2018 CYBER DEFENSE COMPETITION
DOE NATIONAL LABORATORIES

U.S. DEPARTMENT OF ENERGY

Blue Team Rules and Scoring

3RD ANNUAL DEPARTMENT OF ENERGY CYBER DEFENSE COMPETITION

SATURDAY, APRIL 7, 2018

Argonne NATIONAL LABORATORY
OAK RIDGE National Laboratory
Pacific Northwest NATIONAL LABORATORY

Contents

CDC Scenario

Your team has just been hired as the network and security administrators of cyber systems that work in conjunction with the production and delivery of [redacted] for the [redacted] NGDC is the nation's only start-to-finish [redacted] production, transmission, and distribution company. NGDC handles all aspects of this highly valued product from extracting the raw gas resources, processing, transportation, and distribution to residential, commercial, industrial, and electric power consumers. NGDC recently has been hit with multiple "minor" cyber attacks against their pipeline transmission infrastructure and have not successfully been able to review, update, or patch their systems with appropriate mitigation solutions without having to stop all operations. [redacted] NGDC has hired you and your team as subject matter experts help secure this network and has requested that you secure their user supply and marketing portal (distribution) network. These two networks require high availability and should not be taken offline for any reason unless dictated by the Chief Executive Officer – [redacted] Unfortunately, there has not been a solid security team at NGDC in about three years and the network architecture drawings and operational technology (OT) topology are largely out of date. Additionally, NGDC is requesting that a new File-Sharing client and IT communications be set up to allow customers and NGDC to be able to interact without utilizing credentials. [redacted] There has been little or no funding provided for this task until you as a team can demonstrate your capabilities to resolve their issues. This means that you and your team must secure these complex IT and OT systems utilizing free or open-source materials and best practices while maintaining full functionality for the company operators and the end users.

Cyber Defense Competition Rules

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 CyberDefense-Competition@anl.gov if you prefer not to be seen communicating with staff. All competition staff will maintain your confidentiality.

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 mentor will be discussed 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, or your host laboratory. Doing so will disqualify your team from the competition.
- Teams are required to have the services outlined below active at all times, unless noted:
    - HTTP
    - SSH
    - FTP
    - LDAP
    - DNS
    - NTP
    - Help Desk/POP3
    - Modbus
- Team documentation (White and Green) is due to CyberDefense-Competition@anl.gov by no later than March 30, 2018. Early submission is encouraged. Any documentation submitted after this deadline will lose 15 points per day. If not documentation is submitted by competition, you will receive zero points. Please refer to Scoring Breakdown for more information.

- Operational rules and team-related rules are provided in specific sections throughout this document so please read this entire document thoroughly.
- WARNING: Changing an IP that is provided by Microsoft Azure infrastructure may lock you out of your workstations. If you need to change IP addresses, you must do this through the Azure interface.

Updates to Rules

- Any update to rules can be found on the Cyber Defense website under the Guidelines Tab. It is each team's responsibility to be aware of updates to the rules.

The Don'ts

- Do not create more than 10 total virtual machines (VMs) in your environment including the VMs provided. White team will delete the last machine(s) created if more than 10 machines are present.
- Do not change any standard port numbers for scored services.
- Do not delete or make any major version changes or updates to the OSs that are provided.
    - Provided infrastructure must stay at:
        - **Web - Centos 7**
        - **HMI – Ubuntu 16.04**
        - **File/Database - Ubuntu 16.04**
- Do not utilize any software that requires a paid license other than Microsoft Windows/Windows Server. All other software must be open source and free. Trial versions are acceptable.
- 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 modify the sCOARboard VM (scoreboard engine being utilized for competition) or any of the provided VPN machines.

The Do's

- Do create a DNS service that is utilized by all machines on your subnet
- Do create LDAP that is utilized for user authentication on all machines on your subnet
- Do create a help desk service with both SMTP and POP3.
- Do create an NTP service that synchronizes clocks on all machines on your subnet
- Do secure existing services on provided VMs.
- Do ensure that all users specified in the provided Required Users list are created and given appropriate permissions for user by the Green team.

- Do create innovative defense strategies within the constraints of other rules.
- Do keep your services online for the duration of the competition.
- Do clearly document any changes to user passwords.
- Do input the scored services into the sCOARboard prior to competition day.
- Do submit your White team and Green team documentation into the sCOARboard by March 30, 2018 by 11:59pm CT.
- Do include the user information provided in this packet as well any additional users in the Green team documentation.

