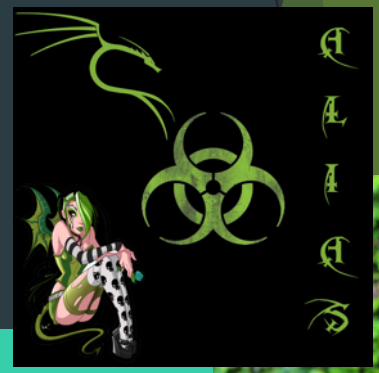
Gophers, whales and.. clouds? Oh my!

Playing with shiny tech, and maybe improving my offensive capacity along the way.

@_devalias #gopherblazer

Who am I?

- Glenn ‘devalias’ Grant
  - http://devalias.net/
  - https://twitter.com/_devalias
  - https://github.com/0xdevalias
  - https://www.linkedin.com/in/glenn-devalias-grant/
- Penetration Tester @ TSS
- Polyglot Developer
- And a few other things..
  - Biohacker, Bulletproof Coach, Snowboarder, Scuba, Skydiver..



@_devalias #gopherblazer

Trends & Buzzwords

(AKA a few things that caught my interest)

@_devalias #gopherblazer

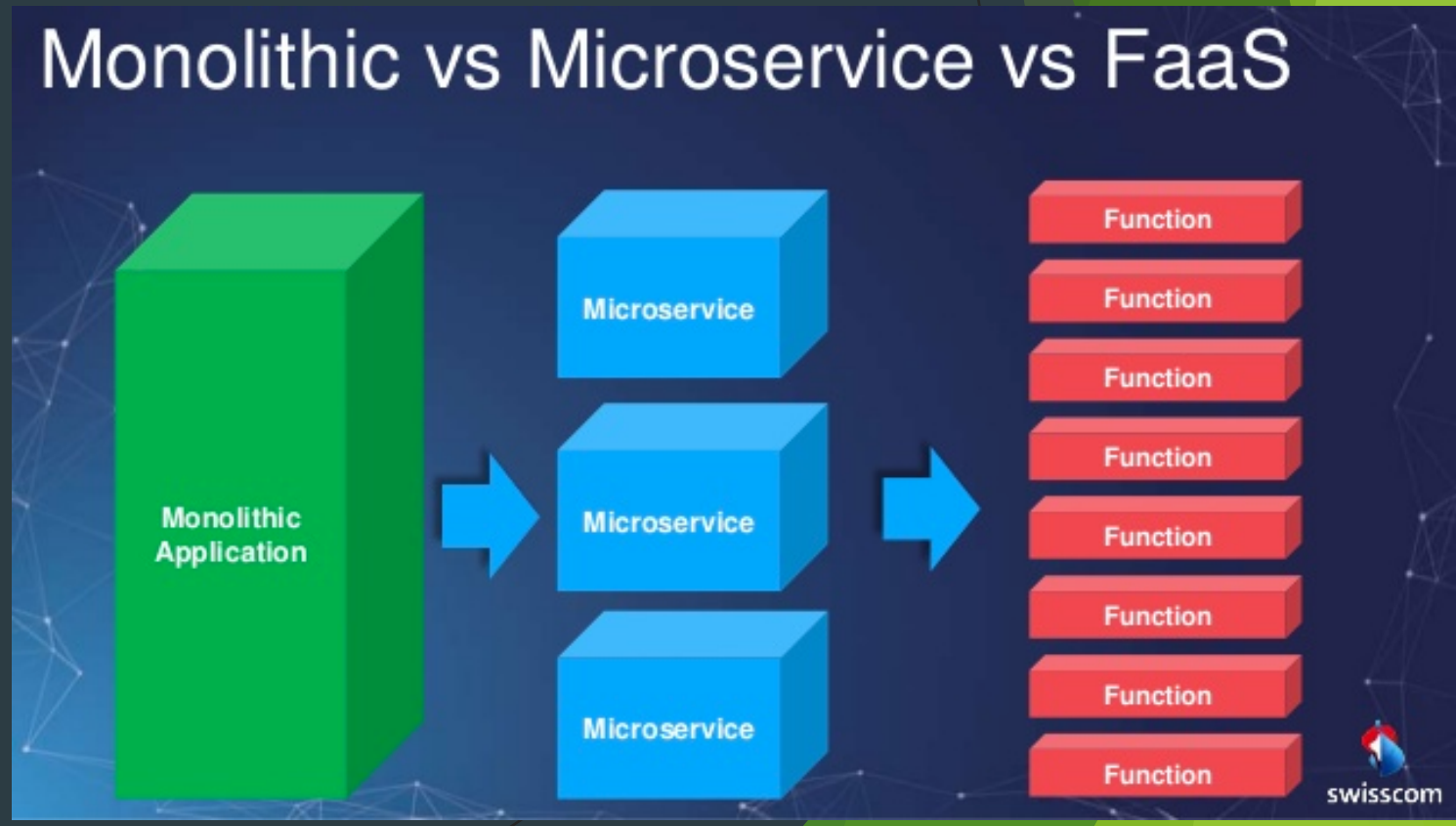
Docker

- https://www.docker.com/
- Containers: Lightweight ‘virtualisation’, shared kernel
- Base OS image, data is layered, layers are shared
  - Alpine Linux base image < 5mb!

- **DevOps:** Build systems, clustering, consistent enviroments..
- **Me:** Toolkit on every box with no more system clutter!
  - `docker run --rm devalias/gobuster -h`

Serverless & FaaS

- Still uses servers, they're just #InTheCloud™ (and somebody else's problem)
