CYBER
DEFENSE
EXERCISE

Scoring Specification 2016

Version 3.0

Purpose of this Document

This specification serves as a guide for scoring in Cyber Defense Exercise 2016 (CDX 2016).

Document Revision History

Version	Change Description	Change Owner	Date
1.0	FIRST DRAFT	Jim Titcomb	29 Oct 2015
2.0	SECOND DRAFT	Jim Titcomb	21 Jan 2016
3.0	FINAL	Jim Titcomb	12 Feb 2016

1.0 CDX 2016 Scoring Overview

1.0.1 The *CDX 2016 Directive* addresses the general principles surrounding scoring. The *CDX 2016 Network Specification* provides details on key network elements that will be evaluated during the exercise by the various scoring processes. This document provides more specifics on the various components of the scoring processes. And, details are given regarding the calculations that shall be used to determine each school's score.

1.1 Scoring Structure

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

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

- 35% - Required Services Availability, weighted by:
  - ▪ 80% - On-Duty hours
  - ▪ 20% - Off-Duty hours
- 35% - Information Confidentiality & Integrity, weighted by:
  - ▪ 70% Required Services Servers
  - ▪ 30% User Workstations
- 10% - Gray Cell usability
- 20% - Challenge Modules, weighted by:
  - o 50% Challenge Elective #1
  - o 50% Challenge Elective #2
  - o The elective #1 and #2 refer to the top two scoring challenges from that school
- White Cell Adjustments at the discretion of White Cell/CC at HQ
  - o Adjustments may be either positive or negative
  - o Adjustments are applied to each school's total score

1.1.3 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 2016. It has the following main components:

- 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.
- 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.
- RubberNeck Local Server – An optional application that is intended to run on each BLUENET; it receives a copy of all of the information that is being 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 will change 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 – both local and all of the remote BLUENETS. It also evaluates the availability of the other user workstations on its BLUENET.

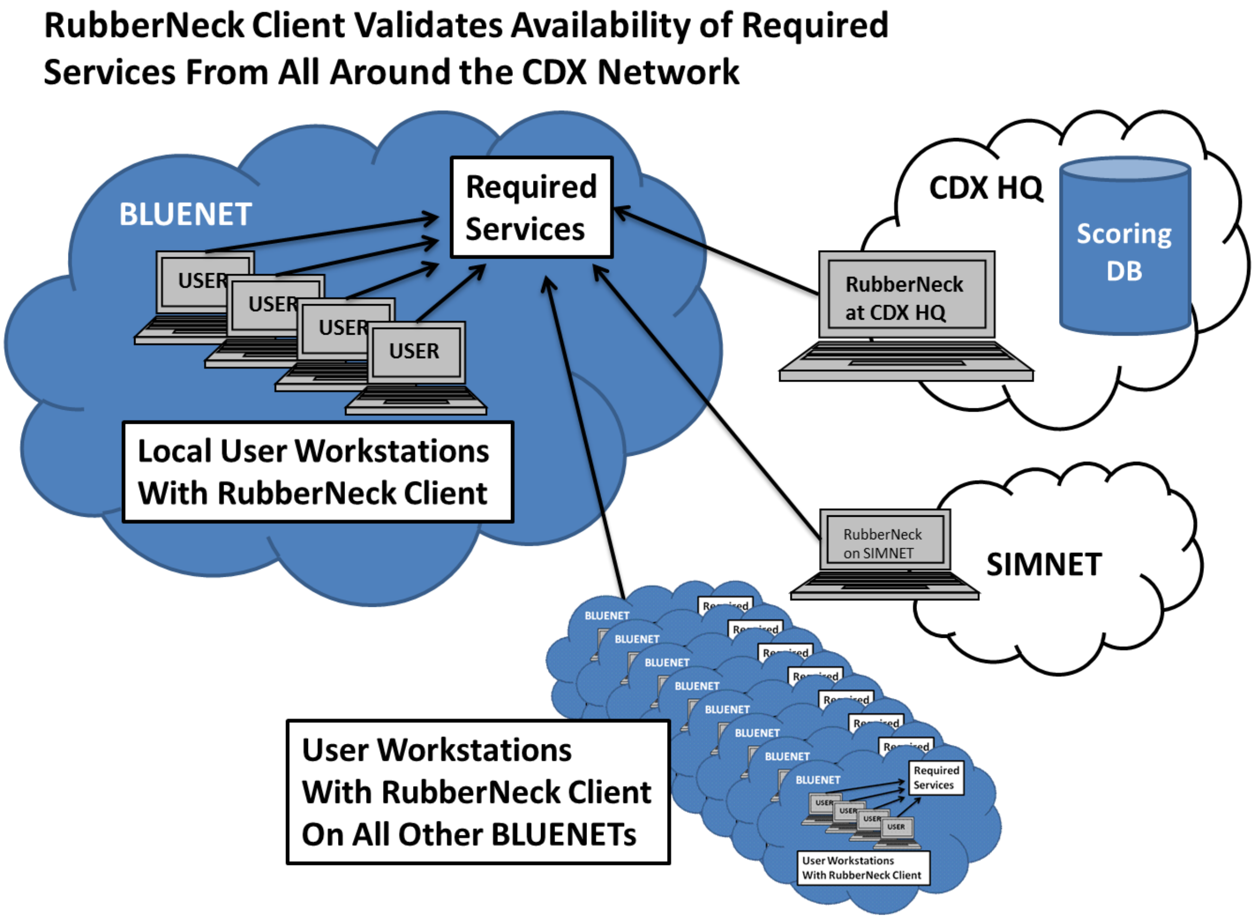
RubberNeck Client Validates Availability of Required Services From All Around the CDX Network
BLUENET
Required Services
USER
USER
USER
USER
Local User Workstations With RubberNeck Client
CDX HQ
Scoring DB
RubberNeck at CDX HQ
RubberNeck on SIMNET
SIMNET
BLUENET
Required
Required Services
USER
User Workstations With RubberNeck Client
User Workstations With RubberNeck Client On All Other BLUENETs

