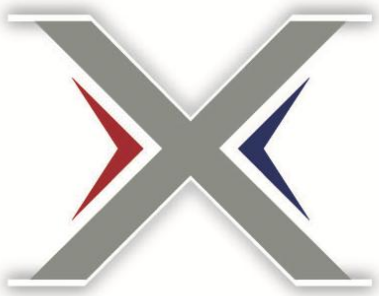

CYBER DEFENSE EXERCISE

Exercise Directive 2016

Version 3.0

Purpose of this Document

This directive serves as a general guide for all participants in Cyber Defense Exercise 2016 (CDX 2016).

Document Revision History

Version	Change Description	Change Owner	Date
1.0	FIRST DRAFT	James Titcomb	29 October 2015
2.0	SECOND DRAFT	James Titcomb	21 January 2016
3.0	FINAL	James Titcomb	25 February 2016

1.0 Cyber Defense Exercise - 2016

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

1.1.1 Core Module with Infrastructure Virtualization Option

- Locally physical infrastructure, OR
- Remotely administered virtual infrastructure

1.1.2 Multiple Challenge Modules

Undergraduate (Competing Teams)

- Reverse Engineering Malware
- Host / Network Forensics
- Gov / Mil Offensive – Capture The Flag (CTF)

Graduate (Non-Competing Teams)

- Reverse Engineering Malware
- Host / Network Forensics
- Gov / Mil Offensive – Capture The Flag (CTF)
- UAV

2.0 CDX 2016 Timeline

EVENT	Projected Dates
Initial Planning Conference (IPC)	**3 Nov 2015**
Final Planning Conference (FPC)	**3 Feb 2016**
VPN Up and Running	**Year-Round**
Virtual Infrastructure available to participating schools	**27 Jan 2016**
Blue Cell - Virtual / Physical Infrastructure Decision	**27 Jan 2016**
Pre-built workstation images delivered to all Blue Cell teams	**14 March 2016**
RubberNeck up for connectivity testing	**14 March 2016**
Finalized Exercise Directive and Network Specification delivered	**14 March 2016**
Service and Final Connectivity Testing (Phones, Internet, Skype, etc…)	**4-11 April 2016**
CDX Kickoff Announcement 1000	**11 Apr 2016**
Red Cell Scanning begins – 1400 hrs EDT	**11 Apr 2016**

CDX 2016	**11-14 Apr 2016**
CDX Daily Hotwash at 1600 hrs EDT	**11-14 Apr 2016**
All services STARTEX at 1400 hrs Eastern Daylight Time (UTC-04:00)	**11 Apr 2016**
Challenge modules assigned to Blue Cells	**21 Mar 2016**
Red Cell attacks start at 0900 hrs EDT	**12 Apr 2016**
Challenge module submissions from Blue Cells due – 1600 hrs EDT	**13 Apr 2016**
Scoring Ends at 1600 hrs EDT	**14 Apr 2016**
Announcement of exercise winner	**Noon, 15 Apr 2016**
Participant Debriefs	**1-2 Weeks Post-CDX**

3.0 CDX Organization

3.1 Blue Cell

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 2016. Each Blue Cell will assign its own organizational components, including the assignment of watch officers who shall be charged with interfacing with Headquarters personnel.

3.1.2 For the core module of CDX 2016, each Blue Cell is required to build and operate its own "BLUENET" network to meet the requirements of this directive and subsequent orders. Successful completion of the exercise will require continued compliance with these rules, often under stressful conditions. For CDX 2016, each student team has an option of implementing their BLUENET either locally or on the remote virtual infrastructure located at CDX HQ. This decision must be confirmed with HQ by the close of business of the Final Planning Conference (FPC) on 3 Feb 2016.

3.1.3 For the Challenge Modules of CDX 2016, each Blue Cell will select the best two of the three available elective challenges to be their main challenges. Each Blue Cell may submit either zero or one response to each of the selected challenges. The challenge event will take place during CDX 2016. Only the first response, per challenge submitted to Parsons by a Blue Cell prior to the end of the challenge event will be graded. Detailed in the Scoring Specification Document, each module will contain (7) flags representing specific and completed levels of difficulty. The number of flags obtained, along with the associated percentage values, will determine the overall score. Should all three challenges be completed

and returned, the two highest scores will be selected. Scoring will be based on a percentage scale from 0% to 100%. Aggregate scores for the challenge modules will not exceed 100%.

