CYBER DEFENSE EXERCISE

CDX 2017 Exercise Directive

CSO

CYBERSECURITY OPERATIONS

The National Security Agency (NSA) is pleased to host Cyber Defense Exercise (CDX) 2017, an intense, academically grounded, week-long competition, designed to sharpen the skills of our Nation's and Allies' next generation of cyber warriors. Since 2001, the Agency has welcomed cadets and midshipmen from the U.S. Coast Guard Academy, the U.S. Merchant Marine Academy, the U.S. Military Academy, the U.S. Naval Academy, the U.S. Air Force Academy, the U.S. Naval Postgraduate School, and the Royal Military College of Canada to participate in this annual competition. Enhancements and challenges are added each year to educate and raise awareness among future military leaders of the role of information assurance in protecting the Nation's critical information systems.

CDX focuses on real-world application of cyber security practices in a high-stakes operational environment. Students design, build, and defend computer networks against simulated intrusions led by NSA experts. Schools are assessed by their ability to maintain network services while detecting and responding to network intrusions and compromises. CDX strives to provide participants a sense of the dangers that exist in a real network environment, along with sound and effective network defense strategies that can be applied to mitigate the threat. This hands-on experience allows students to reinforce learning principles and showcase their cyber skills to successfully outsmart, outmaneuver, and outlast the cyber adversary.

//s//

Cindy Widick
Chief Cybersecurity Operations
NSA/CSS Cybersecurity Mission Manager

TABLE OF CONTENTS

1.0 Cyber Defense Exercise 2017

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

1.1 Core Module with Infrastructure Virtualization Option

a. Locally physical infrastructure, OR

b. Remotely administered virtual infrastructure

1.2 Challenge Modules

Competing Teams (Undergraduates)

a. Malware Analysis/Reverse Engineering

b. Host / Network Forensics

c. Offensive Ethical Hacking

d. Unmanned Aerial Vehicle (UAV)

Non-Competing Teams (Graduates)

a. Malware Analysis/Reverse Engineering

b. Host / Network Forensics

c. Offensive Ethical Hacking

d. Space Cyber Challenge

e. Unmanned Ground Vehicle (UGV)

2.0 CDX 2017 Timeline

Event	Projected Dates
VPN Up and Running	Year-Round
Initial Planning Meeting (IPM)	24 October 2016
Planning Teleconference	5 December 2017
Virtual Infrastructure Available to Participating Schools	15 December 2016
Blue Cell - Virtual / Physical Infrastructure Decision	11 January 2017
Final Planning Meeting (FPM)	23 January 2017
Challenge Modules Assigned to Blue Cells	3 February 2017
RubberNeck Scoring System Up for Connectivity Testing	13 February 2017
CDX HQ Mock Exercise	1 March 2017
Finalized Exercise Directive	10 March 2017
Pre-built Workstation Images Delivered to all Blue Cell Teams	13 March 2017
Service and Final Connectivity Testing (Phones, Internet, Skype, etc…)	7 April 2017
STARTEX – CDX Kickoff Announcement 1000 hrs. EDT	10 April 2017
Red Cell Scanning Begins – 1400 hrs. EDT	10 April 2017
All Services STARTEX at 1400 hrs. EDT	10 April 2017
Red Cell Attacks Start at 0900 hrs. EDT	11 April 2017
CDX 2017	11-13 April 2017
CDX Daily Hotwash at 1600 hrs. EDT	11-13 April 2017
Challenge Module Submissions from Blue Cells Due – 1600 hrs. EDT	12 April 2017
ENDEX – Scoring Ends at 1600 hrs. EDT	13 April 2017
Announcement of Exercise Winner, Noon	14 April 2017
In-Person Participant Debriefs	1 Week Post-CDX

3.0 CDX Organization

3.1 Blue Cells

3.1.1 The Blue Cells are the student teams participating in the exercise, taking the role of component commands involved in the execution of Operation CDX 2017. Each Blue Cell assigns its own organizational components, including the watch officers who interface with Headquarters personnel.

3.1.2 For the core module of CDX 2017, 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 requires continued compliance with these rules, often under stressful conditions. For CDX 2017, each student team may opt to implement their BLUENET either locally or on the remote virtual infrastructure located at CDX HQ. Each Blue Cell must communicate virtual / physical platform decision with CDX HQs by the close of business 11 January 2016.

3.1.3 For the challenge component of CDX 2017, each Blue Cell is provided with a thumb drive and a link to a set of elective challenges. Blue Cells may choose to complete all provided challenges or select the best two for submission. Each Blue Cell may submit either zero or one response to each selected challenge. The challenge event takes place leading up to, and during CDX 2017. Only the first submission for each completed challenge will be graded. As detailed in Appendix A, Scoring Specifications, each module contains seven (7) flags representing specific and completed levels of difficulty. The number of flags obtained, along with the associated percentage values, determines the overall score. Should more than two challenges be completed and returned, the two highest scores will be selected. Scoring is based on a percentage scale from 0% to 100%. Aggregate scores for the challenge modules shall not exceed 100%. In the event of a tie score, the team that completed the challenge fastest within the 56 hour window will be the winner of that challenge.

3.2 White Cell

3.2.1 The White Cell carries out the role of CDX 2017 Headquarters (HQ). White Cell monitors compliance with this directive and assesses sanctions for non-compliance or other performance issues in each BLUENET. White Cell may issue orders to Blue Cells concerning details of the execution of Operation CDX 2017.

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

3.2.3 White Cell monitors Red Cell and Gray Cell personnel for compliance with this directive and the Red Cell Rules of Engagement (ROE).

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 deliberately attempts to compromise each BLUENET system throughout the exercise.

3.3.2 Red Cell shall operate under strict ROE to ensure that all Blue Cell teams receive a realistic and impartial challenge.

3.4 Gray Cell

3.4.1 The Gray Cell simulates 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 work to simulate legitimate operations as a "user" and/or trusted third party operator. Gray Cell users act as "trusted insiders" for each BLUENET: simulating user activity inside each Blue Cell user enclave. Software may be installed on Blue Cell hosts to demonstrate the trusted insider function.

3.4.3 Gray Cell remotely accesses Blue Cell workstations within each BLUENET from CDX HQ via Remote Desktop Protocol (RDP), Secure Shell Protocol (SSH), or Virtual Network Computing (VNC) over SSH via the Gray Cell relay host to simulate legitimate user operations and possible insider threat activity. HQ provides the Gray Cell relay host, which is off limits to Blue Cells and the Red Cell. Additional configuration specifics for the Gray Cell relay host are contained in Appendix B, Network Specifications. Any restrictions or policies that detract from normal Gray Cell operations may result in score deductions.

3.4.4 Gray Cell may act as naïve users to a 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. Each Blue Cell is permitted to deter threatening insider activity; however, applied mitigations that interfere with users' tasks or automated traffic tools may result in various score deductions. Coordinated and successful incident handling can result in some recovery of confidentiality and integrity points (see Appendix A, Scoring Specifications).

3.4.5 Remember, the Gray Cell is a simulated "trusted insider". Automated Gray Cell activities launched at the schools are designed to simulate activity that may be malicious and could cause harm to one or more BLUENETs.

3.4.6 Automation. Gray Cell uses automation software (GRAY_CELL_AUTOMATION) to generate legitimate user traffic as well as simulate an "insider threat" to the Blue Cells. Rather than a physical person located at each Blue Cell, the automation software uses a relay box that acts as an administrative workstation for conducting regular user functions (web searches, emails, links, etc.). This workstation must be able to connect to the CDX HQ and to each workstation in the Blue Cell. The Automated Gray Cell Software is run as a standard user. HQ creates a user called "graycell" and provides the credential information to the Blue Cells. The Automated Gray Cell Software uses a specific transport port: AMQP, which must be open bi-directionally on the relay box and Blue Cell workstations (defined further in Appendix B, Network Specifications).

3.4.7 In addition to providing the Gray Cell remote accesses to Blue Cell workstations, the Gray Cell relay host will be used to perform HQ administrative support to the Blue Cell workstations. HQ Infrastructure Team must be able to remotely access the workstation to troubleshoot issues. The Gray Cell relay is strictly off-limits to the Red Cell. Red Cell members caught accessing the Gray Cell relay are removed from the exercise as directed in the Red Cell ROE.

3.5 Red Cell Rules of Engagement

The following Rules of Engagement are binding on all members of the CDX 2017 Red Cell. Members are required to sign a statement acknowledging that they have read and understood these Rules of Engagement.

3.5.1 Definitions

a. **Active Attack**: Any Red Cell activity that involves direct interaction with Blue Cell hosts or systems. Active attacks include (but are not limited to) running exploits, sending malicious content and performing active port scanning.

b. **Passive Attack**: Any Red Cell activity that does not involve direct interaction with Blue Cell hosts or systems, specifically including passive packet capture.

c. **Denial of Service (DoS) Attack**: Any Red Cell activity that degrades the performance of Blue Cell hosts or systems, whether deliberately or inadvertently. Denial of Service (DoS) attacks include bandwidth flooding, service flooding or the shutdown/reboot of Blue Cell systems.

3.5.2 CDX 2017 Red Cell Policy

a. Red Cell shall be impartial in its attacks against Blue Cell teams. If Red Cell attempts a given attack technique against one Blue Cell team, it must make a good-faith effort to attempt the same attack technique against all Blue Cell teams. Red Cell members shall coordinate their efforts, ensuring that a substantially similar challenge is presented to all Blue Cell teams.

b. Red Cell members may not attack the Availability Scoring Service (RubberNeck) or the Confidentiality/Integrity Scoring Service (Token Agent) to include any services, programs, accounts and/or communication paths they use. Red Cell may alter the actual token files consistent with their intended use, but may not alter any other files, directories, etc. associated with Token Agent. Any Red Cell member who alters such other files or directories is immediately banned from all CDX activity and is asked to leave CDX HQ.

c. Red Cell members shall not perform any DoS attacks between the hours of 2000 and 0900 the following morning.

d. Red Cell members shall not perform any DoS attacks that involve packet flooding or resource exhaustion.

e. Red Cell members shall cease active attacks against any Blue Cell host or network if so directed by White Cell.

f. Red Cell members shall not perform any active or passive attack during times when the Red Cell is specifically directed to stand down.

3.6 CDX 2017 Scoring Guidelines

3.6.1 General Principles

a. Organizers and planners of CDX 2017 are much more concerned about providing a valid educational experience than providing a contest between teams. Because each team approaches CDX with different resources, it is often difficult to achieve and maintain a level playing field. The only true contest is between each school's Blue Cell and the Red Cell.

b. It is clear that scoring represents valuable feedback to the exercise participants. CDX administrators have made scoring easy to understand, so as to provide students with transparent and meaningful decisions. Where possible, CDX administrators automated scoring adjudications. Upon completion, the undergraduate Blue Cell with the most points is named the winner of CDX 2017, and is awarded the NSA CDX Trophy.

c. When the Red Cell attempts to break through Blue Cell defenses, Red Cell exfiltrates information from systems, modifies confidential information, and prevents legitimate users' access to BLUENET network services.

d. Blue Cells are awarded points when they successfully build and operate networks that comply with this directive and orders issued by White Cell during the course of the exercise. Points are removed from Blue Cells that do not provide the required functionality or do not comply with this directive or orders issued by White Cell. Appendix A, Scoring Specifications, contains a full listing of penalties.