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 perform its validation of availability. The CDX 2016 Network Specification provides details on the specific user ID and password requirements for RubberNeck and any password protected services.

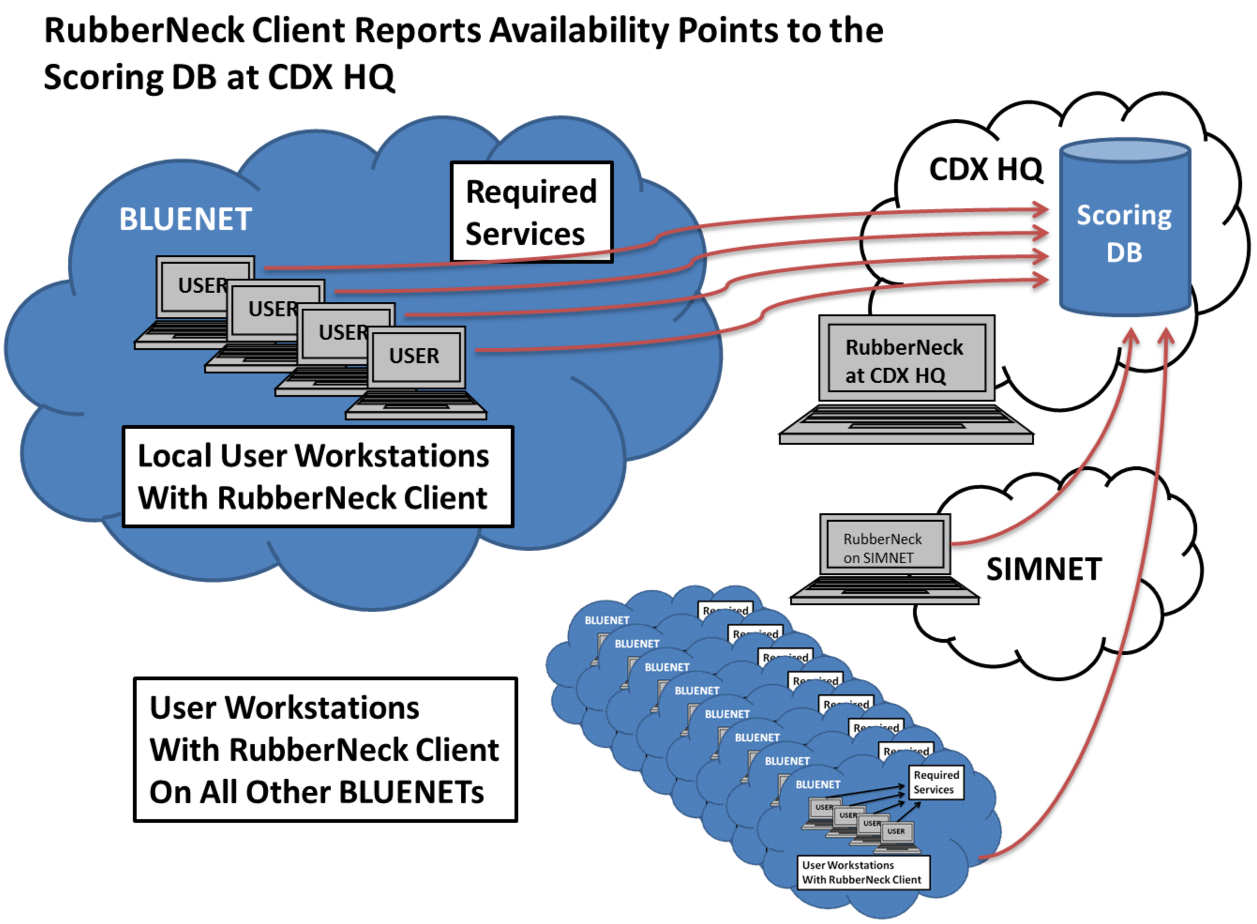
RubberNeck Client Reports Availability Points to the Scoring DB at CDX HQ
BLUENET
Required Services
USER
USER
USER
USER
Local User Workstations With RubberNeck Client
CDX HQ
Scoring DB
RubberNeck at CDX HQ
RubberNeck on SIMNET
SIMNET
User Workstations With RubberNeck Client On All Other BLUENETs
BLUENET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

