Telecommunication
Development Bureau (BDT)

Ref. BDT/IEE/CYB/DM-045

Geneva, 15 May 2015

- Administrations of ITU Member States of the AMS region
- ITU-D Members of the AMS region
- Regional and International Organizations

Subject: **Regional Forum on Cyber Security and Third Cyberdrill Applied Learning for Emergency Response Team for the America Region, Bogota, Colombia, 3-6 August 2015**

Dear Sir/Madam,

We are pleased to invite you to participate in the **Regional Forum on Cyber Security and the Third Cyberdrill Applied Learning for Emergency Response Team for the America Region (ALERT).**

The event will be held from 3 to 6 August 2015 in Bogota, Colombia, at the kind invitation of the Ministry of Information, Technology, and Communications of Colombia and The Colombian Chamber for Informatics and Telecommunications (CCTI). The University of Los Andes, which will be providing the venue, is also providing support and collaboration. The attached annex contains detailed information concerning the Cyberdrill.

The Forum sessions will discuss, among other things, the regional situation and perspectives as well as child online protection, and will also gather viewpoints of the public and private sectors, academia, etc. The Forum will benefit from the participation of regional institutions, experts from different parts of the world, several technical sessions, and additionally the Third Cyberdrill Applied Learning for Emergency Response Team.

We request your participation with a delegation of at least two Cybersecurity professionals of your National Computer Incident Response Team (CIRT). Please consider including in your delegation an expert at decision-making level, since regional support, collaboration and the establishment of an agreement for cooperation and teamwork between the CIRTs of the region will be discussed during the event.

Through the Forum and the third Cyberdrill we aim to encourage cooperation between National CIRTs of the region, to provide capacity building, and to offer scenarios for the analysis of real cases of cyberattacks to inspire teamwork and to improve the incident response effectiveness of the teams. The Forum will establish an agreement between the participating national CIRTs to ensure continuous efforts in achieving regional and global cybersecurity.

To participate, please register on-line using the link available at http://www.itu.int/go/regitud, **no later than 24 July 2015**. Concerned participants are strongly advised to take care as early as possible of your entry visa to Colombia as the approval procedure could take some days and you may be requested to present, to the Colombian Embassy/Consulate in your country, an invitation letter from the Ministry of Information, Technology, and Communications of Colombia.

International Telecommunication Union • Place des Nations • CH-1211 Geneva 20 • Switzerland
Tel: +41 22 730 5111 • Fax: +41 22 730 5545/730 5484 • E-mail: bdtmail@itu.int • www.itu.int/itu-d

Additional information about the event such the agenda and practical information will be available online at the event's web page:

http://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2015/0803-CO-cyberdrill.aspx.

Should you require any further information, Mr Pablo Palacios (ITU Area Office Chile, Pablo.Palacios@itu.int, phone numbers: +56 2 2632 6134 I +56 2 2632 6147), is at your disposal.

Yours faithfully,

Brahima Sanou
Director

Annex: Information of the Cyberdrill ALERT.

ANNEX

Cyber Drill

Table of Contents

Drill Execution

The cyber drill exercise will be based on a fictitious scenario to gauge the CERT incident handling capability. The exercise is structured around a scenario that included several incidents involving the most common types of attacks. The attack details will be sent by the ITU Expert Team recognised as "organiser" to the participants in the form of e-mails. The participant needs to perform their investigation/analysis on the incident and come out with the mitigation solution. The participant is required to submit the solution in the advisory report format back to the organiser email.

Steps

1. The drill scenario commences with all participating teams receiving an email from the **organiser** on an incident
2. The email will contain:
    a. Scenario
    b. Advisory report template
3. Drill **players** need to perform analysis on the incident and come out with the mitigation solution
4. Drill **observers** in the team can assist the main drill player in performing the incident analysis
5. **Participants** need to submit the mitigation solution or recommendation based on the given advisory report template back to the organiser via email
6. **Organiser** will then send an acknowledgement of the email to the participants.

