Exercise Directive

Version 1.0

Purpose of this Document

This directive serves as a general guide for all participants in Cyber Defense Exercise 2015 (CDX 2015).

Document Revision History

Version	Change Description	Change Owner	Date
1.0	FIRST DRAFT	Jonathan Bristow, Capt, USAF	27 Oct 2014

1.0 Cyber Defense Exercise - 2015

1.1 The goal of the annual Cyber Defense Exercise (CDX) is to provide a simulated real-world educational exercise that will challenge university students to build secure networks and defend those networks against adversarial attacks.

1.1.1 *Core Module with Infrastructure Virtualization Option*

- Locally physical infrastructure, OR
- Remotely administered virtual infrastructure

1.1.2 *Multiple Challenge Modules*

- Ghost in the Network
- Reverse Engineering Malware
- Network Forensics
- Host Forensics
- Secure Coding
- Steganography Challenge

2.0 CDX 2015 Timeline

EVENT	**Projected Dates**
Initial Planning Conference (IPC)	**6 Nov 2014**
Final Planning Conference (FPC)	**Jan 2015**
VPN Up and Running	**Year-round**
Virtual Infrastructure available to participating schools	**Jan 2015**
Pre-built workstation images delivered to all Blue Cell teams	**X-28**
Rubberneck up for connectivity testing	**X-28**
Finalized Exercise Directive and Network Specification delivered	**X-21**
Challenge modules assigned to Blue Cells by RIT	**X-14**
Challenge module submissions from Blue Cells due to RIT	**X-7**
Service Connectivity Testing	**X-7**
Final connectivity testing	**X**
CDX 2015	**X – X+3 Apr 2015**
All services STARTEX at x hrs (Eastern Time)	**X**
Scoring and Red Cell recon/attack starts at x hrs	**X**
Scoring Ends at y	**X+3 Apr 2015**
Announcement of exercise winner	**Noon, X+4 Apr 2015**

3.0 CDX Organization

3.1 Blue Cell

3.1.1 The *Blue Cells* are the eight student teams participating in the exercise, taking the role of component commands involved in the execution of Operation CDX 2015. Each Blue Cell will assign its own organizational components, including the assignment of watch officers who shall be charged with interfacing with Headquarters personnel.

3.1.2 For the core module of CDX 2015, each Blue Cell is required to build and operate its own "BLUENET" network to meet the requirements of this directive and subsequent orders. Successful completion of the exercise will require continued compliance with these rules, often under stressful conditions. For CDX 2015, each student team has an option of implementing their BLUENET either locally or on the remote virtual infrastructure located at CDX HQ. This decision must be confirmed with HQ by the close of business of the Initial Planning Conference on 6 Nov 2014.

3.1.3 For the challenge modules of CDX 2015, provided by Rochester Institute of Technology (RIT), each Blue Cell will select two of the available challenges to be their main challenges. Each Blue Cell may submit either zero or one answer to each of the available challenges. The challenge event will begin place two weeks *[negotiable]* prior to the start of CDX 2015 when RIT makes the challenges available, and it will end after seven calendar days. Only answer per challenge submitted to RIT by a Blue Cell prior to the end of the challenge event will be graded by RIT.

3.2 White Cell

3.2.1 The *White Cell* carries out the role of CDX 2015 Headquarters (HQ). White Cell will monitor compliance with this directive and assess sanctions for noncompliance or other performance issues in each BLUENET. White Cell may issue orders to Blue Cells concerning details of the execution of Operation CDX 2015.

3.2.2 White Cell will deploy individuals to each Blue Cell for greater insight into the Blue Cell subnets. These White Cell liaisons will act as trusted agents, and will have authority to make any time-sensitive decisions.

3.2.3 White Cell will monitor Red Cell and Gray Cell personnel for compliance with this directive and the Red Cell Rules of Engagement.

