Cyber Exercise Playbook

Jason Kick

November 2014

MP140714

Wiesbaden, Germany

MITRE

Approved By

Mr. Charles Best Project Leader	Date

Abstract

This paper provides an overview of the cyber exercise process from inception to reporting. It introduces the terminology and life cycle of a cyber exercise and then focuses on the planning and execution aspects of such exercises, to include objectives, scenarios, reporting and assessment procedures, network architecture, tools, and lessons learned from utilizing the scenarios outlined during an exercise with Partner Nations. Reading this document and reviewing the reference materials should enable exercise planners to understand the purpose, objectives, planning, and execution processes for conducting cyber exercises.

This page intentionally left blank.

Acknowledgements

Several MITRE staff members contributed to this paper, either by reviewing it or by writing certain sections. Thank you to everyone who took part in ensuring this paper's accuracy and completeness, especially:

- Mr. Nathan Adams
- Mr. Dan Aiello
- Mr. Charles Best
- Mrs. Margaret MacDonald
- Mr. John Modrich
- Mr. Scott Wilson

Several staff of the US Army also reviewed this paper. Thanks are due to:

- Mr. Aaron Smith
- Mr. Dennis Freed
- Mr. Daniel Crandall

This page intentionally left blank.

Table of Contents

List of Figures

List of Tables

Overview

Achieving objectives through the employment of cyberspace capabilities loosely defines cyberspace operations. In essence, an organization that executes an operation or business function reliant on timely and accurate information, data, networks or communications systems is operating in cyberspace. Cyberspace operations are critical to the success and credibility of any organization— a commercial entity, government agency, sovereign nation, or combination. However, many organizations never evaluate and exercise their cyber capabilities and business processes to determine if those processes will satisfy operations during hostile circumstances. Organizations can execute many different scenarios during an exercise; however, they must always focus on assessing effects on critical systems and data that will have an impact on the operation or mission.

This playbook guides organizations as they exercise and assess capabilities in the realm of cyberspace. It details the key aspects of designing and executing exercises with Partner Nations (PNs) that pit scenario-driven threats against an organization's cyberspace assets. The playbook:

- Defines terminology based on doctrine and practical implementation
- Defines objectives for executing threat scenarios to asses cyberspace operations capabilities
- Outlines threats, ranges, and best practices for operating a Cyber Exercise
- Reports on the effectiveness of cyber injects and scenarios
- Provides the necessary information to execute and assess cyber threat scenarios within an exercise
    - Exercise structures
    - Sample scenarios
    - Sample incident response plan
    - Sample observation and incident reporting formats
    - Sample network architecture
    - Tools that could facilitate various scenarios

Terminology

As U.S. dependence on networks has increased, the nation's reliance on jointly defending cyberspace with its PNs has also increased. Many exercises include multiple PNs, potentially creating confusion about terminology and practices. For the purpose of this document and to establish a common vocabulary across PNs, Table 1 defines key terms related to cyber exercises. The definitions reflect industry-accepted best practices as well as the terminology accepted by the Committee on National Security Systems Instruction (CNSSI) 4009 and National Institute of Standards and Technology Internal Report (NISTIR) 7298.

Table 1. Terminology

Term	Definition
After Action Review (AAR)	An analytical review of training events that enables the training audience, through a facilitated professional discussion, to examine actions and results during a training event. (Source: CJCSM 3500.03D)
Blue Team	The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers. (Source: CNSSI-4009) In application, this role belongs to the training audience.
Cyber Security	The strategy, policy, and standards regarding the security of and operations in cyberspace; encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. (Source NIST NICE)
Cyber Warfare	Very much like kinetic and physical war; however, it takes place over the networks and systems against IT assets and the data contained within them.
Cyber Warfare Exercise	An assessment or evaluation of an organization focusing on the Information Assurance program.
Deconfliction	The process that takes place between an RT and ECG to determine if malicious activity during an exercise originated from the Red Team or is a real-world threat.
Event/Inject	A specific activity executed as part of a MSEL (Source: CJCSM 3500.03D)
Exercise	A simulated wartime operation involving planning, preparation, and execution that is carried out for the purpose of training and evaluation. (Source: CJCSM 3500.03D)
Exercise Control Group (ECG)	Personnel that assist in the management and direction of the execution phase of supported exercises. (Source: CJCSM 3500.03D) In application, this group executes the injects and drives the scenario for the exercise.
Exercise Scenario	Describes the strategic and operating environment in sufficient scope and detail to allow accomplishment of the exercise and training objectives. (Source CJCSM 3500.03D). In application, it is the storyline or plot for the entire exercise, utilized by all planners and participants.
Hotwash	A debrief conducted immediately after an exercise or test with staff and participants. (Source NIST IR 7298)
Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. (Source NIST IR 7298)
Information Assurance (IA)	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Source: CNSSI-4009)
Master Scenario Event List (MSEL)	A collection of pre-scripted events intended to guide an exercise towards specific outcomes. (Source: CJCSM 3500.03D)
Penetration	A test methodology in which assessors, using all available documentation (e.g.,

Test	system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system. (Source NIST IR 7298)
Planners	The group responsible for planning and executing the exercise in a realistic manner. (Source: CJCSM 3500.03D)
Range	Provides a unique testing environment that allows large and small scale networks to be simulated using a mixture of virtual and physical devices. (Source: NIST NICE)
Red Team (RT)	A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. (Source: CNSSI-4009)
Risk Management	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system. (Source: CNSSI-4009)
Rules of Engagement (ROE)	Detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test, and gives the test team authority to conduct defined activities without the need for additional permissions. (Source NIST IR 7298)
Threats	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (Source CNSSI 4009)
Training Audience	An individual, staff element, staff or organization that performs a particular task or set of tasks during the execution of the exercise (Source: CJCSM 3500.03D)
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (Source: CNSSI-4009)
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. (Source: CNSSI-4009)
White Team/ Observers	The group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of their enterprise's use of information systems. The White Team acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission. (Source: CNSSI-4009) In application, this group observes the training audience and provides feedback to the ECG and RT.

Exercise Planning

The exercise planning process determines the participants, exercise scenario, injects and the execution order for the course of the exercise. A group of exercise planners focused on the objectives selects the best means to reach those objectives and develops a complete exercise plan known as the master scenario event list (MSEL). The MSEL serves as the script for the execution of the exercise; it includes the ordering of injects, time of execution, and the expected reactions from the training audience. Appendix A provides a sample.

The structure and planning of a cyber exercise are similar across organizations; however, the execution and scenarios vary depending on the participants and objectives of a specific exercise. Understanding the different types of exercises and the objectives that each fulfills greatly increases exercise realism and effectiveness. Once an organization has established exercise objectives, the exercise planners can begin to take a more detailed look at what type of exercise would match the objectives and provide an effective assessment of the organization's IA program.

A cyber exercise may run as a stand-alone event on an isolated network or as an activity within a larger training exercise on an operational network. The planning processes are similar, except that the latter requires additional coordination between the exercise planners to ensure the exercise both achieves the cyber objectives and supports the greater exercise objectives through controlled impacts to operational networks. The exercise planning process begins by identification of the objectives and outcomes of the exercise, as described below.

Objectives

Without clear objectives, planners cannot design a meaningful exercise. The objectives enable planners to clearly structure the scenarios within the exercise to determine if their organization possesses the capabilities necessary to operate successfully within a hostile cyber environment and defend against cyber threats. Different organizations have different guiding principles, tools, tactics, and procedures, which make it important to establish a baseline for each exercise.

The overarching objective of executing cyber training scenarios that involve multiple entities is to ensure that information systems and networks successfully operate in support of the exercise scenario. This provides the basis for exercise planners to begin building a cyber scenario centered on a coalition network that must be defended in order to accomplish a mission. Table 2 outlines a minimum set of objectives that planners should consider throughout the lifecycle of an exercise, to include training, execution, validation, and reporting; it does not represent a comprehensive list.

