- **Make friends**
  - We have nice people
    - A lot of them like to have fun
  - A lot of them are also a great resource

What will I learn at meetings?

What you may learn	What you probably won't
Methodologies Certain tools Techniques used in CTF or at work Exploitation tactics	How TCP/IP works How Linux works (TBD) 99% of things that can easily be described in a list in a book High prereq knowledge things (i.e. not "what's a stack", but stack smashing exploits may be covered)

News since last meeting

- Our last meeting was months ago
  - So… Plenty?
  - But we’re going to skip over that because I always skip over that
    - Some people were confused by that

Recent Competitions

- AWS Security Coding Challenge
  - 21st of December
  - We didn't organize at all, 4 of us just happened to show up
  - Teams of 5, 5 challenges, we got ⅘, was a 3 way tie
  - Matt and I won Echos when they raffled off

Fall 2017 in Pictures

Upcoming Competitions & Events

- SharifCTF #sharifctf channel
- Cyber Fusion
  - All day, Feb 23
  - At VMI, Invite Only
  - Each college sends one team
- BSidesNOVA
  - Team of 8, $20 registration fee
- CryptoParty
  - March 3 10:30am to 6:00pm
  - Includes food, a little swag, a CTF w/ prizes, etc
  - Register and see schedule at cryptoparty.gmu.io
- VT Summit, UMDCTF

Know of other competitions? *Tell us**

Recon and Scanning

- Recon and Scanning
  - Recon - Gathering information about a target
  - Scanning - Somewhat subjective
- How does it relate to real world work?
  - Any non-shit app requires more than 3 slides and random tools to hack
    - *study on your own as well*
  - There's no reason to run attacks that aren't applicable

