Key CyberForce Competition Rules

- Each team must have 4-6 students.
- One faculty mentor must be present at the national laboratory on the day of the competition. In the case that a faculty member cannot attend, an appropriate substitute mentor will be identified on a case-by-case basis.
- Faculty mentors may not provide any assistance to their teams on the day of the competition. Any team receiving help from a coach or mentor will be warned and penalized points on the first offense and disqualified after a subsequent offense.
- Each national laboratory has their own rules and procedures concerning wireless and site access. You are responsible for understanding and following these rules throughout the competition.
- As a Blue Team member, you are not allowed to perform any offensive measures towards other Blue Teams, the competition network (especially the Azure resources), or your host laboratory. Doing so will disqualify your team from the competition.
- Team documentation (White) is will be uploaded to the sCOARboard no later than 11:59 pm local time on November 27, 2018. Early submission is encouraged, and we will distribute more specific instructions closer to the competition. Any documentation submitted after this deadline will be reduced by 15% of its scored value per day. If no documentation is submitted by competition start, you will receive zero points. Please refer to Scoring Breakdown for more information. Please ensure your documentation is clearly labeled with your team number (i.e., Team 1 – White Team Strategic Security Documentation).
- Operational rules and team-related rules are provided in specific sections throughout this document so please read this entire document thoroughly.
- Each Blue team will have access to their Azure environment beginning on November 12, 2018. The White team operates the administrative accounts on Azure. These White team administrative accounts will not be used maliciously and are only there to ensure proper scoring and rules.
- WARNING: Changing an IP that is provided by Microsoft Azure infrastructure may lock you out of your workstations. Do NOT change the IP address of provided VMs.
- These rules ensure that each team participates under the same circumstances and thus has an equal opportunity to succeed. Depending on the offense, failure to comply with the rules of the competition may result in penalty points or disqualification. Egregious offenses may result in disqualification from the competition. If you see a breach of competition rules, please notify competition staff immediately. You may email CyberForceCompetition@anl.gov if you prefer not to be seen communicating with staff. All competition staff will maintain your confidentiality.

Updates to Rules

Updates to rules will be found on the CyberForce Competition website[1] under the Guidelines Tab. It is each team's responsibility to be aware of any updates to the rules.

[1] http://cyberforcecompetition.com/

The Do's

- Reference the Scoring and Overview documents for additional details beyond what is covered here.
- Make use of only freely available software, or software provided as part of your Azure instances.
- Configure the DNS service for name resolution by all machines on your subnet
- Configure the Active Directory/LDAP service for user authentication on all machines on your subnet
- Create a help desk service that supports mail via SMTP and POP3.
- Configure the NTP service for time synchronization of all machines on your subnet
- Protect and maintain the continuous operations of the cyber-physical asset your team has been entrusted with to ensure your company and its consumers are satisfied.
- Input the scored services into the sCOARboard prior to competition day.
- Keep your services online, on the standard port, for the duration of the competition.
- Ensure all users specified in the provided Required Users list are created and given appropriate permissions.
- Submit and update Green team usernames and passwords to the sCOARboard.
- Include the user information provided in this packet as well any additional users in the Green team user manual, which is hosted the sCOARboard.
- Create and deploy innovative defense strategies within the constraints of other rules.
- Submit White team Strategic Security Documentation by November 27, 2018 by 11:59pm local time.
- Bring all laptops, adapters, extra cables, extra mice/keyboards, monitors, etc. that your team will need to compete. Laptops should have an Ethernet port or come with required adapter to connect to Ethernet or be wireless enabled.

The Do nots

- DO NOT create more than 8 total virtual machines (VMs) in your environment (including the VMs provided). White team will delete the last machine(s) created if more than 8 machines are present.
- DO NOT specifically block or ban IP addresses or ranges. Automated systems that block connections after N failed login attempts (e.g., fail2ban) are NOT allowed.
- DO NOT upgrade the OS (apt upgrade is OK, apt dist-upgrade is NOT OKAY)
- DO NOT physically tamper with any other team's physical devices.
- DO NOT perform offensive actions toward any other teams, the competition network, your host laboratory, or Azure.
- DO NOT modify the logic for the ICS components in RexDraw
- DO NOT attempt to hack or compromise the sCOARboard. This will result in severe penalty and likely disqualification.
- DO NOT use paid or trial Azure software

Competition Environment

Network Topology

You will inherit a /25 Azure subnet and a competition accessible /25 VPN subnet with a competition exposed ICS (which must stay accessible to red and green users).

Any changes to your Blue team infrastructure must be clearly documented in White team Strategic Security Documentation and/or in the user manual provided for the Green team, whenever applicable

Blue Team Login Instructions

VPN Install

The competition uses OpenVPN for access into the Azure environment. You will be provided an OVPN configuration file to connect to your network. Clients for each operating system can be found below:

- Windows - https://openvpn.net/index.php/download/community-downloads.html
    - Place the OVPN file into “C:\Program Files\Openvpn\config”.
- MacOS - https://www.tunnelblick.net.
    - Double click the OVPN file to import it to Tunnelblick.
- Linux - sudo apt (or yum) install openvpn.
    - Run ‘openvpn --config YOUR_OVPN_FILE.ovpn’

Azure Credentials

You have received an email from CyberForceCompetition@anl.gov with your Azure credentials. If you did not, please contact CyberForceCompetition@anl.gov.

