MTR 05B0000052

TECHNICAL DOCUMENT

Cyber Warfare Exercise Overview

August 2005

Jason Kick

Sponsor:		**Contract No.:**	
Dept. No.:	G021	**Project No.:**	
Derived By:	Jason B Kick	**Downgrade To:**	
		Declassify On:	

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

MITRE
Scott Site
Scott AFB, Illinois

MITRE Department / Project Approval: **John M. Boner**

Abstract

The purpose of this paper is to provide an overview of the cyber exercise process from inception to after action report. This paper will introduce the terminology and life cycle of a cyber exercise. The content focuses on the entire planning and execution process, including details about different types of exercises and the resources required to plan and execute an exercise. After reading this document and reviewing the references, the reader should understand the purpose, objectives, planning, and execution process for cyber exercises.

KEYWORDS: IACND, Computer Network Defense, CND, Exercise, Cyber warfare, INFOSEC

Table of Contents

1 Introduction

The term cyber warfare exercise can describe multiple different objectives; however, they are all accomplished using an organization's Information Technology (IT) assets. In most cases, and described in detail below, a cyber warfare exercise is focused on the Information Assurance (IA) and Information Protection (IP) capabilities of an organization's IT resources and how network defense is performed while under attack.

1.1 Terms

There are several terms involved when discussing cyber warfare exercises, including the term itself. Below are definitions for terms that will be used throughout the rest of the document. These definitions are commonly understood and used by the exercise community.

- Information Assurance: The program that is directly responsible for ensuring the security, integrity, and confidentiality of the organization's data
- Information Protection: The program that is responsible for implementing safeguards to protect IT systems
- Vulnerability Assessment: A full knowledge prearranged security review of an organization's IT environment; very thorough
- Penetration test: A no-knowledge assessment performed by a Red Team against an organizations IT environment; focused on gaining access without giving the Red Team any assistance
- No-notice: An exercise that assesses an organization's IA posture and how they react to real world activities with no knowledge that an exercise is ongoing
- Cyber warfare: Very much like kinetic and physical war; however, it takes place over the Internet against IT assets and the data contained within them
- Exercise: Performing an assessment or evaluation of an organization against a set of scenarios
- Cyber warfare exercise: Performing an assessment or evaluation of an organization focusing on the IA/IP program
- Rules of Engagement (ROE): A predefined and coordinated set of guidelines established between the parties participating in the exercise
- Scenario: A scripted event or predefined plan to achieve an expected outcome
- Inject: A scenario that is planned to be executed during the exercise

- Incident: Malicious activity taken against an organization’s systems, data, or other resources that require an action by the IA staff
- Planners: The group responsible for planning and executing the exercise in a realistic manner
- Training audience: The group that will be reacting to the exercise scenarios executed by the planners and defending the environment
- Red team: A force that is used as an aggressor against the organization being assessed
- Blue team: A skillful group of people that perform a thorough assessment of your organization with full knowledge of the environment
- White team: Group that addresses questions, provides observations and lessons learned, and controls exercise execution
- Deconfliction: The process of determining if a malicious activity is from the aggressor organization or a real world threat and taking appropriate actions

1.2 Why Exercise (Purpose)

Information Assurance (IA) and Information Protection (IP) provide the foundation for executing a mission with IT resources. Whether the organization is a commercial entity or government agency, IA/IP programs are critical to the success and credibility of that organization.

Generally, a person exercises to maintain a certain characteristic or attribute related to their health. Executing an IA exercise is also done to determine the health of an organization’s capability. In many cases, the capabilities and business processes within an organization have not been tested to determine if such processes will satisfy the need in hostile circumstances. There are many different scenarios that could be executed during an exercise; however, it is essential to focus on assessing impacts against mission critical systems and data.

The cost of doing IA poorly cannot always be quantified; however, one can surmise that the loss of life, assets, time or reputation are significant reasons to ensure that IA is being done skillfully within an organization. Organizations also need to be concerned about who has access to their data, how much of their data is publicly available, and how to respond in the event that their data is compromised. A term “Cyber Pearl Harbor” came about to describe an organization that could be attacked via IT resources to create a significant impact to that organization without any indication. While this term may still be in use, the cyber attack that it describes can more simply be stated as an unpredicted cyber attack.

