5 Years and 40,000+ Hours Later:

Lessons Learned from Running a National Penetration Testing Competition

Dan Borges & Tom Kopchak
@1njection, @tomkopchak, @NationalCPTC

Agenda

- What is the National Collegiate Penetration Testing Competition?
- What is it about us that makes us so unique?
- How we hacked together a relevant competition
- Review of the competition data
- Sharing some of our success stories
- How to get involved

What is CPTC?

The mile high elevator pitch and scope.

- **What:** An annual college level competition.
- **Why:** To focus on developing consulting skills.
- **How:** Offensive Security + Custom Environment + Business = CPTC

About Us

CPTC
COLLEGIATE PENTESTING COMPETITION

Dan

CPTC Life: OSINT/World Design/Competition Design, w/ CPTC 4 years
Real Life: Senior Internal Red Teamer

Tom

CPTC Life: White Team & Monitoring Team Captain, Competition Director, w/ CPTC since inception
Real Life: Director of Technical Operations

CPTC Advisory Board

CPTC
COLLEGIATE PENTESTING COMPETITION

Participating Colleges - 2019

American University of Sharjah
Augusta Technical College
Augusta University
Baldwin Wallace University
Cabrillo College
California State Polytechnic
California State University, Fullerton
City College of San Francisco
Clemson University
College of Charleston
College of Coastal Georgia
Columbus State University
CSU, Chico
Dakota State University
DePaul University
Drexel University
Excelsior College
Florida State University
Kennesaw State University
Marshall University
Middle Georgia State University
National University
North Dakota State University
Penn State University
Rochester Institute of Technology
Rochester Institute of Technology, Dubai
Southern Methodist University
St. Petersburg College
Stanford University
Syracuse University
Tennessee Tech University
Texas A&M, San Antonio
The University of Texas at San Antonio
Tiffin University
United States Military Academy at West Point
University at Buffalo
University of Advancing Technology
University of California, Berkeley
University of California, Riverside
University of California: Davis
University of Central Florida
University of Florida
University of Maine
University of New Hampshire
University of New Haven
University of Northern Iowa
University of Tulsa
University of Virginia
University, Pomona
US Air Force Academy
Virginia Commonwealth University

What is the National Collegiate Pentesting Competition?

Why Does CPTC Even Exist?

- **CPTC started in 2015 as an idea:**
  - To teach offensive security, but do it responsibly
  - Brainchild of Professor Bill Stackpole (RIT) and Bob Kalka (IBM)
- **It is a competition that has been making great strides to:**
  - Leverage the expertise of those with industry experience
  - Have a grand, (inter)national style with a broad scope

What Makes CPTC Different from a CTF?

Competition in name only:

- Teams compete, but education is the primary goal
- Over 10 specialty awards, highlighting exceptional activity

What CPTC isn't:

- Traditional CTF
- Jeopardy style questions
- King of the hill
- Defense only

What CPTC is:

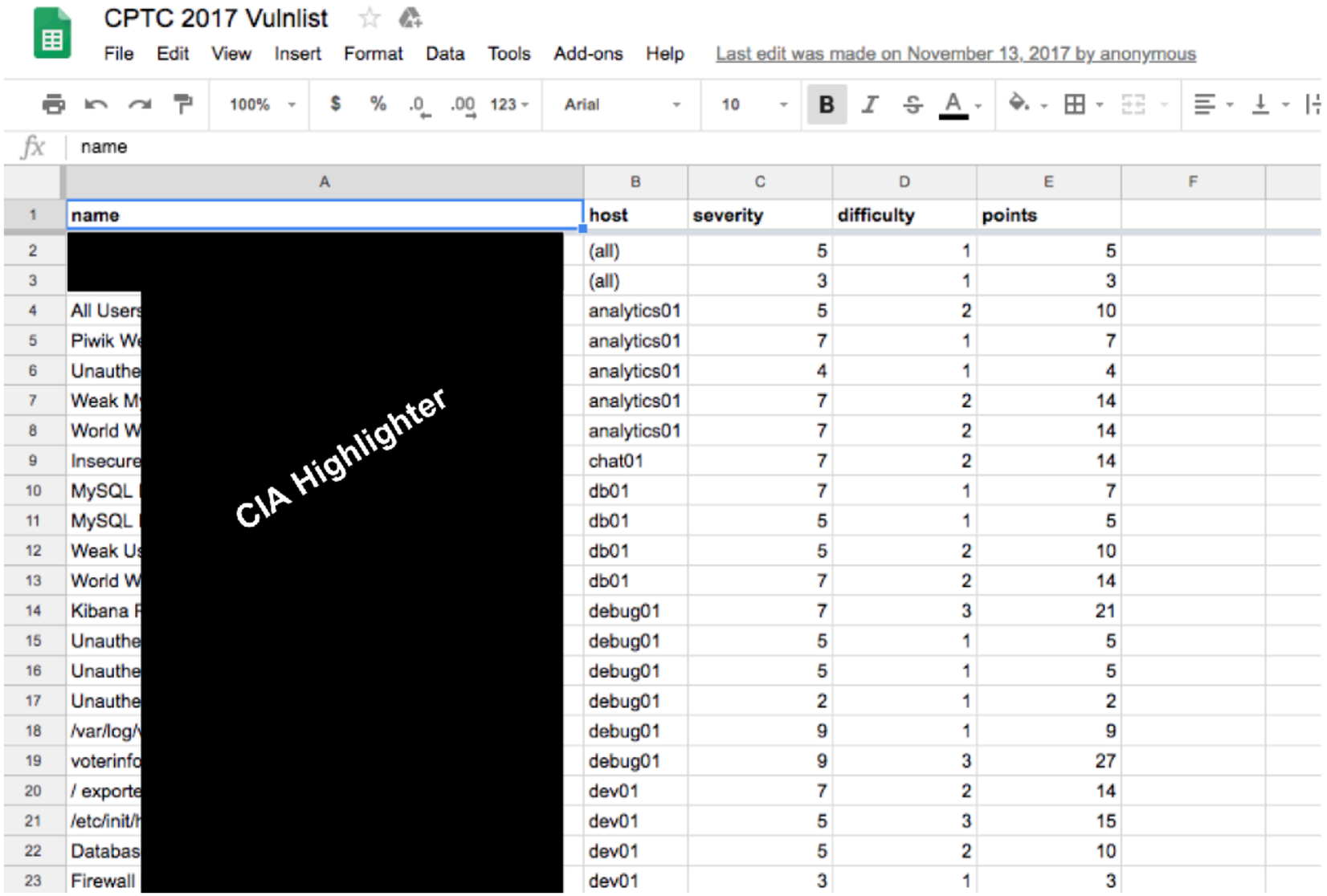
- Professional consulting engagement
- Security assessment for a real(ish) company
- Analogy: Doctor working with patient