Table 2. Common Exercise Objectives

ID	Objective
01	Determine the effectiveness of the cyber education provided to the training audience prior to the start of the exercise
02	Assess effectiveness of the organization's/exercise's incident reporting and analysis guides for remedying deficiencies
03	Assess ability of the training audience to detect and properly react to hostile activity during the exercise
04	Assess the organization's capability to determine operational impacts of cyber attacks and implement proper recovery procedures for the exercise
05	Determine the success of scenario planning and execution between the ECG, RT, and training audience
06	Understand the implications of losing trust in IT systems and capture the work-arounds for such losses
07	Expose and correct weaknesses in cyber security systems
08	Expose and correct weaknesses in cyber operations policies and procedures
09	Determine what enhancements or capabilities are needed to protect an information system and provide for operations in a hostile environment
10	Determine if the injects meet the objectives of the training
11	Enhance cyber awareness, readiness, and coordination
12	Develop contingency plans for surviving the loss of some or all IT systems

Exercise Outcomes

The desired outcomes differ for each exercise, but always revolve around providing a realistic scenario to demonstrate cyber threat methods to the training audience and to assess the success of training programs and tools used to meet exercise objectives. Outcomes should aim at building awareness and assessing response planning to various cyber threats, and should tie back to the overarching objectives of the exercise. Planners must tailor injects for each exercise to meet the desired outcomes.

For example, if the exercise centers on assessing the ability to detect and properly react to hostile activity, the exercise planners would need to structure one or more scenarios that involve hostile activities against the target IT assets. They would design these scenarios to stimulate the training audience and elicit responses that match the desired outcomes of the specific exercise and the overarching objectives.

Table 3 contains a sample of desired cyber exercise outcomes, aligned with the four phases of exercise execution – training, execution, validation, and reporting –discussed in Exercise Execution. Planners should select appropriate outcomes and tailor them to a specific exercise scenario.

Table 3. Desired Cyber Exercise Outcomes

ID	Outcome	Activity	Category
01	Performed cyber awareness training at the appropriate level/language of the training audience	PN end users, system administrators, network administrators, and cyber security administrators will complete cyber awareness training, to include cyber threats, incident response, and responsibilities.	Training
02	Trained cyber defense personnel to operate network and system security tools	Subject matter experts (SMEs) will execute the appropriate cyber tool training that the PN security administrators need for the exercise. This should include any security devices (firewalls, antivirus, intrusion detection systems [IDS)], accreditation [policy and procedures], and procedures [incident detection, log review and incident response]).	Training
03	Ensured the RT applied realistic training scenarios to exercise execution	The RT will utilize unclassified tools and techniques that can be shared with PNs, to include social engineering, spear phishing, fake web sites, physical access attempts, and internal network manipulation to stimulate the exercise in accordance with the mission/scenario.	Execution
04	Ensured the exercise training objectives can be met in lieu of RT success	The ECG will be prepared to inject a "paper card" or notification into a cyber scenario in order to stimulate attainment of PN training objectives in the event the RT actions fail to do so.	Execution
05	Ensured the RT can deconflict questions from the ECG about suspicious activities	In the event a suspicious activity is reported to the ECG, the RT must be able to confirm or deny its involvement within 30 minutes of request from ECG.	Execution/ Validation
06	Validated the ability to operate, defend, and restore availability and integrity of the network	The PN communicators can maintain network operation during the course of the exercise, including the ability to detect, mitigate and report an attack, degradation of capability, disruption or denial of network services.	Validation
07	Validated the cyber defense security procedures (incident response plan) in place for the exercise scenario	The RT stimulates threat scenarios that drive the PN training audience to execute the cyber defense procedures instituted for the exercise (see Appendix B: Sample Exercise Incident Response Plan Appendix C: Sample Incident Response Form).	Validation
08	Provided situational awareness to training audience and leadership for the exercise	As the PN training audience detects an event and executes incident response procedures, or if the RT actions have an impact on IT security occurs, the training audience will provide the appropriate situational awareness within one hour.	Validation

ID	Outcome	Activity	Category
09	Executed a hotwash after completion of exercise	At the conclusion of the exercise the exercise organizers should reveal the RT activities to the cyber training audience to identify the actions executed, the actual response, and the expected response.	Reporting
10	Identified and reported gaps in capability, manning or training	Exercise observers will make note of any gaps in the cyber security training, response procedures, staffing, or roles and responsibilities and report them to exercise planners and leadership (see Appendix D: Sample Exercise Roles and Responsibilities).	Reporting

Know the Training Audience

The United States has established, secured, and defended networks for many years, while many other nations may not even operate their own network and instead rely on commercial services such as Yahoo or Google. Some nations have quite advanced cyber security practices, but may take vastly different approaches to the execution of cyber security. This, combined with a reliance on commercial services and limited exposure to cyberspace operations, can pose a challenge to future cyber scenarios in exercises with the various nations. Table 4 lists factors that planners must consider.

Table 4. Cyber Exercise Considerations

Challenge	Impact	Resolution
Participants have varying levels of training and education about cyber security.	This will create confusion about the goals and activities associated with the cyber scenario.	Ensure that cyber injects match the skills and capacity of the training audience while adequately demonstrating cyberspace threats.
Participants have only a minimal understanding of the concepts of defense in depth, internal security, spearphishing, and other malicious activities.	The exercise participants will not have a common baseline of terminology and experience to on which to base reactions to exercise injects.	Provide a threat briefing to the PNs to increase understanding of spearphishing, malicious logic, attack Tactics, Techniques, and Procedures (TTPs) and defense TTPs.
Participants rely too heavily on what a tool "tells" them versus what the data actually means because they lack an understanding of what is taking place on the network.	The training audience may not respond appropriately to the injects due to a lack of awareness and ability to correlate events occurring on a network or system.	Mentor the training audience on understanding how their enterprise works, what alerts mean, and what tools/data are available to determine actuality of reported events (commercial, military, or other courses already exist).

Challenge	Impact	Resolution
Awareness and understanding of an enterprise baseline are not common concepts in many organizations, especially large ones.	The lack of understanding will make it almost impossible to distinguish what is normal from what is anomalous during the exercise, so that an inject may not elicit the desired response.	Establish real scenarios that allow the training audience to learn the details of their enterprise.
Participants use poor security practices, from weak/default passwords to use of personal computers for the mission.	Poor security practices will allow the RT to succeed in executing its plans and deny/disrupt the exercise as outlined by the ROE.	Establish a baseline for security during exercise training and demonstrate the possible impacts of poor cyber security through the cyber injects used during the exercise.

Types of Cyber Exercises

Cyber exercises take different forms. Over a period of years, organizations may perform the three type of exercises described below. Understanding the characteristics and applicability of these different types yields better results and lessons learned. Table 5 summarizes some characteristics of different exercise categories and their usage.

Table 5. Exercise Structures

Style	Description	Complexity	Timing	Resources	Matches
Table Top	Paper-driven exercise with injects scripted by exercise planners and delivered via paper (cards/ discussion)	This type of exercise can be planned and executed quickly, depending on the number of organizations involved.	Planning: 1–2 months Execution: 1–3 days	Limited resources needed, depending on number of organizations	• Organizations new to exercises and to assessing organizational IA objectives • Organizations that need to validate processes/ train personnel in-between other exercises
Hybrid	Paper injects with some live scenarios facilitated by a RT for realism (probes, scans, e-mail spoofing, etc.)	This type of exercise requires more planning and longer execution times.	Planning: 3–6 months Execution: 3–5 days	Requires more people and time, real targets for scenarios, deconfliction contacts	Organizations familiar with inter- organization exercises and a strong knowledge of their own objectives

Style	Description	Complexity	Timing	Resources	Matches
Full Live	Exercise plan incorporates real scenarios and injects into the exercise. Paper injects only used to stimulate if necessary	This type of exercise requires detailed coordination and planning.	Planning: 6–12 months Buildup: 2–3 months Execution: 7–14 days	Large number of organizational participants, IT resources, travel budget for meetings, deconfliction contacts	Organizations familiar with exercises, RTs, and their own organizational objectives

Ideally, as an organization matures it will progress through the different exercise structures in a "crawl, walk, run" fashion. This approach allows organizations to step their way from smaller table top exercises to complicated, full live exercises. As with most new processes, planners must absorb lessons and must clearly write out sub-processes to make improvements and design meaningful and successful processes.

Table Top (scripted events)

Table top exercises received their name 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 training audience and very well-defined objectives (see Table 6). 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. The injects are hypothetical, entirely pre-coordinated, and written down. Many organizations use table top exercises to establish relationships and share information with other organizations, partners, or countries; test the readiness of response capabilities; and raise awareness within the IA community.

Table 6. Table Top Exercise Overview

Goal	Establish a good baseline for future exercises; raise cyber security awareness and skills
Objectives	Clear, well defined goals: e.g., determine how cyber security staff interact and respond to an incident; validate procedures; observe and describe the processes used to detect, respond and recover from simulated events
Lessons Learned	Focus on what worked well and what requires improvement
Future	Future exercises should enhance training by including live events

This type of exercise could be considered "crawling." This phase is the most simple but can provide many lessons learned depending on the maturity of the organization. The exercise focuses on understanding the mechanics of communication and interaction required among the participants in the exercise. This often represents the first step of opening communication among multiple organizations and determining how information would flow in real world events.