3.6.2 Confidentiality, Integrity, Availability

Blue Teams shall place emphasis on providing the basic components of Information Assurance (IA):

a. **Confidentiality.** Blue Teams' information should only be available to authorized users, excluding information cleared for public consumption. The remainder of the information processed by, or residing on, a BLUENET is considered "Classified." If Red Cell can provide proof to White Cell that it has "**read access**" to any of the "Classified" information, points are deducted from the compromised BLUENET operators' scores.

b. **Integrity.** Blue Teams' information should only be modifiable by authorized users. If Red Cell proves that it has "**modify access**" or "**write access**" to any of BLUENET's token information, integrity points shall be deducted from the operators of the compromised BLUENET. Additional points are deducted if Red Cell proves that **"system" or "root" access has been acquired**.

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

3.6.3 Scoring Components/Overview

a. Each Blue Cell begins the exercise with a score of zero.

b. Challenge Modules [30%] (scores/results are not announced before the final results)*

c. Core Module [70%]

i. Confidentiality/Integrity scored by Token Agent [30%]

ii. Availability scored by RubberNeck [30%]

iii. Gray Cell usability scored by the Automated Gray Cell Software [10%]

iv. White Cell Adjustments [positive or negative]

***** In the event of a tie score, the team that completed the challenge in the least amount of time will win the challenge.***

3.6.4 Service Availability

a. Each required service, as described later in this document, in each BLUENET is continually monitored for availability. Blue Cells are awarded points throughout the exercise based on each service's availability. Services, while available, result in a continual flow of positive points. Services, while not available, do not contribute points. Point recoveries for mitigation may be leveraged and will be handled on a case-by-case basis managed by the White Cell Lead.

b. 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 contribute significantly fewer points.

c. White Cell provides software called RubberNeck to each Blue Cell. RubberNeck generates network traffic and monitors availability. Copies of the software package shall be installed on workstations in each BLUENET, at White Cell locations and at multiple locations on SIMNET.

d. RubberNeck reports and scores the complete picture of service availability. By collecting availability metrics from within each BLUENET, from both White Cell and SIMNET locations, RubberNeck evaluates and scores each BLUENET's total service availability.

e. To maximize availability points, a Blue Cell should be accessible from across the CDX 2017 network. To defend against malicious traffic, Blue Cells may block traffic from any location; however, by doing so, Blue Cells may be blocking an instance of RubberNeck, thus reducing their opportunity to collect points.

3.6.5 Information Confidentiality

a. The Red Cell shall attempt to acquire access to confidential information resident in each BLUENET. Points are deducted from each Blue Cell when Red Cell proves that confidential information has been accessed by unauthorized users.

b. Throughout the exercise, each Blue Cell is automatically given a set of tokens that represents confidential information. These tokens shall be loaded to specific directories on each host associated with each of the required services and on each user workstation. Each token is unique and cryptographically signed. Failure to maintain tokens on each required service and user workstation results in score deductions. Some services may be configured as a system of hosts that separate processing components. In that case, the confidential token shall be placed on each host(s) required for the service so the confidentiality test may prove the actual confidentiality protections of the system as a whole. The White Cell may inspect a Blue Cell's service configuration at any time to determine the appropriate placement of tokens.

Note: Additional hosts added to a Blue Cell network that are found not to have the Token Agent service installed, or are unable to store tokens, are fully open to Red Cell attacks - to include full disruption / destruction of services and / or the host Operating System. Red Cell must inquire, and receive concurrence from White Cell prior to carrying out this action. Deception tactics and techniques are permitted on non-hosts only.

c. Throughout the exercise, Red Cell shall attempt to access the tokens of each Blue Cell. When it accesses a token, Red Cell presents the contents of the token to the scoring system. If the token matches a current token, points are deducted from the associated Blue Cell's score. Red Cell shall document the time and manner of the access, and provide suggestions of defensive measures that could have detected, or prevented the access. The Red Cell lead shall provide detailed information on compromises in the Blue Cell scoring sheet to be delivered no later than 10 days following the conclusion of CDX 2017.

3.6.6 Information Integrity

a. 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 are deducted from the compromised BLUENET operators.

3.6.7 Compliance

a. BLUENET operators are required to comply with this Directive and any subsequent order or request for information from White Cell. Failure to follow an order or to provide a sufficient response to a request for information shall result in a loss of points.

b. During the course of the exercise, White Cell may make patches available to BLUENET operators for Blue Cell workstations. Specific guidelines are provided with each patching instruction. Failure to install these patches in a timely manner is treated as a compliance problem, resulting in the loss of points.

c. White Cell shall ensure Blue Cell grants Gray Cell access to, and use of, the designated Blue Cell workstations. Gray Cell must be allowed to conduct activities consistent with behaviors of a traditional network user (e.g., email, web browsing, and access to shares). Any lack of usability issues including, but not limited to, unrealistic policies shall be noted by White Cell and may result in the loss of points at the discretion of White Cell.

i. Unrealistic policies include, but are not limited to:

1. Requiring Gray Cell to create a new password every hour

2. Preventing the download of all email attachments

3. Intercepting emails for Blue Cell administrator approval before forwarding to Gray Cell

4. Requiring Gray Cell to reconfigure proxies every hour

ii. Realistic policies include, but are not limited to:

1. Running AV scans on email attachments, stripping those that are flagged as malicious

2. Blocking access to domains positively identified as malicious

3. Using application whitelisting

4. Killing processes exhibiting indicators of compromise (i.e. disrupting an attack)

d. White Cell will levy scoring penalties should Blue Cell actions prevent Gray Cell from acting as a network user. Blue Cell must coordinate with the White Cell prior to conducting incident handling on user workstations (i.e. alpha, beta, gamma, delta), in order to determine effects to Gray Cell activity.

e. The Gray Cell is required to, and must be able to:

i. Send and receive email messages to/from any email address on the CDX network, to include participating teams. Recipients must be able to:

1. Open attachments

2. Click on links

ii. Browse the Web (CDX HQ, other BLUENETs and SIMNET)

1. Scripting, .NET, ActiveX, Java and applets must be enabled

iii. Download files from the Web (CDX HQ, other BLUENETs and SIMNET)

iv. Open Office, text and PDF documents

1. Macros enabled

v. Run preloaded applications

vi. Run executable files downloaded/mailed from CDX HQ

vii. Create and access files on local file system

4.0 CDX Network Architecture

4.1 Exercise VPN Configuration

4.1.1 The Cyber Defense Exercise Network 2017 (CDXN) consists of components physically located at a number of different sites, including:

- Royal Military College of Canada – Kingston, Ontario (RMC)
- 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)

4.1.2 At the Initial Planning Conference, each school selects one of two infrastructure options on which to perform the CDX 2017 core module, and within which to build their BLUENET. The first infrastructure option is the traditional method of building a physically local BLUENET. The second infrastructure option is a virtual BLUENET environment, hosted physically at HQ and remotely administered from each school's physical location. This CDX Directive document shall be interpreted to apply equivalently to both infrastructure options unless stated otherwise.

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

4.1.4 Teams who select the traditional physically local infrastructure option 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). Teams who select the virtual infrastructure option set up a VPN, terminated by a Cisco Adaptive Security Appliance (ASA) provided by HQ.

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

4.1.6 All team networks must consist of ‘open source’ or ‘free software’ that is readily available to all participants. Commercial products such as BlueCoat or FireEye may not be lent to, nor procured for, individual participants, as it would provide an unfair advantage and is not beneficial to the overall learning experience.

4.2 Allocation of Network Address Spaces

4.2.1 The CDXN is a Class A private network (10.0.0.0/8); however, actively used IPv4 addresses within the CDXN are restricted to two Class B networks:

a. BLUENET (10.1.0.0/16)

b. SIMNET (10.2.0.0/16)

4.2.2 Actively used addresses within BLUENET are further restricted to the following IPv4 and IPv6 addresses:

Cell	IPv4	IPv6
HQ-Exercise Headquarters	10.1.10.0/24	fda3:1726:8838::/48
USCGA (physical infrastructure)	10.1.40.0/24	fd30:d3fd:204::/48
USMMA (virtual infrastructure)	10.1.50.0/24	fde4:f22e:0ad9::/48
USMA (physical infrastructure)	10.1.60.0/24	fd20:d310:9bc7::/48
USNA (physical infrastructure)	10.1.70.0/24	fdc2:49bb:0ada::/48
RMC (physical infrastructure)	10.1.100.0/24	fd05:ce63:cd34::/48
RMC-U (physical infrastructure)	10.1.110.0/24	fd83:7c38:ec7b::/48
Test	10.1.120.0/24	fd5e:4d21:4cb6::/48
RANGE (virtual infrastructure)	10.1.190.0/24	fd2b:2f63:3266::/48

4.2.3 Since Red Cell is prohibited from targeting specific ranges of addresses (10.1.11.0/24, 10.1.200.0/24, 10.1.120.0/24, and 10.250.0.0/24); these addresses may not be used by any participants without specific approval from White Cell.

4.3 BLUENET

4.3.1 BLUENET simulates a set of local networks operated by a Blue Cell within its Area of Responsibility (AOR). Blue Cell teams design and build BLUENET subnets within constraints imposed by the Network Specification. During the active phase (i.e., STARTEX to ENDEX), Blue Cells use BLUENET to carry out exercise activities, while defending BLUENET systems from hostile attack.

4.3.1 BLUENET has its own Domain Name Service (DNS) hierarchy, which is required to resolve all names within BLUENET. All domain names within BLUENET shall be within the top-level domain .bluenet.

4.4 SIMNET

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

4.4.2 The SIMNET DNS hierarchy is required to resolve all names within SIMNET, and receives all unresolved requests from the BLUENET DNS. SIMNET DNS is considered the final authority (the "root server") for all exercise-related traffic. Domain names within SIMNET may fall within any top-level domain. SIMNET DNS traffic shall be operational no later than (1) week prior to STARTEX.

5.0 BLUENET Operational Requirements

5.1 Required Services

5.1.1 Each participating Blue Cell must design and build a BLUENET network that complies with the requirements listed in this document. The BLUENET design is completely up to each Blue Cell, provided that the design supports all required network services, and that the network is ready to be put into service at STARTEX. After that point, the network must be effectively defended.

5.1.2 Each BLUENET network shall provide the following services (additional details may be found in the CDXN Specification Document):

a. Domain Name Service (DNS)

b. Centralized credentials repository (for example, Active Directory)

c. Network Time Protocol

d. Email

  i. SMTP

  ii. IMAP

e. FTP

  i. With anonymous interface

f. Web Server

  i. With Web Forum functionality

  ii. Supporting IPv4 and IPv6

g. User Workstations Remote Access (within local network)

  i. SSH for Linux Workstations, and

  ii. RDP for Windows Workstations

  iii. Gray Cell Remote Access Relay

5.1.3 Standard service ports must be used for the following services. Schools implementing the below-listed service access rules will be considered in compliance with network service/port availability.

Inbound

Source IP	SourcePort	DestIP	DestPort	Rule	ServiceNote
Any	Any	Bluenet	TCP/80	Allow	Web
Any	Any	Bluenet	TCP/443	Allow	Web
Any	Any	Bluenet	TCP/25	Allow	SMTP
Any	Any	Bluenet	TCP/21	Allow	FTP
Any	Any	Bluenet	TCP/143	Allow	IMAP
Any	Any	Bluenet	TCP/389	Allow	LDAP
Any	Any	Bluenet	TCP/123	Allow	NTP
Any	Any	Bluenet	UDP/53	Allow	DNS
HQ+Local Bluenet	Any	Bluenet	TCP/22		SSH *
HQ+Local Bluenet		Bluenet	TCP/3389	Allow	RDP *
HQ	Any	Bluenet	TCP/5672,3	Allow	AMQP*

* (blocking from SIMNET/Remote BLUENET is OK)

Outbound

Source IP	SourcePort	DestIP	DestPort	Rule	ServiceNote
Bluenet	Any	Any	TCP/80	Allow	Web
Bluenet	Any	Any	TCP/443	Allow	Web
Bluenet	Any	Any	TCP/25	Allow	SMTP
Bluenet	Any	Any	TCP/21	Allow	FTP
Bluenet	Any	Any	TCP/143	Allow	IMAP
Bluenet	Any	Any	TCP/389	Allow	LDAP
Bluenet	Any	Any	TCP/123	Allow	NTP
Bluenet	Any	Any	UDP/53	Allow	DNS
Bluenet	Any	HQ,	TCP/22	Allow	SSH *
Bluenet	Any	HQ	TCP/3389	Allow	RDP *
Bluenet	Any	HQ	TCP/5672,3	Allow	AMQP *

* (blocking to SIMNET/Remote BLUENET is OK)

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 0900-2200 EDT each day. White Cell, Gray Cell, and Red Cell will all be active during regular duty hours from STARTEX to ENDEX. Blue Cell teams must 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 after STARTEX, prior to scoring commencement). 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. Blue Cell members may work on the elective Challenge Modules away from their BLUENET facility outside of regular duty hours.