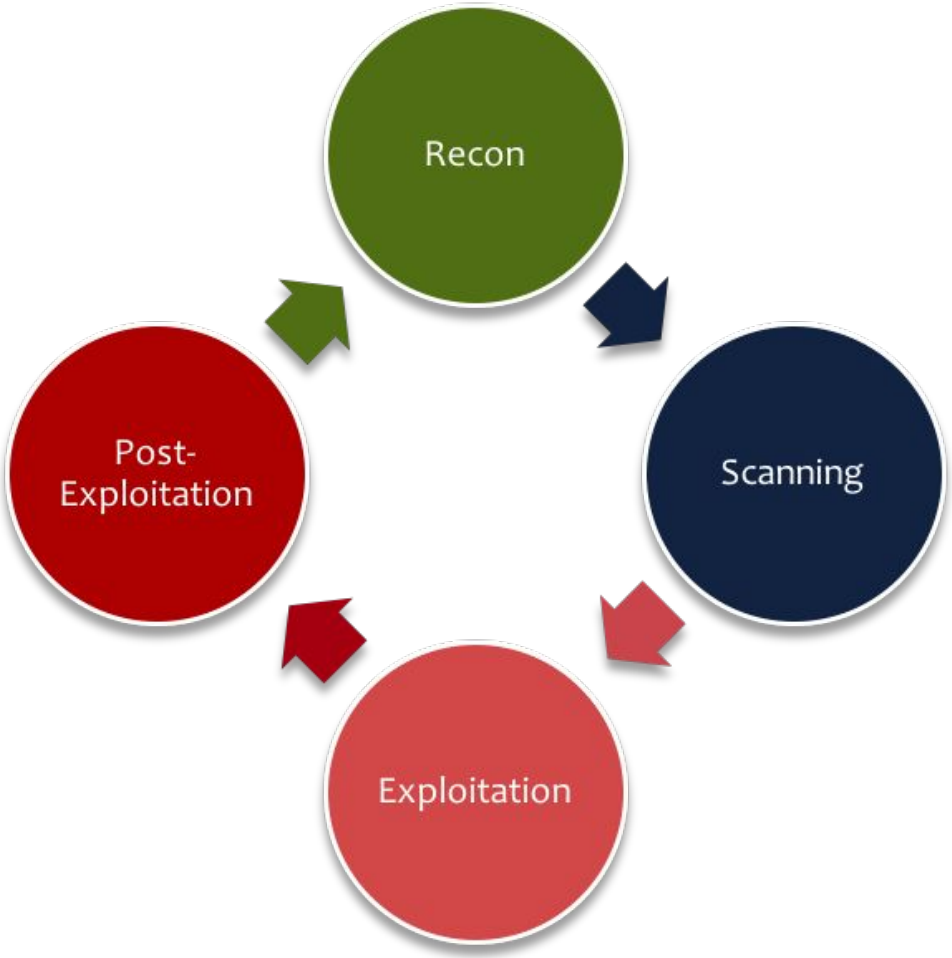
Web: Different Levels of Impact

- What is your ultimate goal?
  - Are you on a bug bounty?
    - What's in scope? Is chaining authorized?
  - CTF?
    - What are they hinting at? What is the competition's context?
  - Pentest?
    - Impact they care about? Rules of engagement? (I guess?)

- This only follows a **subset** of the ways to recon and scan a website
- Templating bugs vs content injection vs domain takeover vs command injection
  - All varying levels of impact

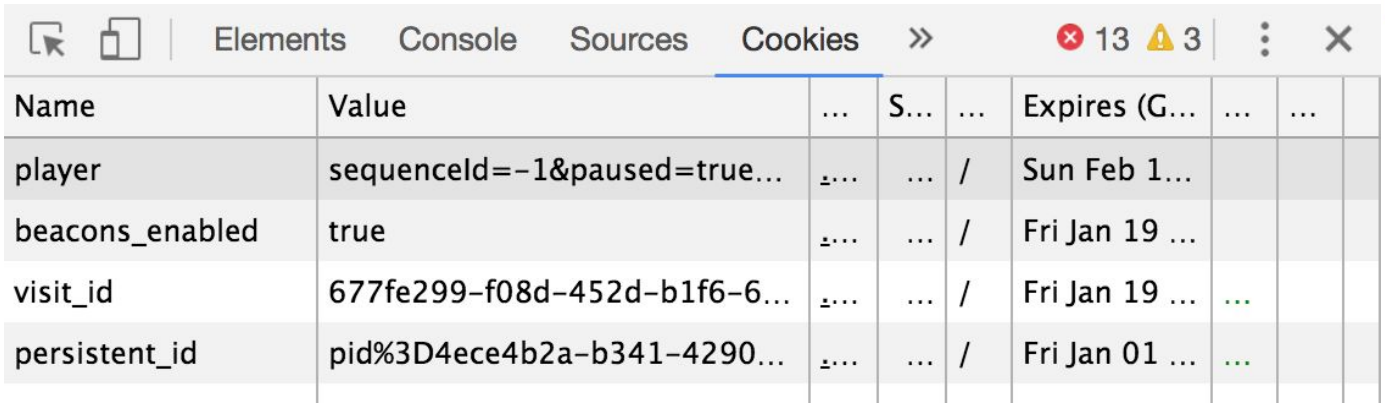
Understanding Cycle

- Where does web fit in the exploitation cycle?



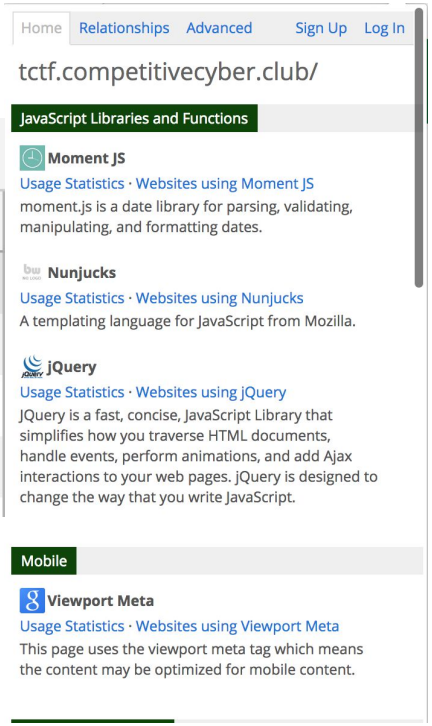
(Chrome) Extensions To Use

- BuiltWith - Discover technologies a site is built with
- EditThisCookie or CookieInspector - Manage cookies
- ModHeader - Modify headers you send to a server
- XSS Radar or comparable scanners (I don't personally use this)