3.2 White Cell

3.2.1 The White Cell carries out the role of CDX 2016 Headquarters (HQ). White Cell will monitor compliance with this directive and assess sanctions for noncompliance or other performance issues in each BLUENET. White Cell may issue orders to Blue Cells concerning details of the execution of Operation CDX 2016.

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

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

3.3 Red Cell

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

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

3.4 Gray Cell

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

3.4.2 Members of the Gray Cell will work to simulate legitimate operations as a "user" and/or trusted third party operator. Gray Cell users will act as "trusted insiders" for each BLUENET: simulating user activity inside each Blue Cell user enclave.

This function may be augmented by simulation software that is installed on Blue Cell hosts and monitored by Gray Cell members at HQ.

3.4.3 Gray Cell will remotely access their workstations within each BLUENET from CDX HQ via Remote Desktop Protocol (RDP) or Secure Shell Protocol (SSH) via a relay host. The relay host will be provided by HQ and is off limits to Blue Cells and the Red Cell. Additional configuration specifics for the Gray Cell remote administration relay host are contained in the Network Specification document. Any restrictions or policies that detract from normal Gray Cell operations may result in score deductions.

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

3.4.5 It is important to remember that the Gray Cell is a 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 the BLUENETS.

3.5 Red Cell Rules of Engagement

The following Rules of Engagement are binding on all members of the CDX 2016 Red Cell. Members will be expected to sign a statement acknowledging that they have read and understood these Rules of Engagement.

3.5.1 Definitions

- **Active Attack:** Any Red Cell activity which 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.

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

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

3.5.2 CDX 2016 Red Cell Policy

- 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 to ensure that all Blue Cell teams are exposed to a substantially similar challenge.

- Red Cell members may not attack the Scoring Service (RubberNeck) or the Confidentiality/Integrity Scoring Service (TokenAgent) to include any services, programs, accounts and/or communication paths used by them. Red Cell may alter the actual token files consistent with their intended use, but may not alter any of the other files, directories, etc. associated with TokenAgent. Any Red Cell member identified as doing such will immediately be banned from participating in any CDX activities and asked to leave CDX HQ.

- Red Cell members shall not perform any Denial of Service (DoS) attacks between the hours of 2000 and 0900 the following morning.

- Red Cell members shall not perform any Denial of Service (DoS) attacks that involve packet flooding or resource exhaustion.

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

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

3.6 CDX 2016 Scoring Guidelines

3.6.1 General Principles

3.6.2 Organizers and planners of CDX 2016 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.

3.6.3 However, it is clear that scoring represents valuable feedback to the exercise participants. Reasonable efforts have been made to ensure scoring is easy to understand by the students, provide transparent and meaningful decisions, and where possible, automate scoring adjudications. At the completion of the exercise, the undergraduate Blue Cell with the most points shall be named the winner of CDX 2016, and shall be awarded the NSA Information Assurance Director's Trophy.

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

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

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

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

- **Integrity.** Information should only be modifiable by authorized users. If Red Cell can provide proof that it has **"modify access" or "write access"** to any of this BLUENET information, points shall be deducted from the operators of the compromised BLUENET. Additional points shall be deducted if Red Cell provides proof that **"system" or "root" access has been acquired**.

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

3.6.7 *Scoring Components*

Scoring Overview:

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

3.7 Service Availability

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

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

3.7.3 White Cell shall provide software to each Blue Cell that will generate network traffic and monitor availability. Copies of the software package, named RubberNeck, shall be installed on workstations in each BLUENET, at White Cell locations and at multiple locations on SIMNET.

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

3.7.5 To maximize availability points, a Blue Cell should be accessible from across the CDX 2016 network. In an effort to defend against malicious traffic, Blue Cells are free to block traffic from any location. However, by doing so, they may be

blocking an instance of RubberNeck and thus reducing their opportunity to collect points.