With this much emphasis on IA/IP, it is important to assess the posture of an IA/IP program. While humans cannot maintain themselves by exercising once a year, it is feasible for an IA organization to plan and execute an exercise at least once a year and achieve valuable training. The resources necessary to plan and execute the exercise can be large and expensive depending on the objectives of the exercise, which may make more frequent exercises unpractical.

2 Objectives

Any great army cannot be established in a day, nor will it be developed into a skilled fighting machine without training. An army has several established goals and objectives built into it by design. Likewise, our IA programs have specific purposes and objectives. An exercise is the time to assess how an organization's IA program is meeting its objectives.

Some common objectives that can be assessed are as follows:

- Assess ability to detect and properly react to hostile activity
- Assess incident reporting and analysis capabilities
- Assess capability to determine operational impacts of cyber attacks and implement proper recovery procedures
- Understand the implications of mission critical data being compromised by an adversary
- Understand the implications of losing trust in IT systems
- Expose and correct weakness in IA systems, operations policies and procedures
- Enhance capabilities needed to protect the information systems and allow continued operations in a hostile cyber environment
- Enhance cyber awareness, readiness, and coordination
- Develop contingency plans to survive the loss of some or all IT systems

2.1 Role of Objectives

Objectives are a critical part of any organization. They are the mark on the wall for an organization to meet. Likewise, exercise objectives are critical to planning an exercise. Objectives are needed to clearly tell exercise planners what type of events and scenarios need to be included in the exercise in order to determine if an organization possesses the capabilities necessary to perform IA. Without clear objectives, the exercise planners are not able to design a meaningful exercise.

As an example, suppose an exercise objective is to assess the ability to detect and properly react to hostile activity. In this situation, the exercise planners are aware of the objective and can now develop an exercise plan that will include scenarios to meet the objective. The exercise planners would need to structure one or more scenarios that involve conducting hostile activities against the target IT assets in order to provide activity for the training audience to resolve.

2.2 Issues With Exercise Simulation

While an exercise is a training event, there is a level of realism that must take place in order to stimulate the training audience. From a security engineering perspective, there is a large difference in being handed a card that states your network is being probed and scanned and actually seeing the scan in the event logs and executing the normal reporting process. In a non-technical world, it could be compared to seeing pictures of Mt. Everest and actually climbing Mt. Everest.

It is important when educating and working with senior leaders to reinforce the need to use real aggressors to execute malicious activity for exercise scenarios to more accurately simulate a threat. Reducing exercise artificialities greatly improves the reactions from the target audience and enhances the exercise lessons learned. This translates to getting buy-in from senior leaders to execute attacks and other malicious activity against the organization. Most leaders hesitate to allow this type of activity for fear of impacting any ongoing mission critical activities. This is a common fallacy because the disruption of mission critical activities can occur with proper exercise design by outlining the proper safeguards in the rules of engagement and educating senior leaders throughout the process.

In some cases it may make sense to develop a replica of your environment or a key system in the environment to use for actual attacks during the exercise in order to simulate reactions by the player audience. While this may appease senior leaders, it will not help assess how your organization reacts to real threats. A real adversary will attack your systems regardless of having your permission.

3 Exercise Structure

The structure and planning process of an exercise is similar across organizations; however, the execution and scenarios vary depending on the objectives of the exercise. It greatly increases the realism and effectiveness of the exercise to understand the different types of exercises and the objectives that each fulfill. Once an organization has established exercise objectives, the exercise planners can begin to take a realistic look at what type of exercise will match the objectives and provide an effective assessment of the organization's IA program.

There are several different types of IA exercises. The four described below are typically performed by an organization over a period of years. Understanding the characteristics and applicability of these different types will yield better results and lessons learned. The following table illustrates some characteristics of different exercise categories and their usage. Detailed descriptions of each will be discussed later.