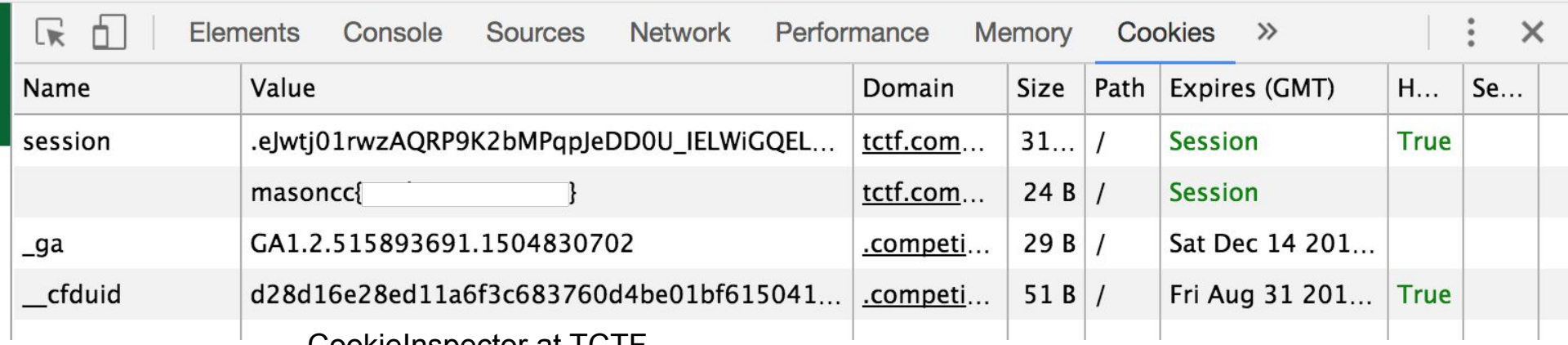
CookieInspector

BuiltWith



Using Said Extensions

- Builtwith is self-explanatory, install, click on it, it tells you technologies
- Any cookie reader if you don't have Chrome suffices
  - Run **document.cookie** in Console if that's not even an option to dump them
- CTF Challenge: **Nom Nom Nom**



CookieInspector at TCTF

Using What You Have

- **Actually visit the site**
  - Get application version, it may not broadcast it in a technical format
  - Related challenge: A few...
- Google/research often and carefully
- **Use built in developer tab**, we'll be using it a few times here
  - Safari: Require you go to advanced preferences, enable **Develop**, then select it from the top nav menu
  - Chrome: Dots to top right -> More tools -> Developer Tools
  - Firefox: Similar to chrome, 3 tabs -> Developer -> Select Option like Web Console
  - **Each looks very similar once you get to it**

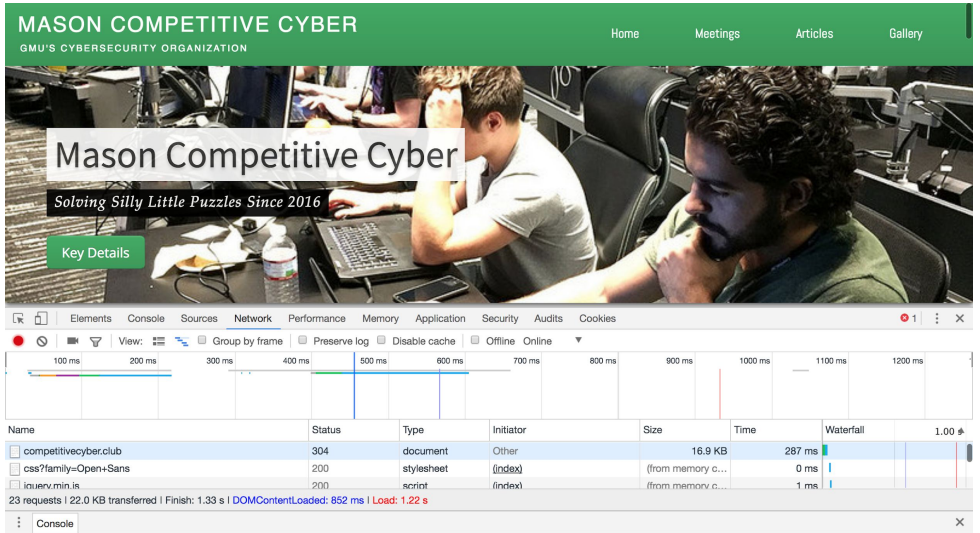
Console Deep Dive

- **Related CTF Challenge: Heads Up**
- There are a variety of tabs available, many self explanatory, we'll focus on three