Beyond the CTF Format - Bringing in Business

- Multiple attack paths
- A realistic corporate environment
- Responsibility for continued function of the infrastructure
- Hundreds of potential configuration issues
- Identify issues of significance and business impact
  - You won’t find everything
  - We won’t find everything
  - Targets aren’t clearly marked - this must be determined during the event
  - Teams MUST consider impact of actions against a running business

Vulnerabilities! (We Have Them)

CPTC
COLLEGIATE PENTESTING COMPETITION



	name	host	severity	difficulty	points
2		(all)	5	1	5
3		(all)	3	1	3
4	All Users	analytics01	5	2	10
5	Piwik We	analytics01	7	1	7
6	Unauthe	analytics01	4	1	4
7	Weak M	analytics01	7	2	14
8	World W	analytics01	7	2	14
9	Insecure	chat01	7	2	14
10	MySQL	db01	7	1	7
11	MySQL	db01	5	1	5
12	Weak Us	db01	5	2	10
13	World W	db01	7	2	14
14	Kibana F	debug01	7	3	21
15	Unauthe	debug01	5	1	5
16	Unauthe	debug01	5	1	5
17	Unauthe	debug01	2	1	2
18	/var/log/	debug01	9	1	9
19	voterinfo	debug01	9	3	27
20	/ exporte	dev01	7	2	14
21	/etc/init/	dev01	5	3	15
22	Databas	dev01	5	2	10
23	Firewall	dev01	3	1	3

The Soft Skills: As Important as Technical

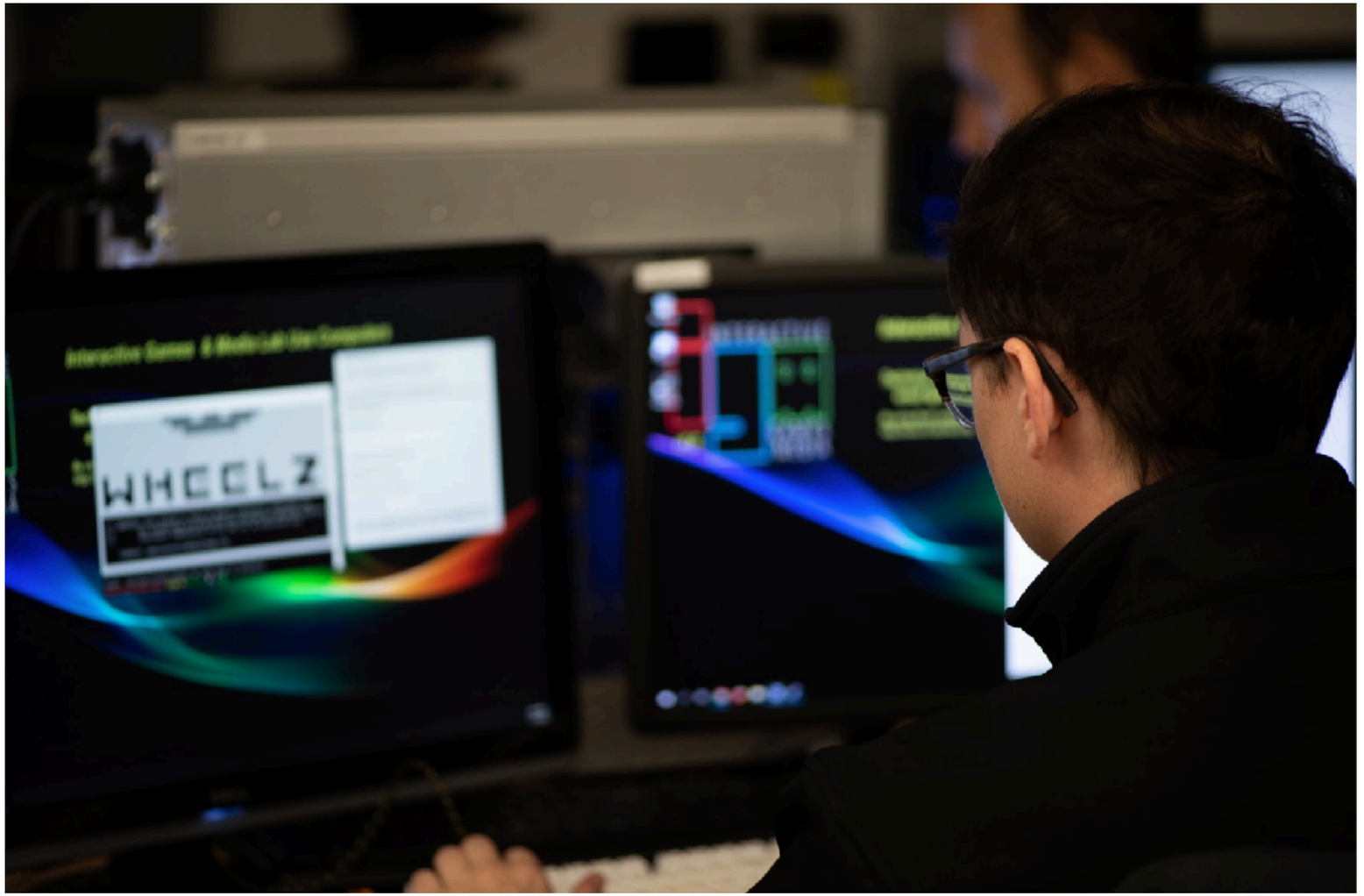
- **Team Deliverables:** Written report and presentation to senior management
- **Reports Scoring:**
  - Technical findings
  - Overall quality/presentation
- **Presentations Scoring:**
  - Quality
  - Appropriateness for executive level audience
- All scoring is done by teams of industry professionals who volunteer their time for the event
- **2018 Addition:** Coaches score all other teams for some events
- Overall Teamwork

Education

- Everything we do revolves around teaching
- How to be a consultant and work with clients
- Teaching real world pentesting skills:
  - How to pass-the-hash?
  - How to mitigate a DDoS attack?
- We can (and do) add to the event in real-time

Hacking Together a Relevant Competition

CPTC
COLLEGIATE PENTESTING COMPETITION



Past Competition Themes

- **2015 -** General Business Infrastructure
- **2016 -** Healthcare
- **2017 -** Elections
- **2018 -** Autonomous vehicles

Future Competition Themes

Time to Announce the 2019 Theme

DinoBank

DINO BANK

DinoBank - Company Overview

DinoBank was originally founded in 2005 as a du novo bank using technology to enable our customers to bank on their terms. Our largest presence is electronic, and we have been a leader in pushing the adoption of new banking innovations. Furthermore, physical branches are expensive, so we don’t have many of them. Those that we do have are placed in strategic locations for those times when you just need in-person help.