Table 1 Exercise Types

Exercise Style	Description	Complexity	Resources	Organization Match
Table Top	Paper exercise scenarios that are scripted by exercise planners	This type of exercise can be quickly planned and executed depending on the number of organizations involved 1-2 months planning 1-3 day execution	Limited number of resources depending on number of organizations	New to exercises and assessing organizational IA objectives
Table/Live	Paper scenarios with some live scenarios facilitated by an aggressor organization (probes, scans, e-mail threats)	This type of exercise requires more planning and execution 3-6 months planning 5-7 day execution	Requires more people and time, real targets for scenarios, deconfliction contacts	Organizations that are familiar with inter-organization exercises and a strong knowledge of their organization's objectives

Exercise Style	Description	Complexity	Resources	Organization Match
Full Live IA	Exercise plan coordinates real scenarios into the exercise. Paper scenarios used to stimulate if necessary	Requires detailed coordination and planning 6-12 months planning 2-3 months build up 7-14 day execution	Large number of organizational participants, IT resources, travel budget for meetings, deconfliction contacts	Organizations that are familiar with exercises, their aggressor organization, and organizational objectives
Full Live IA/ No-Notice	This is an agreement between senior leaders and an aggressor organization to perform a penetration assessment of the organization without the awareness of the training audience	Requires detailed coordination, planning and deconfliction 12-18 months planning 3+ months execution	Senior Leaders, aggressors, deconfliction contacts	Organizations which need to evaluate how the organization does in a true penetration attempt and incident response

3.1 *Sample Exercise Scenarios*

There are many different approaches and possibilities for designing and executing an exercise. One of the most common methods to implement exercises in an organization that has never done one is the "crawl, walk, run" fashion. This approach will allow an organization to step their way from smaller table top exercises to complicated, no-notice exercises. As with most new processes, there are lessons that need to be learned and subprocesses that need to be clearly written out to make improvements and design successful processes that are meaningful.

3.1.1 Table Top (scripted fictitious events)

"Crawling" is a designator given to the initial phase of an exercise. The focus is on understanding the mechanics of communication and interaction required between the participants in the exercise. This is often done as the first step of opening communication between multiple organizations and determining how information would flow in real world events. This phase is the most simple but can provide many lessons learned depending on the maturity of the organization. During this phase, an organization should execute a table top exercise to establish communications and begin the learning process.

Table top exercises are named such because, in most cases, the planners and players of the exercise sit down at one table and execute the exercise. A table top exercise should have a small audience and very well-defined objectives. This type of environment opens up communications between different players and aids in establishing the business processes associated with planning, executing, and training during an exercise. There are no real scenarios that are executed and all scenarios are pre-coordinated and written down.

Table top exercise overview:

- Goal: Establish a good baseline for future exercises
- Objectives: Clear, well defined (Determine how IA staff interact and respond to an incident); validate procedures; observe description of the process used to detect, respond and recover from simulated events
- Lessons learned: Focus on what worked well and what requires improvement
- IA awareness is raised
- Future exercises should include live events

Many organizations are using this technique to establish relationships and share information with other organizations, partners, or countries. Table top exercises are also used to test the readiness of response capabilities and raise awareness within the IA community.

3.1.2 Table Top/Live (scripted fictitious events with real probes/scans)

"Walking" is a designator given to a phase where the focus is on improving communication and interaction between participants in the exercise while increasing the realism of scenarios. This phase often includes using an aggressor team to provide real activity to stimulate scenarios and provide realistic training for the player audience. This phase builds off of the lessons learned from table top exercises and increases the complexity and resources involved in the exercise. During this phase an organization should use a mix of fictitious events and real events to facilitate realism in exercise scenarios.

Table top exercises that include live events increase the realism and training opportunities for the training audience. The exercise planners facilitate the execution of the exercise in conjunction with an aggressor team that executes real events against pre-determined targets. This type of exercise can include multiple organizations and may require deconfliction of real events. The amount of coordination and time required to plan this type of exercise is in the timeframe of 3-6 months. This type of environment stimulates training and assessment of current business processes associated with planning, executing, and training during an exercise. In this case, there are real scenarios that are pre-coordinated by the exercise planners to be executed during planned scenarios

Table top exercise overview:

- Goal: Integrated IA exercise
- Objectives: Train the organization and IA staff; validate procedures; determine ability to detect, respond, and recover from simulated events
- Real probes and scans used to stimulate player action
- Lessons learned: Focus on what went well and what needs improvement
- Security baseline should be evaluated
- Organizational IA awareness is raised
- Future exercises should include real aggressors