3.3 Red Cell

3.3.1 The *Red Cell* acts as an Opposition Force (OPFOR), actively testing each Blue Cell's ability to maintain the integrity, confidentiality and availability of its network. Red Cell will deliberately attempt to compromise Blue Cell systems throughout the exercise.

3.3.2 Red Cell will operate under strict Rules of Engagement (RoE) to insure that all Blue Cell teams are given a realistic and impartial challenge.

3.4 Gray Cell

3.4.1 The *Gray Cell* will simulate normal network activity across the Blue Cells to assist White Cell in monitoring compliance with the Exercise Directive.

3.4.2 Members of the Gray Cell will work to simulate legitimate operations as a "user" and/or trusted third party operator. Gray Cell users will act as "trusted insiders" for each BLUENET: simulating user activity inside each Blue Cell user enclave. This function may be augmented by simulation software that is installed on Blue Cell hosts and monitored by Gray Cell members at HQ.

3.4.3 Gray Cell will remotely access their workstations within each BLUENET from CDX HQ via Remote Desktop Protocol (RDP). Any restrictions or policies that detract from normal Gray Cell operations may result in score deductions.

3.4.4 Gray Cell may act as an "insider threat" to the BLUENET by performing actions as directed by the Gray Cell lead. These actions may introduce malicious code to the host. This activity provides each Blue Cell the opportunity to detect, react and deter malicious activity. Blue Cell is permitted to deter threatening insider activity, but should keep in mind that applied mitigations that interfere with users' tasks or automated traffic tools may result in various score deductions.

3.4.5 It is important to remember that the Gray Cell is a "trusted insider". Gray Cell members deployed to the schools are not aware that their directed activity may be malicious or could cause harm to the BLUENETS.

4.0 CDX 2015 Scoring Guidelines

4.1 General Principles

4.1.1 It should be noted that the organizers of CDX 2015 are much more concerned about providing a valid educational experience than providing a contest between schools. Because each school approaches CDX with different resources, it is difficult to have a level playing field. The only true contest is between each school's Blue Cell and the Red Cell.

4.1.2 But, it is fully understood that scoring represents valuable feedback to the exercise participants. Reasonable efforts have been made to make scoring easy to understand by the students, provide transparent and meaningful decisions, and where possible, automate scoring adjudications. At the completion of the exercise, the undergraduate Blue Cell with the most points shall be named the winner of CDX 2015, and shall be awarded the NSA Information Assurance Director's Trophy.

4.1.3 The Red Cell will attempt to break through Blue Cell defenses. When this happens, they will take advantage of these breaches by exfiltrating information from systems, modifying confidential information and preventing user's access to network services.

4.1.4 Points shall be awarded to Blue Cells that successfully build and operate networks that comply with this directive and other orders that may be issued by White Cell during the course of the exercise. Points shall be removed from Blue Cells that do not provide the required functionality or do not comply with this directive or other orders issued by White Cell. The Scoring Specification contains a full listing of penalties.

4.1.5 Emphasis shall be placed on providing the basic components of Information Assurance:

> **Confidentiality.** Information should only be available to authorized users. Excluding information that is cleared for public consumption, much of the information that is processed by or resides on a BLUENET shall be considered "Classified". *If Red Cell can provide proof to White Cell that it has "**read access**" to any of this information, points shall be deducted from the operators of the compromised BLUENET.*
>
> **Integrity.** Information should only be modifiable by authorized users. *If Red Cell can provide proof that it has **"modify access" or "write access"** to any of this BLUENET information, points shall be deducted from the operators of the*

*compromised BLUENET. Additional points shall be deducted if Red Cell provides proof that **"system" or "root" access has been acquired**.*

Availability. Network services are **required** to be ready and available to assist network users during prescribed times. *Points shall be awarded to network operators who keep network services available*.

4.1.6 In addition to these Information Assurance foundational elements, each BLUENET shall be scored based on:

Compliance. BLUENET operators will be asked to comply with this directive and any subsequent order or request for information. *Failure to follow an order or an insufficient response to a request for information shall result in a loss of points*.

