Fuzzing FTW

DEF CON 26



Newest Slides & Other Training Materials

The newest slides & other training materials for this workshop are on GitHub at:

- https://github.com/cno-io/fuzzing_ftw

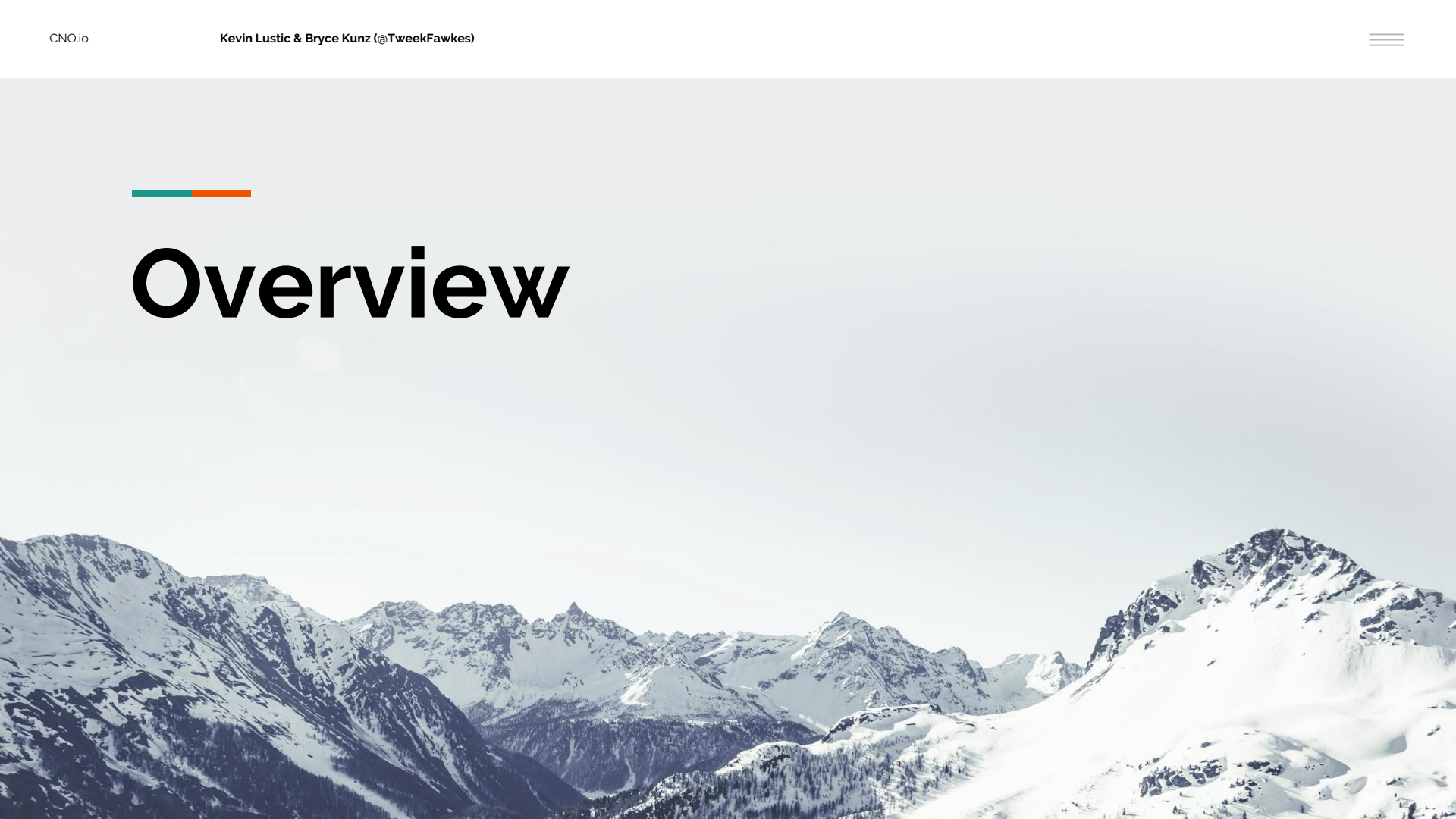


Who Are We?

