

# **CDX 2011**

## **Cyber Defense Exercise**



### **Exercise Directive**

### **DRAFT**

***“Defending a New Domain”***



## **Purpose of this Document**

This directive serves as a general guide for all participants in Cyber Defense Exercise 2011 (CDX 2011).

## **Document Revision History**

<b>Version</b>	<b>Change Description</b>	<b>Change Owner</b>	<b>Date</b>
1.0	FIRST DRAFT	James L. Cody, NSA	27 Jan 2011
2.0	FINAL DRAFT		
3.0	OFFICIAL RELEASE		



## 1.0 Cyber Defense Exercise - 2011

- 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.
- 1.2 For CDX 2011, the exercise theme is *Defending a New Domain* and is referred to as Operation NEWDOMAIN. This is a direct reference to a recently published article by the US Assistant Secretary of Defense which highlighted the increased challenges that military network defenders face (*Defending a New Domain: The Pentagon's Cyberstrategy*, William J. Lynn III, Foreign Affairs. Volume 89, Number 5, September/October 2010, [www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA527707&Location=U2&doc=GetTRDoc.pdf](http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA527707&Location=U2&doc=GetTRDoc.pdf)). Cyber now represents a new domain of warfare and network defenders are on the front lines.

## 2.0 CDX 2011 Timeline

EVENT	Projected Dates
Initial Planning Conference (IPC)	October 2010
Exercise VPN	December 2010
Blue Cells may begin to connect to exercise VPN	December 2010
Mid-Term Planning Conference (MPC)	February 2011
Finalized Exercise Directive and Network Specification complete and delivered to participating schools	February 2011
Red Cell Rules of Engagement ready for faculty review	February 2011
Initial connectivity testing (ping tests) complete	February 2011
White Cell HQ DNS, email server, and file server active	March 2011
Pre-built workstation images delivered to all Blue Cell teams	March 2011
Preliminary connectivity testing involving White Cell and Blue Cells	April 2011
Blue Cell network builds complete	April 2011
Final day for resolution of all technical and connectivity issues – final connectivity testing involving White Cell and Blue Cells	April 2011
CDX 2011	19-21 April 2011
Exercise VPN shut down	22 April 2011



Announcement of exercise winner	22 April 2011
After-Action teleconferences complete	May 2011
NSA completes and delivers After-Action Report for CDX 2011	May 2011

### 3.0 CDX Organization

#### 3.1 Blue Cell

- 3.1.1 The *Blue Cells* are the nine student teams participating in the exercise, taking the role of component commands involved in the execution of Operation NEWDOMAIN. 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 Each Blue Cell is required to build and operate its own local network (BLUENET) 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.

#### 3.2 White Cell

- 3.2.1 The *White Cell* carries out the role of NEWDOMAIN Headquarters. White Cell will monitor compliance with this directive and assess sanctions for noncompliance or other performance issues in each BLUENET.
- 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 Other exercise elements may point out apparent failures of system integrity or availability to White Cell, but will have no independent authority to score the exercise. White Cell will have sole authority to apply scoring rules and assign bonuses or penalties.

#### 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 exercise network. Gray Cell will also assist White Cell in monitoring compliance with the exercise directive.

3.4.2 Some members of Gray Cell will work from exercise headquarters, simulating legitimate actors in the NEWDOMAIN network, along with legitimate third parties operating from the global Internet. Gray Cell will also deploy individuals to each Blue Cell to simulate notional users inside each Blue Cell enclave.

DRAFT

## 4.0 CDX 2011 Scoring Guidelines

### 4.1 General Principles

- 4.1.1 It should be noted that the organizers of CDX 2011 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 will be made to make scoring easy to understand, transparent, meaningful and, where possible, automatic. At the completion of the exercise, the Blue Cell with the most points shall be named the winner of CDX 2011.
- 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 users 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.
- 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 clearing 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 Team provides proof that "system" or "root" access has been acquired.



**Availability.** Network services should 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 base 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 Each Blue Cell shall begin the exercise with a score of zero.

### 4.2.2 **Service Availability**

4.2.2.1 Each required service, as described latter 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, White Cell users, and users from other Blue Cells. 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 assessable from across the NEWDOMAIN network. In an effort to defend again 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 Each morning of the exercise, White Cell shall provide each Blue Cell 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. Each token will be unique and cryptographically signed.
- 4.2.3.3 Each day of the exercise, Red Cell shall attempt to access all of the tokens of each Blue Cell. When a token has been accessed, Red Cell shall present the contents of the token to the White Cell. If it matches the contents of a currently active token, points shall be deducted from the associated Blue Cell's score.

### **4.2.4 Information Integrity**

- 4.2.4.1 Each day of the exercise, Red Cell shall attempt to modify or delete information resident on each BLUENET. 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 Team provides proof that “system” or “root” access has been acquired.

### **4.2.5 Compliance**

- 4.2.5.1 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.

## 4.3 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:

- Air Force Institute of Technology – Wright-Patterson AFB, Ohio (AFIT)
- 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 Physical sites comprising the NEWDOMAIN 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). This VPN will be set up 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).

### 4.3.2 Allocation of Network Address Spaces

4.3.2.1 The NEWDOMAIN network will be a Class A private network (10.0.0.0/8). However, actively used IPv4 addresses within the NEWDOMAIN 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:

Cell	IPv4	IPv6
Exercise Headquarters	10.1.10.0/24	fda3:1726:8838::/48
USAFA	10.1.20.0/24	fded:3b25:bc61::/48

AFIT1	10.1.30.0/24	fd16:de3f:68a2::/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
AFIT2	10.1.80.0/24	fd89:aaa8:c0b3::/48
NPS	10.1.90.0/24	fded:6bb0:c8e8::/48
RMC	10.1.100.0/24	fd05:ce63:cd34::/48

### 4.3.2 *BLUENET*

4.3.2.1 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.

4.3.2.2 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.

### 4.3.3 *SIMNET*

4.3.3.1 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.

4.3.3.2 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 2011 Network Specification*):

- Domain Name Service (DNS)
- Active Directory
- Network Time Protocol
- E-Mail
- FTP
  - With anonymous interface
- VoIP Client
  - With connectivity to Headquarters' VoIP server
- Chat
- Web Server
  - With Web Forum functionality
  - Supporting IPv4 and IPv6
- Network attached printing (i.e., a printer not USB or serially connected)

### 5.2 Hours of Operation

#### 5.2.1 Regular Duty Hours

5.1.2.1 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.

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



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

## **5.2 Off-Duty Hours**

5.2.1 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 NEWDOMAIN network. White Cell and Gray Cell will also stand down. No scoring shall be performed during off-duty hours.

## **5.3 Maintenance Downtime**

5.3.1 Blue Cells are allowed to schedule maintenance downtime as needed. Maintenance downtime must be posted to the Blue Cell team's web site and White Cell must be notified. Posting and notification must be completed at least 2 hours before the commencement of any downtime period. Maintenance is not allowed during off-duty hours.

5.3.1.2 During a maintenance period, network connectivity may be disconnected and any service may be disabled. But, points associated with service availability will be greatly reduced due the lack of service availability from outside the local BLUENET. To maximize point collection, Blue Cells are encouraged to keep maintenance periods focused, rare and short.

## **5.3 Network Monitoring**

5.3.1 Communications traffic on the NEWDOMAIN network will be monitored for research purposes. Participating teams shall be required to sign "consent to monitoring" agreements.