4.2 Scoring Components

4.2.1 Scoring Categories Overview:

- Each Blue Cell shall begin the exercise with a score of zero.
- Challenge Modules [20%] (not announced before the final results)
- Core Module
  - Confidentiality/Integrity scored by TokenAgent [35%]
  - Availability scored by Rubberneck [35%]
  - Gray Cell usability scored by the Automated Gray Cell System [10%]
- White Cell Adjustments [positive or negative]

4.2.2 Service Availability

4.2.2.1 Each required service, as described later in this document, in each BLUENET shall be continually monitored for availability. Blue Cells shall be awarded points throughout the exercise based on each service's availability. Services that are available result in a continual flow of positive points. Services that are not available do not contribute points.

4.2.2.2 To contribute maximum points, a service must be available to local users, users from other BLUENETs, CDX HQ users, and users located on the simulated Internet (SIMNET). Services that are only available to local users will contribute significantly fewer points.

4.2.2.3 White Cell shall provide software to each Blue Cell that will generate network traffic and monitor availability. Copies of the software package, named RubberNeck, shall be

installed on workstations in each BLUENET, at White Cell locations and at multiple locations on SIMNET.

4.2.2.4 RubberNeck has the ability to report and score a complete picture of service availability. By collecting availability metrics from within each BLUENET, from White Cell locations and from SIMNET locations, RubberNeck can evaluate and score each BLUENET's total service availability.

4.2.2.5 To maximize availability points, a Blue Cell should be accessible from across the CDX 2015 network. In an effort to defend against malicious traffic, Blue Cells are free to block traffic from any location. But by doing so, they may be blocking an instance of RubberNeck and thus reducing their opportunity to collect points.

4.2.3 Information Confidentiality

4.2.3.1 The Red Cell shall attempt to acquire access to confidential information resident in each BLUENET. Points shall be deducted from each Blue Cell when Red Cell provides proof that confidential information has been accessed.

4.2.3.2 Throughout the exercise, each Blue Cell will be automatically provided with a set of tokens that will represent confidential information. These tokens shall be loaded to specific directories associated with each of the required services and user workstations. Each token will be unique and cryptographically signed. Failure to maintain tokens on each of the required services and user workstations will result in score deductions.

4.2.3.3 Throughout the exercise, Red Cell shall attempt to access the tokens of each Blue Cell. When a token has been accessed, Red Cell shall present the contents of the token to the scoring system. If the token matches a current token, points shall be deducted from the associated Blue Cell's score.

4.2.4 Information Integrity

4.2.4.1 Throughout the exercise, Red Cell shall attempt to modify and/or delete information (tokens) resident and associated with each required service on each BLUENET. If Red Cell can alter any BLUENET information (tokens), points shall be deducted from the operators of the compromised BLUENET.

4.2.5 Compliance

4.2.5.1 BLUENET operators are required to comply with this Directive and any subsequent order or request for information. *Failure to follow an order or an insufficient response to a request for information shall result in a loss of points*.

4.2.5.2 During the course of the exercise, White Cell may make patches available to BLUENET operators for Gray Cell workstations. Specific guidelines will be provided with each patching instruction. *Failure to install these patches in a timely manner shall be viewed as a compliance issue resulting in the loss of points*.

4.2.5.3 White Cell shall ensure Gray Cell is granted access to and use of the designated Gray Cell workstations. Gray Cell must be allowed to conduct those activities consistent with behaviors of a traditional network user (e.g. email, web browsing, access to shares, etc.). *Any lack of usability issues shall be noted by White Cell and may result in the loss of points.*

Unrealistic policies include, but are not limited to:

- Requiring Gray Cell to create a new password every hour
- Preventing the download of all email attachments
- Intercepting emails for Blue Cell administrator approval before forwarding to Gray Cell

White Cell will levy penalties should Blue Cell actions prevent Gray Cell Agents from acting as a network user.

