A GUIDE TO CYBERFORCE COMPETITION™ RED TEAM RECRUITMENT AND STRUCTURE

Argonne NATIONAL LABORATORY

IMPROVING THE EFFICIENCY OF A CYBER COMPETITION THROUGH DATA ANALYSIS

U.S. DEPARTMENT OF ENERGY'S CYBERFORCE COMPETITION™

DEFENDING U.S. ENERGY INFRASTRUCTURE

AMANDA JOYCE
CyberForce Competition™ Director
Group Lead – Strategic Cyber Analysis and Research
Argonne National Laboratory
amanda@anl.gov

STEVEN DAY
Cyber Security Analyst
Strategic Cyber Analysis and Research
Argonne National Laboratory
days@anl.gov

UCHICAGO ARGONNE LLC U.S. DEPARTMENT OF ENERGY Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.

Huntsville, Alabama

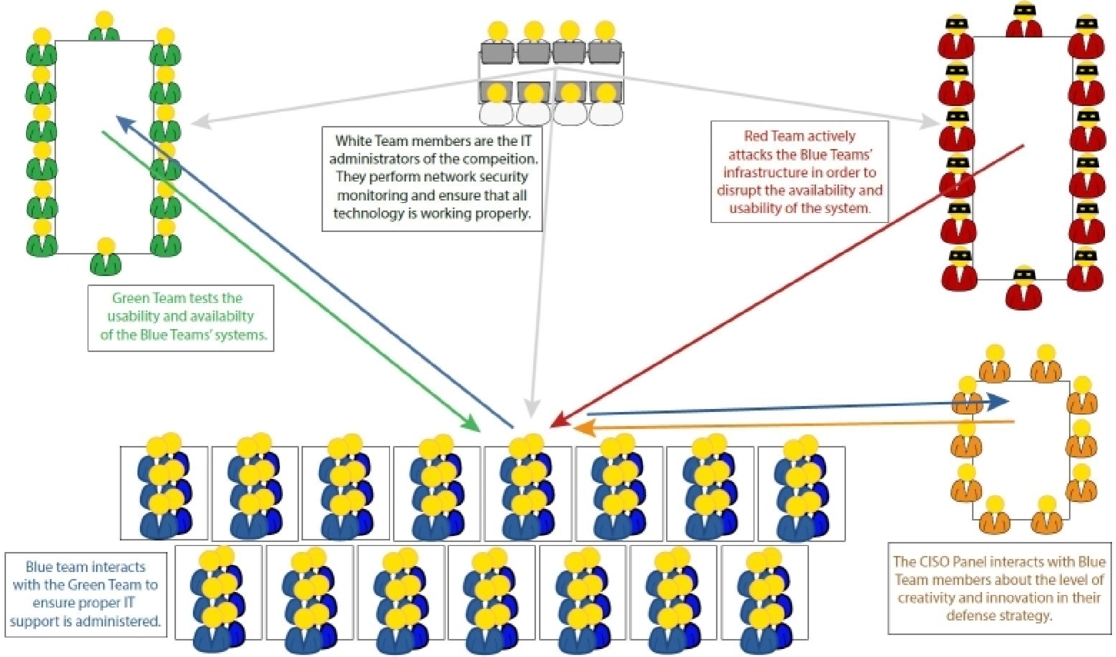
OVERVIEW

- The CyberForce Competition™ is the US Department of Energy’s sponsored annual collegiate cyber defense competition
- It is a collaboration of the Department’s expertise across the National Laboratories
- The day-long scenario-based competition places student teams in competition with each other to defend simulated cyber-physical infrastructure against professional red-team attackers with realistic anomalies and constraints.

GOALS

- Provide a workforce development platform not only for students, but also for industry and government professionals
- Increase awareness into the critical infrastructure and cyber security nexus
- Increase government/industry engagement
- Provide recruiting opportunities for top tier cyber talent

COMPETITION STRUCTURE



White Team members are the IT administrators of the compeition. They perform network security monitoring and ensure that all technology is working properly.

Red Team actively attacks the Blue Teams' infrastructure in order to disrupt the availability and usability of the system.

Green Team tests the usability and availabilty of the Blue Teams' systems.

Blue team interacts with the Green Team to ensure proper IT support is administered.

The CISO Panel interacts with Blue Team members about the level of creativity and innovation in their defense strategy.