- Kevin Lustic - Red Team Lead at Adobe DX
- Bryce Kunz - Stage 2 Security, Red Teaming & Splunk Security Services



Overview



Fuzzing Process
Overview

Fuzzing Process Overview:

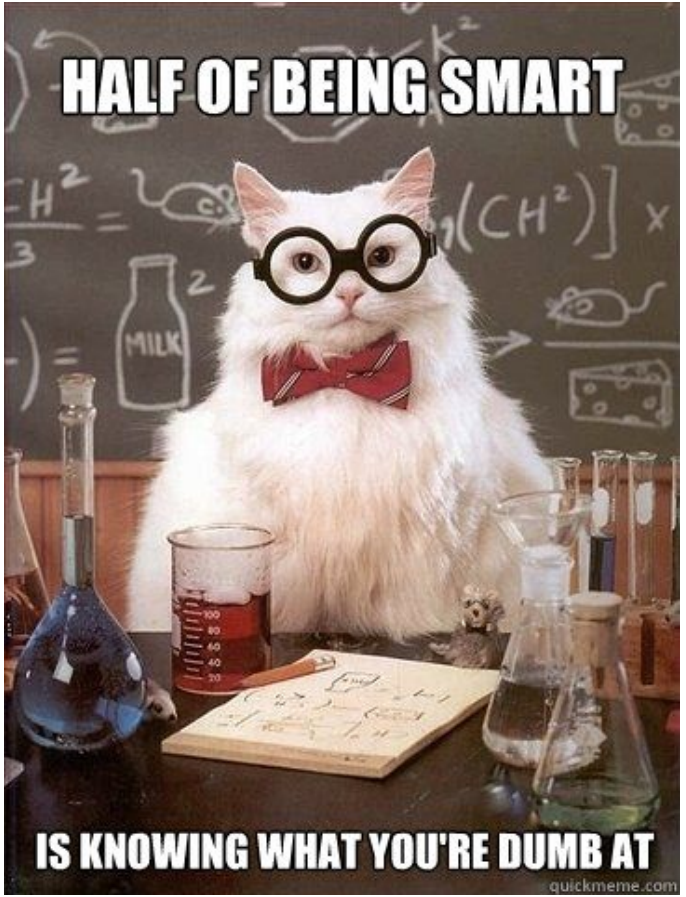
- Acquire Knowledge
- Instrumentation
- Delivery
- Generation
- Scale
- Repeat!



#1 Acquire Knowledge
Fuzzing Process

Just enough to do some effective fuzzing, do not over think it.

- Prior Research
- Stack Overflow
- Documentation
- Code Review
- Reverse Engineering
- Etc...