We utilize advanced Automated Teller Machines (ATM), Mobile Phone Banking, and Online Banking so that customers can use their money on their time. Additionally, by keeping our costs down we can pass on that savings to you.

We are performing a penetration test, as our recent IT exam has shown several issues and our examiners are issuing a Memorandum of Understanding (MOU) with our Board of Directors. One of these items is the requirement to perform a test and resolve these issues. The success of this project is critical to ensure the ongoing viability of our banking operations.

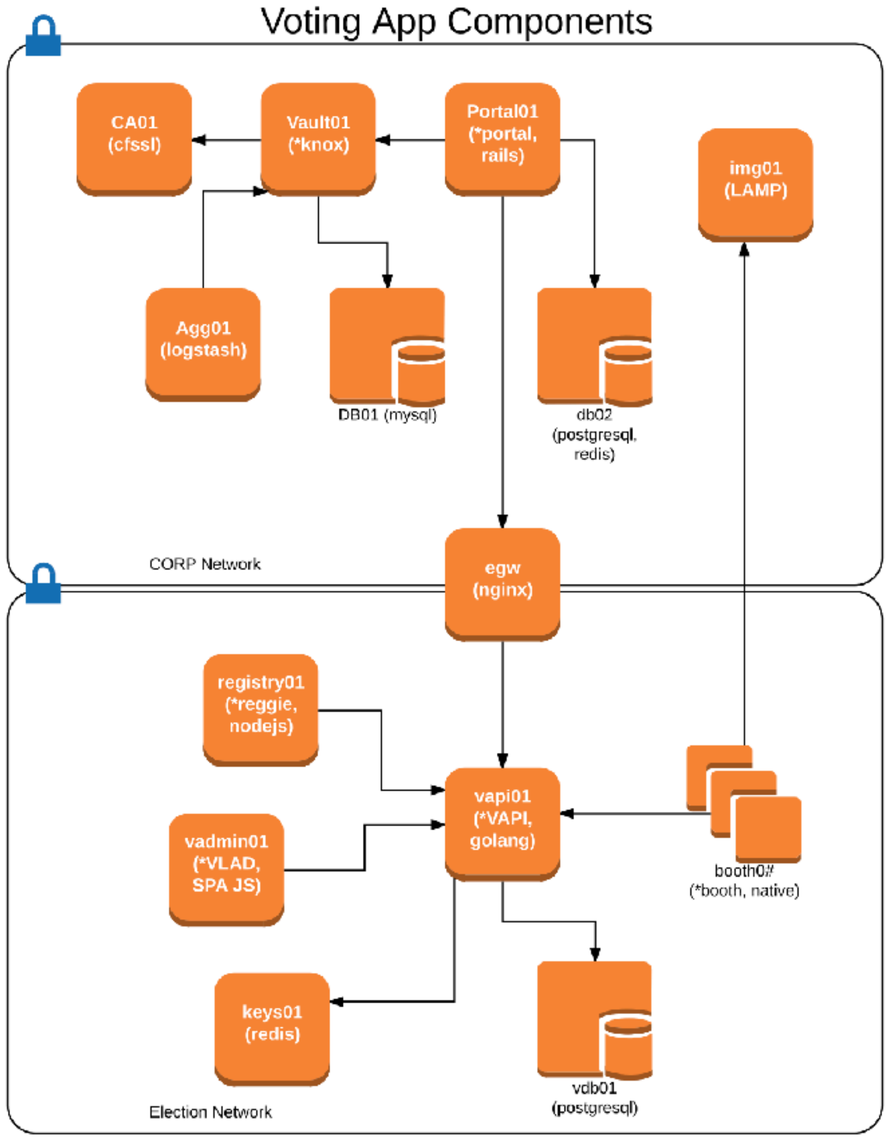
Future Events

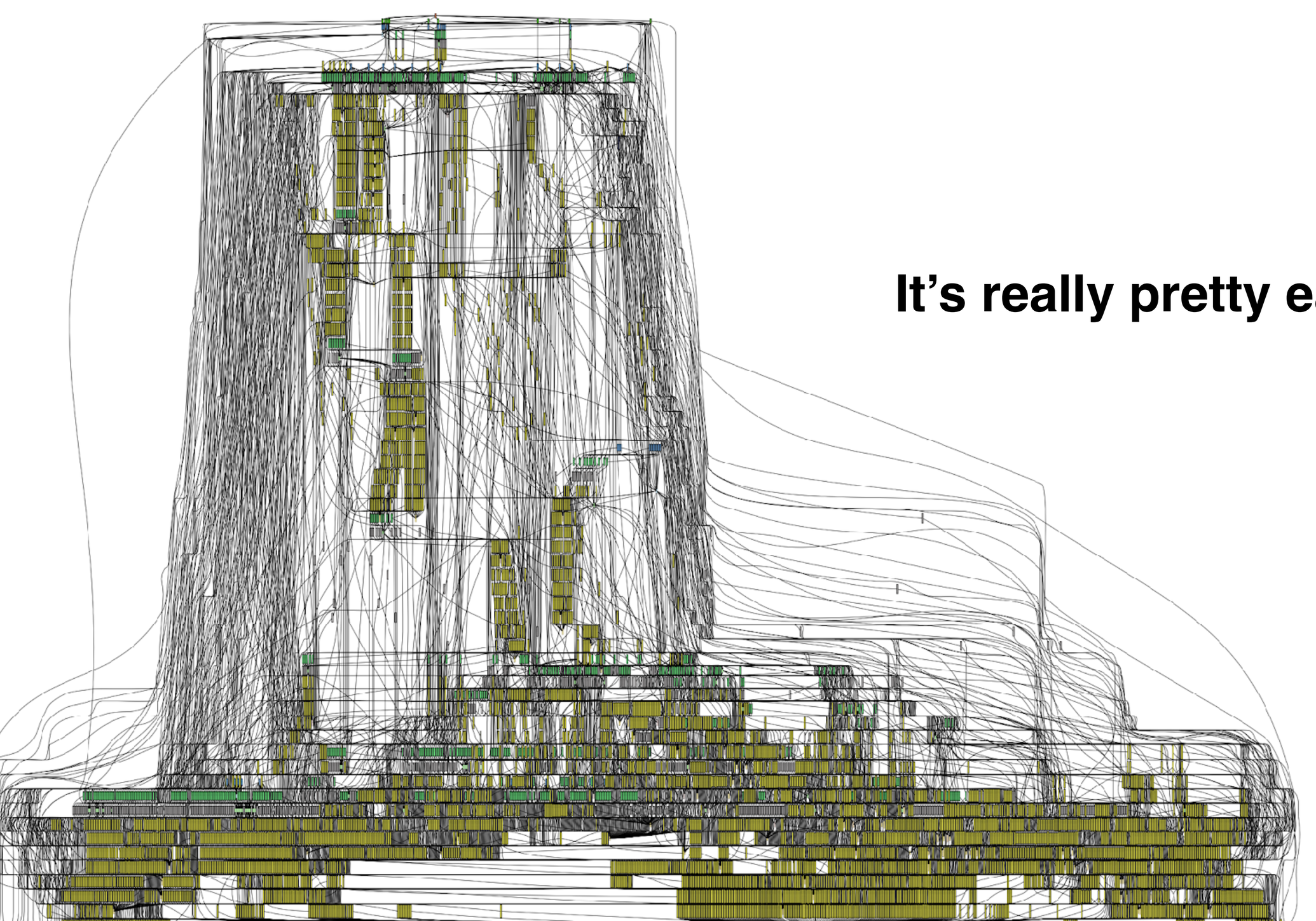
Growth of the event - international regional in 2019!