3.1.3 Full Live IA (real and scripted events)

"Running" is a designator given to a phase where the focus is on assessing communication and interaction between participants in the exercise, while operating in a realistic set of threat scenarios. This phase includes using an aggressor team to provide real activity to drive the realistic scenarios for the player audience to resolve. This phase builds off of the lessons learned from previous exercises and increases the complexity and resources involved in the exercise. The amount of coordination and time required to plan this type of exercise is on the order of 6-12 months. During this phase an organization should rely on the aggressor team and facilitate additional paper scenarios if needed to stimulate player response.

Full IA exercises are based on real events to increase the realism and training opportunities for the target audience. The exercise planners facilitate the execution of the exercise in conjunction with an aggressor team that executes real events against pre-determined targets. Likewise, if the aggressor team discovers a vulnerability that will contribute to the training of the player audience, it may be inserted as a dynamic scenario event. This type of exercise includes multiple organizations and requires deconfliction of real world events since they will appear similar. This type of environment stimulates training and assessment of current business processes associated with planning, executing, and training during an exercise.

Full IA exercise overview:

- Goal – Fully Integrated IA exercise
- Objectives: Train the organization and IA staff; validate procedures via real events and scenarios
- Lessons learned: Focus on what went well and what needs improvement
- Capability assessment for detecting responding and recovering from some simulated and realistic events
- Exercise control facilitated by real events
- IA baseline evaluation and update
- Fix plan for issues/problem areas
- Capabilities of aggressor should be increased

3.1.4 Full Live IA - No-Notice (real events)

A no-notice IA exercise focuses on evaluating IA without your organization knowing that the exercise is happening. The efforts focus on assessing the organization's IA posture and how they react to real world activities with no knowledge that an exercise is ongoing. This phase includes using an aggressor team to provide real activity to drive realistic scenarios for the player audience to resolve. This phase builds off of the lessons learned from previous exercises and increases the complexity and resources involved in the exercise. The amount of coordination and time required to plan this type of exercise is in the timeframe of 12-18 months. During this phase an organization should rely on the aggressor team to execute a real attack and be allowed to compromise the network completely.

No-notice exercises should not have artificialities or simulations. This is the opportunity to assess the organization on how well they protect the network and respond to the real world situation that the red team would provide. To the training audience, this type of exercise will look like actual malicious activity on the network. The exercise planners will facilitate the execution of the exercise;, however, a majority of the work is done by an aggressor team that will execute events like a real adversary does. Likewise, should the aggressor team discover a vulnerability that will further the training of the player audience, it may be inserted as a dynamic event into the exercise. This type of exercise includes multiple organizations and requires deconfliction of real events at a level higher than the training audience. This type of environment is the closest simulation to a real attack and provides many lessons learned on current business processes and IA readiness.

No-notice exercise overview:

- Goal – Fully Integrated no-notice IA exercise
- Objectives: Assess the organizations defensive posture and IA staff ability to detect, respond, and recover from real events
- Lessons learned: Focus on what went well and what needs improvement, remain flexible and dynamic
- Fix plan for issues/problem areas
- Capability effectiveness evaluation
- Scope may expand beyond IA into critical infrastructure protection, social engineering, or physical access
- Performance result assessment and evaluation for future exercises

4 Exercise Planning

The exercise planning process determines the scenarios and the execution of those scenarios for the exercise. A group of exercise planners focused on the objectives will determine the best means to reach those objectives and develop a complete exercise plan. This plan will include the order of scenario execution and the expected reactions to the scenarios.

As expected, the exercise plan must be coordinated among the appropriate staff. This means that planning should start several months before the exercise is to take place. There is a significant amount of time put into planning and coordinating an exercise, especially if it includes multiple organizations. Any organization that will be a participant in the exercise should be involved in the development of the exercise plan in order to provide details about their organization's role in the exercise.

The exercise planners must be empowered by senior leaders. If senior leaders do not provided this authority, it will make planning exercise scenarios difficult. Senior leadership must clearly understand why the organization is undergoing an exercise and empower the planners to facilitate a realistic scenario-driven exercise.