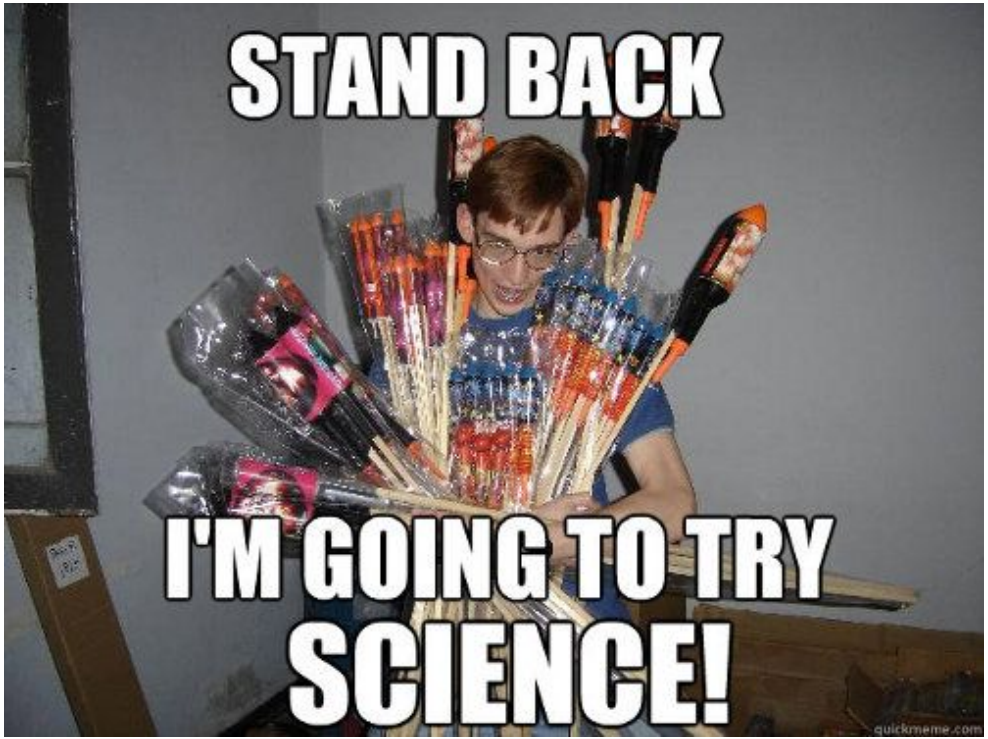
#2 Instrumentation
Fuzzing Process

How will we know when the process has crashed?



#3 Delivery
Fuzzing Process

How will we get our fuzzed payloads to the target?



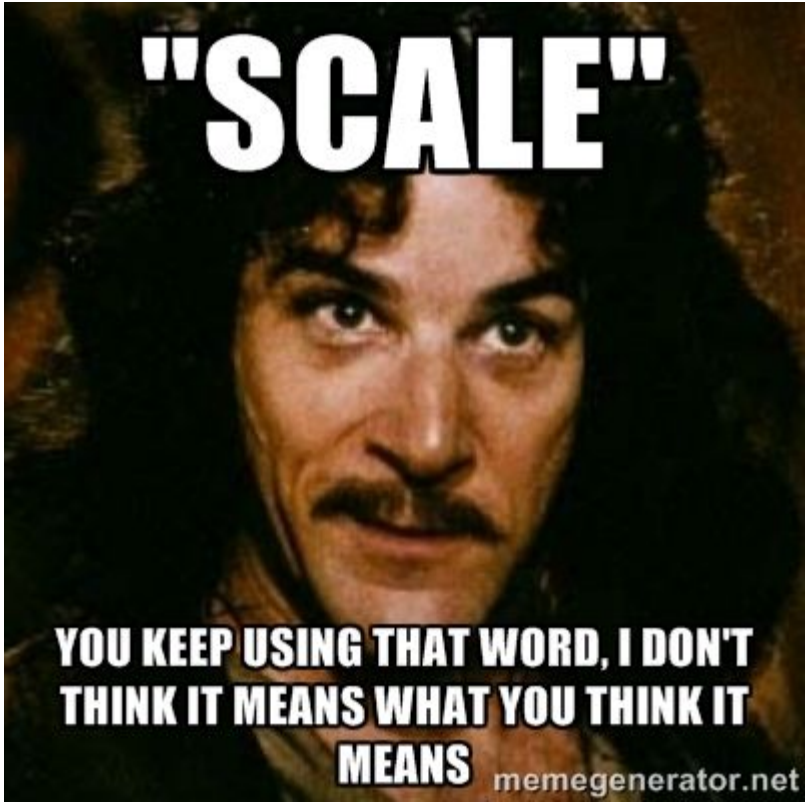
#4 Generation
Fuzzing Process

How will we generate new fuzzed payloads?



#5 Scale
Fuzzing Process

How will we scale this fuzzing operations?