We are already working with exciting partners to make 2020 one of our most interactive environments ever!

What's the Environment Like?

- Increasing scale at each event
  - Custom tooling to make it happen
    - Past LaForge talk, BSides LV 2018
- Emphasis on custom apps and pivoting
- Mix of open source and commercial applications
- Multiple networks
- 40+ targets per team
- 100s of "employees"

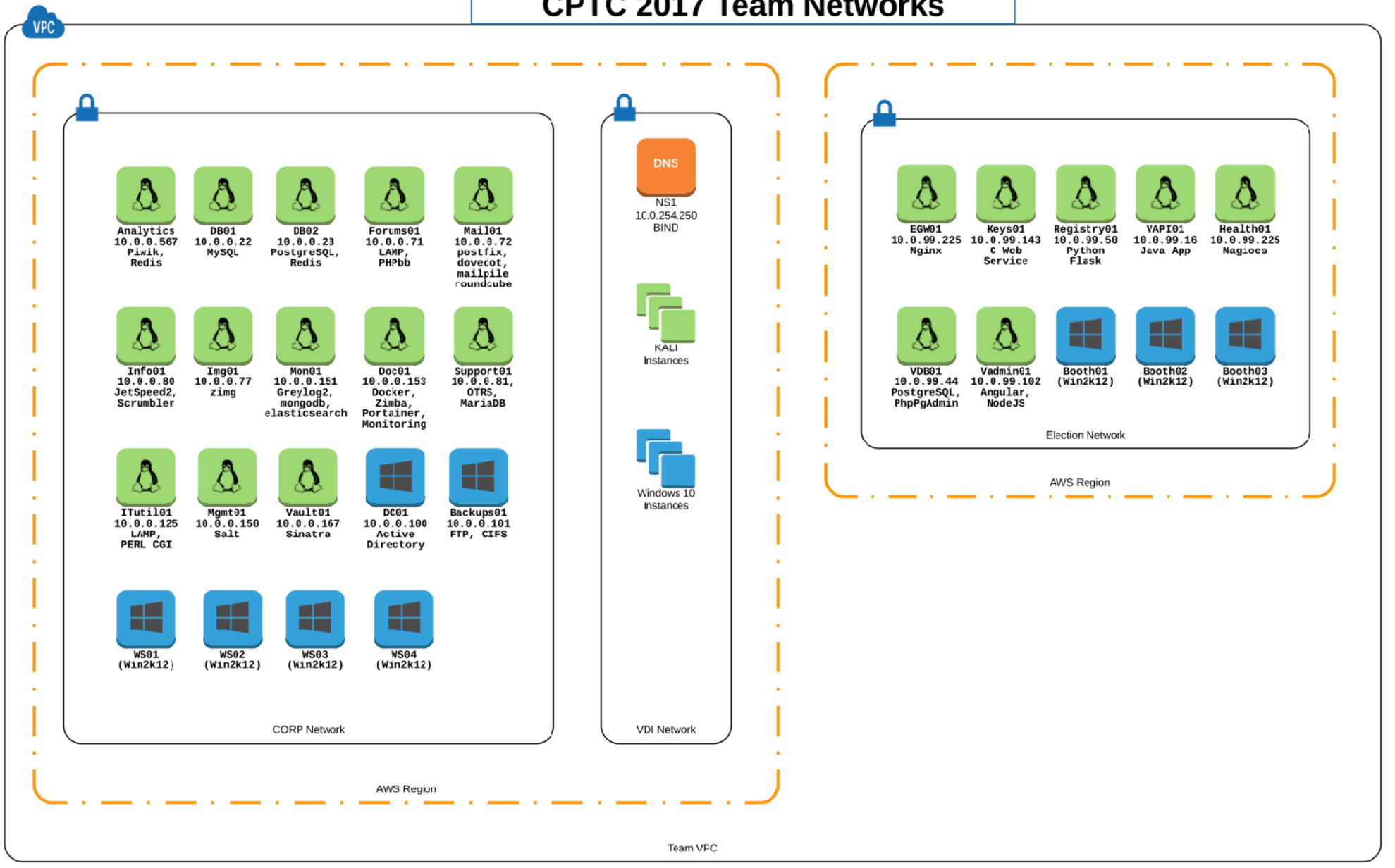




CPTC
COLLEGIATE PENTESTING COMPETITION

It’s really pretty easy….