Hybrid (scripted injects with real probes/scans)

Table top exercises that include live events increase the realism and training opportunities for the training audience (see Table 7). The exercise planners facilitate the exercise in conjunction with an RT that executes real events against pre-determined targets. This type of exercise can include multiple organizations and may require deconfliction of real events, especially if using an operational network. Coordinating and planning a hybrid exercise requires approximately 3–6 months. This environment stimulates training and assessment of current business processes associated with planning, executing, and training during an exercise. For hybrid exercises, the planners pre-coordinate real injects to be executed during planned scenarios.

Table 7. Hybrid 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 Evaluate security baseline Raise organizational IA awareness is raised
Future	Future exercises should include live Red Teaming

This type of exercise could be considered "walking." This phase often includes using an RT to engage in real activity to stimulate scenarios and provide realistic training for the player audience. This phase builds on 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. This exercise approach would focus on improving communication and interaction among participants in the exercise while increasing the realism of scenarios.

Full Live (real and scripted events)

Full live exercises are based on real events to increase the realism and training opportunities for the target audience. The exercise planners facilitate the exercise in conjunction with an RT that executes real events against pre-determined targets set by the exercise planners and defined in the MSEL. Likewise, if the RT discovers a vulnerability that would contribute to the training of the player audience, a relevant action may be inserted as a dynamic scenario event. Full live exercises include multiple organizations and requires deconfliction with real-world events, since they will appear similar on a network. This environment stimulates training and assessment of current business processes associated with planning, executing, and training during an exercise (see Table 8).

Table 8. Full Live Cyber Exercise Overview

Goal	Fully integrated cyber 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 Assess capability for detecting, responding to, and recovering from some simulated and realistic events Use real events to facilitate exercise control Evaluate and update IA baseline Create remediation plan for issues/problem areas Increase RT capabilities
Future	Future exercises should include more advanced injects to demonstrate sophisticated threats and reinforce positive cyber security behaviors and training

The realism of exercise injects and of the training audience responses determine the success of the cyber exercise. Planners must understand the types of threats the training audience would face in a day-to-day situation and then develop injects that will utilize those methods during the exercise. Planners must inform leadership to any possible impact to normal operations because of the exercise injects so that leadership can socialize and manage the possible impacts. Additionally, planners must understand the risk to operations if a live network is utilized for the exercise so that senior leaders are informed about possible impacts. This can be complex when working with multiple PNs, but will ultimately provide realistic aspects to an otherwise artificial exercise environment.

Ranges

Many organizations are familiar with the concept of a "range," but associate it with different purposes. A software company's "range" may consist of an integration lab where developers can "play" with the software and test how it functions in different situations. A police squad has a shooting range where officers safely train, maintain, and test proficiency with weapons. Similarly, a cyber range can provide a controlled environment in which organizations can execute cyber exercises without harming a live networks systems or operations.

A cyber range is a controlled electronic computing environment with systems, networks, services, and users generally isolated from a live network. Such a range has a defined baseline that could be physical or virtual with one or more instances configured for a specific exercise scenario. A range can provide access to participants from any nation without depending on the participants' ability to provide their own equipment.

A cyber range can offer an excellent means to demonstrate desirable and undesirable features of an IT environment to a training audience. Such a range is easy to reset and reconfigure, and allows for full use of RT capabilities without disruption of real-world networks and systems. It can allow leadership to ask difficult "what if" questions, discover

where improvements might be needed, or confirm the existing architecture, procedures, or training are adequate.

However, a range may have the drawback of creating unrealistic or artificial settings to which the training audience would not normally have access. As an example, if participants who do not host their own email services are expected to run an email server during the exercise in the range, this can create additional training challenges that may hinder the exercise. This highlights the need to know the training audience.

Threats

Threats may occur naturally or result from human actions. A threat requires a motive and attack vector in order to stimulate the training audience during the exercise. Table 9 outlines some common threats and methods used to simulate threats within a cyber exercise scenario. The more realistic the threats, the better the audience will respond.

Table 9. Common Threats and Methods

Threat	Example	Simulation Method
Natural disaster	Storm causes power failure Earthquake destroys infrastructure	Inject power outage or accident (e.g., toxic chemical spill) that forces staff to evacuate the facility
Ignorant user	User introduces a virus due to poor security practice	Inject internal network scanning, virus alerts, file loss
Malicious internal user	Internal user launches a virus to delete organizational data	Inject internal network scanning, virus alerts, file loss
Hacker	Script kiddy or sophisticated entity gains unauthorized access to data/systems	Inject external network scanning, email phishing, malicious website access, social engineering

Sample Exercise Threats

Table 10 lists a series of malicious activities that an RT could execute during an exercise to assess the training audience's response. This table also demonstrates the mapping of a cyber scenario to the exercise goals and objectives for the training audience. It obviously does not represent a comprehensive list of possible injects. The injects could be executed by an RT or injected by the white cell via "paper card." Exercise planners can find additional concepts for injects by referring to the SANS top 20 or CWE weakness database (see References).

Table 10. Sample Cyber Injects

ID	Title	Description	Objective[1]	Outcome[2]
IA-1	Network virus	The RT sends the training audience a spearphishing email, supposedly signed by the exercise leader, indicating the need to view a webpage for updated exercise information that contains the simulated eicar virus test string. The email is designed to simulate the installation of malicious software and trigger incident reporting.	01, 02, 04, 07, 08, 09, 10, 11	01, 03, 06, 07, 08, 10
IA-2	Network Denial of Service (DoS)	The RT generates an abnormally high amount of network traffic against the training network in order to simulate reduced network capabilities visible in system performance statistics and volume of log data. Additional notification from the training audience about reduced network capability or inability to access website should prompt the incident response process and associated troubleshooting.	01, 02, 03, 04, 06, 07, 08, 09, 10, 11, 12	03, 04, 06, 07, 08, 10
IA-3	Unauthorized computer on network	The RT attempts to connect an unauthorized laptop to the training network to see if it is detected.	01, 02, 04, 07, 08, 09, 10, 11	02, 03, 06, 07, 08, 10
IA-4	Malicious external scanning	The RT executes an external scan of the exercise network to see if it detected. May also be used to facilitate training and education about firewalls and IDS.	01, 02, 03, 04, 06, 07, 08, 09, 10, 11	02, 03, 06, 07, 08, 10
IA-5	Malicious internal scanning	The RT connects a device to the training network and scans the exercise network from an internal location to facilitate training and education about firewalls and IDS.	01, 02, 03, 04, 06, 07, 08, 09, 10, 11	02, 03, 06, 07, 08, 10
IA-6	Computer compromise	Members of the RT walk around and exploit unattended computers with no password screen saver lock by placing a note in the on-screen txt editor that the computer has been compromised and to contact cyber security.	01, 02, 04, 07, 08, 09, 10, 12	02, 03, 06, 07, 08, 10
IA-7	Frequency phishing via email	The RT sends a spearphishing email to the training audience attempting to elicit sensitive information being used in the exercise.	01, 02, 04, 07, 08, 09, 10, 12	01, 03, 05, 06, 07, 08, 10

Exercise Planning Cycle

Not surprisingly, the exercise plan must be coordinated among the appropriate exercise planners and participants. This means that planning should start several months before the exercise is to take place and factor in issues the logistics issues for PNs. Planning and

[1] See Table 2.
[2] See Table 3.

coordinating an exercise takes a significant amount of time, especially if the exercise includes multiple entities within one organization or multiple PNs. All organizations that will participate in the exercise should be involved in developing the exercise plan so that they can provide details about their organization's role in the exercise. This concept is critical when involving multiple PNs with different capabilities, languages or needs.

Concept Development Meeting

Depending on the exercise complexity and style, a concept development meeting (CDM) should take place anywhere from 2 to 12 months prior to the actual exercise. The number of organizations involved in the exercise and the exercise scenario determines the complexity: the more organizations, the more time required for planning.

This CDM should involve the exercise planners from within the lead organization. The senior leaders of the organization must empower these planners to design an exercise that will meet the organization's objectives. The CDM should be an internal meeting to discuss ideas, determine objectives, and decide what other organizations, SMEs, or RTs to include in the initial planning meeting.