Competition Team Descriptions

Red Team - Volunteers

The Red team's goal is to compromise the Blue teams' networks. However, neither Red team nor other Blue team members are allowed to physically touch your equipment during the competition. If this occurs, please notify competition staff immediately. This is grounds for disqualification. Note that red team members have plenty of tools to gain access to blue team systems within these guidelines!

Green Team - Volunteers

The Green team is meant to simulate a real-life user of the system. This team is comprised of volunteers that have a wide range of knowledge and skill sets that mirror a typical work environment. When preparing documentation, please keep in mind that Green team volunteers will not know what any of your systems look like prior to the day of the competition. Normal workplace environments have a diverse set of users ranging from administrative assistants, to technical specialists, and everything in-between. The Green team will review and evaluate the Blue teams' work and submit points based on documentation, overall performance, and helpfulness of Blue team. The role of the Green team and the use cases supplied for the competition emulate day-to-day work and provide challenges that also manifest themselves in real life.

White Team - National Laboratory

The White team is the competition architecture team. These members are available for assistance by any team in the event of network failures, hardware issues, documentation issues, rules questions, or industrial control system failures. While this team is available, some requests will cost your team points (for example complete restoration of competition environment). This team will be wearing white CDC T-shirts.

Procedures and Responsibilities

Each Blue team is assigned a subnet of IPs for devices and services.

The items listed below will be provided to your team and will need to be secured. If a Blue team damages non-physical components (e.g., virtual machines) beyond the point of recovery, the White team (National Laboratory) can provide a fresh, default image of the system, but your Blue team will incur a scoring penalty of 50 points per re-install per box. To prevent this, you may wish to create backups or snapshots of the system along the way, especially before and after any major infrastructure changes. Blue teams may not perform any offensive actions aimed at other participants' networks, the Azure network, or the Laboratory network - doing so will result in disqualification and immediate removal from the competition site.

Items Provided for Competition

Hardware

Each Blue team will have access to their Azure environment beginning the week of March 5. 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.

There is a 10 virtual machine limit in your Azure environment (this includes all provided VMs). The White team will delete any machine created over 10 without prior notification.

Each team will be provided a cyber-physical device at their competition site on Friday. Please be aware that altering the logic to these devices may result in damage to the physical model during the competition. Replacing physical components often results in 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. Please 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.

If there is a suspected network outage or your industrial control system is not working properly during the competition, contact the White team immediately.

Software

All software used in the competition must be either freely available or provided by the Azure instance. Any new virtual machines must use a free operating system or Microsoft Windows (provided in Azure).

Free trials of paid software within the trial period are allowed; however, the White team cannot provide support for these or for any software not initially provided by the White team.

Provided Support Prior to Competition

Remote Setup

Student setup will be available remotely 24/7 after March 5, 2018. White team support will be provided via the #DOE-CDC-2018 Slack channel during the following hours:

Monday – Friday
8am-6pm ET / 7am-5pm CT / 5am-3pm PT

Students will be provided a registration link that is valid for 48 hours to the #DOE-CDC-2018 Slack channel available in the Slack app. If you need a new registration link, please email CyberDefense-Competition@anl.gov. When registering in Slack, please be sure to include your school institution in your username (i.e., Iowa – Janet; UIC – Bob). Any questions posted after support hours will be logged and answered to the best ability on the next business day.

Blue teams are encouraged to seek help during the setup phase from either their mentors or the White team. Questions are welcomed at any time from Blue team members; in addition to regular support hours, specific times for Q&A's are outlined below. These Q&A's will occur via the Slack Channel.

- **Technical/Infrastructure Q&A** - March 12, 2018 at 12pm ET / 11am CT / 9am PT.
- **Green/White/Creativity Documentation Q&A** - March 22, 2018 at 2pm ET / 1pm CT / 11am PT.
- **Rules/Scoring Q&A** - March 29, 2018 at 2pm ET / 1pm CT / 11am PT.

Access to your Raspberry Pi (ICS HMI) will be removed on Thursday, April 5 beginning at 8:00am local time of the competition site. Blue teams will have access back to their Pi once onsite setup begins.

Onsite Setup

Teams will gain physical access to their competition space and their Raspberry Pi on Friday, April 6, 2018. Your assigned National Laboratory site will supply the industrial control system (ICS) device as well as all necessary hardware that supports it. The following will be provided:

- Industrial Control System
- 2 Power Strips
- 1 Unmanaged Switches
    - Internet access to allow VPN access to competition space

The National Laboratories **will not** provide any adapters for competition use. You are strongly encouraged to 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.