  - Cheap!
  - On demand
  - Automatic scaling
- Function(s) as a Service (FaaS)
  - Serverless design pattern
  - Decompose, then decompose again
  - Modular, Reusable
  - Easier to comprehend and maintain



@_devalias #gopherblazer

Maybe you've head of it?

AWS Lambda

Azure

@_devalias #gopherblazer

Golang

- https://golang.org/
  - Google, 2009
- C-esque (without a lot of those mind-bending bits)
- Compiled, cross platform, statically typed, memory safe, simple concurrency..
  - Not functional though D:
- Growing fast, good library support, and no heavy-weight interpreter..
  - ..looking at you Scala.
- Fun!

An Unexpected Journey

How this all started

@_devalias #gopherblazer

Gobuster on Lambda

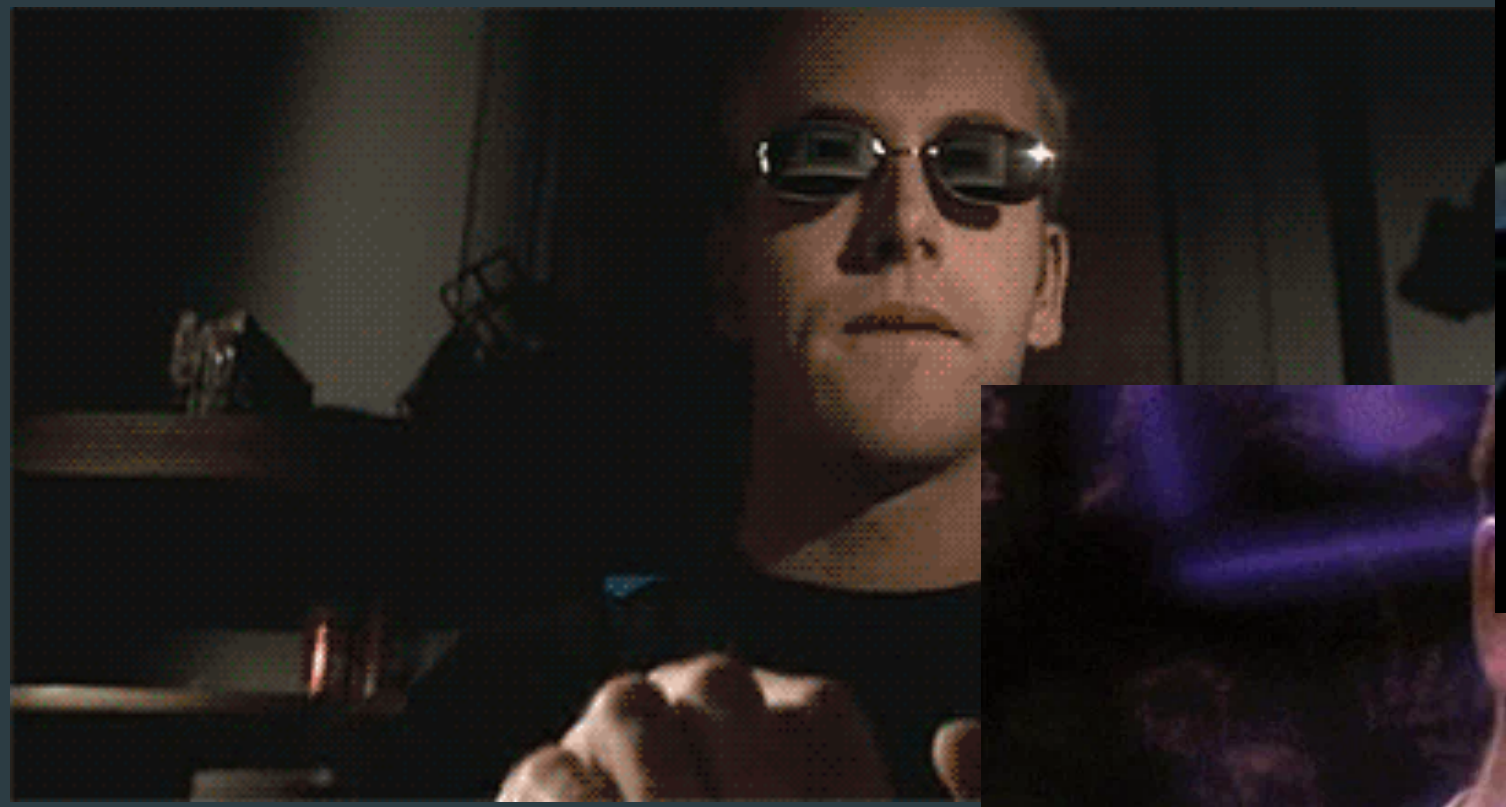
- https://github.com/OJ/gobuster
  - “Directory/file & DNS busting tool written in Go” by OJ (@TheColonial)
- Go + Lambda != <3
  - Native support coming at some stage..
  - Many projects to help in the meantime!
- https://github.com/apex/apex
  - Easy to (compile), deploy and invoke lambda functions (including Go!)

