Blue Team: Procedures and Responsibilities

Students will form teams consisting of 3–6 students to address the challenge presented in the Scenario document. Students will set up and secure a system that must remain usable by the Green Team while being defended against attacks from the Red Team.

Each Blue Team will be assigned a domain name (***siteN.cchc.competition***) and a subnet of IPs on which to make its services available.

Some of the services listed in the Scenario document will be provided and will need to be secured. If a Blue Team damages a provided service beyond the point of recovery, the White Team can provide a fresh image of the system, but the Blue Team will incur a scoring penalty of **50 pts** per re-install.

Blue Teams may not perform any offensive action toward any other participant or the network. Doing so may result in a penalty up to disqualification.

Remote Setup

Setup will be available remotely 24/7. Support will be provided during specific hours of the day and support requests can always be emailed to cyberdefense-competition@anl.gov. Include your team number in all correspondence. Blue Teams are encouraged to seek help from anyone (including the White Team) during this phase.

- **Hardware**

Each Blue Team will have access to the VMware vCenter server environment. The White Team operates the administrative accounts on vCenter. These accounts will not be used maliciously, and therefore there is no need to secure the VMware environment.

The Blue Teams will be held accountable for missing or damaged hardware at the end of the competition. If hardware becomes damaged or is missing, contact the White Team immediately.

If hardware fails during the competition or there is a suspected network outage, contact the White Team immediately.

- **Software**

All software used in the competition must be either freely available or provided by Argonne National Laboratory (see the ISO folder in VMware). Trials of non-free software that do not exceed the trial period are allowed.

- **Accounts and Passwords**

A list of users and their passwords will be provided. These must work for the services described in the Scenario document. You may change the password for these users, but the Green Team must be informed of this change. Note that users may be furloughed or fired from their organization and must have their access disabled or removed swiftly if this occurs.

Network Documentation for White Team

Documentation for the White Team represents the reports that real-world companies require of their IT staff (examples: network architecture, security controls). In it, the Blue Team should explain, in detail, its plan for setting up and securing its network. The Blue Team must provide this documentation prior to the scheduled start of the competition by submitting it to the White Team. Documentation is worth up to **200 pts** and should contain the following:

- Details of your network layout (IP addresses, firewalls, whether you have chosen to use NAT).
- Network diagram(s).
- Discussion of the operating systems, software, etc., that you have chosen to run each of your
- Discussion of special measures you've taken to secure your network (Intrusion Detection Systems, specific firewall rules, mandatory access controls, etc.).
- Anything else that you feel demonstrates your preparedness to the White Team.

This document needs to be professional and thorough. Documentation is scored on the following criteria:

- Detail **(0–80 pts)**
- Professionalism **(0–60 pts)**
- Supporting diagrams, figures, and tables **(0–40 pts)**
- Effectiveness of plan **(0–20 pts)**

User Documentation for Green Team

This documentation instructs your users (the Green Team) on how to use your services. The Blue Team must submit this documentation prior to the scheduled start of the competition. Keep in mind that the usability scores given by Green Teams will be severely affected if this documentation is not present. Teams often underestimate the importance of usability. Ensure that your networks have a good balance between usability and security. This documentation is worth up to **200 pts** and should include instructions for users with little or no computer experience on how to use all of the services you have provided.

It is scored on the following criteria:

- Detail of Instructions **(0–40 pts)**
- Clarity **(0–40 pts)**

- Completeness **(0–40 pts)**
- Professionalism **(0–40 pts)**
- Supporting graphics, figures, and diagrams **(0–40 pts)**

Onsite Setup

Argonne will supply the emulated industrial control system as well as all necessary hardware that supports it. To do this, we will be leveraging virtualization accomplished through VMware software. You do not need to bring any hardware, but we suggest you consider bringing a laptop to help you research unusual behavior, write reports, and access your system. We will provide each Blue Team with one machine to access your hardware and VMware console, but we recommend that you bring other machines. We will provide a safe network, isolated from the Red Team attacks, onto which you can connect your personal computers and manage the machines directly.

Attack Phase

During the attack phase, the Red Team will arrive onsite and attempt to gain access to your services. This effort will begin at 9 AM on the day of the competition. We will announce the start of the attack phase on the competition floor before it begins.

Since our small-world network won't emulate the diversity of the actual internet, IP blocks will be considered a denial of service to potential customers and will result in a deduction of points. Blue Teams are not allowed to specifically block or ban specific IPs or IP ranges. Automated systems that block connections for a few minutes after N failed login attempts (e.g., fail2ban) are allowed. If applicable, justify any blocks made after N failed login attempts within your network documentation. The White Team reserves the right to determine whether an IP blocking policy is beyond realistic and thus in violation of the rules.

The Blue Teams may not receive help from anyone other than their team members or the White Team. Receiving help from others, including mentors, friends, etc., will result in a **400-pt** penalty.

- **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 from the White Team via a printed piece of paper. They will be worth varying point values, based on the level of difficulty, and will be designated as such on the hard copy. Blue Teams will need to submit responses to anomalies before they expire in order to earn points.

Responding to anomalies is optional unless stated otherwise. Blue Teams that refuse or do not submit a response will not be awarded any points. Anomalies will account for a significant number of points, and teams are therefore highly encouraged to respond to them.

Blue Team members are in charge of ensuring that the responses to anomalies are submitted on time with professional documentation.

- **Service Uptime**

To help score availability, an automated service scanner will be used every few minutes to ensure that your services are online. These data will be automatically incorporated into scoring results and displayed for all to see in near-real time throughout the competition.

- **Intrusion Reports**

In real-world IT, management requires regular reports on the security of the network, as well as in-depth analysis of any intrusions. Blue Teams are expected to turn in intrusion summary reports at 11:00 am, 1:00 pm, and 3:00 pm. These times can be changed or cancelled at the discretion of the White Team, and any such changes will be announced to the Blue Teams. These reports should cover, in detail, any intrusions noted (in your IDS or otherwise), assessment of the impact, mitigation measures employed by your team, and any evidence acquired to support your analysis. **A simple printout of a log file or a "No Intrusions Detected" document without any evidence to support your claim will not earn any points.** Each report is worth up to **25 pts** and must be submitted to the White Team. Intrusion reports are scored on the following criteria:

- Detail **(0–7 pts)**
- Supporting evidence **(0–5 pts)**
- Insightful analysis **(0–5 pts)**
- Mitigating actions **(0–8 pts)**