The Gray Cell is required to be able to:

- Send and receive email messages to/from any email address on the CDX network
  - Ability to open attachments
  - Ability to click on links
- Browse the Web (CDX HQ, other BLUENETs and SIMNET)
  - Scripting, .NET, ActiveX, Java and applets enabled
- Download files from the Web (CDX HQ, other BLUENETs and SIMNET)
- Open Office, text and PDF documents
  - Macros enabled
- Run preloaded applications
- Run executable files downloaded/mailed from CDX HQ
- Create and access files on local file system
- Place phone calls from VoIP phones

4.3 CDX Network Architecture

4.3.1 Exercise VPN Configuration

4.3.1.1 The Cyber Defense Exercise Network (CDXN) will consist of components physically located at a number of different sites, including:

- Naval Postgraduate School – Monterey, California (NPS)
- Royal Military College of Canada – Kingston, Ontario (RMC)
- United States Air Force Academy – Colorado Springs, Colorado (USAFA)
- United States Coast Guard Academy – New London, Connecticut (USCGA)
- United States Merchant Marine Academy – Kings Point, New York (USMMA)
- United States Military Academy – West Point, New York (USMA)
- United States Naval Academy – Annapolis, Maryland (USNA)

4.3.1.2 Each school shall be presented an option of infrastructure on which to perform the CDX 2015 core module. Each school shall choose one option at the Initial Planning Conference, and will build their BLUENET within that infrastructure. The first option is the traditional method of building a physically local BLUENET. The second option is a virtual environment hosted physically at HQ and remotely administered from each school's physical location. This Directive shall be interpreted to apply equivalently to both infrastructure options unless stated otherwise.

4.3.1.3 Physical sites comprising the CDX 2015 network will be connected over the public Internet. Exercise traffic must be completely insulated from non-exercise systems, so the physical sites will interact with one another solely by way of a Virtual Private Network (VPN).

4.3.1.4 The schools which select the traditional physically local infrastructure option will set up a VPN using Dynamic Multipoint Virtual Private Network (DMVPN) technology, requiring each site to connect to the Internet through a properly configured Cisco router (2800-series or better). The teams who select the virtual infrastructure option will set up a VPN using an OpenVPN client using a configuration provided by HQ.

4.3.1.5 Any computing device, either physical or virtual, that connects to or touches traffic from the CDX network by either VPN technology (DMVPN or OpenVPN) or as part of a BLUENET enclave should be considered potentially exploited and shall not then connect to nor touch traffic from the Internet.

4.3.2 Allocation of Network Address Spaces

4.3.2.1 The CDX 2015 network will be a Class A private network (10.0.0.0/8). However, actively used IPv4 addresses within the CDX 2015 network will be restricted to two Class B networks:

- BLUENET (10.1.0.0/16)
- SIMNET (10.2.0.0/16)

4.3.2.1 Actively used addresses within BLUENET will be further restricted to the following IPv4 and IPv6 addresses *[subject to change based on virtual infrastructure choices]*:

Cell	IPv4	IPv6
Exercise Headquarters	10.1.10.0/24	fda3:1726:8838::/48
USAFA	10.1.20.0/24	fded:3b25:bc61::/48
USCGA	10.1.40.0/24	fd30:d3fd:204::/48
USMMA	10.1.50.0/24	fde4:f22e:0ad9::/48
USMA	10.1.60.0/24	fd20:d310:9bc7::/48
USNA	10.1.70.0/24	fdc2:49bb:0ada::/48
NPS	10.1.90.0/24	fded:6bb0:c8e8::/48
RMC	10.1.100.0/24	fd05:ce63:cd34::/48
RMC-U	10.1.110.0/24	fd83:7c38:ec7b::/48
Scoring Baseline	10.1.190.0/24	fd5e:4d21:4cb6::/48
NSA Cyber Defense Development Program	10.1.170.0/24	fddb:a0be:9b64::/48

4.3.2.2 Since Red Cell is prohibited from targeting specific ranges of addresses (10.1.11.0/24, 10.1.200.0/24, and 10.250.0.0/24), these addresses may not be used by any participants without specific approval from CDX HQ.