This meeting centers on identifying the objectives, participating organizations or PNs, exercise style, scenario, possible locations, and resources needed to facilitate the exercise. The CDM should take the form of an open discussion that reviews the lessons learned from prior exercises, exercise objectives, scenarios, MSELs, and styles in order to shape the concept for the present exercise.

Products of the Concept Development Meeting

- Draft initial exercise scenario (high level)
- Selected style (table top, hybrid, full live)
- Defined exercise objectives
- Defined outcomes
- Identification of additional organizations/PNs to participate in the initial planning meeting
- Identification of logistical needs (location, visa, language, lodging, etc.)
- Identification of possible required resources (range, type of networks, systems, etc.)
- Assigned action items, completion dates, and points of contact (POCs)

Initial Planning Meeting

The initial planning meeting (IPM) should occur 2 to 8 weeks after the CDM. This meeting should include all of the internal and external planners associated with the exercise. In fact, it is crucial that external organizations and or PNs take part in the exercise planning process as early as possible to ensure that all entities understand what is being planned and the level of support expected from each participant.

The IPM starts by reviewing all of the work accomplished in the CDM. This brings all of the exercise planners from external organizations or PNs into the planning process. During this

meeting the participants must review the exercise scenario and objectives to ensure that everyone agrees with the plan.

At the conclusion of the IPM, the lead exercise planner must record a list of action items for each organization or PN so that the exercise planners can be made accountable for the items about which they must provide information. In some cases, these action items may range from developing an exercise scenario to drafting the ROE in concert with various organizations. The planners should avoid significantly modifying the objectives and scenario after this meeting, as these critical documents determine several actions.

Products of the IPM

- Finalized exercise objectives
- Defined exercise scenario
- Develop understanding of the ROE (produced with RT)
- Dates for the follow-on planning sessions and exercise execution
- Comprehensive POC list, including language preference when working with PNs
- Organization/PN planner assigned to oversee the notifications/coordination process with eternal organizations/PNs
- Organization/PN planner assigned to begin coordinating the logistics plan (exercise location, visa, translators, lodging, transportation, physical security, food/water/hygiene aspects of life support, etc.)
- Organization/PN planner assigned to begin coordinating the required resources (range, type of networks, diagrams (see Appendix E: Sample Network Architecture), systems, etc.)
- Assigned action items, completion dates, and POCs

MSEL Planning Meeting

Exercise organizers may need to hold an MSEL planning meeting between the IPM and the mid-term planning meeting (MPM) to clearly define all of the injects needed to support the exercise scenario. This meeting requires attendance from all of the SMEs, RT members, and planners supporting the exercise scenario. At this focused meeting the participants work through the technical and non-technical details of drafting all of the injects – "real" or scripted – that support the exercise scenario.

The most successful MSEL meetings begin with an overview of the exercise scenario and planning documentation from the IPM and of the MSEL and lessons learned from prior events. As the meeting progresses it is critical that the planners outline a series of injects that will drive the objectives of the exercise but not overwhelm the training audience. Planners involved in the MSEL development process must understand the characteristics of the training audience – the capabilities of the external organizations or PNs participating in the exercise – in order to develop meaningful injects.

Products of MSEL Planning Meeting

- Draft of the exercise MSEL
- Refined exercise scenario based on RT capability, realism of the scenario, and anticipated operational risk; especially if utilizing an operational IT environment
- Assigned action items, completion dates, and POCs

Mid-Term Planning Meeting

The MPM should take place 2 to 8 weeks after the IPM. It is essential that the same planners who took part in the IPM participate to prevent misunderstanding, confusion, and changes to the scenario and MSELs. In addition, the required SMEs, RT, and PN representatives should attend the MPM.

This meeting starts with a review of the scenario, updates to the action items assigned from the IPM, review of the ROE, and review of the draft MSEL to ensure all planners have a similar understanding of the exercise. Next, the group must finalize the objectives and the scenario to identify any additional logistical or training requirements for exercise.

During this meeting planners may need to have breakout sessions that focus on each aspect of the exercise and then to have an out briefing with the entire group. As an example, separating the logistics discussion from the MSEL and scenario discussion can improve effectiveness because the topics differ vastly and discussions involving the entire group could become counter productive.

Products of the MPM

- Finalized exercise scenario and senior leader approval briefing
- Finalized understanding of the ROE (produced with RT)
    - In a hybrid or full-live style exercise, the RT will begin preliminary assessments, research, and network/system infiltration after this meeting with a signed ROE.
- Draft exercise logistics plan (suitable location, dates, travel, translators, physical security, transportation, accommodations, equipment shipping instructions, etc.)
- Organization/PN assigned to plan and develop the training materials needed for the training audience (operating environment, procedures, policies, expectations, technical training, etc.)
- Organization/PN planner assigned to continue coordinating the resources required at the exercise location (range, type of networks, diagrams, systems, etc.)
- Organization/PN planner assigned to finalize coordinating the logistics plan (location, visa, translators, lodging, transportation, physical security, food/water/hygiene aspects of life support, etc.)
- Criteria for the GO/NO GO decision on execution of exercise
- Dates for the final planning meeting
- Assigned action items, completion dates, and POCs

Final Planning Meeting

The final planning meeting (FPM) should take place one month prior to the beginning of the exercise. This meeting must include the same planners in addition to all organizations involved to review previous action items and finalize any remaining details of the exercise. Except in highly unusual situations, participants should not introduce new outcomes, or change the exercise scenario or MSEL. The logistics to bring everyone and everything into the right location to execute the exercise as designed pose the most significant challenge at this point.

This meeting starts with a review of the scenario, updates on the action items assigned from the MPM, review of the ROE, review of the MSEL, and review of the logistics plan to ensure all planners have a similar understanding about the exercise. Next, the group must finalize all remaining details for the execution of the exercise. Again, this meeting may function best with breakout sessions that focus on each of the various aspects of the exercise, followed by an out briefing with the entire group.

At this meeting the exercise leaders make the final GO/NO GO decision on the execution of the exercise. The leadership makes this decision on the basis of the criteria established in the MPM. As an example, if an internal conflict in the host country might endanger the exercise participants, planners may elect to find an alternate location or to cancel the exercise. In a less extreme case, participants might be unable to ship the equipment needed to facilitate the exercise to the chosen location, the equipment might be stuck in customs, or might become unavailable at the last moment. In such a case, planners must determine a work around or possibly cancel the exercise.

Products of FPM

- Finalized exercise scenario with senior leader approval
- Finalized ROE signed by appropriate leadership (network owner and RT lead)
    - In a hybrid or full-live style exercise, the RT will continue assessments, research, and infiltration (see Appendix F: Sample Red Team Exercise Data).
- Finalized exercise logistics plan (location, visas, translators, lodging, flight plans, customs/visa letters, transportation, physical security, food/water/hygiene aspects of life support, etc.)
- Finalized training materials needed for the training audience in appropriate languages (operating environment, procedures, policies, expectations, technical training, etc.)
- Finalized resource plan so resources arrive at the exercise location
- Organization/PN planner assigned to finalize coordinating the logistics plan
- Review of any changes that affect the GO/NO GO decision on execution of exercise
- Assigned action items, completion dates, and POCs

Exercise Execution

The ECG oversees exercise execution. During this period the ECG controls the exercise inject releases and interactions with the training audience. The information flow is outlined in Figure 1. Provided the planning process has been thorough, the execution phase is a matter of following the exercise plan and monitoring the training audience responses through the designated exercise observers.

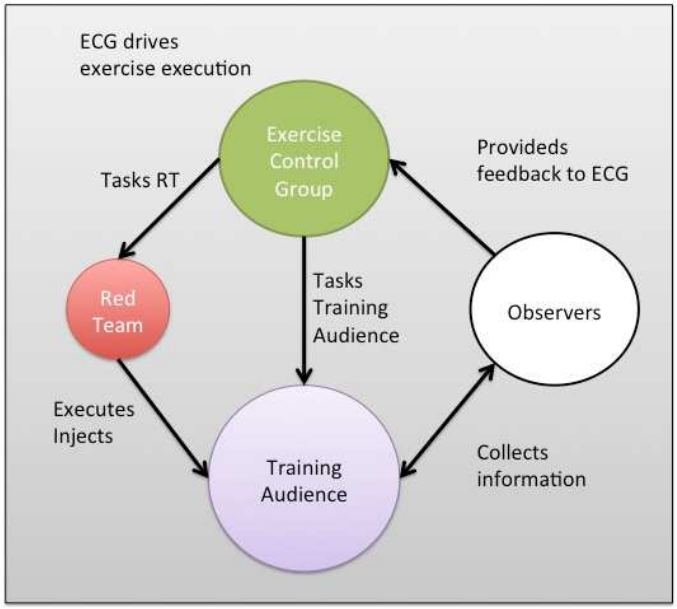

Figure 1. Exercise Information Flow

Inevitably, the exercise scenario and injects will change slightly based on conditions during the exercise; this is a normal occurrence but not a substitute for thorough planning and coordination. Multiple factors may have an impact on the execution of the exercise, most of them related to logistic issues. These challenges are difficult to anticipate, especially depending on the location or nation the exercise is hosted. The Lessons Learned capture some common challenges.