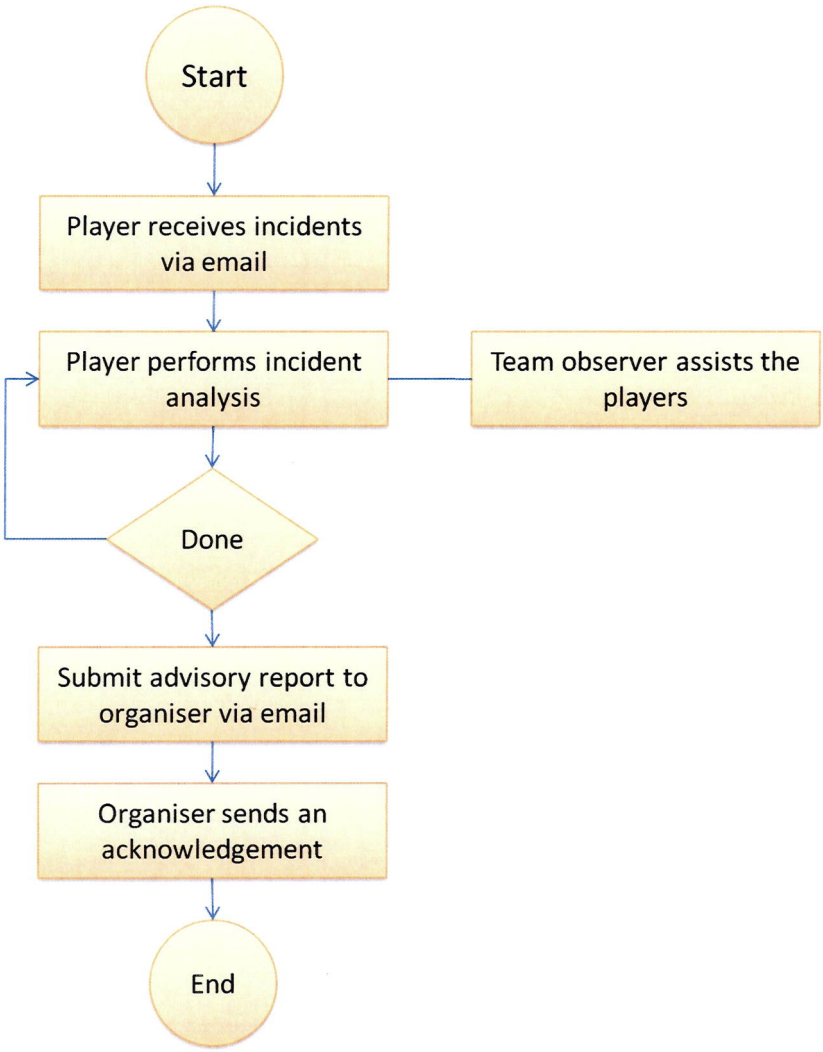

Figure 1: Drill Execution Flowchart

Drill – Do's and Don'ts

Do's

- Participants can use their own software tools
- Participants can use Google or any other reference website to search for information
- Participants can communicate with other participant teams via IRC channel
- Participants can seek assistance from the organiser via IRC channel

Don'ts

- No malicious activity is allowed that can cause harm to the network such as Scanning, Sniffing, DOS or any attempt to attack the drill infrastructure (e.g. IRC Server, Web Server)
- No misuse of internet is allowed

Drill Communications

Mail Server	All formal communications between the organiser and participants will go through this mail server
IRC Server	Will be used for: • Informal communication between organiser, participants and observer • Channel for participants to ask questions or tips on the scenario • A quick notification purpose from the organiser • Collaborate with other participating CIRT teams as well as the organiser
DNS Server	Local DNS server