3.8 Information Confidentiality

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

3.8.2 Throughout the exercise, each Blue Cell will be automatically provided with a set of tokens that will represent confidential information. These tokens shall be loaded to specific directories on each host associated with each of the required services and on each user workstation. Each token will be unique and cryptographically signed. Failure to maintain tokens on each of the required services and user workstations will result in score deductions. Some services are sometimes configured as a system of hosts that separate processing components. The confidential token shall be placed on each host(s) that is required for the service so that 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 discovered and found not to have the TokenAgent 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.**

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

3.9 Information Integrity

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

3.10 Compliance

3.10.1 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 an insufficient response to a request for information shall result in a loss of points.**

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

3.10.3 White Cell shall ensure Gray Cell is granted access to and use of the designated Gray Cell workstations. Gray Cell must be allowed to conduct those activities consistent with behaviors of a traditional network user (e.g., email, web browsing, access to shares). **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.**

Unrealistic policies include, but are not limited to:

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

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

The Gray Cell is required to be able to:

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

- Create and access files on local file system

4.0 CDX Network Architecture

4.1 Exercise VPN Configuration

4.1.1 The Cyber Defense Exercise Network (CDXN) will consist 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 Each school shall be presented an option of infrastructure on which to perform the CDX 2016 core module. Each school shall choose one option at the Initial Planning Conference, and will build their BLUENET within that infrastructure. The first option is the traditional method of building a physically local BLUENET. The second option is a virtual environment hosted physically at HQ and remotely administered from each school's physical location. This Directive shall be interpreted to apply equivalently to both infrastructure options unless stated otherwise.

4.1.3 Physical sites comprising the CDX 2016 network will be connected over the public Internet. Exercise traffic must be completely insulated from non-exercise systems, so the physical sites will interact with one another solely by way of a Virtual Private Network (VPN).

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

4.1.5 Any computing device, either physical or virtual, that connects to or touches traffic from the CDX network by either VPN technology (DMVPN or OpenVPN) or as part of a BLUENET enclave, 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, FireEye, or other products may not be lent to individual participants or procured, 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 CDX 2016 network will be a Class A private network (10.0.0.0/8). However, actively used IPv4 addresses within the CDX 2016 network will be restricted to two Class B networks:

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

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

Cell	IPv4	IPv6
Exercise Headquarters	10.1.10.0/24	fda3:1726:8838::/48
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
USCC (virtual infrastructure)	10.1.150.0/24	fd1d:46d1:290a::/48
Test	10.1.120.0/24	fd5e:4d21:4cb6::/48
Scoring Baseline	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, 10.1.190.0/24, 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 will simulate a set of local networks operated by a Blue Cell within its Area of Responsibility (AOR). BLUENET subnets will be designed and built by Blue Cell teams, within constraints imposed by the Network Specification. During the active phase, Blue Cells will use BLUENET to carry out exercise activities, while also defending BLUENET systems from hostile attack.

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

4.4 SIMNET

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

4.4.2 The SIMNET DNS hierarchy will be required to resolve all names within SIMNET, and will receive all unresolved requests from the BLUENET DNS. SIMNET DNS will be considered the final authority (the "root server") for all exercise-related traffic. Domain names within SIMNET may fall within any top-level domain. SIMNET DNS traffic will 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 shall be responsible for designing and building a BLUENET network that complies with a uniform set of requirements listed in this document. The design of the network is completely up to each Blue Cell--what's important is that the design supports all of the required network services and that the network is ready to be put into service at the start of the exercise. After that point, it will be important that the network can be effectively defended.

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

- Domain Name Service (DNS)
- Centralized credentials repository (for example, Active Directory)
- Network Time Protocol
- E-Mail
  - SMTP
  - IMAP
- FTP
  - With anonymous interface

- Web Server
  - With Web Forum functionality
  - Supporting IPv4 and IPv6
- User Workstations Remote Access (within local network)
  - SSH for Linux Workstations, and
  - RDP for Windows Workstations
  - Gray Cell Remote Access Relay

5.1.3 Standard service ports must be used:

- HTTP TCP 80
- HTTPS TCP 443
- SSH TCP 22
- RDP TCP 3389
- SMTP TCP 25
- IMAP TCP 143
- FTP TCP 21
- AMQP TCP 5672 (Gray Cell user simulation control)
- LDAP TCP 389
- NTP UDP 123
- DNS UDP 53

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

6.0 Hours of Operation

6.1 Regular Duty Hours

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

they shall not perform any function or keyboard activity (including logging in) on any BLUENET system prior to 0900 EDT. 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 will serve as the initial point of contact for any official communications while on watch. It is expected that the watch officer will be physically present in the Blue Cell facility throughout the watch. The scheduling and rotation of watch officers is left to Blue Cell discretion.