Observation

Observation during the exercise is key to a successful training experience. ECG and RT observations can identify difficulties in how the training audience responds to the exercise scenarios, offers adjustments during the exercise execution, and support deconfliction between real world and exercise injects (see Appendix G: Sample Red Team Event Log).

The ECG should document observations in a pre-defined format and the exercise planners and the training audience should then review them. The observations collected should highlight deficiencies that become apparent to the ECG during exercise execution. This information will allow the organization to assess its deficiencies and implement a plan to improve its readiness. Appendix H includes a sample observation format.

Each inject to the exercise presents an opportunity to assess, teach, and learn with the training audience. Often a feeling of "us against them" may arise during the exercise. This concept can prove toxic to the exercise and must be dispelled. The RT motto is "we win, we lose," meaning that if the RT succeeds the Blue team has missed the mark and the organization must work to improve its processes. Exercise observers fill a critical role in bridging this gap between the training audience and the ECG/RT. The feedback provided by the observers can identify significant challenges the training audience experiences and offer an opportunity to address problems in real time during the exercise (see Figure 2).

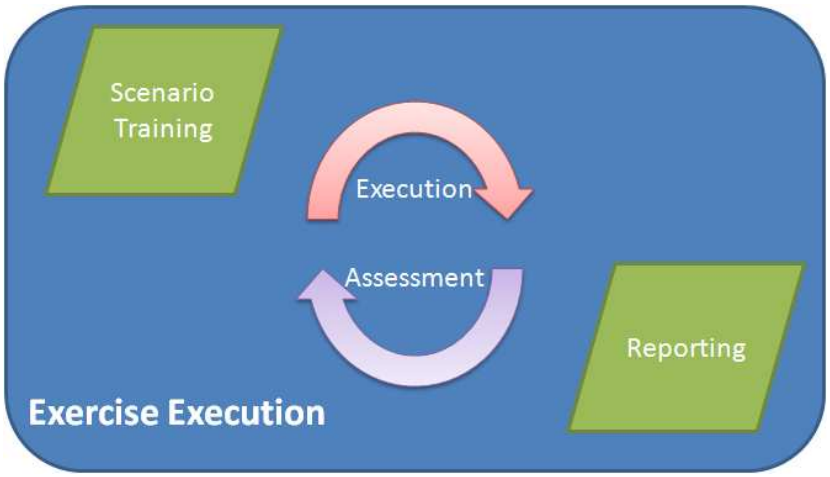

Figure 2. Exercise Observation Cycle

Observation Scenario

As an example scenario, the ECG tasks the RT to execute inject IA-5: an external port scan against the systems on the network. The ECG expects the training audience to detect, report, and if necessary react to the inject based on the exercise incident response plan. During the execution of the inject observers see no reaction from the training audience: no reporting or discussion occurs about the activity and the Blue team makes no entries in the audience master station log (MSL in Appendix I). The observers must report this critical feedback to the ECG and RT to determine how best to guide the training audience to achieve maximum value from the exercise. As a resolution the RT and ECG might agree that an RT member or skilled observer should provide hands-on mentoring with the training audience on the use of the firewall and IDS logs. The ECG and RT would execute a similar inject later in the exercise to reaffirm the lessons of the on-site mentoring.

This type of intervention may go against traditional views about RT/observer involvement in the exercise. However, it can provide valuable learning that could not have taken place in another forum.

Post Exercise

Given the significant amount of resources applied toward the exercise, the organization must collect information from exercise participants, observers, the RT, and the ECG to strengthen future exercises. Three main vectors are used to acquire this data.

RT and observer observation forms completed throughout the course of the exercise help retell the story of what actually took place. These observations not only capture the detailed responses to injects during execution and allow modification of the exercise direction during execution, but also provide lessons learned after the exercise.

The hotwash should occur on site while events remain fresh in the participants' memories, and should involve all who participated in the exercise, from the training audience through the ECG. It provides immediate feedback and serves as a good forum for senior leaders to discover the key successes or focus areas for future exercises. The hotwash session should be led by a moderator and consist of a focused discussion on what worked well, what must improve, and what the organization should consider for the next exercise. Additionally, the moderator could distribute a survey consisting of a series of yes/no questions about aspects of the exercise and free-form fields to capture feedback. In exercises involving several nations, all documents and discussions may have to be in multiple languages to meet the needs of the environment.

Exercise planners should write the AAR within 21 days. The planners should then review it to capture the lessons learned and to shape the desired outcomes for the next exercise. As an example, if the training audience responded too quickly and effectively to many injects, the following year's scenario might be more complex and the RT might use more advanced techniques. Alternatively, the AAR may also prove that injects were too complex for the intended audience and must be scaled down for follow-on exercises. These lessons will directly influence the outcomes for future exercises and must consider the specific training audience.

The AAR, in conjunction with the observation logs, will become the record of activities from the exercise. Appendix J provides a sample AAR format.

Lessons Learned

The ECG should document the knowledge gained from the exercise, both bad and good, as lessons learned. The lessons learned should capture and account for the different approaches to "security" across exercise participants. The results of an exercise often expose successful techniques or deficiencies within the organization's IA program that can be built upon or improved.

Exercise scenarios provide the opportunity to discover an organization's deficiencies within a controlled environment. Organization leadership must then create remediation plans and follow up on deficiencies identified during the exercise. Conversely, exercises can also highlight those processes, capabilities, etc., that proved highly effective.

Exercise Planning Pitfalls

During the planning and execution of the exercise, organizations also collect lessons learned about the exercise itself and gain valuable information on how to improve the planning and execution for future exercises. Organizations must avoid multiple pitfalls during the development of cyber exercise goals and scenarios. The main source of consternation comes from the possible impact on real-world activities (or on the main exercise scenario if the cyber scenario supports a larger organizational exercise, as noted in

Exercise Planning). Planners can overcome many of these pitfalls if they ensure that proper planning and socialization take place in relation to the cyber scenario of the exercise.

Table 11. Common Cyber Exercise Pitfalls

Situation	Impact	Resolution
Cyber scenario objectives not clearly defined.	Senior leaders and exercise planners may not be willing to allow certain injects that could affect another, broader exercise, thus limiting the ability for real RT activities.	Ensure the cyber exercise scenario ties to the broader exercise scenario with multiple options for executing an inject to facilitate the cyber scenario if leaders do not allow RT play.
Rules of engagement not clearly defined.	The RT may access/execute activities outside the scope of the exercise or cause unplanned impacts.	Ensure that the scope of systems/targets/methods is clearly defined for the RT ahead of the exercise.
Reduced awareness due to Senior leaders not involved in planning.	Leaders often resist actions that "may impact the exercise."	The cyber exercise scenario must be clear enough for senior leaders to understand what will/not be affected during the exercise and the mediation plan.
Training audience apathetic or not responding to injects.	Cyber exercise training objectives will not be met, or information needed from an inject will not be available to stimulate other aspects of the exercise.	Ensure that the cyber exercise scenario is clearly defined, realistic, documented, purposeful, and in line with the technical capabilities of the training audience and is endorsed/encouraged by senior leadership.
Cyber injects are not executed as planned.	Cyber exercise training objectives will not be met, or information needed from an inject will not be available to stimulate other aspects of the exercise.	Ensure that the injects are appropriately spaced out to account for reaction time; in addition, plan multiple methods for executing critical injects.
Training audience fights against scenario instead of acting as a willing participant.	Cyber exercise training objectives will not be met, or information needed from an inject will not be available to stimulate other aspects of the exercise.	The ECG must make certain that the scenario is realistic and engaging, and that the training audience understands that the exercise represents an opportunity to learn. It is NOT a test or exam: it is a training opportunity to determine where to focus additional efforts.
RT inability to deconflict exercise inject versus real world activity in a timely means.	An entire exercise can be derailed if there is not a positive means of control and information exchange between the RT and the Exercise control group.	Ensure that the RT tracks their activities thoroughly and is able to provide deconfliction within 30min of their activities vice other activities that may occur on a real network.