@_devalias #gopherblazer

The Plan

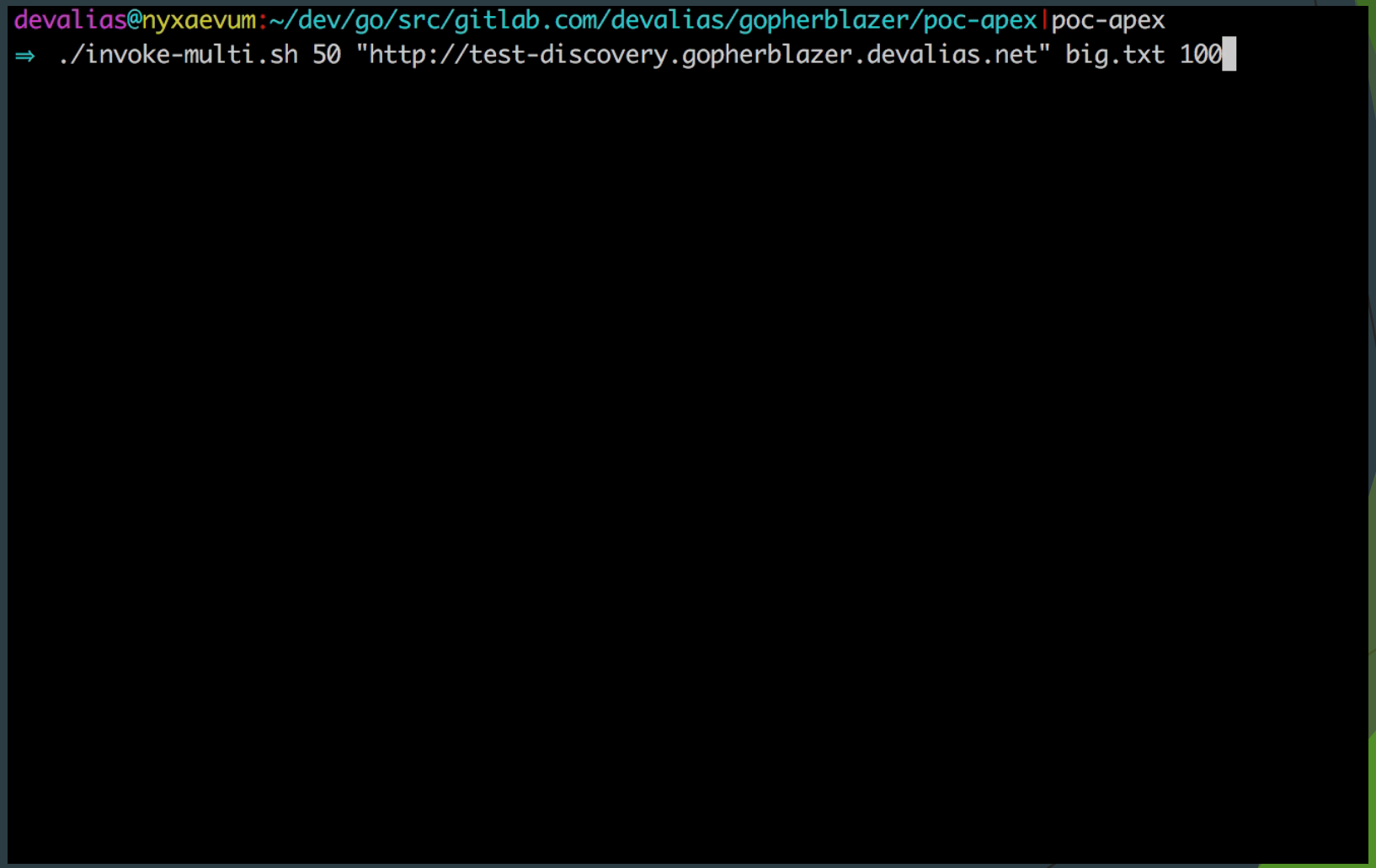
- DirBusting is too slow
  - I want to see all the things NOW!
- Slice up the wordlist into X slices
- Run each slice in parallel #InTheCloud™ with Lambda
- ???
- Profit!
  - HACK ALL THE THINGS!