Figure 2, RubberNeck Client Reports Findings to CDX HQ

2.3 RubberNeck Client Disruptions and VM Rollbacks

2.3.1 The RubberNeck Server has the ability to 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 has the ability to 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:

Availability Score = Points Collected / Points Available

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

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

2.4.4 Given that RubberNeck clients are spread 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.

2.5 On-Duty vs. Off-Duty Scoring

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

2.6 Overall Availability Scoring

2.6.1 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 and 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 2016. It has the following main components:

- 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.
- CDX Tokens – Files created by Token Agent that are completely 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 in order to prove that the system's confidentiality or integrity has been compromised. Each token is valid for a short period of time.
- 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 is expected that they will create a "confidentiality" compromise. If Red Cell gains root (system) access it is expected that they will create an "integrity" compromise.

3.1.4 Hosts added to a Blue Cell network that are discovered and found not to have the Token Agent service installed, or 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 which 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 1.6 or higher 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.

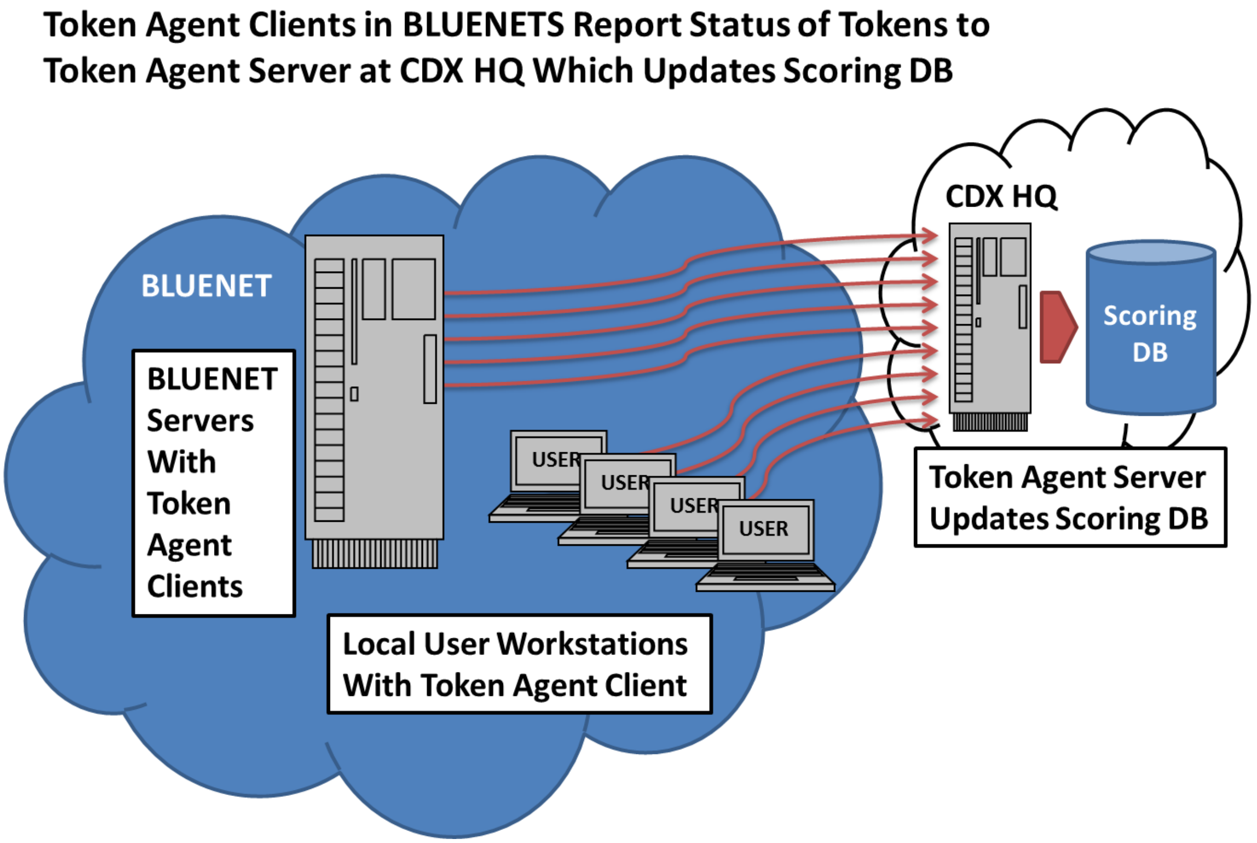
Token Agent Clients in BLUENETS Report Status of Tokens to
Token Agent Server at CDX HQ Which Updates Scoring DB
BLUENET
BLUENET Servers With Token Agent Clients
USER
USER
USER
USER
Local User Workstations With Token Agent Client
CDX HQ
Scoring DB
Token Agent Server Updates Scoring DB

Figure 3, Token Agent Client Reports Status of Tokens

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 2016 required services and use the specified directory structures:

• **EMAIL** Server	Windows:	C:\TOKEN_AGENT37\MAIL\
	Linux:	/TOKEN_AGENT37/**MAIL**/
• **WEB** Server	Windows:	C:\TOKEN_AGENT37\WEB\
	Linux:	/TOKEN_AGENT37/ **WEB** /

• **DNS** Server	Windows:	C:\TOKEN_AGENT37\DNS\
	Linux:	/TOKEN_AGENT37/**DNS**/
• **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:

• **Workstation**	Windows:	C:\TOKEN_AGENT37\WORKSTATION\
	Linux:	/TOKEN_AGENT37/**WORKSTATION**/