Exercise Logistical and Technical Considerations

Throughout the course of the exercise multiple issues may arise related to logistics and the reliance on technology. The particular problems experienced may affect the execution of the exercise or real world operations depending on the availability of alternate options. Organizations should consider many of these items in the planning process, taking the location and scope of the exercise into account. Thus, organizations should:

- Establish a primary and secondary communications and logistics plan.
- Ensure safeguards are in place prior to executing malicious activity on any network
    - RT deconfliction process is functioning with ECG.
    - Proper coordination/training must be done on handling malware.
- Compensate for issues with proper power – voltage, phase (1,2,3), adapters, or cables – and communications capabilities.
    - Leased/local communications are not always available or reliable and cannot be the primary means of communication.
    - Wi-Fi hot spots can be invaluable if service exists.
    - Participants' cell phones may be locked or unable to use the local cell network.
- Ensure consideration of contingencies/failures of equipment.
- Take all necessary software on CD/USB drive; bandwidth may not be available or site s may be blocked for downloading (see Appendix K Software Tools).
- Carry spares of everything from cable/fiber termination kits, SIM card cutters, repair kits spare parts, power generation, etc.
- Plan on taking everything participants may need because local purchases are expensive or items may not be available

Conclusions

An exercise presents an opportunity to explore an organization's "what-if scenarios." From a cyber perspective, it allows safe execution of the real-world scenarios that concern security experts. The results may identify where an organization should improve or may reaffirm the adequacy of existing architectures, procedures, or training. Table top, hybrid, or full live exercises involving network attack can allow an organization to assess its own security posture and the ability of the training audience to defend mission-critical data and enable the organization to respond more effectively to real-world incidents when (not if) they occur.

The training audience, planners, observers, and RT must work together and understand that all parties benefit from the exercise experience. Exercises are not performed to make an organization look bad; instead, they help to train and equip the organization for dealing with inevitable malicious activities. They allow a friendly force to pose as a threat and report how and what techniques it utilized to attack a security posture. All parties benefit from an exercise that underscores the RT motto: "we win, we lose.

Appendix A: Sample Master Scenario Event List

The MSEL contains all injects for the exercise scenario and is used to ensure timely and organized execution of injects (see Figure 4).

ID	Local Time	Delivery Method	Target	Title	Description	Assumptions	Notes	Expected Actions	Measuer of Performance
IA-5	8:50	Email	All	Urgent Message for Leadership	You just received an email from a @yahoo.com address with the SUBJECT LINE of "URGENT MESSAGE for Exercise Leadership." The Email requests that you access the following link to download a file containing important information. Http://172.16.1.75	If you received this by hand then you can simulate accessing the link by typing it into your internet browser.	The file is suppose to simulate a file that contains a virus.	The Recipient should not access the link without verifying its authenticity	Incident report completed in accordnace of response plan
IA-9	9:00	RT	Net	Malicous External scanning	The RT will try and do a external scan of our ntetwork	FW will block all SCAN attempts	Inform observers once inject is kicked off	The IA team will notice the scan, see it is blocked and do a report	Incident report completed in accordnace of response plan
SE-4	10:30	Phone	Card	Missing Person	The United Nations received a call about a missing person in the exercise AOR. Last sighted 10 miles east of the training area.			Notionally order all available units to search around the last known location	
EV	16:30	N/A	All	Daily Hotwash	Event Item Only - No Inject				
IA-13	TOO	RT	All	Computer compromised	The RT will attempt to locate a computer no password screen saver lock he will write a word doc that the computer has been compromized	Event is a target of opportunity by RT	Inform observers once inject is kicked off	The offending user should notify seucirty their and report and remediale training done	Incident report completed in accordnace of response plan

Figure 3. Sample Master Scenario Event List

Appendix B: Sample Exercise Incident Response Plan

Exercise Incident Response Plan [1]

As the complexity and connectivity of an information system and the associated risk for this system increase, organizations must establish procedures for reacting to any incidents affecting their information systems. Table 12 lists the types of incidents, the reporting requirements, and processes to be utilized during the exercise. The table divides security incidents into three categories, based on their severity and possible impact on the exercise.

Table 12. Sample Incident Response Categories

Category	Reportable Incident/Event	Time to Report
1	Any attacks affecting critical assets Denial-of-Service attacks that isolate or impede critical service or network performance Malicious logic (virus) attacks that isolate enclaves Administrator/root-level access obtained by unauthorized personnel	Within 30 minutes
2	Significant trends suspected in incidents or events Indication of multiple suspected systems Suspected e-mail spoofing Unauthorized probes or scans of the network	Within 1 hour
3	Unusual system performance or behavior Unplanned system crashes, outages, or configuration changes Suspicious files identified on a server Missing data, files, or programs Unexplained access privilege changes Poor security practices Unusual after-hours system activity Simultaneous logins by the same user from different IP addresses Unauthorized activity by privileged users Malicious logic (virus)	Within 2 hours

[1] Incident response plan adapted from the Africa Endeavor 2013 Handbook

Reporting Procedures

The exercise training audience should report security incidents or suspicious activity to their security representative utilizing the incident reporting form. As incidents are resolved, the security representatives should update the report and master station log appropriately. The security representatives should review events, perform analysis, develop responses, and provide reporting for the event to the ECG.

Incident Response Process

1. Upon detection the user will disconnect the computer from the network.
2. The user will contact his/her security representative.
3. The security representative will complete the Incident Response form with the user and provide it to the cyber security team with a copy to the leader of the exercise.
4. The cyber security team will perform research to identify the source and level of threat before authorizing the security representative to proceed.
5. The security representative may remove the threat once approved by the cyber security team.
6. The security representative will finalize reporting in coordination with the cyber security team.

Appendix C: Sample Incident Response Form

EXERCISE XXXX INCIDENT REPORT FORM [1]

1	**Date/Time**	
2	**Name/Organization**	
3	**Contact Information**	
4	**Location of system**	
5	**Type of Incident** **(Denial of service, Virus, Unauthorized access)**	
6	**System(s) involved**	
7	**How incident was detected**	
8	**Addition Details**	

[1] Incident response form adapted from the Africa Endeavor 2013 Handbook

Appendix D: Sample Exercise Roles and Responsibilities

Training Audience User Role Responsibilities [1]

- Do not use a computer to harm other people or their work.
- Do not use or copy software that is not approved for the exercise network.
- Do not steal other people's intellectual property.
- Do not use a computer to pose as another person.
- Do not use other people's computer resources without approval.
- Do not send sensitive information over data (email, sms) or by voice (phone/radio) unless it is secured.
- Do not use media received from unknown sources.
    - All media will be scanned for virus on a stand alone system prior to usage.
    - Every USB drive must be checked by the cyber security team.
    - CDs will be used only by the cyber security team.
- Choose a password that is 12 or more characters in length
    - Your password should be a mixture of at least 1 uppercase, at least 1 lowercase, at least 1 number, and at least 1 special character.
        - Example: 7Uj@3As!1Rt&
    - Use alphanumeric combinations or phrase associations to create passwords that are easy for you to remember, and hard for others to guess.
    - Avoid using words or phrases that can be found in a dictionary in any language.
    - Do not use personal information such as the names or birthdays of family members, pets, color, sports teams, or places when creating your password.
    - Once you have created your password, memorize it and do not write it down or share it with others.
    - Change your password on a regular basis.

Users who discover information security incidents will report using the form specified below to their designated security representative.

[1] Roles and responsibilities adapted from the Africa Endeavor 2013 Handbook

Training Audience System Administrator Role Responsibilities

In addition to the user responsibilities, an administrator must also ensure that all reporting and remediation are completed in accordance with the incident response policy.

- If you think that you have encountered malware, a phishing email, or anything else out of the ordinary on your information system, contact the technical or security representative.
- Complete the Incident Response Form promptly and accurately.
  - If the incident cannot be confirmed a cyber security team member will be dispatched to the location of the device to confirm the incident and fix the issue if possible.
  - A security officer will compile reports and determine if the incident requires reporting to the ECG.
- Update firewalls, IDS, anti-virus software, and other services as required.

Appendix E: Sample Network Architecture

Exercise planners and SMEs should modify the notional network architecture shown in Figure 3 to meet the needs of the exercise scenario. This example shows multiple internal enclaves that connect to the Internet through one centralized point with firewall, IDS, and proxy server. This architecture allows for adequate inject execution to support the scenario of the training audience and provides for sustainment of the exercise as well as the cyber exercise training objectives.