6.1.2 Within regular duty hours, each Blue Cell team must designate one watch officer. The watch officer serves as the initial point of contact for any official communications while on watch. The watch officer must be physically present in the Blue Cell facility throughout the watch. The scheduling and rotation of watch officers is at each Blue Cell team's 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 2201-0859 EDT each day. Blue Cell teams must stand down and vacate their physical facilities, leaving all network systems fully-operational and connected to the CDXN. White Cell and Gray Cell personnel deployed to a Blue Cell must also stand down and vacate the facility during off-duty hours. Red Cell may be active at any time, even in off-duty hours. Scaled down availability scoring is performed during off-duty hours.

7.0 Additional Requirements

7.1 Java Run Time Environment (JRE)

a. JRE version 1.7 or newer is required on any system (server, workstation, etc…) for the Token Agent service to run.

7.2 Network Monitoring

a. Communications traffic on the CDXN is subject to monitoring. Participating teams shall sign "consent to monitoring" agreements.

7.3 Role of Faculty

a. Faculty and staff involvement is limited to background support throughout all phases of the CDX. The intent is for the substantive portion of the exercise to be predominantly student-run. Faculty and staff may provide minimal 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 not typically taught as part of IA coursework. The level of involvement is subjective and subject to oversight by White Cell.

7.4 Computer Network Attacks by Students

a. CDX is a defense and survivability exercise for BLUENET participants. No one, other than the designated Red Cell, shall partake in any form of Offensive Cyber Operations (OCO) or other offensive actions. Determination and scoring weight of offensive actions are at the discretion of White Cell. **Unless specifically directed otherwise by CDX HQ, any unauthorized offensive action by a Blue Cell team shall result in a per violation penalty of up to 50% of the total points awarded to the offending Blue Cell team during CDX 2017, as determined by the White Cell.**

8.0 Challenge Module Descriptions

8.1 Reverse Engineering (RE) / Malware Analysis Challenge

a. Learning Objectives

i. Analyze potentially malicious code via static and dynamic methods

ii. Analyze malware to determine its functionality

iii. Based on those analyses, determine ways to mitigate the malware

b. Activity

i. A malware analysis scenario requiring reverse engineering of executables to achieve defined objectives, with points given for each successful step accomplished.

c. Deliverables

i. Answers to the questions posed for the Reverse Engineering (RE) / Malware Analysis Challenge

ii. Provide Easy, Medium, and Difficult areas of focus

d. Assessment

i. Weighted score on the challenges in Section 8.0

e. Completion Time

i. Module is due 56 hours following STARTEX, but no later than 1600, 13 April 2017

8.2 Host / Network Forensics Challenge

a. Learning Objectives

i. Determine which network and host activity is malicious

ii. Determine critical factors (e.g., time, origin, target, purpose, etc.) associated with malicious network and host activity

b. Activity

- A network and host forensics scenario requiring teams to achieve defined objectives, with points given for each successful step accomplished

c. Deliverables

i. Answers to the questions posed for the Network / Host Forensics Challenge

ii. Provide Easy, Medium, and Difficult areas of focus

d. Assessment

i. Weighted score on the challenges in this Section 8.0

e. Completion Time

i. Module is due 56 hours from STARTEX, but no later than 1600, 13 April 2017

8.3 Offensive Ethical Challenge

a. Learning Objectives

i. Acting as an adversary, determine how to overcome various system defenses to obtain the defined objectives

b. Activity

i. A scenario requiring offensive hacking of various targets to achieve defined objectives, with points given for each successful step accomplished

c. Deliverables

i. Answers to the questions posed for the Hacking / CTF Challenge

ii. Provide Easy, Medium, and Difficult areas of focus

d. Assessment

i. Weighted score on the challenges in this Section 8.0

e. Completion Time

i. Module is due 56 hours from STARTEX, but no later than 1600, 13 April 2017

8.4 Unmanned Aerial Vehicle (UAV) Challenge

a. Description

i. Doctrine defines cyberspace as one of the five interdependent domains and uniquely characterizes it as the only non-physical domain (Cyberspace Operations, Joint Publication 3-12 (R), 5 February 2013). Cyber assets possess a dual presence in the cyber/physical domains and effects generation through cyber is inextricable linked to both domains. Cyber education and training must provide strong links between the cyber and physical domain with an emphasis on mission assurance.

ii. This challenge strongly couples air and cyber operations through a problem that requires integrated, multi-domain fires to achieve a desired operational end state. The challenge requires participants to interpret intelligence, develop a strategy to achieve a desired end state, coordinate multi-domain fires and coordinate the execution of air and cyber elements.

b. Learning Objectives

i. We outline learning objectives for the activity in terms of Bloom's Taxonomy, each bullet includes the cognitive level of achievement paired with a brief description of the objective.

1. Comprehension – express the relationships between the cyber and physical domains

1. Application – demonstrate leadership skills in a multi-domain environment

2. Synthesis – create a strategy to achieve a desired end state from tactical objectives

3. Application – interpret intelligence to understand the adversary order of battle

4. Synthesis – plan an integrated cyber/physical op to achieve tactical objectives

5. Synthesis – design and develop a mechanism to secure an Unmanned Vehicle (UV) Command and Control (C2) link

c. Activity

i. We decompose the challenge problem into two activities: Intelligence Preparation of the Battle Space (IPBS) and Mission Execution (ME). IPBS includes all activities required to plan the cyber and physical components of a mission to strike targets on the Joint Prioritized Target List (JPTL). ME encompasses all activities that result in cyber or physical fires and the flight of the UV during the live portion of CDX. The IPBS and ME require participation by the team over a 72-hour window prior to the live portion of CDX. During this time, the team has access to their own UV assets and can observe/interact with adversary UV assets. During the live portion of CDX, the UV autonomously flies a reconnaissance mission. At the start of any contiguous 72-hour window prior to the live portion of CDX, the on-site AFRL Support Team provides the team with the following planning/operating documentation, software, assets, and access.

ii. Joint Force Commander's Desired End State

iii. Joint Force Commander’s Joint Prioritized Target List

iv. Adversary expected static order of battle

v. Technical description of the adversary UV capabilities and implementation details

vi. ICARUS User Manual: Operator instructions for C2 of Unmanned Aerial Vehicles

vii. Cyber needs description of the requirement to protect coalition UV C2 links

viii. ICARUS: C2 interface to control UV’s (Software – Binary)

ix. 4x UV with Air to Ground capability (Sim Vehicle)

x. 1x UV with Radar capability (Sim Vehicle)

xi. 1x Development UV for testing mechanisms to protect C2 links

xii. 5X telnet access to UAV (Access)

1. During the 72-hour window the team has access to their own UV assets to navigate the battle space, prototype software, and determine adversary capabilities in order to create protections for their own UV assets in the ME portion of the challenge. The on-site AFRL Support Team will not reconstitute any friendly or adversary UV assets lost during this time. The team will have the capability to reconstitute the development UV as part of their testing.

2. The on-site AFRL Support Team scores the team for successful strikes on JIPTL targets, protecting their C2 link and preserving their UV’s. There are five JIPTL targets with the following profiles:

SAURON Airfield – Home to Bombers ***16,670 points***
Airfield with conventionally equipped strategic bombers and protected by autonomous defensive counter air UAV assets.

SPECTRE Industries – Advanced UV Facility ***16,670 points***
UV research and development facility with critical defense implications and protected by autonomous defensive counter air UAV assets.

Phosphex Production and Research Facility ***16,670 points***
Industrial facility responsible for the creation of the Phosphex chemical agent protected by defensive counter air UAV assets.

SMAUG Airfield – Home to Strategic Bombers ***16,670 points***
Airfield with Phosphex equipped strategic bombers and protected by autonomous defensive counter air UAV assets.

SHELOB Airfield – Home to A2A Assets ***16,670 points***
Airfield with conventionally equipped defensive counter air UAV assets.

3. During the IPBS and ME teams will develop their plans to strike the JIPTL targets and develop software to protect their own UV C2 link. The requirements for these activities include:

Protect UV C2 Link ***16,670 points***
The C2 link between ICARUS and the UV systems provides no intrinsic security. The team must develop their own mechanism to retain positive control of their UV's. The team will deliver the solution to the on-site AFRL Support Team. The team cannot add hardware to the UV and must operate within the processing, memory and storage constraints of the UV system. The on-site AFRL Support Team will load the solution to the vehicles prior to ME according to the Tech Order provided by the team.

Efficiency and Speed ***16,670 points***
The team earns a score based on the number of their own assets preserved at the end of ME and at the rate at which they compromise Iron Zone Industries. The vehicles are worth 50% of these points, with a linear scale starting at 0 points if no UAVs remain. The compromise of Iron Zone Industries is measured by planting flags on each machine that has been taken. The scoring system automatically checks these flags and adds to the team score so long as the flag remains for the 72-hour window.

d. Deliverables

i. The team must provide the on-site AFRL Support Team deliverables within 24 hours of the close of the 72-hour IPBS.

1. UV component of software developed to protect their UV C2 link

2. Tech Order describing how the on-site AFRL Support Team shall load the software to the UV

e. Assessment

i. The on-site AFRL Support Team scores this challenge problem out of 100,000 points with the breakdown described in the Activity section. Mission scoring for the five JIPTL targets is binary, with credit given only for successful mission completion. The on-site AFRL Support Team scores the protect UV C2 link activity progressively through ME, with full points if the UV remain operational for the full duration of CDX. An on-site AFRL Support Team Mission Server scores these elements automatically. We score the Efficiency and Speed automatically during the 72-hour window prior to the start of CDX.

f. Completion Time

i. The team has 72 hours to plan, develop and test on the live network prior to the start of CDX.

8.5 Unmanned Ground Vehicle (Graduate / Non-Competing Teams)

a. Learning Objectives

i. We outline learning objectives for the activity in terms of Bloom's Taxonomy, each bullet includes the cognitive level of achievement and a brief description of the objective.

b. Activity

i. We decompose the challenge problem into two activities: Intelligence Preparation of the Battle Space (IPBS) and Mission Execution (ME). IPBS occurs during prior to the Cyber Defense Exercise. IPBS starts with a 72-hour window for the team to access their own UV assets and to observe/interact with adversary UV assets. At the start of the 72-hour window, the on-site CDX AFRL Support Team provides the team with the following planning/operating documentation, software, assets and access.

ii. Joint Force Commander's Desired End State

iii. Joint Force Commander's Joint Prioritized Target List

iv. Adversary expected static order of battle

v. Technical description of the adversary UV capabilities and implementation details

vi. ICARUS User Manual: Operator instructions for C2 of Unmanned Aerial Vehicles and Unmanned Ground Vehicles

vii. Cyber needs description of the requirement to protect coalition UV C2 links

viii. ICARUS: C2 interface to control UV's (Software - Binary)

ix. Python Binary for an adversary SAM control system (Software – Packed Binary)

x. Payload framework for a VENOM hypervisor jailbreak (Software – Source)

xi. 4x UAV with Air to Ground capability (Sim Vehicle)

xii. 1x UAV with Radar capability (Sim Vehicle)

xiii. 1x UGV with wireless card in promiscuous mode (Physical Vehicle)

xiv. 5x telnet access to UAV (Access)

xv. 1x telnet access to UGV (Access)

xvi. 1x SSH as user access to a Linux web server (Access)

1. During the 72-hour IPBS the team has access to their own assets to navigate the battle space, prototype software, and determine adversary capabilities in order to develop their operational for the ME portion of the

challenge. The on-site AFRL Support Team will reconstitute any friendly UAV or UGV assets that are accidentally destroyed at 0800 EST each day during the 72-hour IPBS window.

