



CYBER DEFENSE EXERCISE

Red Cell Rules of Engagement Version 3.0



Purpose of this Document

This specification serves as a guide for Red Cell activities in support of 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 Red Cell Rules of Engagement

1.0.1 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.

1.1 Definitions

1.1.1 **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.

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

1.1.3 **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.

2.0 CDX 2016 Red Cell Policy

2.1 *Red Cell shall be impartial in its attacks against Blue Cell teams.*

2.1.1 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. This is especially true if the attack technique was successful and resulted in a scoring penalty against any Blue Cell team. Red Cell members shall coordinate their efforts to ensure that all Blue Cell teams are exposed to a substantially similar challenge.

2.2 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.

- **In the event that additional hosts added to a Blue Cell network 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.**



- **Prior to performing any attacks on a system found without tokens, or are missing the TokenAgent service, MUST receive concurrence from a White Cell representative prior to launching any attacks against the system.**
- 2.2.1 Any Red Cell member identified as doing such will immediately be banned from participating in any CDX activities and asked to leave CDX HQ. The two services are the core of the CDX exercise and they must remain operational!
- 2.3 Red Cell members shall not perform any Denial of Service (DoS) attacks between the hours of 2000 and 0900 the following morning.
- 2.4 Red Cell members shall not perform any Denial of Service (DoS) attacks that involve packet flooding or resource exhaustion; However, the shutting down of systems during the day is allowed.
- 2.5 Red Cell members shall cease active attacks against any Blue Cell host or network if directed by White Cell.
- 2.6 Red Cell members shall not perform any active or passive attack during times when the Red Cell has been specifically directed to stand down.

Including, but are not limited to:

- Between the hours of 1400 Monday – 0900 Tuesday, Red Cell may only enumerate/scan.
 - Red Cell may not start active or passive attacks until 0900 Tuesday
- 2.7 Red Cell shall not attempt to compromise any user account that has been specifically placed off-limits by White Cell.
 - 2.8 Red Cell members shall not target any IP address or Fully Qualified Domain Name (FQDN) which has been specifically placed off-limits by White Cell.

Including, but are not limited to:

- Any IP address of the form 10.1.xx.1 (Blue Cell head-end routers)
- Grey Cell Automation Servers
- 10.1.10.105 (RubberNeck server)
- 10.1.10.45 (Scoring server)
- 10.1.10.110 (Token server)



- Any IP address of the form 10.1.11.xx (DMVPN monitoring hosts)
- Any IP address of the form 10.1.200.xx (Core DMVPN network addresses)
- Any IP address of the form 10.1.190.xx (Scoring Baseline)
- Restricted list as specified by White Cell

2.9 Red Cell members shall not make any use of the Gray Cell remote access relay host(s) within any BLUENET, including the associated domain name(s) IP addresses. This host is reserved for Gray Cell remote administration use only. White Cell will provide Red Cell with the list of Gray Cell remote access hosts.

2.10 Red Cell members shall document all successful active attacks.

2.10.1 Each documented event must include, at a minimum, the wall-clock time and date, a description of what action was taken and a description of the results. All Red Cell documentation must be in a form that can be captured for after-action analysis. The preferred procedure is to post the attack information on the Red Cell Wiki.



3.0 Red Cell Member Acknowledgement

3.0.1 I acknowledge that I have studied the *CDX 2016 Red Cell Rules of Engagement*. Further, I understand that any failure to follow these instructions or the instructions of the CDX Leadership as it pertains to Red Cell activities may have a serious and negative effect on CDX 2016 and may result in my early exit from the exercise.

Name (Last, First): _____

Organization: _____

Signature: _____

Date: _____