Console - Run Javascript

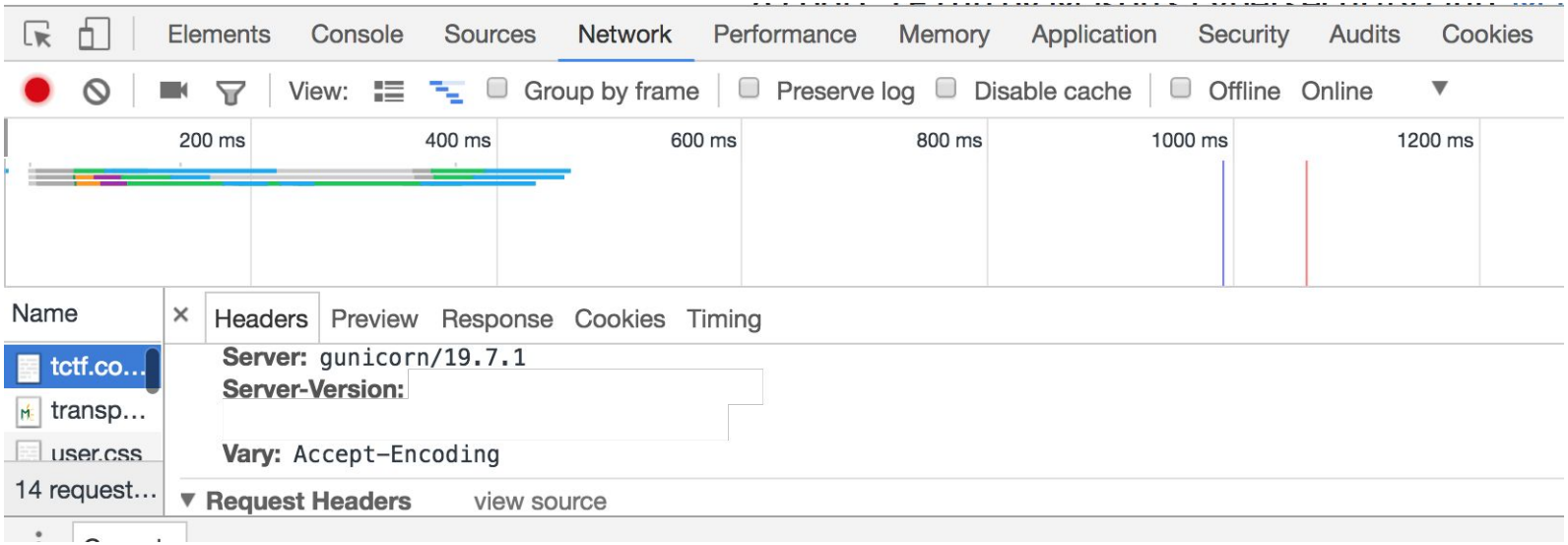
Elements - Breakdown of "DOM tree", or the page's design (similar to Right Clicking and hitting View Source/View Page Source, but more visual)

Network - My personal favorite, records requests/responses related to the page



More on Network Tab

- Click on interactions to view details about them, both their request and response
  - In Chrome, **Headers** and **Response**
- Good for determining higher level versions of what the sites running, such as language, web server, HTTP version, any sort of caching, etc
- Pay special attention to Headers in TCTF when you load it.