CPTC 2017 Team Networks



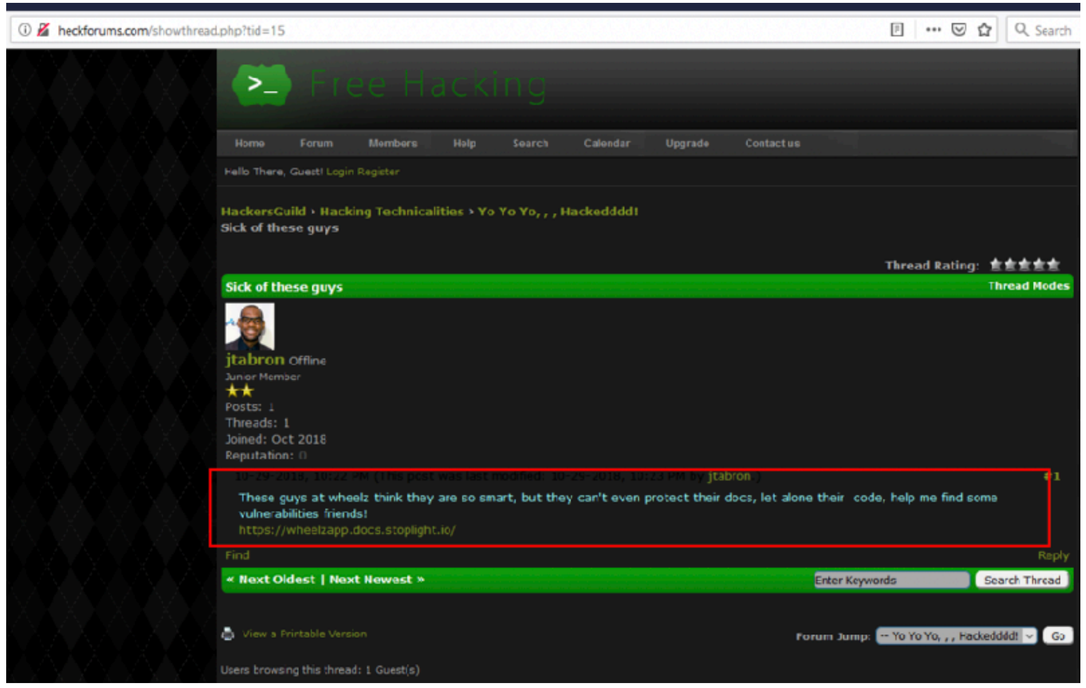
World Building

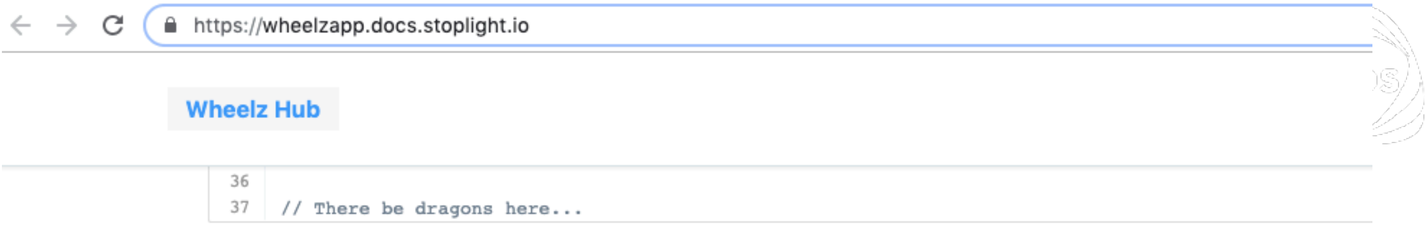
Significant emphasis on making the company exist:

- Online presence
- Social media profiles of key individuals
- Environment seeded with data to tell the story
  - Chat server with dialog between employees
  - Database with information that can lead to other access
  - Credentials in random text files

Stories

Public disclosure of custom APIs
(e.g. https://wheelzapp.docs.stoplight.io/)





Wheelz Production

Microservices

- DAPI - source of truth for authN/authZ, identity, and login
- LAPI - realtime trips, locations, and bookings
- Warren Buffet - Payments and transactions
- Compass - GPS guidance and navigation
- Armada - Administrative fleet tracking UI
- Golden Snitch - Safety and maintenance monitoring
- Scotty - Autonomous vehicle stack

Shared Libraries

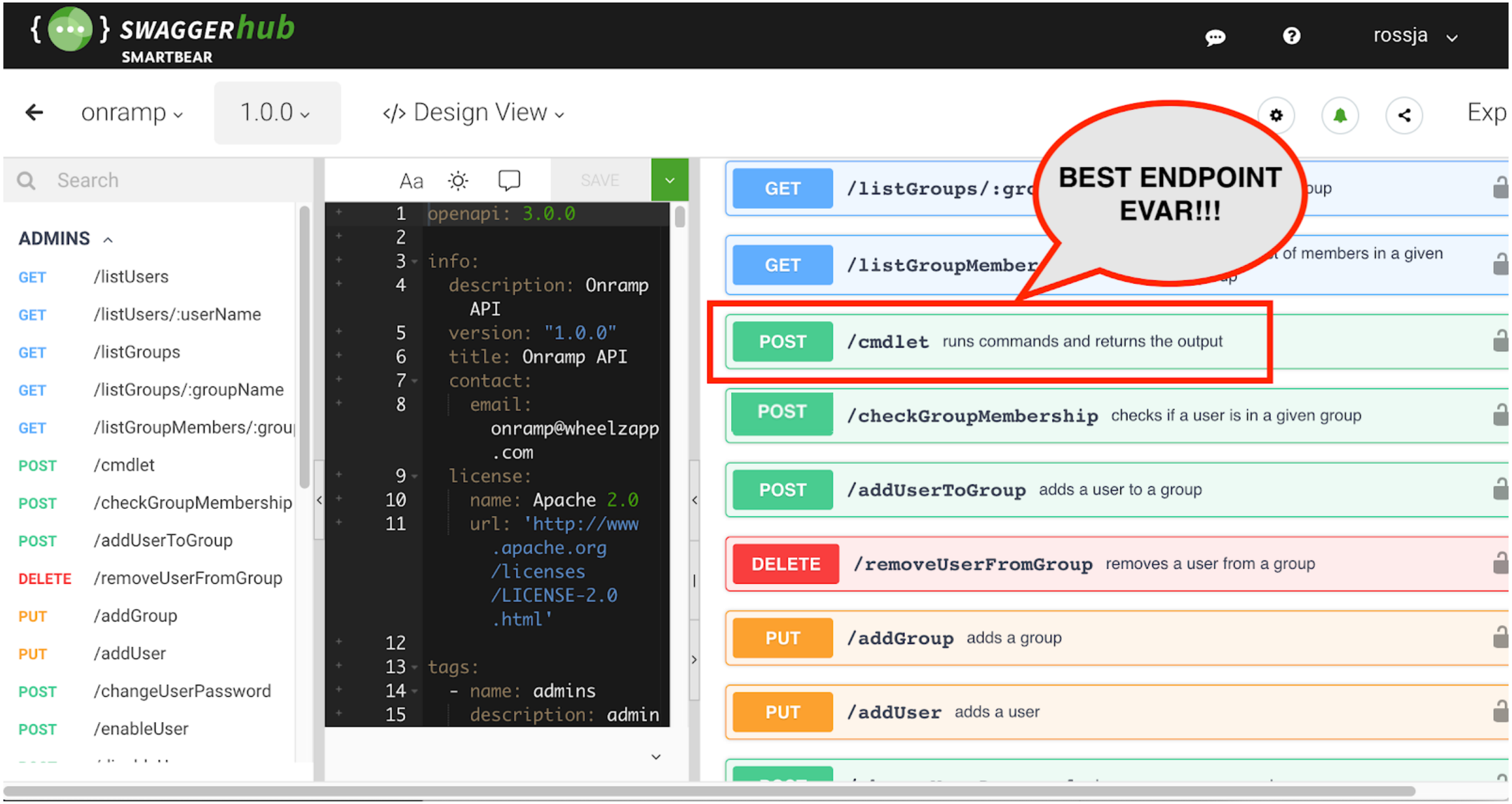
These are the shared libraries used by most services:

- **authorizer** - Shared AuthN/AuthZ lib. Implements an API Authorizer interface for the SOA APIs as well as wraps
- **wheelz** - This is where the primary models live. Do **not** edit any file in that package that has an autogenerated script.
- **wheelzdb** - Database toolkit for the API services. Has a bunch of stuff setup to automatically setup data persis Redis
- **wheelzlog** - Generalized logging library that uses a singleton model and creates a bunch of turnkey stuff for cr
- **wheelzutil** - Misc. stuff including a random Token generator and an object merge that works with two objects

Developing APIs

The only place you need to write code for any of the backends are in some very specific files. Every app has a `cli`
Inside `restapi`, you'll find files with the prefix `handlers_`. These files contain the implementations for each Oper
reference, check out `dapi/restapi/handlers_admin.go`.

Our APIs Have Fun Quirks and Features



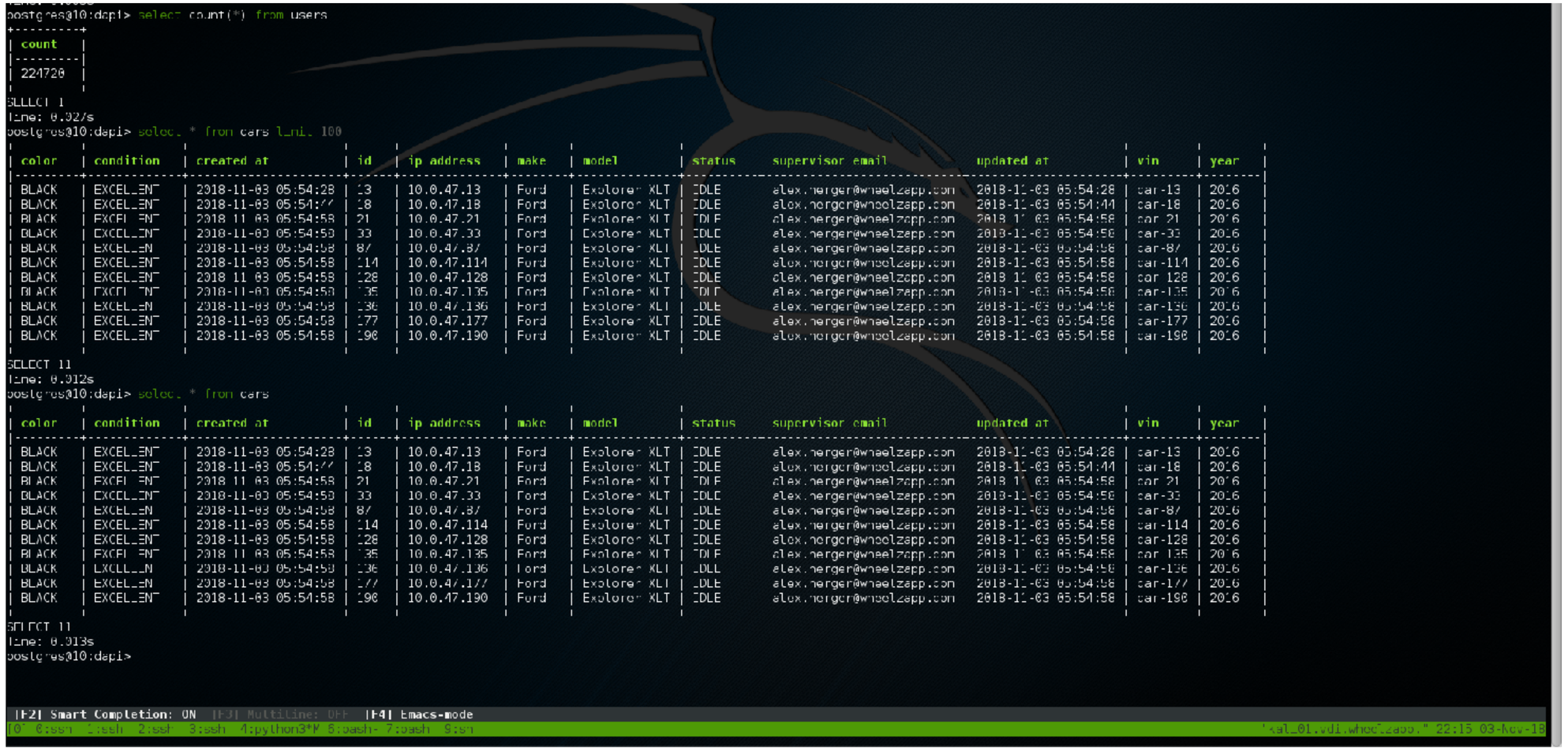
Stories

Database with information that can lead to other access

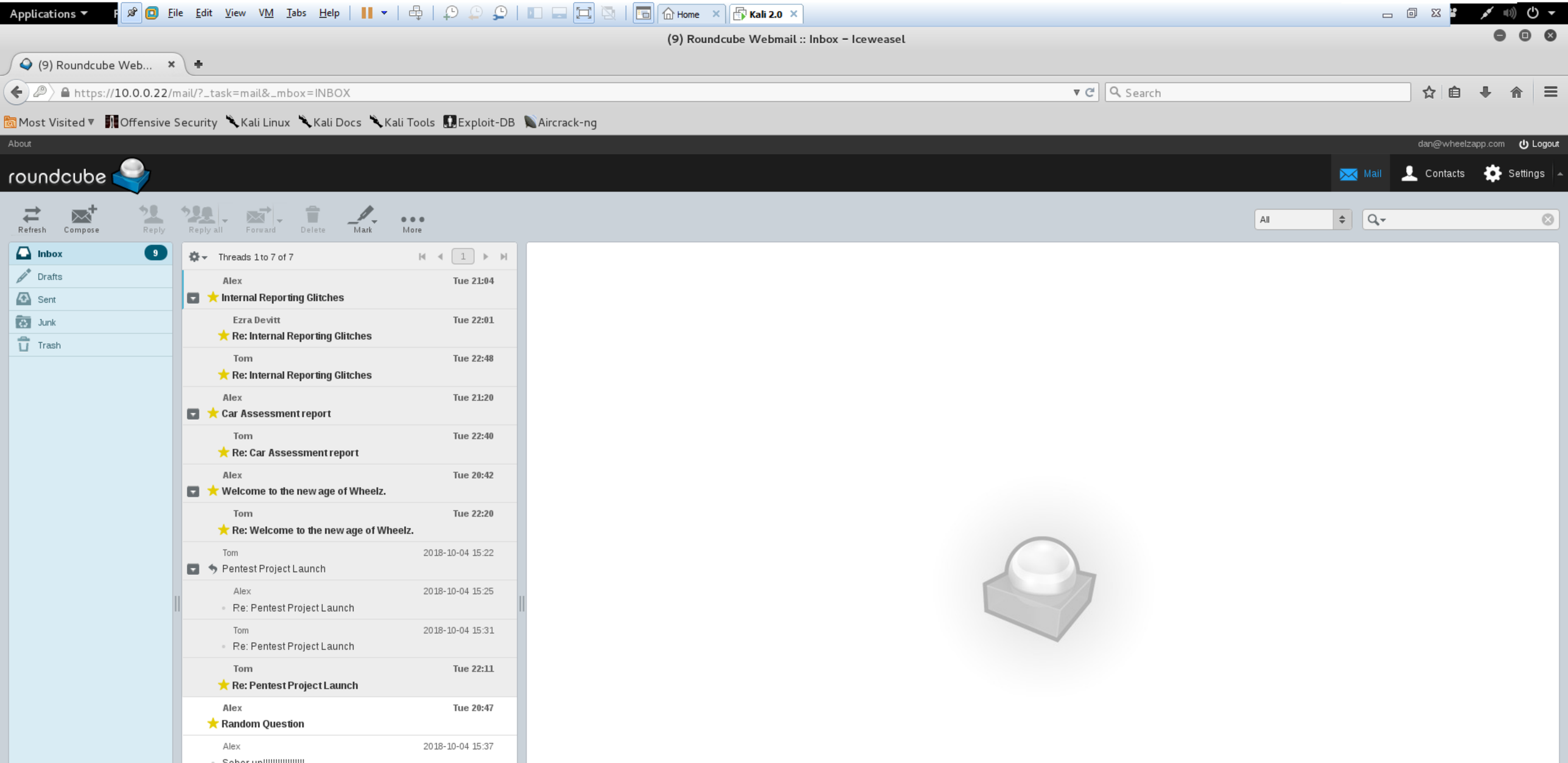
```
/envs/nationals-cptc team-1/kali06 @rocketchat # mongo 10.0.0.20
MongoDB shell version v3.6.3
connecting to: mongodb://10.0.0.20:27017/test
MongoDB server version: 3.6.3
Server has startup warnings:
2018-11-03T13:02:16.790+0000 I STORAGE  [initandlisten]
2018-11-03T13:02:16.790+0000 I STORAGE  [initandlisten] ** WARNING: Using the XFS filesystem is strongly recommended w
ith the WiredTiger storage engine
2018-11-03T13:02:16.790+0000 I STORAGE  [initandlisten] **          See http://dochub.mongodb.org/core/prodnotes-files
ystem
2018-11-03T13:02:18.645+0000 I CONTROL  [initandlisten]
2018-11-03T13:02:18.645+0000 I CONTROL  [initandlisten] ** WARNING: Access control is not enabled for the database.
2018-11-03T13:02:18.645+0000 I CONTROL  [initandlisten] **          Read and write access to data and configuration is
 unrestricted.
2018-11-03T13:02:18.645+0000 I CONTROL  [initandlisten]
> show dbs
admin       0.000GB
config      0.000GB
local       0.000GB