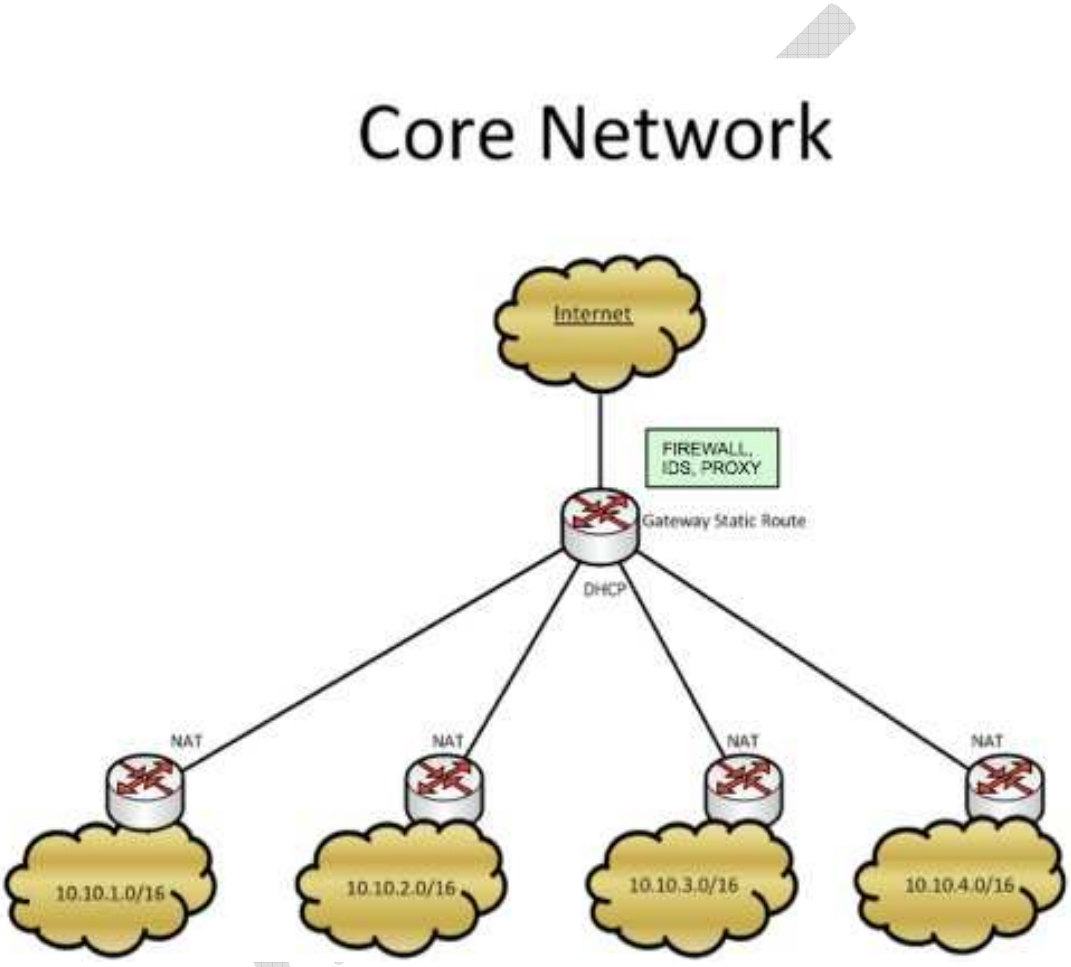

Figure 4. Sample Network Architecture [1]

[1] Network architecture adapted from the Africa Endeavor 2013 Handbook

Appendix F: Sample Red Team Exercise Data

Various types of information are critical to collect during the exercise and for reporting purposes after the exercise. The ECG can use everything from email messages, screen capture, and system logs c to help educate the exercise audience and generate a better final report.

Email Address List

exerciseleader@yahoo.com -account used to send spearphishing email from

unita@yahoo.com - email account for Exercise Unit A

unitb@yahoo.com - email account for Exercise Unit B

IP addresses for Exercise

172.16.11.66 – Network gateway IP

172.16.11.75 – Malicious laptop for RT

192.168.1.254 - Internal firewall

Logs from web server

Access logs:

172.16.11.70 - - [13/Aug/2013:10:57:29 +0200] "GET / HTTP/1.1" 304 -
172.16.11.70 - - [13/Aug/2013:11:06:35 +0200] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)"
172.16.11.70 - - [13/Aug/2013:12:19:50 +0200] "GET / HTTP/1.0" 200 109 "-" "-"
172.16.11.70 - - [13/Aug/2013:13:00:35 +0200] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)"
172.16.11.70 - - [13/Aug/2013:13:08:24 +0200] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0

Logs accessing the contaminated zip file

172.16.11.70 - - [13/Aug/2013:14:25:28 +0200] "GET /reports/water_report.zip HTTP/1.1" 200 184 "http://172.16.11.75/water_report.html" "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)"
172.16.11.70 - - [13/Aug/2013:14:35:28 +0200] "GET /reports/water_report.zip HTTP/1.1" 304 - "http://172.16.11.75/water_report.html" "Mozilla/5.0 (compatible; MSIE

Initial Spearphishing email: Site Introduction Email (non malicious)

ALCON:

Please take a moment to review the news reporting from the “exercise times website” website about media updates on the exercise situation.

S'il vous plait prenez un moment pour examiner le " exercise times website" au sujet des mises a jour sur la situation d’exercice.

http://172.16.11.75

Cheers/Merci

CDR

EXERCISE EXERCISE EXERCISE

Water contamination report spearphishing (malicious link to website)

ALCON:

Please take a moment to review the water contamination report due to the situation.

S'il vous plait prenez un moment pour examiner le rapport de la contamination de l'eau à cause la situation.

http://172.16.11.75/water_report.html

Cheers/Merci

Commander

EXERCISE EXERCISE EXERCISE

Appendix G: Sample Red Team Event Log

Tables 13 and 14 outline sample reporting of the activities conducted by the RT during the course of the exercise. The RT should keep a log of all activities during the course of the exercise to provide deconfliction and status of injects for the exercise control group (ECG).

Table 13. Sample Red Team Event Log Day 1

Time	Activity	Notes	Comments
0900	Began external network scanning	Source IP 172.16.11.75 Target IP 1721.6.11.70; SMTP is open on the firewall	
1000	Introductory spearphishing email	Email from fake email address exercisecommadner@yahoo.com introducing a legitimate news paper for reporting on the notional scenario	Non malicious email – builds trust
1030	Physical security checks	Walk around exercise site(s) for looking for weaknesses or possible exploitation avenues	Computer screens not locked when unattended, server room not secured
1039	Email response received	Training audience confirmed email receipt	Valid address and relationship
1405	Malicious spearphishing email	Email from exerciseleader@yahoo.com to view a webpage for updated water contamination information that contains the eicar embedded test virus to simulate the installation of malicious software and trigger incident reporting	
1420	Email response	Training audience responds to email notice and viewing information	Check web server logs
14:25	Eicar download	Apache logs show that the training audience downloaded the simulated virus.	
1448	Email response	Training audience responds about the spearphishing email on water contamination containing a virus	This is good, but the incident response process was not executed
1511:11	Eicar download	Apache logs show that the training audience downloaded the simulated virus.	

Table 14. Sample Red Team Event Log Day 2

Time	Activity	Notes	Comments
0840	Executed spearphishing email	Email from exercisecommadner@yahoo.com with the updated webpage reporting link	
0850	DOS attack	Began DOS attack by reducing network port to 10MB and executing large packet ping attack against the firewall	Performed mentoring with training audience to identify and outline attack and response options
0945	Ended DOS attack	Per cyber lead	Activity was identified by training audience
1030	Radio Frequency phishing via email	Email from exerciseleader@yahoo.com with an urgent request to provide current radio frequencies being used because of recent changes	This was after the training audience was educated about the possible spearphishing taking place
1045	Unauthorized device on network	A laptop was successfully added a Unit A network without question from training audience	Can use this later for internal scanning
1130	Internal network scanning started	Internal network scanning – not detected in the firewall	
1147	Email Response	Unit A replies that they received the email, but does not provide frequencies	This was after the training audience was educated about the possible spearphishing taking place
1440	Email Response	Unit C replies with radio frequencies	Force radio frequency change due to compromise

Appendix H: Sample Inject Observation Form

This appendix shows a sample observation form outlining the important types of information to collect for each event/inject executed during an exercise. These are created prior to the exercise and utilized during the exercise to assist observers in accurately assessing the training audience's responses to exercise injects.