Getting briefly into Linux

- **Basically everyone should be familiar, especially if you're a STEM major and plan on going to a STEM career**
- If you have a Gmail, visit: https://go.gmu.edu/linux
  - This will wipe after a while
- If you don't but are a GMU student, visit: https://go.gmu.edu/gmuvcl
  - New Reservation, Note the HTML5 RDP Session option when you wait a few seconds after you hit "Connect!"
  - For meeting purposes, pick any Ubuntu based VM
- Be prepared to install Docker at some point

Actually Using Linux

- Tools we're gonna use today in Linux:
  - dirb - Directory buster
  - dnsrecon - DNS reconnaissance tool

apt-get install dnsrecon -y **wget go.gmu.edu/dnslist -O /tmp/dnslist**	**curl -L go.gmu.edu/dirb|sudo bash**

when done, you should be able
to run **dirb** and **dnsrecon**

Dir Busting

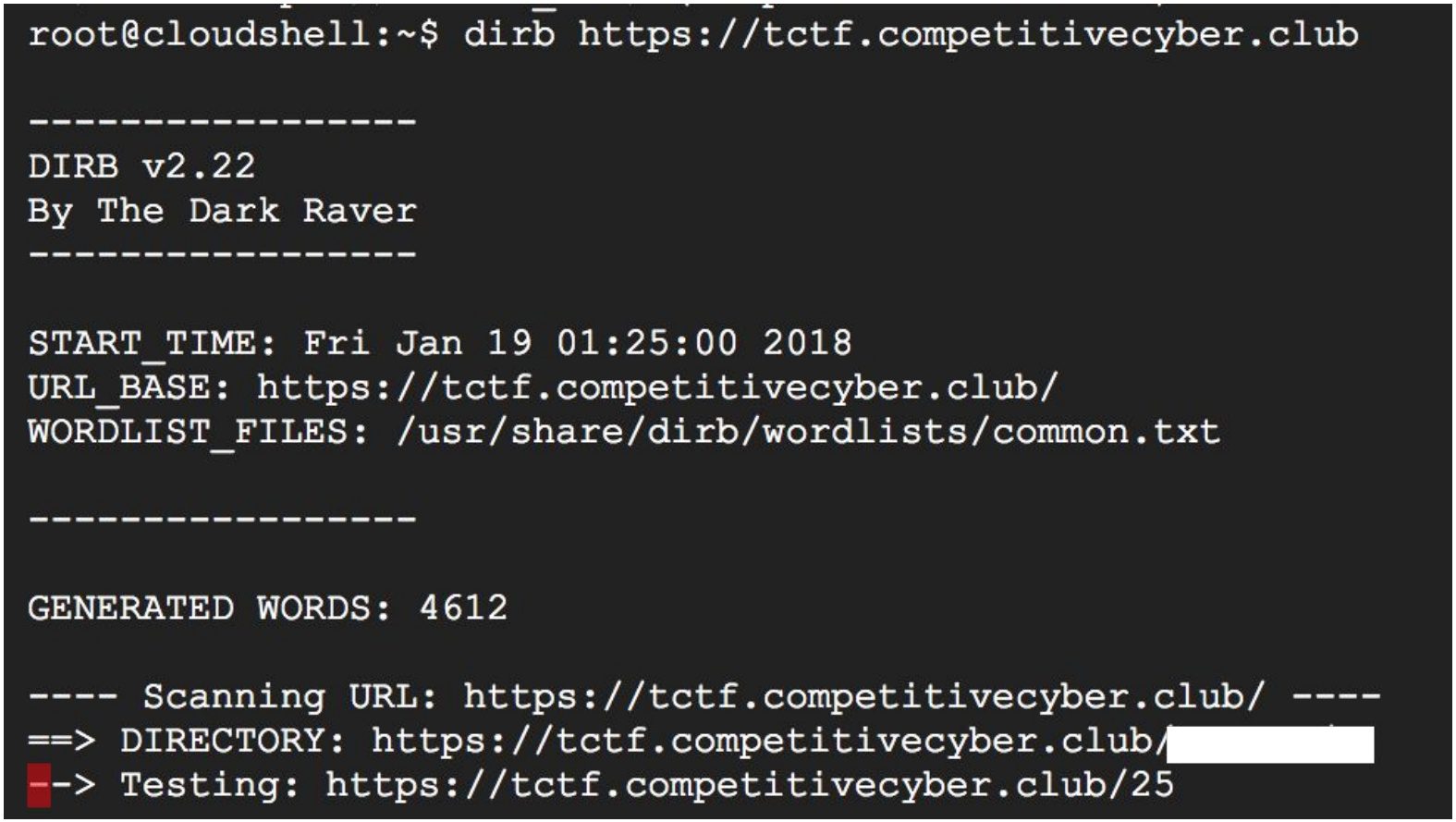
- Appeared in a HackEd CTF challenge
- Brute forces files and directories in a website
- /uploads, /admin, etc among app-specific ones
- Uses a “wordlist”, a list of words to try, also used in our dnsrecon demo