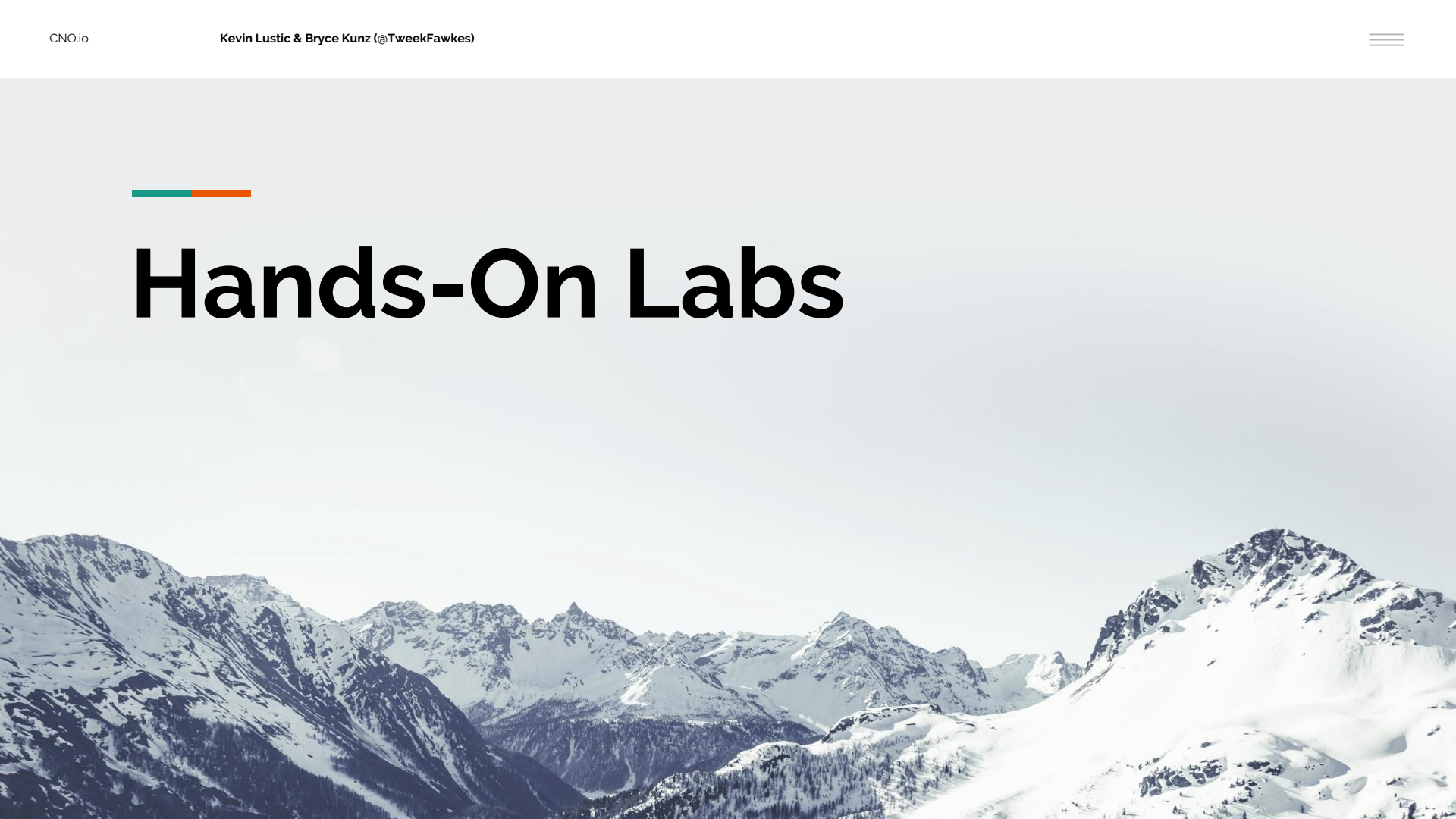


#6 Repeat!
Fuzzing Process

Get a minimal viable fuzzing operations underway ASAP, then come back to each of these steps and progressively improve the operation over time.