2. Mission Execution begins at the start of live portion of CDX and completes at the conclusion of the live portion of CDX. The on-site AFRL Support Team scores the team for successful strikes on JIPTL target, protecting their C2 link and preserving their UV's. During this time, the on-site AFRL Support Team shall not reconstitute any lost vehicle assets. There are four JIPTL targets with the following profiles:

SAURON Airfield – Home to Phosphex Bomber ***16,670 points***
Airfield with Phosphex equipped strategic bombers protected by a next generation A2A UAV. The UAV C2 link is authenticated via a shared secret and SHA-2 hash with the form Hash (secret + message). This form is vulnerable to a length extension attack to divert/crash the UAV and open an attack corridor.

Phosphex Production and Research Facility ***16,670 points***
Industrial facility responsible for the creation of the Phosphex chemical agent protected by a next generation A2A UAV. The UAV C2 link is encrypted with AES 256 in CBC mode. The link has no replay protection and the team can replay captured packets open an attack corridor.

SMAUG Airfield – Home to A2A Assets ***16,670 points***
Airfield with advanced A2A assets protected by a networked SAM Battery. SAM control is hosted on a shared, secure cloud running the Xen hypervisor. This hypervisor is vulnerable to the VENOM exploit. The on-site AFRL Support Team provides teams with user access to a VM hosted on the same hypervisor and the framework for the VENOM exploit to enable a hypervisor jailbreak. Access to the hypervisor allows the team power down the networked SAM Battery and open an attack corridor.

SHELOB Airfield – Home to Bombers ***33,340 points***
Airfield with bombing assets protected by an on-site, standalone SAM battery. The SAM battery is hosted on a network with localized RF connectivity and is controlled by software the on-site AFRL Support Team provides to the team. The RF connection is emulated by an 802.11g wireless router located at the Parsons facility. The team must navigate a ground vehicle into position to intercept the WPA2 handshake to gain access to the network. With access, the team can use information gleaned from reverse engineering the SAM control software provided by the on-site AFRL Support Team to open an attack corridor.

3. During the IPBS teams will develop their plans to strike the JIPTL targets and develop software to protect their own UV C2 link. The requirements for these activities include:

Protect UV C2 Link ***16,670 points***
The C2 link between ICARUS and the UV systems provides no intrinsic security. The team must develop their own mechanism to retain positive control of their UV's. The team will deliver the solution to the on-site AFRL Support Team. The team cannot add hardware to the UV and must operate within the processing, memory and storage constraints of the UV system. The on-site AFRL Support Team will load the solution to the vehicles prior to ME according the Tech Order provided by the team.

Mission Planning ***16,670 points***
The team must create a mission plan to achieve the JFC objectives. The on-site AFRL Support Team will assess the document for accuracy and completeness. The team should note any relevant planning information that cannot be gathered until ME. A specific form for the planning document is not required, but the on-site AFRL Support Team recommends the document generally follow the form prescribed in JP-5-0.

c. Deliverables

i. The team must provide the on-site AFRL Support Team deliverables within 24 hours of the close of the 72-hour IPBS. The team may continue planning, refining and working on their solutions during the intervening time until ME. However, the on-site AFRL Support Team will not accept any changes to the deliverables themselves.

1. UV component of software developed to protect their UV C2 link.

2. Tech Order describing how the on-site AFRL Support Team shall load the software to the UV.

3. Mission Plan describing the cyber and physical operations required to achieve the JFC objectives.

d. Assessment

i. The on-site AFRL Support Team scores this challenge problem out of 100,000 points with the breakdown described in the Activity section. Mission scoring for the four JIPTL targets is a binary, with credit given only for successful mission completion. The on-site AFRL Support Team scores the protect UV C2 Link activity progressively through ME, with full points if the UV remain operational for the full duration of CDX. An on-site AFRL Support Team Mission Server scores these elements automatically. We score the Mission Plan scored based on completeness, correctness and professionalism according to a rubric.

e. Completion Time

i. The team has 72-hours to plan, develop and test on the live network prior to the start of CDX. Once ME begins, the team has until the conclusion of CDX to strike the JIPTL targets and maintain their UV fleet.

8.6 Space Cyber Challenge (Graduate / Non-Competing Teams)

a. Learning Objectives

i. Secure and defend communications on satellites to include the telemetry, tracking, and command (TT&C) link, data link, and internal bus traffic

ii. Prevent an attack on a network accessed ground station and satellite by an unknown adversary

iii. Perform an attack on network accessed ground stations and satellites

iv. Perform set of objectives

b. Activity

i. Secure and defend own Linux VM with ground station application

ii. Perform missions utilizing satellite capabilities

iii. Maintain control of ground station application and satellite

iv. Plan and execute attacks on ground stations and satellites

c. Deliverables

i. Answers to challenge questions and injects

- Sensor data collection
- Image collection
- Correct course
- Etc.

ii. Keep control of ground station and satellite

iii. Prevent adversarial hacking of ground station and satellite

iv. Proof of attacks (copied files, knowledge of secured info, disrupted systems, etc.)

v. Provide a list of easy, medium, and difficult areas of focus

d. Assessment

i. Score will be based on completion of missions and overall defensive/offensive maneuvers

e. Completion Time

i. Module will begin with delivery of ground station and satellite (CubeSat) for students to become familiar with application (March 2017)

ii. Module will be executed (missions, defense, and offense) during the Core Exercise (April 2017)

9.0 Top Ten NSA IA Mitigations

CDX Leadership is committed to adhering to most of the NSA/IA mitigation strategies to make CDX a realistic and educational experience. Please see Appendix C, NSA /IA Mitigation Strategies.

Appendix A Scoring Specifications

OVERVIEW

The *CDX 2017 Exercise Directive* addresses the general principles surrounding scoring. *Appendix B*, *Network Specifications* provides details on key network elements evaluated during the exercise by the various scoring processes. *Appendix A, Scoring Specifications* provides more specifics on the various components of the scoring processes. In addition, details are defined regarding the calculations that shall be used to determine each school's score.

1.0 Scoring Structure

1.0.1 Blue Cell scores shall be displayed as a percent value within the range of: 0% to 100%.

1.0.2 Blue Cell scores shall be calculated using the following weighting scheme:

a. 30% - Required Services Availability, weighted by:

i. 80% - On-Duty hours

ii. 20% - Off-Duty hours

b. 30% - Information Confidentiality & Integrity, weighted by:

i. 70% Required Services Servers

ii. 30% User Workstations

c. 10% - Gray Cell usability

d. 30% - Challenge Modules, weighted by:

i. 50% Challenge Elective #1

ii. 50% Challenge Elective #2

iii. The elective #1 and #2 refer to the top two scoring challenges from that school

e. White Cell Adjustments at the discretion of White Cell/CC at HQ

i. Adjustments may be either positive or negative

ii. Adjustments are applied to each school's total score

1.0.3 In the event of a tie score, the total number of availability points shall be used to break the tie.

2.0 Availability Scoring

2.1 RubberNeck Traffic Generator / Availability Evaluator

2.1.1 RubberNeck is a set of software applications that combine to form a sophisticated traffic generator and availability evaluation system for CDX 2017. It has three main components:

a. **RubberNeck Client** – Software application that runs on all user workstations in each BLUENET and at various locations in the CDX HQ as well as in SIMNET; the application evaluates the availability of required services at each BLUENET and reports its findings to a server at CDX HQ.

b. **RubberNeck Server** – A CDX HQ application that performs the command and control function in the RubberNeck system; it maintains configuration control and version checking for each instance of the RubberNeck Client; and it collects availability scoring points from each RubberNeck Client. All communication between the RubberNeck Client and the RubberNeck Server are encrypted.

c. **RubberNeck Local Server** – An optional application that is intended to run on each BLUENET; it receives a copy of all information sent to the RubberNeck Server at CDX HQ and provides situational awareness to the Blue Cell through a series of web site updates.

2.1.2 RubberNeck Client and the Rubberneck Local Server are available for download at the CDX HQ portal (http://www.hq.bluenet/traffic.html).

2.1.3 RubberNeck features a dynamic configuration. Throughout the exercise, its behavior changes based on configuration changes made at CDX HQ.

2.2 RubberNeck Operations on Each BLUENET

2.2.1 Each RubberNeck Client evaluates the required services on each BLUENET within both the local remote BLUENETS. It also evaluates availability of the other user workstations on its BLUENET.

RubberNeck Client Validates Availability of Required Services From All Around the CDX Network

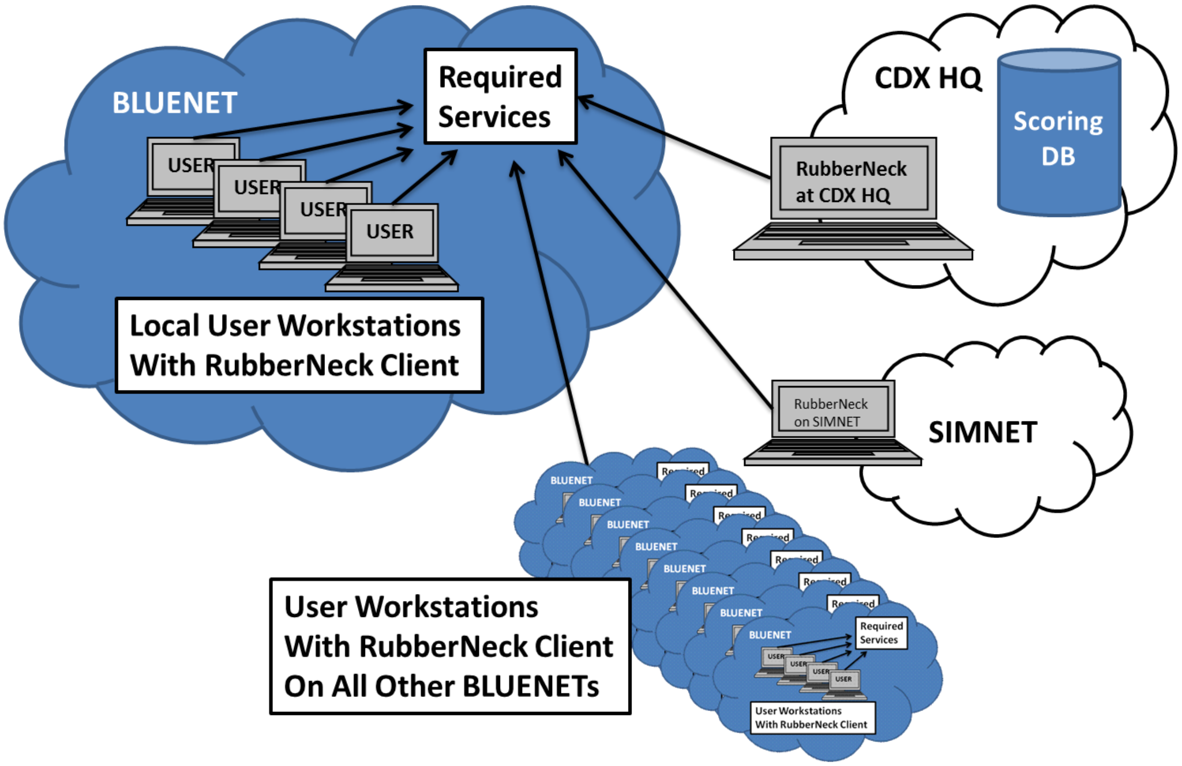

BLUENET
Required Services
USER
USER
USER
USER
Local User Workstations With RubberNeck Client
CDX HQ
Scoring DB
RubberNeck at CDX HQ
RubberNeck on SIMNET
SIMNET
User Workstations With RubberNeck Client On All Other BLUENETs
BLUENET
Required Services
User Workstations With RubberNeck Client

Figure 1, RubberNeck Client Validates Required Services

2.2.2 Each RubberNeck Client communicates availability status results to the RubberNeck Server at CDX HQ using HTTPS. If web proxies are in use, settings in the RubberNeck configuration file must be changed.