We’re gonna need a montage..



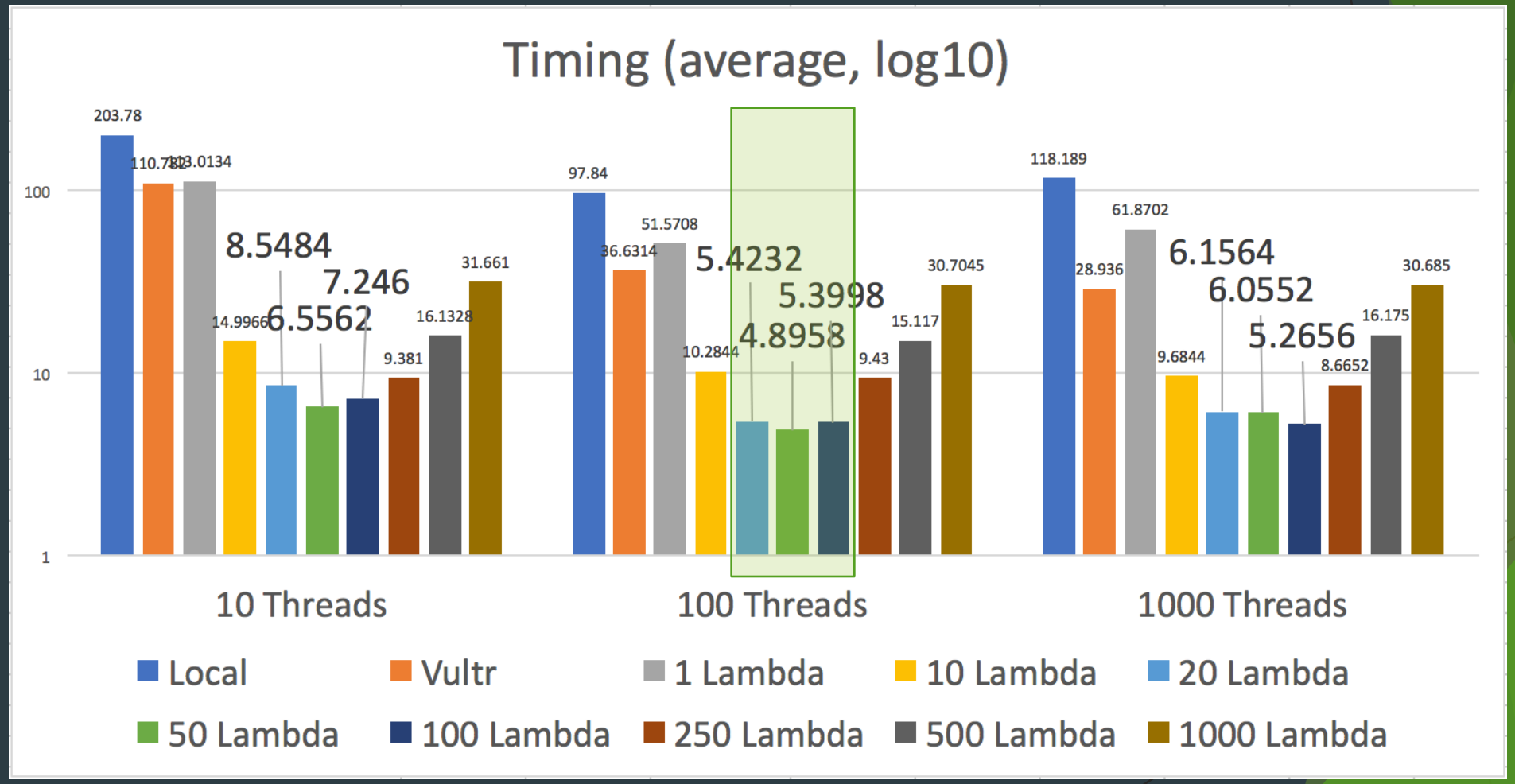
@_devalias #gopherblazer

Pray to the demo gods..



@_devalias #gopherblazer

Now I'm no data scientist..



@_devalias #gopherblazer

Today I Learned

- Use 50 lambda slices with 100 gobuster threads each (~4.89sec/~20.4k words)
  - Though 20-100 slices really close
- Lambda is really (really!) cheap ($1 == ~5.5 days compute time)
  - Total cost: $0.05
  - Invocations: 17,218
  - Duration: 6h 3m 32.265s
- Collecting data and making charts takes a while..
- Try it at home
  - https://github.com/0xdevalias/gopherblazer/tree/poc-apex

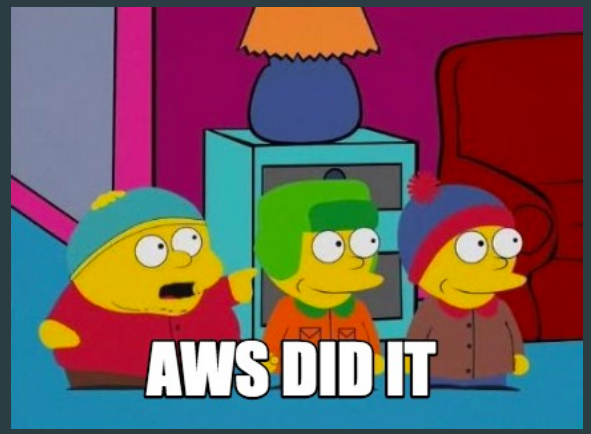
@_devalias #gopherblazer

Better, FaaSter, Stronger!

- What other stuff could we do?
  - Nmap UDP scans
  - Port scanning entire subnets
  - Website crawling, screenshots, basic checks..
  - XSS/XXE/etc payload callbacks
  - Distributed fuzzing
- So much potential for disruptive tooling!
  - Limitations of the Lambda environment might be annoying..

AWS already did that..

- Elastic Compute Cloud (EC2) + Auto Scaling
- EC2 Container Service (ECS): EC2++ for containers
- Batch: define a job, connect a queue, runs on ECS
- <thing you need>
  - Launching ~2 weeks before you think you need it



amazon web services

OpenFaaS

- https://www.openfaas.com/ (@OpenFaaS, #OpenFaaS)
  - "Serverless Functions Made Simple"
  - Since December 2016
- Cloud functions, your hardware, with the full power of Docker
- Really easy to use
  - `faas-cli build -f https://hakt.us/funcs.yml`
  - `faas-cli deploy -f https://hakt.us/funcs.yml`
  - `echo "Hack" | faas-cli invoke TheGibson > /root/.workspace/.garbage`