4.1 Initial Planning Meeting

The initial planning meeting should involve the internal organization's exercise planners. These staff members must be empowered by the senior leaders of the organization to plan an exercise that will meet the exercise objectives. Depending on the amount of complexity required for the exercise, this should be done anywhere from 6-12 months prior to the actual exercise. The complexity can be determined by the number of organizations involved in the exercise and the size of the target set. The more organizations, the more time required for the planning. The initial planning meeting should be an internal meeting to discuss ideas, determine the objectives for the exercise, and decide what other organizations or aggressors need to be contacted for the first planning meeting.

4.1.1 Outcomes of the Initial Planning Meeting

- Draft initial exercise plan (high level)
- Defined scope (table top, full IA, no knowledge, 24x7 operations)
- Defined organization objectives
- Identify additional organizations needed to participate
- Assigned action items

4.2 First Planning Meeting

The first planning meeting should be one to two months after the initial planning meeting. This meeting should include all of the internal exercise planners and exercise planners from outside organizations. It is crucial that outside organizations are included as early as possible in the exercise planning process to ensure that all entities are aware of what is being planned and what is expected.

During this meeting the exercise plan and objectives need to be reviewed so that everyone is in agreement with the plan. As this meeting comes to a close, a list of action items for each organization needs to be recorded so that the exercise planners can be accountable for the items they need to provide information on. In some cases, these action items may range from developing an exercise scenario to drafting the rules of engagement with outside aggressor organizations. It is important not to modify the objectives and exercise plan after this meeting, as several other items are being coordinated around these critical documents.

4.2.1 Outcome of First Planning Meeting

- Draft exercise plan
- Draft Rules of Engagement (ROE) with aggressors (if necessary)
- Finalized exercise objectives
- Create Point Of Contact (POC) list
- Define Exercise scenario overview
- Assigned action items

4.3 Mid-planning Meeting

The mid-planning meeting is just that. One to two months after the first planning meeting, the group should gather and go over the action items from the first meeting, finalize the objectives and exercise plan if necessary to accommodate an organization’s needs, review the exercise plan and determine what actions items still need to be completed.

4.3.1 Outcome of the Mid-planning Meeting

- Finalized exercise plan
- Assigned actions items

4.4 Final Planning Meeting

The final planning meeting should happen one month prior to the beginning of the exercise. Again, this meeting must include all organizations. This meeting is a review of previous action items and a finalization of exercise scenarios to be executed in the exercise plan. This is not the time to introduce new scenarios or change the exercise plan and objectives. After this meeting there should only be minimal activity left, such as updating POC lists for the exercise and determining any schedules or visit requests necessary for outside organizations.

4.4.1 Outcome of Final Planning Meeting

- Exercise plan final review
- Organizations aware and prepared
- Aggressors and planners in sync
- Scenarios or objectives have not been changed
- Action items (if any) assigned

5 Exercise Execution

Exercise execution is performed by the white team. During this period the white team controls the exercise scenario release and interactions with the training audience. Provided the planning process has been thorough, the execution phase is a matter of following the exercise plan, ensuring that the proper scenarios are being executed, and ensuring that the player audience is responding appropriately. Performing observation during the exercise is key to a successful training experience. White team observations can identify deficiencies in how the training audience is responding to the exercise scenarios and all for adjustment in exercise execution if necessary.

5.1 Observation

Observations should be documented in a pre-defined format and should be reviewed by the exercise planners and the training audience. These are the observations from the exercise planners who were present during the exercise and any identified by the training audience. Between the two sets of observations, key members of the staff can begin to address the deficiencies with the organization's leaders.

An observation format has been included in Appendix B. The basic principal involved in collecting observations is to highlight deficiencies that become apparent to the white cell during exercise execution. Collecting this information will allow the organization to assess the deficiencies and implement a fix plan to improve the organization's readiness.

5.2 Lessons Learned

Knowledge gained based on the exercise, both bad and good, should be documented as lessons learned. The objectives of an exercise often times expose deficiencies within the IA program that can be improved. An IA exercise is the opportunity to find out what deficiencies exist within the organization in a controlled environment. It is important to create fix plans and follow up on deficiencies that have been identified during the exercise. Conversely, exercises can also highlight those processes, capabilities, etc. that were very effective.