2.2.3 The RubberNeck Client may need to log in to various services in order to validate availability of required services. The CDX 2017 Network Specification provides details on the specific user ID and password requirements for RubberNeck and any password protected services

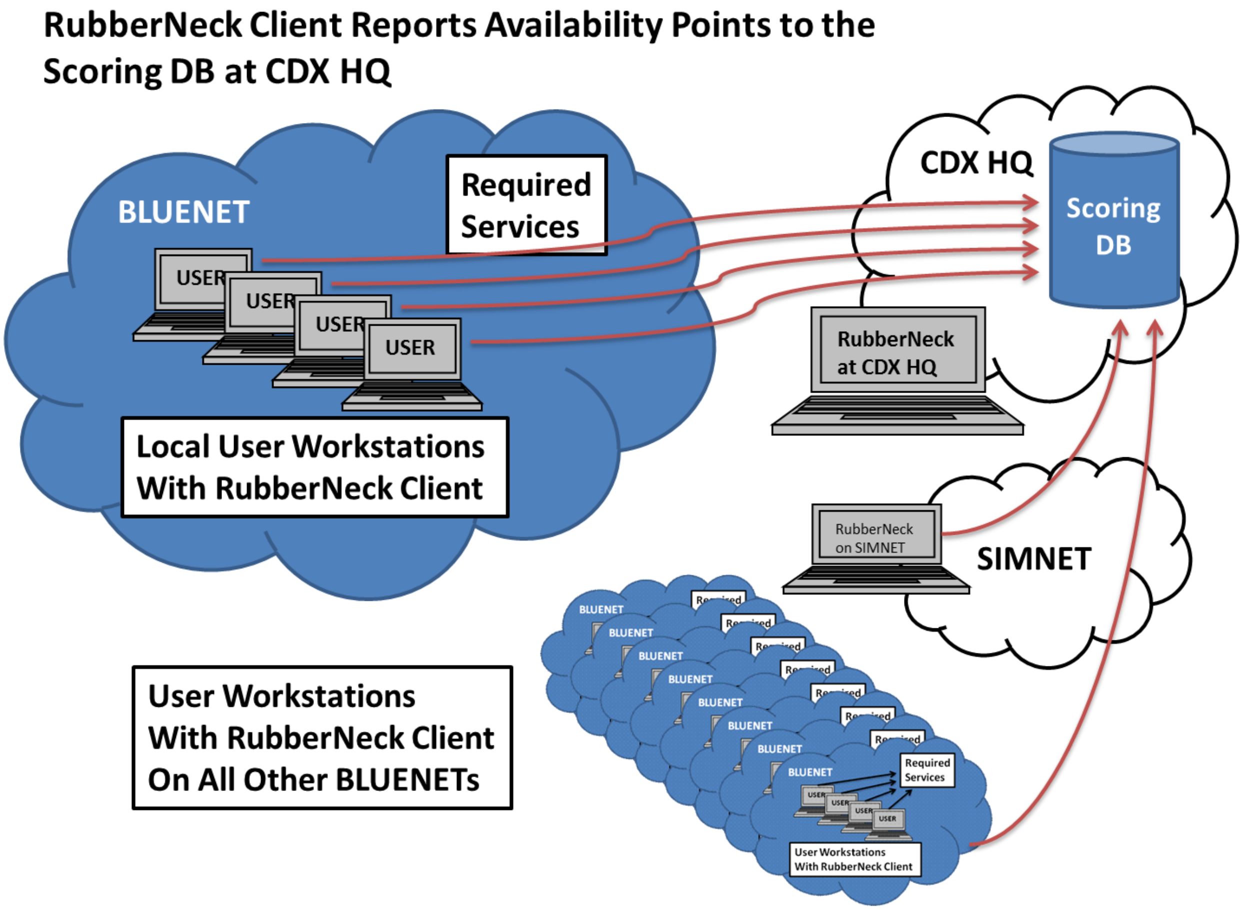

RubberNeck Client Reports Availability Points to the Scoring DB at CDX HQ
BLUENET
Required Services
USER
USER
USER
USER
Local User Workstations With RubberNeck Client
CDX HQ
Scoring DB
RubberNeck at CDX HQ
RubberNeck on SIMNET
SIMNET
BLUENET
Required Services
User Workstations With RubberNeck Client
User Workstations With RubberNeck Client On All Other BLUENETs

Figure 2, RubberNeck Client Reports Findings to CDX HQ

2.3 RubberNeck Client Disruptions and VM Rollbacks

2.3.1 The RubberNeck Server can detect unauthorized changes to the RubberNeck Client. This feature is designed to prevent tampering with the system. Any unauthorized changes to RubberNeck Client, such as rolling back a VM hosting RubberNeck shall result in the loss of points equal to one full hour of availability reporting from that workstation.

2.3.2 The RubberNeck Server can detect when the RubberNeck Client has been restarted. If the RubberNeck Client is restarted for any reason, such as resetting the workstation, shall result in the loss of points equal to one quarter hour of availability reporting from that workstation.

2.4 Availability Scoring, Continuous Postings

2.4.1 Each BLUENET shall be continuously monitored, scored and posted to reflect the availability of required services, stated as a percentage. This score shall be calculated by using the following formula:

2.4.2 Availability Score = Points Collected / Points Available

2.4.3 Each BLUENET and SIMNET RubberNeck client generates one point each time it validates that a required service is operational at a school's BLUENET.

2.4.4 The CDX HQ RubberNeck client generates two points each time it validates that a required service is operational at a school's BLUENET.

2.4.5 Given that RubberNeck clients are located across the entire CDX Network and that each RubberNeck client validates all of the required services at all schools, a considerable number of data points are available for this calculation. This information is stored in a database at the CDX HQ and is available to each school throughout the exercise.

2.4.6 On-Duty vs. Off-Duty Scoring

2.4.7 Note that the first hour of each on-duty time period (9:00 to 10:00 EDT) shall be scored with off-duty weighting (20%). Accordingly, each day of the exercise shall include 12 hours of on-duty scoring, from 10:00 to 22:00 EDT. Each day shall also include 12 hours of off-duty scoring, from 22:00 to 10:00 EDT.

2.5 Overall Availability Scoring

2.5.1 Each school's cumulative availability score shall be a weighted average of the hourly scores, allowing for a significantly higher weight for on-duty hours. Scores shall be calculated using the following formula:

Overall Availability Score = (Average **On-Duty** Availability Score *** .80**)
+ (Average **Off-Duty** Availability Score *** .20**)

3.0 Information Confidentiality and Integrity Scoring

3.1 Token Agent

3.1.1 Token Agent is a set of software applications that combine to form a sophisticated confidentiality and integrity evaluation system for CDX 2017. It has the following main components:

a. **Token Agent Client** – Software application that runs on selected BLUENET servers and workstations; both Windows and Linux are supported. The application places CDX Tokens on BLUENET systems, monitors the integrity of these tokens and reports status to CDX HQ. Specific aspects of the Token Agent Client for Linux are configurable by Blue Teams by means of editing the “token_agent_curl.cfg” file – see installation instructions for details.

b. **CDX Tokens** – Files created by Token Agent that are unique and identifiable by Token Agent. CDX Tokens represent confidential information stored on BLUENET systems. Red Cell will attempt to copy or alter the contents of these files to prove that the system's confidentiality or integrity was compromised.

c. **Token Agent Server** – A CDX HQ application that collects Token Agent status and reports that status to the CDX Scoring Database. All communication between the Token Agent Client and the Token Agent Server are encrypted by default.

3.1.2 Token Agent Client is available for download at the CDX HQ portal (http://tokens.hq.bluenet/static). An automated installation procedure is included in the download.

3.1.3 Token Agent Client runs at the "root" or "system" level and creates CDX Tokens that are readable by all user accounts. If Red Cell gains user level access to a system, it constitutes a "confidentiality" compromise. If Red Cell gains root (system) access, it constitutes an "integrity" compromise.

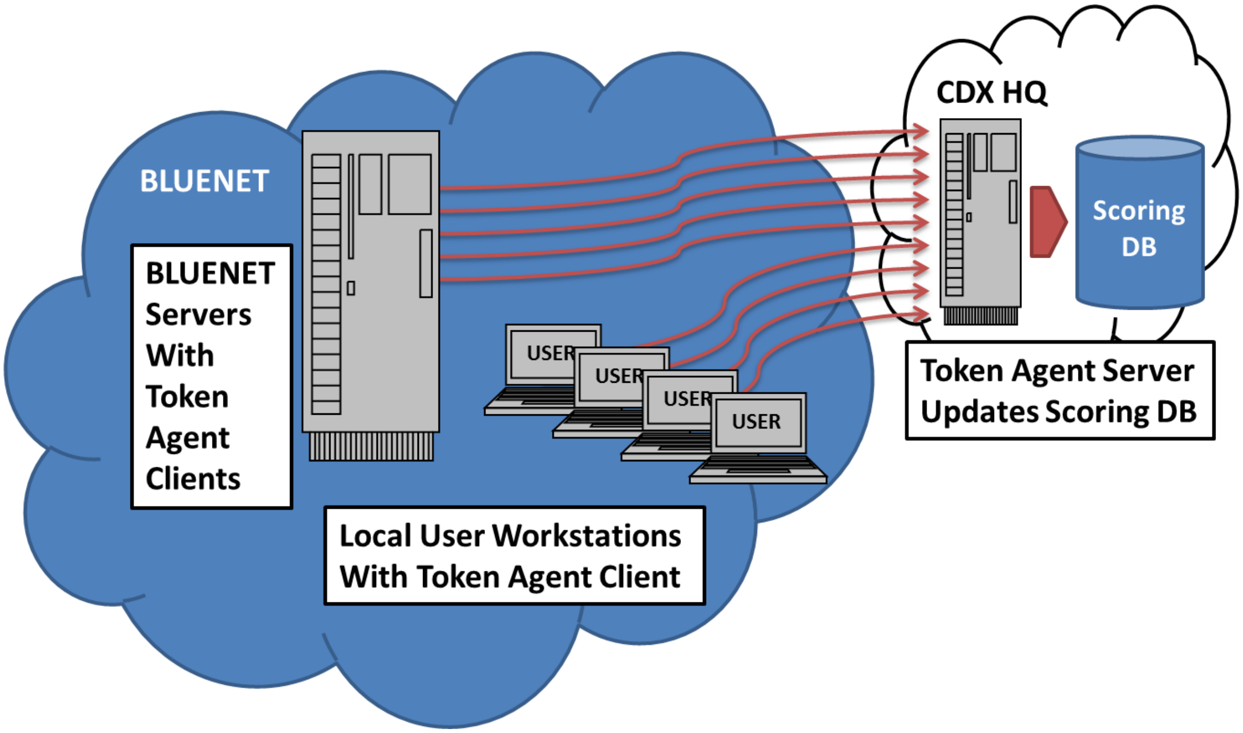
3.1.4 Hosts added to a Blue Cell network discovered and found not to have the Token Agent service installed, or that are unable to install tokens, are fully susceptible to Red Cell attacks - to include full disruption / destruction of services and / or the host Operating System. These attacks will affect the overall availability of the system.