Required Services and their Port Numbers

All Blue Teams are required to establish and maintain the following services throughout the competition.

- HTTP – 80/TCP
- SSH – 22/TCP
- FTP – 21/TCP
- LDAP – 389/TCP
- DNS – 53/UDP
- NTP – 123/UDP
- SMTP – 25/TCP
- POP3 – 110/TCP
- Modbus – 502/TCP
- DNP3 – 20000/TCP

Industrial Control System Devices

- If there is a suspected network outage or your ICS device is not working properly PRIOR TO the competition, please contact technical support as outlined later in this document.
- If there is a suspected network outage or your industrial control system is not working properly DURING the competition, contact the White team. This may incur the reimaging penalty.
- Altering the logic of these devices may result in damage to the physical model during the competition. This may incur the reimaging penalty.
- Replacing physical components often requires long-lead times in the real world and for this competition—any physical damage to the ICS components may not be repairable during the competition. This may incur the reimaging penalty.

Required Users

The following users are required to have administrative privileges to the ICS and must be entered into your Active Directory/LDAP service.

NAME	USERNAME
Alec Dozac	a.dozac
Amanda Jeel	a.jeel
Andrea Thompson	a.thompson
Ben Cakely	b.cakely
Brad Wells	b.wells
Chuck Wheeler	c.wheeler
Crystal Licht	c.licht
Daniel Brady	d.brady
Frank Castle	f.castle
Holly Peterson	h.peterson
James Hoyt	j.hoyt
Jane Wright	j.wright
Jennifer Bowler	j.bowler
Josh Bile	j.bile
Karen Holmes	k.holmes
Lisa Delrose	l.delrose
Michael Haynes	m.haynes
Nate Kevans	n.kevans
Patricia Emerson	p.emerson
Paulina Luther	p.luther2
Piotre Luther	p.luther
Ronald Variable	r.variable
Sandra Wilhelm	s.wilhelm
Scott Harlem	s.harlem
Shannon Bott	s.bott
Simon Smith	s.smith
Steven Jobs	s.jobs
Susan Taylor	s.taylor

Ted Fritz t.fritz

sCOARboard

Use the sCOARboard to enter your services and other information required by the White Team.

- Your team will receive an invitation via email the week of November 26 to register each team member using your school's .edu email address. A follow-up email will be sent with the registration link and how to enter your services the week prior to the competition.
- These values should be entered by Friday, November 30, 2018 to ensure that your scoring is accurate during the competition.

Restoring Systems to Initial State

If a Blue team damages a virtual machines beyond the point of recovery, the White Team can provide a fresh, default image of the system. However, your team will incur a scoring penalty of 100 points per restoration. To prevent this, your team is encouraged to create backups or snapshots of each system as it is set up and configured, especially before and after any major infrastructure changes.

Provided Hardware and Equipment

Teams will gain physical access to their competition space and their Raspberry Pi on Friday, November 30, 2018. The following will be provided:

- Industrial Control System
- Power Strip(s) with a minimum of 10 outlets
- One 8-port switch
- Internet access to allow VPN access to competition space
- One monitor, keyboard, and mouse

The National Laboratories **will not** provide any display, network, power, or other adapters for competition use.

Required Documentation

White Team Strategic Security Documentation

Blue teams must develop an overview document for the White Team detailing their strategy for assessing the threats to their environment, hardening and monitoring their network, and responding to incidents. Details on requirements can be found in the scoring guidelines.

Green Team User Guide

Blue teams must develop a User Guide for their Green Team members. This manual must be included on the sCOARboard. A template for this guide will be distributed via email prior to the competition. The guide should be written for new users who have no experience with your environment. Please note that each Green team member will only have 20-25 minutes to assess your system using the manual you provide. Details on requirements can be found in the Scoring guidelines.

Competition Structure

Setup Phase

Blue teams will be given access to their Azure environment in advance of the competition. During this phase, no offensive or reconnaissance activities may take place by any individual. Blue teams should use this time to assess, build, and test their system prior to the competition.

Information Gathering Phase

Red team members will be scanning networks and gathering background information about Blue team systems on the setup day before the competition (Friday). This will be limited to passive reconnaissance only. Nothing invasive or destructive may occur during this period. If Blue team members notice unauthorized access attempts or other invasive actions to their system, they should notify a White team member immediately.

Attack Phase

On the day of the competition itself (Saturday), the Red team will attempt to gain access to Blue Team services while the Green team attempts to use them. The White team will be monitoring Blue Team service uptime. Blue teams must monitor their systems, submit incident reports to the white team (as described in the Scoring guidelines), choose anomalies they wish to complete for additional points, and support their Green team users. The red team will perform attacks that leverage different aspect of security and are not limited to breaching the perimeter.

During this phase, the Blue team may not receive help from anyone not registered as a competitor on their own team or the White team. Receiving help from others, including mentors, external parties, etc., will result in a penalty. Any teams that explicitly block red team IP addresses will incur a penalty.


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