Common process deficiencies:

- Business processes are ineffective
- Reporting process is not understood
- Required notifications are not made
- Senior staff members are not brought in when needed
- Outside organizations are not brought in when needed
- Documentation does not match practice
- Documentation does not exist
- Technical/Technology issues
- Administrators unavailable
- Logs not audited/not available
- Minimal troubleshooting expertise

- Staff not trained

During the planning and execution of the exercise, an organization will collect lessons learned about the exercise itself. An organization will be able to gain valuable information to improve the exercise planning and execution process for future exercises.

Common exercise deficiencies:

- Senior leaders are not involved with the planning
- IA scenarios are limited due to lack of awareness
- Communication inconsistencies introduce confusion
- Rules of Engagement are not clear with the aggressor
- Staff that are not empowered cannot execute an assessment
- Planning must be coordinated
- The training audience must understand the scenario that they are participating in
- Aggressor and controller must communicate clearly
- Activities must be purposeful and realistic
- Exercise is viewed as evaluation vice training
- Constraints on aggressors limit the return on investment

6 Conclusions

Executing an IA exercise within your organization will provide meaningful insight into the capability and readiness of the organization. Players and planners need to understand that exercises are not done to make an organization look bad. Instead, they are done to train and equip an organization in preparation for real world malicious activities.

Having a well trained and equipped organization that is able to detect and respond to malicious activity is one of the largest challenges facing an organization. If an organization does not take the time to train and assess how their organization handles malicious activity, then it will not be able to efficiently respond to real world incidents. An exercise is a controlled opportunity to run malicious attacks against the network and assess the security posture of the environment and the ability of the IA staff to defend the mission critical data.

The exercise planning process is critical to ensuring that the exercise execution occurs without difficulty and the objectives of the exercise are met. This process must be thorough to ensure that all of the necessary people and agreements are in place early, in order to have a successful exercise.

Finally, the organization as a whole must be willing to learn from the deficiencies. An organization that does not take the time to provide lessons learned and create fix plans has diminished the return on investment. Likewise, the organization has reduced the ability to defend, detect, and respond to real incidents.

7 Appendix A (References)

General Information

http://www.afcea.org/signal/articles/anmviewer.asp?a=42&z=17

http://www.military-information-technology.com/article.cfm?DocID=472

http://iac.dtic.mil/iatac/resources.html

http://blackhat.com/presentations/bh-federal-03/bh-fed-03-dodge.pdf

Red Teaming

http://www.mitre.org/news/digest/archives/2000/defense_red_team.html

http://www.sandia.gov/idart/whatwedo.html

Table Top exercise

http://www.thunderbay.ca/index.cfm?fuse=html&pg=2730

http://www.armidale.local-e.nsw.gov.au/news/pages/4761.html

http://www.scdf.gov.sg/html/info/pdf/GUIDELINES%20ON%20TABLE-TOP%20EXERCISE.pdf

http://english.people.com.cn/200410/21/eng20041021_161054.html

8 Appendix B (Observation format)

Observation Number: 1

Originator: IA White Team Member

Point Of Contact: John Doe

Phone: xxxxxxxx

Exercise Name: IA Table Top

Date Observed: June 6 2005

Observation Title: Ineffective Incident Response

Observation:

XYZ system was compromised and the IA staff were unaware of the proper reporting procedures and incident handling process.

Discussion:

On 6 June 2005 the exercise planners executed a system compromise scenario in order to observe the incident response plan. The scenario included notifications to the system administrators and users of the XYZ system that it had been compromised as part of the IA exercise and that all of the data had been stolen.

This scenario did not prompt an immediate response from the contacted parties. After 6 hours, the white cell notified the training audience that they had been notified of a compromised system and needed to investigate the incident.

After the initial contact it became very apparent that the IA staff was unaware of what processes and procedures needed to be implemented to respond to the incident and determine the scope of the system compromise.

Recommendation:

IA staff should develop incident response procedures, develop contact lists of outside organizations, and perform training prior to the next IA exercise.