3.2 Token Agent Operations on Each BLUENET

3.2.1 Java Run Time Environment (JRE) Version 1.7 or newer is required on any system (server, workstation, etc…) for the Token Agent service to run.

3.2.2 Each Token Agent Client communicates CDX Token status checking results to the Token Agent Server at CDX HQ using HTTPS by default.

Token Agent Clients in BLUENETS Report Status of Tokens to Token Agent Server at CDX HQ Which Updates Scoring DB


BLUENET
BLUENET Servers With Token Agent Clients
USER
USER
USER
USER
Local User Workstations With Token Agent Client
CDX HQ
Scoring DB
Token Agent Server Updates Scoring DB

3.2.3 Token Agent Client monitors CDX Tokens that reside in the same directory. For example, on a Windows machine that is performing as a Web Server, Token Agent Client software and the CDX Tokens that it monitors would reside and operate in the C:\TOKEN_AGENT\WEB\ directory.

3.2.4 Token Agent monitors CDX Tokens associated with a subset of the CDX 2017 required services and use the specified directory structures:

a.	**EMAIL** Server	Windows:	C:\TOKEN_AGENT37\MAIL\
		Linux:	/TOKEN_AGENT37/**MAIL**/
b.	**WEB** Server	Windows:	C:\TOKEN_AGENT37\WEB\
		Linux:	/TOKEN_AGENT37/ **WEB** /
c.	**DNS** Server	Windows:	C:\TOKEN_AGENT37\DNS\
		Linux:	/TOKEN_AGENT37/**DNS**/
d.	**FTP** Server	Windows:	C:\TOKEN_AGENT37\FTP\
		Linux:	/TOKEN_AGENT37/**FTP**/

3.2.5 Token Agent monitors CDX Tokens associated with all user workstations and uses the following directory structures:

a. **Workstation** Windows: C:\TOKEN_AGENT\<servicename>\
Linux: /TOKEN_AGENT/<servicename>/

3.3 Confidentiality and Integrity Scoring – Four Scoring Periods Per Day

3.3.1 Blue Cell shall be notified of one score for every six hour period to reflect the effectiveness of their defenses against Confidentiality and Integrity (C&I) attacks. C&I scoring is assessed in finer increments, but is reported to the public scoring system less often so as to not artificially tip off network defenders to malicious activity. Scoring notification periods shall be as follows:

a. 10:00 to 16:00

b. 16:00 to 22:00

c. 22:00 to 04:00

d. 04:00 to 10:00

3.3.2 Confidentiality and integrity scoring shall begin on day two of the exercise at 10:00.

3.4 Scoring Period Confidentiality and Integrity Score Calculation

3.4.1 Each period's confidentiality and integrity score shall be stated as a percentage value within the range of: 0% to 100%.

3.4.2 The Token Agent determines whether any confidentiality or integrity compromises have been detected; i.e., has Red Cell turned in a CDX Token or has a CDX Token been altered.

3.4.3 The scoring system keeps a tally of the number of unique compromises in the scoring period per instance of the Token Agent Client; therefore, Red Cell cannot drive the score down by repeatedly taking the same action in the same period. For example:

If the Token Agent Client reports that the FTP server, for example, has multiple reports of a confidentiality breach in a scoring period, it is treated as one unique compromise.

3.4.4 For each scoring period, the scoring system sorts these compromises in two groupings:

a. Required Services

b. User Workstations

3.4.5 Confidentiality and integrity period scores are calculated using a weighted average:

Confidentiality and Integrity Score = (Required Services Score *** .70**)
+ (User Workstation Score *** .30**)

3.4.6 For each unique confidentiality and integrity compromise, the score for that period is reduced (weighted by the server and workstation formula above). Each exploit is its own breach. The following rules are used to determine the period score:

a. Each period starts with a score of 100%

b. Each Confidentiality breach = 25% deduction

c. Each Integrity breach = 50% deduction

d. Maximum deduction = 100% per period

3.4.7 Confidentiality and integrity scoring period examples:

a.	0 required services confidentiality breaches	100%	*	.70	=	70%
	1 user workstation confidentiality breach	75%	*	.30	=	23%
		Period Score				93%
b.	1 required service confidentiality breach	75%	*	.70	=	53%
	0 user workstation confidentiality breaches	100%	*	.30	=	30%
		Period Score				83%
c.	2 required services confidentiality breaches	50%	*	.70	=	35%
	1 user workstation integrity breach	50%	*	.30	=	15%
		Period Score				50%
d.	2 required services confidentiality breaches	50%	*	.70	=	35%
	2 user workstation confidentiality breaches	50%	*	.30	=	15%
		Period Score				50%
e.	1 required service integrity breach	50%	*	.70	=	35%
	1 user workstation confidentiality breach	75%	*	.30	=	23%
		Period Score				58%

3.4.8 A scoring scenario that demonstrates unique/non-unique compromises:

Service-1 confidentiality compromised at time 1100 [unique]
Service-1 confidentiality compromised (possibly in a different manner) at 1200
Service-2 confidentiality compromised at 1300 [unique]
Service-3 confidentiality compromised at 1400 [unique]
Workstation-1 confidentiality compromised at 1200 [unique]
Workstation-1 confidentiality compromised (possibly in a different manner) at 1300
Workstation-1 confidentiality compromised (possibly in a different manner) at 1400
Workstation-1 integrity compromised at 1230 [unique]

Total unique service integrity compromises:	0	
Total unique service confidentiality compromises:	3 ==> -75%	
Total unique workstation integrity compromises:	1 ==> -50%	
Total unique workstation confidentiality compromises:	1 ==> -25%	
3 required services integrity breaches	25% * 0.70 =	17.5%
1/1 user workstation confidentiality/integrity breaches	25% * 0.30 =	7.5%
Period Score for 1000-1600		25.0%

3.5 Token Agent Client Disruptions and VM Rollbacks

3.5.1 The Token Agent Client constantly validates the integrity of its associated CDX Tokens. It also refreshes these tokens on a routine basis. Any changes to CDX Tokens, even from administrative actions, such as deleting a token directory or file, is treated as a loss of information integrity and shall result in the reduction of score equal to any other integrity compromise on that machine.

3.5.2 Rolling back a VM hosting Token Agent Client is detected by the Token Agent Server as a VM snapshot reversion and results in a score penalty equal to 1 hour of availability points for the reverted VM (workstation or service). Restoring the token files or directories from an old backup will also be detected as a roll-back, resulting in the same score penalty

3.6 Overall Confidentiality and Integrity Scoring

3.6.1 Each school's cumulative confidentiality and integrity score shall be a straight average of the scores from all of the scoring periods.

3.7 Challenge Modules

3.7.1 For each Challenge Module, there are varying degrees of difficulty. The Challenge Modules are measured with a "Capture the Flag" type scoring system. Each module has seven flags based on completions of specific tasks in increasing difficulty. Flags are scored as follows:

- Flag 1 – 11% -- Easy
- Flag 2 – 13%
- Flag 3 – 14%
- Flag 4 – 15%
- Flag 5 – 15%
- Flag 6 – 16%
- Flag 7 – 16% -- Difficult
- **Total – 100%**

3.7.2 Scoring is calculated and provided to the teams at the conclusion of the exercise.

4.0 Role of White Cell in Scoring

4.1 White Cell and Scoring

4.1.1 The CDX White Cell scoring objective is to oversee the exercise so that scoring is evenly and fairly applied to all schools. Other exercise elements may point out apparent failures of information confidentiality, integrity or availability to White Cell, but have no independent authority to score the exercise. Headquarters White Cell has sole authority to apply scoring rules and assign bonuses or penalties (adjustments).

4.1.2 White Cell shall enforce all written exercise directives, specifications, orders, tasking and instructions. Failure to follow stated rules shall result in negative adjustments to a Blue Team's score. Although White Cell shall make every attempt to base its rulings on data collected by the scoring system and/or direct observations by White Cell personnel deployed at the various schools, White Cell may make subjective rulings.

4.1.3 The CDX 2017 scoring model does not set aside a certain number of points for White Cell Compliance. As the competition progresses, White Cell shall determine if participants are fully complying with the items listed in Section 4.1.2 of this Scoring Specifications document and make adjustments to Blue Cell scores as needed. All White Cell Compliance scoring entries shall include a numeric value (two decimal places) and a description field that shall be visible to all participants. Adjustments are applied to each school's individual score, and efforts shall be made to keep the live scoring information as up-to-date as practical.

4.2 Scoring Disputes

4.2.1 Blue Cells may, in writing, dispute scores by emailing their dispute to the CDX HQ White Cell, copying, at a minimum, their local White Cell individual. The dispute request email should be as specific as possible – if the request is not specific, it will be returned to the Blue Cell for clarification.

4.2.2 White Cell may consult any relevant party to discuss a dispute. All dispute requests and relevant correspondence, including the final decision and related scoring actions shall be logged to a location visible to all Blue Cells.

4.2.3 If a Blue Cell is not satisfied with the White Cell's dispute decision, the Blue Cell may appeal the decision to the CDX Technical Lead who shall log all appeal requests and relevant correspondence, including the final decision and related scoring actions to a location visible to all Blue Cells. The decision of the CDX Technical Lead shall be final.

4.2.4 Scoring challenges that require research must be submitted by 1530 daily if the issue is to be discussed at the 1600 daily hot wash.

Appendix B Network Specifications

OVERVIEW

Appendix B, Network Specifications clarifies rules and guidelines for the design of Blue Cell networks during the build phase of the Cyber Defense Exercise (CDX).

1.0 BLUENET Required Services

1.0.1 Section 1.0 specifies the required services that must be available on each BLUENET. These services must be available to both local users, including White Cell and Gray Cell users, and external users.

1.0.2 Blue Cells may configure these services on any number of physical or virtual machines. Blue Cells are encouraged to consider the tradeoff associated with having multiple services running on one computer as opposed to spreading these services over multiple computers.

1.0.3 Throughout the exercise, the availability scoring system (RubberNeck) tests for the required services being available from a wide variety of locations:

a. BLUENET user workstations

b. BLUENET user workstations at other Blue Cells

c. CDX Headquarters

d. SIMNET

1.0.4 Blue Cells may block traffic in CDX 2017, but such blocking might seriously affect availability scoring due to the potential of blocking RubberNeck traffic.

1.0.5 For required services where authentication is necessary, RubberNeck requires a user ID and password. For each required services, the following credentials shall be used:

User ID	**rubberneck**
Password	**Rubb3r#N3ck**

1.0.6 Failure to use this authentication information shall result in a loss of availability scoring because RubberNeck will not be able to verify that password protected services are available.

1.1 Domain Name Service

1.1.1 Required port usage: UDP 53

1.1.2 Each Blue Cell team must provide name resolution for all “outward-facing” systems within their network; i.e., those that will be directly accessed by other BLUENET or SIMNET sites.