Provided Support during the Competition

The following support can be provided during the competition but will be limited in scope:

- Image refresh
- Connectivity issues
- Industrial Control System issues

If your team needs support during the competition, please be sure to find a staff member (in white t-shirts) to assist you. It is imperative that you ensure your competition environment is set up properly the day before the competition. There will be staff present to assist and troubleshoot errors before they count against you in competition.

Network throughout the Competition

Required Services and their Port Numbers

- HTTP – 80
- SSH – 22
- FTP – 21
- LDAP – 389
- DNS – 53
- NTP – 123
- Help Desk System/POP3 – 110/25
- Modbus – 502

Network Topology

Teams will be inheriting a /25 Azure subnet and a /25 VPN subnet with a required publicly exposed ICS. Teams are encouraged to think innovatively in their defensive strategies of their network. Any changes to your Blue team infrastructure must be clearly documented in White team documentation and/or Green team documentation.

Information Gathering Phase of the Competition

Red team members will be scanning networks and gathering background information about Blue team systems on the setup day before the competition. This will be limited to network scanning,

vulnerability scanning, etc. Nothing invasive should occur during this probing period. If any Blue team members notice unauthorized access attempts or other invasive actions to their system, they should notify a White team member immediately.

Attack Phase of the Competition

During the attack phase, the Red team will attempt to gain access to your services. This effort will begin at the announced start of the competition.

Since our small-world network will not emulate the diversity of the actual internet, blocking IP addresses will be considered a denial of service to potential users and employees and will therefore result in a deduction of points. Blue teams are not allowed to specifically block or ban IPs or IP ranges. Automated systems that block connections after *N* failed login attempts (e.g., fail2ban) are NOT allowed. Templates for incident reports will be provided.

The Blue team may not receive help from anyone other than his or her own team members or White team. Receiving help from others including mentors, external parties, etc. will result in a penalty.

Blue Team Login Instructions

VPN Install

We will be utilizing OpenVPN. 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'

You will be provided an OVPN configuration file to connect to your network.

Azure Credentials

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

sCOARboard

You will receive an invitation email asking you to register using your school's .edu email address. Please use the sCOARboard to enter your services and other requested information. We strongly recommend entering these values by Friday, April 6, 2018 to ensure that your scoring is not hindered during the competition. A follow-up email will be sent with the registration link and how to input your scores the week prior to the competition.

Scoring Breakdown

Overall Scoring Breakdown

Red Team	1500 points	30%
Uptime	1500 points	30%
White Team	1000 points	20%
Green Team	750 points	15%
Creativity	250 points	5%
Total	**5000 points**	**100%**

Red Team Scoring

Red team members will perform attacks on Blue team networks, topography and software. Red team points will be based on the how teams identify, protect, and respond to attacks as well as for sportsmanship demonstrated by the team during the competition. Red team score will be updated 2 times throughout the day: mid-point and end of day.

TASK:	TOTAL POINTS: 1500
Mid-day	500
End-of-day	1000

Uptime Scoring

Service Uptime is based on the required services and their uptime. Total number of points for uptime scoring is 1500. For services that fail to be up during the required competition hours, teams will lose points. Blue teams are responsible for entering their required services into the sCOARboard.

White Team Scoring

White team members will evaluate two Blue team tasks:

TASK:	TOTAL POINTS: 1000
Documentation	800
Intrusion Reports	200

Documentation must be submitted on or before March 30, 2018 at 11:59pm CT, prior to competition. Documentation submitted after the deadline will result in the loss of 15 points PER DAY. Additional information regarding the required documentation to be submitted to the White team is provided below. An example of Documentation that earned high scores from the White team was included in Rules and Scoring email.

Below are the key components that must be included in documentation submitted to the White team. Please note that Blue teams are playing out a scenario and, like the real world, presentation and professionalism will play a factor in final scores.