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

6.2 Off-Duty Hours

6.2.2 Off-duty hours are defined as 2200-0900 EDT each day. Blue Cell teams must stand down and vacate their physical facilities, leaving all network systems fully-operational and connected to the CDX 2016 network. Any White Cell and Gray Cell personnel deployed to a Blue Cell will also stand down and vacate the facility. Red Cell may be active at any time, even in off-duty hours. Scaled down availability scoring shall be performed during off-duty hours.

7.0 Additional Requirements

7.1 Java Run Time Environment (JRE)

- JRE version 1.6 or higher is required on any system (server, workstation, etc…) for the Token Agent service to run.

7.2 Network Monitoring

- Communications traffic on the CDX 2016 network will be subject to monitoring. Participating teams shall be required to sign “consent to monitoring” agreements.

7.3 Role of Faculty

- The involvement of faculty and staff will be 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 that are 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

- 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 HQs, any unauthorized offensive action by any member of a Blue Cell team will cause a penalty of up to 50% total points awarded during the exercise, per violation, as determined by the White Cell.**

8.0 Challenge Module Descriptions

- **Reverse Engineering (RE) / Malware Analysis**
  - Learning Objectives
    - Analyze via static and dynamic methods potentially malicious code
    - Determine function of malware
    - Determine ways to mitigate malware based of analysis of it
  - Activity
    - A scenario requiring malware analysis and reverse engineer of executables to achieve defined objectives, with points given for each successful step accomplished.
  - Deliverables
    - Answers to the questions posed for the Reverse Engineering (RE) / Malware Analysis challenge
    - Provide Easy, Medium, Difficult areas of focus
  - Assessment
    - Weighted score on the challenges
  - Completion Time
    - Module is due 56 hours from the time of opening, but no later than 1600, 13 April 2016

- **Host / Network Forensics**
  - Learning Objectives
    - Determine what network and host activity is malicious
    - Determine critical factors (e.g., time, origin, target, purpose, etc.) associated with malicious network and host activity
  - Activity
    - A scenario requiring network and host forensics success to achieve defined objectives, with points given for each successful step accomplished
  - Deliverables
    - Answers to the questions posed for the Network / Host Forensics challenge
    - Provide Easy, Medium, Difficult areas of focus
  - Assessment
    - Weighted score on the challenges
  - Completion Time
    - Module is due 56 hours from the time of opening, but no later than 1600, 13 April 2016

- **<u>Government / Military Offensive - Capture the Flag (CTF)</u>**
  - Learning Objectives
    - Utilizing an adversarial mindset, determine how to overcome various system defenses to obtain the defined objectives
  - Activity
    - A scenario requiring hacking various targets to achieve defined objectives, with points given for each successful step accomplished
  - Deliverables
    - Answers to the questions posed for the Hacking / CTF challenge
    - Provide Easy, Medium, Difficult areas of focus
  - Assessment
    - Weighted score on the challenges
  - Completion Time
    - Module is due 56 hours from the time of opening, but no later than 1600, 13 April 2016

- **<u>UAV (Graduate / Non-Competing Teams)</u>**
  - Learning Objectives
    - How to develop secure communications for military based platform that will be attacked by an unknown adversary
    - How to hack and take control of an Unmanned Aerial Vehicle (UAV)
  - Activity
    - Secure communications between Teams, BLUENET, and UAV residing on Simulated Internet (SIMNET)
    - Perform missions with secure UAV
    - Attack adversarial UAVs that enter allied airspace
  - Deliverables
    - Answers to the questions posed for the UAV Hacking challenge
    - Take control of adversarial UAVs
    - Prevent adversarial hacking of schools UAVs
    - Provide Easy, Medium, Difficult areas of focus
  - Assessment
    - Weighted score on the challenges
  - Completion Time
    - Module will be executed during the Core Exercise (11-14 April 2016)

9.0 IAD Top Ten Mitigations

9.3 CDX Leadership is dedicated to adhering to most of the IAD / IA mitigation strategies to make CDX a realistic and educational experience. Refer to:

- Web: https://www.iad.gov/iad/library/ia-guidance/security-tips/iad-top-10-information-assurance-mitigation-strategies.cfm
- Attached Doc: IAD-Top-10-IA Mitigation Strategies.PDF