Drill Setup

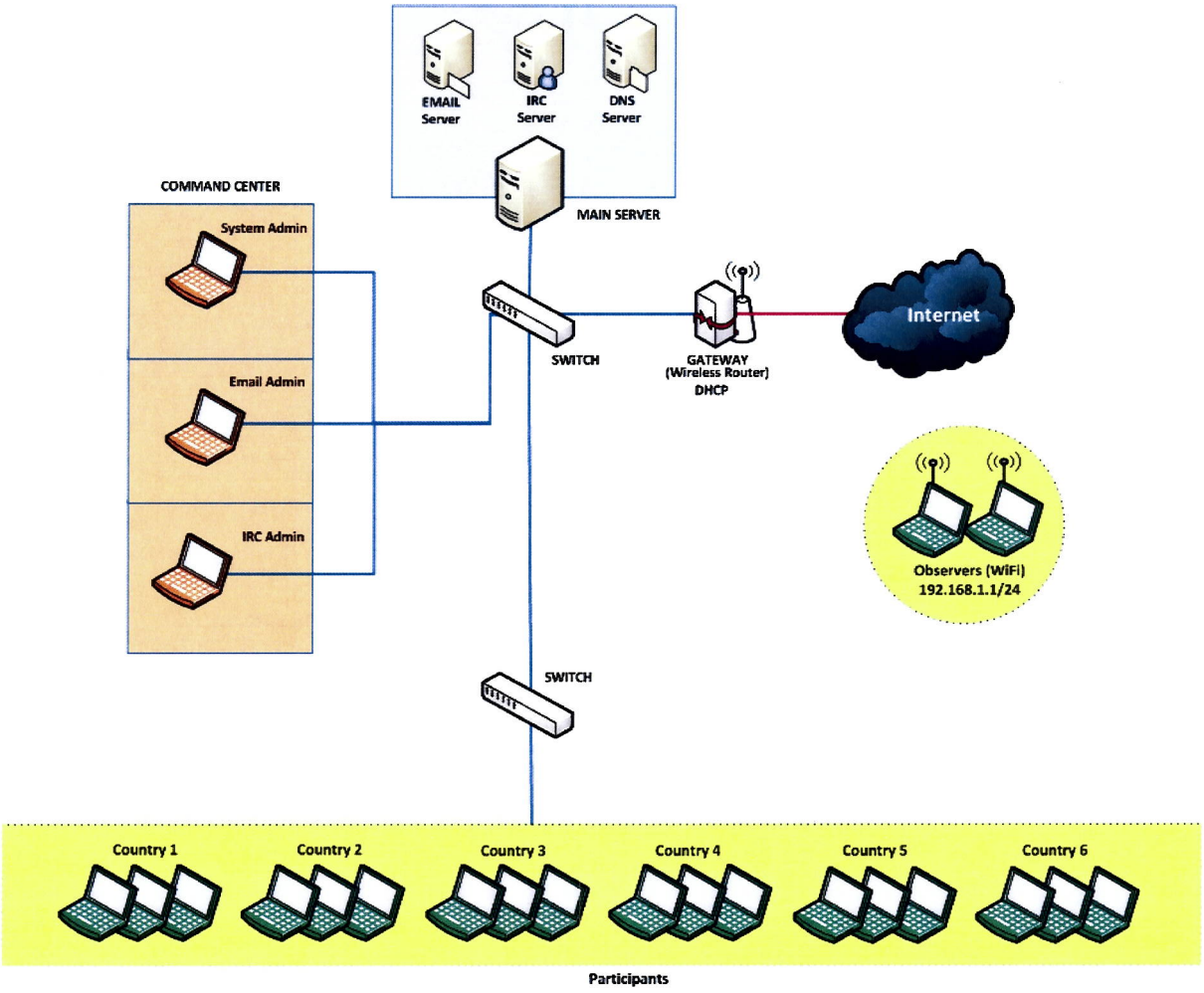

Figure 2: Drill Set Up

Participants – Roles & Responsibilities

Player	• Perform incident analysis on the scenario and send mitigation solution or recommendation based on the given advisory report template back to the organizer • . Main areas in which the participants should have knowledge in: o Familiar with Linux OS and command line o Familiar with Windows OS and file system o Packet sniffing tools o Mobile malware analysis tools o Log analysis tools o Basic knowledge in text encoding and decoding o Basic knowledge of network security o Good understanding of cyber attack techniques
Observer	• Observe and assist the players in his team during the drill

Organiser – Roles & Responsibilities

Drill Director	• Overall co-ordination with the drill experts and participating countries
Drill Facilitator	• Manage the cyber drill by co-ordinating the activities of the drill experts and participating countries • Assist participants during the cyber drill • Guide the teams through the scenarios during deployment for the cyber drill • Present summary of the cyber drill to participants
Drill Manager	• Drill administration and coordination for the cyber drill • Assist participants during the cyber drill
System Administrator	• In charge of servers and virtual machines for the cyber drill • Manage the deployment of scenarios to all the participants • Manage and contain the drill activities on the infrastructure provided to the participants • Assist participants during the cyber drill
Mail Administrator	• In charge of email communications for the cyber drill • Help co-ordinate the activities of the participants for the duration of the drill through e-mail communications • Introduce additional scenario elements through e-mail communications during the entire drill • Capture salient points for post drill summation and analysis. • Assist participants during the cyber drill
IRC Administrator	• In charge of IRC communication channel for the cyber drill. • Communicate and co-ordinate the activities of the drill participants to reach a conclusion on the scenarios provided. • Manage scenarios presented during the drill. • Capture salient points for post drill summation and analysis. • Assist participants during the cyber drill

IT and Technical Support	• To develop and support IT infrastructure which involves setting up and dismantling the cyber drill environment for the hardware, software and operating systems • Provide troubleshooting, security and management of all network devices, servers and infrastructure • Assist participants during the cyber drill

Pre-Requisite for Participants

The cyber drill participants are required to bring their own notebooks.

Hardware/Software requirements:

- Notebook with minimum 2GB RAM and wireless card
- Operating system running on Windows XP and above
- Latest web browser (IE, Firefox or Chrome) with flash and Java installed
- Word processing application (MS Words, OpenOffice, AbiWord, etc.)

It is recommended that the participants should have knowledge in the following areas:

- Information gathering
- Log analysis
- Packet analysis

The participants also should be familiar with the following tools:

- Wireshark
- UNIX command

Each participating team must have a minimum of two (2) and a maximum of three (3) representatives to participate in the drill.

Post Drill Activities

All participating teams are to submit a feedback of the drill to the organiser. The feedback form will be provided by the organiser.

The organiser will consolidate the feedback and prepare a post-mortem report.