@_devalias #gopherblazer

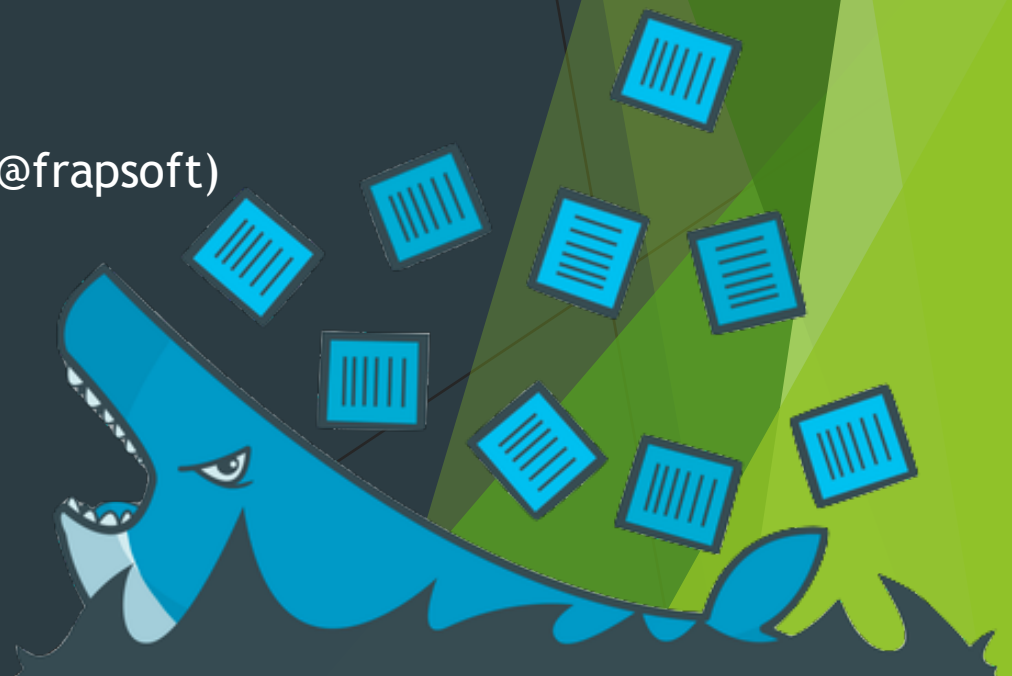
Image to OpenFaaS in 1..4

- Turn an existing Docker image into an OpenFaaS function
- It just takes 4 lines:
  - `FROM foo/existing:image`
  - `ADD https://github.com/openfaas/faas/releases/download/0.6.11/fwatchdog /usr/bin`
  - `ENV fprocess="run-my-program"`
  - `CMD ["fwatchdog"]`

@_devalias #gopherblazer

Offensive Docker

- Familiar collections
  - https://hub.docker.com/r/kalilinux/kali-linux-docker/
- Common tools
  - https://hub.docker.com/r/devalias/gobuster/
  - https://github.com/ellerbrock/docker-security-images (@frapsoft)
    - (nmap, scanssh, tcpdump, arpon, aircrack-ng, snort, nikto..)
  - https://hub.docker.com/u/ilyaglow/(@ilyaglotov)
    - (beef, empire, sqlmap, masscan, metasploit, quark, timesketch..)