Key White Team Documentation Components	Point Distribution

- Details of the team's network layout
  o IP Addresses
  o Firewalls
  o Decisions on NATs
- Network diagram(s)
- Discussion of:
  o Operating systems
  o Software
  o Other items you have chosen to run
- Discussion of special measures you have taken to secure your network
  o Intrusion Detection Systems
  o Specific firewall rules
  o Mandatory access controls, etc.
- Creativity Statement explaining specific creativity elements that can be found within your environment and defensive mechanisms that are novel in nature or approach.
	- Supporting diagrams: 225pts
	- Detailed write up: 225pts
	- Professionalism: 50pts
	- Effectiveness of plan: 50pts
	- Creativity Statement: 250pts

Intrusion reports are required of every team every other hour beginning at 1pm ET / 12pm CT / 10am PT. These reports should be entered via the template provided in sCOARboard. Analysis should be provided with each intrusion report. Each report is worth 50 points.

Key Intrusion Report Components	Point Distribution

- Details provided within template
  ○ Completeness
  ○ Thoroughness
- Accuracy
  ○ Details about attacks and countermeasures
	- Detailed write up : 25pts
	- Accuracy: 25pts

Green Team Scoring

The Green team will review and evaluate the Blue teams' work and submit points based on documentation, overall performance, and helpfulness from Blue team. The Green team will assess their ability to conduct routine business tasks using the following two categories:

TASK:	TOTAL POINTS: 750
Documentation	250
Usability	500

Blue teams are required to develop a "How-to"/User Guide for their Green team members. This manual is required prior to the competition on March 30, 2018 and will receive a reduction of 15 points per day for tardiness. 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. Your manual should include how to:

1. Download Blue team user documentation from sCOARboard.
2. Log in to your competition WordPress site
3. View their Energy Production Dashboard
4. Purchase Energy Units
5. Access the ICS Human Machine Interface
6. Request support from the Help Desk (if needed)
7. Download any updates to the user documentation from sCOARboard.

While some of these steps may result in the customer (Green team) not having access, you should recognize that all Green team members will be using the same manual, so it is imperative that you clearly outline the anticipated result for each user.

Below are the key components the Green team will use to assess the user manual.

Key Green Team Documentation Components	Point Distribution
- Documentation clearly instructs the Green team users on how to use Blue team services. - Usability of Blue team services on day of competition, based primarily on documentation. - Balance between usability and security. - Clarity of user manual for users with little to no computer experience.	- Detail of instructions: 50pts - Clarity: 50pts - Professionalism: 50pts - Completeness: 50pts - Supporting documentation: 50pts

Creativity

In many companies, cyber security professionals are asked to update and advocate for additional opportunities and resources with executive leadership. To simulate this kind of real-world activity, the competition has enlisted a mock Chief Information Security Officers (CISOs) panel. For additional points, Blue Teams will have the opportunity to request time in front of the CISOs panel to advocate any unique defensive approaches they took during the competition. Their pitch to this panel will need to describe the approach, how it was implemented, result of implementation and lessons learned. The panel will decide how many points each team is awarded based on the creativity of their approach and pitch. This meeting will be up to 2-minutes and can be requested via the CISOs panel calendar - https://calendly.com/anlcyberdefense/ciso-panel/04-07-2018. It is highly encouraged to request your time as early as possible on Saturday as there is a 30-minute minimum scheduling notification requirement.

Teams are encouraged to think about which approach is their most creative and how are they going to pitch it in a 2-min window. Examples of unique approaches include but are not limited to how a Blue team: answered an anomaly, unique defense against an attack, how your defense approach changed based on an event, etc. This 2-minute pitch is worth up to 250 points and will be a comparative score against all participating Blue teams

Additional Scoring Breakdown

Anomalies

In the real world of information assurance, there is never a dull moment. Anomalies simulate the stream of requests that IT employees and cybersecurity analysts must be prepared to handle. During the competition, anomalies will be delivered to you via the sCOARboard. They will be worth varying point values based on level of difficulty. Blue teams will need to submit responses to anomalies before they expire in order to earn points.

Responding to anomalies is **optional**. Blue teams that do not submit a response will not be awarded any points for that anomaly and no points will be deducted. Anomalies will be worth up to 500 additional points and teams are strongly encouraged to respond to them.

Blue team members are responsible for ensuring that responses to anomalies are submitted on time with completed documentation in order to earn points.

Penalties

Penalties will be invoked in the event a Blue team does not abide by the competition rules and guidelines. Teams should be aware of the following penalty deductions:

- Reimaging = 50 points per reinstall
- Receiving help from anyone outside Blue team members and White team during competition = 250 points each instance. This includes mentor help.
- Offensive action towards other teams' networks or hardware and/or network = Disqualification

Required Users

All 30 of these users are required to have administrative privileges to the ICS and must be inputted into your LDAP/AD.

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