rocketchat  0.004GB
> use rocketchat
switched to db rocketchat
>
```

Stories

Database Access



Stories


Applications
File Edit View VM Tabs Help
Home
Kali 2.0
(9) Roundcube Webmail :: Inbox – Iceweasel
(9) Roundcube Web...
https://10.0.0.22/mail/?_task=mail&_mbox=INBOX
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
About
dan@wheelzapp.com
Logout
roundcube
Mail
Contacts
Settings
Refresh
Compose
Reply
Reply all
Forward
Delete
Mark
More
All
Inbox 9
Drafts
Sent
Junk
Trash
Threads 1 to 7 of 7
1
Alex Tue 21:04
Internal Reporting Glitches
Ezra Devitt Tue 22:01
Re: Internal Reporting Glitches
Tom Tue 22:48
Re: Internal Reporting Glitches
Alex Tue 21:20
Car Assessment report
Tom Tue 22:40
Re: Car Assessment report
Alex Tue 20:42
Welcome to the new age of Wheelz.
Tom Tue 22:20
Re: Welcome to the new age of Wheelz.
Tom 2018-10-04 15:22
Pentest Project Launch
Alex 2018-10-04 15:25
Re: Pentest Project Launch
Tom 2018-10-04 15:31
Re: Pentest Project Launch
Tom Tue 22:11
Re: Pentest Project Launch
Alex Tue 20:47
Random Question
Alex 2018-10-04 15:37

Chat

Hurr CPTC COLLEGIATE PENTESTING COMPETITION

Passwords & Politics

pentest

November 2, 2018

jerrold.reddick 3:49 PM
Has joined the channel.

Hey guys, I think my credentials have been compromised 😓

jerrold.reddick:4arthurbrandy

let me know what to do

joesph.tabron 4:49 PM
Has joined the channel.

https://lgtm.com/blog/apple_xnu_icmp_error_CVE-2018-4407

lgtm.com
Kernel RCE caused by buffer overflow in Apple's ICMP packet-handling code (CVE-2018-4407)
The networking implementation in iOS and macOS contained a heap buffer overflow, which could be triggered by sending a malicious pa

Thats not good **@jerrold.reddick** !

admin Owner 3:21 PM
this is the ongoing pentest chat

alex.herger 5:05 PM
meh, this pentest is a bad idea

dan 5:20 PM
@alex.herger that attitude really dosn't help, **@tom** sees the importance of this

tom Admin 5:23 PM
@alex.herger this test is really important to us, there is a lot going on right now behind the scenes so we will need everyones full compliance!