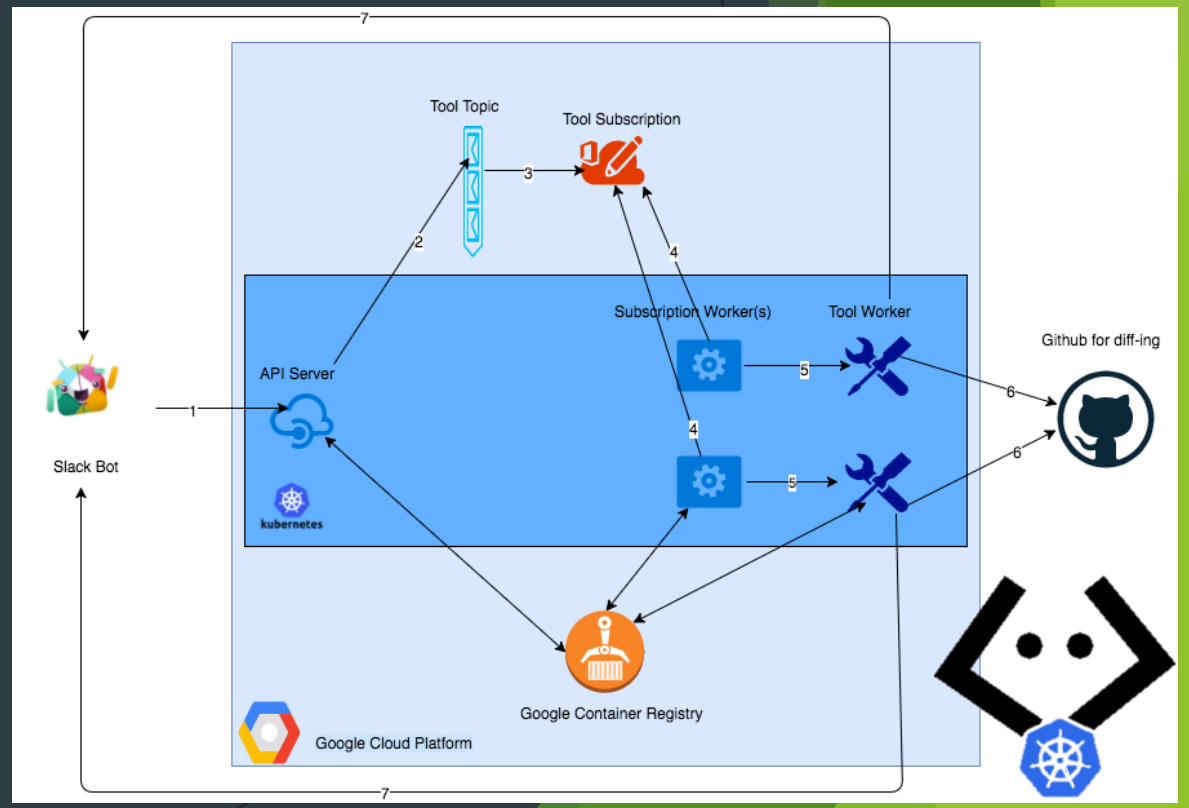
@_devalias #gopherblazer

Brutesubs

- https://github.com/anshumanbh/brutesubs (@anshuman_bh)
  - "An automation framework for running multiple open sourced subdomain bruteforcing tools (in parallel) using your own wordlists via Docker Compose"
- Tools
  - gobuster (@TheColonial)
  - Recon-ng + enumall (@LaNMaSteR53, @Jhaddix)
  - Sublist3r / subbrute (@aboul3la, TheRook)
  - Altdns (@infosec_au)

Kubebot

- https://github.com/anshumanbh/kubebot (@anshuman_bh)
  - "A security testing Slackbot built with a Kubernetes backend on the Google Cloud Platform"
- Features
  - Initiate scans from Slack, request queued
  - Tools scheduled, run on Kubernetes cluster
  - Results stored in Git
  - Differential results returned to Slack
- `/runtool nmap|-Pn -p 1-1000|google.com`



@_devalias #gopherblazer

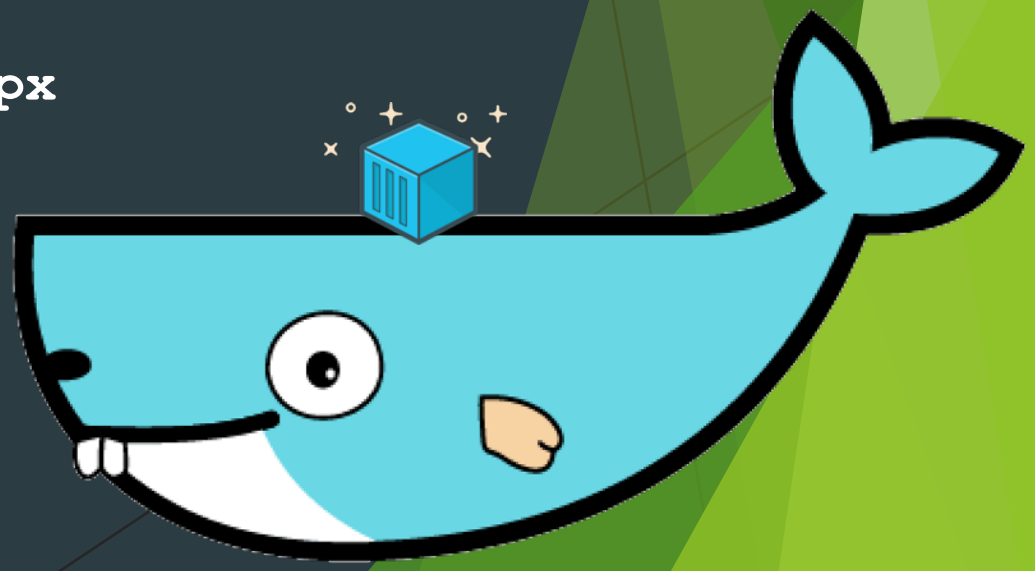
Choosing Wisely

- Heaps of dockerised tooling out there, only a Google away
- But how do you know which to use?
- Things I look for:
  - Official: Is it the official image for the project?
  - Stars: Is it the most starred or pulled image for this project?
  - Source: Is the Dockerfile available?
  - Automated: It is an automated build?
  - Updated: When was it last pushed?
  - Size: How big is it?