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 will actually be assessed in finer increments, but will be reported to the public scoring system less often in order to not artificially tip off network defenders to malicious activity. Scoring notification periods shall be as follows:

- 10:00 to 16:00
- 16:00 to 22:00
- 22:00 to 04:00
- 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 if any confidentiality or integrity compromises have been detected – 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:

- Required Services
- User Workstations

3.4.5 Confidentiality and integrity period scores shall be 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 shall be reduced (weighted by the server and workstation formula above). Each exploit is its own breach. The following rules shall be used to determine the period score:

- Each period starts with a score of 100%
- Each Confidentiality breach = 25% deduction
- Each Integrity breach = 50% deduction
- Maximum deduction = 100% per period

3.4.7 Confidentiality and integrity scoring period examples:

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

- 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, shall be 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 will be detected by the Token Agent Server as a VM snapshot reversion and will result 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 be detected as the same and also result in a 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 will be varying degrees of difficulty. These will be measured with a “Capture the Flag” type scoring system. Each module will have seven flags based on completions of specific tasks in increasing difficulty. Flags will be 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 will be 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 will have no independent authority to score the exercise. Headquarters White Cell will have 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. It is recognized that White Cell may have to make subjective rulings. Every attempt shall be made to base these rulings on data collected by the scoring system and/or direct observations by White Cell personnel deployed at the various schools.

4.1.3 The CDX 2016 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 4.1.2 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 will be applied to each school's individual score, and efforts will 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 further work.

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, it may be appealed 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 **Issues that require research must be submitted by 1530 daily if the issue is to be discussed at the 1600 daily hot wash.**