HISTORY OF RED TEAM

Event Date	No. of Participating Labs	No. of Blue Teams	No. of Red Team Volunteers
April 2016	1	8	13
April 2017	1	15	15
April 2018	3	25	85
December 2018	7	64	170
November 2019	9	~100[*]	≥200[+]

[*] denotes the anticipated team count

[+] denotes the goal of red team based on anticipated blue teams

RED TEAM RECRUITMENT

- For 2016 and 2017, recruitment was local and had very little strategic direction.
- For April 2018 and December, with additional laboratory participation, the competition committee asked volunteers to provide information in the following areas:
  - Full time occupation
  - Years of experience
  - Cybersecurity-related Certifications
  - Previous participation in cyber defense competitions
  - Comfort level with specific cyber-attack and defense tools and techniques
  - Comfort level assessing various operating systems

RECONNAISSANCE AND ATTACK PHASES

2016 – APRIL 2018

- No pre-competition reconnaissance
- Only allotted window on Friday prior to competition to scan
- Large delay seen of Red Team “action”
- Communication channel prior to competition (April 2018)

DECEMBER 2018

- No pre-competition reconnaissance for non-Red Team Leads
- Allotted 8-hour window on Friday prior to competition to scan
- Communication channel prior to competition
- Provided inherent vulnerabilities on Friday/Saturday along with associated scripts.

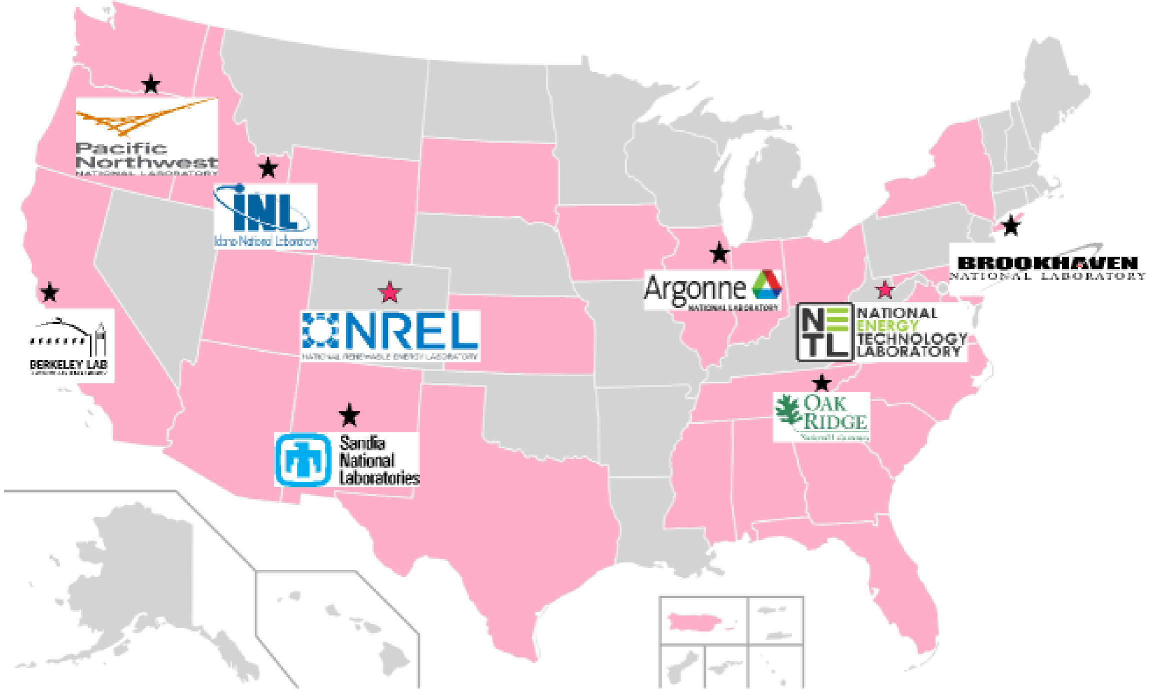
RAW RED TEAM SCORES FOR DECEMBER 2018

Laboratory	No. of Teams Scored	Low Red Score	High Red Score	Mean Red Score	Delta
All labs	62	0	1500	1025.4	
Argonne	16	0	1500	1071.88	+46.48
Brookhaven	5	450	1075	730	-295.4
Idaho	6	525	1425	845.83	-179.57
Lawrence Berkeley	4	1100	1450	1318.75	+293.35
Oak Ridge	10	375	1425	1092.5	+67.1
Pacific Northwest	13	300	1475	1067.31	+41.91
Sandia	8	500	1225	953.13	-72.27

LESSONS LEARNED

- Better use of Red Team skills and time prior to the competition
- Increase communication channels
- Red Team scoring still needs to be tweaked
- More clear guidance on what is or is not allowed during the competition
- Increase participation of competition alumni who have experience with the competition

NEXT EVENT: NOVEMBER 15-16, 2019


Pacific Northwest NATIONAL LABORATORY
INL Idaho National Laboratory
BERKELEY LAB
NREL NATIONAL RENEWABLE ENERGY LABORATORY
Sandia National Laboratories
Argonne NATIONAL LABORATORY
NATIONAL ENERGY TECHNOLOGY LABORATORY
OAK RIDGE National Laboratory
BROOKHAVEN NATIONAL LABORATORY

QUESTIONS?

Amanda Joyce
CyberForce Competition™ Director
Group Lead – Strategic Cyber Analysis and Research
Argonne National Laboratory
amanda@anl.gov

Steven Day
Cyber Security Analyst
Strategic Cyber Analysis and Research
Argonne National Laboratory
days@anl.gov