4.3.3 BLUENET

4.3.3.1 BLUENET will simulate a set of local networks operated by a Blue Cell within its Area of Responsibility (AOR). BLUENET subnets will be designed and built by Blue Cell teams, within constraints imposed by the Network Specification. During the active phase, Blue Cells will use BLUENET to carry out exercise activities, while also defending BLUENET systems from hostile attack.

4.3.3.2 BLUENET will have its own Domain Name Service (DNS) hierarchy, which will be required to resolve all names within BLUENET. All domain names within BLUENET will be within the top-level domain .bluenet.

4.3.4 SIMNET

4.3.4.1 SIMNET will simulate the global Internet. Gray Cell and Red Cell members will operate a number of hosts with SIMNET addresses, stimulating the BLUENET with both benign and hostile traffic.

4.3.4.2 The SIMNET DNS hierarchy will be required to resolve all names within SIMNET, and will receive all unresolved requests from the BLUENET DNS. SIMNET DNS will be considered the final authority (the "root server") for all exercise-related traffic. Domain names within SIMNET may fall within any top-level domain.

5.0 BLUENET Operational Requirements

5.1 Required Services

5.1.1 Each participating Blue Cell shall be responsible for designing and building a BLUENET network that complies with a uniform set of requirements listed in this document. The design of the network is completely up to each Blue Cell - what's important is that the design supports all of the required network services and that the network is ready to be put into service at the start of the exercise. After that point, it will be important that the network can be effectively defended.

5.1.2 Each BLUENET network shall provide the following services (additional details may be found in the *CDX Network Specification*):

- Domain Name Service (DNS)
- Centralized credentials repository (for example, Active Directory)
- Network Time Protocol

- E-Mail
  - SMTP
  - IMAP
- FTP
  - With anonymous interface
- VoIP
  - Physical VoIP phones (provided by CDX HQ)
  - SIP/SCCP/RTP client software integrated into scoring system (RubberNeck) client for user workstations
- Web Server
  - With Web Forum functionality
  - Supporting IPv4 and IPv6
- User Workstations Remote Access (within local network)
  - SSH for Linux Workstations, and
  - RDP for Windows Workstations (also must allow inbound for Gray Cell)

5.1.3 Standard service ports must be used:

- HTTP TCP 80
- HTTPS TCP 443
- SSH TCP 22
- RDP TCP 3389
- SMTP TCP 25
- IMAP TCP 143
- FTP TCP 21
- LDAP TCP 389
- NTP UDP 123
- DNS UDP 53
- SIP UDP 5060
- SCCP UDP 2000
- RTP UDP 16384-32678 (all, inclusive)

5.1.4 Strict adherence to licensing agreements is required for all systems and components that participate in a BLUENET. All software on all operational systems shall be fully licensed to include commercial licenses (e.g. Windows operating systems) and licenses that grant free use to academic institutions or the federal government (e.g. open source network analysis tools). “Free for personal use” licenses are unacceptable. The intent is to allow innovative solutions at nominal cost, but deny the advantage of purchasing packaged security solutions such as high-end intrusion prevention systems.

6.0 Hours of Operation

6.1 Regular Duty Hours

6.1.1 Regular duty hours are defined as 0900-2200 EDT each day. White Cell, Gray Cell and Red Cell will all be active throughout this time period. Blue Cell teams will be expected to actively maintain and defend their networks throughout regular duty hours. Outside of regular duty hours, Blue Cell shall not access their systems in any fashion (except the first day). Blue Cell members may be physically within their BLUENET facility up to one hour prior to the start of regular duty hours but they shall not perform any function or keyboard activity (including logging in) on any BLUENET system prior to 0900 EDT.

