Teaching Consulting, Pentesting and Ethics:

Lessons Learned from Running a National Penetration Testing Competition

Presenters and Panelists:
Dan Borges, Tom Kopchak, Lucas Morris, Jason Ross
@1njection, @tomkopchak, @lucasjmorris, @rossja

@NationalCPTC / nationalcptc.org

Agenda

- What is the National Collegiate Penetration Testing Competition?
- What is it about us that makes us so unique?
- Ethics & CPTC
- Scenarios & Panel Discussion

Who Are We?

CPTC
COLLEGIATE PENTESTING COMPETITION

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

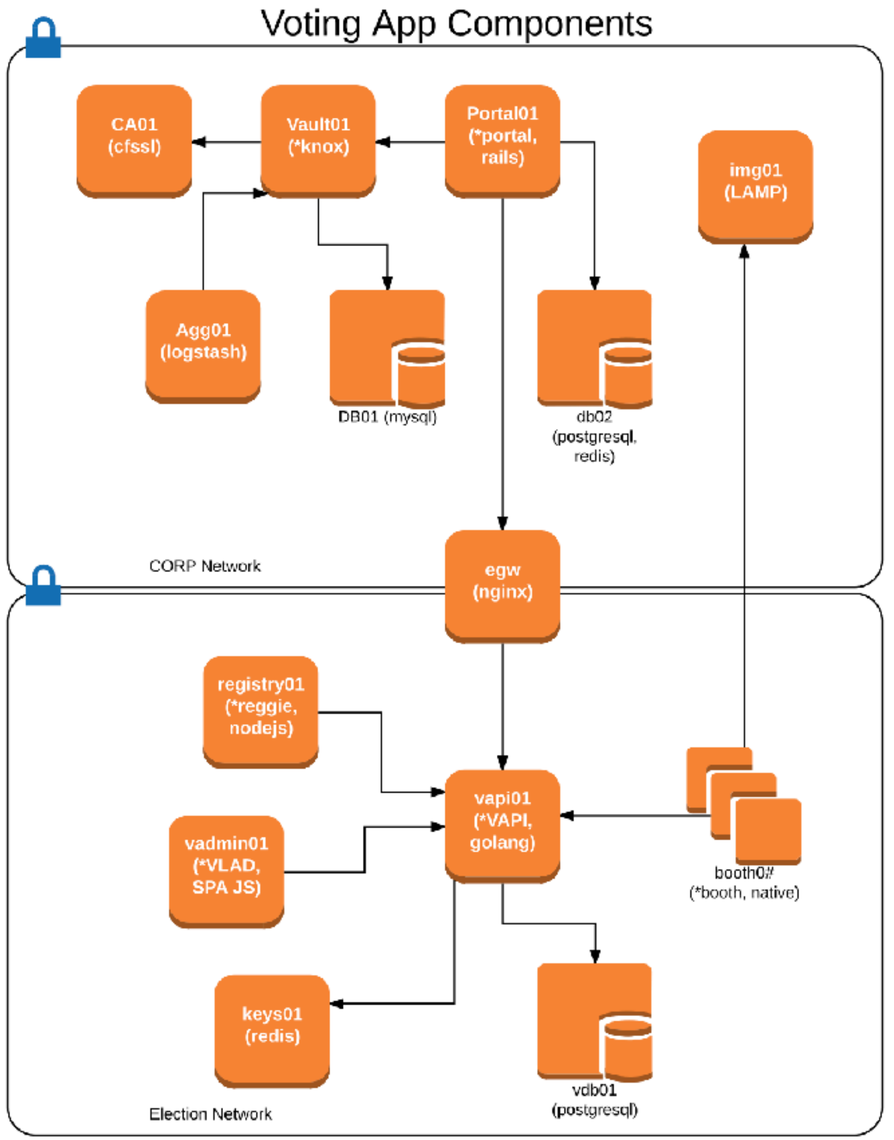
A Competition? Or an Engagement?