INJECT OBSERVER FORM [1]

CONTROL AND OBSERVER EYES ONLY

Inject Number: IA-2 Inject Title: NETWORK VIRUS	Inject Date: 25JUN2014 START TIME (Local): _____ COMPLETE TIME (Local) _____

Observer Name: Jane Doe	Inject Delivered Via: CARD or ELECTRONIC	Target Group/Unit/Position: Unit A

Inject description, ASSUMPTIONS and references:

Your antivirus SW has just alerted a virus. Take appropriate actions in accordance with standard policies and procedures. Notify the Exercise Observer when you have completed all required actions.

Assumptions: Simulated virus triggers user anti virus software on device

References: (Source or document that states required actions)

Cyber Ops & IA; Cyber Incident Management Guide; (page 27-28)

Expectation:

"(e) Each virus incident must be reported as soon as possible to Cyber Security Team. The Cyber Security Team will then issue a virus warning to the other units the unit's appointed senior communications officers if necessary.

Assessment of training audience response: *CIRCLE ONE*

COMPLETED: (3) PART COMPLETE: (2) INCOMPLETE: (1) N/A (Explain Below):____

Was event documented in Master station log? Yes / No
Was incident response form completed? Yes / No

Observation and notes:

[1] Inject observer form adapted from the Africa Endeavor 2013 Handbook

Appendix I: Sample Master Station Log

The training audience uses the master station log (MSL) to track all of the events reported during the exercise. As an example, the information assurance team would maintain a MSL to log all incidents or activities reported by the training audience during the course of the exercise.

MASTER STATION LOG [1]

Date/Time	Exercise Impact Yes/No	Description of Event	Action Taken	Initials

[1] Master station log adapted from the Africa Endeavor 2013 Handbook

Appendix J: Sample After Action Report

This AAR concludes the XYC Exercise 2014. This report captures the areas to continue utilizing for future exercises (Sustain) and areas that should be reviewed to better meet training objectives (Improve)

Sustain.

(1) Issue: Cyber response and threat training.

Discussion: The Cyber Security team conducted thorough and accurate threat information about exercise and real world threats ensuring the training audience was well prepared for the exercise mission.

Recommendation: Continue aggressive cyber preparations for all exercise scenarios to ensure training audience awareness.

(2) Issue:

Discussion:

Recommendation:

Improve.

(1) Issue: Realism of the spearphishing attempts.

Discussion: The spearphishing emails that were attempted during the exercise did not tie into the scenario and were unsuccessful in eliciting responses from the training audience.

Recommendation: Ensure that future spearphishing injects are tightly coupled to the exercise scenario, utilizing information form the exercise, are free of typographical errors and have accurate language translation.

(3) Issue:

Discussion:

Recommendation:

Appendix K: Software Tools

Multiple well-known and tested freeware and open-source scanning tools are available to conduct cyber aspects of an exercise. Organizations can ensure the safety of open-source and freeware tools by downloading these tools from known sources, observing their functions in laboratory conditions, or comparing published signatures to the computed hash code of each tool. The items mentioned below do not represent an exhaustive list of recommended or approved tools.

Curl (http://curl.haxx.se/) – an open-source command line tool for transferring files with Uniformed Resource Locator (URL) syntax.

Google (http://www.google.com) - an Internet search engine. Google attempts to catalog the Internet contents through its crawling technology.

Httprint (http://net-square.com/httprint/) – a web server fingerprinting tool. It relies on web server characteristics to accurately identify web servers, despite the fact that they may have been obfuscated by changing the server banner strings, or by plug-ins such as mod_security or servermask. Httprint can also be used to detect web enabled devices that do not have a server banner string, such as wireless access points, routers, switches, cable modems, etc. Httprint uses text signature strings; it is very easy to add signatures to the signature database.

Mozilla and Firefox Web Browsers (http://www.mozilla.org) – freeware Web browsers used to manually browse and inspect the Web application and associated forms. The Mozilla cookie manager is especially useful in viewing the values of cookies to ensure that they were randomly generated from one session to the next.

Netcat (http://packetstormsecurity.nl/UNIX/netcat/) – an open source utility which reads and writes data across network connections, using Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Nmap (http://www.insecure.org/nmap/) – a free open-source utility for network exploration or security auditing through UDP and TCP port scanning. MITRE uses Nmap to scan large networks rapidly. Nmap uses raw IP packets to determine which hosts are available on the network, what services (i.e., application name and version) the hosts offer, what operating systems (OS) and OS versions they run, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Nikto (http://www.cirt.net/code/nikto.shtml) – a free open-source, command-line, Web server scanner which is used to perform comprehensive tests against Web servers for multiple items, including over 3100 potentially dangerous files, Common Gateway Interfaces (CGIs), versions on over 625 servers, and version specific problems on over 230 servers. Nikto is not designed as an overly stealthy tool and will test a Web server in the shortest time span possible. The nikto scan is an aggressive scan and the developers of this scanning tool warn users that the nikto scan can crash un-patched or mis-configured servers.

Openssl (http://www.openssl.org/) – an open source library that provides cryptographic functionality to applications such as secure Web servers.

OpenVAS (https://www.openvas.org/) – an open source vulnerability scanner and management framework.

Burb (http://portswigger.net/burp) – a local web proxy tool used to evaluate the security of Web applications. Through Burp's proxy nature, all Hyper-text Transmission Protocol (HTTP) and Hyper-text Transmission Protocol-Secure (HTTPS) data between server and client, including cookies and form fields, can be intercepted and modified.

SLAX (https://slax.org/) – a small bootable Unix instance, useful tool to host webpages, relay email, spoof DNS, DHCP and other network services.

SSLDigger (http://www.foundstone.com/) – provides a GUI to a freeware tool used to assess the strength of Secure Socket Layer (SSL) servers by testing the supported cipher.

Stunnel (http://www.stunnel.org/) – an open source program available on both UNIX and Windows that allows you to encrypt arbitrary TCP connections inside SSL.

Wireshark (http://www.wireshark.org) – a popular network protocol analyzer. It has a rich and powerful feature set, and runs on most computing platforms including Windows.

Zentyal (http://www.zentyal.org/) – an Ubuntu Linux based Zentyal Server offers a drop-in Linux replacement for Microsoft Small Business Server™ and Microsoft Exchange Server™ with security features to include Firewall, Web Proxy, Intrusion Detection System.

Appendix L: References

Papers

CJCSM 3500.03D Joint Training Manual for the Armed Forces of the United States 15 August 2012

CJCSI 6510.01F Information Assurance (IA) and Support to Computer Network Defense (CND) 10, October 2013

CNSSI No. 4009 National Information Assurance Glossary 26 April 2010

DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT) 12 March 2014

JP 3-0 Joint Operations, 11 August 2011

JP 6-0 Joint Communications Systems, 10 June 2010

NIST SP 800-53, 800-61, SP 800-84

NISTIR 7298 Glossary of Key Information Security Terms May 2013

NIST National Initiative for Cyber security Education September 2012

Africa Endeavor 2013 C4I Handbook

Web Resources

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

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

http://www.dtic.mil/doctrine/training/cjcsm3500_03d.pdf

http://technet.microsoft.com/en-us/library/cc723507.aspx

http://cwe.mitre.org/data/index.html#release_notes

http://www.mitre.org/sites/default/files/pdf/05_1135.pdf

http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

http://idart.sandia.gov/index.html

http://www.sans.org/critical-security-controls

http://stormsecurity.files.wordpress.com/2010/01/guide-for-designing-cyber-security-exercises.pdf

http://www.tisn.gov.au/Documents/Cyber+Storm+II+Final+Report.doc

http://www.webroot.com/us/en/home/resources/articles/pc-security/computer-security-threats

Appendix M: Acronyms

AAR	After Action Review
CDM	Concept Development Meeting
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CNSSI	Committee on National Security Systems Instruction
ECG	Exercise Control Group
DOS	Denial of Service
FPM	Final Planning Meeting
IA	Information Assurance
IPM	Initial Planning Meeting
MPM	Mid-term Planning Meeting
MSEL	Master Scenario Event List
NISTIR	National Institute of Standards and Technology Internal Report
PN	Partner Nation
POC	Point of Contact
ROE	Rules of Engagement
RT	Red Team
SME	Subject Matter Expert
TOO	Target of Opportunity