Role Playing and In-Character Interaction

Real-World Interactions with Students

- **Advisory board members interact with students in character**
  - Give students injects throughout the day
  - In-character walkthroughs and check-ins
  - Students prepare reports and give presentations to advisory board members
- **Real-time reliance on email during the event to mimic corporate communication**
- **Exposure to corporate politics**

COTHAM
ELECTIONS

Competition Data

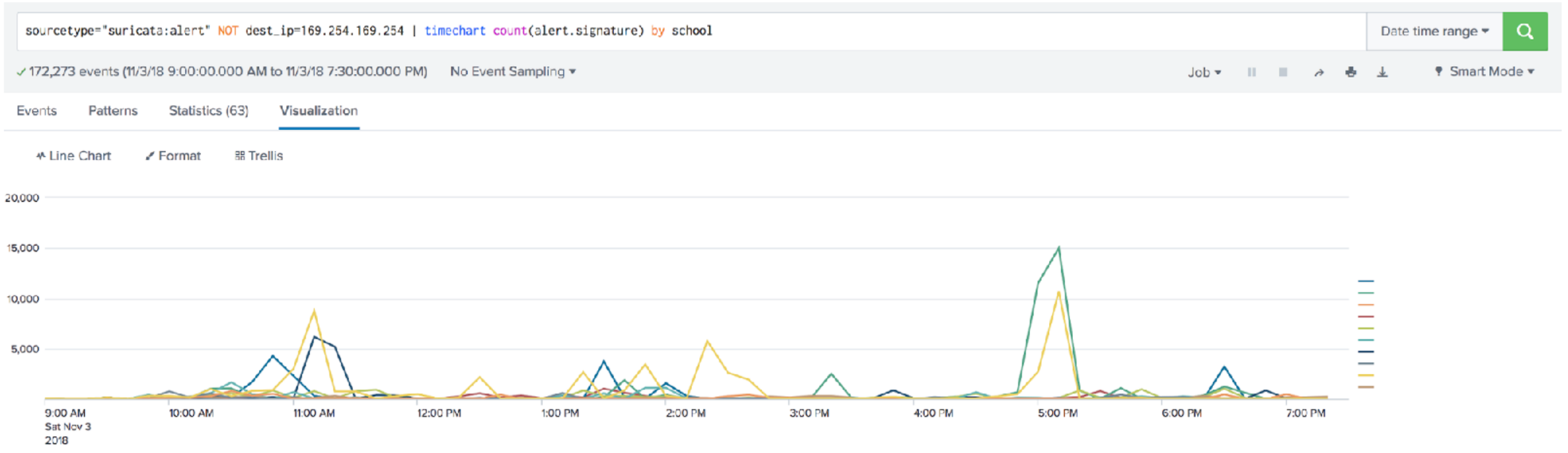
Competition Data

ls	3127	13.435593
clear	866	3.720890
cd ..	693	2.977572
exit	469	2.015124
ls -la	356	1.529604
ls -al	160	0.687462
ls -l	148	0.635903
cd	115	0.494114
ls -a	86	0.369511
ifconfig	80	0.343731

Competition Monitoring

- Extensive monitoring for competition integrity and research
- Goal is to provide insight into both sides of a security assessment: attacker and target
- Sample tools:
  - Suricata IDS on all hosts
  - Splunk Universal Forwarders
  - OS Query
  - Sysmon

Viewing is open to the public! We try to make it entertaining to watch.



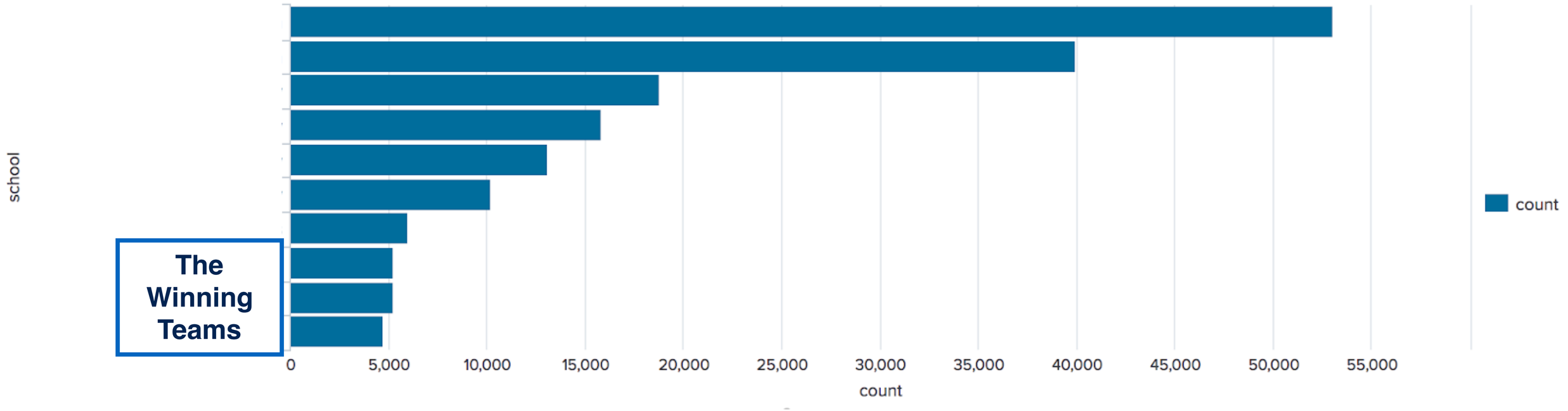
```
index=ids sourcetype="suricata:alert" NOT dest_ip="169.254.169.254" | stats count by school | sort - count
```

Date time range

✓ 172,273 events (11/3/18 9:00:00.000 AM to 11/3/18 7:30:00.000 PM) No Event Sampling Job Fast Mode

Events Patterns Statistics (10) **Visualization**

Bar Chart Format Trellis



The Winning Teams

CPTC Supported Research Initiatives

- Publicly available dataset: http://mirrors.rit.edu/cptc/
- Ongoing research effort: Understand the attacker mindset
- Codify attacker behavior
- Identify the team's approach (tactics and techniques) and map them to the MITRE ATT&CK framework

Success Stories

Hunt CPTC
COLLEGIATE PENTESTING COMPETITION

The industry needs people: people with technical and business skills

Successes from previous competitors

- Students have landed jobs through CPTC
- Zero-day discovery in competition environment by Stanford University Team (Disclosed to vendor, pending CVE, https://fsi.stanford.edu/cyber/news/stanford-applied-cybersecurity-student-team-places-first-cptc-nationals)

Get Involved!

CPTC
COLLEGIATE PENTESTING COMPETITION

Be an influence in training the next wave of cyber security professionals!

Help coach a team/start a team

Volunteer/Advisory Board

Audience Participation: Feedback on what we can do to improve

See you soon!

nationalcptc.org // @NationalCPTC

Dan Borges & Tom Kopchak
@1njection, @tomkopchak

directors@nationalcptc.org, dan@nationalcptc.org, tom@nationalcptc.org

Want to learn more? Visit us at Ethics Village @ 4:00 PM on Saturday!

The End