Tiny Golang Containers

- Golang static compilation
  - `RUN CGO_ENABLED=0 GOOS=linux \`
  - `go build -ldflags="-s -w" -o gobuster`
- Docker multi build stage (since v17.05) + 'FROM scratch'
- UPX: the Ultimate Packer for eXecutables
  - `RUN upx --brute gobuster -ogobuster.upx`

- Example Dockerfile (~1mb container)
  - https://github.com/0xdevalias/docker-gobuster



@_devalias #gopherblazer

Golang CLI's with Cobra

- https://github.com/spf13/cobra
  - Program and library for creating easy, powerful command line (CLI) applications, in Go.
- No more boilerplate-based new project delays..
  - `go get -u github.com/spf13/cobra/cobra`
  - `cobra init github.com/myUsername/fooApp`
  - `cd $GOPATH/src/github.com/myUsername/fooApp`
  - `cobra add bar`
  - `go run main.go`
- https://github.com/0xdevalias/gopherblazer/tree/poc-cli/poc-cli

@_devalias #gopherblazer

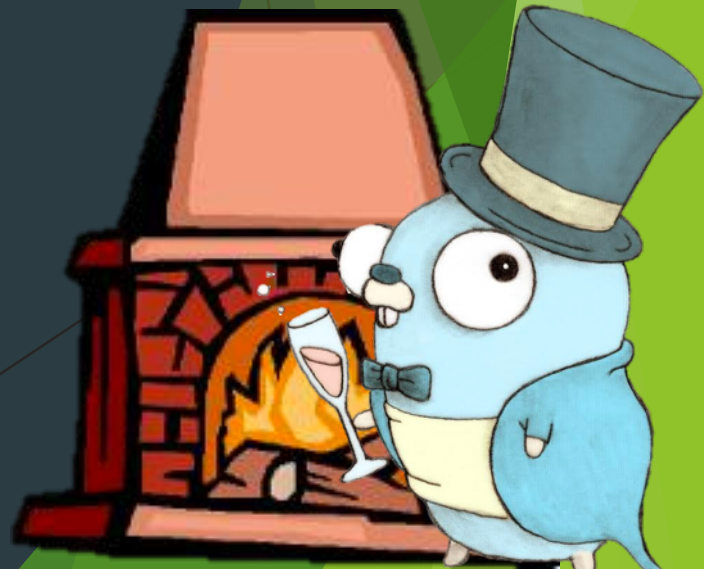
My own pretty CLI, just like Docker!

```
devalias@nyxaevum:~/dev/go/src/github.com/devalias/fooApp
⇒  go run main.go
A longer description that spans multiple lines and likely contains
examples and usage of using your application. For example:

Cobra is a CLI library for Go that empowers applications.
This application is a tool to generate the needed files
to quickly create a Cobra application.

Usage:
  fooApp [command]

Available Commands:
  bar         A brief description of your command
  help        Help about any command

Flags:
      --config string   config file (default is $HOME/.fooApp.yaml)
  -h, --help            help for fooApp
  -t, --toggle          Help message for toggle

Use "fooApp [command] --help" for more information about a command.
```

@_devalias #gopherblazer

GopherBlazer

- The Plan
  - Single ‘source of truth’ for my pentest tool stack, shareable
  - Replace shell script wrappers
  - Add ‘connectors’ to wrap Docker run commands, AWS lambda, OpenFaaS, etc
- Currently
  - Not that much.. 😅
  - Spent a lot of time playing with ideas, PoCs and rabbit holes
- Where?
  - https://github.com/0xdevalias/gopherblazer (TBC..)



@_devalias #gopherblazer

Future Directions

- Actually code GopherBlazer CLI tool.. 😅
- More tools
- More automation
- Explore other ways to (ab)use Docker
  - Eg. SONM (Supercomputer Organized by Network Mining)
    - https://sonm.io/

Takeaways

- Be Curious
- Play
- Disrupt
- Share

@_devalias #gopherblazer

Think Different

"Here's to the crazy ones. The misfits. The rebels. The troublemakers. The round pegs in the square holes. The ones who see things differently.

Because the people who are crazy enough to think they can change the world, are the ones who do."

– Steve Jobs / Rob Siltanen

Questions?

@_devalias #gopherblazer