6.1.2 Within regular duty hours, each Blue Cell team must designate one watch officer. The watch officer will serve as the initial point of contact for any official communications while on watch. It is expected that the watch officer will be physically present in the Blue Cell facility throughout the watch. The scheduling and rotation of watch officers is left to Blue Cell discretion.

6.1.3 Each Blue Cell team must post its daily watch-bill and any scheduled periods of under manning to its web site.

6.2 Off-Duty Hours

6.2.1 Off-duty hours are defined as 2200-0900 EDT each day. During this, Blue Cell teams must stand down and vacate their physical facilities, leaving all network systems fully operational and connected to the CDX 2015 network. White Cell and Gray Cell will also stand down. Red Cell may be active at any time, even in off-duty hours. Scaled down availability scoring shall be performed during off-duty hours.

6.0 Network Monitoring

6.0.1 Communications traffic on the CDX 2015 network will be monitored for research purposes. Participating teams shall be required to sign “consent to monitoring” agreements.

7.0 Role of Faculty

7.0.1 The involvement of faculty and staff will be limited to background support throughout all phases of the CDX. Though this is a subjective call, the ethical intent is for the substantive portion of the exercise to be predominantly student-run. Faculty and staff are

allowed and encouraged to provide some degree of assistance to the students. Faculty and staff shall refrain from hands-on performance of any but the most basic and necessary systems administration tasks, such as low-level systems details that are not typically taught as part of IA coursework.

8.0 Computer Network Attacks by Students

8.0.1 The CDX is a defense and survivability exercise for BLUENET participants. No one, other than the designated Red Cell, shall partake in any form of Computer Network Attack (CNA) operations or other offensive actions according to the discretion of the White Cell. ***Any unauthorized offensive action by any member of a Blue Cell team will cause a loss of up to 50% total points awarded during the exercise per violation by the White Cell.***

Challenge Module Example Proposals (potentially similar to final versions)

(Rochester Institute of Technology (RIT) will provide final proposals at the IPC for discussion.)

- Ghost in the Network
    - Given a small network (30 machines?) of a variety of OS/services find which machines have malicious activity occurring, simulated by flag tokens.
    - Deliverables:
        - Report denoting what machines contain malicious activity.
    - Assessment
        - Did the school identify what machine(s) had malicious activity
        - Was the school able to mitigate the activity
    - Learning Objectives:
        - Identify and investigate malicious activity present on a network
        - Determine and implement mitigation actions to neutralize the malicious activity
- Reverse Engineering/Malware Analysis
    - Have a set of increasing difficulty RE challenges with points associated.
    - Deliverable:
        - Flag from the RE challenges they were able to solve
    - Assessment:
        - Weighted score on the challenges
    - Learning Objectives:
        - Analyze via static and dynamic methods malicious logic
        - Determine malware function
- Network Forensics
    - Have a set of increasingly difficult Network Forensics challenges with points associated.
    - Deliverable:
        - Flag from the NF challenges they were able to solve
    - Assessment:
        - Weighted score on the challenges
    - Learning Objectives
        - Determine critical factors (e.g., time, origin, target, purpose, etc) associated with malicious network activity

- Host Forensics
    - Have a set of increasing difficulty Host Forensics challenges with points associated.
    - Deliverable:
        - Flag from the HF challenges they were able to solve
    - Assessment:
        - Weighted score on the challenges
    - Learning Objectives
        - Determine critical factors (e.g., time, origin, target, purpose, etc) associated with malicious host activity
- Vulnerability Mitigation (Secure Coding)
    - Have a website with several poor coding issues that you know are susceptible to web attacks. Students must identify and fix the code.
    - HQ deliverable: a website containing a variety of coding issues. Including SQL injection, eval, PHP, cross site scripting, etc.
    - Blue Cell Deliverable:
        - A repaired website
        - A report detailing what errors exist. Must include erroneous line(s) of code with repairs.
    - Assessment:
        - Score on what coding errors were fixed/left vulnerable.
    - Learning Objectives
        - Identify code vulnerabilities in an existing software
        - Select and apply appropriate mitigation strategies