1.1.3 Domain names for the various BLUENET subnets shall be:

Organization	Domain Name
HQ	hq.bluenet
RMC	rmc.bluenet
RMC-U	rmcu.bluenet
USCGA	uscga.bluenet

Organization	Domain Name
USMA	usma.bluenet
USMMA	usmma.bluenet
USNA	usna.bluenet

1.1.4 Some of the required services described elsewhere in this document must be associated with specific domain names:

Server	Domain Name
Domain Name Service (DNS)	ns1.xxxx.bluenet ns2.xxxx.bluenet (and so on)
Email (SMTP) service	smtp.xxxx.bluenet
Email (IMAP) service	imap.xxxx.bluenet
FTP service	ftp.xxxx.bluenet
IPv6 Web service	www6.xxxx.bluenet
Web service	www.xxxx.bluenet
Gray Cell Remote Admin	grayadmin.xxxx.bluenet

1.1.5 Blue Cells must place one outward-facing DNS server at IP address 10.1.xx.5. Optionally, Blue Cells may employ a secondary outward facing DNS server by placing it at 10.1.xx.6. The CDX HQ DNS server is set up to forward all requests for a given Blue Cell subnet to that address. This convention shall not be changed for the duration of the exercise.

1.1.6 The IP address for the primary DNS server at HQ is 10.1.10.5 (HQ DNS). Each Blue Cell team should set up its DNS server(s) to forward requests outside the local subnet to the HQ DNS. A secondary DNS server for CDX HQ is placed at 10.1.10.6.

1.1.7 The HQ DNS server *does not accept zone transfers* from any Blue Cell subnet at any time.

1.1.8 The IPv6 Web server must have an appropriate AAAA record on the DNS server.

1.1.9 To facilitate email routing, Blue Cells may configure DNS for reverse lookups.

1.1.10 To facilitate availability scoring from RubberNeck clients and to provide for user access, DNS shall resolve both externally and internally originated domain name requests.

1.1.11 To facilitate availability scoring from RubberNeck clients and to provide for user access, the domain controller at each BLUENET shall be named "**dc1**".

1.1.12 The following network device names must be resolved within each BLUENET:

a. alpha

b. beta

c. delta

d. gamma

e. dc1

f. smtp

g. imap

h. ns1

i. ns2

The following service names must be resolved publicly:

a. www

b. www6

c. ftp

d. imap

e. grayadmin

1.2 Domain Controller supporting LDAP

1.2.1 Required port usage: TCP 389

1.2.2 Each Blue Cell team must create and maintain a domain controller holding a centralized credentials repository for its own BLUENET subnet.

1.2.3 Within each BLUENET, all Windows user workstations, all Linux user workstations, domain controller, the email server, the internal DNS server (if separate from the domain controller) and at least one administrative workstation (Windows or Linux) must authenticate through the domain controller. Any other servers or clients may authenticate through the domain controller, if desired.

a. The administrative users of the administrative workstation(s) shall be able to log on to the workstation(s) using domain credentials and then seamlessly connect to the servers in the domain (i.e., domain controller, email server, DNS server) by using domain credentials and perform various administrative functions. White Cell shall monitor to determine compliance.

1.2.4 Each Blue Cell domain shall be stand-alone and shall not perform replication with the HQ domain controller or with any other Blue Cell's domain controller.

1.3 Network Time Protocol (NTP) Service

1.3.1 Required port usage: UDP 123

1.3.2 Each BLUENET must synchronize time services with the CDX Headquarters' Network Time Server, available at ntp.hq.bluenet.

1.4 Email Service

1.4.1 Required port usage: SMTP TCP 25, IMAP TCP 143

1.4.2 Email shall be used as the primary means of communication throughout CDX 2017 execution. Implementation of email services must meet the following requirements:

a. Each Blue Cell must create the following valid and working email addresses for the unit commander (or duty officer) and the White Cell liaison (acting as Coalition Partner):

Commander (Duty Officer)	CDR@xxxx.bluenet
Coalition Partner	CP@xxxx.bluenet

b. Official correspondence, tasking orders from White Cell HQ, and other exercise messages shall be sent to the above addresses.

c. Unofficial correspondence may also arrive at the above addresses.

d. Blue Cells shall create working email addresses for their own individual members to be used as convenient. White Cell HQ shall not contact individual members directly without notice to the unit commander and the White Cell liaison.

e. All email servers must support the Simple Mail Transfer Protocol (SMTP) when communicating with other Blue Cell enclaves, White Cell HQ or with SIMNET

f. Internet Message Access Protocol (IMAP) must be supported as a public service with connections expected from other BLUENET domains, CDX HQ and SIMNET; IMAP, in effect, supports traveling users.

g. Email must support unencrypted connections to the IMAP service.

h. Email servers must support RubberNeck credentials (see section 2.0.5).

i. The default mailbox for RubberNeck user must be “Inbox”

j. No email connection limits are allowed.

k. Mailboxes must have a capacity of at least 10GB.

l. No “auto-ban” mechanism for connections/failed attempts are allowed.

m. Spam filtering must be disabled.

n.

The message queuing time recommended setting for sent emails is one minute to minimize message failures and to ensure message timeliness.

1.5 File transfer Protocol (FTP) Service

1.5.1 Required port usage: TCP 21 control port + a range of BLUENET chosen data TCP ports

1.5.2 Note: Choosing a small range of data ports may result in connection failures during the exercise. A range of at least 1000 ports is recommended.

1.5.3 The FTP folders shall include at least two primary folders: /private and /public. The /private folder shall be accessible only to local users, to include the local Gray Cell user. The /public folder shall be accessible to local users as well as anonymous users from other Blue Cells, CDX HQ, and SIMNET.

1.5.4 Each Blue Cell must provide an FTP server configured as follows:

a. Must support passive mode

b. Must support Anonymous access

c. Anonymous users must have the following permissions in at least the /public folder and sub-folders

i. Create

ii. Rename

iii. Read

iv. Write

v. Delete

vi. Append

d. Local users must have the following permissions in at least the /private folder, /public folder, and sub-folders:

i. Create

ii. Rename

iii. Read

iv. Write

v. Delete

vi. Append

e. No restriction on file types

f. No maximum number of concurrent users

1.6 Web Server Service

1.6.1 Required port usage: HTTP TCP 80; HTTPS TCP 443

1.6.2 Each Blue Cell team must maintain at least one outward-facing web server. This server must be responsive to HTTP and HTTPS requests from all valid BLUENET and SIMNET addresses. Blue Cells are free to redirect requests from HTTP to HTTPS (or the reverse). What is important is that the web server be able to service the user’s request using both formats.

1.6.3 Each Blue Cell website must include a page or pages, visible to any visitor to the site from anywhere in the BLUENET or SIMNET, linked from the front page of the site, providing the following static information:

a. Organization chart detailing the Blue Cell's command structure

b. Watch bill detailing watch officer schedule

c. Name, rank, position, email address for all local Blue Cell team members

d. A list of all Blue Cell point of contact telephone numbers (e.g., Watch Officers, White Cell, etc.)

e. A means of obtaining public keys for all participants on the local BLUENET subnet. All Blue Cell team members (e.g., Watch Officers, White Cell, and Gray Cell) shall make their public keys available on their local web site.

1.6.4 Each Blue Cell website must provide a dynamic message board or "forum," linked from the front page of the site, meeting the following criteria:

a. The message board must be "threaded," collecting posts into threads or topics for convenient reading.

b. Users must be able to create new threads, post to existing threads, edit or delete their own existing posts, quote text from earlier posts, and define signature blocks that automatically append to their posts.

c. Users must be able to embed hyperlinks and images into their posts, and must be able to use standard HTML markup to format their posts.

d. Users must be able to create personal profiles, to include at least a full name, email address, personal web site URL, and personal description.

e. Users must have the ability to upload and download files to the forums. In particular, users must have the ability to upload "avatar" images that are automatically displayed as part of their own posts.

f. At a minimum, the board must have two sections, titled Customer Support and Public Discussion, in which any BLUENET or SIMNET user may participate. At their own discretion, Blue Cell teams may create additional sections with more limited access.

g. The board may require user registration and password authentication before granting posting access. If so, a new user must be able to register without requiring any action on the part of the Blue Cell team. The user registration process may include automated methods for verifying an applicant's legitimacy (i.e., verification of an email address, a CAPTCHA code, and so on).

h. Users must be able to recover their account passwords if forgotten, without requiring any action on the part of the Blue Cell team.

1.7 IPv6 Web Server Service

1.7.1 Each Blue Cell must configure their BLUENET web servers as dual-stacked machines that respond to both IPv4 and IPv6. The web server(s) must be able to service the user's request using both formats.

1.8 Secure SHell (SSH)

1.8.1 Required port usage: TCP 22

1.8.2 All Linux workstations must respond (full session) to SSH logins from the Gray Cell Relay box~~es~~ using domain credentials.

1.9 Remote Desktop Protocol (RDP)

1.9.1 Required port usage: TCP 3389

1.9.2 All Windows workstations must respond (full session) to RDP logins from the Gray Cell Relay box~~es~~ using domain credentials.

1.9.3 Gray Cell's Relay box must be able to respond (full session) to Gray Cell user RDP logins from the HQ subnet.

2.0 Advanced Message Queuing Protocol (AMQP)

2.1.1 Required port usage: TCP 5672

2.1.2 Gray Cell automated simulation Control. TCP port 5672 must be opened bi-directionally between all local BLUENET user workstations and Gray Cell automation server located at HQ.

2.2 Virtual Network Computing (VNC)

2.2.1 Required port usage: TCP 5901 (NOTE: The VNC server connection on the workstations will be directed to an SSH tunnel. Therefore, VNC traffic will flow between the user workstations and the Gray Cell relay host through this SSH tunnel.)

2.2.2 All Linux workstations must respond (full session) to VNC logins from the Gray Cell Relay boxes using domain credentials.

3.0 User Workstations

3.0.1 White Cell provides user workstation images to each Blue Cell in the course of exercise setup. For each BLUENET, user workstations shall share a common subnet to be used by White Cell and Gray Cell personnel. From STARTEX to ENDEX:

a. User workstations shall not be available to Blue Cell in any fashion while White Cell or Gray Cell is using them: Blue Cell shall not use these workstations, log into them locally or remotely, monitor or execute processes on them, or monitor White or Gray Cell workstation activity through physical or virtual means.

b. During regular duty hours, if Blue Cell wishes to perform maintenance on a user workstation, Blue Cell must gain permission of the local White Cell representative who will take into consideration the mission needs of the Gray Cell user prior to allowing for Blue Cell access. Blue Cell may perform user workstation maintenance without White Cell permission if the Gray Cell has left for the day.

c. Participants *must* use the workstation images provided for the exercise. Removal and replacement of the images with *clean* images is strictly prohibited and will result in scoring penalties to be determined by the White Cell.

3.0.2 Two Windows user workstations are provided in the form of virtual machine images about one month before STARTEX. They are based on Windows 7 (Service Pack 1). Both workstations may be tainted with pre-positioned configuration errors and malware. Blue Cell is encouraged to closely examine these workstations and remove any suspicious files and change security settings – keeping in mind the users' operational needs and White Cell's approved software list (published separately and available on the CDX HQ web site). Blue Cell shall advise White Cell of each file removed or modified. To facilitate scoring, these Windows workstations shall be named:

a. **delta**

b. **gamma**

**** Note – Both DNS *and* Machine (Host) Name must resolve as their represented names: "delta" / "gamma". Host names for these workstations shall not be changed.**

3.0.3 Two Linux user workstations are provided in the form of virtual machine images about one month before STARTEX. They are based on RedHat Centos or Ubuntu. Both workstations may be tainted with pre-positioned configurations errors and malware. Blue Cell is encouraged to closely examine these workstations and remove any suspicious files and change security settings – keeping in mind the users' operational needs and White Cell's approved software list (published separately and available on the CDX HQ web site). Blue Cell shall advise White Cell of each file removed or modified. To facilitate scoring, these Linux workstations shall be named:

a. alpha

b. beta

**** Note – Both DNS *and* Machine (Host) Name must resolve as their represented names: "alpha" / "beta." Host names for these workstations shall not be changed.**

3.0.4 The user workstations shall simulate systems controlled by each Blue Cell, but not necessarily properly configured or maintained by those units. White Cell and Gray Cell shall use the user workstations to generate traffic on the exercise network, evaluate service availability, and simulate the behavior of normal users.