Related TCTF problem: Busted Deer

Using Windows? Run DirBuster
Using Linux (or MacOS)? Run **dirb**

Usage: **dirb https://tctf.competitivecyber.club**

Dirb Run Example



```
root@cloudshell:~$ dirb https://tctf.competitivecyber.club

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jan 19 01:25:00 2018
URL_BASE: https://tctf.competitivecyber.club/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://tctf.competitivecyber.club/ ----
==> DIRECTORY: https://tctf.competitivecyber.club/[redacted]
--> Testing: https://tctf.competitivecyber.club/25
```

DNS Brute Forcing

- **In bug bounties and pentests, I recommend dnsdumpster.com** in addition to this technique
- Simply run **dnsrecon** to expose options

```
root@cloudshell:~$ dnsrecon
Version: 0.8.10
Usage: dnsrecon.py <options>

Options:
   -h, --help                 Show this help message and exit.
   -d, --domain       <domain> Target domain.
   -r, --range        <range>  IP range for reverse lookup brute force in formats (first-last) or in (range/bitmask).
   -n, --name_server  <name>   Domain server to use. If none is given, the SOA of the target will be used.
   -D, --dictionary   <file>   Dictionary file of subdomain and hostnames to use for brute force.
   -f                          Filter out of brute force domain lookup, records that resolve to the wildcard defined
                               IP address when saving records.
   -t, --type         <types>  Type of enumeration to perform:
                               std       SOA, NS, A, AAAA, MX and SRV if AXRF on the NS servers fail.
                               rvl       Reverse lookup of a given CIDR or IP range.
                               brt       Brute force domains and hosts using a given dictionary.
                               srv       SRV records.
                               axfr      Test all NS servers for a zone transfer.
                               goo       Perform Google search for subdomains and hosts.
                               snoop     Perform cache snooping against all NS servers for a given domain, testing
                                         all with file containing the domains, file given with -D option.
                               tld       Remove the TLD of given domain and test against all TLDs registered in IANA.
                               zonewalk  Perform a DNSSEC zone walk using NSEC records.
   -a                          Perform AXFR with standard enumeration.
   -s                          Perform a reverse lookup of IPv4 ranges in the SPF record with standard enumeration.
   -g                          Perform Google enumeration with standard enumeration.
   -w                          Perform deep whois record analysis and reverse lookup of IP ranges found through
                               Whois when doing a standard enumeration.
   -z                          Performs a DNSSEC zone walk with standard enumeration.
   --threads          <number> Number of threads to use in reverse lookups, forward lookups, brute force and SRV
                               record enumeration.
   --lifetime         <number> Time to wait for a server to response to a query.
   --db               <file>   SQLite 3 file to save found records.
   --xml              <file>   XML file to save found records.
   --iw                        Continue brute forcing a domain even if a wildcard records are discovered.
   -c, --csv          <file>   Comma separated value file.
   -j, --json         <file>   JSON file.
   -v                          Show attempts in the brute force modes.
```

DNS Brute Forcing Command

- **Related CTF Challenge: A Record to Remember**
- dnsrecon -D /tmp/dnslist -d tctf.competitivecyber.club -t brt
- Should produce any records in the wordlist
- Some wordlists are much larger, and as such take longer to run
  - This one is *quite* small

```
   -v                              Show attempts in the brute force modes.
root@cloudshell:~$ dnsrecon -D /tmp/dnslist -d tctf.competitivecyber.club -t brt
[*] Performing host and subdomain brute force against tctf.competitivecyber.club
[*]      A                                      54.172.0.227
[*] 1 Records Found
root@cloudshell:~$
```

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™