Hands-On Labs



Blind Fuzzing with Radamsa

Hands-On Lab

...



Function Fuzzing with libFuzzer

Hands-On Lab

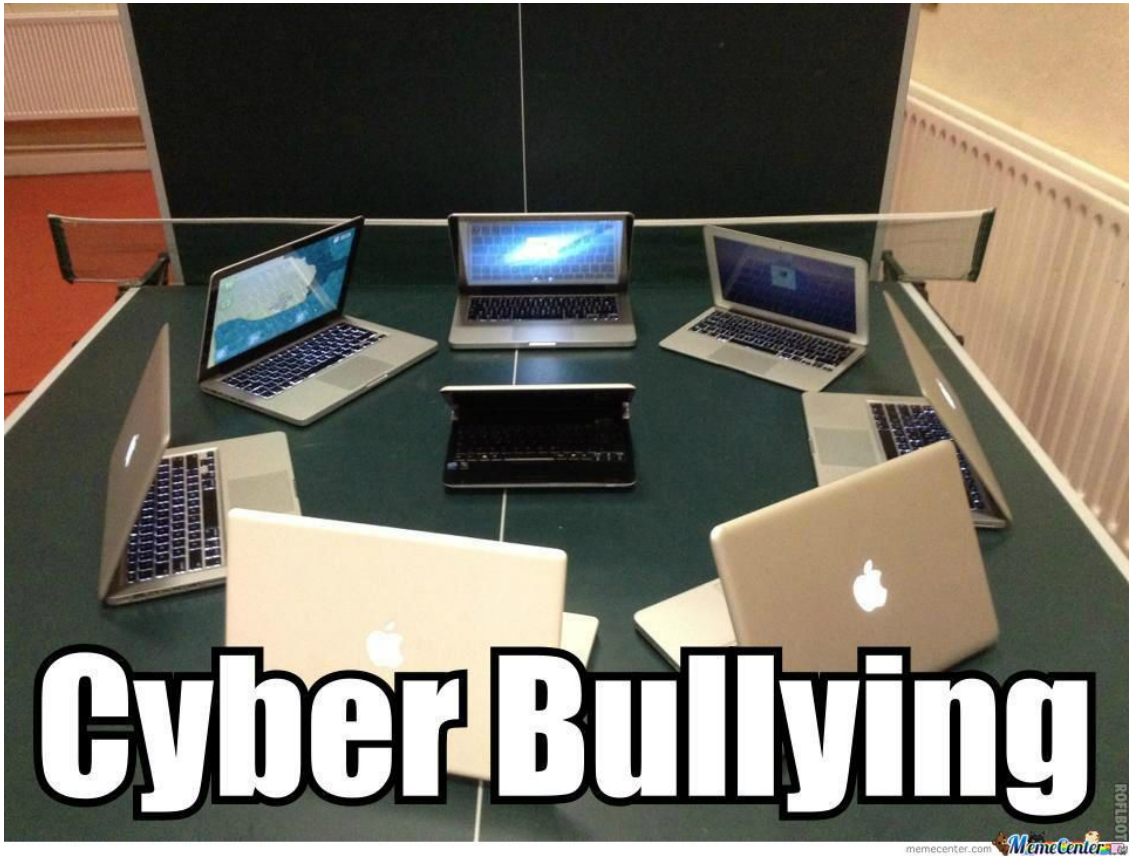
...



File Fuzzing with AFL

Hands-On Lab

...



Network Fuzzing with BooFuzz (Sulley)

Hands-On Lab

...



API Fuzzing with Bradamsa

Hands-On Lab

...



Thank you!

- CNO.io
  - https://github.com/cno-io/fuzzing_ftw