3.0.5 The user workstations come preloaded with software from the Approved Software List – which shall remain installed from STARTEX to ENDEX. Software may be removed (or added) during a maintenance period but, no software that is on the White Cell Approved Software List shall be permanently removed (or added) from the user workstations without explicit White Cell approval.

3.0.6 From STARTEX to ENDEX, Blue Cell shall not add, in any fashion, any software, task, process, or any other component on the user workstations except for those specifically provided by White Cell and designated in a tasking order during the course of the exercise. If a workstation is taken off line for maintenance, diagnostic software may be run on the system. Before bringing the machine back online, this diagnostic software must be removed.

3.0.7 Note that user workstations *will not* have up-to-date patches at STARTEX. Blue Cell teams *may update them* using provided patches located on HQS update servers and in accordance with White Cell advisories and instructions. Necessary patching instruction are provided by White Cell during the course of the exercise.

3.0.8 If Blue Cell believes one or more files are of suspicious origin, Blue Cell teams may *replace* specific files already installed on any user workstation with a known-good copy of the same software (available from White Cell at the CDX HQ web site). The new files must be from exactly the same software version and patch level as the files being replaced. Files that are not available from the White Cell at the CDX HQ web site shall not be introduced to the user workstations without approval from White Cell.

3.0.9 Any additional workstations built by Blue Cell personnel are considered administrative workstations, and are be subject to the provisions of this section (Section 3.0). The additional workstations are used by Blue Cell personnel, are not normally required to support White Cell or Gray Cell activities, and are patched at Blue Cell discretion.

3.0.10 Blue Cell may configure user workstations to operate in a virtual machine (VM) environment; however, White Cell and Gray Cell users are very active and require continuous access to the network. Points are lost if these workstations are not simultaneously available.

3.0.11 For maintenance reasons, Blue Cells may find it convenient to rollback workstation VMs to a previous versions. The scoring system will survive VM rollbacks but points shall be lost for this action due to the resetting of the configuration files and version control features that are on each user workstation – giving the appearance that the Blue Cell has tampered with the scoring system. And, rolling back might interfere with White or Gray Cell local file systems – resulting in further loss of points.

3.0.12 Any software preloaded on user workstations (as provided by White Cell) may be reconfigured or implemented by Blue Cell.

4.0 Traffic Generator / Scoring System

4.0.1 Each user workstation shall run a White Cell-provided traffic generator (RubberNeck) that is used for checking service availability and plays a significant role in scoring. Failure to keep these user workstations running will negatively impact scoring.

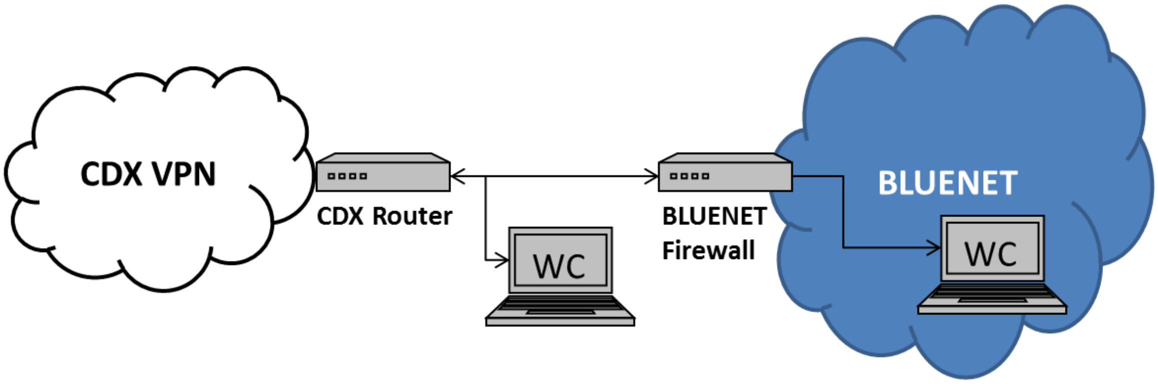
4.0.2 RubberNeck checks the availability of all user workstations on the local BLUENET by accessing remote administration functionality. Windows workstations must have RDP configured. Linux workstations must have SSH configured. Note: this functionality only needs to be accessible within the BLUENET; RubberNeck does not perform this validation from external locations (RDP on the user workstations still must be accessible to Gray Cell users remotely from CDX HQ).

RubberNeck also checks the availability of all services across the exercise network, including both public services from other BLUENETs, and local services within the local BLUENET.

4.0.3 Automated scoring also takes into account elements of information confidentiality and integrity. Scoring software (Token Agent) distributes and validates unique “Tokens” that shall be loaded on (ALL NODES) to BLUENET servers. Details, including the location of token directories and the operation of Token Agent, are provided in the CDX *Scoring Specifications*.

5.0 White Cell Connectivity on Each BLUENET

5.0.1 Each BLUENET implementing the locally physical infrastructure option for CDX 2017 shall maintain two dedicated connections into its local network for potential use by the local White Cell liaison. Each BLUENET implementing the remote virtual infrastructure shall also permit connections to its virtual network by White Cell, and White Cell shall establish two virtual hosts at any point within the BLUENET. These two access points and their IP addresses shall be off limits to the Red Cell.



5.0.2 The first network connection is for network diagnostic purposes only and shall be placed within the inner VPN interface, but outside of the outermost Blue Cell firewall.

5.0.3 The second network connection is for White Cell email and other operational uses and shall be placed inside the Blue Cell’s interior network, preferably in the same subnet as the Gray Cell user workstations, with full access to all BLUENET user services.

5.0.4 These two access points and their IP addresses shall be provided to the White Cell and shall be used solely for White Cell testing, diagnostics, and messaging purposes – they shall be off limits to the Red Cell.

6.0 Public Key Infrastructure

6.0.1 Blue Cells may use Public Key Infrastructure (PKI) to digitally sign and encrypt sensitive data. To facilitate Blue Cells’ PKI use, White Cell shall establish a root Certificate Authority within the CDX HQ domain.

6.0.2 White Cell shall create valid certificates for all required accounts. Blue Cells shall install the certificates in the appropriate manner.

7.0 Network Performance Standards

7.0.1 Each BLUENET shall maintain a network connection to the CDX Network with minimum bandwidth of 1 megabit per second and with an average latency of 200 milliseconds or less. Failure to maintain these standards negatively affects Blue Cell scores.

7.0.2 CDX HQ shall monitor network performance throughout the exercise, while actively balancing the allowable bandwidth between each Blue Cell and CDX HQ to allow for uniform throughput by each Blue Cell participant.

7.0.3 Blue Cells may block network traffic, but must remember not to block traffic associated with scoring.

7.0.4 Blue Cells shall not perform any traffic shaping – neither inbound nor outbound. This includes temporarily blocking or delaying inbound connections (otherwise known as tarpitting).

Appendix C IA Migrations

NSA’s Top 10 Information Assurance Mitigation Strategies

Fundamental aspects of network security involve protection, detection and response measures that can be grouped into four mitigation goal areas. These four mitigation goal areas target critical steps in the intrusion life cycle — creating a technical layered defense approach that supports the ability to “fight through” a contested cyber environment:

- Device Integrity—maintaining and measuring device health/integrity. Devices often represent the attack surface area or the persistent living-space for the advanced persistent threat (APT).
- Damage Containment—when intrusions occur, limiting losses of information, systems, and mission capabilities.
- Defense of Accounts—protecting credentials from misuse and enabling trusted authentication and access.
- Secure and Available Transport—maintaining the privacy and reliability of data communications.

These goal areas will support current and future cyber defense efforts, helping to set priorities, and contributing to the desired end-state of denying adversaries the ability to operate on our networks and impact our missions. Efforts that can be implemented now are listed below as NSA’s Top Mitigations. By blocking critical points in the attack life cycle, these mitigations are effective against entire classes of attacks, including new unknown variants.

1.1 Application Whitelisting

Application Whitelisting is a proactive security technique that allows a limited set of approved programs to run, while all other programs and most malware are blocked from running by default. Application Whitelisting enables only the administrators, not the users, to decide which programs are allowed to run.

1.2 Control Administrative Privileges

Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are restricted from normal users. Network owners should only grant Administrator privileges when absolutely necessary and should take steps to ensure Administrator accounts are not exposed to the internet and other sources of increased risk. More robust protections can be achieved through the use of two-factor authentications for administrators and other privileged accounts.

1.3 Limit Workstation-to-Workstation Communication

Pass-the-Hash (PtH) is a hacking technique that allows an attacker to authenticate to a remote system by using the underlying hash of a user's password rather than having to know the actual password itself. Hackers generally use hashes from the current machine to springboard to other machines, grabbing higher privileged credentials as they progress. A range of security measures are required to fully mitigate all the facets of Pass-the-Hash. One scalable and highly effective mitigation involves limiting workstation-to-workstation communication, thereby thwarting an attacker's ability to leverage PtH to move laterally within the network.

1.4 Use Anti-Virus File Reputation Services

Most of today's host security products augment their product's core host controls with intelligence from cloud-hosted threat databases. In order to gain the most complete threat picture, organizations need to leverage these threat intelligence clouds.

1.5 Enable Anti-Exploitation Features

Many operating systems and applications have advanced anti-exploitation and sandboxing features that should be harnessed to defend against common attacks. For example, in Windows, the Enhanced Mitigation Experience Toolkit (EMET) is a host-based application that hooks into processes and watches for common memory exploitation techniques, such as buffer overflow attacks. When EMET detects an exploit attempt, it promptly kills the targeted process, logs the attempt, and notifies the user that it has shut down the application. EMET offers fundamental protection against common classes of exploitation used as building blocks of zero day attacks.

1.6 Implement Host Intrusion Prevention System (HIPS) Rules

Standard signature based host defenses are overwhelmed by exploit kits that continually morph attack components. HIPS technology focuses on threat behaviors and can better scale to entire sets of intrusion activities. For an enterprise with a well configured and managed network, HIPS can be tuned to learn and allow normal network functionality while flagging anomalies characteristic of intrusions.

1.7 Set a Secure Baseline Configuration

Perhaps the most scalable way to control an enterprise's attack surface is through secure host baselines. This includes generation of standard images which provide approved and secured application and operating system configurations with layered security containing best practice mitigation strategies to counter cyber threats.

1.8 Use Web Domain Name System (DNS) Reputation Services

Various commercial services offer feeds rating the trustworthiness of web domains. Enterprises can protect their hosts by screening web accesses against such services and redirecting dangerous web requests to a warning page. Inspection can be implemented at either the web proxy or browser level.

1.9 Take Advantage of Software Improvements

Operating systems and application software routinely have security upgrades through new versions and intermediate patches. Apply these updates in a timely manner to reduce vulnerability exposure and maximize software reliability and protections.

1.10 Segregate Networks and Functions

Plan for the possibility of a successful intrusion and design the network architecture and management procedures to separate segments based on role and functionality. Closely monitor the interactions between the sections, so that a compromise of one part can be detected and does not directly lead to the compromise of others.

Disclaimer of Endorsement

The information and opinions contained in this document are provided “as is” and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.