Instead of competing for flags, hosts, or hills, students are expected to:

- Act as consultants
- Use business and communication skills
- Test a company's network for technical issues
- Maintain professionalism throughout
- Communicate issues through deliverables

What's the Environment Like?

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



CPTC
COLLEGIATE PENTESTING COMPETITION

Ethics and CPTC

- Teaching is our emphasis
- Teams have the opportunity to be dangerous
- Limits (and scope) are free to discover
- Better to learn now and not at an actual customer

What We've Learned

- Technically-minded college students haven't had the opportunity to interact with clients and executives
- Scope of work = suggestion? (nope)
- In-character interaction is an adjustment
- Hackers have no boundaries?
- There's a huge difference between being a student and a consultant
- Official rules allow broad latitude for competition organizers to encourage ethical behavior

Real-World Interactions with Students

- **Volunteers interact with students in-character:**
  - Students are given tasks throughout the competition
  - Walkthroughs and check-ins with engineers and executives
  - 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**

Ethical Challenges

We present them.

We cause them.

They happen.

Importance of Ethics

Rule updates:

Violations of the rules can be deemed unprofessional conduct if determined to be intentional or malicious by White Team officials. Attempts to circumvent or otherwise violate the spirit of the CPTC rules may be deemed unprofessional conduct at the discretion of the White Team officials or Competition Director.

Panel Discussions

Hurricane Labs

Questions

- How did the team mess up?
- How have we seen this in the real world?
- What are we trying to teach?
- Audience experiences?

Scenario #1

Publicly Available Helpdesk Slack in OSINT

One Team Left False Information In “Client” System

Questions

- How did the team mess up?
- How have we seen this in the real world?
- What are we trying to teach?
- Audience experiences?

Scenario #2

Team creating LinkedIn account - impersonating target

Questions

- How did the team mess up?
- How have we seen this in the real world?
- What are we trying to teach?
- Audience experiences?

Scenario #3

“The Mexican APT”

Questions

- How did the team mess up?
- How have we seen this in the real world?
- What are we trying to teach?
- Audience experiences?

Scenario #4

Dirtycow

Questions

- How did the team mess up?
- How have we seen this in the real world?
- What are we trying to teach?
- Audience experiences?

Scenario #5

Scanning Public Infrastructure

Questions

- How did the team mess up?
- How have we seen this in the real world?
- What are we trying to teach?
- Audience experiences?

Scenario #6

Malware Triage

Questions

- How did the team hand the situation?
- How have we seen this in the real world?
- What are we trying to teach?
- Audience experiences?

Scenario #7

The Coach Environment

Questions

- How do we keep the competition fair?
- What risks do we face?
- What are we trying to teach?
- Audience experiences?

Scenario #8

Professionalism

Questions

- How have teams handled professionalism in the past?
- What are we trying to teach?
- Audience experiences?

Scenario #9

Scope - and scope expansion

Questions

- What scenarios merit a scope expansion?
- What are we trying to teach?
- Audience experiences?

Scenario #10

Client asks you to leave something out of the report

Questions

- How have we seen this in the real world?
- What are we trying to teach?
- Audience experiences?

Scenario #11

We build relationships over the year, how do we avoid bias and conflict of interest in the competition?

Questions

- Do volunteers from past competitions have a bias for their school / team?
- How have we seen this in the real world?
- What are we trying to teach?
- Audience experiences?

Real World Lessons

- Human element
  - Impromptu interviews, discussion
- Communication with clients and management
- Managing stressful situations
- Public speaking
- How to handle disagreements
- Attitude
- Never make your client look bad - remember who you’re working for
- It’s not a competition, except it is

Get Involved!

CPTC
COLLEGIATE PENTESTING COMPETITION

Be an (ethical) 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, Lucas Morris, Jason Ross
@1njection, @tomkopchak, @lucasjmorris, @rossja

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

The End